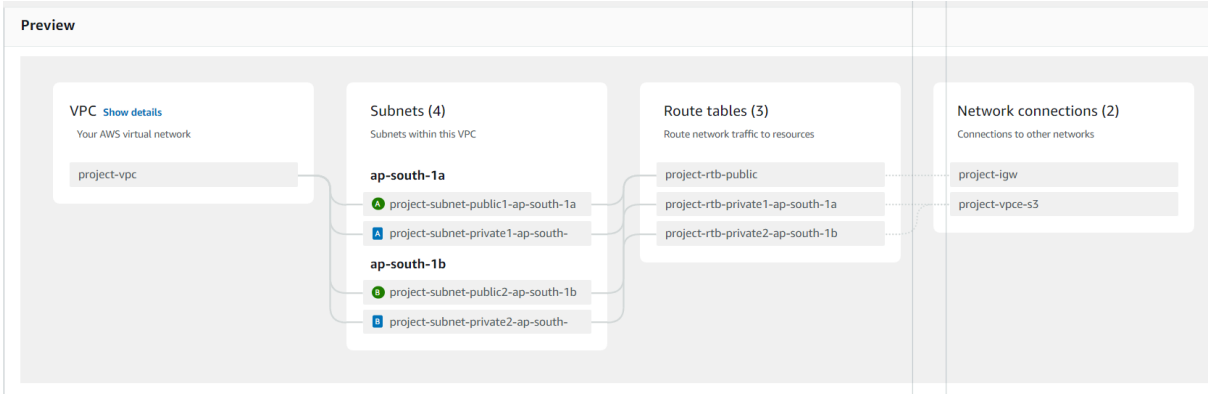
AWS -VPC

Amazon Virtual Private Cloud (VPC) allows users to create isolated, customizable networks within the AWS cloud. A VPC enables control over network configuration, including IP address ranges, subnet creation, routing tables, and network gateways. It's essential for running secure applications and services in the cloud.

Key Features of AWS VPC:

1. **Network Isolation**: A VPC is logically isolated, offering control over internal networking separate from other users' networks.
2. **Subnets**: VPCs can be divided into public and private subnets to control access to instances and services.
    - **Public Subnets**: Directly accessible from the internet; suitable for web servers.
    - **Private Subnets**: Not accessible from the internet; ideal for databases or backend applications.
3. **Security Controls**: Enhanced security through:
    - **Security Groups**: Act as a virtual firewall for instances, controlling inbound/outbound traffic.
    - **Network ACLs**: Stateless filters that control traffic to and from subnets.
4. **Elastic IP Addresses**: Static IPs can be assigned to instances in a VPC for reliable, consistent access.
5. **Internet Gateway (IGW)**: Allows public instances to access the internet.
6. **NAT Gateway**: Allows instances in private subnets to access the internet without being directly accessible.
7. **Peering & VPN Connections**: Connects VPCs across regions and establishes secure connections to on-premises networks.



Private IP:

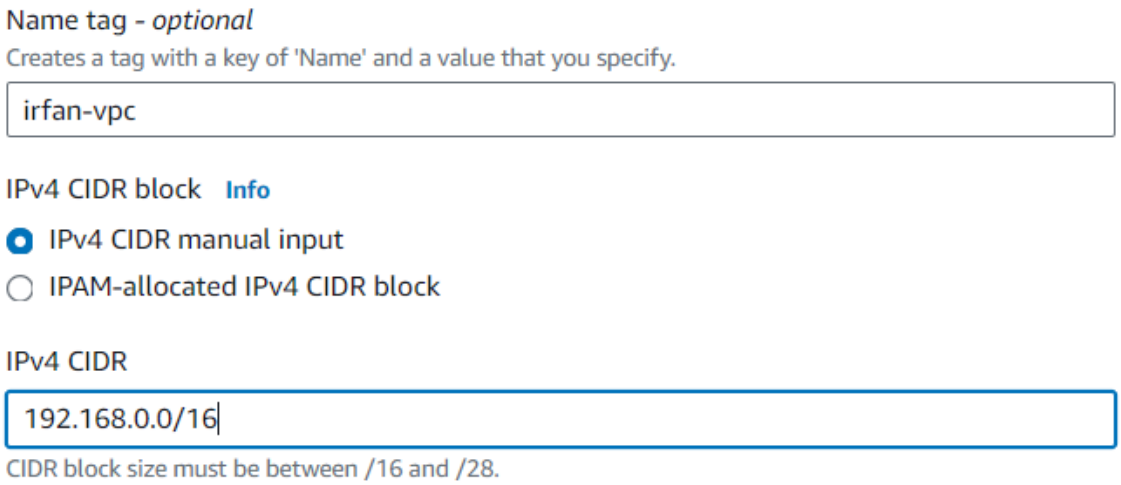
Private IP ranges are defined by the Internet Engineering Task Force (IETF) in RFC 1918 and are reserved for use within private networks. These addresses aren't routable on the public internet and are typically used within LANs (Local Area Networks), VPNs, or cloud VPCs.

