AWS – VPC

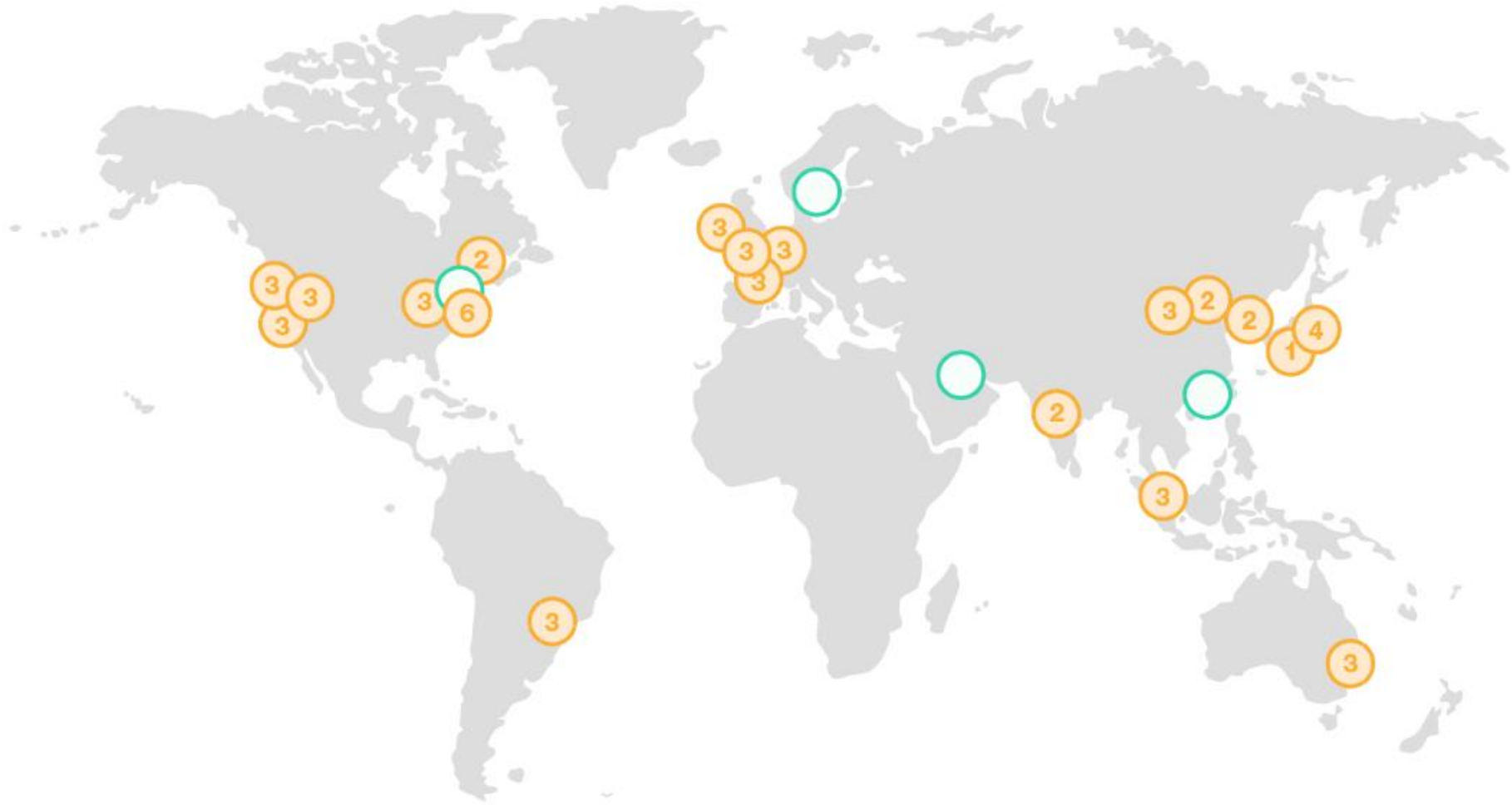
VISHWANATH M S

VISHWACLOUDLAB.ORG

Concepts of Region and Availability Zone

- AWS has 18 regions , out of which 3 are China Regions, which are not accessible.
- Each region has min of 2 Datacenter’s (Availability Zone) and max of 6 AZ.
- Each datacenter(Availability Zone) are interconnected with HIGH BANDWIDTH (BACKHOLE LINK, more than 1000Gbps)
- Each Region is also connected with other region. (The speed might be less when compared to above).
- REGION IS NOT EQUAL TO COUNTRY

Global Infrastructure



**Region & Number of Availability Zones**

New Region (coming soon)

List of Region and AZ count

Region & Number of Availability Zones

US East
N. Virginia (6),
Ohio (3)

US West
N. California (3),
Oregon (3)

Asia Pacific
Mumbai (2),
Seoul (2),
Singapore (3),
Sydney (3),
Tokyo (4),
Osaka-Local (1)[1]

Canada
Central (2)

China
Beijing (2),
Ningxia (3)

Europe
Frankfurt (3),
Ireland (3),
London (3),
Paris (3)

South America
São Paulo (3)

AWS GovCloud (US-West) (3)

New Region (coming soon)

Bahrain

Hong Kong SAR, China

Sweden

AWS GovCloud (US-East)

Creation of VPC (Basic networking)

- Basic Four Steps to create an basic Network platform for your Virtual Datacenter.
  - **Create a VPC**
  - Create Subnet
  - Create Internet Gateway
  - Modify/update Routing Table.

