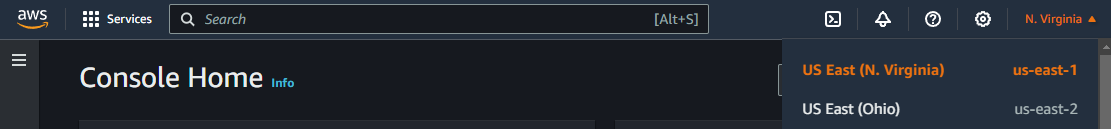
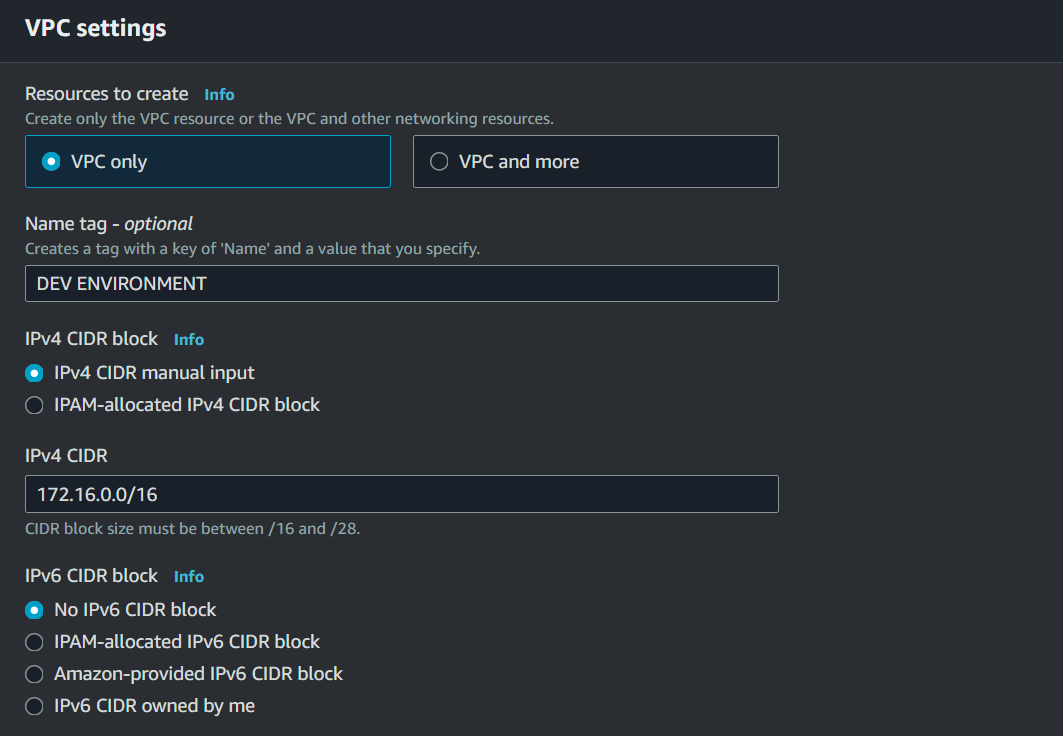
Start-to-Finish NAT INSTANCE LAB

# Set region to us-east1



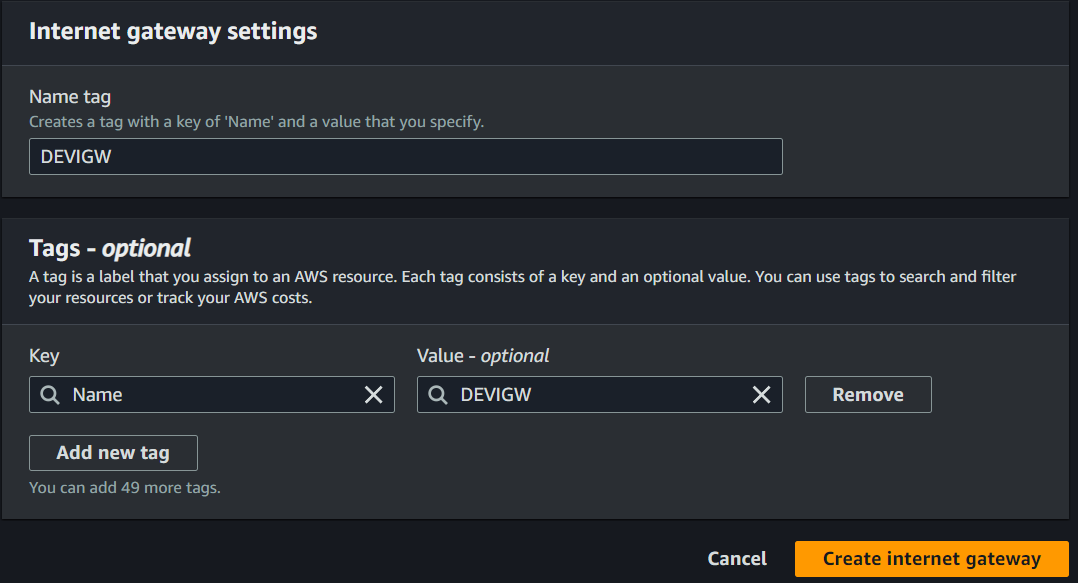
# Create VPC

* Search vpc in the searchbar
* Click vpc in the results > create vpc
* Vpc only
* Name: DEV ENVIRONMENT
* IPv4 CIDR - 172.16.0.0/16
* Create vpc



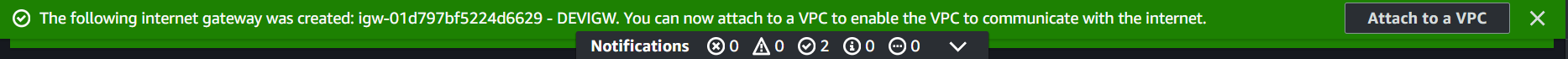
# Create Internet Gateway

* On the left side panel, click Internet Gateways & Create internet Gateway
* Name: DEVIGW
* Create internet gateway

