Creating AWS VPC Networking Environment for the Café

Overview of AWS VPC

Isolated Network

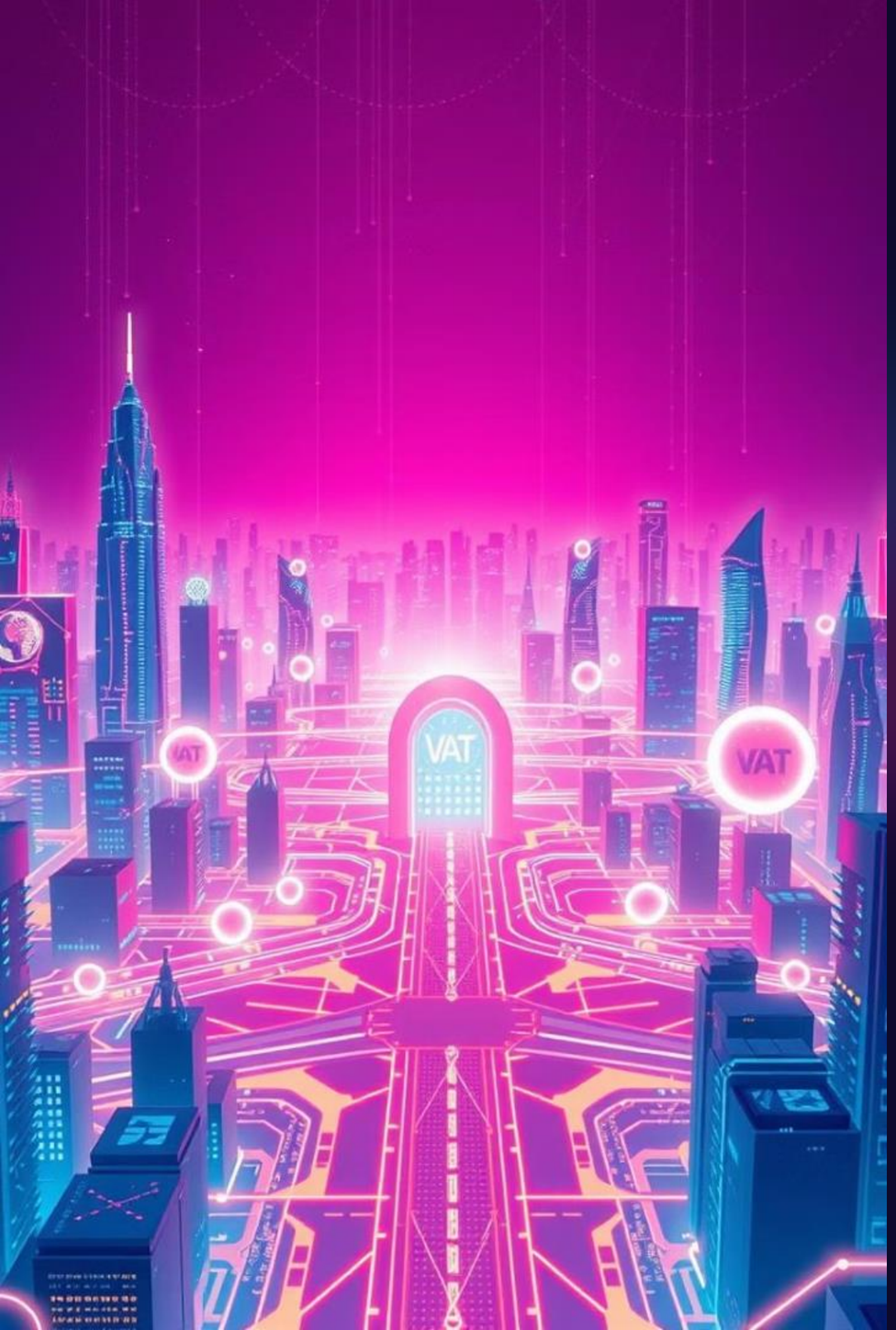
A VPC provides a logically isolated section of the AWS Cloud.