Private IP Ranges:

1. **10.0.0.0 – 10.255.255.255** (10.0.0.0/8)
    - Class A private IP range, allowing for a large number of addresses (16 million).
2. **172.16.0.0 – 172.31.255.255** (172.16.0.0/12)
    - Class B private IP range, with around 1 million addresses.
3. **192.168.0.0 – 192.168.255.255** (192.168.0.0/16)
    - Class C private IP range, often used in home and small business networks.

Usage:

Private IP ranges are commonly used to allocate IP addresses to devices within a private network, allowing communication within the network while remaining isolated from the public internet. In cloud environments like AWS, private IPs are often used within VPC subnets for instances that don’t need direct internet access.



IPv4 uses 32-bit addresses (4.3 billion addresses), while IPv6 uses 128-bit addresses (340 undecillion), offering far greater address space and enhanced security. IPv6 also supports auto-configuration, essential for modern, connected devices.

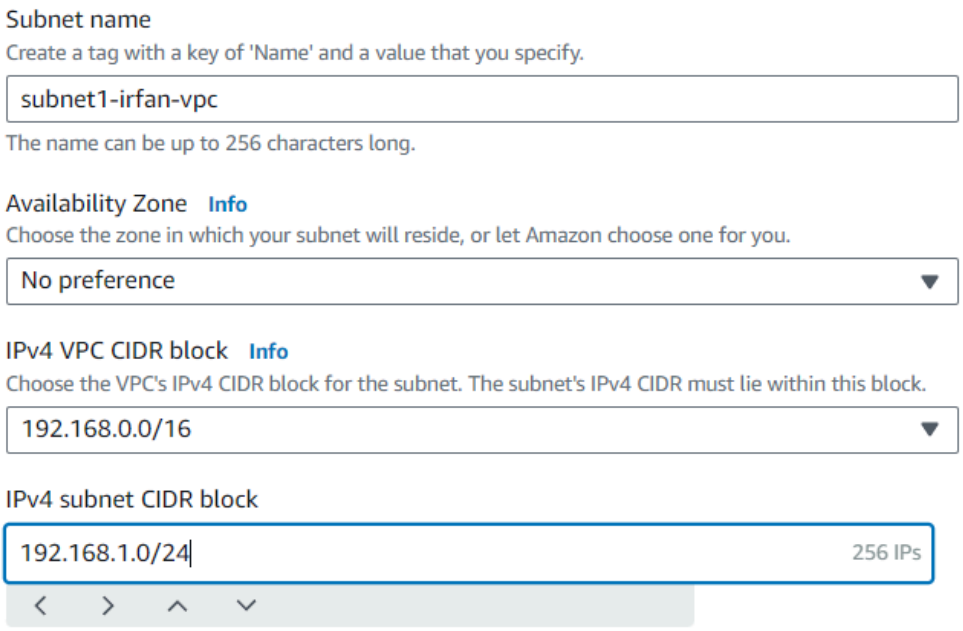
An IPv4 CIDR (Classless Inter-Domain Routing) block defines IP address ranges, using a format like `192.168.1.0/24`. The number after the slash indicates the subnet mask (e.g., `/24` equals 255.255.255.0), determining the range's size. (the number of bits from starting that will be kept static. As +91 in mobile phones of India).

Subnetting divides a large IP network into smaller sub-networks, improving management, security, and reducing broadcast traffic. It's achieved by adjusting the subnet mask (e.g., `255.255.255.0` or `/24`), controlling the number of available hosts per subnet.

