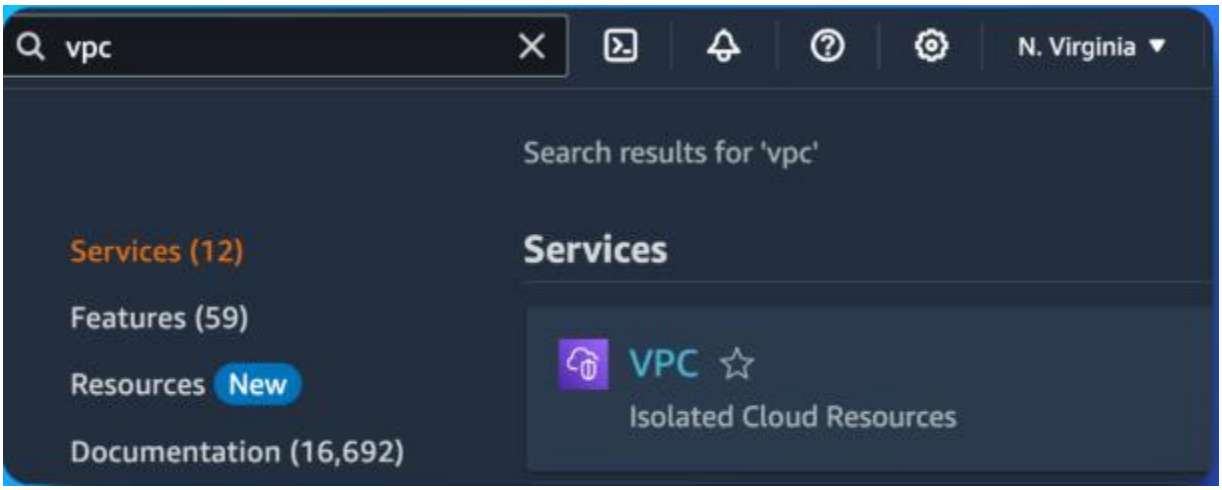
BUILDING A VIRTUAL PRIVATE CLOUD (VPC)

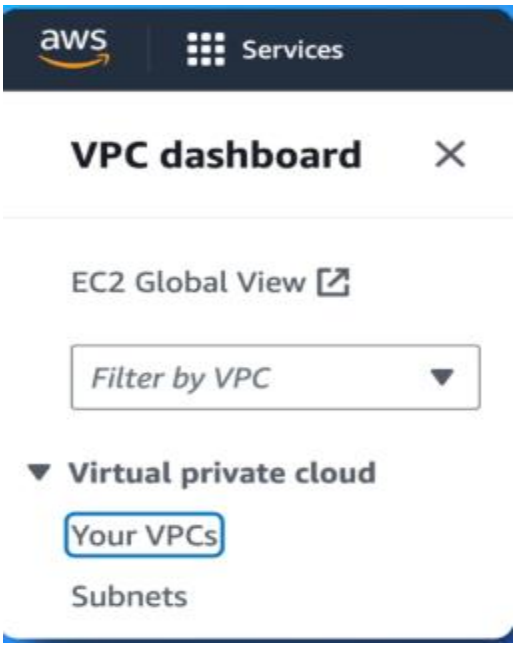
VPCs are logically isolated network in the cloud. You can think of it as a custom-made virtual network where you decide who gets in, who gets out and how everything connects. Amazon VPC is a service that allows you create a private network in the AWS cloud. It is useful as it is secure, flexible, integrates well with other services and gives you a customizable environment to run applications in the cloud.

➢ CREATE A VPC

- In the **AWS Management Console** search field, type VPC.
- Select **VPC** from the drop down menu.

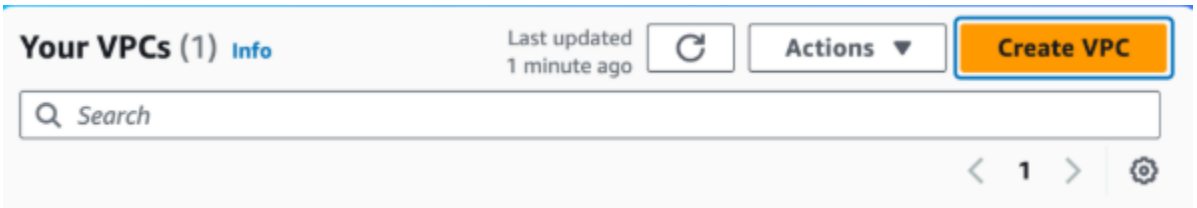


- In the left navigation pane, choose **Your VPCs**.



VPCs are the reason why resources can be made private to you. You also get control over resources in a VPC, so you can organize how they communicate and integrate with each other without the public internet. You'll notice that there is already a VPC in your account. This is because when you create your AWS account, AWS automatically sets up a default VPC for you!

- Choose **Create VPC**.

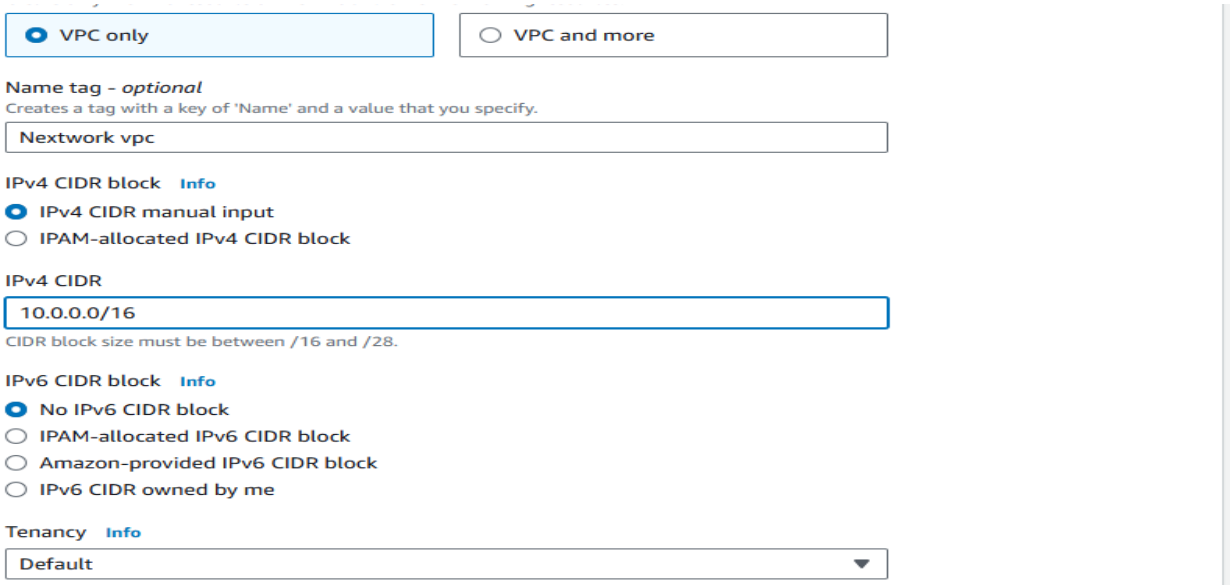


- Choose **VPC Only**.
- **Name tag:** NextWork VPC
- **IPv4 CIDR:** 10.0.0.0/16

An IP address is like a unique street address or coordinates for the resources in your VPC. Your resources would use IP addresses to identify other resources and communicate/exchange data.

IPv4 stands for Internet Protocol version 4, which is the most common way to write an IP address. IPv4 addresses are written as four sets of numbers separated by dots (e.g., 192.168.0.1).Each number between the dots ranges between 0 and 255. This means IP addresses start from 0.0.0.0 and go all the way to 255.255.255.255. In general, two devices cannot share the same IPv4 address in the same network e.g. within the same VPC.

CIDR (which stands for Classless Inter-Domain Routing) is a way to assign a whole block of IP addresses, kind of like creating a zone/area in a city. For example, 10.0.0.0/16 means the first 16 bits of your IP address (10.0) are fixed, but the remaining 16 bits (i.e. the second half of the IP address) can be allocated however you like. Addresses within this CIDR block start at 10.0.0.0 and go up to 10.0.255.255.

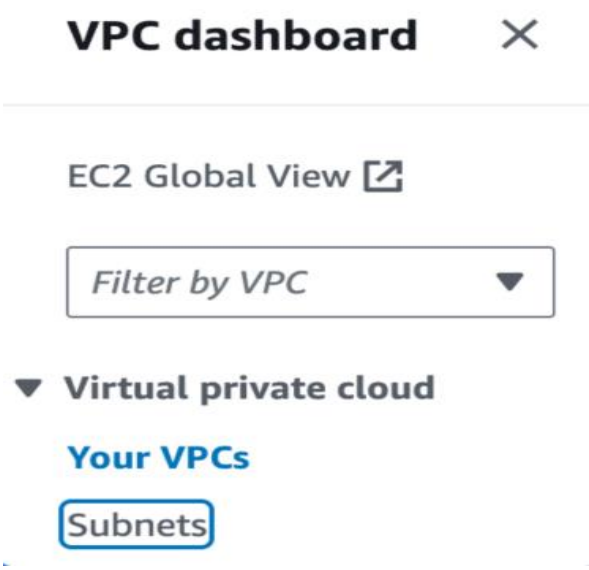


- Select **Create VPC** to finish setting up your VPC.

