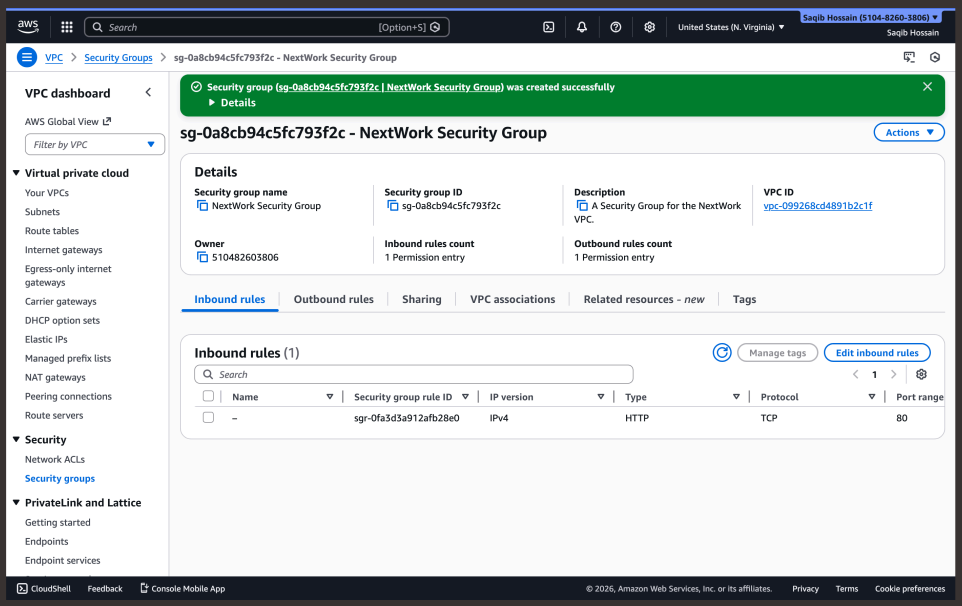
nextwork.org

VPC Traffic Flow and Security

saqibh49@gmail.com




saqibh49@gmail.com
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

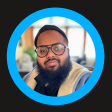
Amazon VPC is a virtual private network in AWS where you can securely launch and manage cloud resources in your own isolated environment, and it is useful because it gives you full control over networking, security, IP addressing, and how your resources connect to the internet and each other.

How I used Amazon VPC in this project

In today’s project, I used Amazon VPC to build security groups, network ACLs, and internet gateways to control traffic flow, protect resources, and enable secure internet connectivity within my cloud network.

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

One thing I didn't expect in this project was there to be so much complexity behind the scenes that so many people dont even realize is there in their everyday lives as they access apps and websites.



saqibh49@gmail.com
NextWork Student

This project took me...

This project took me about an hour

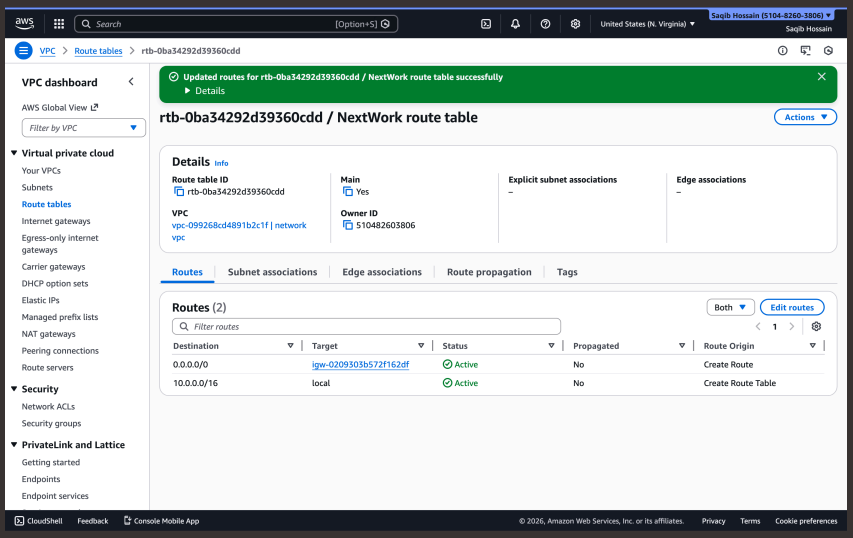
saqibh49@gmail.com
NextWork Student

nextwork.org

Route tables

Route tables are essentially instructions for where to send traffic based on the IP address.

