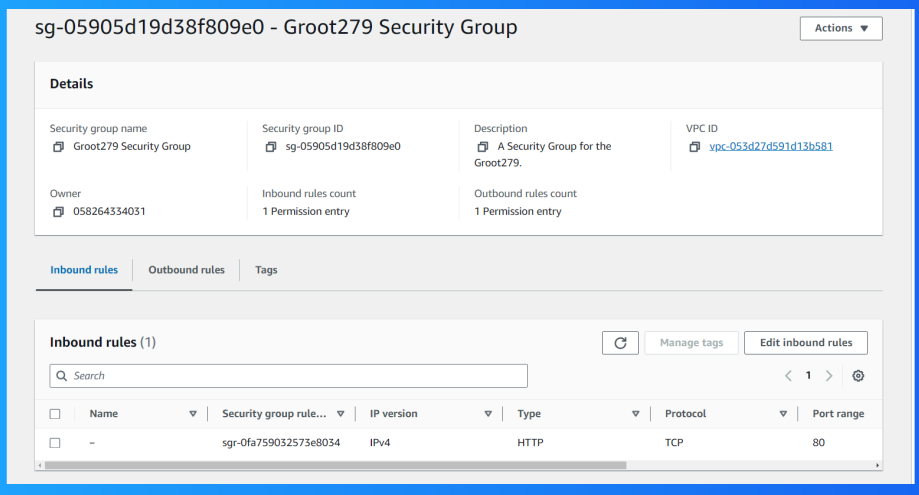
NextWork.org

VPC Traffic Flow and Security

TA tahirgroot@gmail.com



TA
tahirgroot@gmail.com
NextWork Student
NextWork.org

Introducing Today's Project!

What is Amazon VPC?

Amazon Virtual Private Cloud (Amazon VPC) is a virtual network within the AWS cloud that gives you full control over your virtual networking environment. It allows you to create a private, isolated network within the public cloud.

How I used Amazon VPC in this project

Designing VPC architectures based on specific requirements. by creating a route table, create a security group and create a network acl.

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

inbound and outbound traffic

This project took me...