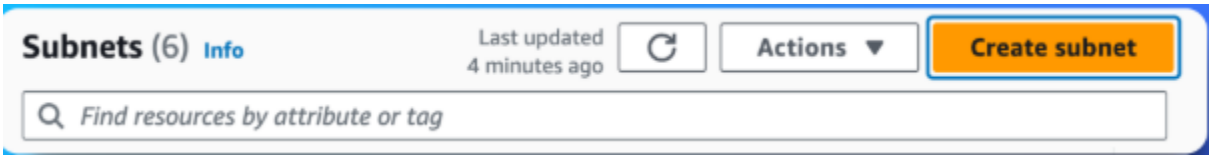
➢ CREATE SUBNETS

Subnets are smaller networks within a larger network. Subnets are used to organize and isolate resources based on different needs such as security and availability. You use subnets to group resources with similar access rules and restrictions. Some subnets might be public areas that all resources can access (public subnets) while others are private areas with limited access (private subnets). A VPC can have as many public and private subnets as you need, but subnets in the same VPC cannot have overlapping IP address CIDR blocks. This means each subnet must have a unique range of IP addresses.

- In the **VPC Dashboard**, under **Virtual Private Cloud**, choose **Subnets**.



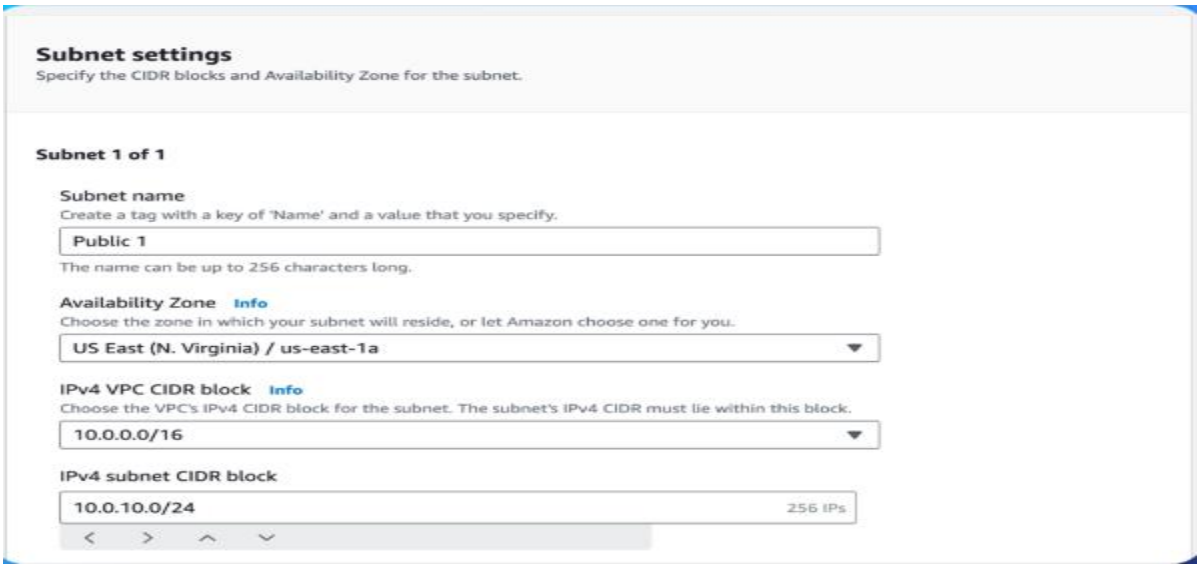
- Choose **Create subnet**



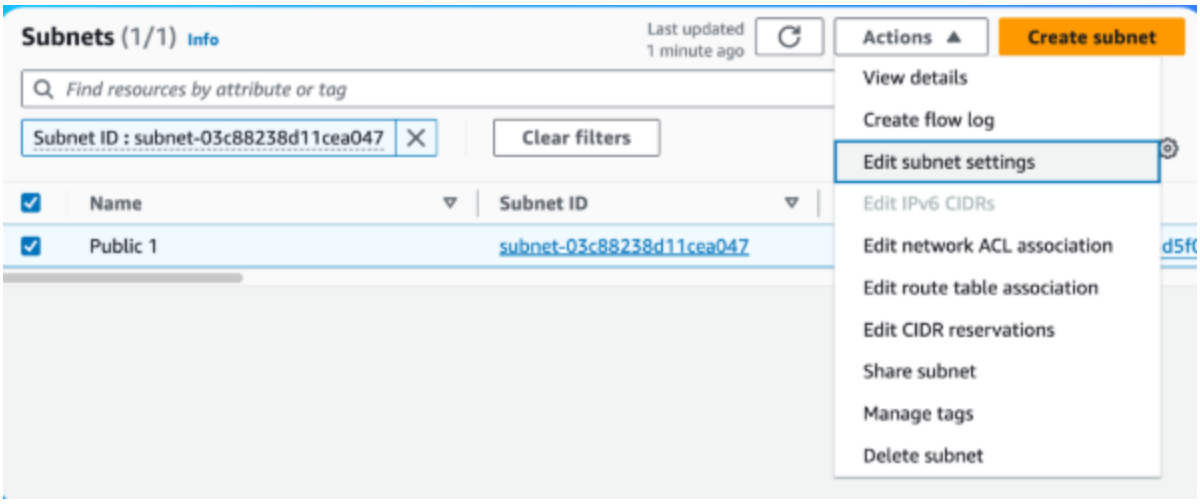
- Configure your subnet settings:

Subnets could be private or public. A public subnet is connected to the internet**.** Resources inside a public subnet can communicate with external networks. A private subnet does not have direct internet **access.** You use it for internal resources that don't need to be publicly accessible.

VPC ID: NextWork VPC
Subnet name: Public 1
Availability Zone: Select the first Availability Zone in the list.
IPv4 VPC CIDR block: 10.0.0.0/16
IPv4 subnet CIDR block: 10.0.0.0/24

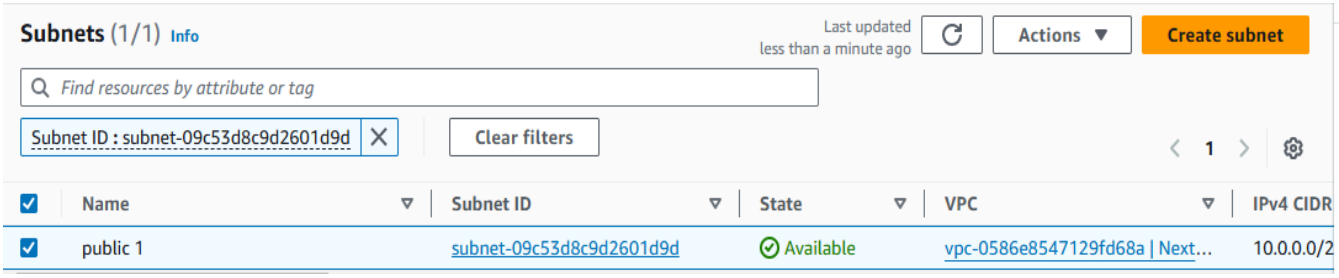


- Choose **Create subnet.**
- Select the checkbox next to **Public 1**.
- In the **Actions** menu, select **Edit subnet settings.**



- Check the box next to **Enable auto-assign public IPv4 address.**
- Choose **Save.**

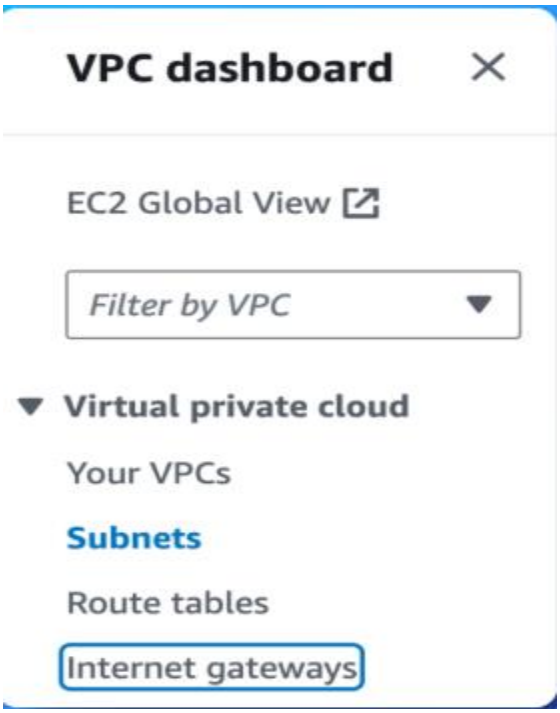
When you enable **auto-assign public IPv4 address** for a subnet, any EC2 instance launched in that subnet will instantly get a public IP address so you won't have to create one manually



