General Immersion Day

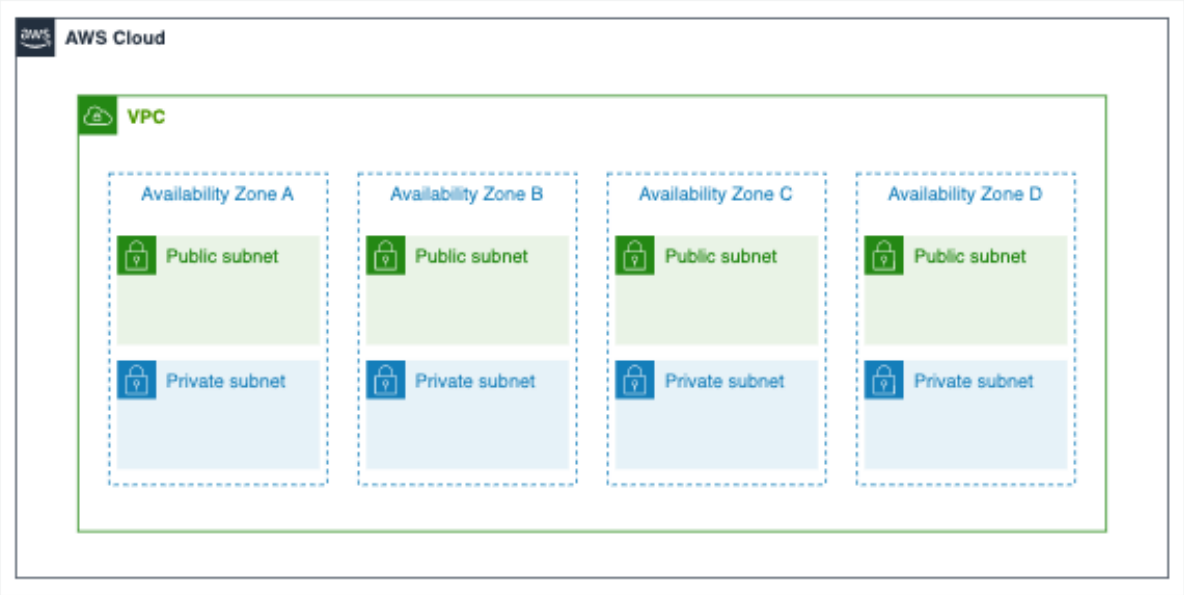
Lab 3

Network - VPC Hands on Lab

VPC Hands on Lab

Amazon VPC(Virtual Private Cloud) Overview

Amazon Virtual Private Cloud(Amazon VPC) enables you to launch AWS resources into a virtual network that you've defined. This virtual network closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of AWS.
Amazon VPC lets you provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways. You can use both IPv4 and IPv6 in your VPC for secure and easy access to resources and applications.

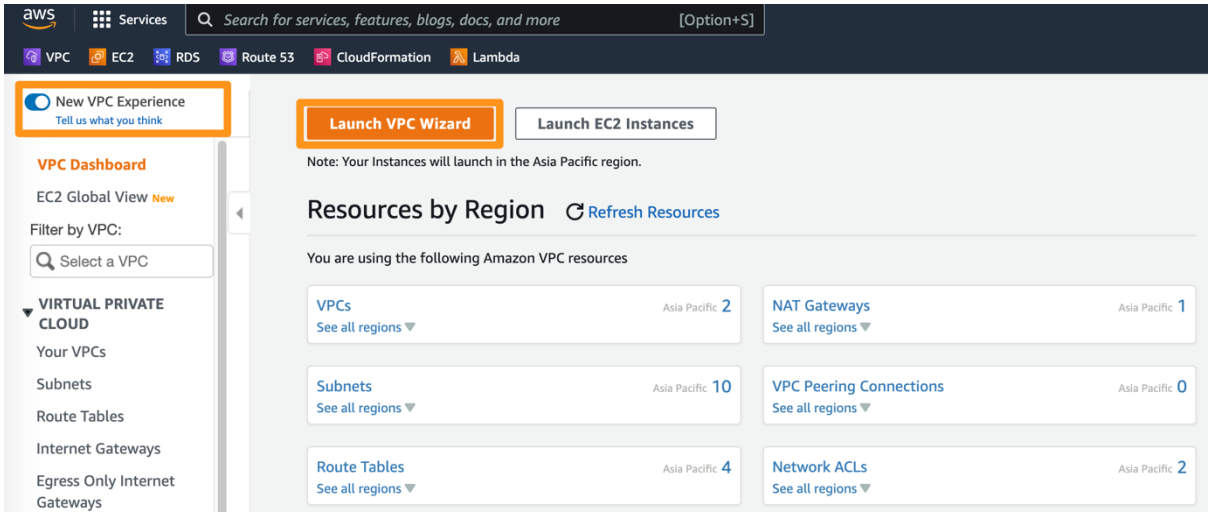


Configure your own network by going through the labs in the order below:

