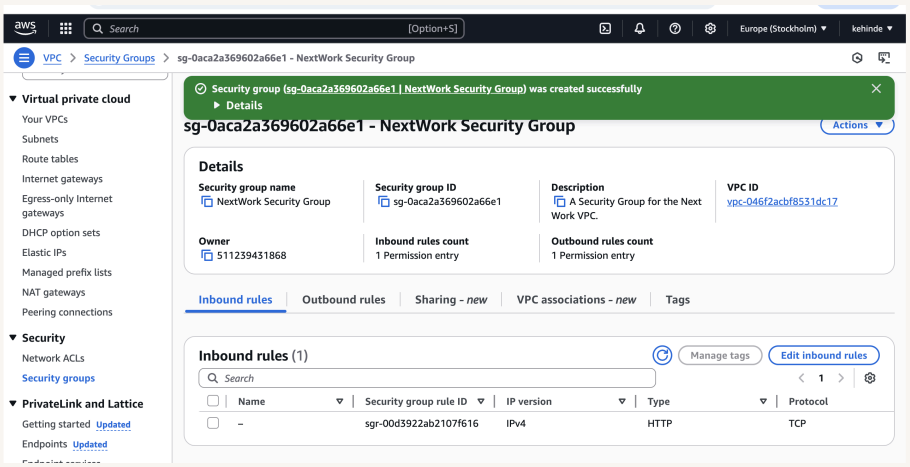
nextwork.org

VPC Traffic Flow and Security

Kehinde Abiuwa



Kehinde Abiuwa
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a customizable virtual network in the AWS cloud that is useful because it gives you full control over networking, security, and connectivity for your cloud resources

How I used Amazon VPC in this project

I created an Amazon VPC and created subnets, route tables and internet gateway, i linked all of them together in the vpc and then created security groups for my resources and network acls for my subnets to control the inbound and outbound traffic flowing in my VPC

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

Nothing really

This project took me...

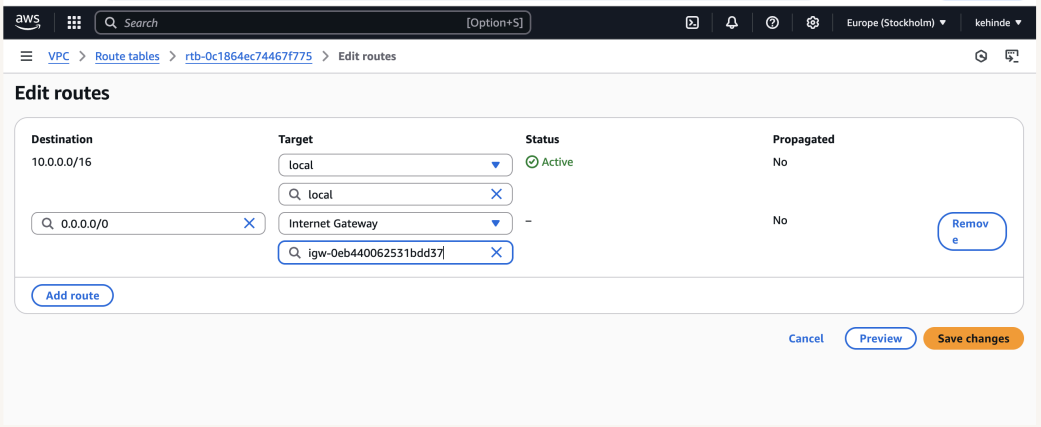
25 mins

Kehinde Abiuwa
NextWork Student

Route tables

Route tables are a set of rules that determines how network traffic is directed within your VPC

Routes tables are needed to make a subnet public because they define how traffic from that subnet can reach the internet

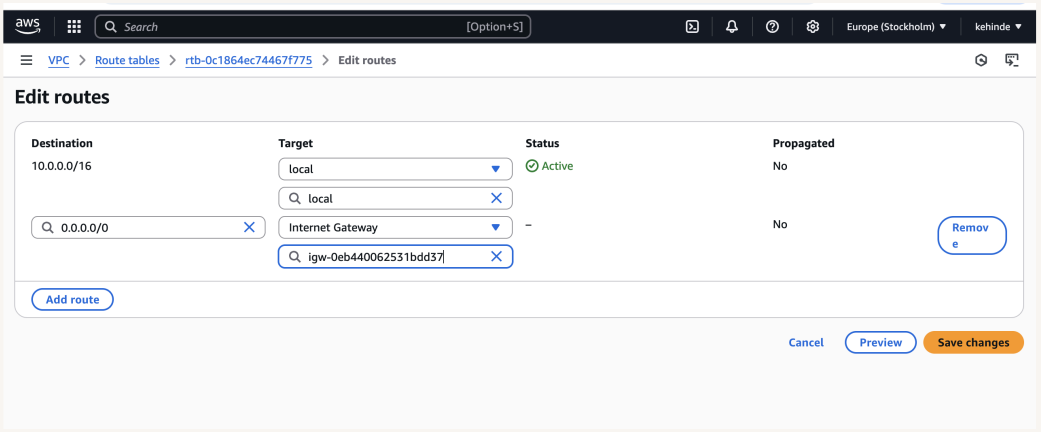


Kehinde Abiuwa
NextWork Student

Route destination and target

Routes are defined by their destination and target, which mean the destination specifies the IP address range of the traffic, and the target specifies where that traffic should be sent, such as an internet gateway