Customizable Network

Configure subnets, routing tables, and security groups to your needs.

Enhanced Security

Isolate your resources, controlling access with security groups.



Designing the VPC network topology

1

Subnet Planning

Determine the number and type of subnets needed.

2

Placement Groups

Strategically place resources for optimal performance.

3

Connectivity

Plan connections to on-premises resources.

Configuring subnets and routing tables

Public Subnets

Connect to the internet via an Internet Gateway.

Private Subnets

For internal resources, access via NAT Gateway.

Routing Tables

Direct traffic between subnets and the internet.

Implementing network security

1 **Security Groups**

Manage inbound and outbound traffic at the instance level.

2 **Network ACLs**

Control traffic at the subnet level.

3 **Firewall Rules**

Define rules based on IP addresses and ports.

Connecting the VPC to on-premises resources

1. **VPN Connection**

   Securely connect using an encrypted tunnel.

2. **Direct Connect**

   Dedicated, high-bandwidth connection.

3. **AWS Site-to-Site VPN**

   Establish a secure connection between networks.

Monitoring and managing the VPC environment

CloudWatch

Monitor network performance and resource utilization.

Security Hub

Identify and mitigate potential security risks.

CloudTrail

Audit VPC activities for compliance and troubleshooting.

Best practices for VPC administration

Regular Security Audits	Implement strong passwords and MFA.
Cost Optimization	Use resource tagging and right-sizing.
Scalability	Design for future growth and flexibility.

Exploring AWS Identity and Access Management (IAM)

Understanding IAM Fundamentals

1 **Users**

Individuals accessing AWS resources. They are assigned policies.

2 **Groups**

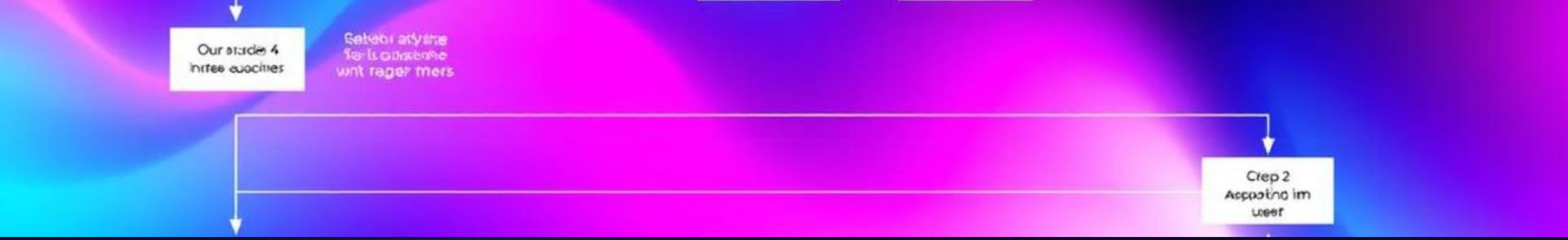
Collections of users. Simplifies permission management.

3 **Roles**

Temporary security credentials for services. No passwords needed.

4 **Policies**

Define permissions granted to users and roles. Control access.



Implementing IAM Policies

1

Create Policy

Define permissions using JSON or the console.

2

Attach Policy

Associate the policy with users or roles.

3

Test Policy

Verify that the policy works as intended.

Managing IAM Users and Groups

User Creation

Create users with unique access keys.

Group Management

Organize users into groups for efficient management.

Access Keys

Manage and rotate access keys regularly.

Securing API Access with IAM Roles

1

Service Request

A service requests temporary credentials.

2

IAM Role

IAM provides temporary security credentials.

3

Access Granted

The service securely accesses the needed resources.