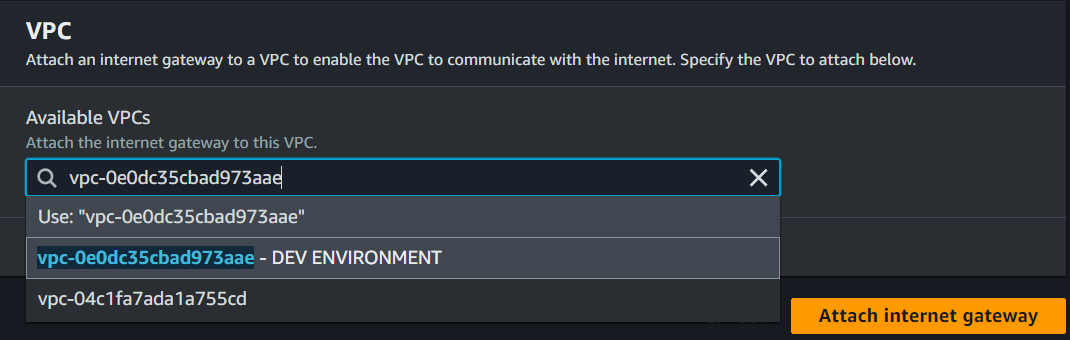


# Attach Internet Gateway

* Click the green attach to vpc

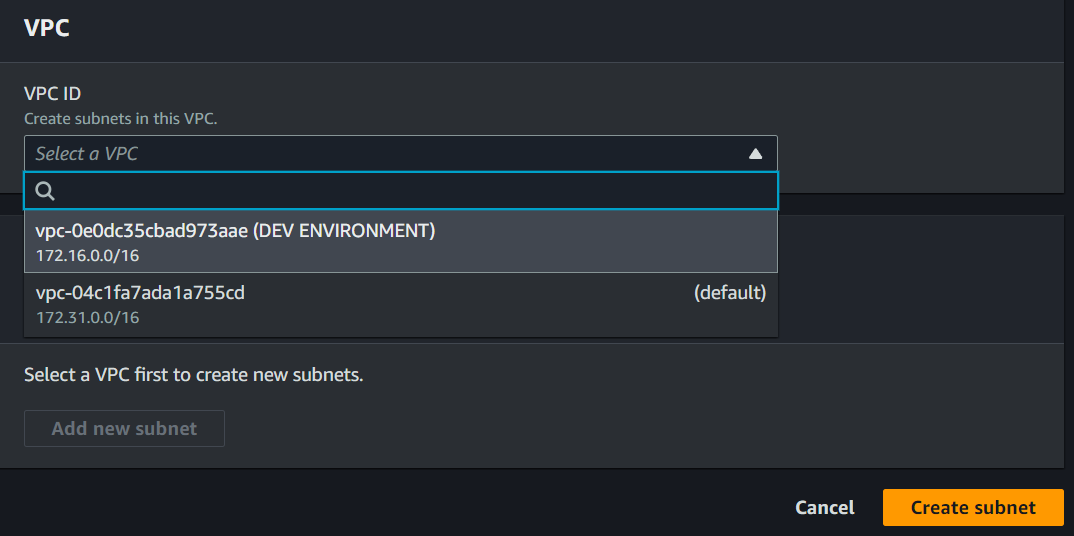


* Select the DEV ENVIRONMENT vpc
* Click Attach internet gateway



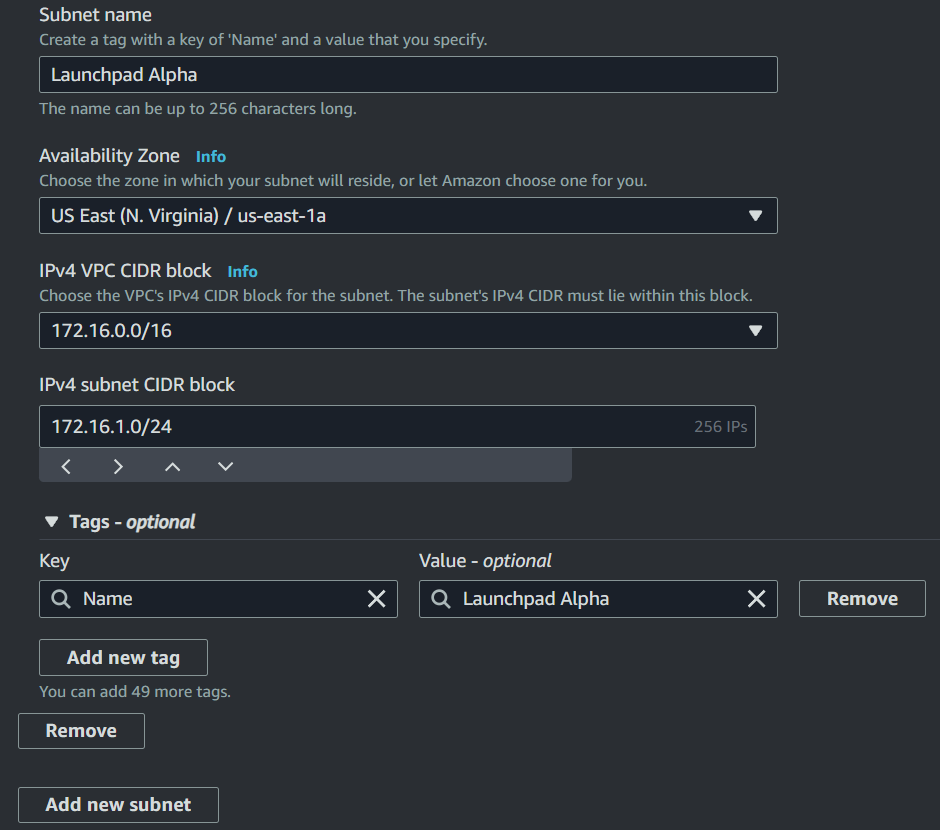
# Create Public Subnets

* On the left side panel, click subnets
* Click Create subnet
* Under VPC ID, Select DEV ENVIRONMENT



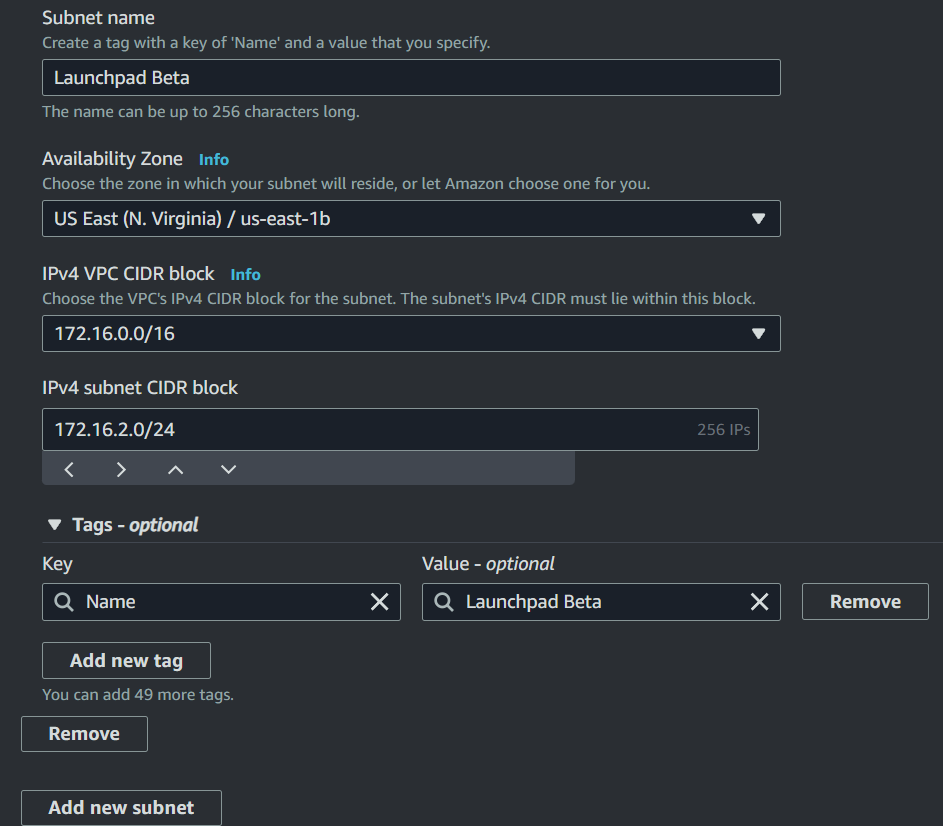
# Launchpad Alpha

* Name the first public subnet: Launchpad Alpha
* Availability zone: us-east-1a
* IPv4 VPC CIDR block: (should auto-populate) 172.16.0.0/16
* IPv4 subnet CIDR block 172.16.1.0/24
* Click add new subnet



# Launchpad Beta

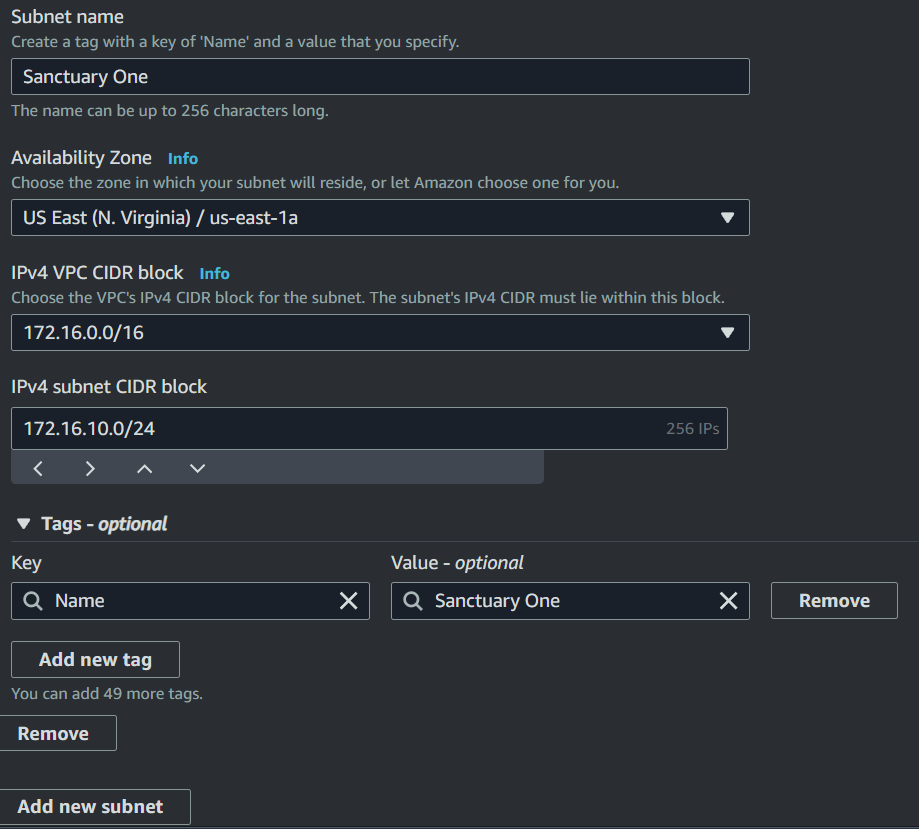
* Name the second public subnet: Launchpad Beta
* Availability zone: us-east-1b
* IPv4 VPC CIDR block: (should auto-populate) 172.16.0.0/16
* IPv4 subnet CIDR block 172.16.2.0/24
* Click add new subnet



