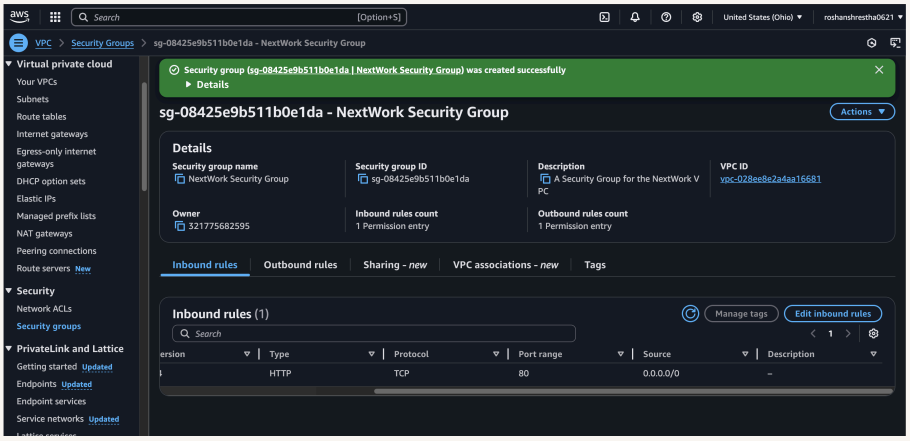
nextwork.org

VPC Traffic Flow and Security

Roshan Shrestha



R
Roshan Shrestha
NextWork Student

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a service provided by AWS that allows us to create a logically isolated section of the AWS cloud, where we can launch and manage resources in a secure and controlled environment.

How I used Amazon VPC in this project

I used Amazon VPC in this project to add a security group to my resource within a subnet in a VPC and also a network ACL to the subnet. I also created a route table that directs traffic from the internet gateway to the resoures in the subnet.

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

The various security layers for a resource inside a subnet in a VPC.

This project took me...

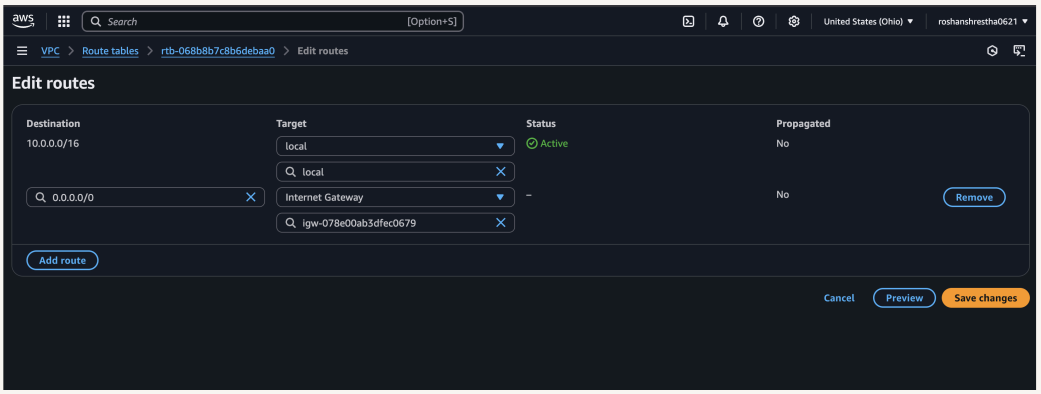
About an hour.

Roshan Shrestha
NextWork Student

Route tables

Route tables are a table of rules, called routes that decide where data in the network should go. Like GPS/Maps for data. Every subnet in your VPC needs to be linked to a route table, because the table tells your subnet's traffic where to travel to.

Routes tables are needed to make a subnet public because the routes direct the resources within the subnet to the internet via the internet gateway.

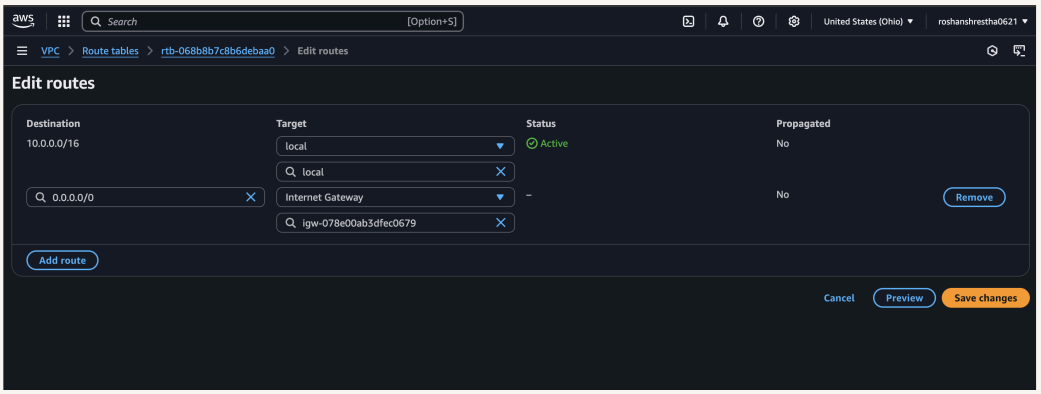


Roshan Shrestha
NextWork Student

Route destination and target

Routes are defined by their destination and target, which mean the ip address range that the traffic wants to reach and the road or path the traffic will have to take to get to its destination respectively.

