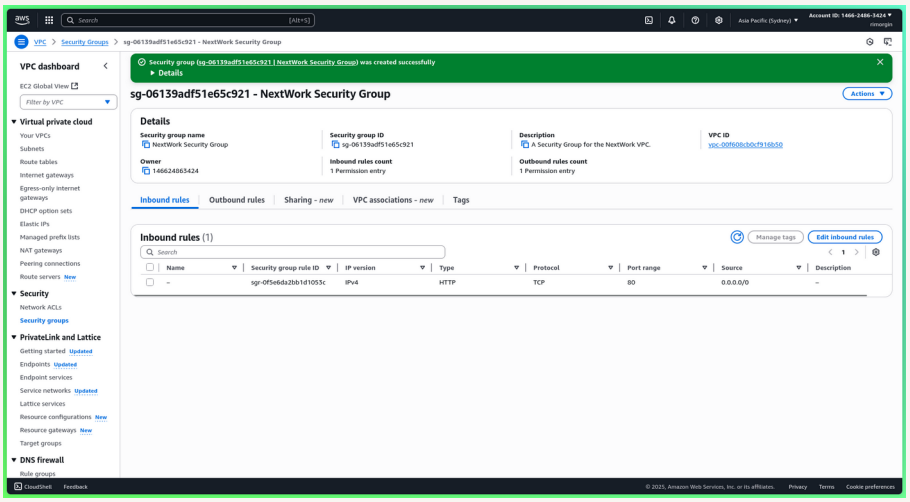
nextwork.org

VPC Traffic Flow and Security

Sean Calderon



Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is a useful for providing granularity and streamlined management of virtual networks in the cloud. It is useful in a way you create networks, segment the network with subnets and group resources according to what's the best fit for you.

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to create a streamlined flow of ingress and egress traffic with routing table and without defining a strict rules on network ACLs nor on security groups.

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

One thing I didn't expect in this project was setting up both network ACLs and security groups at the same time.

This project took me...

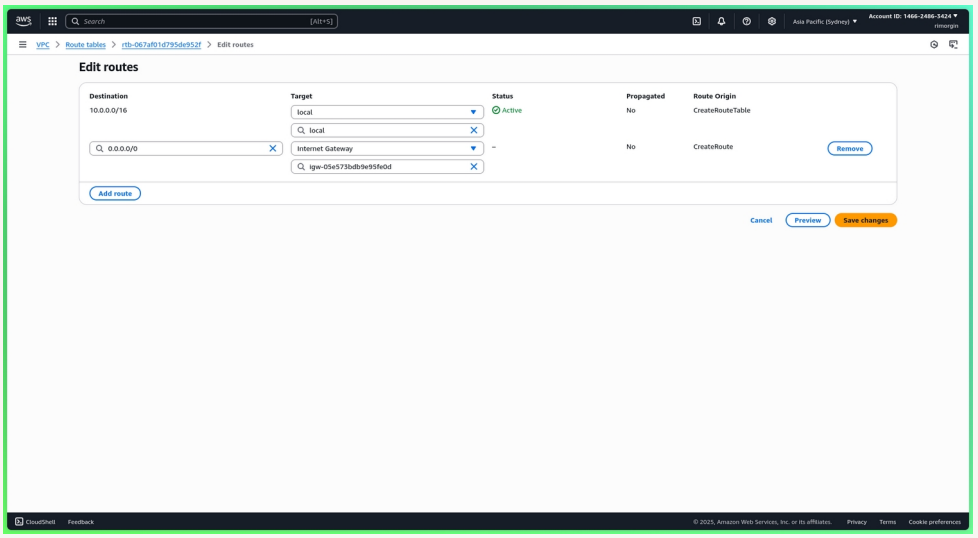
This project took me 40 minutes. It was rewarding to understand the flow of traffic when it first arrive at Internet Gateway, then forwards to the VPC, all the way to route tables, network ACLs , security groups, and down to the resource itself.


Sean Calderon
NextWork Student

Route tables

Route tables are table of rules that define how traffic flow is routed within VPC or to the internet.

Route tables are needed to make a subnet public because routing table serves as a local gateway or router that instructs traffic flows within VPC or rather directs traffic to internet via internet gateway.

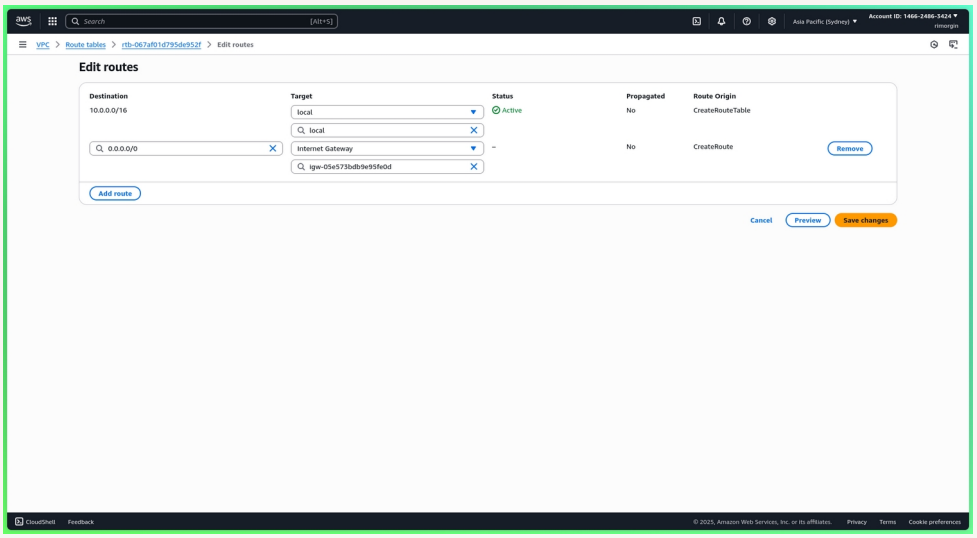



Sean Calderon
NextWork Student

Route destination and target

Routes are defined by their destination and target, which means an instruction of traffic flow coming from a destination traffic going to the target. The target is where the destination traffic will be directed/routed to.