# 

# Create Private Subnets (Sanctuary One)

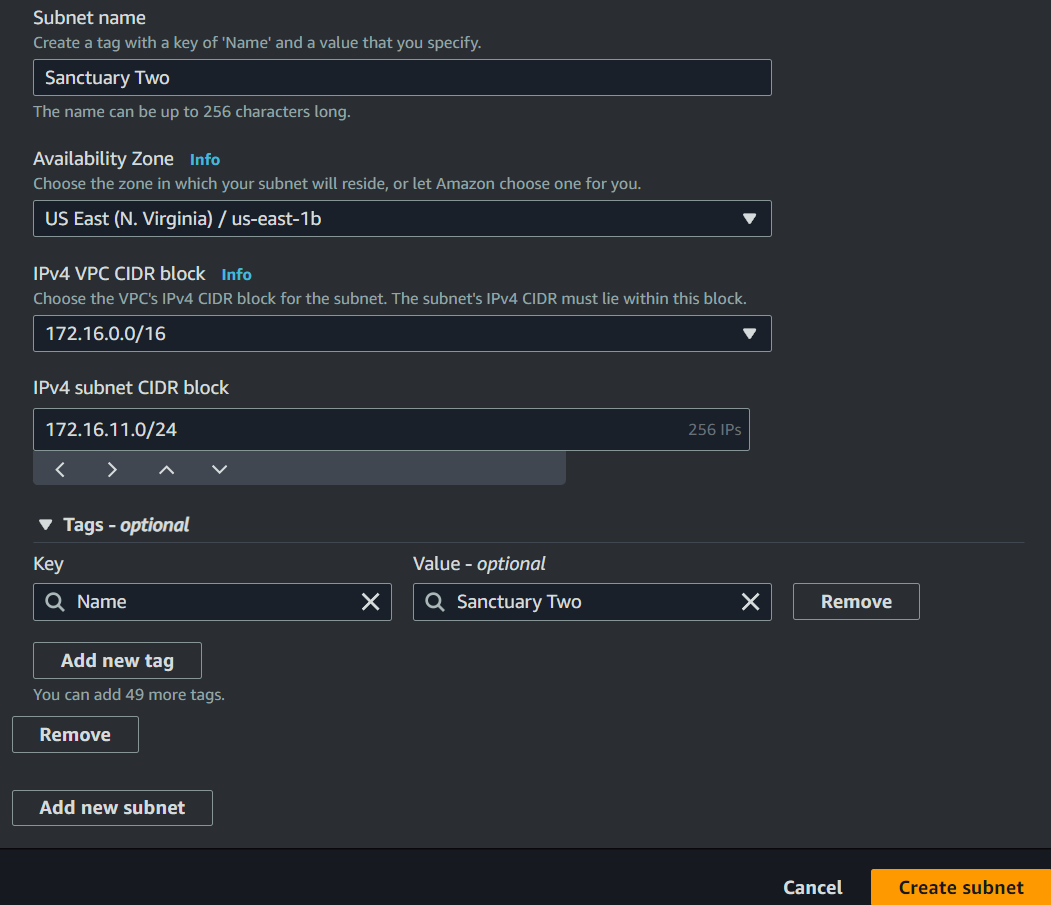
* Name the first private subnet: Sanctuary One
* Availability zone: us-east-1a
* IPv4 VPC CIDR block: (should auto-populate) 172.16.0.0/16
* IPv4 subnet CIDR block 172.16.10.0/24
* Click add new subnet



# 

# Sanctuary Two

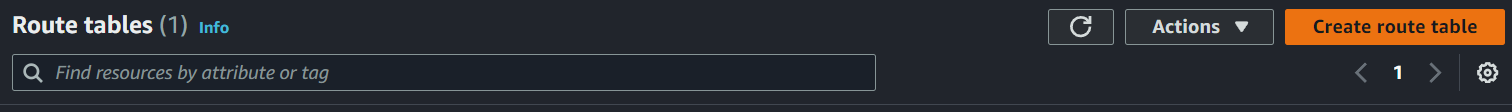
* Name the first private subnet: Sanctuary Two
* Availability zone: us-east-1b
* IPv4 VPC CIDR block: (should auto-populate) 172.16.0.0/16
* IPv4 subnet CIDR block 172.16.11.0/24
* Click Create subnet



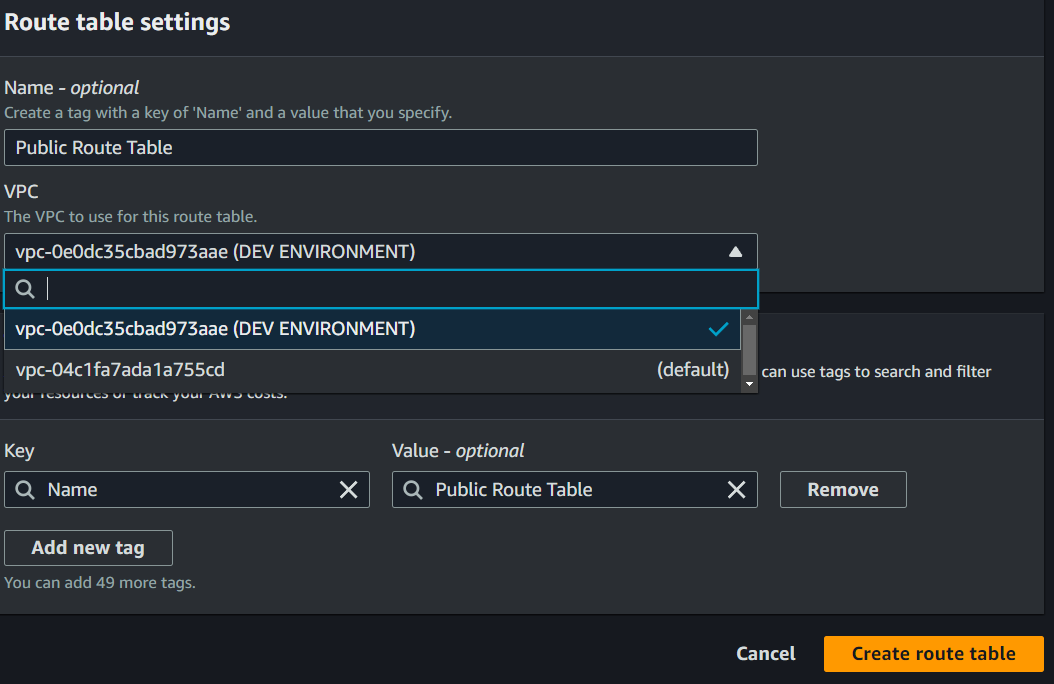
# 

# Create Public Route Table

* On the left side panel, click route tables, then Create route table



* name: Public Route Table
* Select DEV ENVIRONMENT



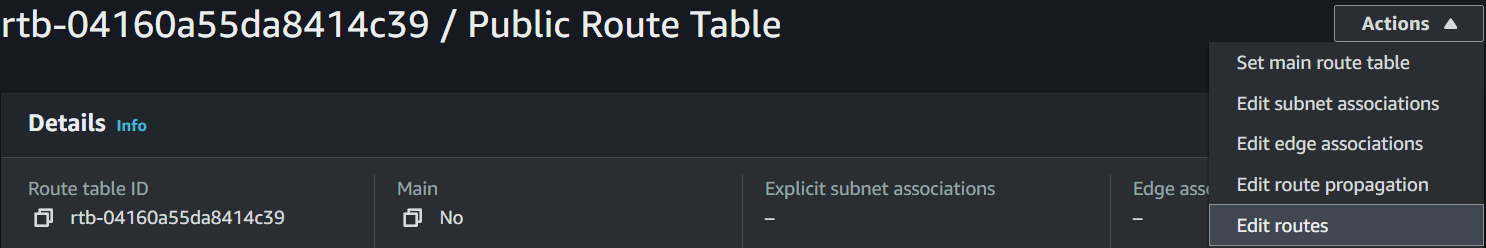
# 

# 

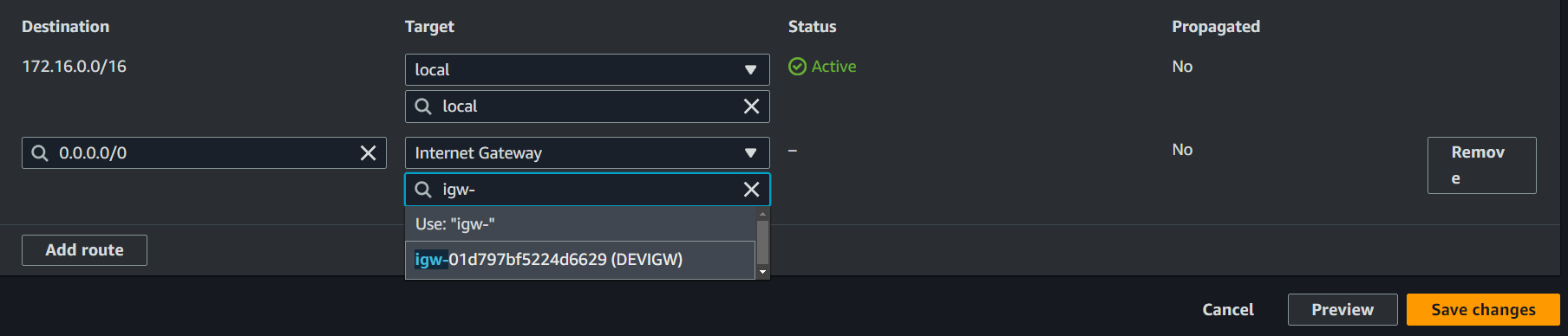
# 

# Edit Public Route Table

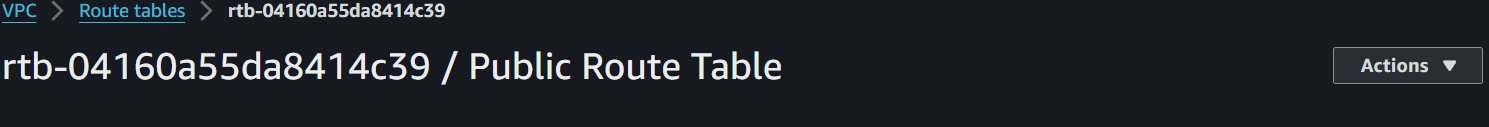
* Under Actions, Edit Routes



* Add route > 0.0.0.0/0 (Universal IP for internet access)
* Select Internet Gateway > Select DEVIGW > Save Changes

