SET 1

Scenario : 1
Context:

You are an AWS cloud engineer for a growing e-commerce platform. The platform hosts its web application on EC2 instances and is segmented into multiple tiers for security and availability. The organization requires a robust network design to ensure smooth traffic flow between these tiers and proper segmentation for public-facing and internal resources. As part of the project, you need to configure public, private, and isolated subnets with appropriate routing rules and test network communication. The team also wants the isolated subnet to securely access AWS services without internet exposure.

Requirements:

1. The application should be hosted across public and private subnets to separate internet-facing resources (e.g., web servers) from internal resources (e.g., application servers).
2. Implement a fully isolated subnet that cannot directly access the internet or communicate with other subnets unless explicitly allowed.
3. Ensure that resources in the private subnet can access the internet for updates and patches using a NAT Gateway.
4. Enable secure access to AWS services (e.g., S3) for the isolated subnet without providing direct internet connectivity.

Questions:

1. How would you design a VPC with public, private, and isolated subnets to ensure proper segmentation and security?

2. What routing configurations would you set up to enable internet access for the public and private subnets while keeping the isolated subnet fully secure?

3. How would you set up a NAT Gateway to enable the private subnet to reach the internet, and how would you test this connectivity?

4. How would you enable resources in the isolated subnet to securely access AWS services without internet exposure (e.g., S3 bucket)?

5. What specific test cases would you implement to verify that the public, private, and isolated subnets are correctly configured?

Scenario 2 :
Context:

You are an AWS cloud engineer managing a growing infrastructure for a distributed microservices-based architecture. The services are split across multiple VPCs to isolate various parts of the system for security and manageability. However, some services in different VPCs need to communicate securely with each other. Additionally, you are tasked with implementing strict security measures at both the subnet (NACLs) and instance level (SGs).

Requirements:

1. Establish secure communication between services running in different VPCs using VPC Peering.
2. Implement Network ACLs (NACLs) to control traffic at the subnet level, ensuring only necessary traffic is allowed to pass between the subnets.
3. Configure Security Groups (SGs) to manage instance-level access, allowing only the necessary ports and protocols for inter-service communication.
4. Ensure that the security measures allow traffic between services in peered VPCs while blocking all other unnecessary traffic.

Questions:

1. How would you set up VPC Peering between two VPCs to enable secure communication between instances running in different VPCs?

2. What Network ACL rules would you configure to restrict traffic at the subnet level, while still allowing necessary communication between peered VPCs?

    - Specifically, how would you allow communication only between specific ports and IP ranges, while blocking all other inbound and outbound traffic?

3. How would you configure Security Groups to manage instance-level access, ensuring that only specific services in different VPCs can communicate with each other?

4. What is the best approach to test whether your VPC Peering connection is working properly and that both NACLs and SGs are allowing or blocking the expected traffic?

5. How would you ensure that this setup remains secure and scalable, especially as more VPCs and services are added in the future?