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-0eb440062531bdd37



Kehinde Abiuwa
NextWork Student

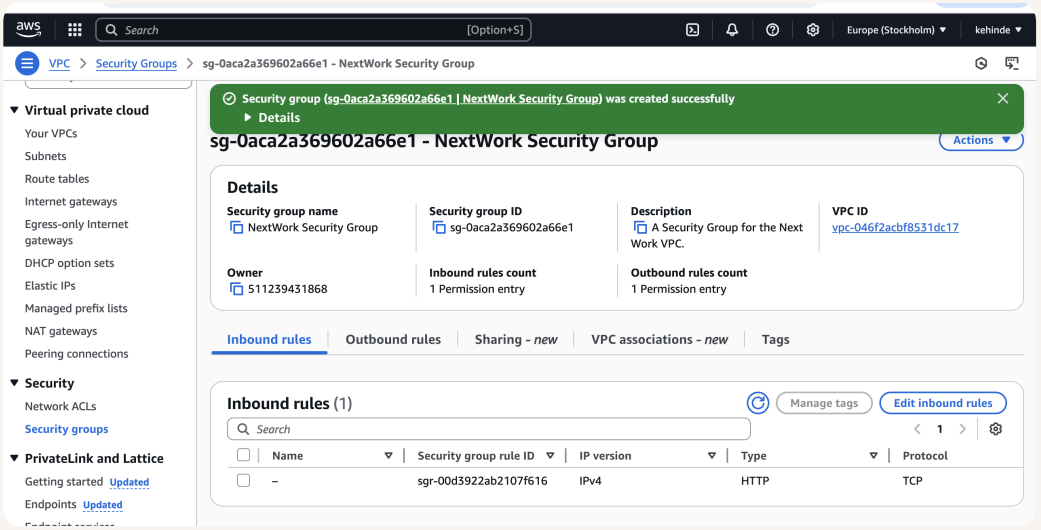
Security groups

Security groups are virtual firewalls that control inbound and outbound traffic for your resources in a VPC (e.g ec2 instances)

Inbound vs Outbound rules

Inbound rules are rules that control the data that can enter the resources in your security group. I configured an inbound rule that allows any IP address to access your resource

Outbound rules are rules that control that data that your resources can send out. By default, my security group's outbound rule allows all outbound traffic


aws
Search
[Option+S]
Europe (Stockholm)
kehinde
VPC > Security Groups > sg-0aca2a369602a66e1 - NextWork Security Group
Security group (sg-0aca2a369602a66e1 | NextWork Security Group) was created successfully
Details
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only Internet gateways
DHCP option sets
Elastic IPs
Managed prefix lists
NAT gateways
Peering connections
Security
Network ACLs
Security groups
PrivateLink and Lattice
Getting started Updated
Endpoints Updated
sg-0aca2a369602a66e1 - NextWork Security Group
Actions
Details
Security group name
NextWork Security Group
Security group ID
sg-0aca2a369602a66e1
Description
A Security Group for the Next Work VPC.
VPC ID
vpc-046f2acbf8531dc17
Owner
511239431868
Inbound rules count
1 Permission entry
Outbound rules count
1 Permission entry
Inbound rules
Outbound rules
Sharing - new
VPC associations - new
Tags
Inbound rules (1)
Manage tags
Edit inbound rules
Search
1
Name
Security group rule ID
IP version
Type
Protocol
–
sgr-00d3922ab2107f616
IPv4
HTTP
TCP

K
Kehinde Abiuwa
NextWork Student

Network ACLs

Network ACLs are used to set broad traffic rules that apply to an entire subnet. For example, blocking incoming traffic from a particular range of IP addresses or denying all outbound traffic to certain ports

Security groups vs. network ACLs

The difference between a security group and a network ACL is that security groups operate at the instance level and allow only specified traffic, while network ACLs operate at the subnet level and allow or deny traffic using stateless rules

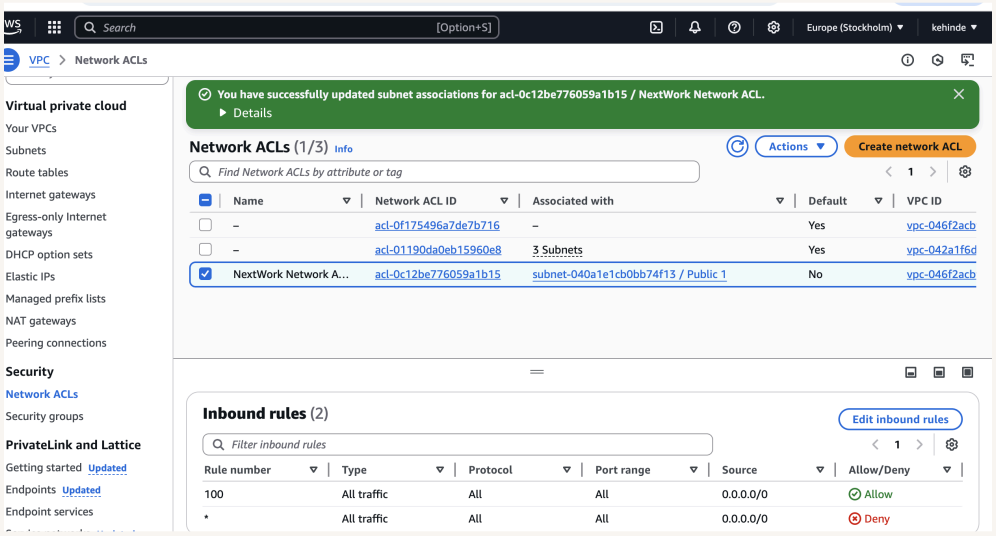
Kehinde Abiuwa
NextWork Student

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 if it's the default ACL, or deny all traffic if it's a custom ACL with no rules defined

In contrast, a custom ACL's inbound and outbound rules are automatically set to deny all traffic until you explicitly add allow or deny rules



The place to learn & showcase your skills

Check out nextwork.org for more projects