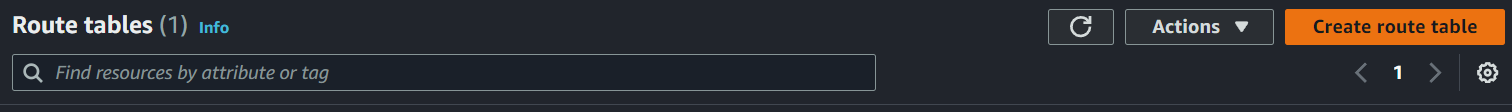


* Go back to Route Tables (highlighted blue)

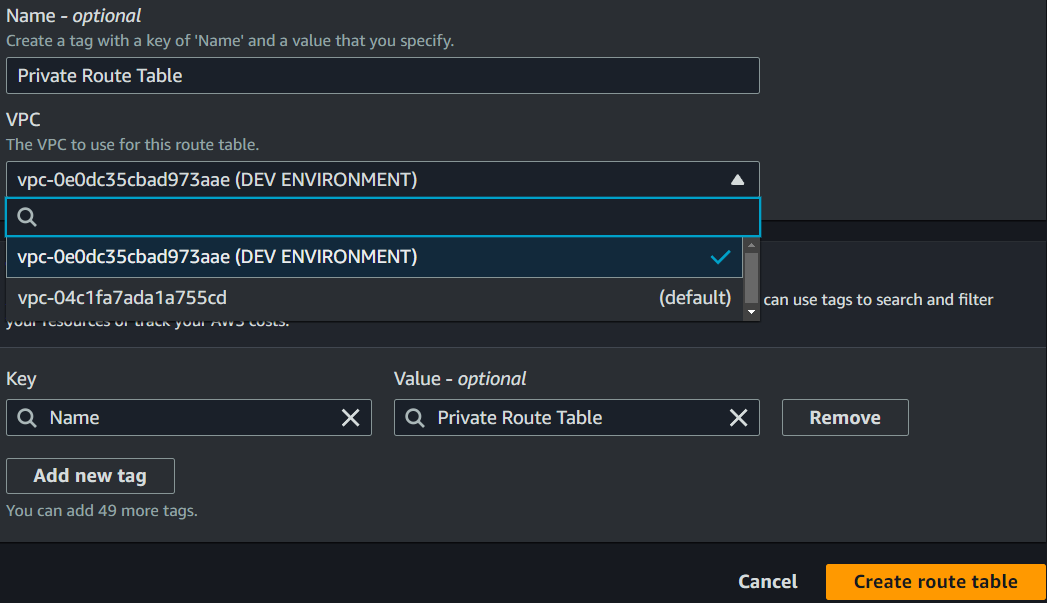


# Create Private Route Table

* Click Create route table

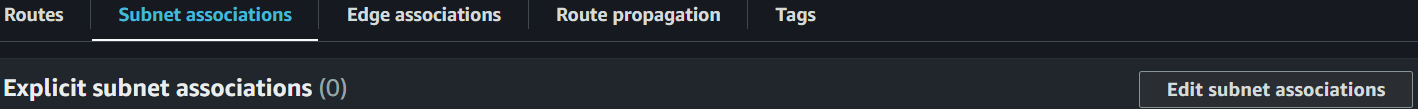


* name: Private Route Table
* Select DEV ENVIRONMENT > Create route table (this one does not get edited)

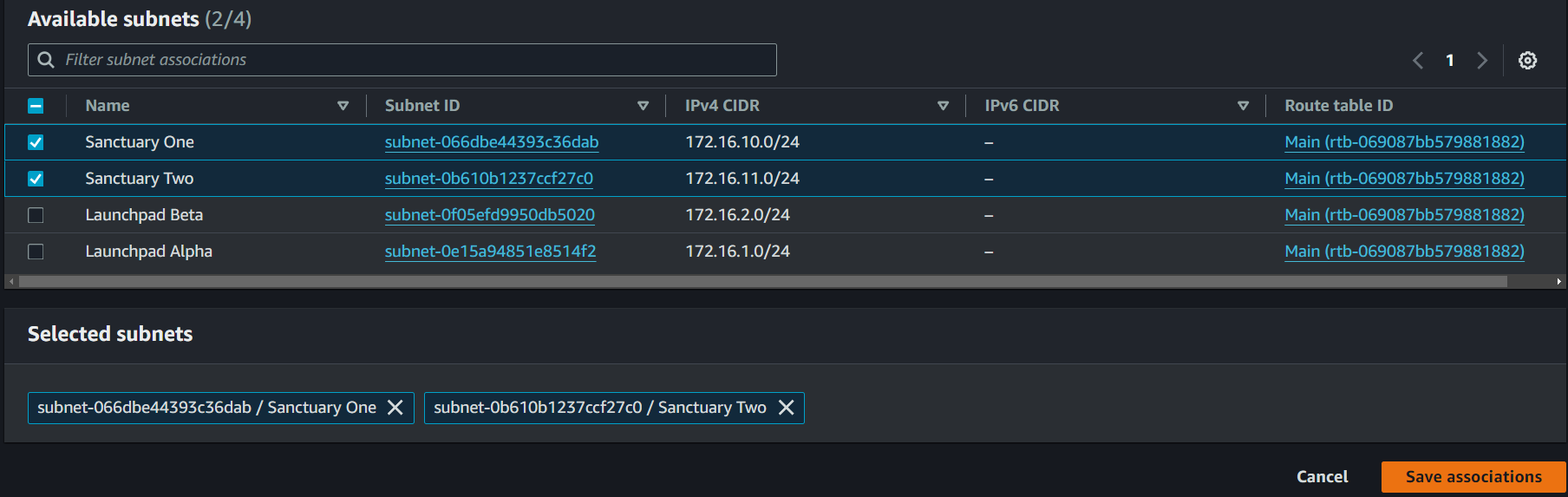


# Private Route Table Subnet Associations

* Click Subnet Associations > Edit subnet associations

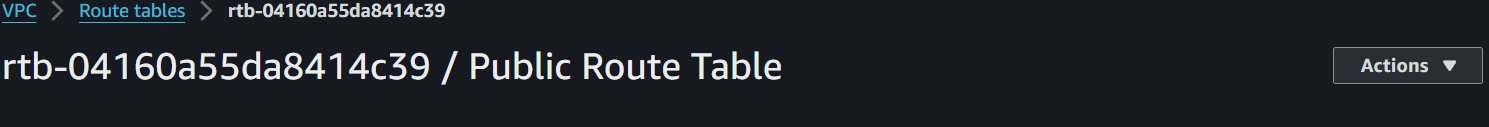


* Select sanctuary one and two, hit Save associations

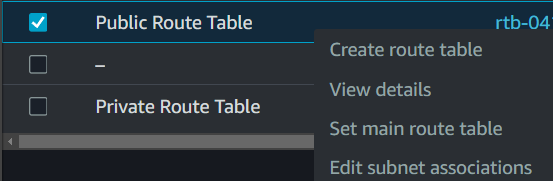


# Public Route Table Subnet Associations

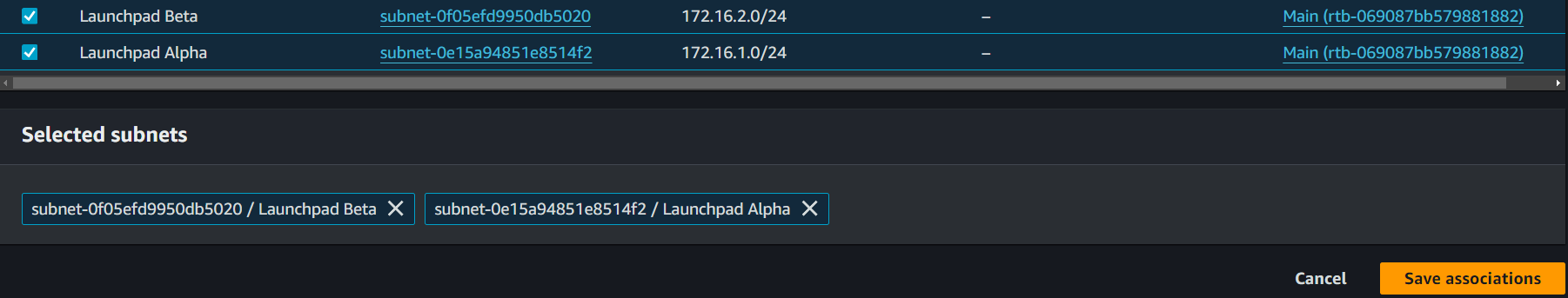
* Go back to Route Tables (highlighted blue)