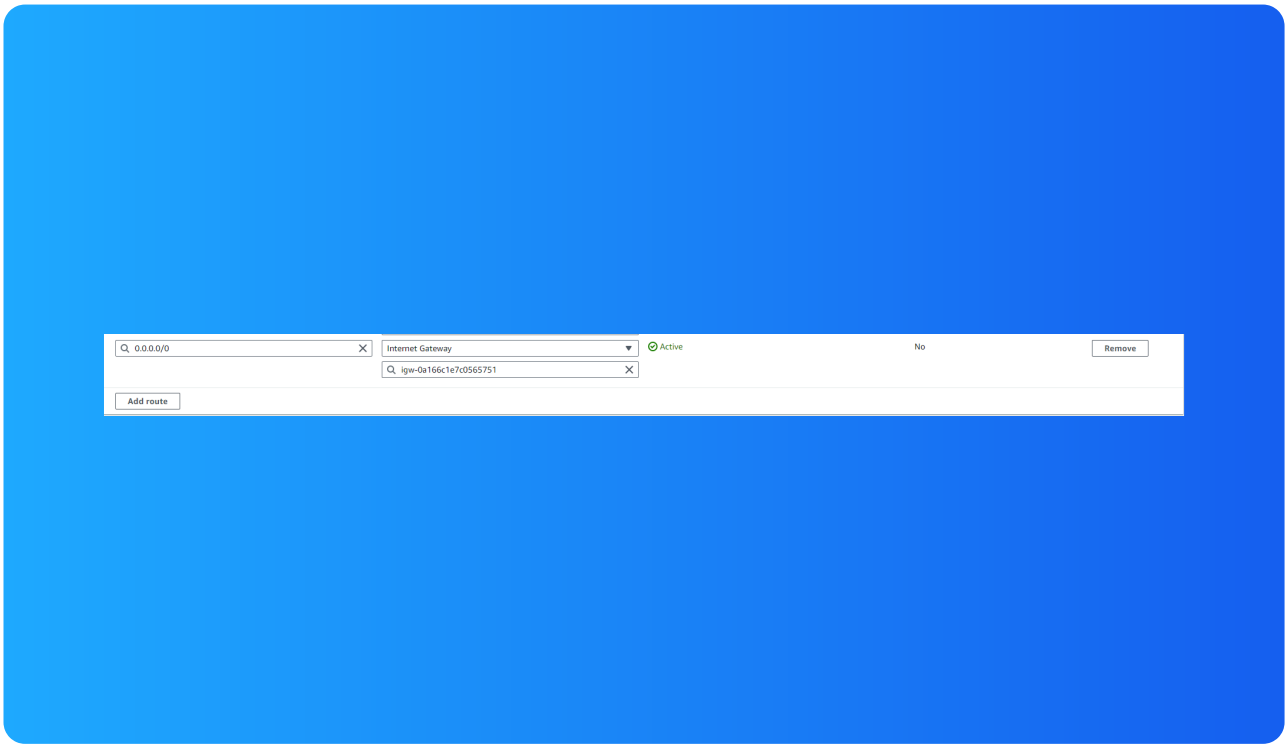
30 minutes

TA
tahirgroot@gmail.com
NextWork Student

Route tables

Route tables are databases used by routers to determine the best path for data packets to their destination, based on network addresses and associated metrics.

Route tables are needed to make a subnet public because they define the path network traffic takes. To access the public internet, a subnet requires a route pointing to an internet gateway within its route table.

