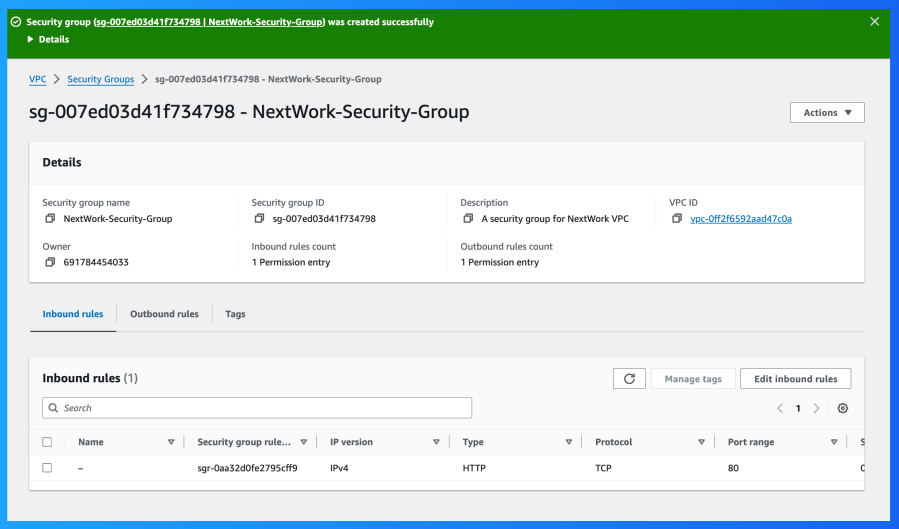
NextWork.org

VPC Traffic Flow and Security

Juncheng Wang



Juncheng Wang
NextWork Student

NextWork.org

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC enables you to build a virtual network in the AWS cloud. You can define your own network space by controling how your network and the Amazon EC2 resources inside your network are communicating to the internet.

How I used Amazon VPC in this project

I set up a security group for my resource in the subnet and a network ACL for my subnet.

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

There are more layer of security options than I thought.

This project took me...

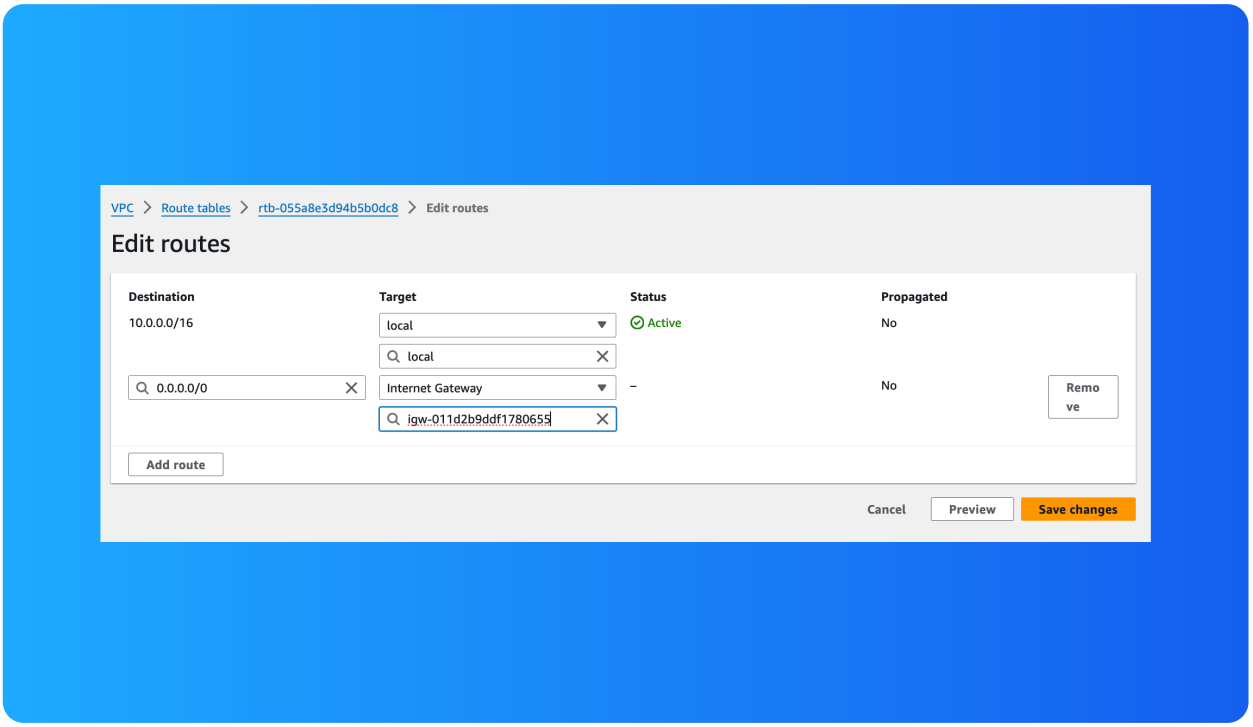
1 hour

Juncheng Wang
NextWork Student

Route tables

A route table contains a set of rules, called routes, that determine where network traffic from your subnet or gateway is directed.