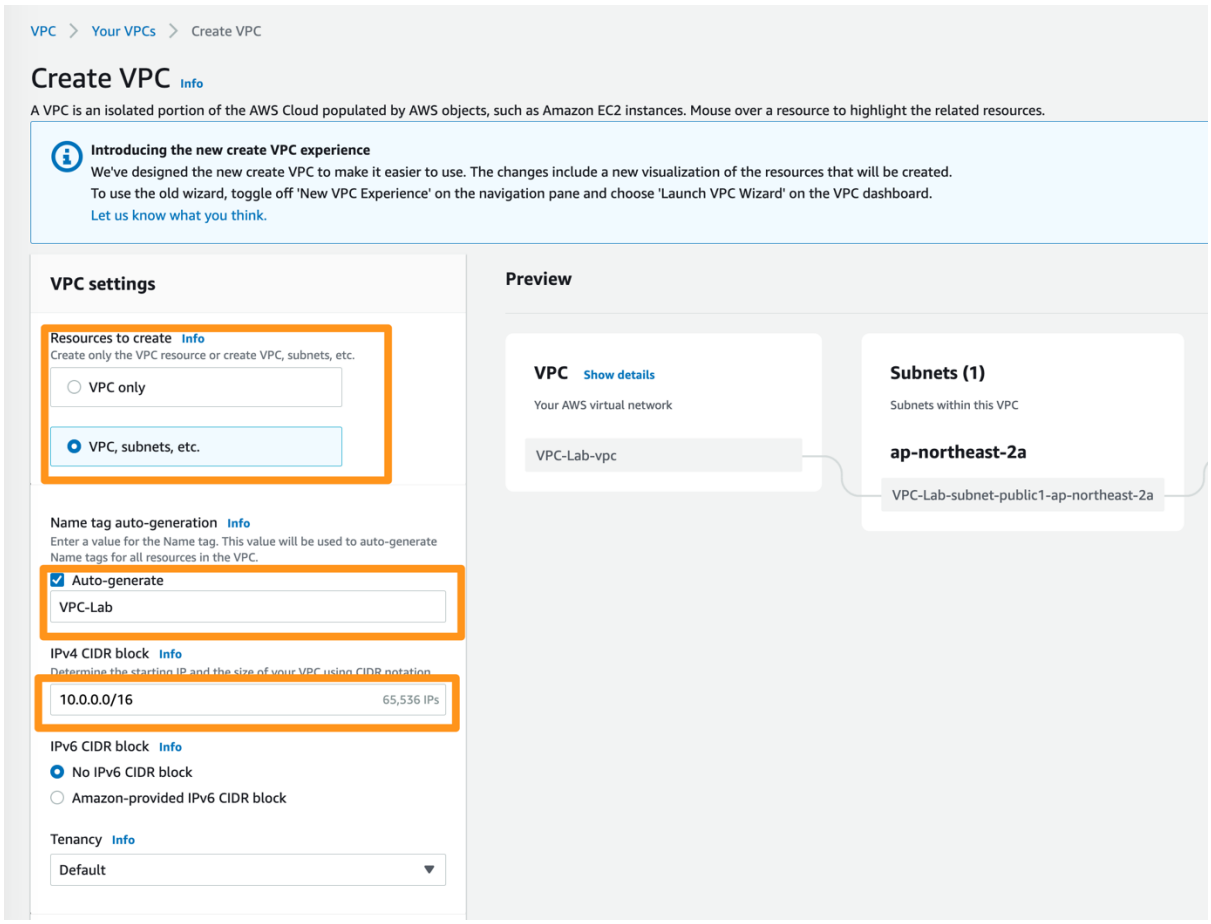
1. Create a VPC
2. Create additional subnets
3. Edit the routing table
4. Create a Security Group
5. VPC Flow Logs (Optional)
6. Clean up resources

3-1 Create a VPC

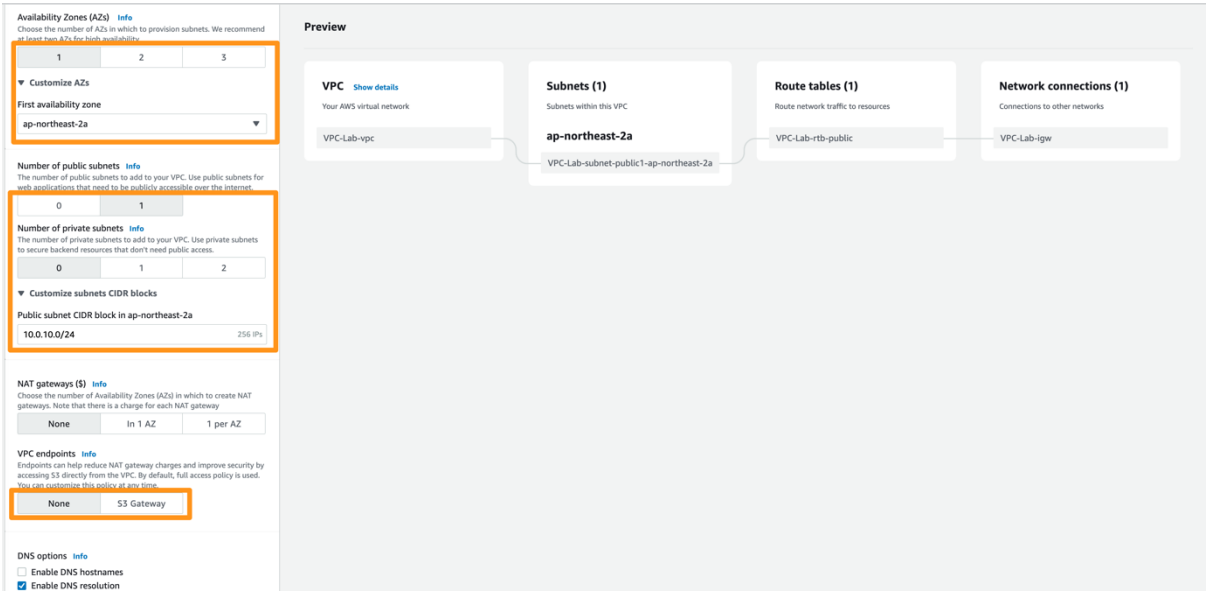
1. Log in to VPC Console .
2. Click **Launch VPC Wizard** on the screen below to start the Launch VPC wizard. The Launch VPC wizard makes it easy to create a non-default VPC configuration.



3. Under VPC Settings, select **VPC, Subnet, etc.**. For the name, type **VPC-Lab**.Set the CIDR block to the default value **10.0.0.0/16**.

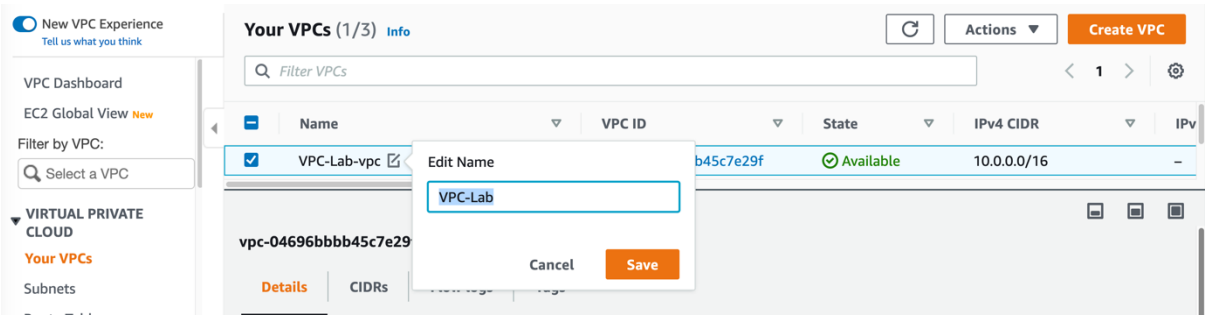


4. Choose 1 Availability Zone (AZ) and select **ap-northeast-2a**. The Availability Zone is a subset of the VPCs that you set up eariler. Select the number of public subnet as 1 and set the CIDR block to **10.0.10.0/24**. You do not create private subnet for this part so select 0. Then click **Create VPC** button at the bottom.

