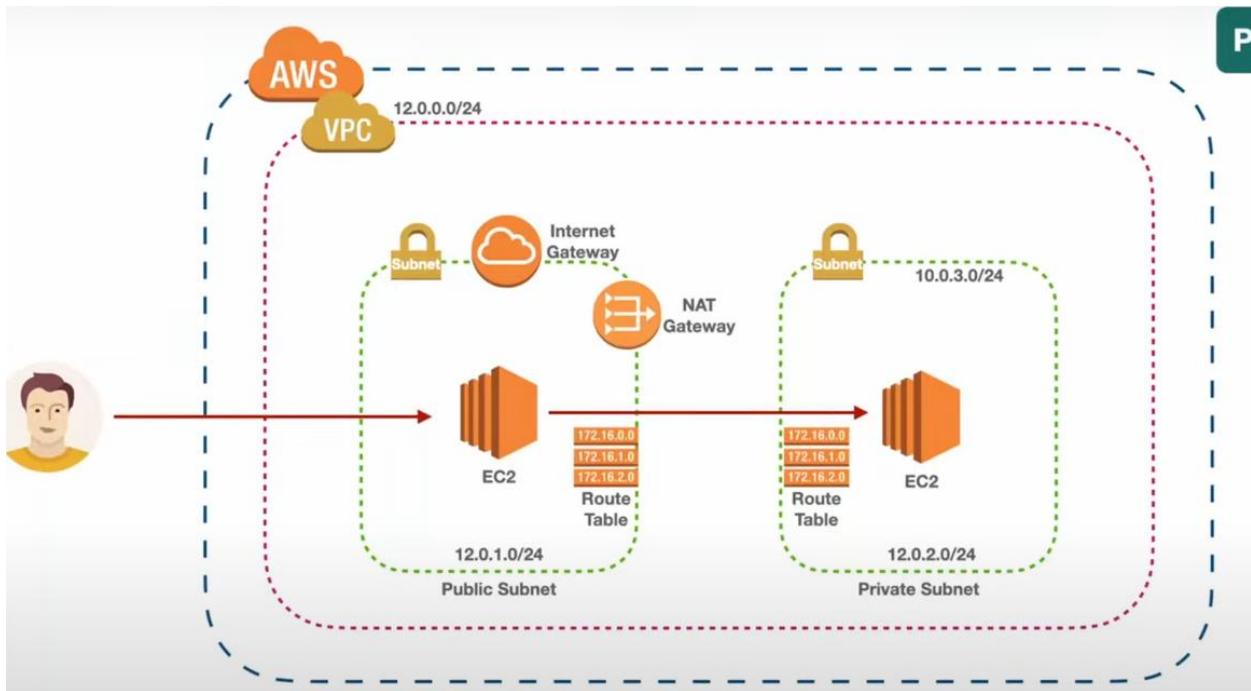


Demo-4



What is a NAT Gateway in AWS?

A **NAT (Network Address Translation) Gateway** in AWS allows instances in a **private subnet** to access the **internet** (for updates, patches, etc.) **without exposing them to incoming internet traffic**. It acts as a **middleman** between private resources and the internet.

- 📌 **Key Features of NAT Gateway:**
- ✓ **Enables outbound internet access for private instances.**
- ✓ **Prevents inbound internet traffic for security.**
- ✓ **Automatically scales up to 45 Gbps of bandwidth.**
- ✓ **Requires an Elastic IP (EIP) to function.**
- ✓ **High availability within a single Availability Zone.**

How NAT Gateway Works?

- 1 **Private EC2 instances** in a subnet need internet access (e.g., software updates).
- 2 The instances send requests **to the NAT Gateway**.
- 3 The NAT Gateway **modifies the source IP** to its **Elastic IP (EIP)**.
- 4 The request reaches the **internet**, and the response is sent back to the NAT Gateway.
- 5 The NAT Gateway forwards the response **back to the EC2 instance**.

Important:

- **A NAT Gateway is placed in a public subnet** and requires an **Elastic IP**.
 - The private subnet must have a **route pointing to the NAT Gateway**.
-

How to Create a NAT Gateway in AWS?

1 Using AWS Console

- 1 Navigate to **VPC Dashboard** → Click **NAT Gateways**
- 2 Click **Create NAT Gateway**
- 3 Select a **Public Subnet**
- 4 Allocate or attach an **Elastic IP (EIP)**
- 5 Click **Create NAT Gateway**
- 6 Update the **Route Table** of the Private Subnet to point to the NAT Gateway

2 Using AWS CLI

NAT Gateway vs Internet Gateway vs NAT Instance

Feature	NAT Gateway	Internet Gateway (IGW)	NAT Instance
Purpose	Enables private instances to access the internet	Provides internet access to public subnets	Custom alternative to NAT Gateway
Inbound Traffic Allowed?	 No	 Yes	 Yes (if configured)
Managed by AWS?	 Yes	 Yes	 No (manual setup needed)
High Availability?	 Yes	 Yes	 No (requires failover setup)
Scalability	 Auto-scales up to 45 Gbps	 No limit	 Manual scaling needed

Why Use NAT Gateway?

- ✓ **Ensures security** – Keeps private resources safe from direct internet exposure.
- ✓ **Easy to manage** – Fully managed by AWS, no manual maintenance needed.
- ✓ **Scalable** – Handles large traffic loads up to **45 Gbps**.
- ✓ **High availability** – Resilient within an **Availability Zone**.

Real-World Use Cases

- Updating Private EC2 Instances** – Enable package updates & security patches without exposing instances to the internet.
- Connecting to External APIs** – Private apps can call third-party APIs securely.
- Database & Application Server Security** – Ensure that backend resources remain private while accessing cloud services.
- Hybrid Cloud Networking** – Connect on-premises resources to AWS securely.

What is an Elastic IP (EIP) in AWS?

An **Elastic IP (EIP)** in AWS is a **static, public IPv4 address** that can be associated with an **EC2 instance, NAT Gateway, or other AWS resources**. It ensures that your **public IP remains constant** even if an instance is restarted or replaced.

Key Features of Elastic IP:

- Static Public IP** – Remains unchanged even if an instance stops or restarts.
- Reassignable** – Can be transferred between instances within the same AWS account.
- Fault Tolerance** – Helps maintain access to critical services by reassigning IPs.
- Used for NAT Gateways, Load Balancers, and VPNs**.
- Limited per account** – AWS provides a few free EIPs, additional ones incur costs.

Why Use an Elastic IP?

Common Use Cases:

- Maintain a fixed IP address** for external users accessing your EC2 instance.
- Reassign the IP address** quickly in case of instance failure.
- Required for NAT Gateways** to provide internet access for private subnets.
- Used with Bastion Hosts** to enable SSH access with a consistent IP.
- Helps in Disaster Recovery** by quickly switching the IP to a standby instance.