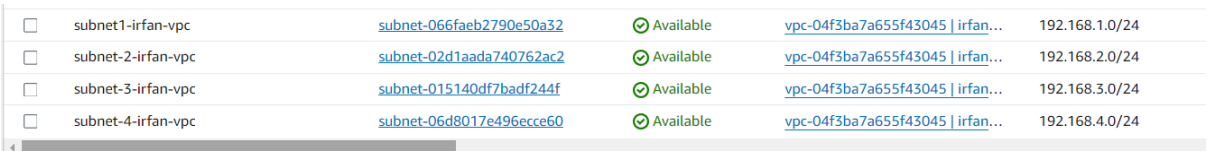
```
192.168.0.0/16
192.168.0.0-192.168.255.255

network 1:
192.168.1.0-192.168.1.255
192.168.1.0/24

network 2:
192.168.2.0-192.168.2.255
192.168.2.0/24
```

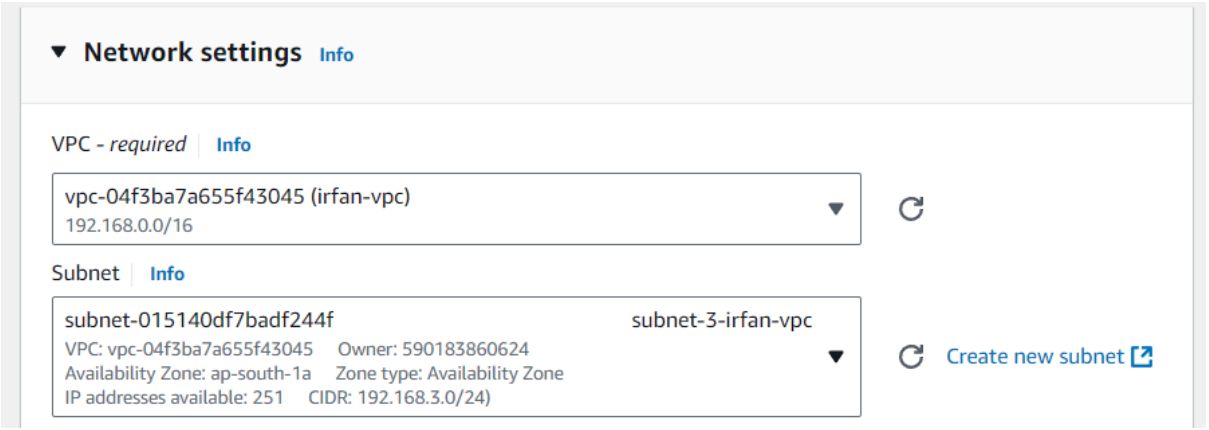


Created 4 subnets.



subnet1-irfan-vpc	subnet-066faeb2790e50a32	Available	vpc-04f3ba7a655f43045 | irfan...	192.168.1.0/24
subnet-2-irfan-vpc	subnet-02d1aada740762ac2	Available	vpc-04f3ba7a655f43045 | irfan...	192.168.2.0/24
subnet-3-irfan-vpc	subnet-015140df7badf244f	Available	vpc-04f3ba7a655f43045 | irfan...	192.168.3.0/24
subnet-4-irfan-vpc	subnet-06d8017e496ecce60	Available	vpc-04f3ba7a655f43045 | irfan...	192.168.4.0/24

Now while creating an EC2 instance.
When we select a VPC built by us. We get 4 subnet to choose from.

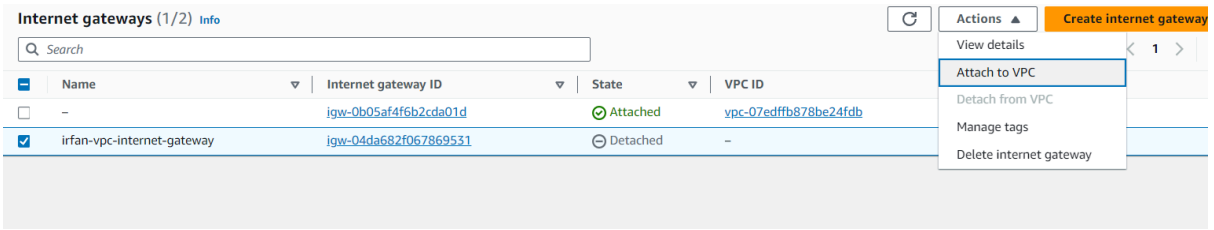


Security Group.
When we create a VPC. we get a security group with it. We are going to select that Security group with it.

