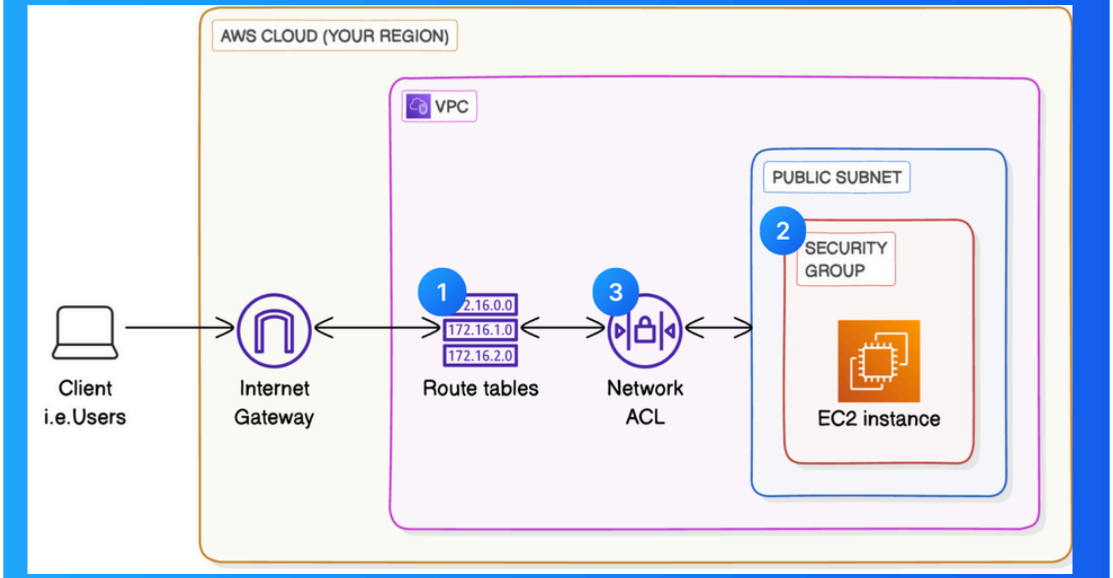
NextWork.org

VPC Traffic Flow and Security

Shridhar Ballal



S

Shridhar Ballal

Introducing Today's Project!

What is Amazon VPC?

Amazon Virtual Private Cloud gives you full control over your virtual networking environment, including resource placement, connectivity, and security. VPCs provide more precise control over the cloud network, which can enhance data and security

How I used Amazon VPC in this project

Intoday's project, I implemented asecure AWS VPC withpublic and private subnets, configured an Internet Gateway and set up Security Groups and Network ACLs for traffic control.

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

it was a challenging and a very exciting project

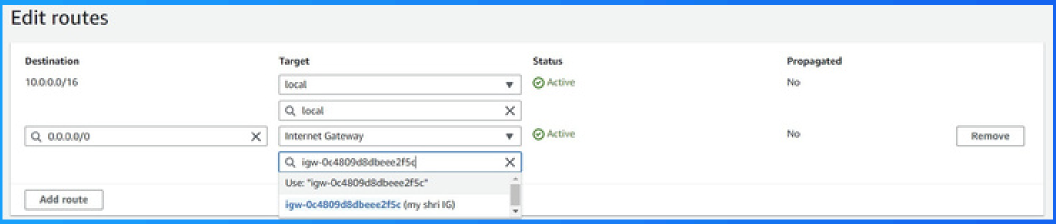
This project took me...

The project took me less than anhour to complete. Documentation took me less than an hour to write as well.

Route tables

'Route tables are like the GPS that directs traffic within my VPC to the correct destination.

Routes tables are needed to make a subnet public because a subnet need to have a route to an internet gateway in order to be considered public. A route table is the only way to establish this connection.



Edit routes

Destination	Target	Status	Propagated	
10.0.0.0/16	local local	Active	No	
0.0.0.0/0	Internet Gateway igw-0c4809d8dbeee2f5c	Active	No	Remove

Use: "igw-0c4809d8dbeee2f5c"

