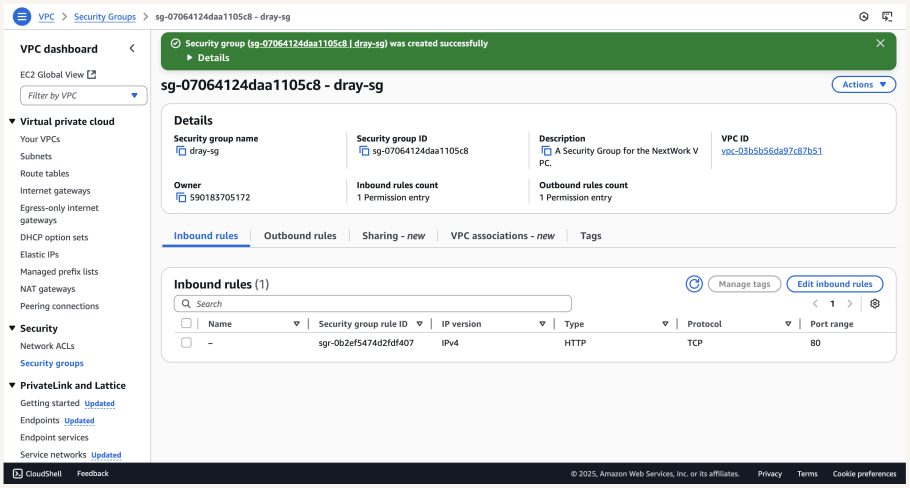
nextwork.org

VPC Traffic Flow and Security

Gaurav Balpande



Gaurav Balpande
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a fundamental networking tool in AWS which help in creating our own private space within the AWS region.

How I used Amazon VPC in this project

In Todays projet, I used Amazon VPC to create route table,security group and network ACL.

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

I am thrilled by knowing the security which aws provide. The data packet has to pass various level to reach and leave the VPC.

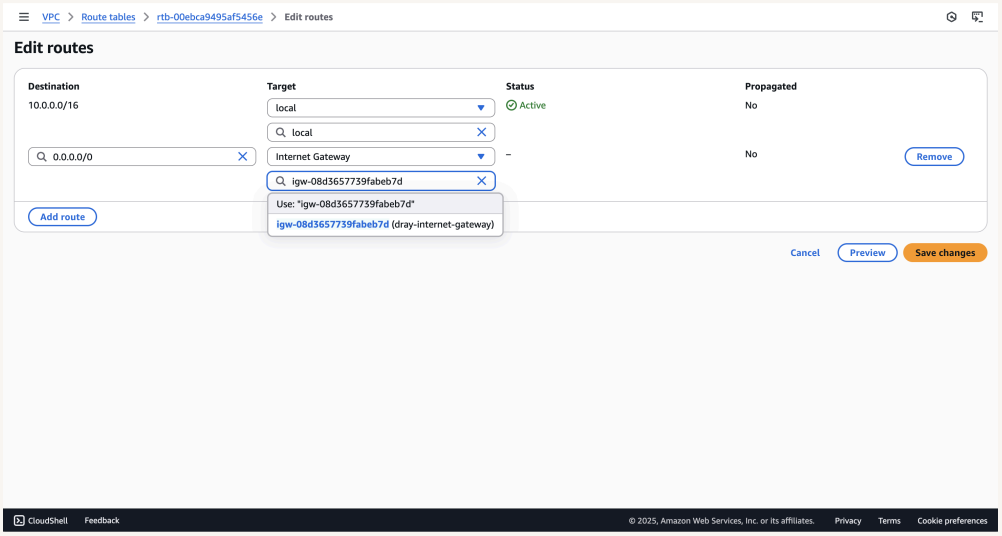
This project took me...

it hardly take 1 hrs as it is a easy project.

Route tables

Route tables are collection of routes which is like a gps for a resources. It help the resources to reach the destination by choosing the target.

Routes tables are needed to make a subnet public because it gives the path to the internet gateway and without Internet gateway it would not be possible to become public.

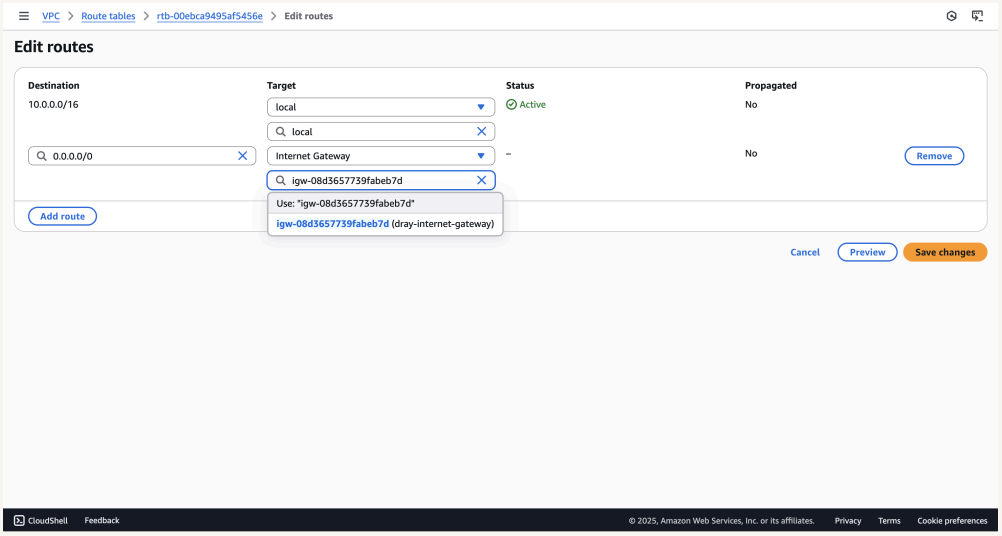


Gaurav Balpande
NextWork Student

Route destination and target

Routes are defined by their destination and target, which mean the location to reach and the path taken to reach the 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 internet gateway we had created.