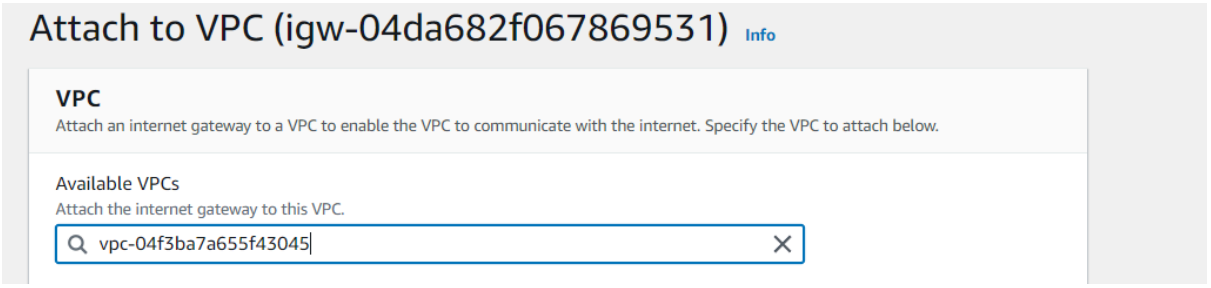
Now when we try to connect with this EC2 instance. We will not be able to connect with it.

Internet Gateway (IGW) and Route Table

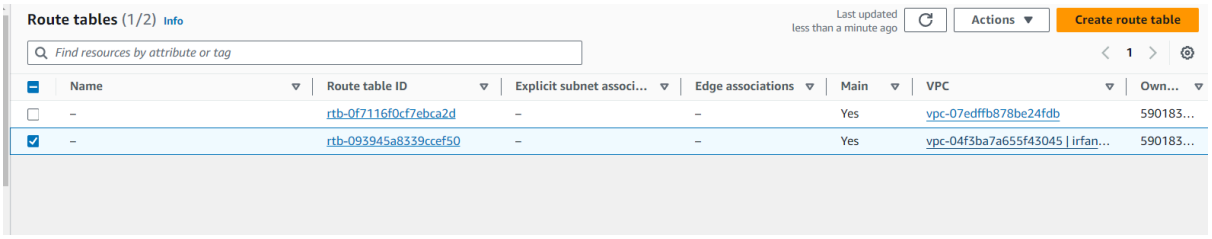
Attaching Internet Gateway to our VPC.

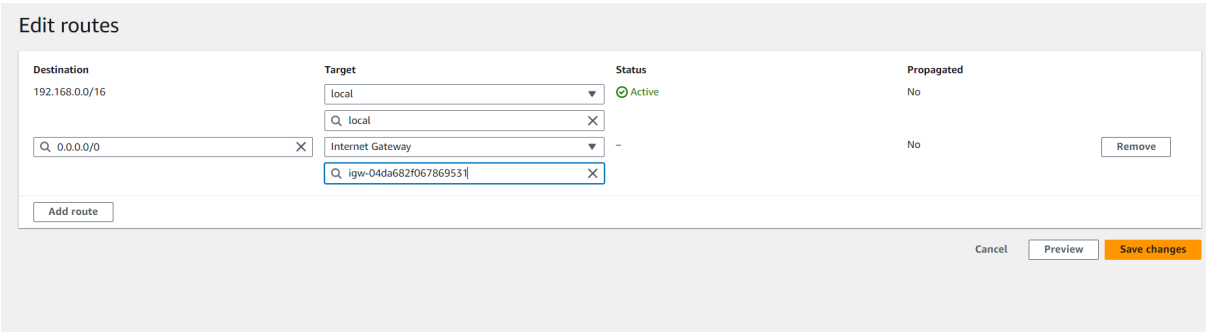
1. Create an IGW.
2. 

