NAT Gateway for Private Subnet Internet Access

Why Use a NAT Gateway?

A **private subnet** has **no internet access** — you **can't update or install** anything (e.g., yum, apt).

➞ So we use a **NAT Gateway**, which:

- Allows **outbound** internet traffic from private EC2 instances
- Blocks **inbound** traffic from the internet (more secure)

Step-by-Step: Configure NAT Gateway

Step 1: Create a NAT Gateway

1. Go to **VPC > NAT Gateways**
2. Click **Create NAT Gateway**
   - **Name**: `my-nat`
   - **Subnet**: Select your **public-subnet-1**
   - **Elastic IP**: Allocate new one

Click **Create**

Step 2: Create a Route Table for Private Subnet

1. Go to **VPC > Route Tables → Create**
   - **Name**: `private-rt`
   - **VPC**: `my-vpc`
2. Add route:
   - **Destination**: `0.0.0.0/0`
   - **Target**: Your **NAT Gateway**

Step 3: Associate Route Table with Private Subnet

1. Go to **Subnet Associations**
2. Attach to `private-subnet-1`

Now your private subnet can **access the internet**, but is **not reachable from outside**

Step 4: Launch EC2 in Private Subnet

1. Launch EC2 → Name: `private-server`
2. Network: `my-vpc`
3. Subnet: `private-subnet-1`
4. **Auto-assign public IP: Disabled**
5. Use a Security Group allowing **SSH from only VPC**

Step 5: SSH via Bastion (Public EC2)

You **can’t access** the private EC2 directly. You’ll use **public EC2 as a jump server**:

```
# SSH into public EC2 first
ssh -i my-key.pem ec2-user@<public-ec2-public-ip>

# From there, connect to private EC2 using private IP
ssh -i my-key.pem ec2-user@<private-ec2-private-ip>
```

Step 6: Test Internet Access from Private EC2

```
ping google.com
sudo yum install wget
```

If these work, **your NAT Gateway is working perfectly!**

Diagram of Architecture

```
    INTERNET
       │
 ┌─────────────┐
 │ Internet GW │
 └─────────────┘
       │
Public Subnet (10.0.1.0/24)
 - EC2: Bastion
 - NAT Gateway
       │
┌────────────────┐
│ VPC: 10.0.0.0/16  │
└────────────────┘
       │
Private Subnet (10.0.2.0/24)
 - EC2: Backend DB / App
```

Summary

Component	Purpose
NAT Gateway	Gives internet to private subnet
Private EC2	Secure, can't be reached directly
Bastion EC2	Jump server in public subnet
Route Table	Controls NAT routing
Elastic IP	Public IP attached to NAT