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-078e00ab3dfec0679



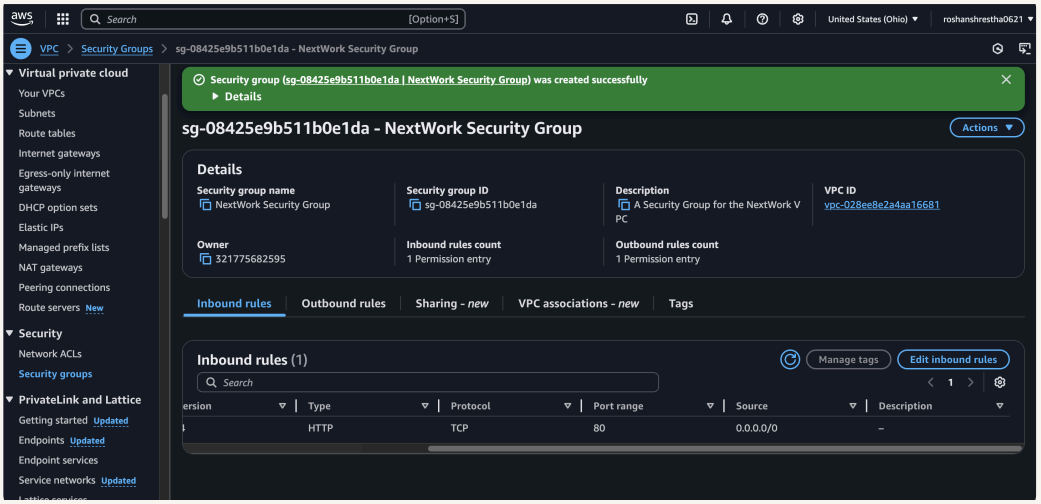
Security groups

Security groups are like guards to resources within a subnet inside a VPC. Every resource must be associated with a security group. If a resource is launced without a security group, AWS associates it to the default security group created for the VPC

Inbound vs Outbound rules

Inbound rules are rules that control the data that can enter the resources within a security group. I configured an inbound rule that set source as 0.0.0.0/0 and allows any IP address to access my resources in the public subnet

Outbound rules are rules that control the data that your resources can send out. eg. email, request data from other service. By default, my security group's outbound rule allows all outbound traffic unless specified otherwise.


aws
Search
[Option+S]
United States (Ohio)
roshanshrestha0621
VPC > Security Groups > sg-08425e9b511b0e1da - NextWork Security Group
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
Route servers New
Security
Network ACLs
Security groups
PrivateLink and Lattice
Getting started Updated
Endpoints Updated
Endpoint services
Service networks Updated
Security group (sg-08425e9b511b0e1da | NextWork Security Group) was created successfully
Details
sg-08425e9b511b0e1da - NextWork Security Group
Actions
Details
Security group name
NextWork Security Group
Security group ID
sg-08425e9b511b0e1da
Description
A Security Group for the NextWork VPC
VPC ID
vpc-028ee8e2a4aa16681
Owner
321775682595
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)
Search
Manage tags
Edit inbound rules
1
ersion
Type
Protocol
Port range
Source
Description
HTTP
TCP
80
0.0.0.0/0
–

R
Roshan Shrestha
NextWork Student

Network ACLs

Network ACLs are broad traffic rules that apply to an entire subnet. One ACL per subnet. They check each data packet against a table of ACL rules before allowing them through.

Security groups vs. network ACLs

The difference between a security group and a network ACL is that security groups allow granular control managing access to each individual resource while a network ACL applies to an entire subnet.

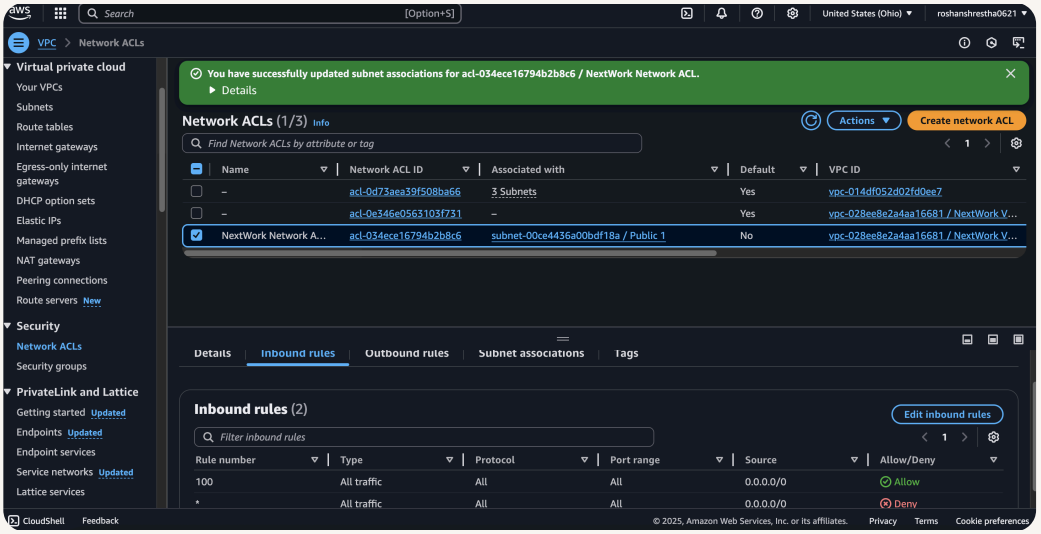
Roshan Shrestha
NextWork Student

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 inbound and outbound traffic.

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



The place to learn & showcase your skills

Check out nextwork.org for more projects