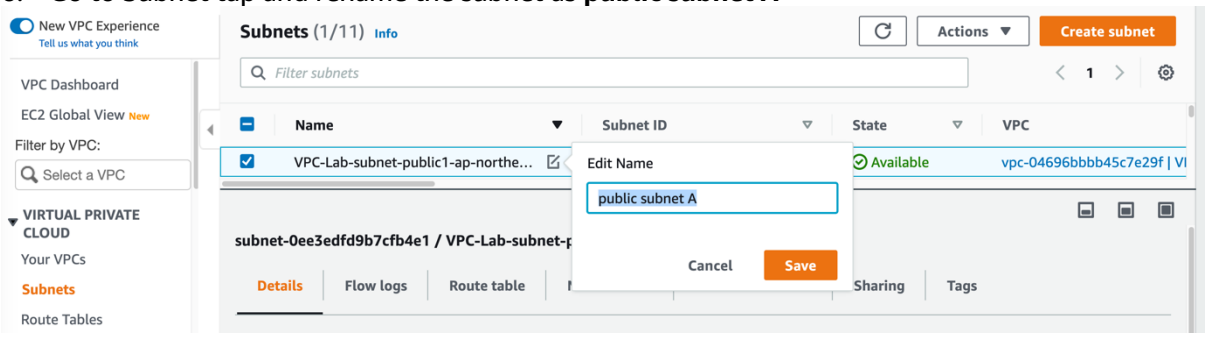


Note: When entering a value for the VPC IPv4 CIDR block, it is important to allocate it so that the address does not overlap with networks that are likely to connect directly in the future. Also, allocate addresses large enough for future expansion.

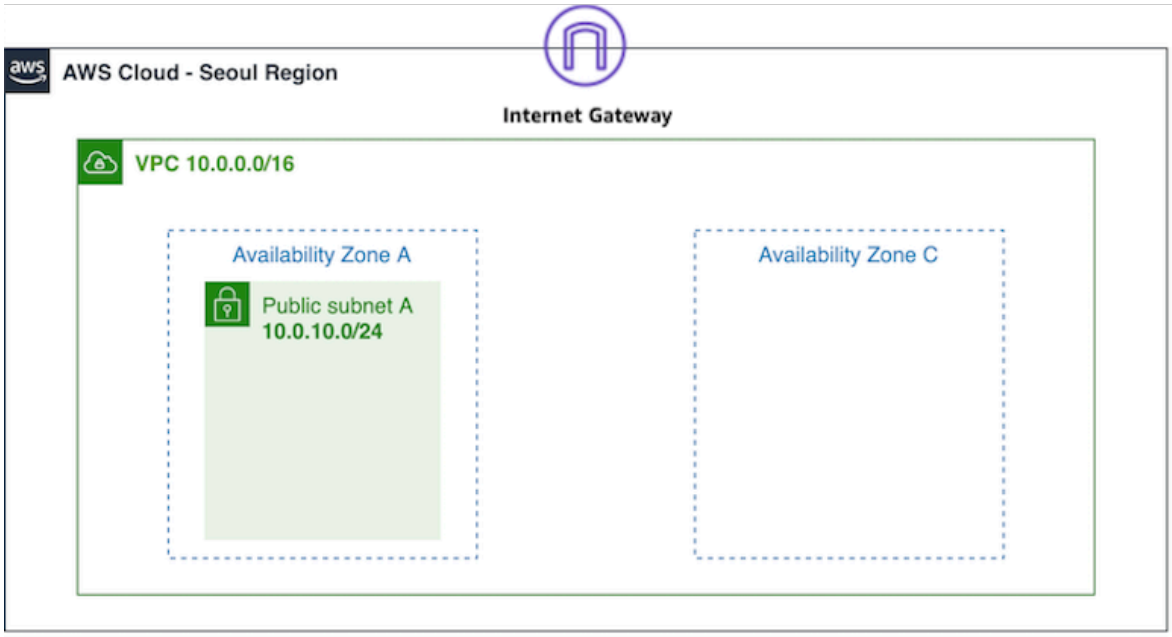
5. After you create the VPC, you can see a VPC with the name **VPC-Lab-vpc**. Rename it as **VPC-Lab**