Concepts VPC

- VPC is the Base for all the connectivity's inside your Virtual Datacenter on AWS.
- VPC is part of one region only.
- By Default 2 different VPC's **DOES not** talk to each other
- All the Network's Within the same VPC can talk to each other.
- An Subnet can be part of "1" VPC only with assigned to "1" AZ only.

Step1 : Creation of VPC

- By default in an account, all the Regions has an Default VPC created by AWS With **“172.31.0.0/16”**
- Also default “Subnets” are created for these VPC’s in the Regions, eg:-- **“172.31.0.0/20”**
- We should be creating VPC with “**IPV4 Private IP**” ranges only.

Private IPV4

Class A – 10.0.0.0 to 10.255.255.255

Class B – 172.16.0.0 to 172.31.255.255

Class C – 192.168.0.0 to 192.168.255.255

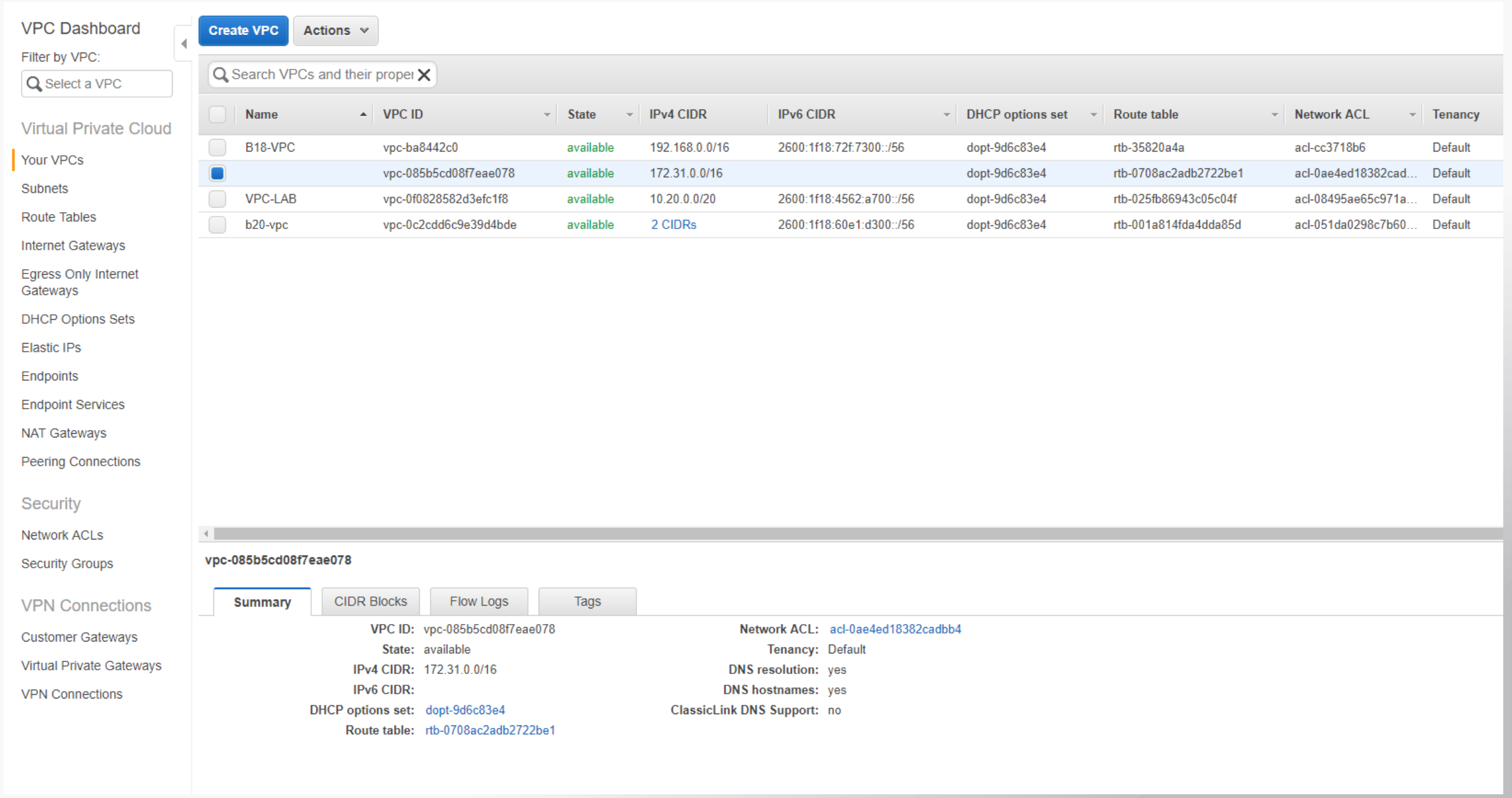
- Select a VALID NETWORK FOR VPC CIDR

After Creation of VPC

- An VPC ID is created.
- IPv6 public address block is assigned by AWS to your VPC (**if enabled**)
  - By default the public network would be **"/56" Network**.
- Default DHCP option Set gets assigned.
  - DNS Resolution is by default "yes". This helps all the VM's In the VPC to resolve any "Name" to "ip address".
  - DNS Hostname is by default "No". Change it to "yes", this helps to provide an public DNS hostname to your VM's.
- Default Routing Table gets created.
- Default Network ACL gets created. → By default all the Traffic Inbound and Outbound are **ALLOWED.**

Note:-- NACL – Network Access Control List

We can add "Main Network" to the same VPC.



Limitations of VPC

- Cannot create a VPC only on **IPV6.**
-

Creation of VPC (Basic networking)

- Basic Four Steps to create an basic Network platform for your Virtual Datacenter.
  - Create a VPC
  - **Create Subnet**
  - Create Internet Gateway
  - Modify/update Routing Table.