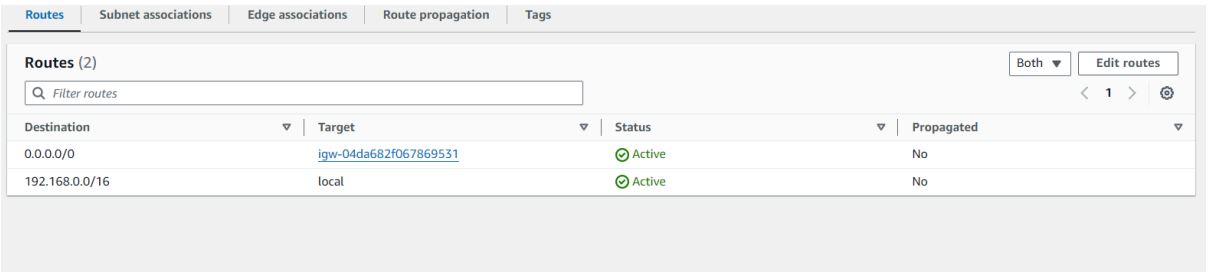
3. Attach to VPC.

4. 

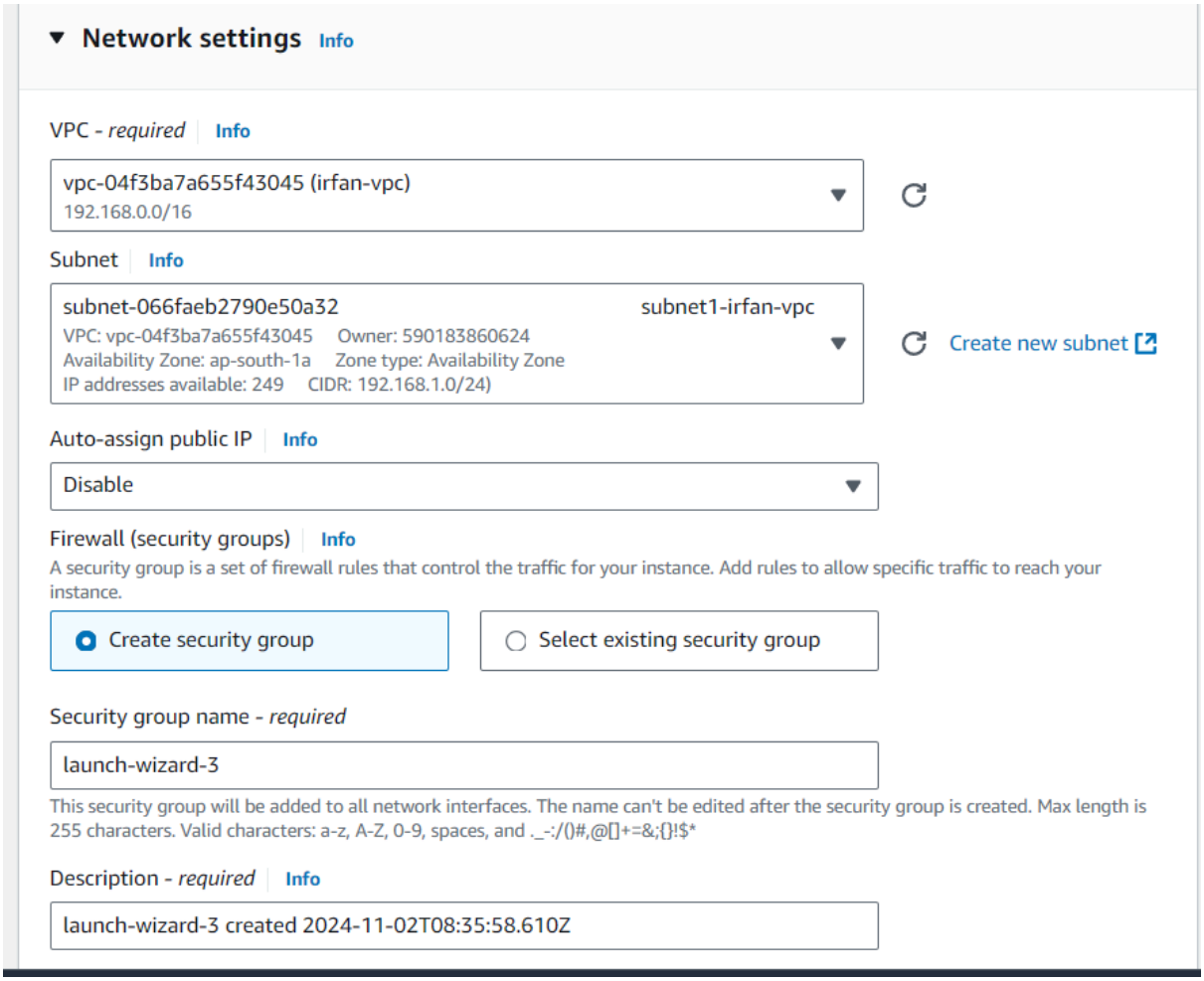
5. A route table directs network traffic within a network, containing rules (routes) that specify paths for traffic to various destinations. In AWS VPCs, route tables control traffic flow between subnets, internet gateways, and other VPC connections.