6. Go to Subnet tap and rename the subnet as **public subnet A**

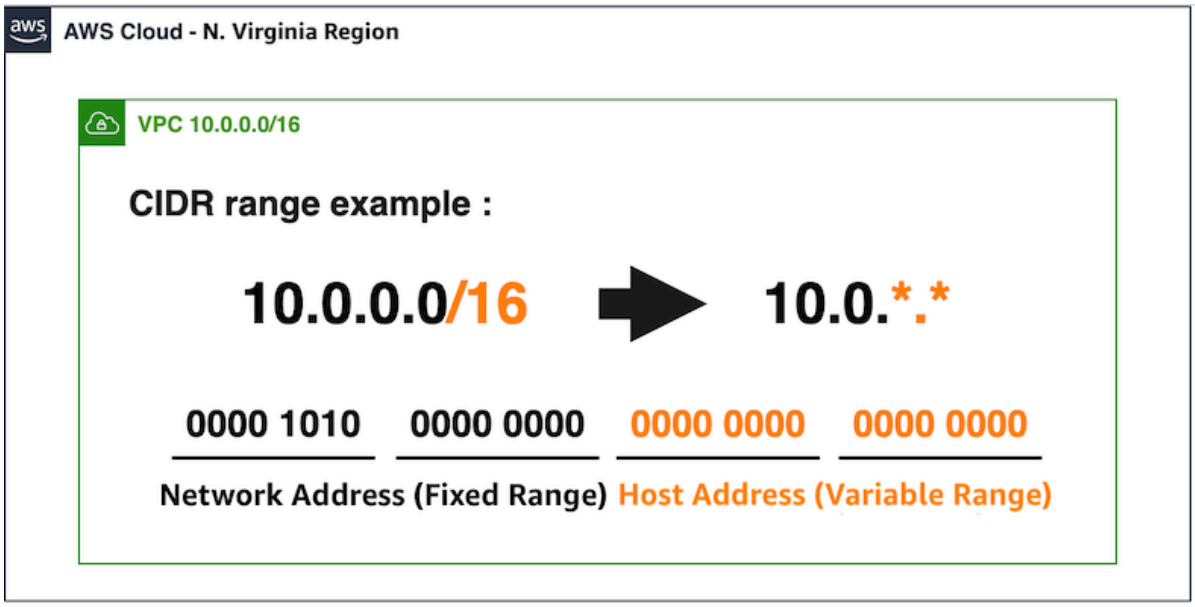


7. The architecture, as of now, is below.



Understanding CIDR address range

CIDR (Classless Inter-Domain Routing) is one of the ways to express the address and size of the network. The VPC you created above uses a range of IP addresses with 16 as the subnet value. The number of IPs that can be given to each resource is 65,536, which is 2 to the power of 16.



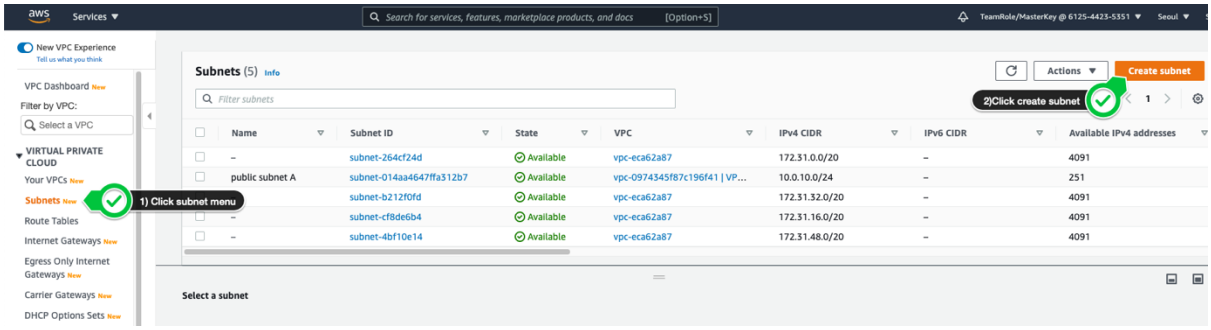
When specifying a VPC CIDR block, the allowed block size is /16 netmask (65,536 usable IP addresses) ~ /28 netmask (16 usable IP addresses). In each subnet CIDR block, the first 4 IP addresses and the last IP address are not available to users and cannot be assigned to instances. For example, in the subnet of the 10.0.0.0/24 CIDR block, the following 5 IP addresses are reserved.

Key	Value
10.0.0.0	Network address
10.0.0.1	Reserved for VPC routers from AWS
10.0.0.2	DNS server address
10.0.0.3	Reserved for future use from AWS
10.0.0.255	Network broadcast address

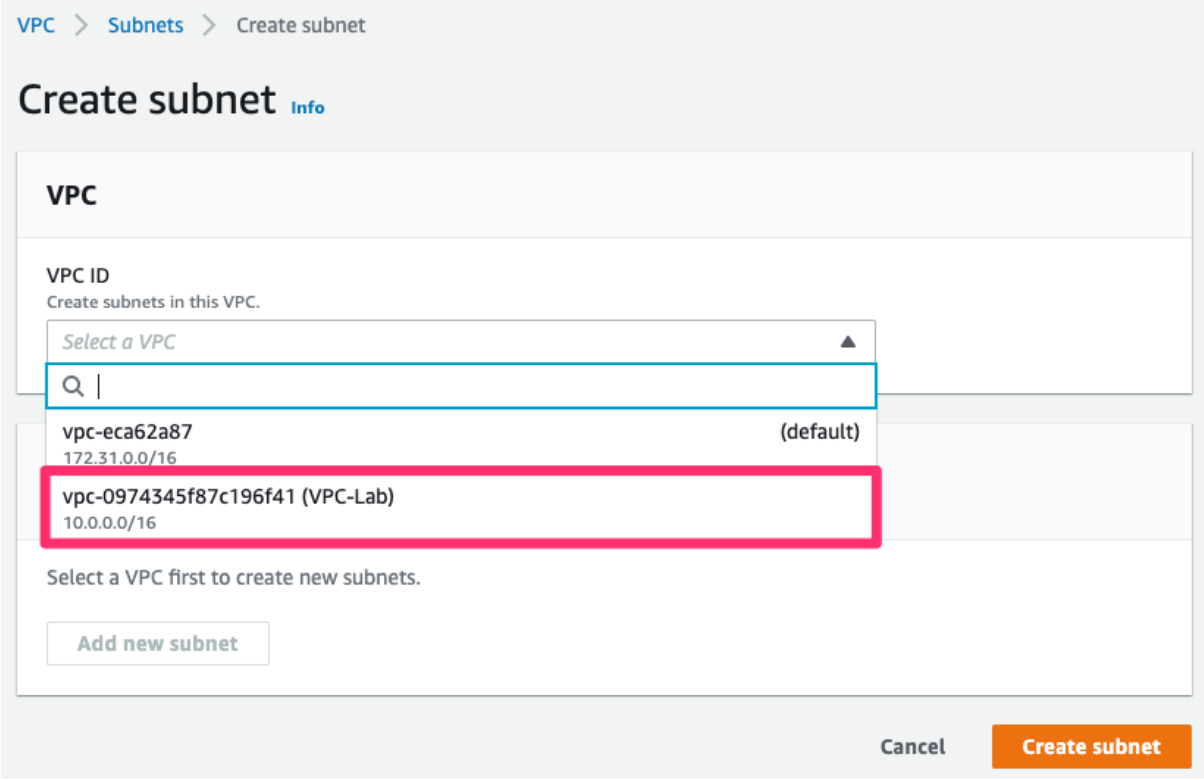
3-2 Creating Additional Subnets

To maintain high availability, it is important to deploy services across multiple Availability Zones. So, in this lab, you will create a subnet in an Availability Zone C, which is different from the Availability Zone A, where the subnet created earlier is located.