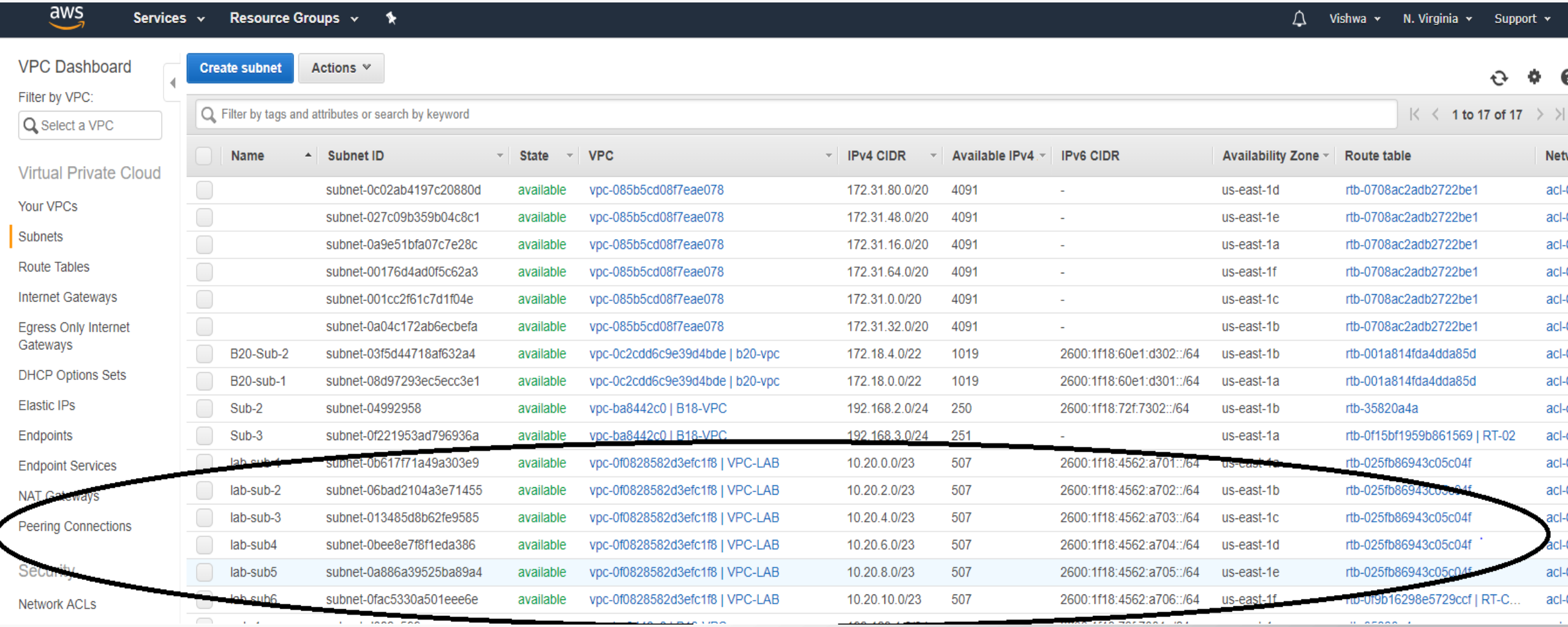
Step2: Creation of Subnet

- After manual Subnetting of the VPC CIDR, we would be creating the Subnets.
- Select the Appropriate “VPC”
- Assign the “CIDR” for the Subnet. (Means the Subnetwork)
- Assign the Availability Zone (Datacenter)
  - Eg: -- “Us-east-1” refers to N.Virginia and “a” to “f” refers to the Datacenters available in that Region.
  - **SUBNET CANNOT BE CHANGED TO A DIFFERENT AVAILABILITY ZONE AFTER CREATION OF IT.**
- Allocated IPv6 from the given ::/64 Network.

After Creation of Subnets

- Subnet ID is created.
- if IPv6 was enabled, each Subnet get "**/64**" subnet network from the main Network assigned in the VPC.
- Each subnet has **"5"** Ip's blocked for AWS usage.
  - The First IP is the Network ID, eg:-- **172.30.1.0/24**
  - The Second IP is the First usable IP also called as Default Gateway for the subnet: **172.30.1.1/24**
  - The Last IP is the Broadcast, eg:-- **172.30.1.255/24**
  - There are 2 more IP's , that are used internally by the **"Virtual Router"** for Failover.

Note: -- VPC's one of the function is "Virtual Router"