The route in my route table that directed internet-bound traffic to my internet gateway had a destination of 0.0.0.0/0 which means any ip address and a target of internet gateway...



Security groups

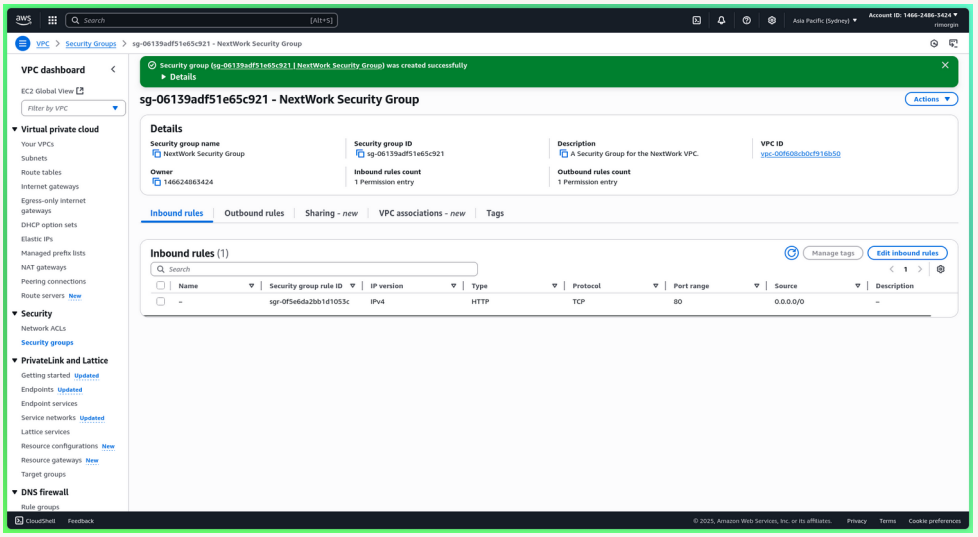
Security groups are attached to resources to control traffic going in or out of the resources. This is more useful when you want to control traffic e.g from EC2 instances going to another EC2 instances that resides on the same subnet.

Inbound vs Outbound rules

Inbound rules are for defining ingress traffic or traffic going in. By default, my custom security group's inbound rule is deny all traffic and I configured it to accepts any kind of traffic for simplicity.

Outbound rules are for defining egress traffic or traffic going out. By default, my custom security group's outbound rule is deny all traffic and I configured it to allow any kinds of traffic for simplicity.

Sean Calderon
NextWork Student



Network ACLs

Network ACLs define strict control policies or rules in sequence, the lower the sequence number takes precedence over higher sequence number. NACLs are checkpoints that checks what traffic permits or denies on the entire subnet scope.

Security groups vs. network ACLs

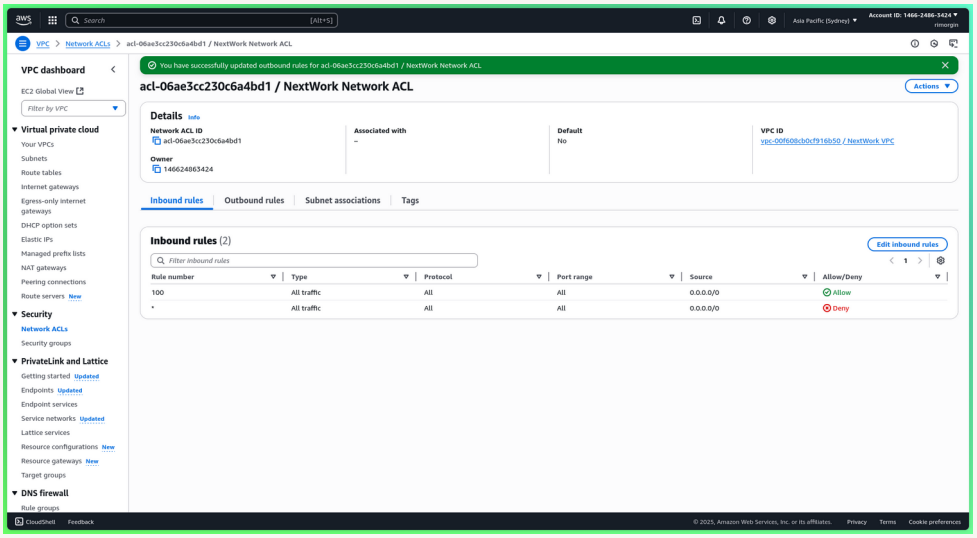
The difference between a security group and a network ACL is that SG is strictly confined to per resources control only which is more granular, while network ACLs are declared on the entire subnet and controls traffic in more wider scope.

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 permit any kinds of traffic.

In contrast, a custom ACL’s inbound and outbound rules are automatically set to deny any kinds of traffic.



The place to learn & showcase your skills

Check out nextwork.org for more projects