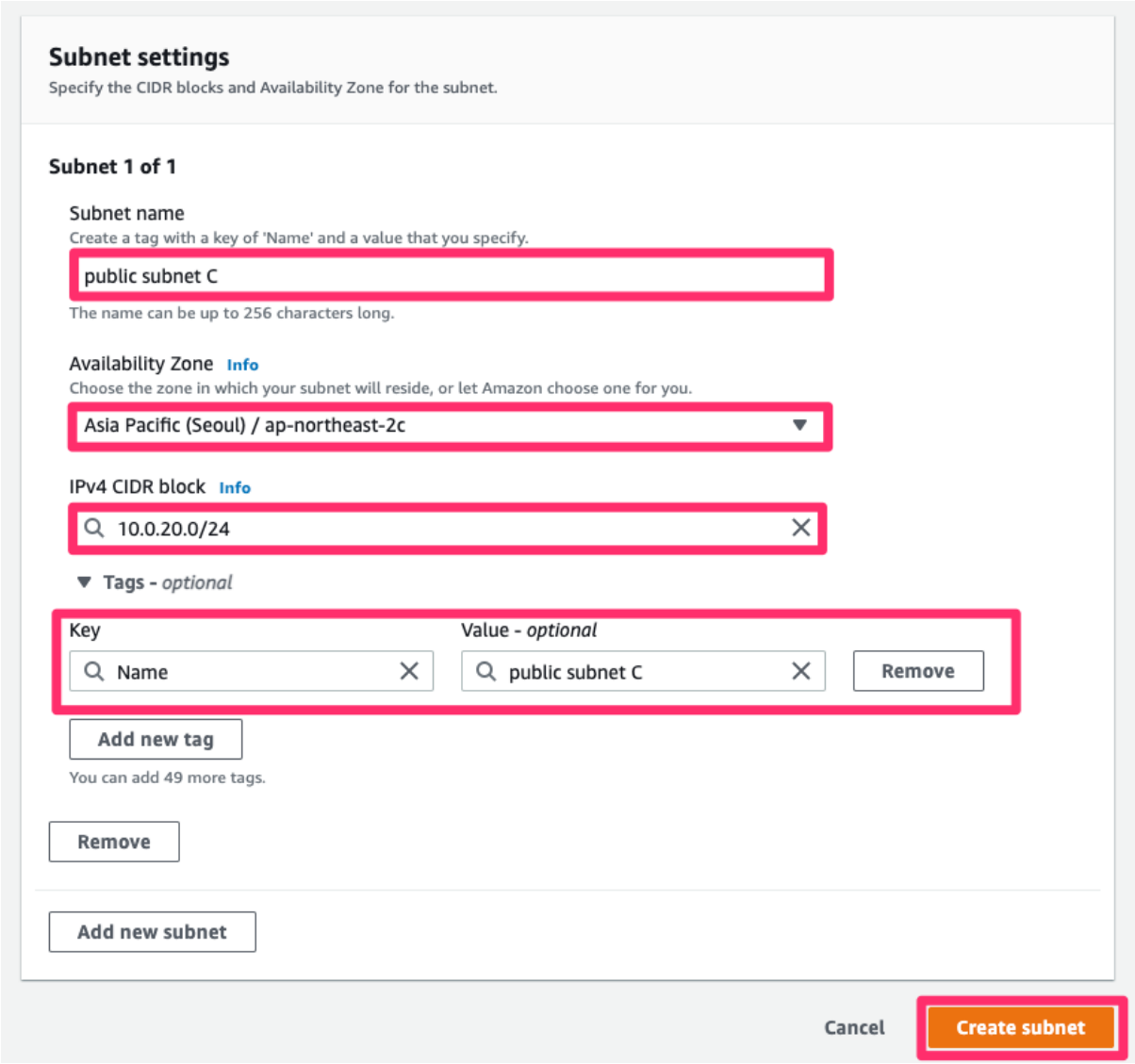
1. Click the **Subnet** menu on the left sidebar, then click the **Create Subnet** button.