* RIght click Public Route Table > Edit subnet associations



* Select Launchpad Alpha and Beta > Save associations

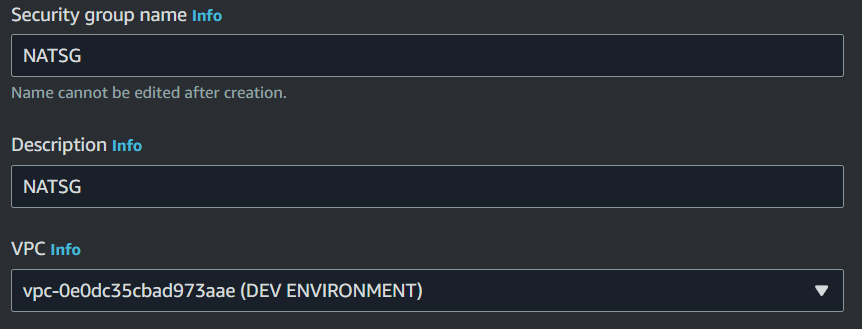


# Create NAT Security Group

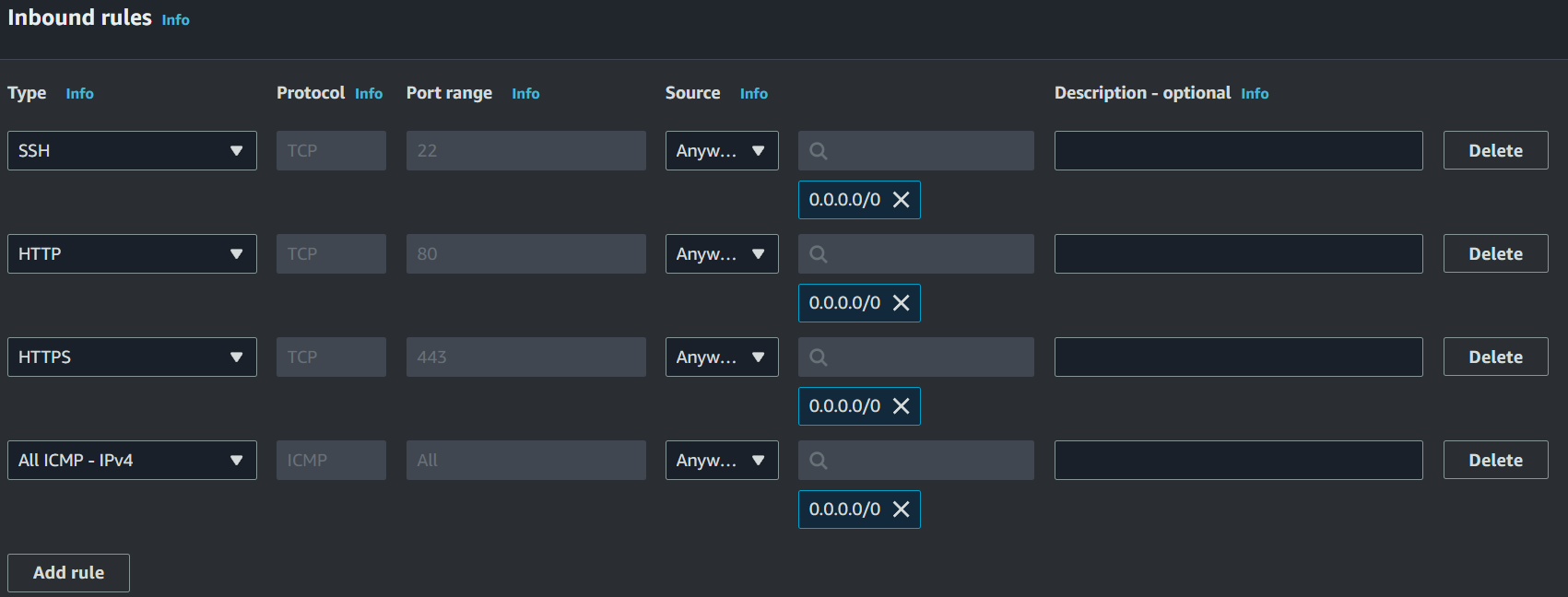
* On the left side look for Security > Security Groups
* Click create security group



* Name: NATSG > description: NATSG > select DEV ENVIRONMENT VPC



* Under Inbound rules, Add SSH Anywhere IPv4, Add HTTP Anywhere IPv4, Add HTTPS Anywhere IPv4, Add All ICMP - IPv4 Anywhere IPv4

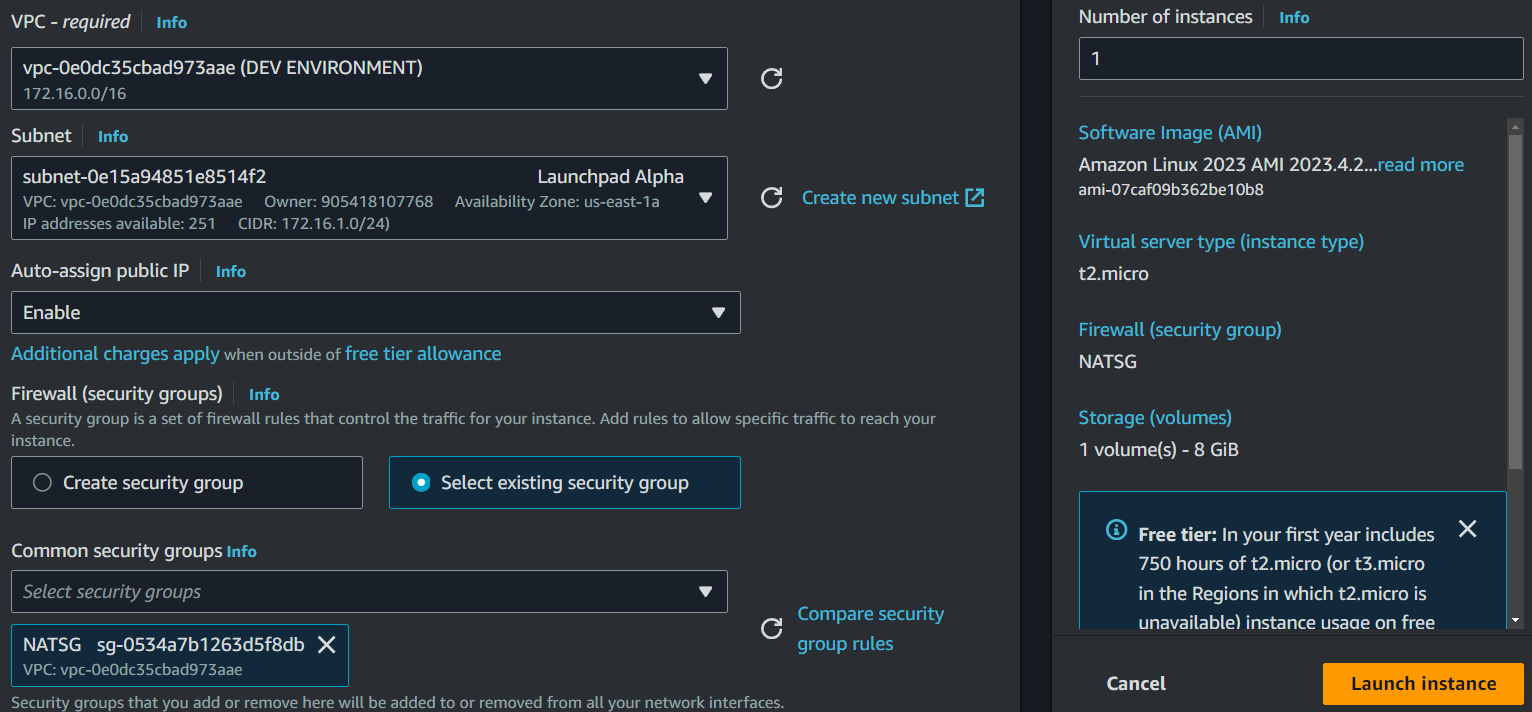


* Scroll down to the bottom of the page and hit Create security group



# Create EC2: JUMP SERVER

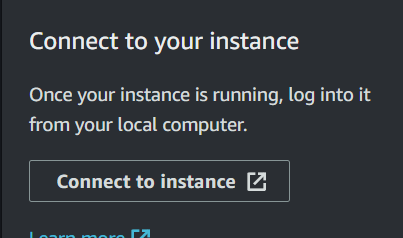
* Go to the ec2 dashboard > launch instance
* Enter name. JUMP SERVER
* Linux image
* Select key pair previously created
* Edit network settings
* Select DEV ENVIRONMENT VPC
* Subnet Launchpad Alpha (1a)
* Enable auto assign public ip
* Select existing security group > select NATSG (might need to hit refresh button)
* Launch instance



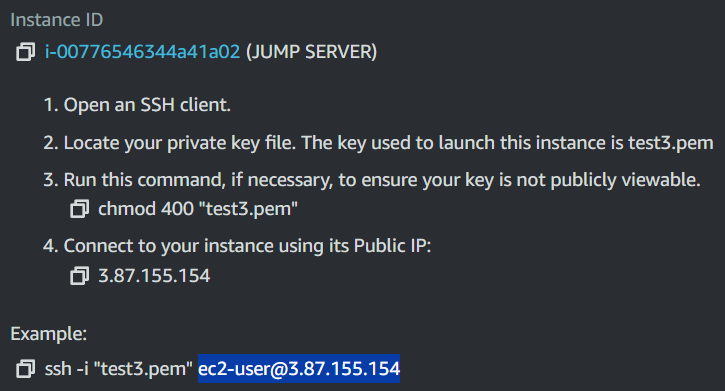
# 

# Connect to JUMP SERVER ec2 instance

* (wait a few minutes to allow instance to go into running state) Look for the connect to instance button right after creation