Routes tables are needed to make a subnet public because this is the only way that traffic from the internet can be sent to and from the subnet.

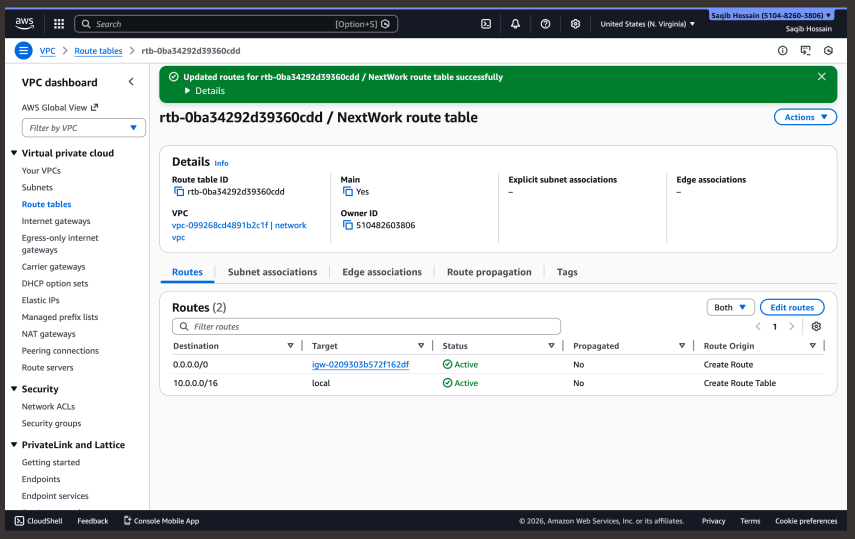


saqibh49@gmail.com
NextWork Student

Route destination and target

Routes are defined by their destination and target, which mean the IP addresses to be passed through that route, and what that route should lead to respectively.

The route in my route table that directed internet-bound traffic to my internet gateway had a destination of 0.0.0/0, which is all IP addresses not specified to be sent elsewhere and a target of my internet gateway.




saqibh49@gmail.com
NextWork Student

Security groups

Security groups are essentially sets of rules that dictate who can and cant access certain resources without a VPC.

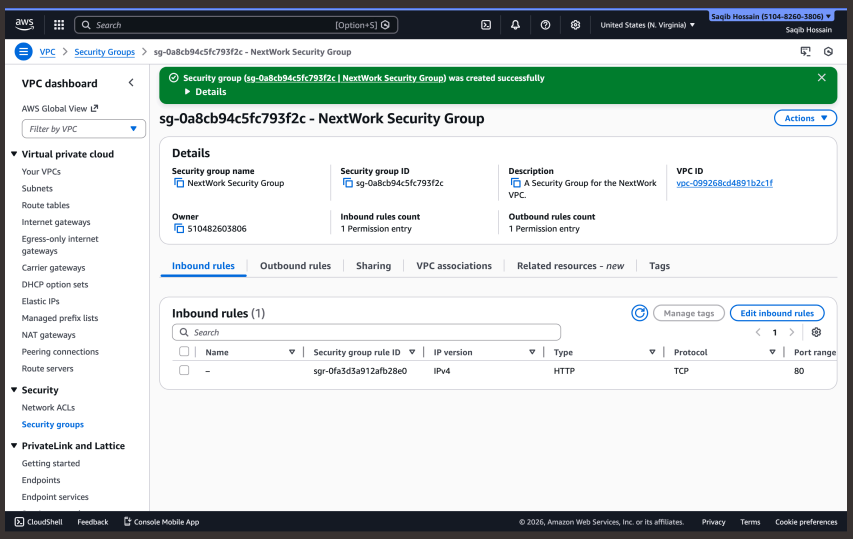
Inbound vs Outbound rules

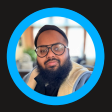
Inbound rules are rules related to which IP addresses are allowed to view a VPC. I configured an inbound rule that allows any IP address coming in from the internet to view my VPC content.

Outbound rules are rules dictating where and what information from the VPC can be sent. By default, my security group's outbound rule is what AWS sets automatically, which allows data to sent anywhere as needed.

saqibh49@gmail.com
NextWork Student

nextwork.org




saqibh49@gmail.com
NextWork Student

Network ACLs

Network ACLs are rules for what can enter and exit a subnet within my VPC.