Routes tables are needed to make a subnet public because route table acting like a GPS telling the resources in your subnet where to go. Without it, the resources wouldn't know where to send or receive data.

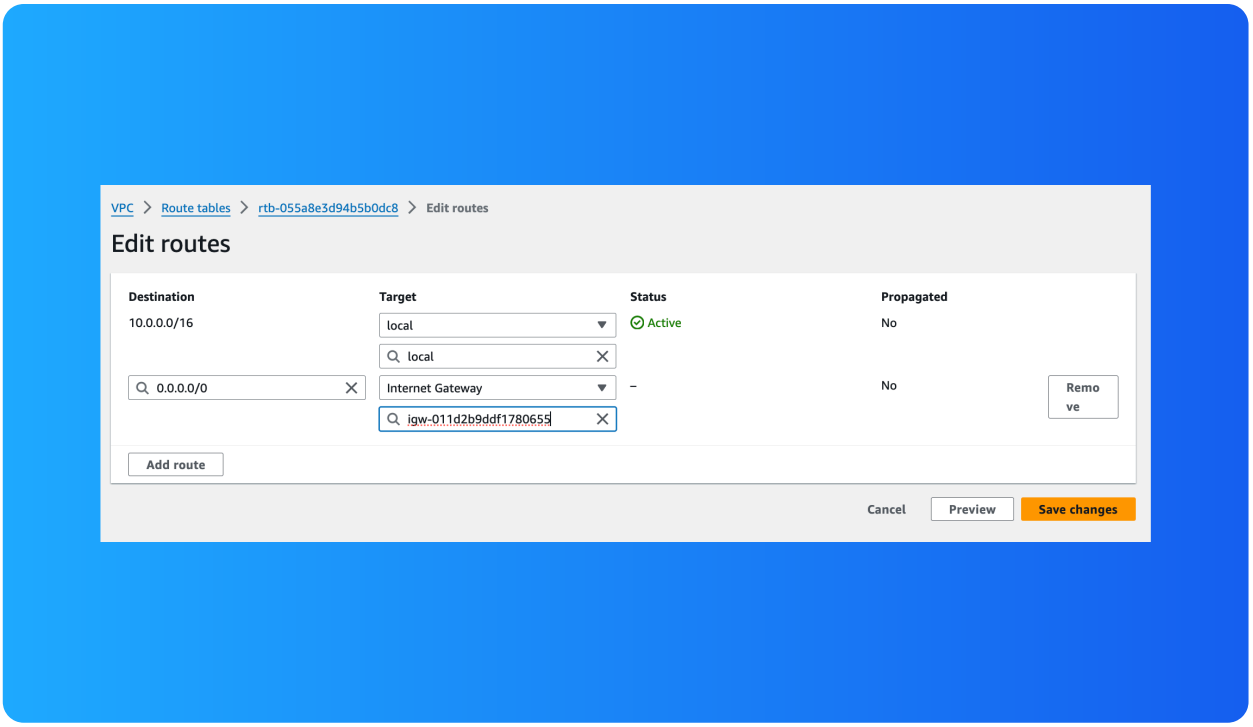


Juncheng Wang
NextWork Student

Route destination and target

Routes are defined by their destination and target, which means the destination is The IP address range that traffic wants to reach and the target is the road or path that the traffic will have to take to get to its destination.

The route in my route table that directed internet-bound traffic to my internet gateway had a destination of 10.0.0.0/16 and a target of local, as well as 0.0.0.0/0 and a target of internet gateway.