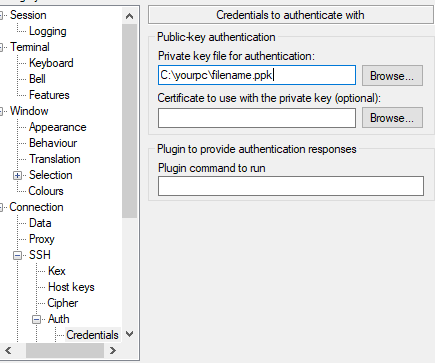


* This page will have all the info needed to connect to your instance.
* I will be using Putty, copy the “ec2-user@IP” and paste into the putty session host name

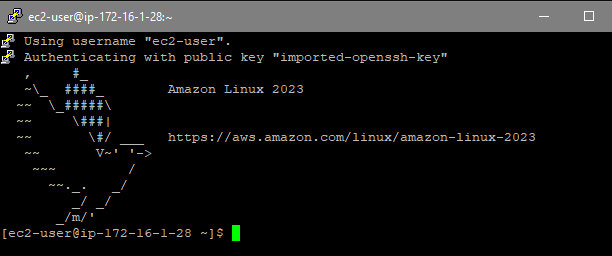




* Under the category dropdown menus, expand ssh > auth > click on credentials and browse for your ppk file

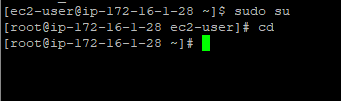


* Click open and accept
* If everything was done correctly you should see this

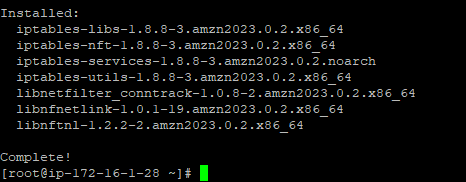


# JUMP SERVER COMMANDS

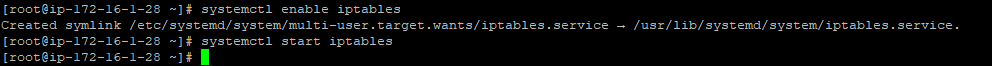
* Type these in manually, and enter the commands in the exact order shown (case sensitive) . Sometimes if you try to copy and paste it will add extra spaces and other formatting issues, causing syntax errors.
* sudo su (gives you root permissions)
* cd (takes you back to the root directory)



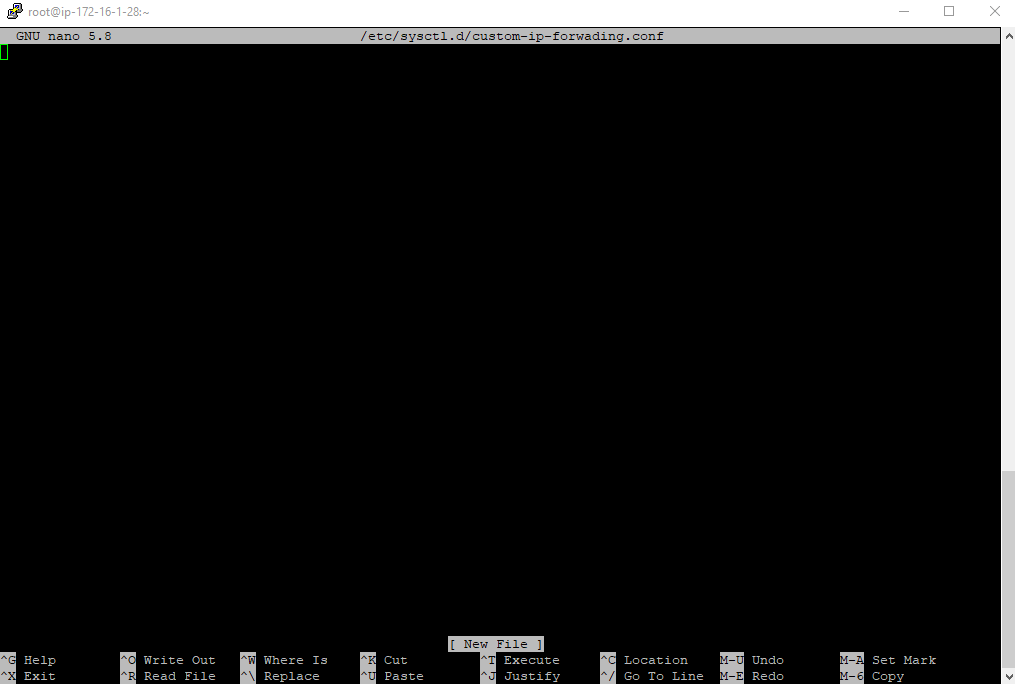
* yum update -y
* yum install iptables-services -y
* A download should have started, you should see the following packages for ip-tables installed and complete



* systemctl enable iptables
* systemctl start iptables



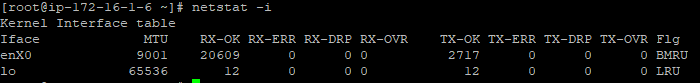
* The next commands are for enabling IP forwarding such that it persists after reboot
* nano /etc/sysctl.d/custom-ip-forwarding.conf
* The nano text editor should now be opened



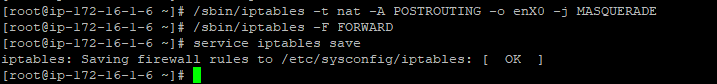
* Enter this line of text: net.ipv4.ip\_forward=1
* Ctrl S > Ctrl X
* Apply the configuration file we just created:
* sysctl -p /etc/sysctl.d/custom-ip-forwarding.conf
* A good output looks like this



* netstat -i (make note of the primary network interface enX0, lo is the loopback interface)

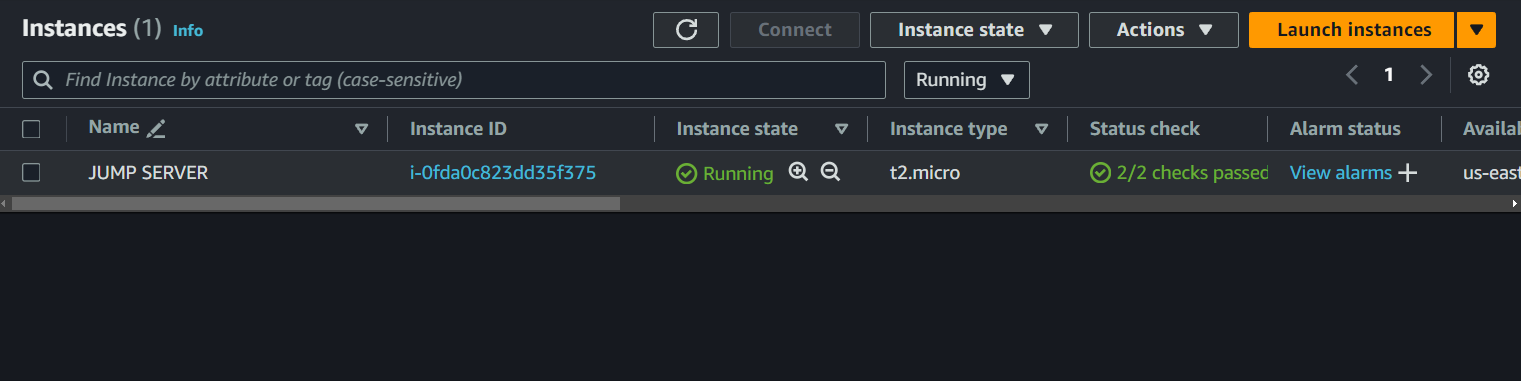


* /sbin/iptables -t nat -A POSTROUTING -o enX0 -j MASQUERADE
* /sbin/iptables -F FORWARD
* service iptables save

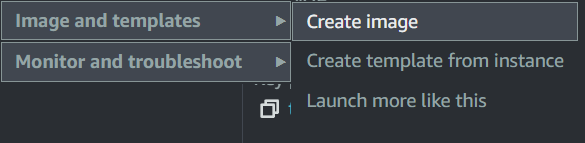


# Create NAT INSTANCE AMI Image

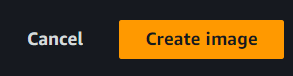
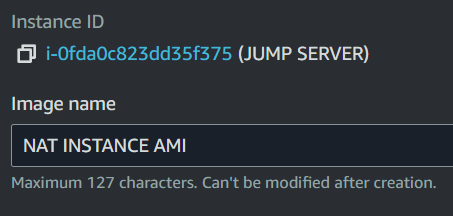
* Go to the ec2 dashboards where you can see all your instances



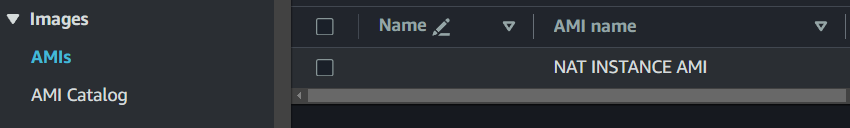
* Right click the jump server > Image and templates > create image



* Name: NAT INSTANCE AMI (we will soon be using this same name for an ec2 instance created from this template, using the same name for simplicity)
* Scroll down and click Create image



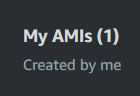
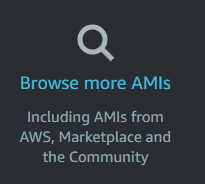
* On the left side panel, go to images > AMIs you should see the NAT INSTANCE AMI