6. 





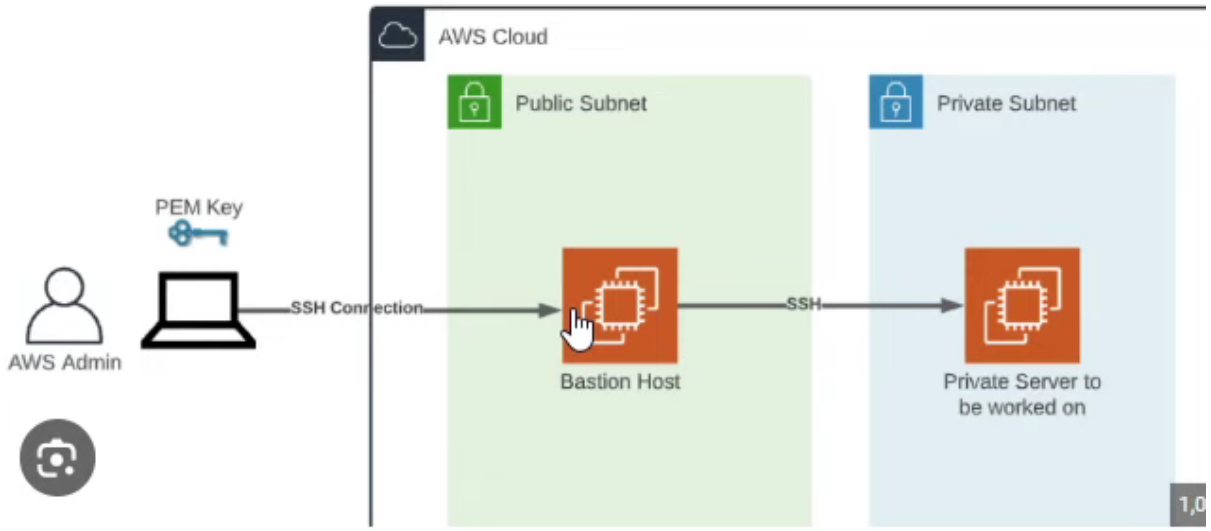
Private IP address of our EC2 instance.




```
root@ip-192-168-1-181:~# apt-get update
Hit:1 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:3 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
```

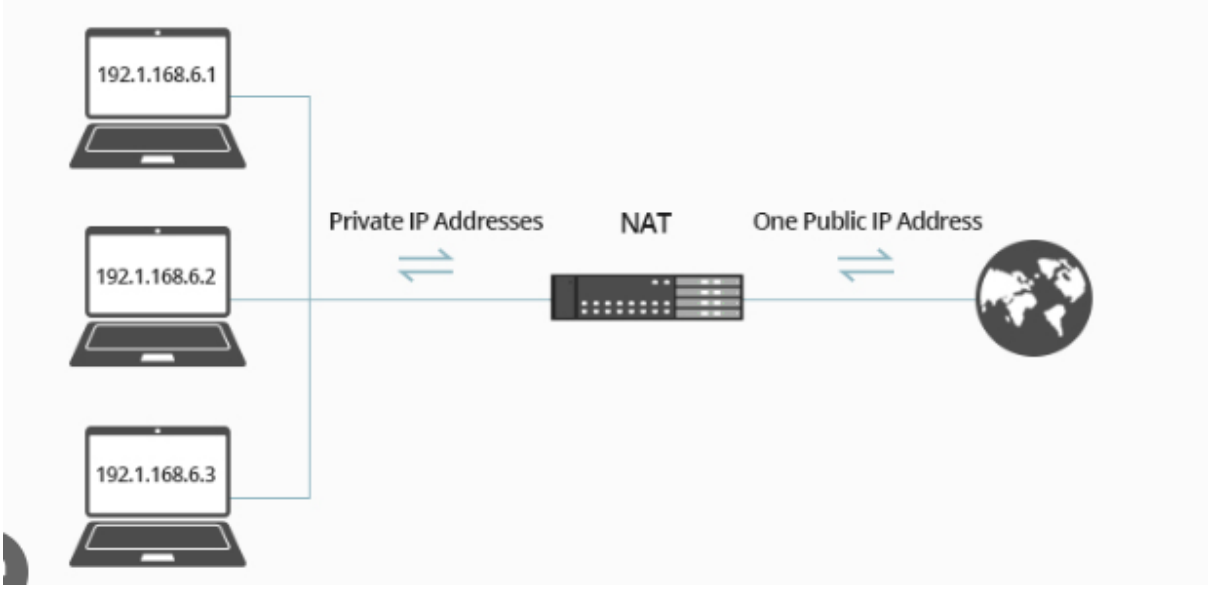
Internet is accessible.

