1 Amazon VPC (Virtual Private Cloud)

- **VPC (Virtual Private Cloud)** is a logically isolated network within AWS.
- It allows you to define your **own IP address range, subnets, route tables, and security settings**.
- A **single AWS account can have multiple VPCs**.
- Each VPC is **limited to a single AWS Region**.
- You can **connect VPCs using VPC Peering or AWS Transit Gateway**.

VPC Components:
✓ **CIDR Block:** Defines the IP address range (e.g., 10.0.0.0/16).
✓ **Subnets:** Divide a VPC into **smaller networks**.
✓ **Route Tables:** Control how network traffic is directed.
✓ **Internet Gateway (IGW):** Allows **public internet access**.
✓ **NAT Gateway:** Allows **outbound-only** internet access from **private subnets**.
✓ **Security Groups & NACLs:** Act as **firewalls** for controlling traffic.

2 Subnets & IP Addressing

- **A subnet is a smaller section of a VPC**.
- **Each subnet is tied to an Availability Zone (AZ)**.
- Subnets can be classified as:
    - **Public Subnet** → Has access to the internet via **Internet Gateway (IGW)**.
    - **Private Subnet** → No direct internet access; can use a **NAT Gateway**.
    - **VPN Subnet** → Used for private connections via **AWS Direct Connect or VPN**.

💡 **Best Practice:** Place public-facing resources (e.g., web servers) in a **public subnet** and backend resources (e.g., databases) in a **private subnet**.

3 Internet Access in a VPC

There are **two ways to connect AWS resources to the internet**:

🔹 **Public Access** (Requires Internet Gateway)

✓ Instance must be in a **public subnet**.

✓ Must have a **public IP address or Elastic IP (EIP)**.

✓ Route table must have an entry for **0.0.0.0/0 → IGW**.

🔹 **Private Access** (Requires NAT Gateway)

✓ Instance is in a **private subnet** (no public IP).

✓ Uses a **NAT Gateway** to reach the internet **outbound only**.

✓ Route table points to **NAT Gateway** for internet-bound traffic.

4 Route Tables

- Route tables define **how network traffic is routed within a VPC**.
- Every **subnet must be associated with a route table**.
- The **Main Route Table** applies to all subnets unless explicitly changed.

Example: **Public Subnet Route Table**

Destination	**Target**
0.0.0.0/0	Internet Gateway (IGW)
10.0.0.0/16	local (within the VPC)

Example: **Private Subnet Route Table**

Destination	**Target**
10.0.0.0/16	local (within the VPC)
0.0.0.0/0	NAT Gateway (for outbound access)

5 Security Groups vs. Network ACLs

AWS provides two types of security controls for VPC traffic:

🔹 **Security Groups (SGs)** (Instance-Level Firewall)

✓ Controls **inbound & outbound traffic** for EC2 instances.

✓ **Default behavior:**

- **Inbound:** All traffic **denied**.
- **Outbound:** All traffic **allowed**.
  ✓ **Stateful**: If an inbound rule allows traffic in, the response is automatically allowed.

🔹 **Network ACLs (NACLs)** (Subnet-Level Firewall)

✓ Controls traffic at the **subnet level**.

✓ **Default behavior:**

- All inbound & outbound traffic **allowed**.
  ✓ **Stateless**: **Inbound and outbound rules must be explicitly defined**.

💡 **Best Practice:**

- Use **Security Groups** to control instance-level access.
- Use **NACLs** to apply **broader security rules at the subnet level**.

6 Connecting AWS to External Networks

AWS provides multiple options to connect AWS resources to external networks:

Networking Option	Purpose
Internet Gateway (IGW)	Allows public access to the internet.
NAT Gateway	Allows private subnets to access the internet **outbound only**.
VPC Peering	Connects two VPCs **privately**.
AWS Transit Gateway	Centralized networking hub for multiple VPCs.
VPN (Virtual Private Network)	Secure connection between AWS and an on-premises network.
Direct Connect	Dedicated, private connection between AWS and a data center.

1. **Which AWS service allows instances in a private subnet to access the internet?**
   A. Internet Gateway (IGW)
   B. NAT Gateway
   C. VPC Peering
   D. AWS Direct Connect
   ✅ **Answer: B. NAT Gateway**

2. **What is required for an EC2 instance in a public subnet to access the internet?**
   A. Security Group
   B. NAT Gateway
   C. Internet Gateway (IGW) and Public IP
   D. AWS Transit Gateway
   ✅ **Answer: C. Internet Gateway (IGW) and Public IP**

3. **What is the primary function of a Route Table in an Amazon VPC?**
   A. Control access to S3 buckets
   B. Define how traffic is routed within a VPC
   C. Encrypt data in transit
   D. Assign IP addresses to instances
   ✅ **Answer: B. Define how traffic is routed within a VPC**

4. **Which AWS component acts as a stateful firewall at the instance level?**
   A. Security Groups
   B. Network ACLs
   C. Route Tables
   D. Internet Gateway
   ✅ **Answer: A. Security Groups**

5. **Which networking service allows private communication between two different VPCs?**
   A. Internet Gateway
   B. NAT Gateway
   C. VPC Peering
   D. AWS Direct Connect
   ✅ **Answer: C. VPC Peering**

6. **A _____ allows resources in a private subnet to access the internet outbound but blocks inbound connections.**
   ✅ **Answer:** NAT Gateway

7. **A VPC must have at least one _____ to host resources.**
   ✅ **Answer:** Subnet

8. **_____ is used to securely connect an on-premises network to AWS.**
   ✅ **Answer:** VPN (Virtual Private Network)

9. **A public subnet must have a _____ to allow internet access.**
   ✅ **Answer:** Internet Gateway (IGW)