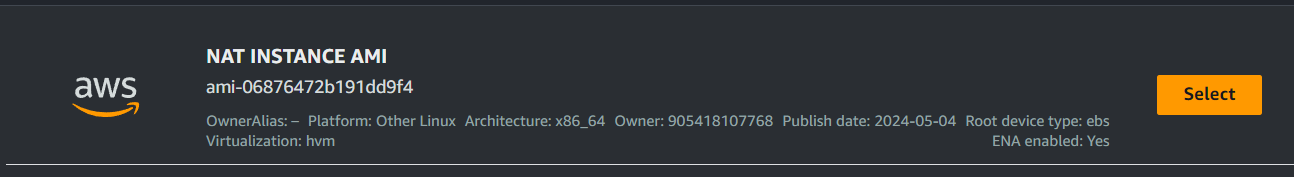


* You can now launch an ec2 instance using this snapshot

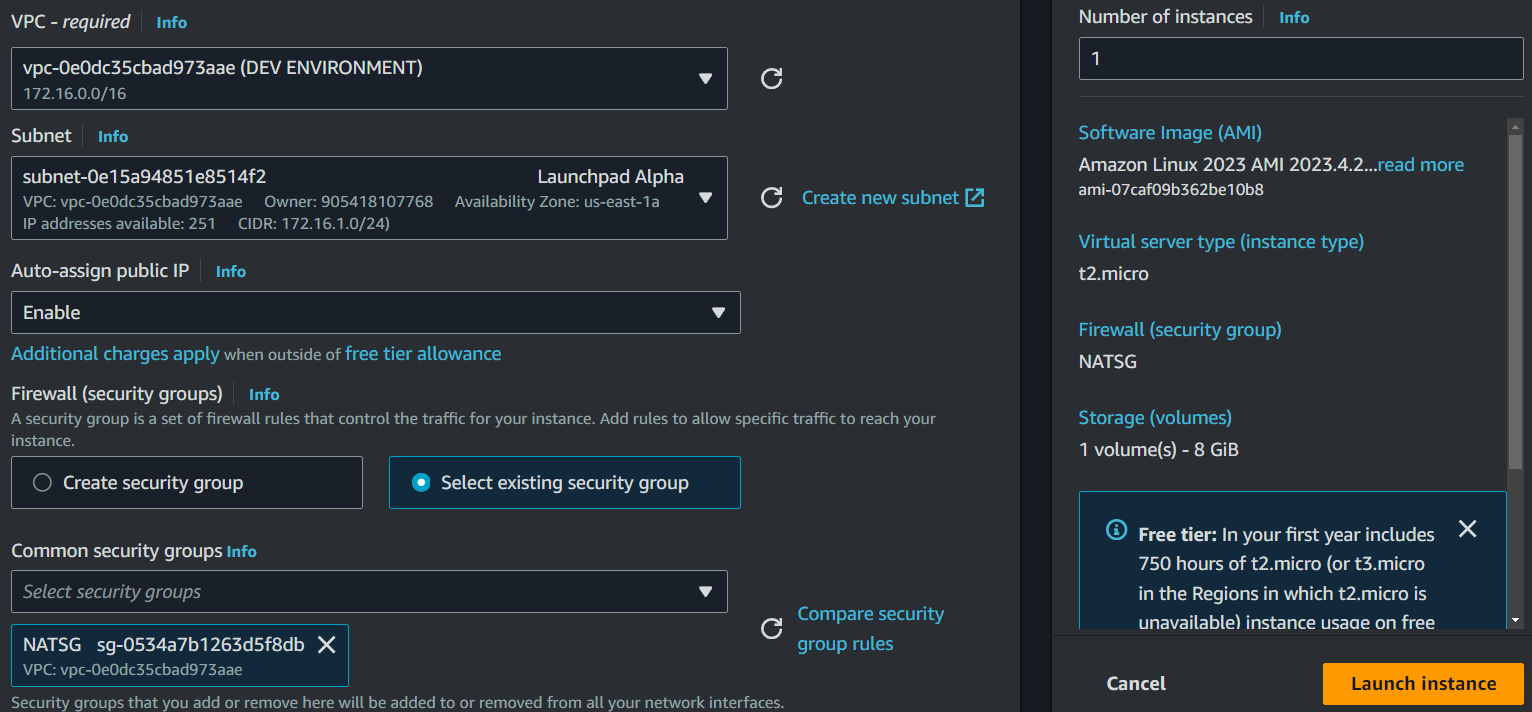
# Create EC2 NAT INSTANCE from Image Template

* Go to ec2 dashboard and launch a new instance
* Name: NAT INSTANCE AMI
* Browse more AMIs > My AMIs > select NAT INSTANCE AMI



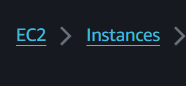


* Choose your keypair
* Edit network settings
* Select DEV ENVIRONMENT VPC
* Subnet: Launchpad Alpha
* Enable auto assign ip
* Select existing security group
* Select NATSG > Launch instance

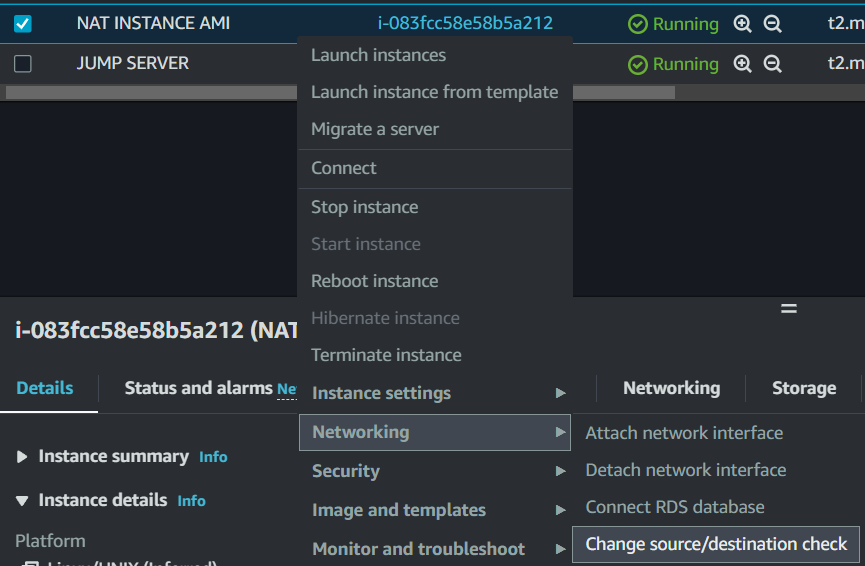


# Disable source/destination checks

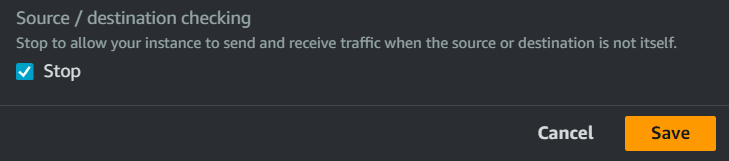
* Go back to instances (highlighted blue)



