**VPC Peering**

Why is VPC Peering Needed?

In AWS, a Virtual Private Cloud (VPC) acts as a protective layer for all resources within a specific AWS account. For instance, when an AWS account holder launches an EC2 instance, it is automatically attached to the default VPC. By default, resources within one VPC cannot access resources in another VPC.

To enable resource access across VPCs—whether within the same AWS account, between different AWS accounts, or even across regions—VPC Peering is required. VPC Peering establishes a network connection between two VPCs, allowing them to communicate securely while maintaining isolation from other network

Steps and process to create VPC peering

1. Enter the VPC name
2. VPC ID (Requester-Id)
3. Select Another VPC to whome we want to peer
   1. Account
      1. My Account
      2. Another Account
   2. Region
      1. This Region
      2. Another Region
   3. VPC ID (Accepter)

On

Once the requester VPC create VPC the accepter must accept the peering request

Now the VPC peering is established

Next, we need to manually update the route tables for both subnets. In the route table, we specify the source IP as the CIDR block of the other VPC and set the target as the VPC Peering ID.

Additionally, we can configure the security groups for the EC2 instances in both VPCs to allow specific ports for communication.