We can create Private and Public Subnet.
We can ping Our private instance with public instance.



NAT:-

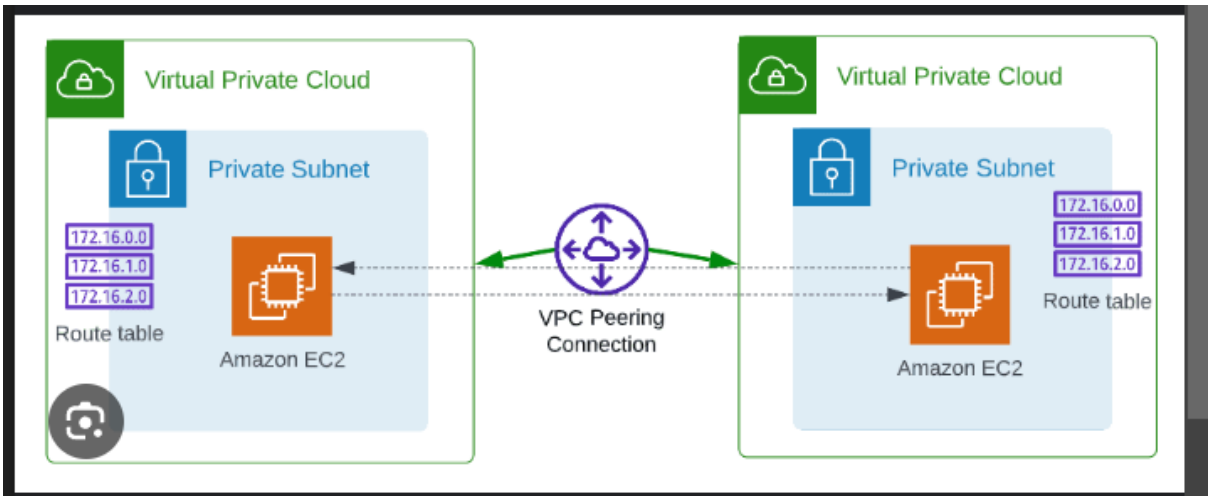
Network Address Translation (NAT) enables private network devices to access the internet by translating private IP addresses to a public IP. In AWS, a NAT Gateway allows instances in private subnets to initiate internet connections without exposing them to inbound traffic.