* Right click NAT INSTANCE AMI > Networking > change source/destination checks

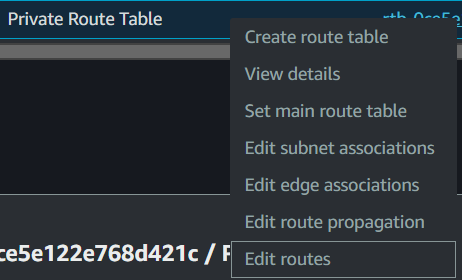


* Check stop > save

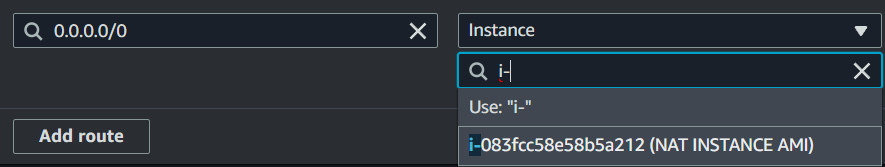


# Update the private route table

* Go back to the VPC dashboard and go back to route tables

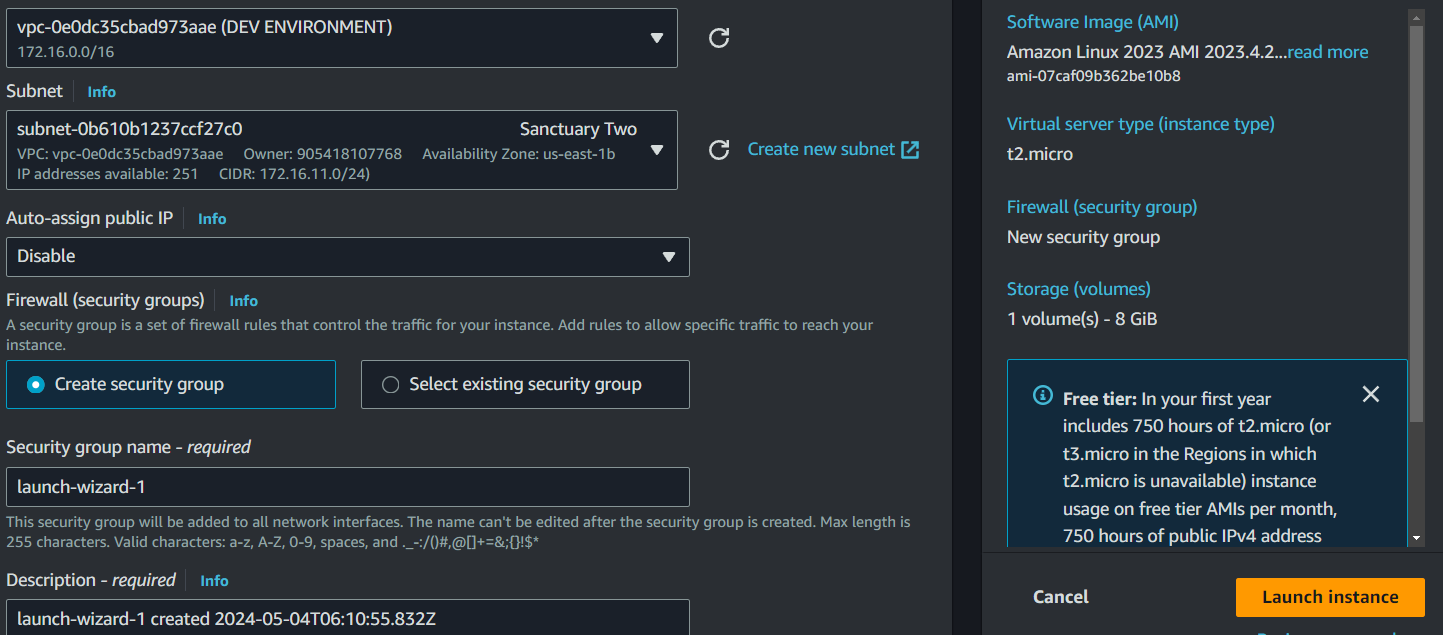


* Click add route
* 0.0.0.0/0 target: instance
* Click inside of the i- field and select NAT INSTANCE AMI > save changes

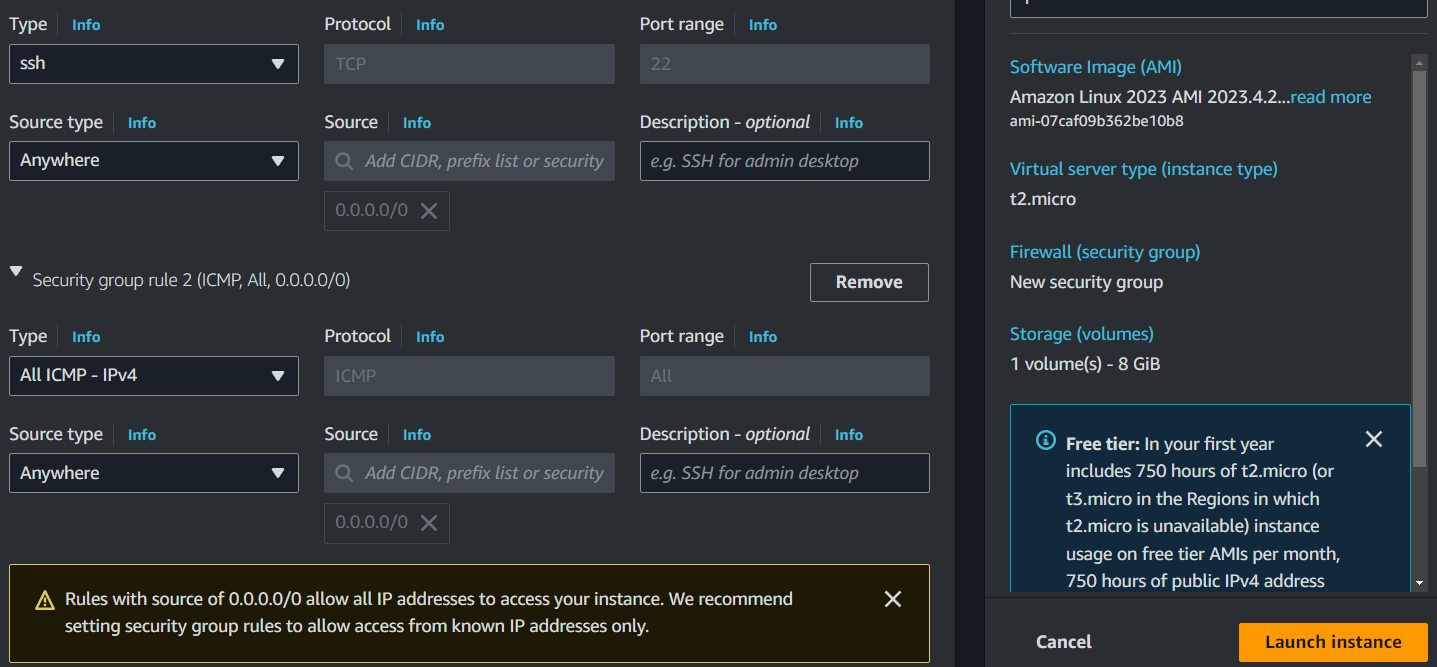


# Create Private EC2: SECURE SANCTUARY

* Go to the ec2 dashboard > launch instance
* Enter name. SECURE SANCTUARY
* Linux image
* Select key pair previously created
* Edit network settings
* Select DEV ENVIRONMENT VPC
* Subnet Sanctuary Two (1b)
* Disable auto assign public ip
* Create security group

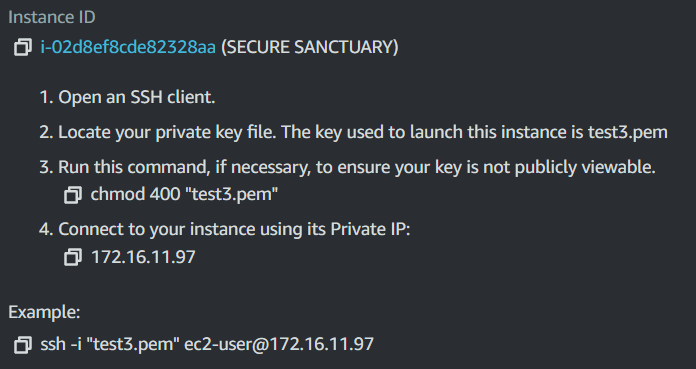


* Add security group rule: ALL ICMP - IPV4 / source Anywhere > Launch instance



# Connect to Secure Sanctuary from the jump server

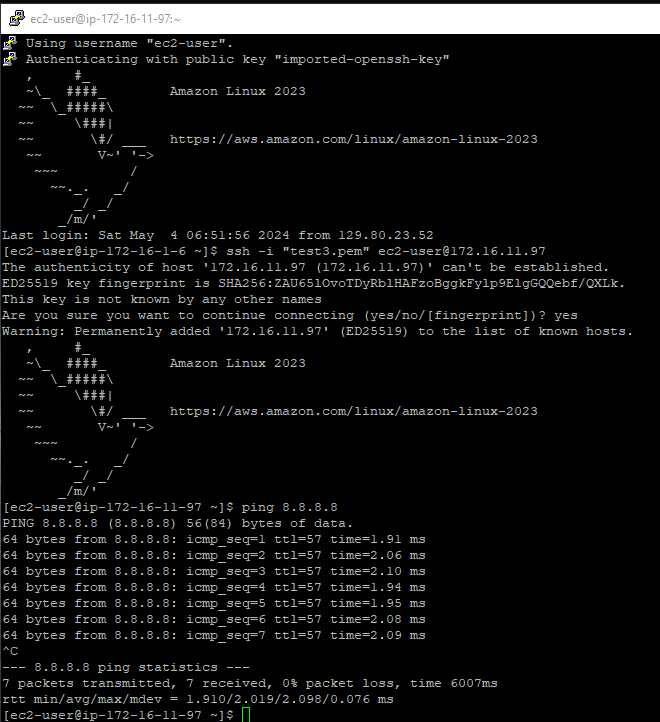
* NOTE: your Jump Server instance may have disconnected at some point during the process, go back to the list of ec2 instances and find the instructions for the Jump Server on your connect page. You shouldn’t have to enter the commands again just ssh back in.
* Go back to where your instances are shown, find the Secure Sanctuary connect page, these are the steps you will need to follow



* Before you begin, you will need to paste the contents of your pem file key into a new text file with a 100% matching filename on the jump server.
* To do this, go to your jump server in putty and type this command:
* nano yourkeyname.pem ←– make sure this file name matches what you have under the SSH client tab on the connect to instance screen
* This should open a newly created text file in the nano editor

# Preparing Key for ssh connection

* Locate the pem file you used to create your key on your computer
* Right click and open with a text editor (i just use notepad.exe)
* Ctrl a to select all contents, ctrl c to copy (cant screenshot what my key looks like)
* Right click inside the nano text space and your key should be pasted inside.
* Ctrl S > CTRL X
* Now you can proceed with the instructions shown on the connect to instance page
* chmod 400 "yourkeyname.pem"
* Example: ssh -i "test3.pem" ec2-user@172.16.11.97
* Yes to accept fingerprint
* You should now see two birds
* Note: if you get a permission error, it means the chmod command failed. You may have to generate new keys, which will require you to make all the instances again with the new key.



* If you can ping google (ping 8.8.8.8) then you have successfully completed the NAT INSTANCE LAB :)