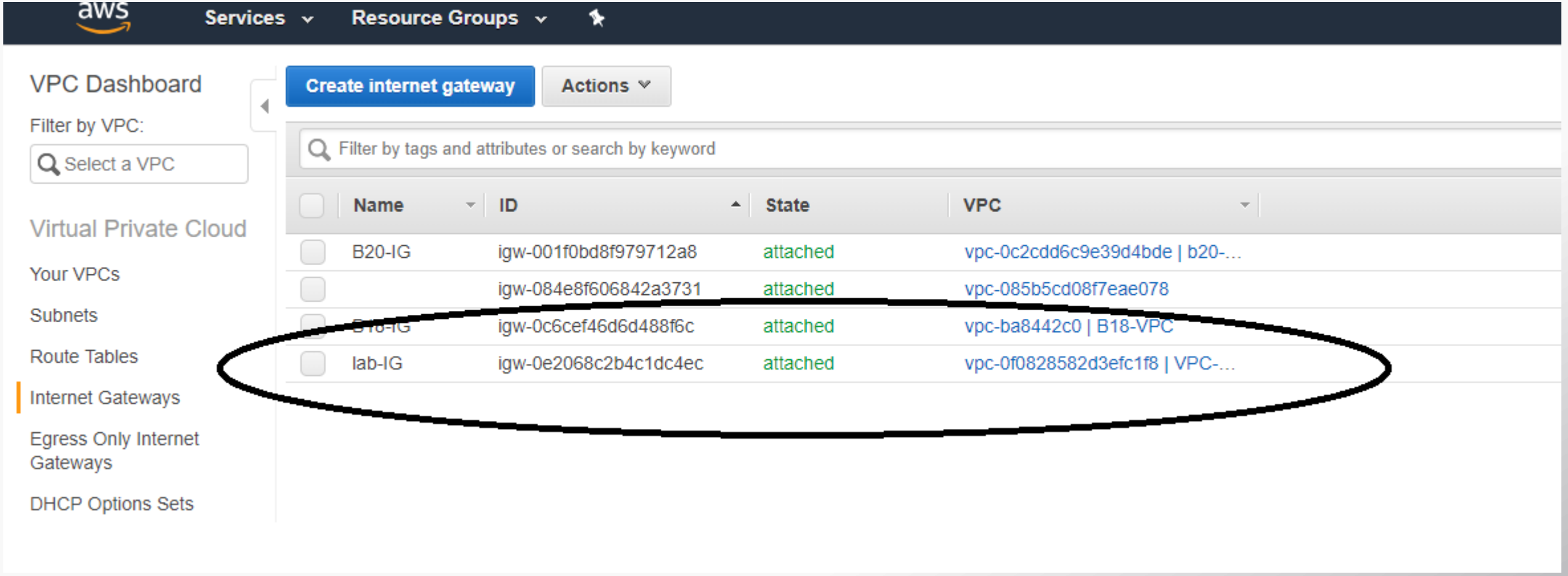
Creation of VPC (Basic networking)

- Basic Four Steps to create an basic Network platform for your Virtual Datacenter.
  - Create a VPC
  - Create Subnet
  - **Create Internet Gateway**
  - Modify/update Routing Table.

Step3: Creation of Internet Gateway

- Internet Gateway is created to intimate VPC that it would have internet connection
- Its just an Interface that gets created on the VPC
- After creating the Internet Gateway, we would need to Attach it to an VPC.

•Note:-- ONE VPC CAN HAVE ONLY ONE INTERNET GATEWAY

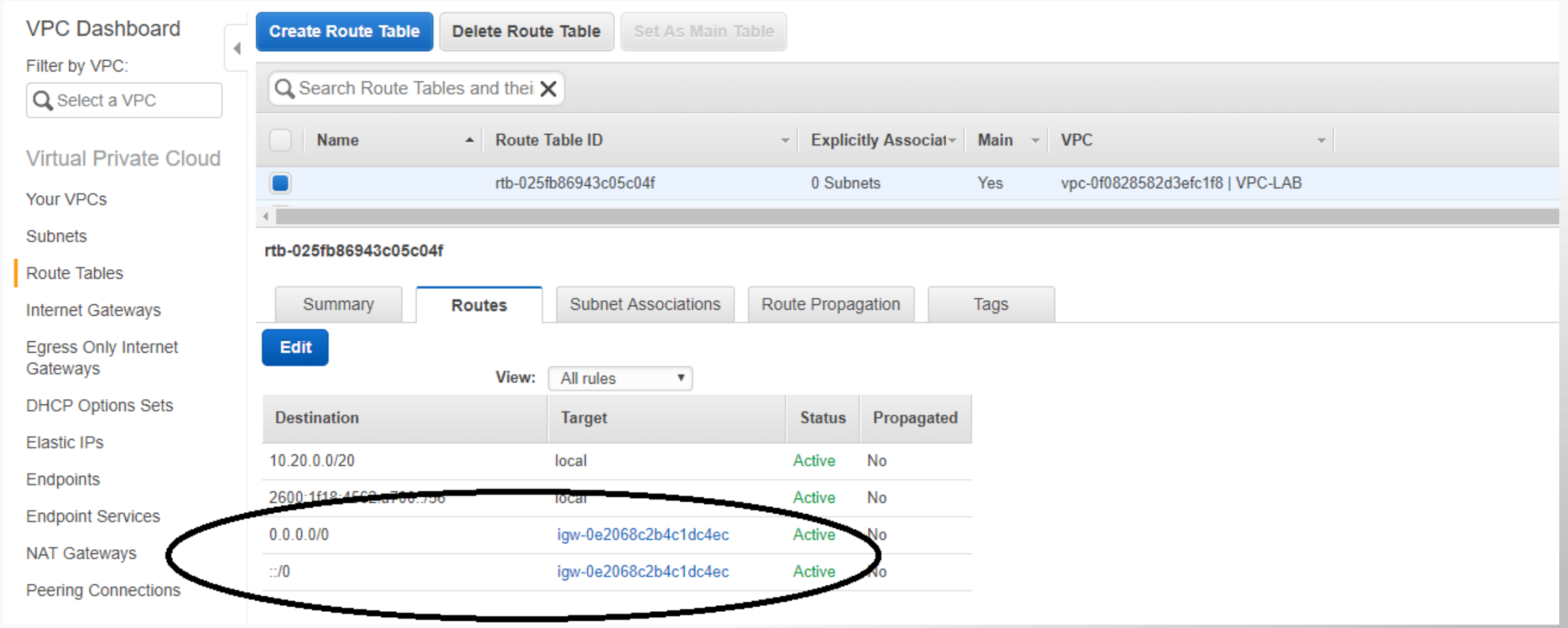


Creation of VPC (Basic networking)

