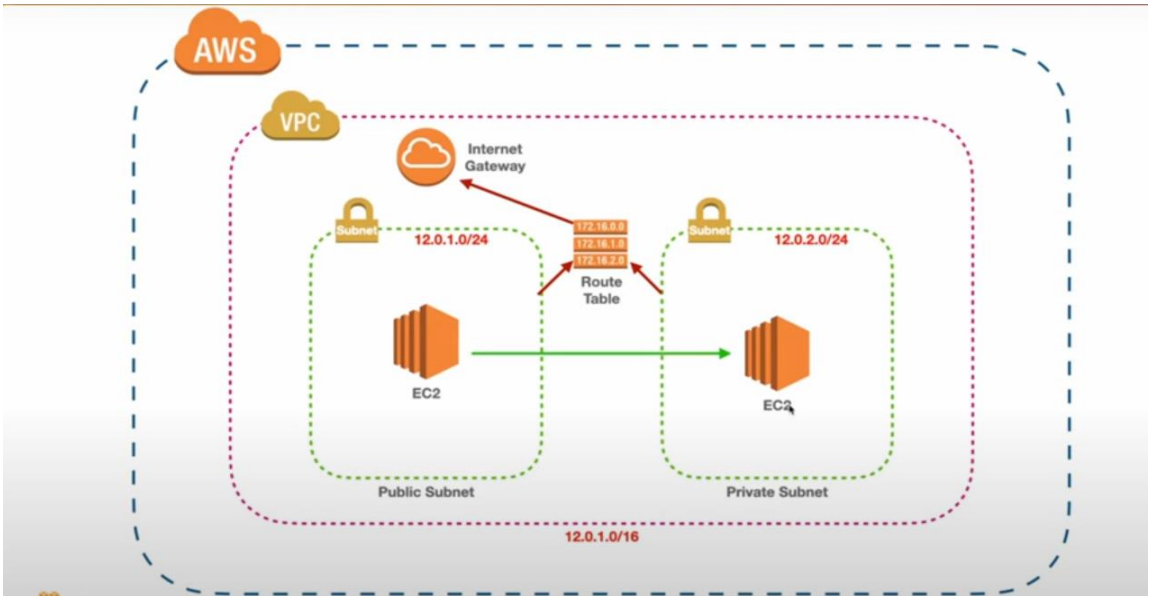
What is VPC (Virtual Private Cloud) in AWS? 🌐☁️



A **VPC (Virtual Private Cloud)** in AWS is a logically isolated **private network** where you can launch AWS resources, such as EC2 instances, databases, and containers. It allows you to define your **own IP range, subnets, routing, and security settings** to control traffic and access.

📌 **Key Features:**
✔ **Fully isolated** private cloud environment
✔ **Customizable IP address range** (CIDR block)
✔ **Supports multiple subnets** (public & private)
✔ **Control inbound & outbound traffic** using Security Groups & NACLs
✔ **Enable internet or VPN access** with Internet Gateway, NAT Gateway, or VPN

Components of a VPC

Component	Description
CIDR Block	Defines the IP address range for the VPC (e.g., `10.0.0.0/16`).
Subnets	Divide the VPC into smaller networks (Public & Private).
Route Table	Controls how network traffic is directed.
Internet Gateway (IGW)	Enables communication between VPC and the internet.

Component	Description
NAT Gateway	Allows private instances to access the internet without being publicly accessible.
Security Groups (SGs)	Act as virtual firewalls for instances, controlling inbound/outbound traffic.
Network ACLs (NACLs)	Additional security layer for controlling traffic at the subnet level.
Peering Connection	Allows communication between two VPCs.
VPC Endpoint	Securely connects to AWS services without using the public internet.

Types of Subnets in VPC 🌍

1️⃣ Public Subnet

- Connected to the Internet Gateway (IGW).
- Used for web servers, bastion hosts.
- Example: Web applications, public-facing APIs.

2️⃣ Private Subnet

- No direct internet access.
- Used for databases, application servers.
- Example: Backend servers, RDS, Redis.

3️⃣ VPN-Only Subnet

- Used for internal corporate networks with a VPN connection.

Why Use VPC? 🎯

✔ **Secure & Isolated Environment** 🔐
✔ **Custom Network Control** 🛠️
✔ **Scalability & High Availability** 📈
✔ **Multi-tier Architecture Support** 🏗️
✔ **Integration with On-Premises Networks** 🌍

What is a Subnet in AWS? 🌐🔗

A **Subnet (Subnetwork)** in AWS is a division of a **VPC (Virtual Private Cloud)** that allows you to segment your network into smaller, manageable sections. Each subnet resides in a **single Availability Zone (AZ)** and helps **control access, security, and routing** of AWS resources.

