A **NAT (Network Address Translation) Gateway** enables instances in a private subnet to connect to the internet or other AWS services, while preventing inbound traffic from the internet. It’s primarily used when you want to keep EC2 instances in private subnets, without direct access from the internet, but allow them to access the internet to download patches or updates.

**How NAT Gateway Works:**

1. **Outbound Traffic Only**: NAT Gateway allows instances in private subnets to initiate outbound traffic to the internet or other AWS services while blocking any inbound traffic.
2. **High Availability**: NAT Gateway is automatically scalable and highly available within the availability zone.
3. **Managed Service**: AWS manages the creation, scaling, and availability of the NAT Gateway. You don't need to manually configure routing or handle the underlying network infrastructure.

**Steps to Configure a NAT Gateway and Connect EC2 in Public and Private Subnets:**

**1. Create a VPC**

* Go to **VPC Dashboard** in the AWS Console.
* Click on **Create VPC**.
  + Specify the name, CIDR block (e.g., 10.0.0.0/16), and other settings.

**2. Create Subnets**

* Create a **Public Subnet**:
  + CIDR: e.g., 10.0.1.0/24.
  + Ensure to enable **Auto-assign public IPv4** for the public subnet.
* Create a **Private Subnet**:
  + CIDR: e.g., 10.0.2.0/24.

**3. Create an Internet Gateway (for Public Subnet)**

* Go to **Internet Gateways** in the VPC Dashboard.
* Click **Create Internet Gateway**.
* Attach the Internet Gateway to your VPC.

**4. Update the Route Table for the Public Subnet**

* Go to **Route Tables**.
* Select the Route Table associated with the public subnet.
* Add a route that directs all traffic (0.0.0.0/0) to the Internet Gateway.

**5. Launch an EC2 Instance in the Public Subnet**

* Launch an EC2 instance in the public subnet with a public IP.
* This instance will act as the **bastion host** (to access the private subnet instances) or a web server.

**6. Create a NAT Gateway**

* Go to **NAT Gateways** in the VPC Dashboard.
* Click **Create NAT Gateway**.
  + Choose the public subnet for the NAT Gateway.
  + Allocate a new Elastic IP (EIP) for the NAT Gateway.
* Ensure the NAT Gateway is created in the **Public Subnet**.

**7. Update the Route Table for the Private Subnet**

* Go to **Route Tables**.
* Select the Route Table **associated with the private subnet.**
* Add a route for outbound traffic:
  + Destination: 0.0.0.0/0.
  + Target: Select the **NAT Gateway**.

**8. Launch an EC2 Instance in the Private Subnet**

* Launch an EC2 instance in the private subnet.
* This instance will not have a public IP, but with the NAT Gateway, it can access the internet for outbound traffic (e.g., downloading updates).

**9. Test Connectivity**

* **Public EC2**:
  + You should be able to SSH into the EC2 instance in the public subnet using its public IP.
* **Private EC2**:
  + SSH into the public EC2 instance first (bastion host) and then SSH into the private EC2 instance.
  + From the private EC2 instance, you should be able to ping or access internet resources (e.g., ping google.com).

**10. Security Groups and NACLs**

* Ensure security groups and network ACLs are configured to allow communication between the public and private EC2 instances as well as internet access