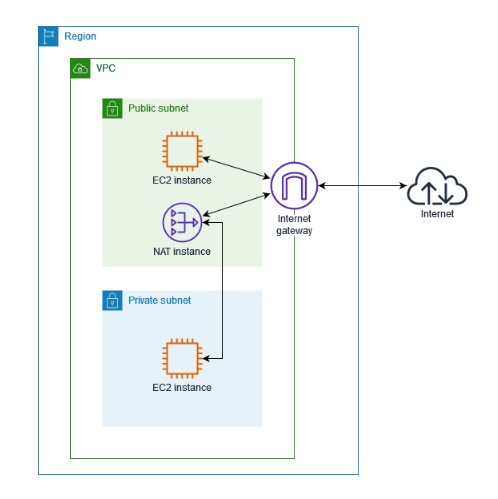
**Project :- VPC project - Securing Connectivity: Enabling Internet Access for Servers in Private Subnets via NAT Instance or NAT Gateway**

**Summary:- This project aims to enhance the security and connectivity of servers placed in private subnets by enabling internet access through a combination of NAT instance or NAT Gateway. By implementing this solution, we ensure that servers in private subnets can securely access resources on the internet while maintaining a protected network environment.**

**Diagram:-**



Execution Steps:-

1. \*Create a VPC\*: Navigate to the Amazon VPC service in the AWS Management Console. Create a new Virtual Private Cloud (VPC) with a CIDR block of your choice.

2. \*Set Up Subnets\*: Create at least two subnets within your VPC: one public subnet and one or more private subnets. Ensure that the public subnet has a route to the internet gateway (IGW), while the private subnet(s) do not have direct internet access.

3. \*Launch NAT Instance or NAT Gateway\*:

- \*NAT Instance\*:

- Launch a new EC2 instance in the public subnet.

- Choose an Amazon Machine Image (AMI) that includes NAT functionality (e.g., Amazon Linux).

- Disable source/destination checks on the instance.

- Assign an Elastic IP (EIP) to the instance for static public IP addressing.

- Update the route table of the private subnet(s) to route internet-bound traffic (0.0.0.0/0) through the NAT instance.

- \*NAT Gateway\*:

- Navigate to the NAT Gateways section in the VPC dashboard.

- Create a new NAT Gateway, selecting the public subnet and allocating an Elastic IP (EIP).

- Update the route table of the private subnet(s) to route internet-bound traffic (0.0.0.0/0) through the NAT Gateway.

4. \*Security Group Configuration\*:

- Configure security groups for the NAT instance or NAT Gateway to allow outbound traffic from private subnets and inbound traffic only on necessary ports (e.g., SSH for management).

5. \*Update Network Access Control Lists (NACLs)\*:

- If needed, adjust the network ACLs associated with the private subnet(s) to allow outbound traffic initiated by the instances and necessary inbound traffic (e.g., responses to outbound requests).

6. \*Testing and Verification\*:

- Launch instances in the private subnets and verify that they can access the internet for tasks like downloading updates or accessing external services.

- Ensure that the instances in the private subnets are not directly accessible from the internet.

7. \*Monitoring and Maintenance\*:

- Regularly monitor the NAT instance or NAT Gateway for performance and cost optimization.

- Keep security configurations up-to-date and follow AWS best practices for VPC security.