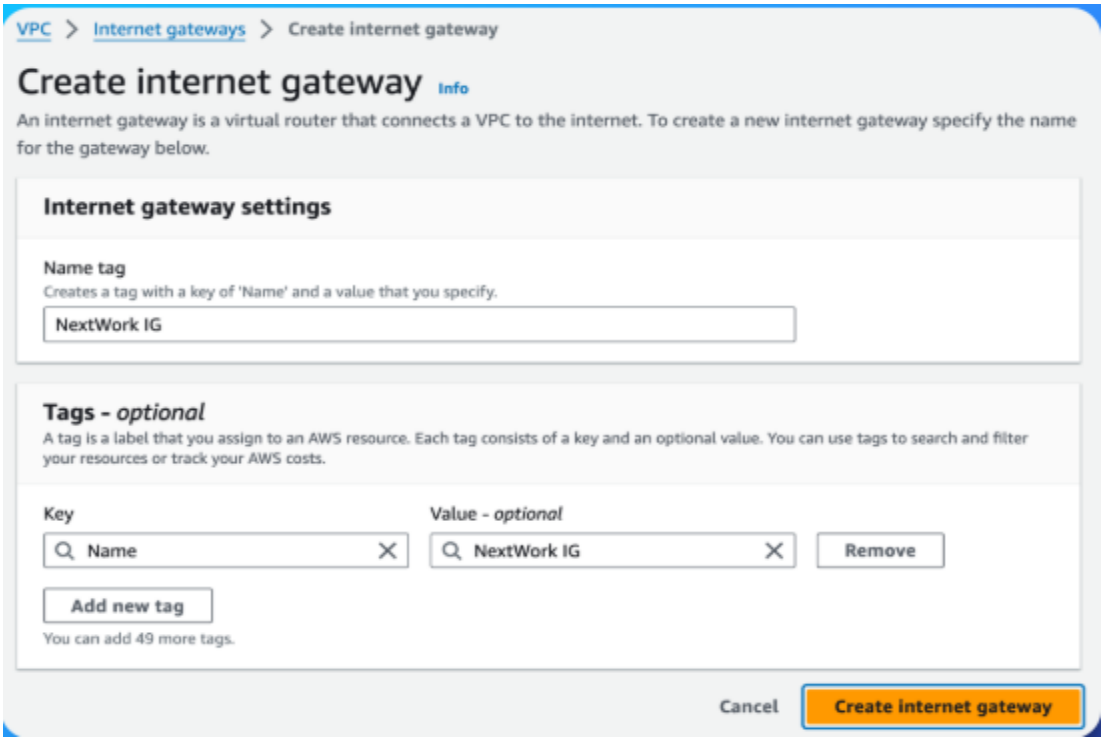
➢ CREATE AN INTERNET GATEWAY (IGW)

Internet gateways are keys to making applications available on the internet. By attaching an internet gateway, your instances can access the internet and be accessible to external users. An internet gateway connects your city (VPC) and the outside world (internet). This is like building a bridge (internet gateway) that links your private city (VPC) to the outside world (the internet), so your resources can communicate beyond your private space.

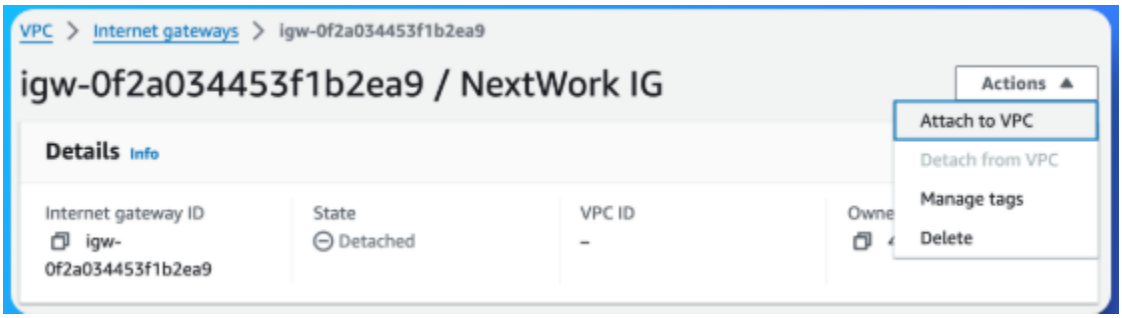
- In the left navigation pane, choose **Internet gateways**.



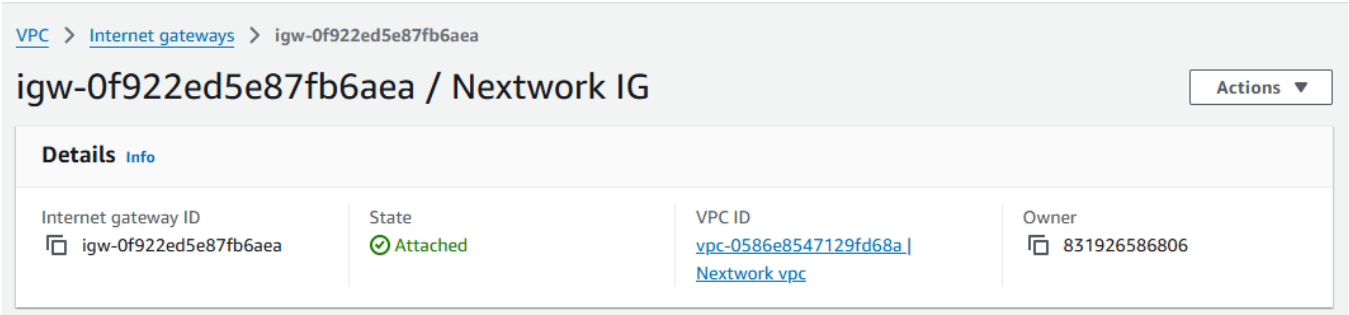
- Choose **Create internet gateway**.
- Configure your internet gateway settings:
  - **Name tag:** NextWork IG
- Choose **Create internet gateway**.



- Select your newly created internet gateway and choose **Actions**, then **Attach to VPC**.



- Select **NextWork VPC**.
- Select **Attach internet gateway**.

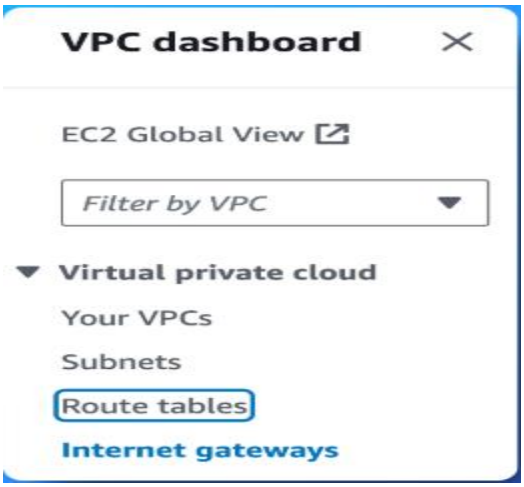


Attaching an internet gateway means resources in your VPC can now access the internet. The EC2 instances with public IP addresses also become accessible to users, so your applications hosted on those servers become public too.

➢ CREATE A ROUTE TABLE

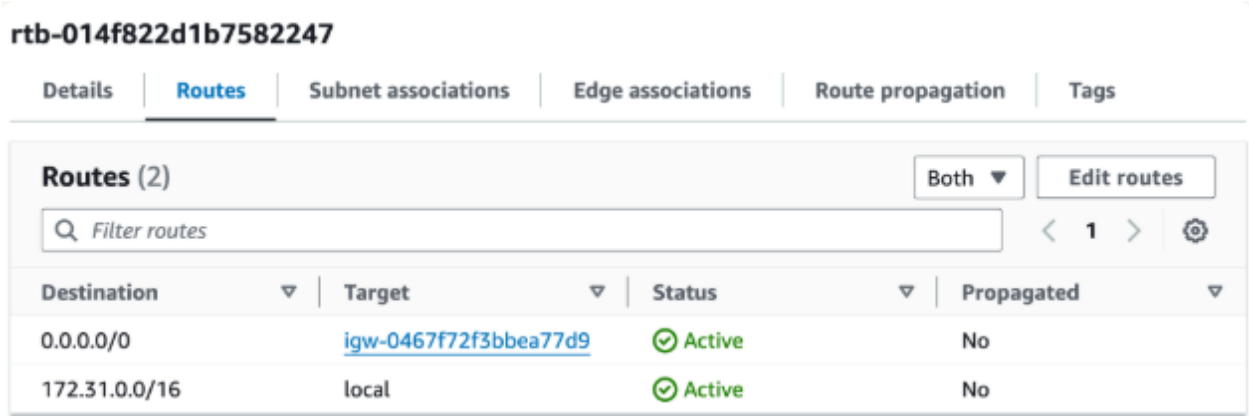
Route tables are used to control the routing of network traffic within your VPC. They define how traffic is directed from one subnet to another and how it can access the internet or other networks. Think of a route table as a GPS for the resources in your subnet. Just like a GPS helps people get to their destination in a city, a route table is a table of rules, called routes, that decides where the data in your network should go. Without a route table, your resources wouldn't know where to send or receive data.