📌 **Key Features of a Subnet:**
✔ **Divides a VPC into smaller networks** for better organization.
✔ **Each subnet is tied to one Availability Zone (AZ)**.
✔ **Can be Public or Private** based on routing configurations.
✔ **Supports multiple instances, databases, and AWS services**.
✔ **Security is controlled using Security Groups & Network ACLs**.

Types of Subnets in AWS 🏗️

1️⃣ Public Subnet 🌍

- Connected to the **Internet Gateway (IGW)**, allowing **direct internet access**.
- Used for hosting **web servers, bastion hosts, and public APIs**.
- **Example:** A web server in a public subnet can serve requests directly from the internet.

2️⃣ Private Subnet 🔒

- No direct internet access (requires a **NAT Gateway** for outbound traffic).
- Used for **databases, application servers, and backend services**.
- **Example:** A database server in a private subnet is protected from external traffic.

Why Use Subnets? 🎯

✔ **Network Segmentation** – Organize resources efficiently
✔ **Enhanced Security** – Isolate critical resources from the internet
✔ **Load Distribution** – Spread traffic across multiple AZs
✔ **Better Performance** – Optimized network communication

What is an Internet Gateway (IGW) in AWS? 🌐🚀

An **Internet Gateway (IGW)** is a **highly available and scalable AWS component** that allows **EC2 instances in a public subnet** to communicate with the **internet**. It acts as a **bridge** between a **VPC and the internet**, enabling both **inbound and outbound** traffic.

📌 **Key Features of IGW:**
✔ **Allows internet access** for public instances.
✔ **Stateless, redundant, and highly available**.
✔ **One IGW per VPC** (can't attach multiple IGWs to a single VPC).

✔ **No additional cost** (only standard data transfer fees apply).
✔ **Works with Route Tables and Security Groups** to manage traffic.

How Internet Gateway Works? 🚪

1. **Created and attached to a VPC**.
2. **Public Subnets** route traffic to the IGW.
3. **Elastic IP (EIP) or Public IP** is assigned to instances for internet access.
4. **Security Groups & NACLs** control traffic to and from instances.

Steps to Set Up an Internet Gateway in AWS 🛠️

1️⃣ Using AWS Console

1. Go to **VPC Dashboard** → Click **Internet Gateways**
2. Click **Create Internet Gateway** → Give it a name
3. Attach the IGW to a **VPC**
4. Update **Route Table** to allow internet traffic
5. Launch an **EC2 instance in a Public Subnet**
6. Assign a **Public IP or Elastic IP** to the instance
7. Modify **Security Groups** to allow inbound/outbound traffic

Why Use an Internet Gateway? 🎯

✔ **Essential for public-facing applications** like web servers, APIs
✔ **Allows communication between AWS and the internet**
✔ **Cost-effective and scalable** solution for internet access
✔ **Secure when combined with Security Groups & NACLs**

What is a Route Table in AWS? 🛣️🖥️

A **Route Table** in AWS is a set of **rules (routes)** that determine how network traffic is directed within a **VPC (Virtual Private Cloud)**. It controls how packets move between **subnets, internet gateways, NAT gateways, VPC peering, and VPNs**.

📌 **Key Features of a Route Table:**
✔ **Manages network traffic** within a VPC.
✔ **Each subnet in AWS must be associated with a route table**.
✔ **Multiple subnets can share the same route table**.
✔ **Can route traffic to Internet Gateway (IGW), NAT Gateway, VPNs, or Peering Connections**.
✔ **Default Route Table (Main Route Table) exists in every VPC**.

Types of Route Tables in AWS 📜

1️⃣ Main Route Table 🏠

- Automatically created when a **VPC is created**.
- Controls routing for **subnets that are not explicitly associated** with any custom route table.

2️⃣ Custom Route Table 🛠️

- Created manually for **custom routing needs** (e.g., private & public subnet separation).
- Can be assigned to specific subnets for **custom traffic control**.

Why Use Route Tables? 🎯

✔ **Control network traffic within a VPC**
✔ **Enable secure communication between subnets & external networks**
✔ **Facilitates hybrid cloud networking** (VPNs, Peering)
✔ **Allows public/private subnet isolation**