Security groups vs. network ACLs

The difference between a security group and a network ACL is that security groups are for control over specific resources in a subnet whereas network ACLs are for controlling access to an entire subnet.

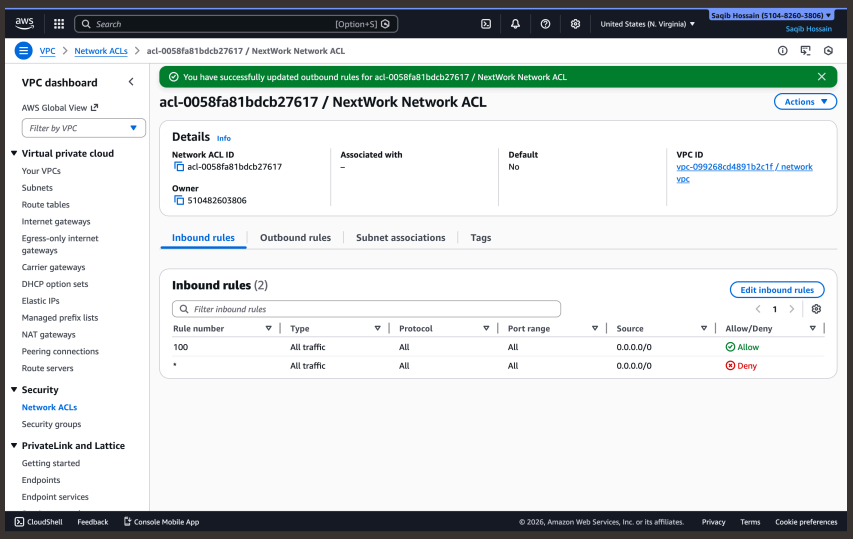
saqibh49@gmail.com
NextWork Student

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 to allow all traffic with a catchall rule that if any traffic doesn't match the first rule that it be denied.

In contrast, a custom ACL’s inbound and outbound rules are automatically set to deny all to give space to add exceptions of what is allowed.




saqibh49@gmail.com
NextWork Student

Tracking VPC Resources

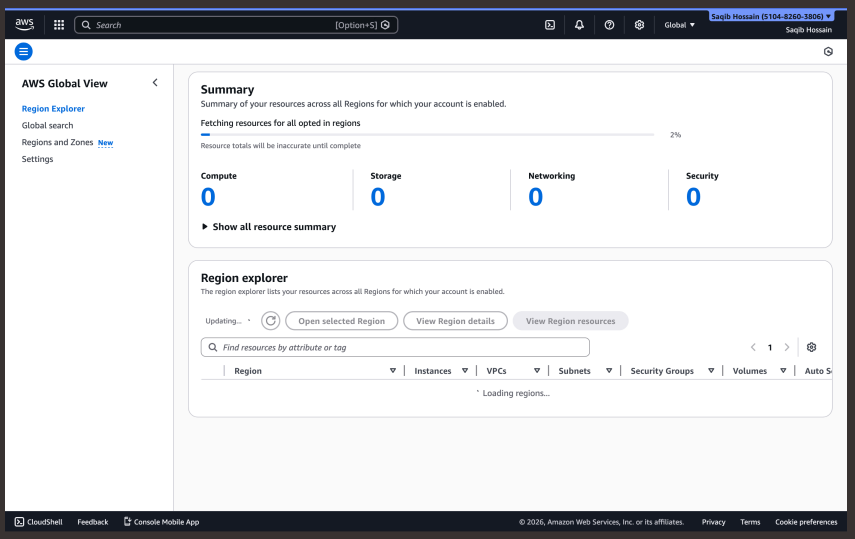
I created an additional VPC, internet gateway and security group Instead of my usual region, I used us-west-1. Teams would use multiple regions to make sure even if one region went down, the resources would still be available in other regions.

EC2 Global View is a tool where you can find all your EC2 resources across regions, I could even narrow down my search by region, resource type, or instance details Without EC2 Global View, you'd have to manually switch between regions to check your resources one at a time.

Now that I’ve learned about EC2 Global View, I’d use it again to quickly monitor, locate, and troubleshoot EC2 resources across multiple regions without having to switch views manually.

saqibh49@gmail.com
NextWork Student

nextwork.org



nextwork.org

The place to learn & showcase your skills

Check out nextwork.org for more projects