- In the left navigation pane, choose **Route tables**.



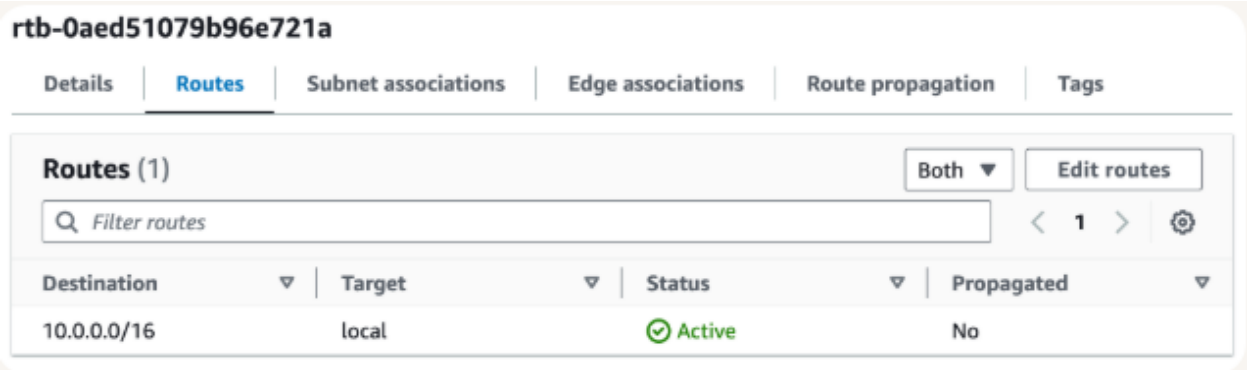
- Select the checkbox for the first route table at the top of the list, then select the **Routes** tab.
- Uncheck that route table, and switch to the bottom route table.
- Select the **Routes** tab again.

One of your route tables was created with your AWS account's default VPC! This is the route table with two routes inside:



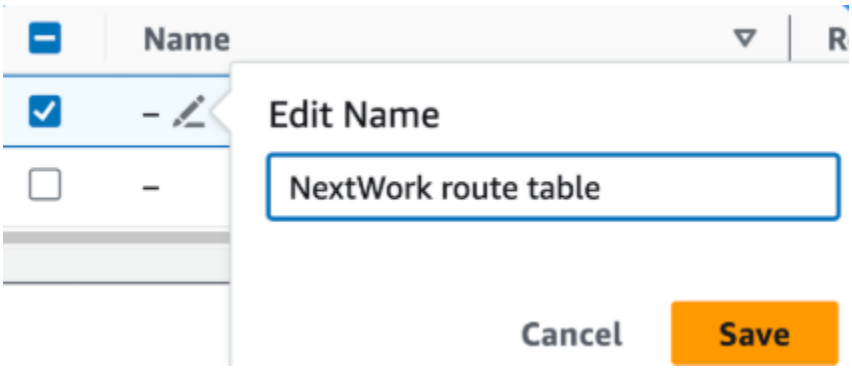
1. **Route 0.0.0.0/0 | igw-** directs traffic to the default internet gateway.
2. **Route 172.31.0.0/16 | local** is helps manage **internal** traffic within the VPC.

AWS also created the other route table automatically when you set up **NextWork VPC.**

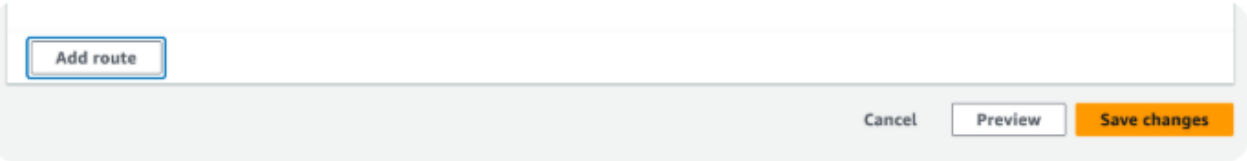


1. This route table has a single route that allows traffic within the **10.0.0.0/16** CIDR block to flow within the network.
2. There is no route with an internet gateway as the target! This means there is no route for traffic to leave your VPC.

- Let's rename your NextWork VPC route table so it's easier to recognize.
- Make sure you have your NextWork VPC route table selected - this is the route table with a single route to 10.0.0.0/16.
- Select the pencil icon in the **Name** column of your route table.
- Enter the name NextWork route table.



- Select the **Routes** tab.
- Choose **Edit routes.**
- Choose **Add route** near the bottom of the page.

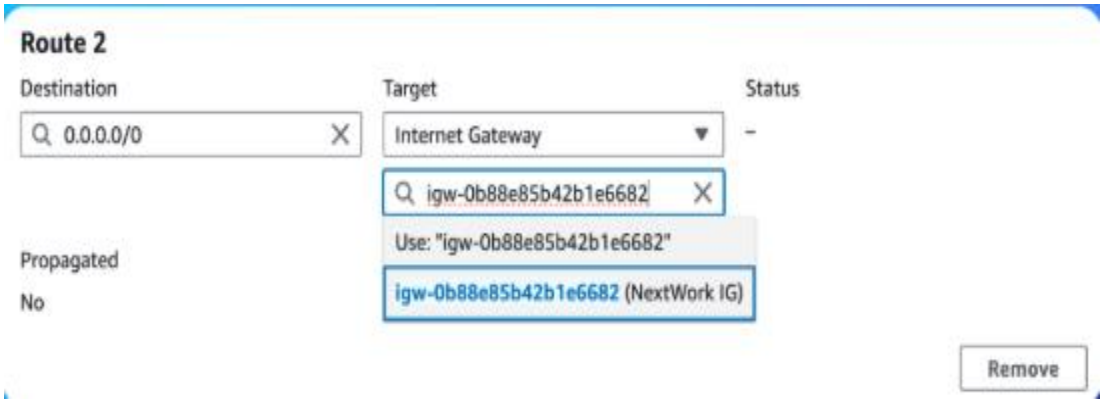


- Destination: 0.0.0.0/0

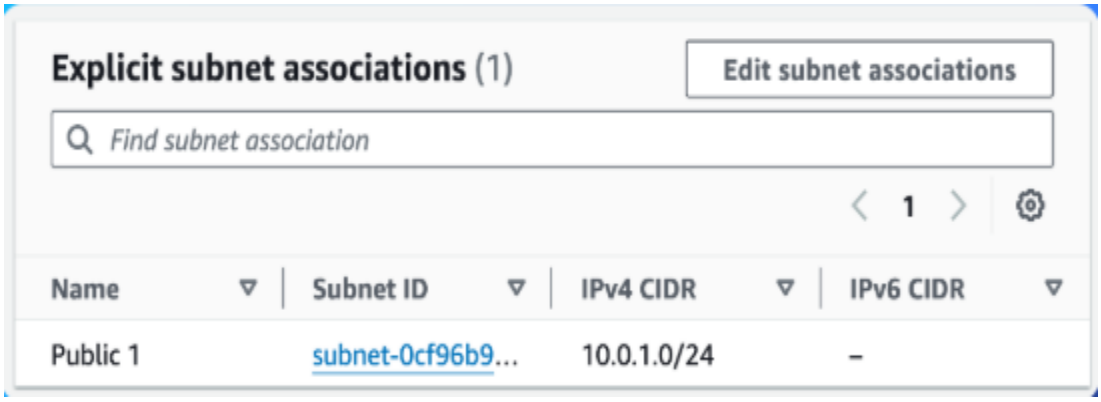
0.0.0.0/0 means all IPv4 addresses! When you set 0.0.0.0/0 as the destination in a route table, you are creating a default route that sends any traffic that doesn't match more specific routes

on your route table. Since the only other route has a destination of 10.0.0.0/16, this means all traffic that is not bound for another resource within your VPC is bound for the internet gateway. The internet gateway then forwards this traffic to the internet, allowing your resources to communicate with external networks and users.

- Target: **Internet Gateway**.
- Select the only **Internet Gateway** id option.