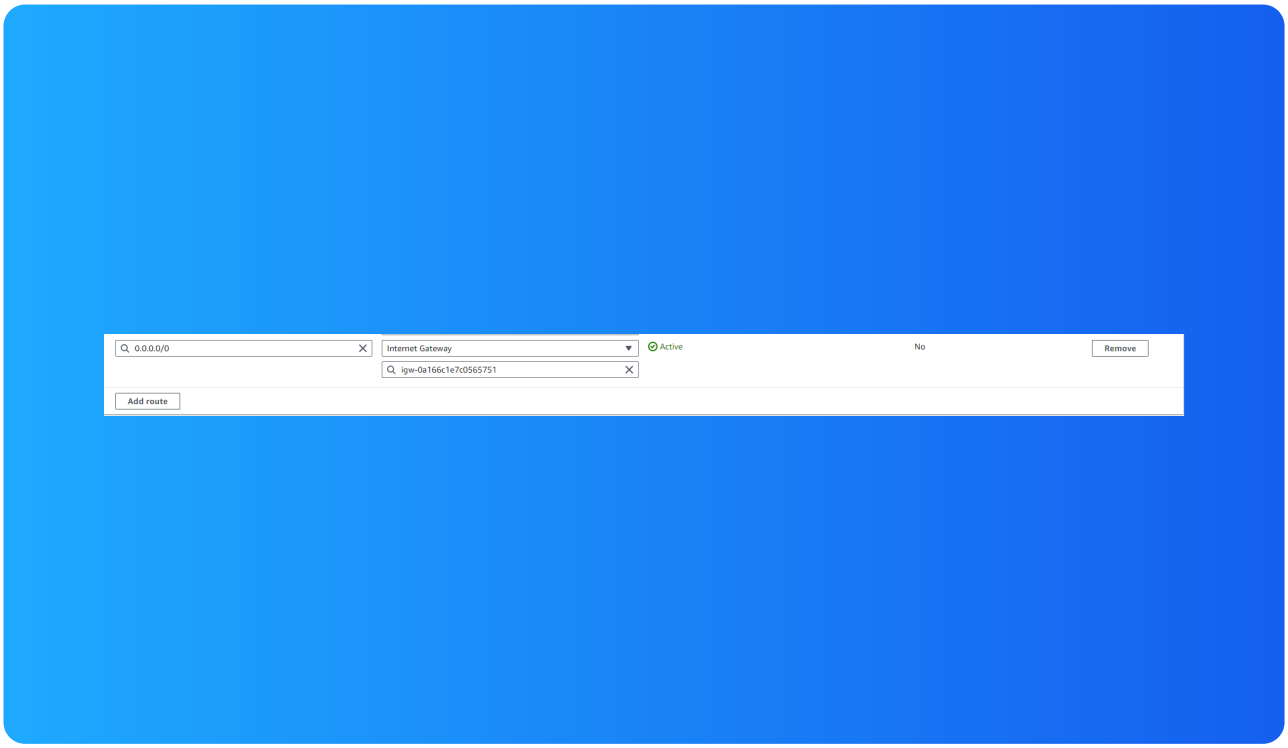


TA
tahirgroot@gmail.com
NextWork Student

Route destination and target

Routes are defined by their destination and target, which mean: Destination: The network address or range of addresses where the traffic is headed Target: The next hop or device where the traffic should be sent to reach 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 and a target of Groot279 IG (Internet Gateway)



TA
tahirgroot@gmail.com
NextWork Student

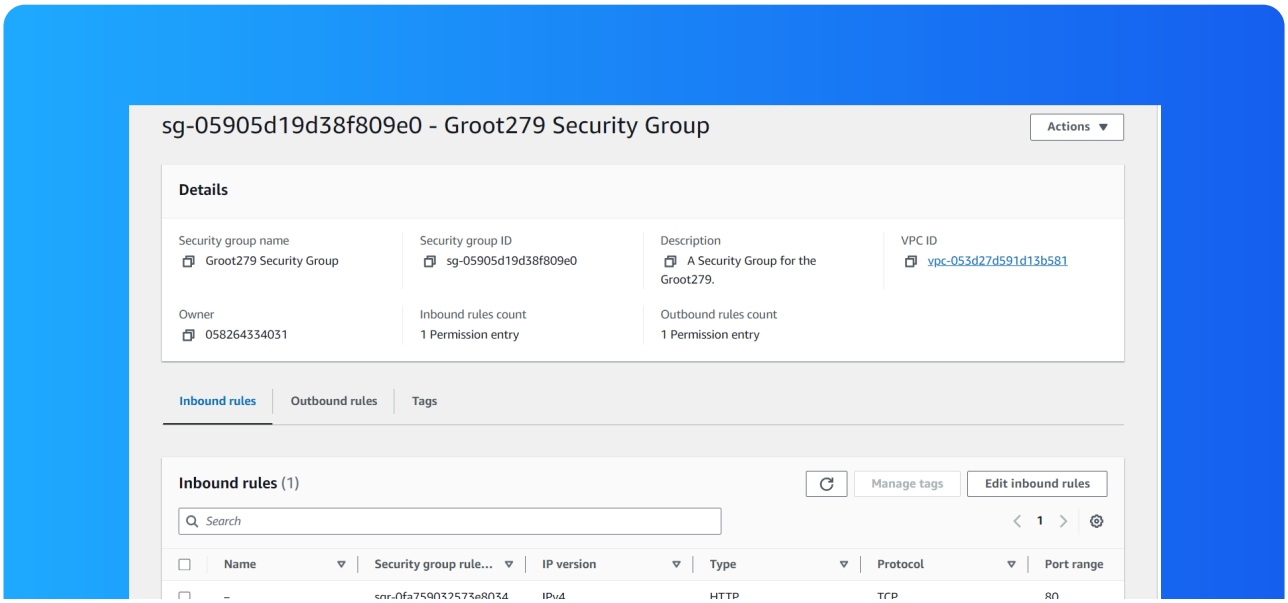
Security groups

Security groups are virtual firewalls that control inbound and outbound traffic at resource level. They act as a barrier, allowing or denying traffic based on specified rules, ensuring only authorized access.

Inbound vs Outbound rules

Inbound rules are permissions that dictate which traffic can enter a resource. They define the source, port, protocol, and allowed traffic. I configured an inbound rule that permits SSH traffic (port 80) from my IP address to enable secure access

Outbound rules are permissions that dictate which traffic can exit an EC2 instance. They define the destination, port, protocol, and allowed traffic. By default, my security group's outbound rule allows all outbound traffic.