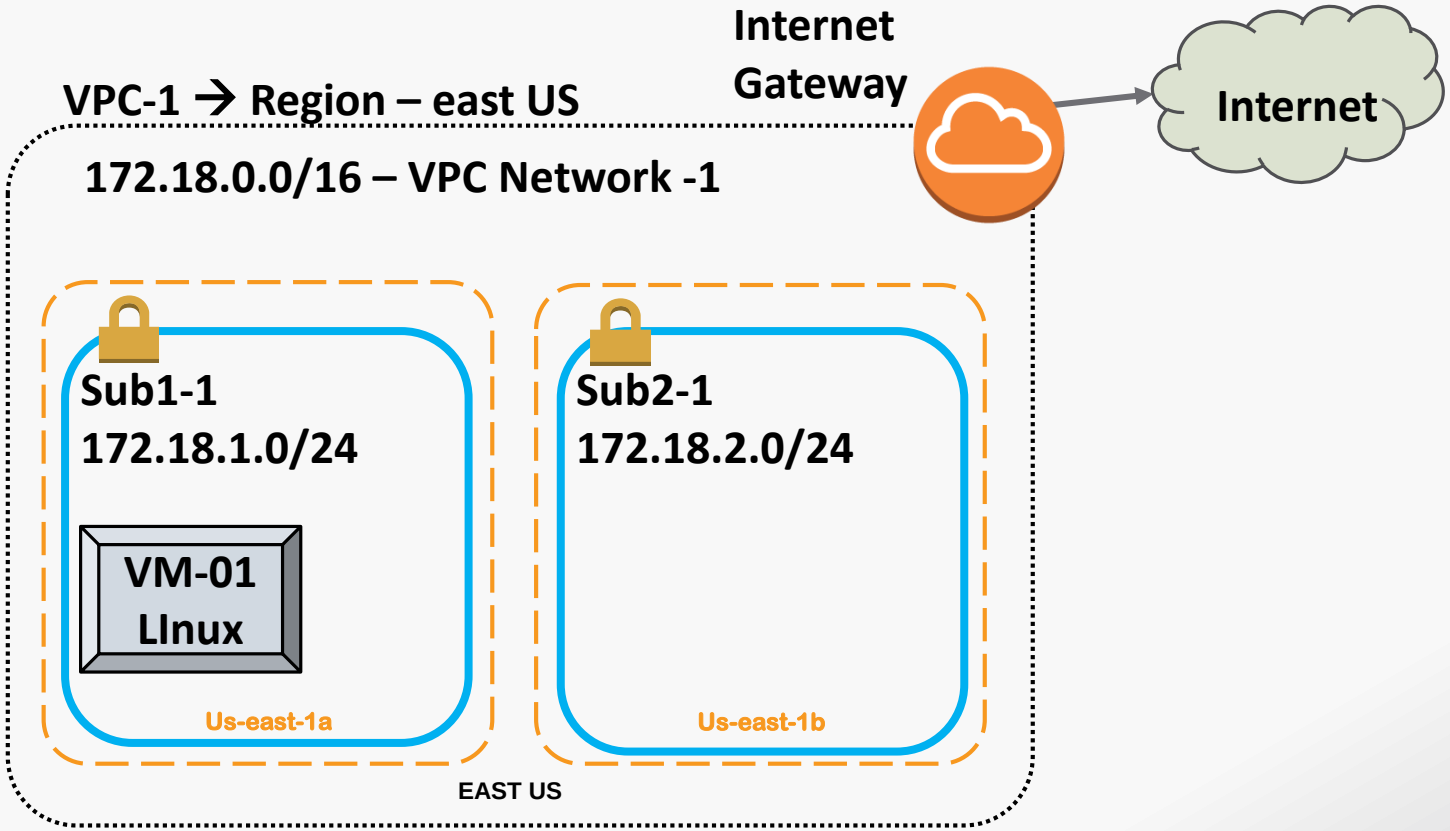
- Basic Four Steps to create an basic Network platform for your Virtual Datacenter.
  - Create a VPC
  - Create Subnet
  - Create Internet Gateway
  - **Modify/update Routing Table.**

Step4: Modify the Route Table

- Properties of the Routing Table
  - All the Subnets are by default part of the Default Routing Table for that VPC.
  - By default, all the Private Network and the IPv6 Public Network assigned by AWS is part of the Routing table
  - By Default, there is **NO route for the Internet Traffic.**
  - Custom Route Table does not have any Subnets Associated to it by **DEFAULT.**
- We need to manually add the route for Internet Traffic.
  - For IPv4 **“0.0.0.0/0”** is added for allowing all Traffic towards Internet (Bi-Directional)
  - For IPv6 **“::/0”** is added for allowing all Traffic towards Internet (Bi-Directional)