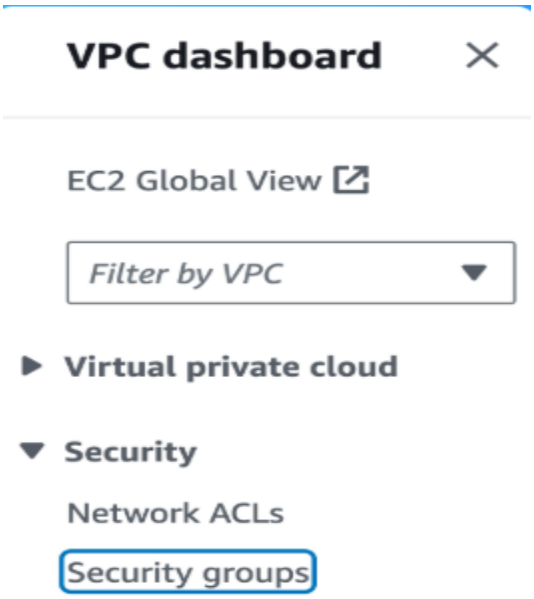
- Choose **Save changes.**
- Choose the **Subnet associations** tab.
- Under the **Explicit subnet associations** tab, choose **Edit subnet associations**
- Select **Public 1**.
- Choose **Save associations.**



➢ CREATE A SECURITY GROUP

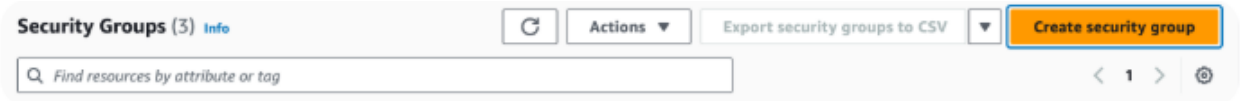
Security groups are responsible for checking who comes in and out. They have strict rules about what kind of traffic can enter or leave the resource based on its IP address, protocols and port numbers.
Protocols are special rules that help data move across the internet, each designed to send data for a specific kind of task (HTTP, FTP, SSH). Think of port numbers as specific doors or delivery docks on a building where data will enter or exit..

- In the left navigation pane, choose **Security groups**.



AWS automatically creates a default security group for each new VPC, which allows all traffic between resources within the same VPC. This default rule enables secure communication between resources without exposing them to external threats.

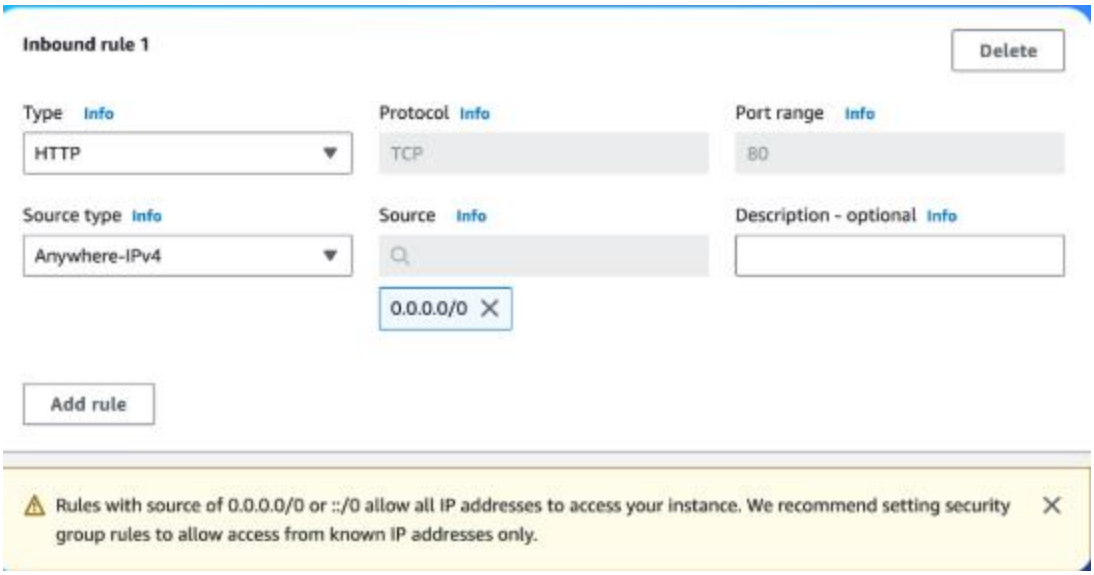
- Choose **Create security group**.



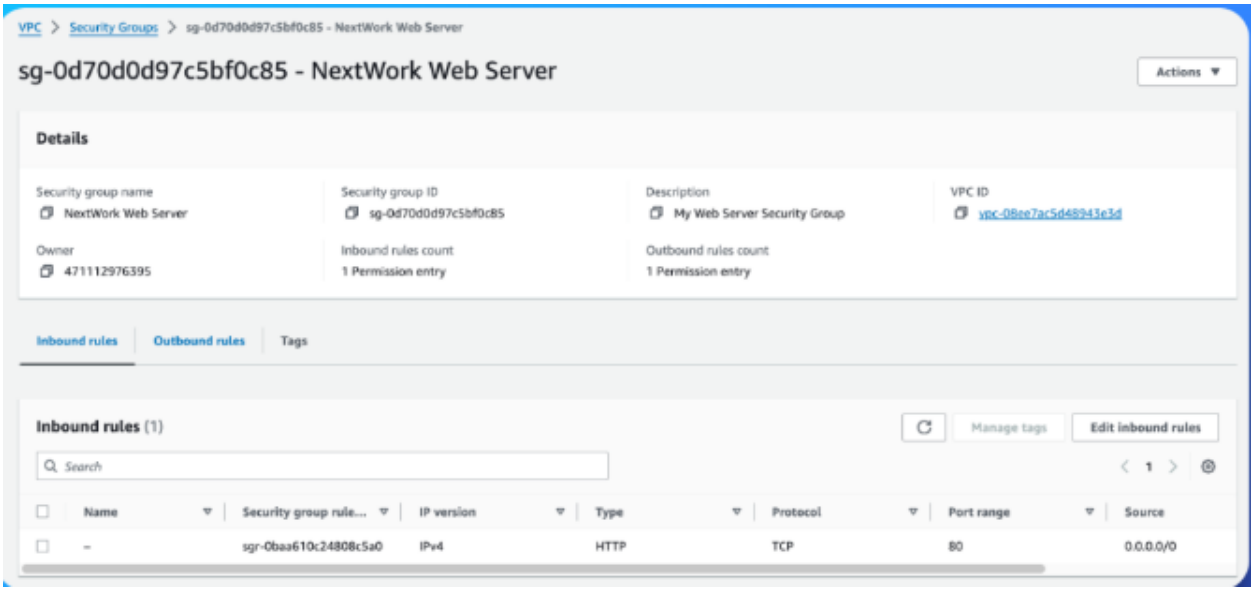
- Security group name: NextWork Security Group
- Description: A Security Group for the NextWork VPC.
- VPC: **NextWork VPC**
- Under the **Inbound rules** panel, choose **Add rule.**

Inbound rules control the data that can enter the resources in your security group, while outbound rules control that data that your resources can send out. In this context, setting up inbound rules is important for allowing users to access your public website, while outbound rules help manage how your server interacts with other parts of the internet.

- **Type**: HTTP
- **Source**: Anywhere-IPv4



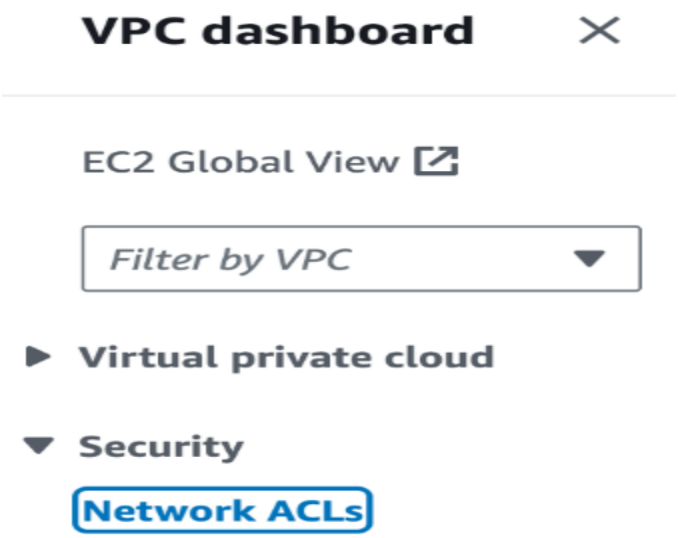
- At the bottom of the screen, choose **Create security group.**