2. For VPC ID, choose the VPC you just created.

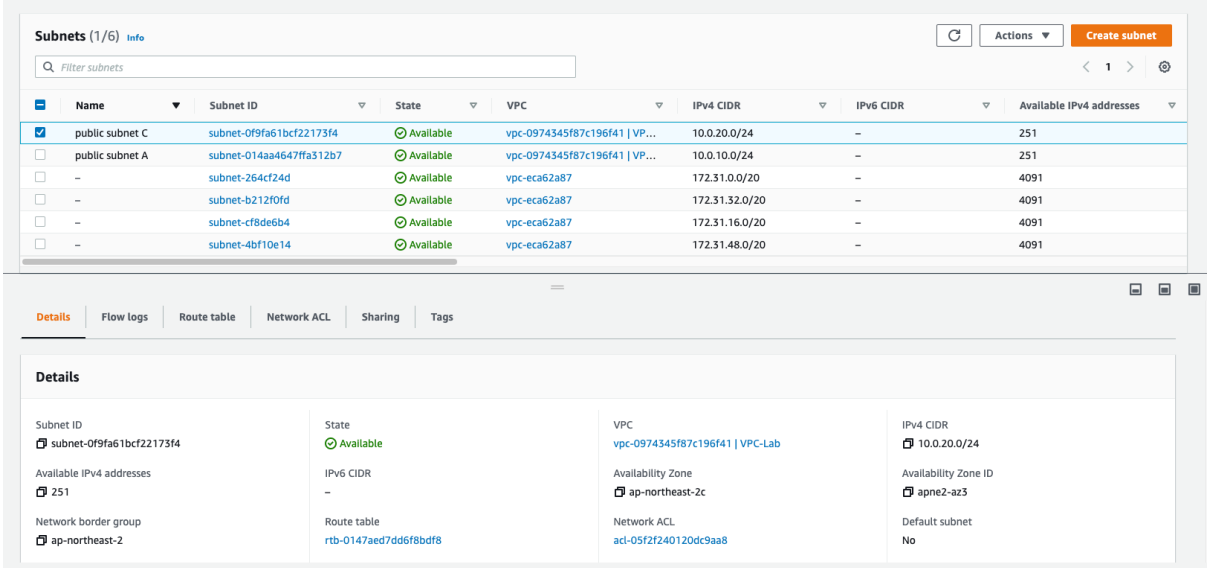


3. In the **Subnet settings** below, enter values as shown on the screen and click the **Create subnet** button.

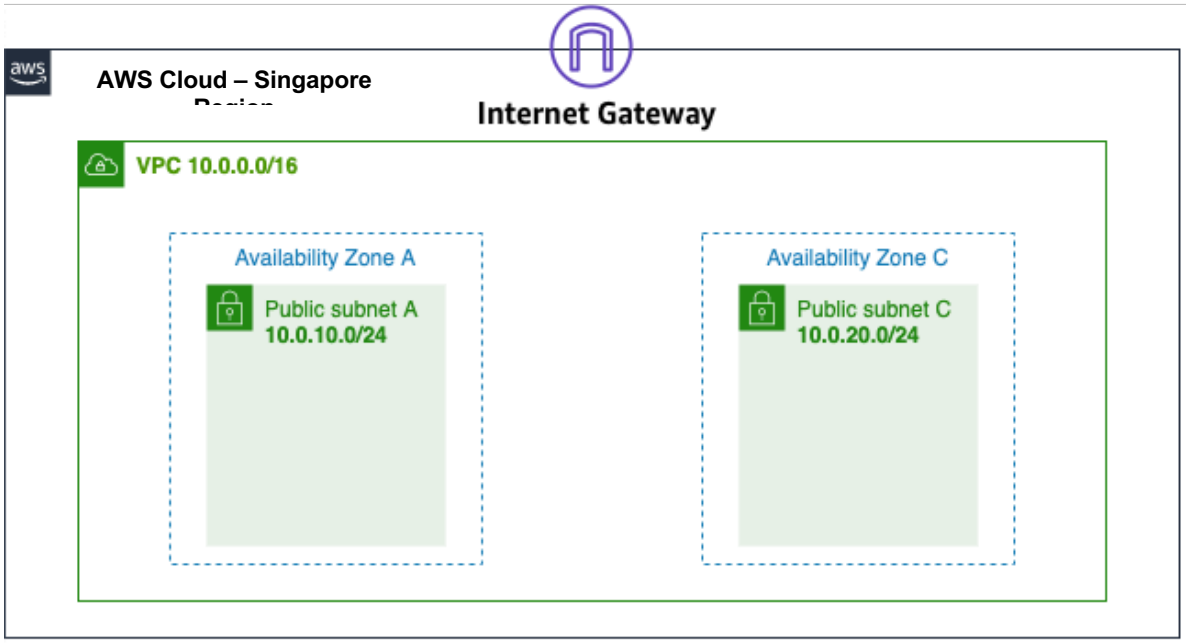


key	value
Subnet name	public subnet C
Availability Zone	ap-northeast-2c
IPv4 CIDR block	10.0.20.0/24
Name	public subnet C

4. You can see that both **public subnet A** and **public subnet C** have been created.



5. The architecture so far is as below.



3-3 Edit the routing table

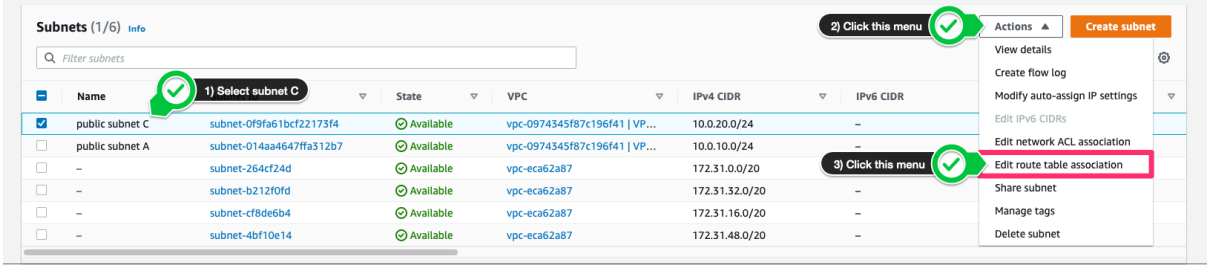
Understanding VPC route table

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

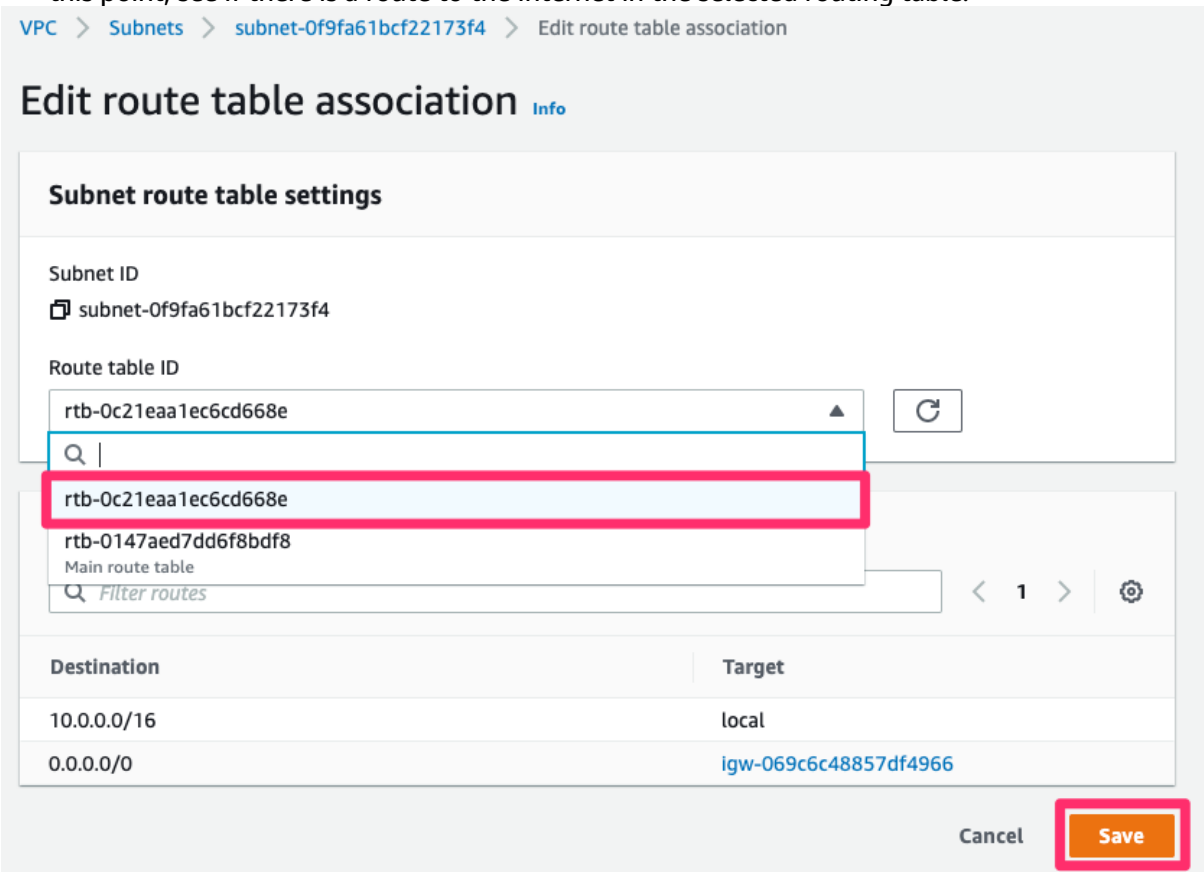
- **Main route table** automatically comes with your VPC. It controls the routing for all subnets that are not explicitly associated with any other route table.
- **Custom route table** A route table that you create for your VPC.