Gaurav Balpande
NextWork Student

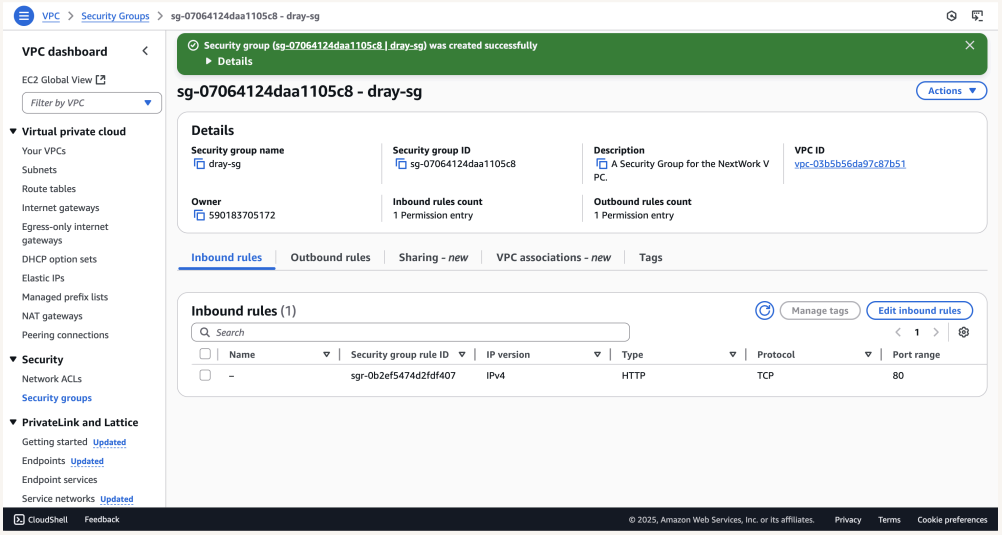
Security groups

Security groups are like a private watchman for each resourcesand work at resource level. It has the responsibilty to allow and deny incoming and outgoing traffic to the resource.

Inbound vs Outbound rules

Inbound rules are the rule which define who are allowed to access the resources I configured an inbound rule that that allow http from any IP address.

Outbound rules are the rules which defined to whon our resouces can access By default, my security group's outbound rule is 0.0.0.0/0


VPC > Security Groups > sg-07064124daa1105c8 - dray-sg
VPC dashboard
EC2 Global View
Filter by VPC
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
Endpoint services
Service networks Updated
Security group (sg-07064124daa1105c8 | dray-sg) was created successfully
Details
sg-07064124daa1105c8 - dray-sg
Actions
Details
Security group name
dray-sg
Security group ID
sg-07064124daa1105c8
Description
A Security Group for the NextWork VPC.
VPC ID
vpc-03b5b56da97c87b51
Owner
590183705172
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
Name
Security group rule ID
IP version
Type
Protocol
Port range
–
sgr-0b2ef5474d2fdf407
IPv4
HTTP
TCP
80
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Gaurav Balpande
NextWork Student

Network ACLs

Network ACLs are defined as Network Access List. It tell at subnet level by allowing or denying the traffic.

Security groups vs. network ACLs

The difference between a security group and a network ACL is that Security group work at resouce level and network ACL work at subnet level.

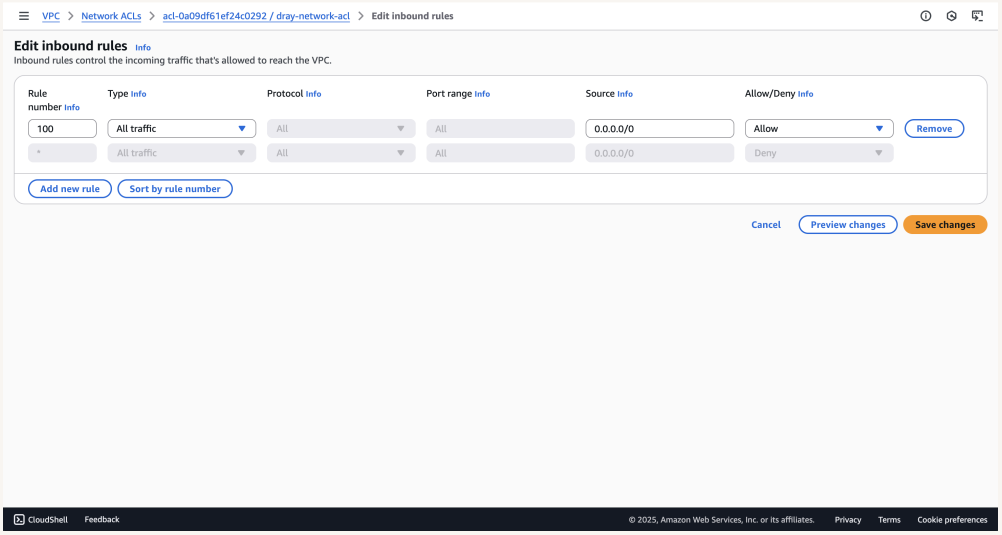
Gaurav Balpande
NextWork Student

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.

In contrast, a custom ACL's inbound and outbound rules are automatically set to deny all traffic which include inbound and outbound.



The place to learn & showcase your skills

Check out nextwork.org for more projects