VPC – Demo – Setup - Details

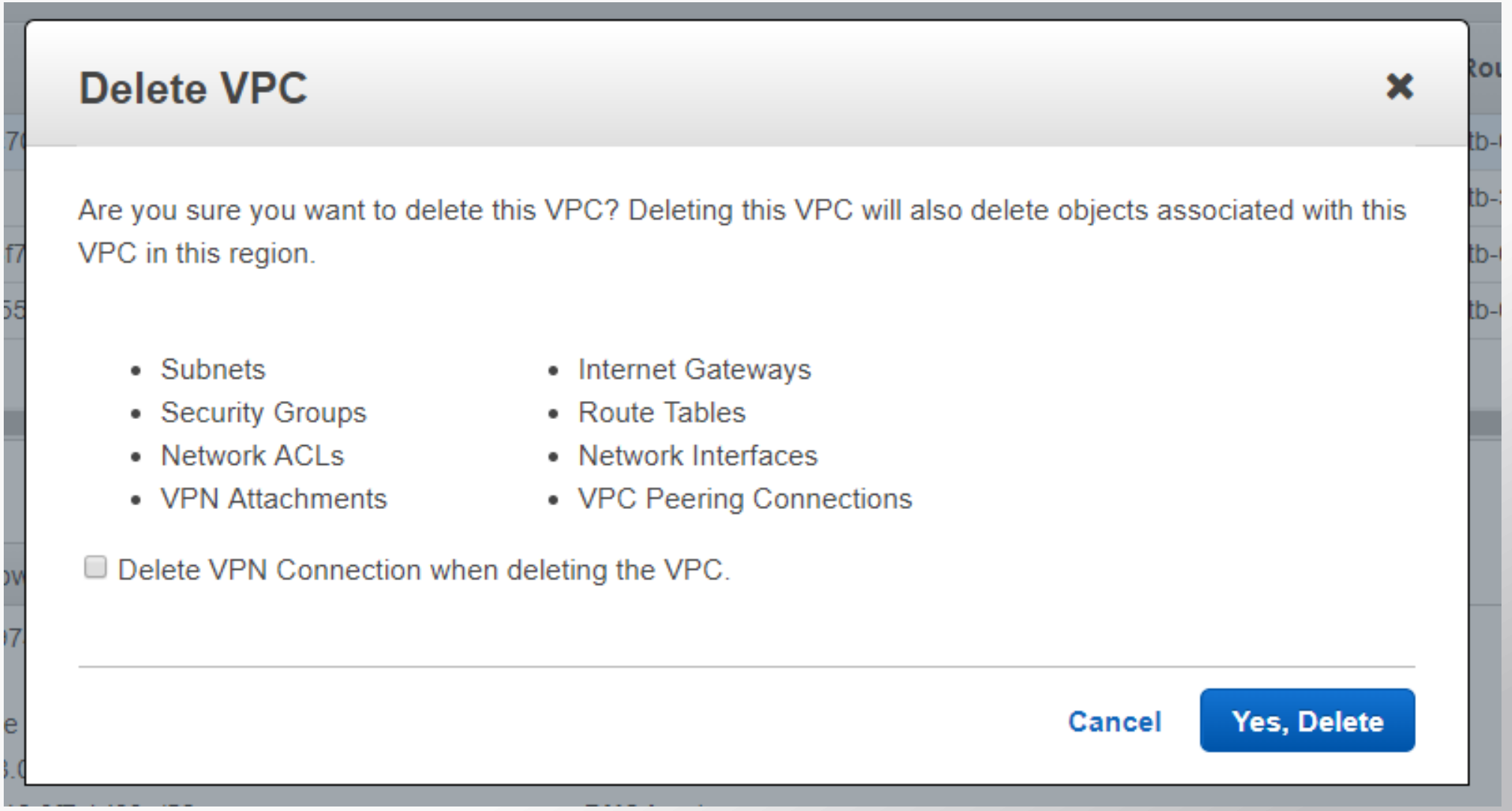


Add routing entry on VPC-1 routing table
0.0.0.0/0 – Internet Gateway
::/0 – Internet Gateway

Hurrey….

NOW CREATE AN BASIC VIRTUAL MACHINE(EC2) AND YOU ARE DONE WITH THE VM ON THE CLOUD WITH INTERNET ACCESS.

Deleting VPC



Creating Multiple Route Tables.

- We could have multiple Route Tables for Different Subnets in an Single VPC.
- A subnet can be part of a single Route TABLE only.