Enabling Federated Access with IAM

Identity Provider

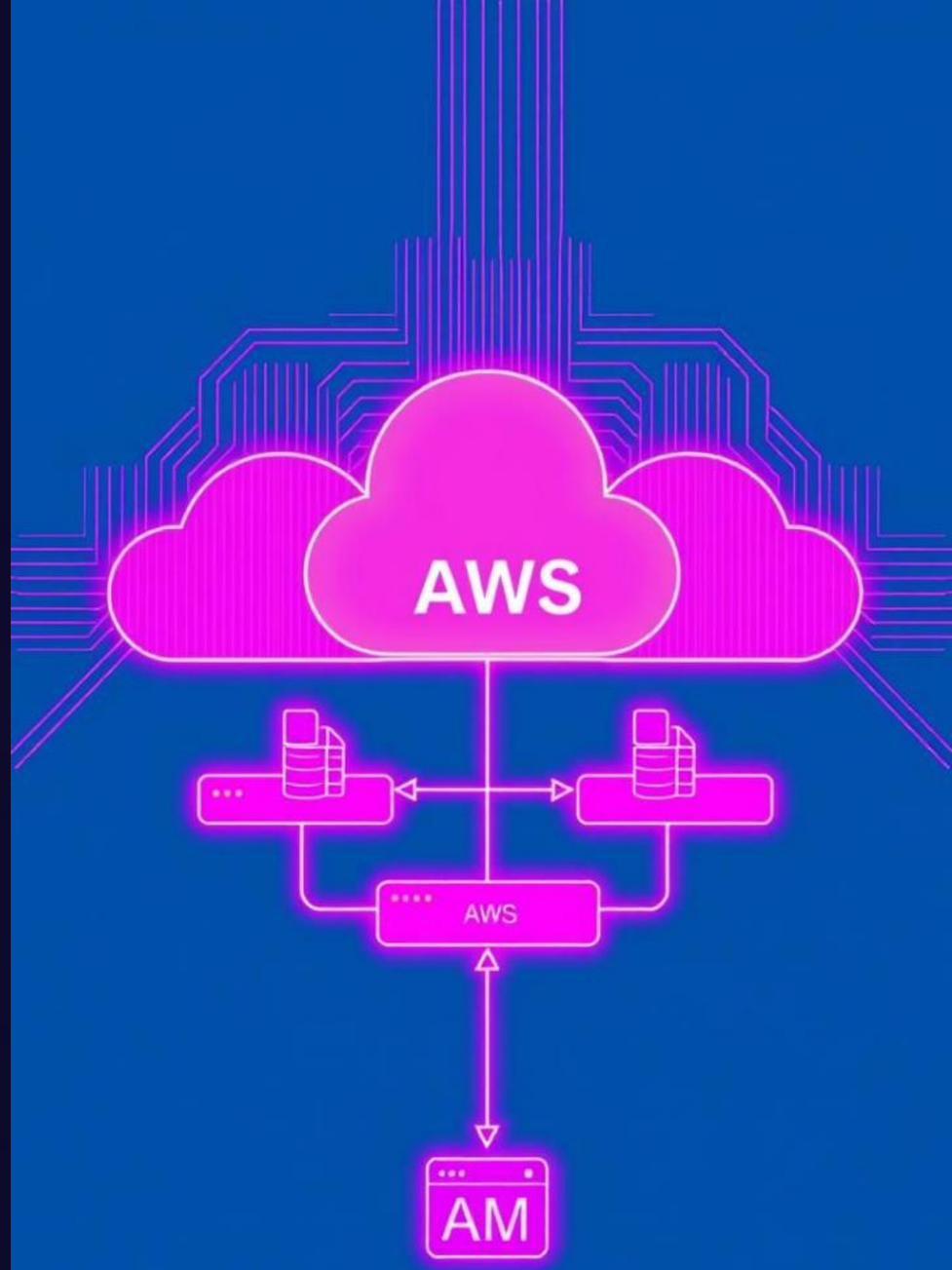
An external system authenticating users.

Federation

IAM trusts the identity provider for authentication.