TA
tahirgroot@gmail.com
NextWork Student

Network ACLs

Network ACLs are stateful firewalls that control inbound and outbound traffic at the subnet level. They provide an additional layer of security by filtering traffic before it reaches security groups.

Security groups vs. network ACLs

The difference between a security group and a network ACL is that a security group acts as a firewall at the resource level,while a network ACL is a firewall at the subnet level, controlling controlling traffic in and out of entire subnets.

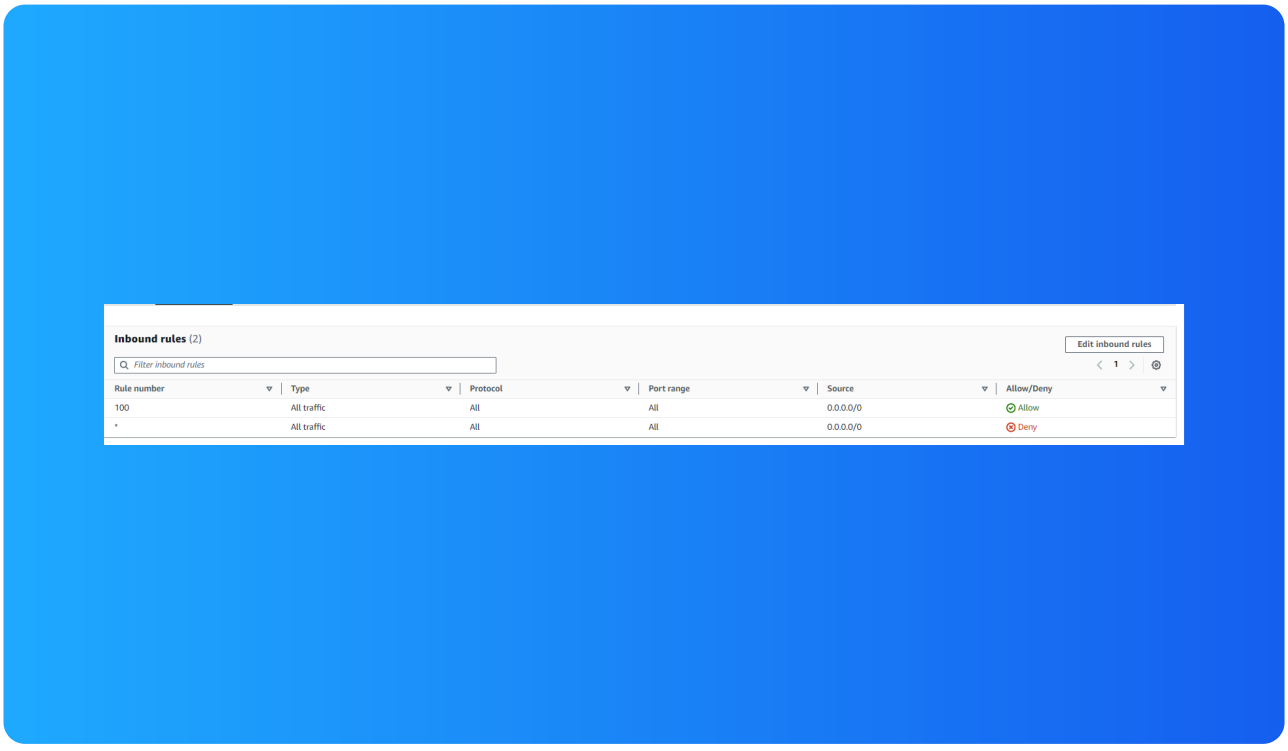
TA
tahirgroot@gmail.com
NextWork Student

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 create a dual layer of security that make sure inbound/outbound traffic go through at least two checks.

In contrast, a custom ACLâ€™s inbound and outbound rules are automatically set to deny all traffic. This means you must explicitly define rules to allow specific traffic, providing granular control over network access



Everyone should be in a job they love.

Check out nextwork.org for more projects