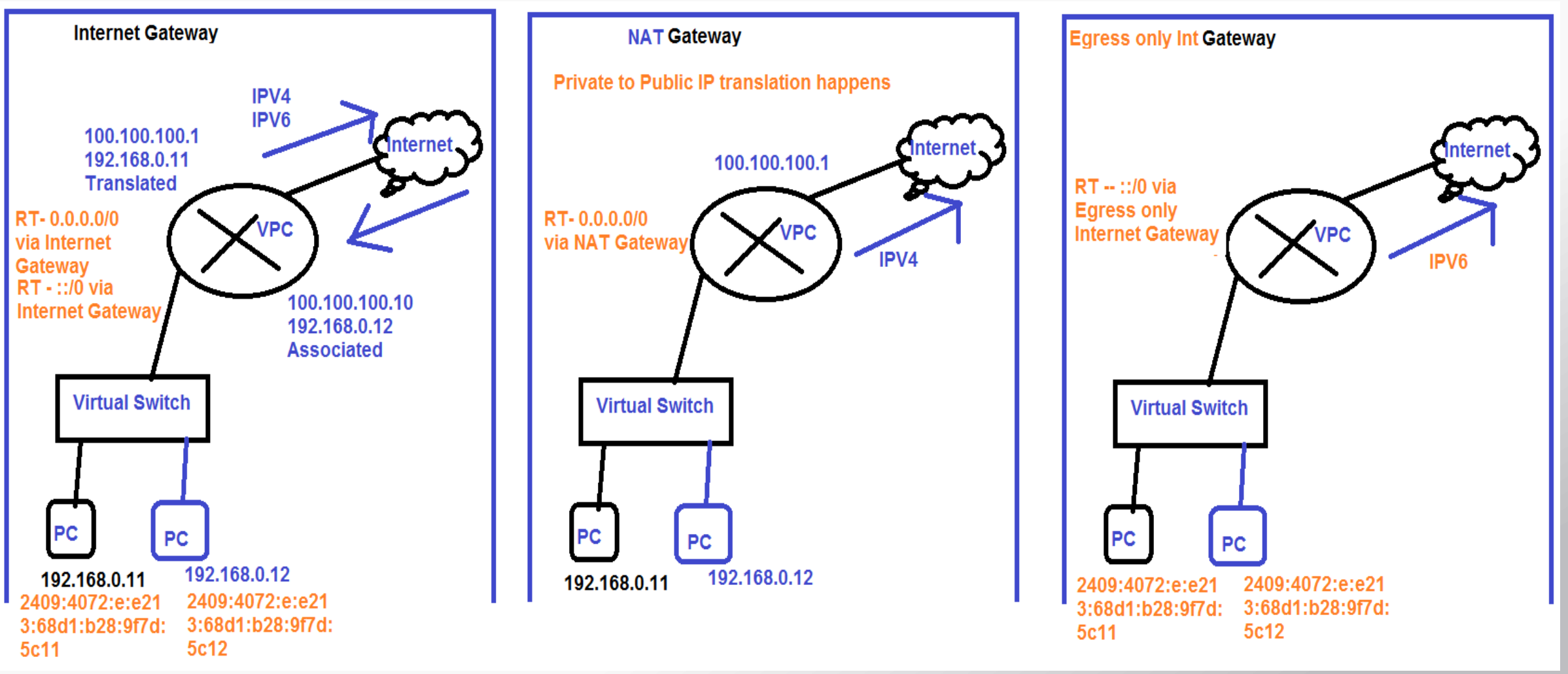
IP Address details of EC2 (VM)

- **Private IPv4** → The assigned IPV4 to the VM is Static IP, and does not change even if the VM is shutdown or restarted and stays until the VM is "**Terminated**"
- **Public IPv4** → This is a dynamic IP **allocated** to the VM. It would change once the Vm shutdown and start back. But the IP would remain if the VM is restarted.
  - The public IPv4 is not assigned to the VM, the VPC maintains the "**NAT**" rule for private to Public mapping,
- **Public IPv6** → This is an static IP, assigned to the VM and stays until the VM is **"terminated"**

- **Static Public IPv4 –** Create an **Elastic IP and assign(Associate) the VM to public ip.**
  - This is CHARGED per Hour.

Different Gateways in VPC

- **Internet Gateway →**
  - It provides an path to the internet for the Virtual Machines in the VPC.
  - The Traffic is 2 ways, both inbound and outbound is allowed for IPv4 and IPv6.
- **Egress only Internet Gateway →**
  - It provides an path to the internet for the Virtual Machines in the VPC on IPv6 only.
  - The Traffic is **One way**, only outbound is allowed for IPv6 from the Virtual Machine.
- **NAT Gateway →**
  - It provides an path to the internet for the Virtual Machines in the VPC on **IPv4 only**.
  - The Traffic is **One way**, **only outbound is allowed** for IPv4 from the Virtual Machine.
  - There is an **Public IP assigned on the Gateway**, and there is NO USE of public ip on the Virtual machine.
  - This is NOT available for IPv6, as “NAT Gateway” is used to conserve IPv4.
  - We cannot PING any of the public ip from the VM.



Steps to Create NAT Gateway

1. **Create an separate routing table for the private Subnet and associate the subnet.**
2. **Create an NAT Gateway assigning it to the Public subnet for the Internet access and assign an Elastic IP to the same**
3. **Update the custom Routing table created in Step1, with default route pointing towards NAT Gateway.**

PRICING

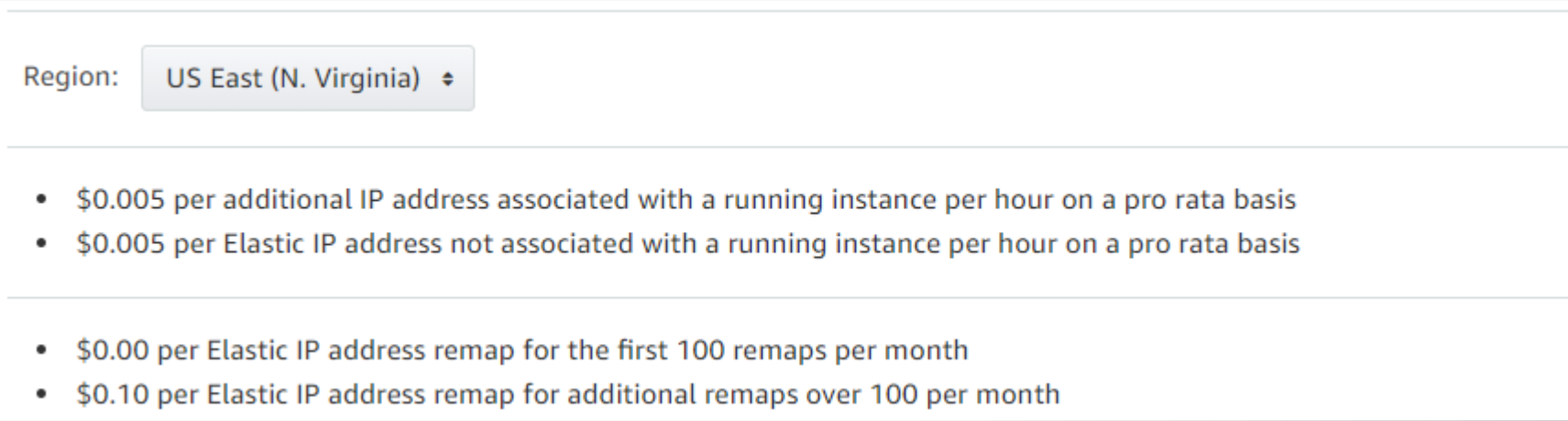
- **VPC – NOT Charged**
- **Subnets – NOT Charged**
- **Internet Gateway – NOT Charged**
- **Routing Table – NOT Charged**
- **NAT Gateway – Charged, as there is an Public IPv4 assigned to it.**
- **Egress only IG – NOT Charged**
- **VPN -- Charged, as there is an Public IPv4 assigned to it.**