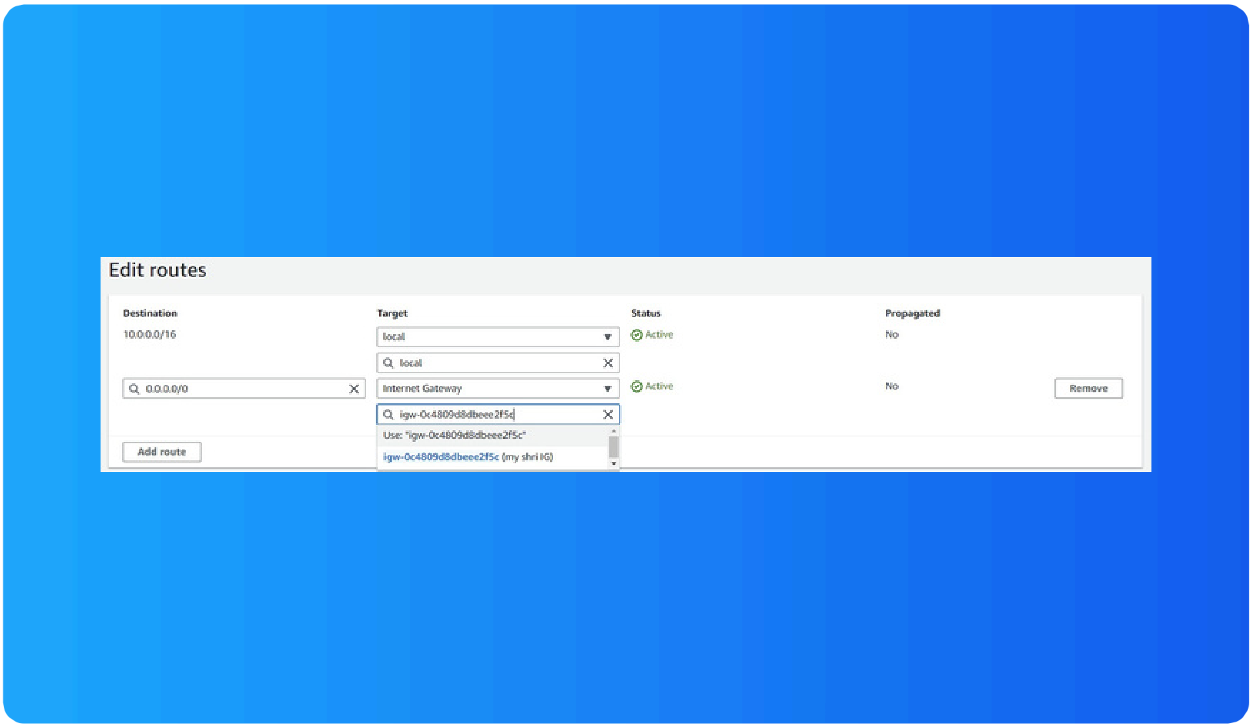
igw-0c4809d8dbeee2f5c (my shri IG)

Shridhar Ballal

Route destination and target

Routes are defined by their destination and target, which mean The destination is the range of IP addresses that traffic in my VPC is trying to reach. The target is the road/path that the traffic will use to get to their 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 my shri IG (internet gateway)



Edit routes

Destination	Target	Status	Propagated	
10.0.0.0/16	local local	Active	No	
0.0.0.0/0	Internet Gateway igw-0c4809d8dbeee2f5c	Active	No	Remove

Use: "igw-0c4809d8dbeee2f5c"

igw-0c4809d8dbeee2f5c (my shri IG)