➢ CREATE A NETWORK ACL

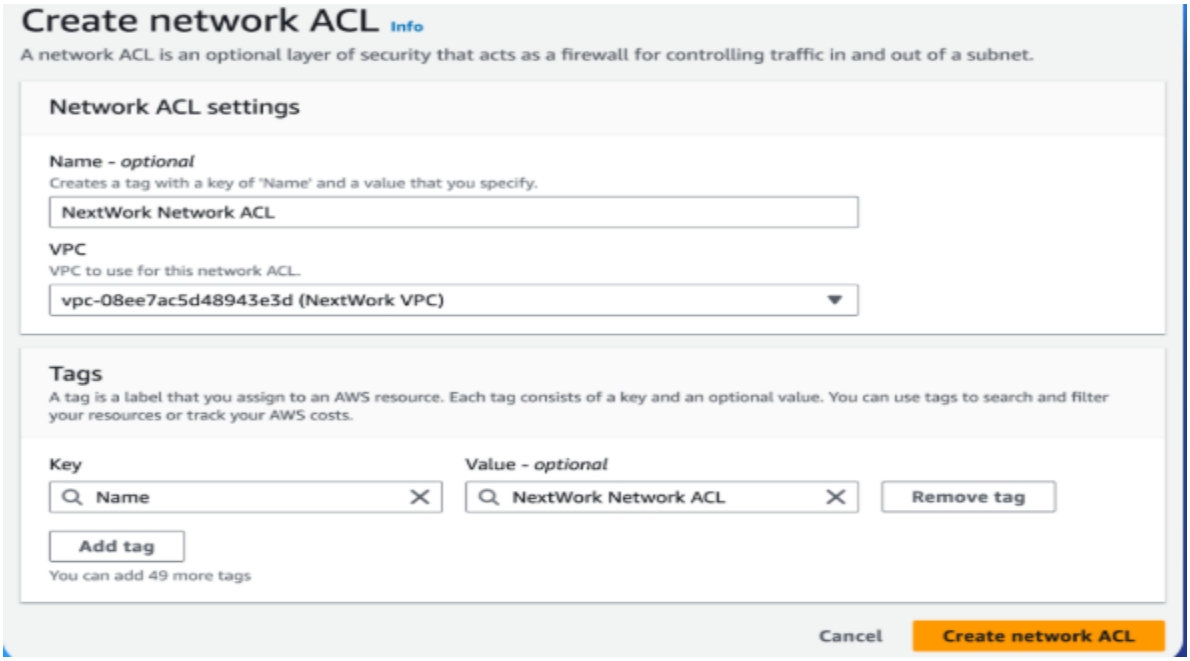
Think of Network ACLs as traffic cops stationed at every entry and exit point of your subnet, checking each data packet against a table of ACL rules before allowing them through.

- In the left navigation pane, choose **Network ACLs**.

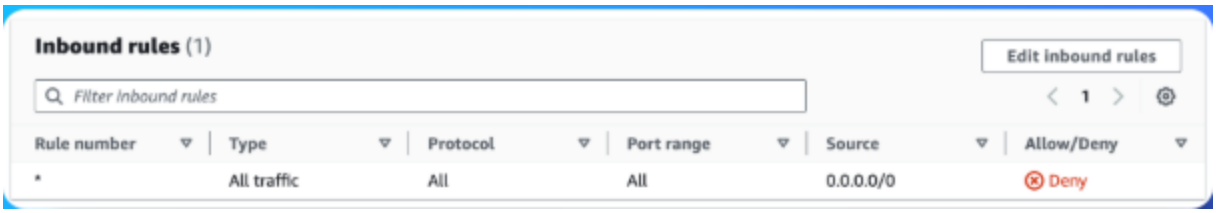


- Select **Create new network ACL.**
  Name: NextWork Network ACL
  VPC: **NextWork VPC**

- Select **Create network ACL**



- Select the checkbox next to your **NextWork Network ACL**
- Select the **Inbound rules** tab.



- Select **Edit inbound rules.**
- Select **Add new rule**.
- Rule number: 100

In network ACLs, rule numbers decide the order that rules are checked—lower numbers go first. Starting at 100 gives you room to add new rules before it if you need to

- Type: **All traffic.**

When you selected "All traffic" for the traffic type, this choice implies that your rule will apply to all protocols and port ranges, so there's no need to specify them anymore.

- Source: 0.0.0.0/0

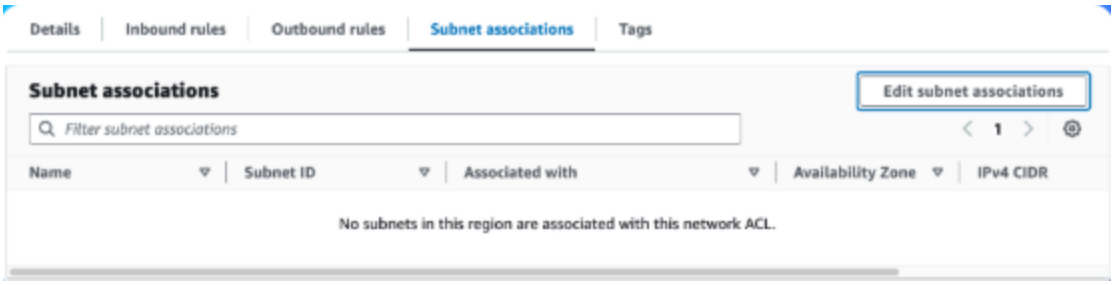
- Click **Save changes.**

Set up the same for your Network ACL's outbound rules

- Select the **Outbound rules** tab.
- Select **Edit outbound rules.**
- Select **Add new rule**.
- Rule number: 100
- Type: **All traffic.**
- Source: 0.0.0.0/0

If your network ACL isn't associated with any subnets, all of the rules you define won't affect your VPC's traffic. Your network ACL isn't actually securing any part of your network

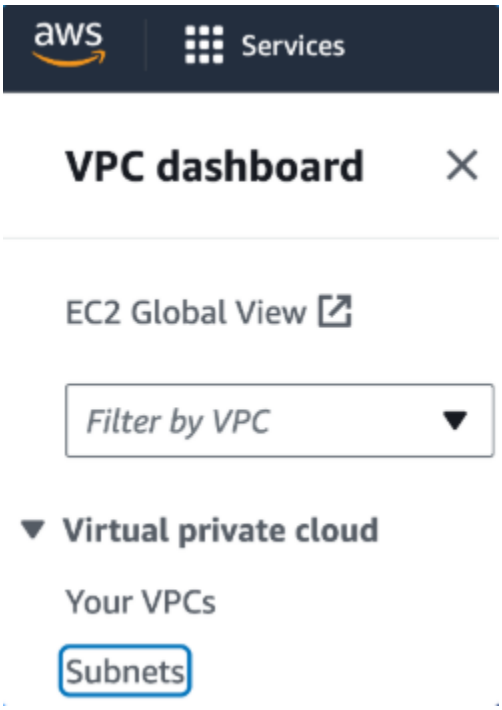
- Under the **Subnet associations tab**, select **Edit subnet associations.**



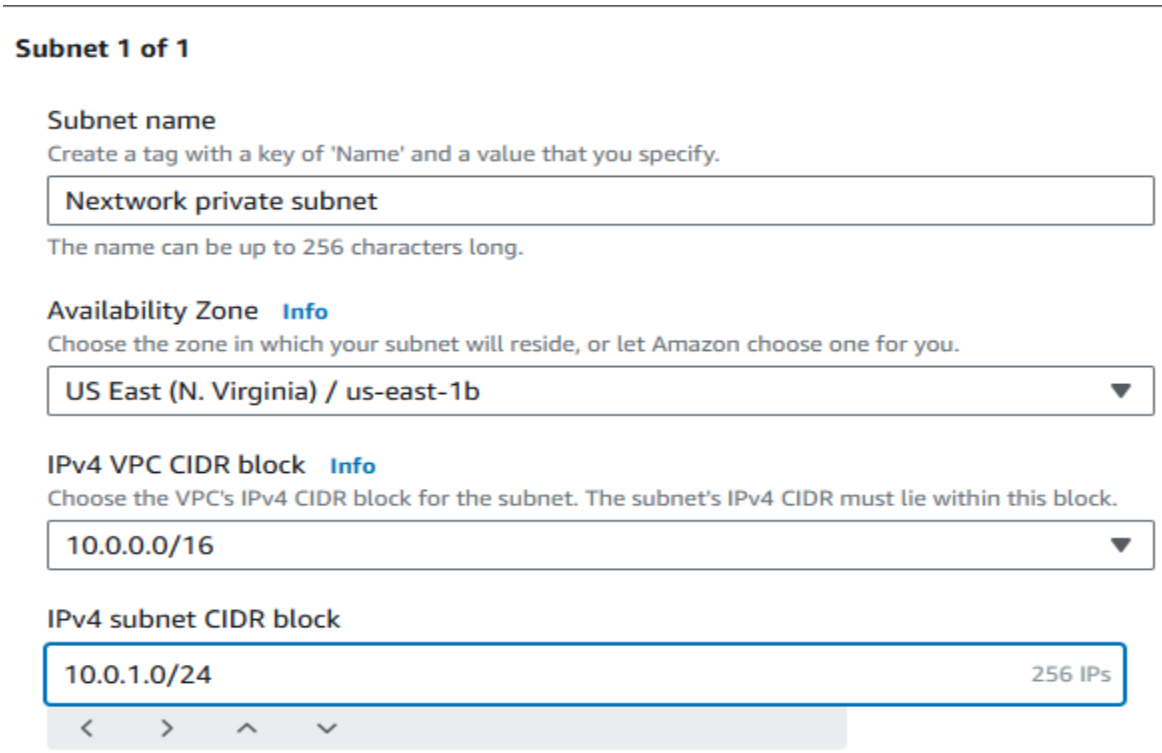
- Select your **Public 1** subnet.
- Select **Save changes.**