Elastic IP pricing

An Elastic IP address doesn’t incur charges as long as the following conditions are true:

- The Elastic IP address is associated with an EC2 instance.
- The instance associated with the Elastic IP address is running.
- The instance has only one Elastic IP address attached to it.

You're charged by the hour for each Elastic IP address that doesn't meet these conditions.

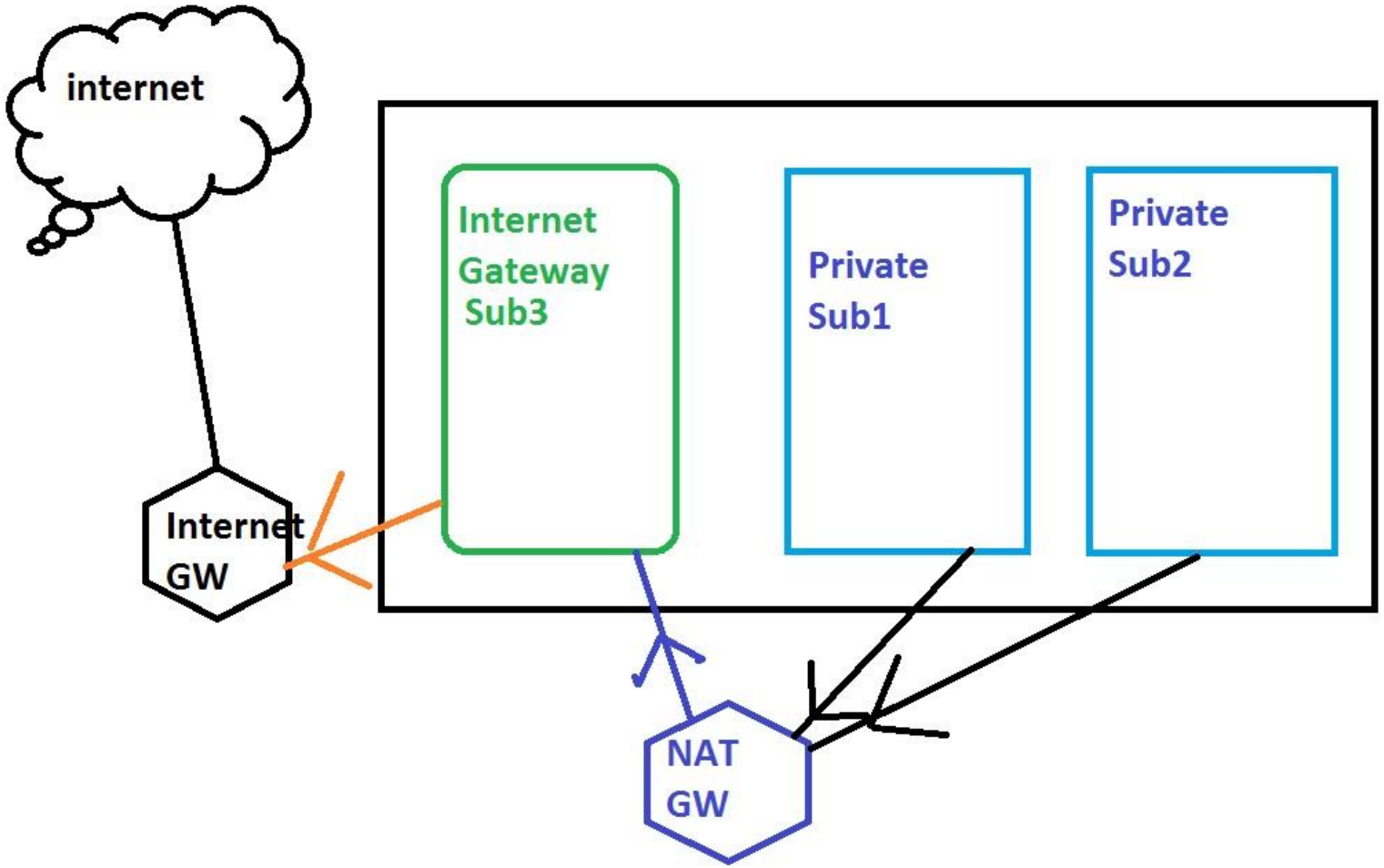


Troubleshooting VPC

Basic Troubleshooting steps if the EC2 instance is not getting connected.

- Check Weather “Internet gateway” is created an assigned to “Routing Table”.
- If custom Route table created, weather “Subnet’s” are associated to the new Routing table.
- Weather “PORTS” are allowed in the security group for “inbound” and “outbound”.

- https://aws.amazon.com/premiumsupport/knowledge-center/troubleshoot-vpc-route-table/


internet
Internet
Gateway
Sub3
Private
Sub1
Private
Sub2
Internet
GW
NAT
GW