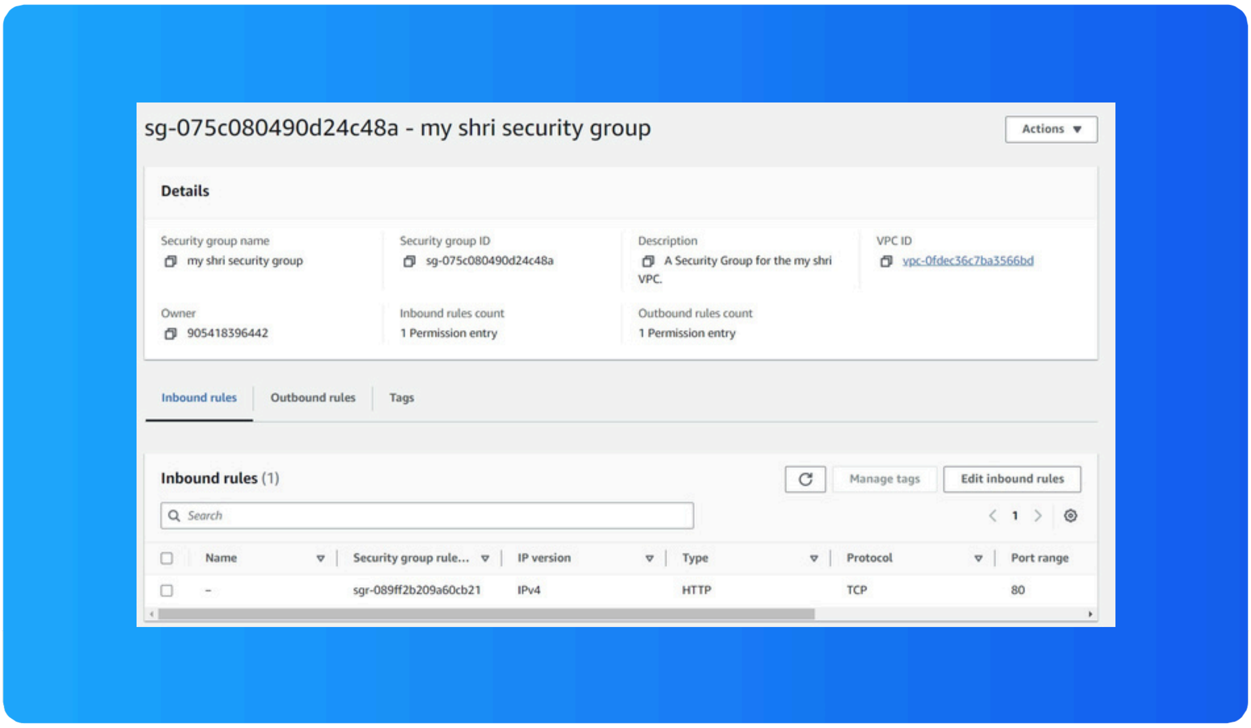
Security groups

Security groups are like security guards that monitor both inbound and outbound traffic at the resource level i.e. every single resource in a subnet /VPC has a security group.

Inbound vs Outbound rules

Inbound rules are the rules that monitor/restrict inbound traffic e.g. users visiting a web app I'm hosting I configured an inbound rule that allow all inbound HTTP traffic.

Outbound rules are rule that monitor/restrict outbound traffic e.g. my web app requesting data from a public source. By default, my security group's outbound rule will allow all outbound traffic



sg-075c080490d24c48a - my shri security group

Details

Security group name: my shri security group

Security group ID: sg-075c080490d24c48a

Description: A Security Group for the my shri VPC.

VPC ID: vpc-0fdec36c7ba3566bd

Owner: 905418396442

Inbound rules count: 1 Permission entry

Outbound rules count: 1 Permission entry

Inbound rules (1)

□	Name	Security group rule...	IP version	Type	Protocol	Port range
□	-	sgr-089ff2b209a60cb21	IPv4	HTTP	TCP	80

Shridhar Ballal

Network ACLs

Network ACLs are like community watchmen that secures my network at a subnet level.

Security groups vs. network ACLs

The difference between a security group and a network ACL is that a scope i.e. a security group secure my network at the resource level , while network ACLS secures my network at the subnet level.

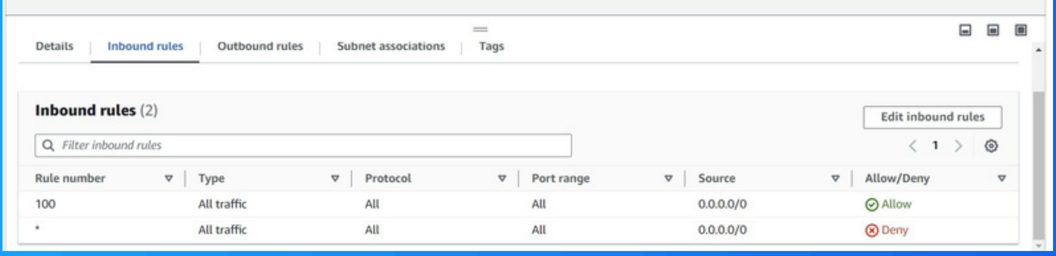
Shridhar Ballal

Default vs Custom Network ACLs

Similar to security groups, network ACLs use inbound and outbound rules

Bydefault,a network ACL'sinbound andoutbound rules willIt isat aSubnet level and has separate inbound and outbound rules, and each rule can either allow or deny traffic.

In contrast, a custom ACL̓s’ inbound and outbound rules are automatically set to deny all incoming/outgoing traffic.



Inbound rules (2)

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	✓ Allow
*	All traffic	All	All	0.0.0.0/0	⊗ Deny