Edit routing table connection

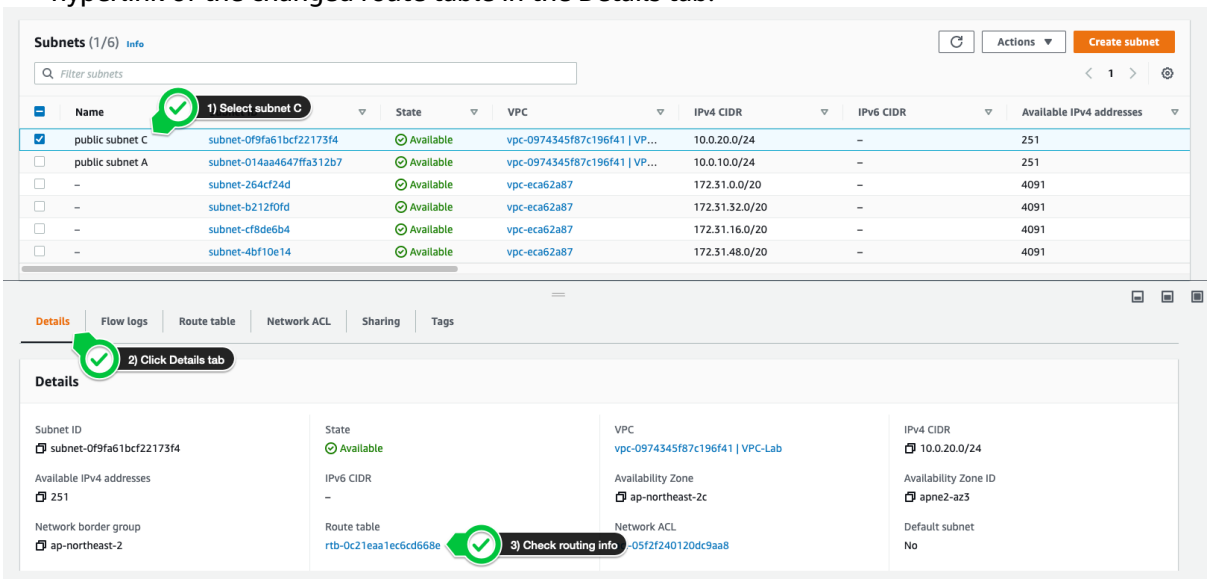
1. Click the **Actions** button in the **Subnet** menu and select **Edit routing table association**.



2. Select a route table **other than** the main route table from the route table ID and save it. At this point, see if there is a route to the Internet in the selected routing table.



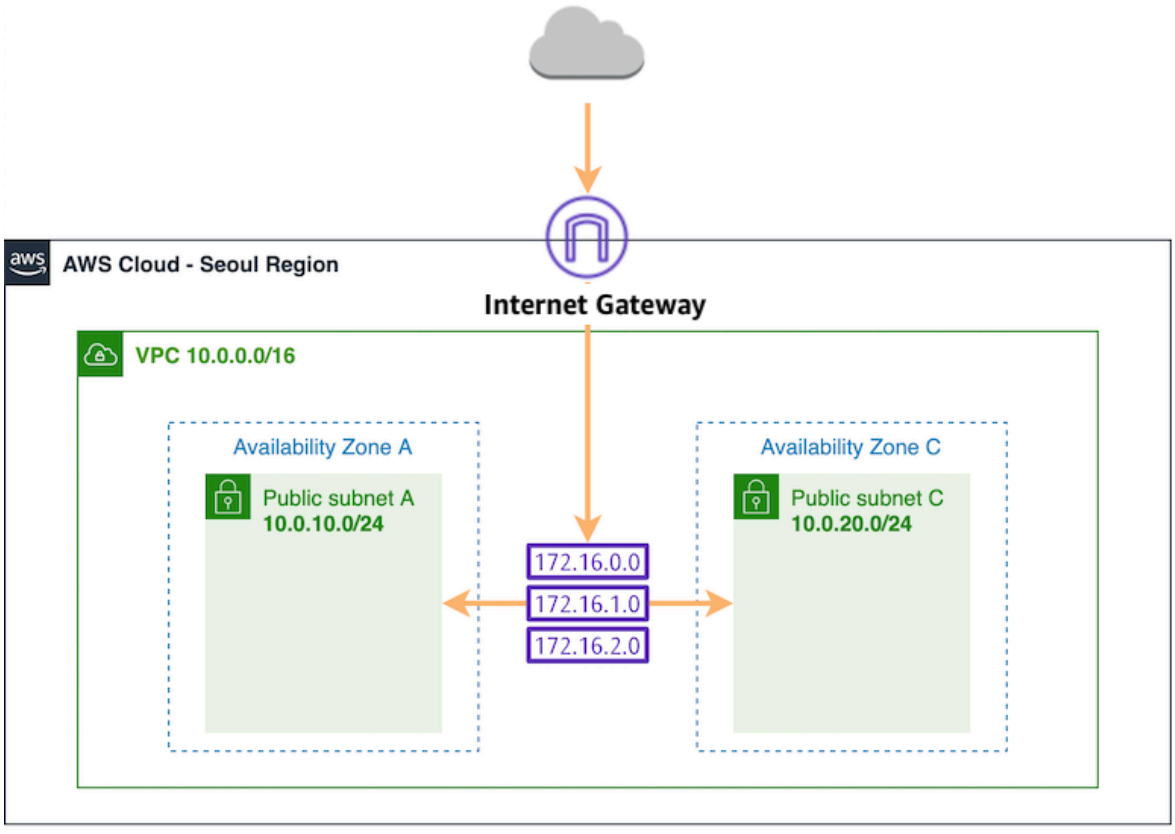
3. After selecting **public subnet C**, you can see the routing information by clicking the hyperlink of the changed route table in the Details tab.