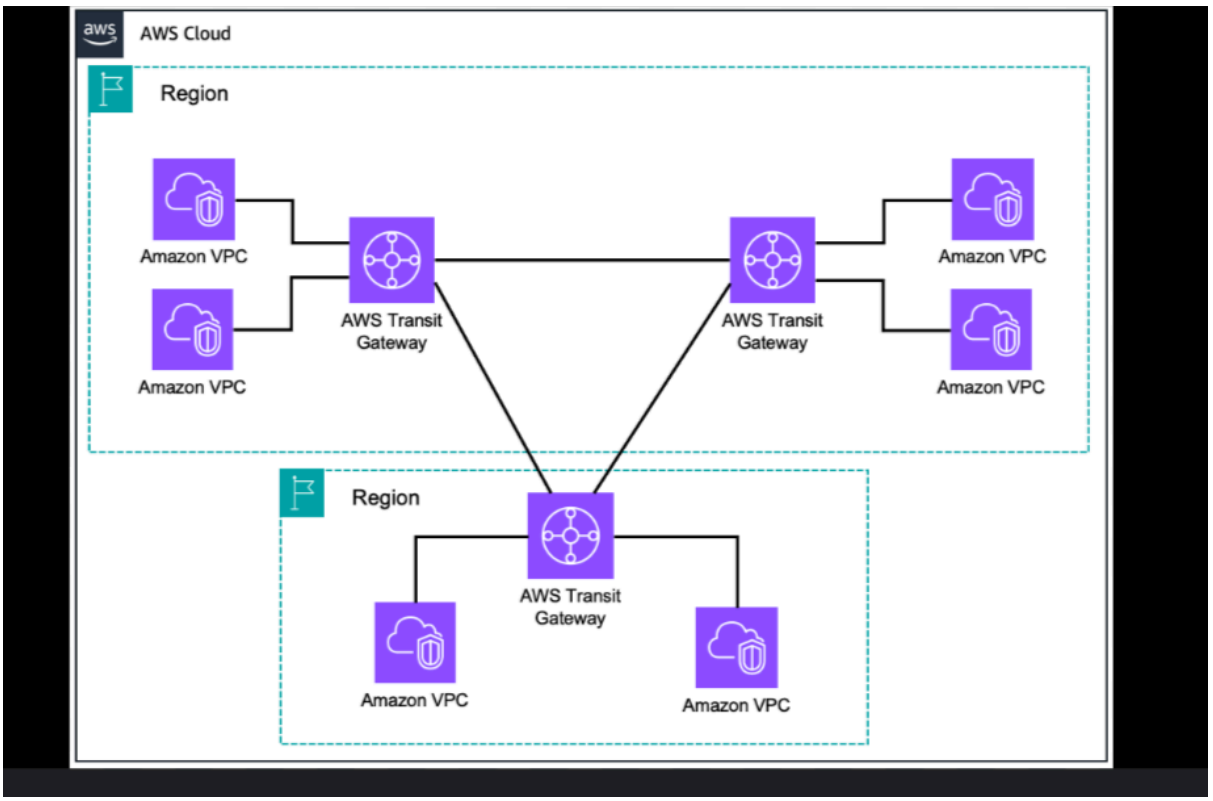
A Network Access Control List (NACL) is a stateless firewall for controlling inbound and outbound traffic at the subnet level in AWS. It provides an extra layer of security, allowing or denying traffic based on IP, protocol, and port rules.

Feature	Security Group	NACL (Network Access Control List)
Statefulness	Stateful (automatic response for allowed requests)	Stateless (requires rules for both inbound and outbound)
Level of Control	Controls traffic at the instance level	Controls traffic at the subnet level
Default Behavior	Implicit deny all traffic unless allowed	Allows all traffic by default (can be configured to deny)

VPC Peering allows two Virtual Private Clouds (VPCs) to connect directly, enabling resources in different VPCs to communicate as if they were within the same network. It is often used for resource sharing, and it supports both inter-region and intra-region connections without needing an internet gateway, VPN, or separate hardware.



AWS Transit Gateway simplifies network management by enabling the connection of multiple VPCs and on-premises networks through a single gateway. It facilitates inter-VPC communication, reduces complexity, and scales easily to handle large networks, providing centralized routing and improved security.



Example:

In a large e-commerce company, different departments (e.g., marketing, inventory, and finance) have their own VPCs for specific applications. By using AWS Transit Gateway, the company can connect all these VPCs for seamless communication, enabling the marketing team to access inventory data for promotional campaigns while maintaining security and efficient network management without needing multiple peering connections.

A **VPC Endpoint** allows secure, private connectivity between VPCs and AWS services without using the public internet. This improves security and reduces latency by keeping traffic within the AWS network, commonly used for accessing services like S3 and DynamoDB directly from a VPC.

Example:
A financial company storing sensitive customer data in Amazon S3 can use a VPC Endpoint to access S3 directly from within its VPC, ensuring data transfers don’t traverse the public internet. This setup enhances security and complies with regulatory standards by keeping data confined to AWS's private network.