Juncheng Wang
NextWork Student

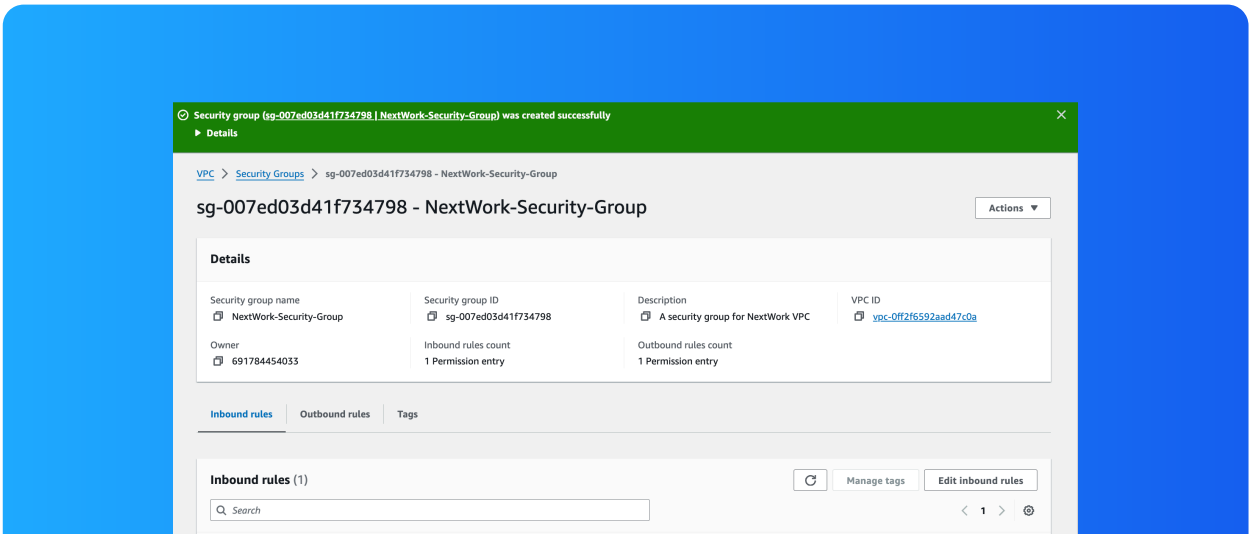
Security groups

Security group is like a security guard, at the entrance of each resource in the subnet. It has strict rules about what kind of traffic can enter or leave the resource based on its IP address, protocols and port numbers.

Inbound vs Outbound rules

Inbound rules are rules that control the data that can enter the resources in your security group such as visitors to your website and receive form submissions. I configured an inbound rule that allows any IP address to access my resource.

Outbound rules control what data your resources can send out, such as server requests data from another service, and sends out an email notification. My security group's outbound rule has allowed all outbound traffic by default.



Juncheng Wang
NextWork Student

NextWork.org

Network ACLs

Network ACLs are network access control lists that act as an optional layer of security that acts as a firewall for controlling traffic in and out of a subnet. A subnet can be associated with only one network ACL at a time.

Security groups vs. network ACLs

The difference between a security group and a network ACL is that the security group is acting at the resource level in the subnet while ACL act at the subnet level.

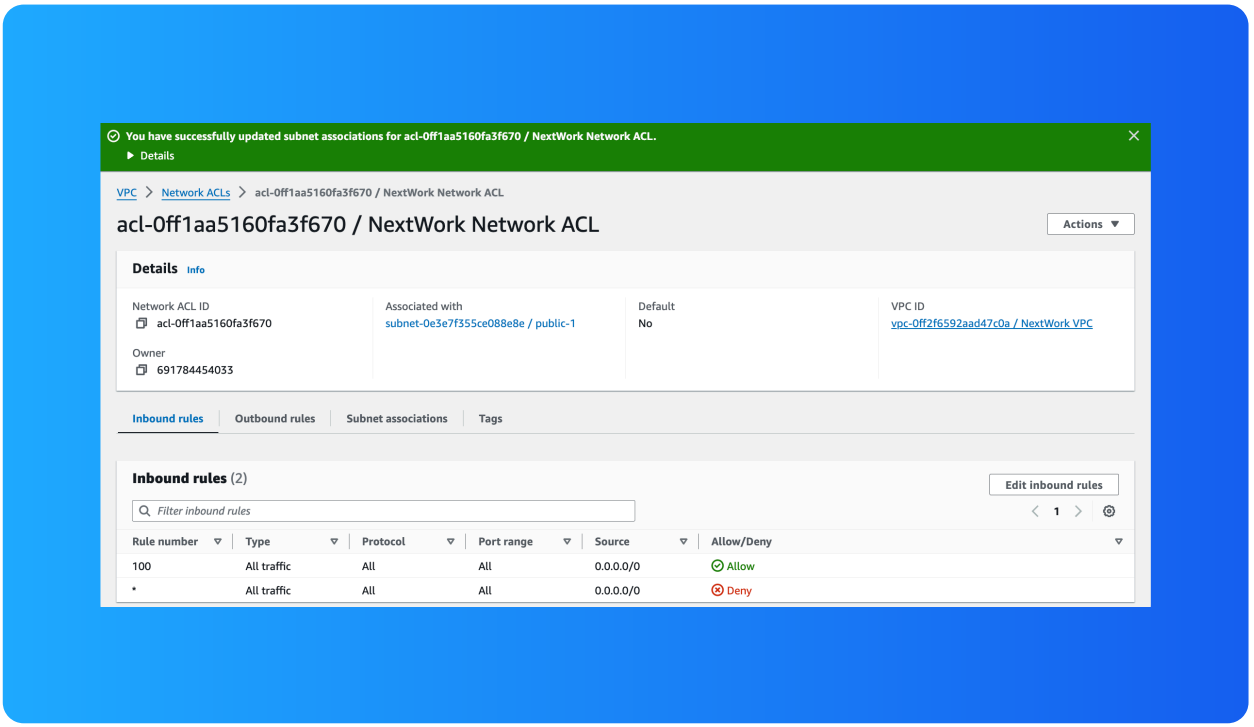
Juncheng Wang
NextWork Student

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 deny all inbound and outbound traffic.



Everyone should be in a job they love.

Check out nextwork.org for more projects