After clicking the routing table, what you can see from **Route** tab is as below. As a result, we can confirm that a route to the internet has also been created for public subnet C.

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-OOO

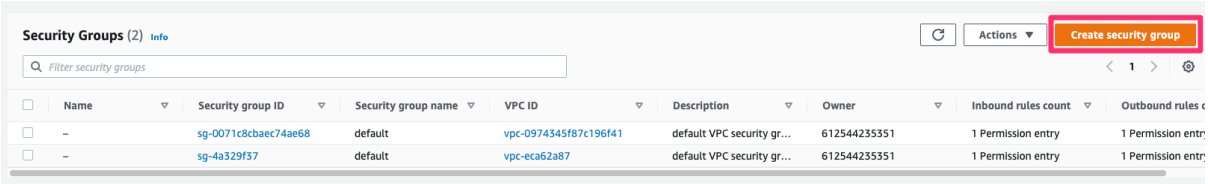
4. The architecture, so far, is as below.



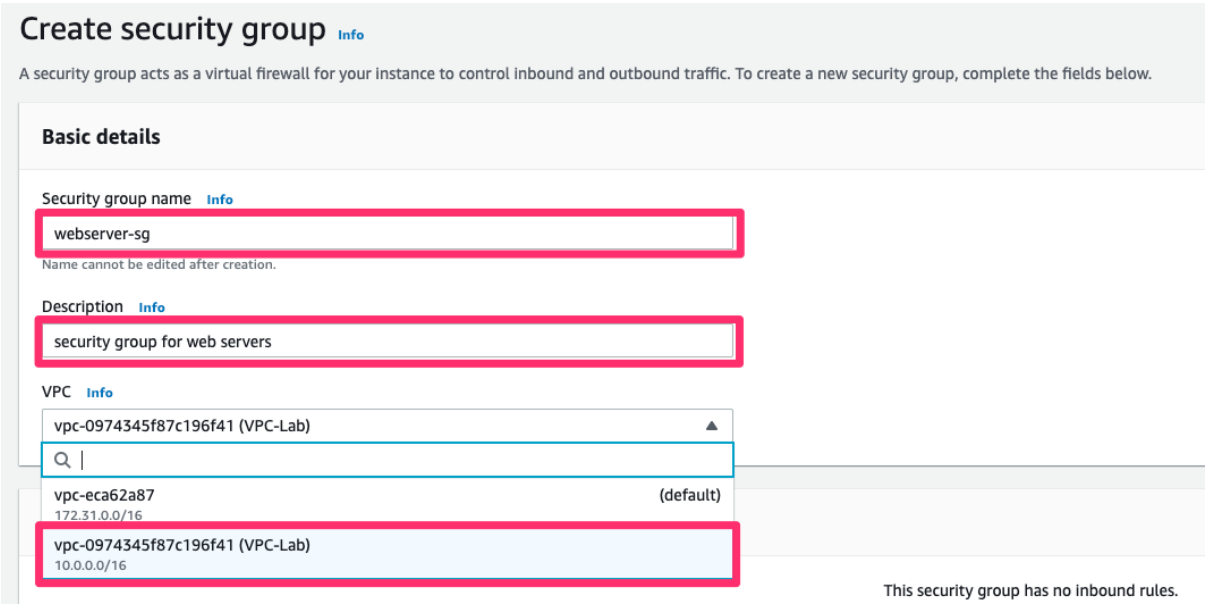
3-4 Create a security group

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic.

1. Click the **Security Groups** menu on the left sidebar, then click the **Create security group** button.

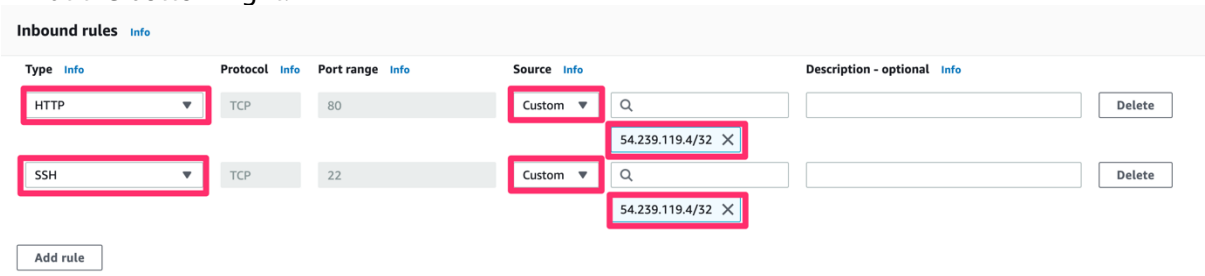


2. Enter the Security group name and Description as shown on the below screen and select the **VPC you created in this lab**



key	value
Security group name	webserver-sg
Description	security group for web servers
VPC	VPC-Lab

3. Add rules to the **Inbound rules** as shown below, and click the **Create security group** button at the bottom right.



Type	Source
HTTP	Custom: [Input your private IP address followed by a /32] (You can find you local IP by searching What is my IP.)
SSH	Custom: [Input your private IP address followed by a /32] (You can find you local IP by searching What is my IP.)

4. Review that the inbound rule has been created as shown below