➢ CREATING A PRIVATE SUBNET

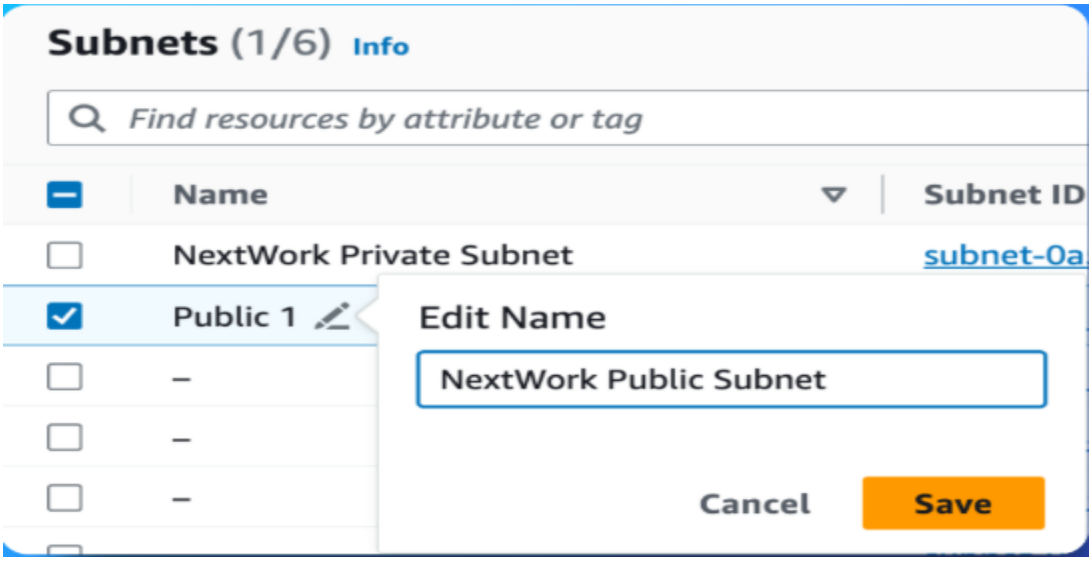
Still in your VPC console, select the **Subnets** tab again.



- Select **Create subnet**.
- For the **VPC ID,** select **NextWork VPC**.
- Set the **Subnet name** as NextWork Private Subnet
- For the subnet's **Availability Zone**, use the second AZ on the dropdown (not the first!)
- The IPv4 VPC CIDR block should be 10.0.1.0/24.



- Select **Create subnet**.
- Retitle your **Public 1** subnet to **NextWork Public Subnet.**

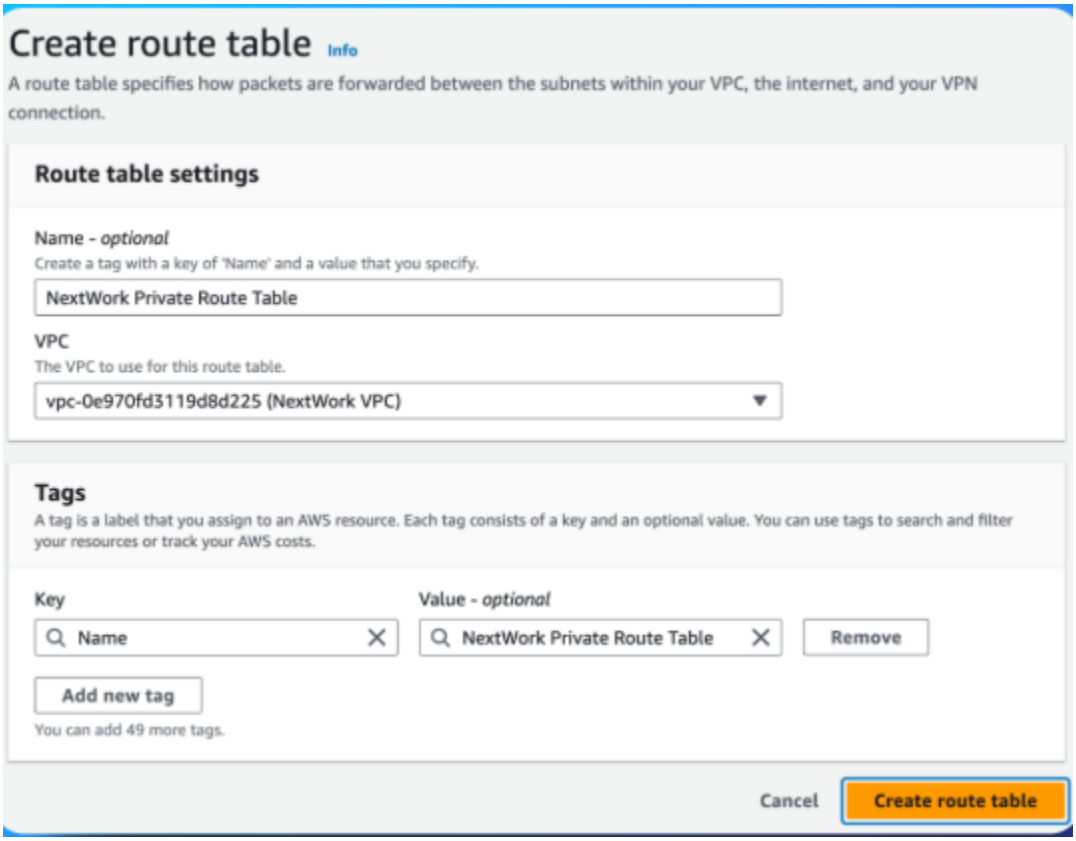


➢ SET UP A PRIVATE ROUTE TABLE

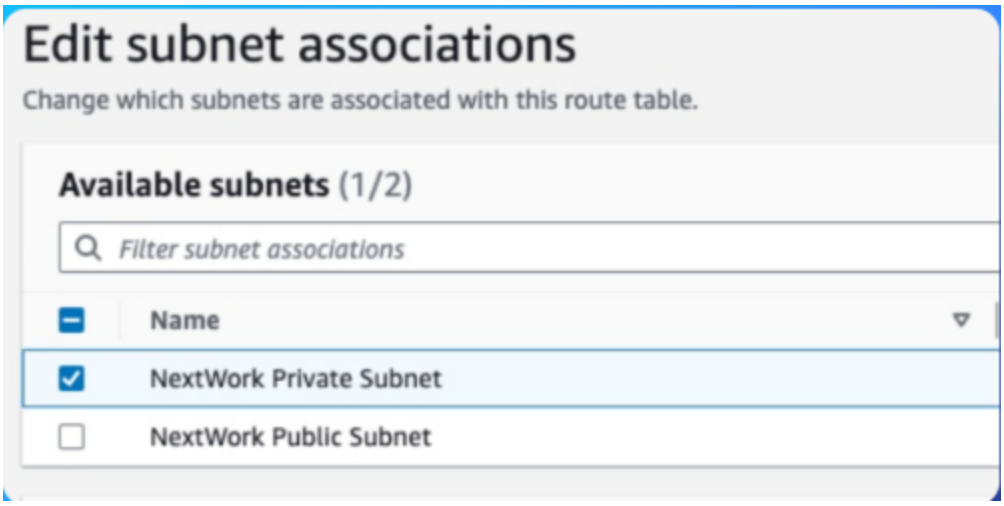
Like your public subnet, a private subnet also needs to be associated with a route table

- Head to the **Route tables** page in your console.

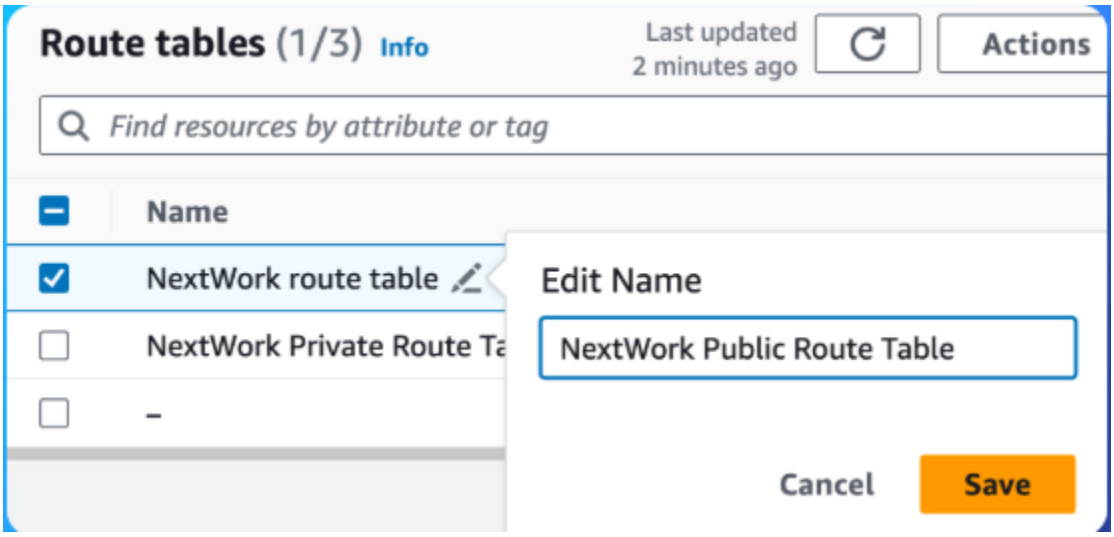
- Select **Create route table**.
- Name your new route table **NextWork Private Route Table**
- Under **VPC**, select **NextWork VPC**.
- Select **Create route table.**



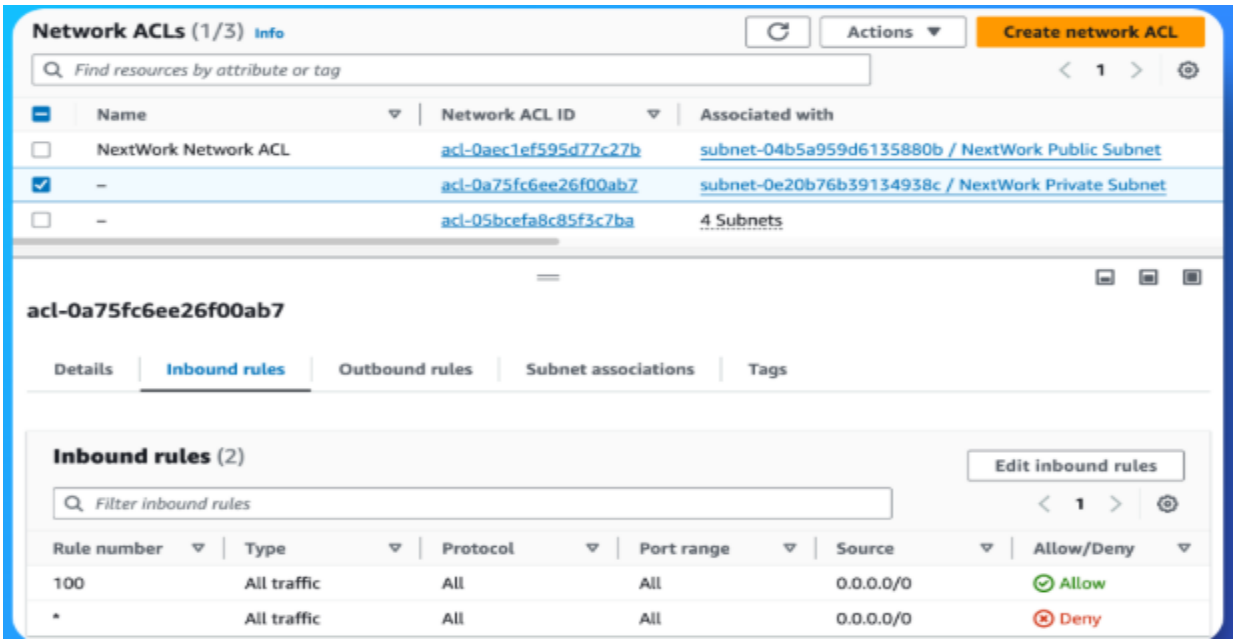
- Select **NextWork Private Route Table**.
- Check the **Routes** tab - does it only have one default route with a **local** target?
- Switch tabs to **Subnet associations.**
- Select **Edit subnet associations** under the **Explicit subnet associations** tab.
- Select the checkbox next to **NextWork Private Subnet**.
- Select **Save associations**.



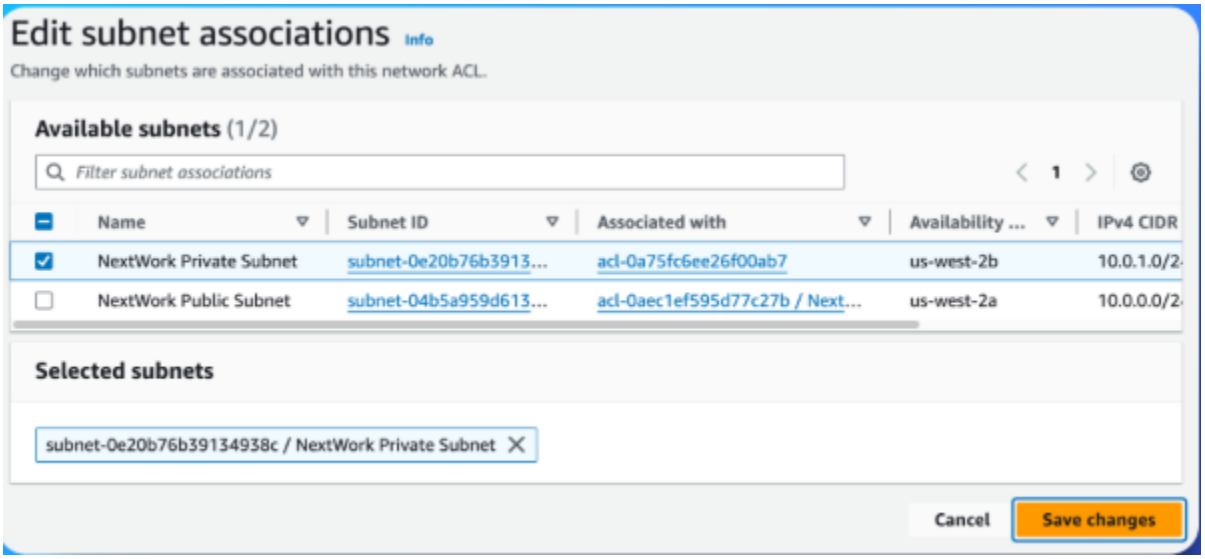
- Retitle **NextWork route table** to NextWork Public Route Table



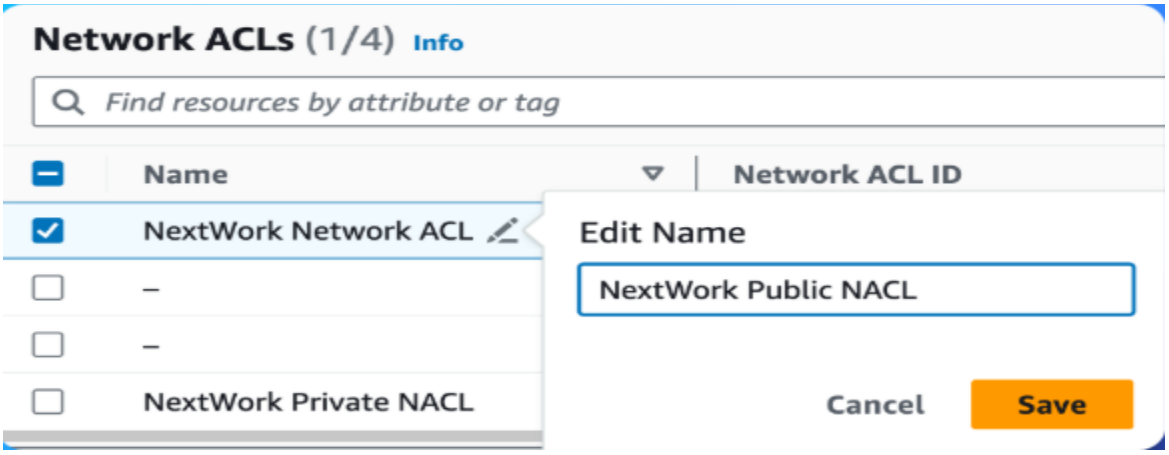
- Select **Network ACLs** from the left hand navigation panel.
- Select the checkbox next to the default ACL for your VPC.
    - Note that this is NOT **NextWork Network ACL** - your default ACL isn't named!
- Select the **Inbound rules** and **Outbound rules** tabs



- So while the default ACL is very convenient in allowing all traffic types, we'll create a new custom network ACL to keep our private subnet safe.
- Select **Create network ACL** on the top right.
- For the name, enter NextWork Private NACL.
- Select **NextWork VPC**.
- Select **Create network ACL**.
- Switch tabs to **Subnet associations.**
- Select **Edit subnet associations.**
- Select your private subnet.
- Select **Save changes.**



To tidy up your Network ACLs' naming conventions, let's also rename **NextWork Network ACL** to **NextWork Public NACL.**



➢ DELETE YOUR RESOURCES

SECURITY GROUPS:

- Go to AWS Console
- Select the custom security groups linked to your VPC.
- Click Actions and Delete security group(s).

NETWORK ACLs:

- Go to VPC Dashboard
- Navigate to Network ACLs
- Select the custom Network ACLs linked to your VPC.
- Click Actions
- Click Delete.

ROUTE TABLES:

- Go to AWS Console
- Navigate to VPC Dashboard
- Navigate to Route Tables and select the custom route tables you had created.
- Click Actions and Delete

INTERNET GATEWAY:

- Go to AWS Console
- Navigate to VPC Dashboard
- Navigate to Internet Gateways and select the Internet Gateway attached to your VPC
- Click Actions
- Detach from VPC

- Click Actions and Delete

SUBNETS:

- Go to AWS and navigate to the VPC Dashboard.
- Select all the subnets in the VPC.
- Click Actions and Delete Subnets.

VPC:

- In your **VPC console**, select the checkbox next to **NextWork VPC**.
- Select the **Actions** dropdown.
- Select **Delete VPC**.