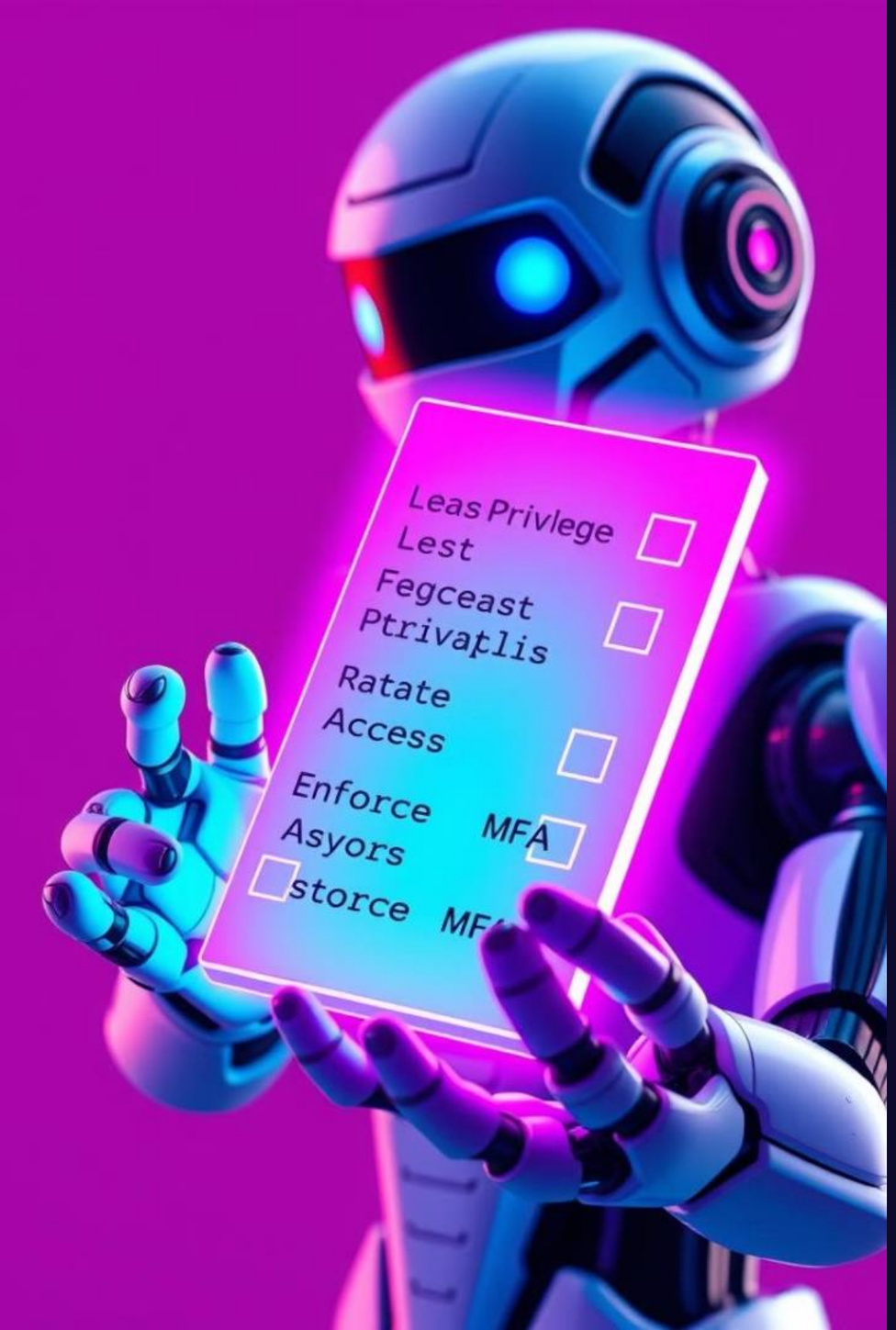
AWS Access

Users gain access to AWS resources via the provider.



Monitoring and Auditing IAM Activities

CloudTrail	Logs all IAM activity.
CloudWatch	Monitors IAM metrics and events.
IAM Access Analyzer	Analyzes resource access patterns.



Best Practices for IAM in AWS

Least Privilege

Grant only necessary permissions.

MFA

Enable multi-factor authentication.

Key Rotation

Rotate access keys frequently.

Regular Audits

Review and update IAM configurations.

Creating AWS VPC Peering Connection

What is VPC Peering?

Definition

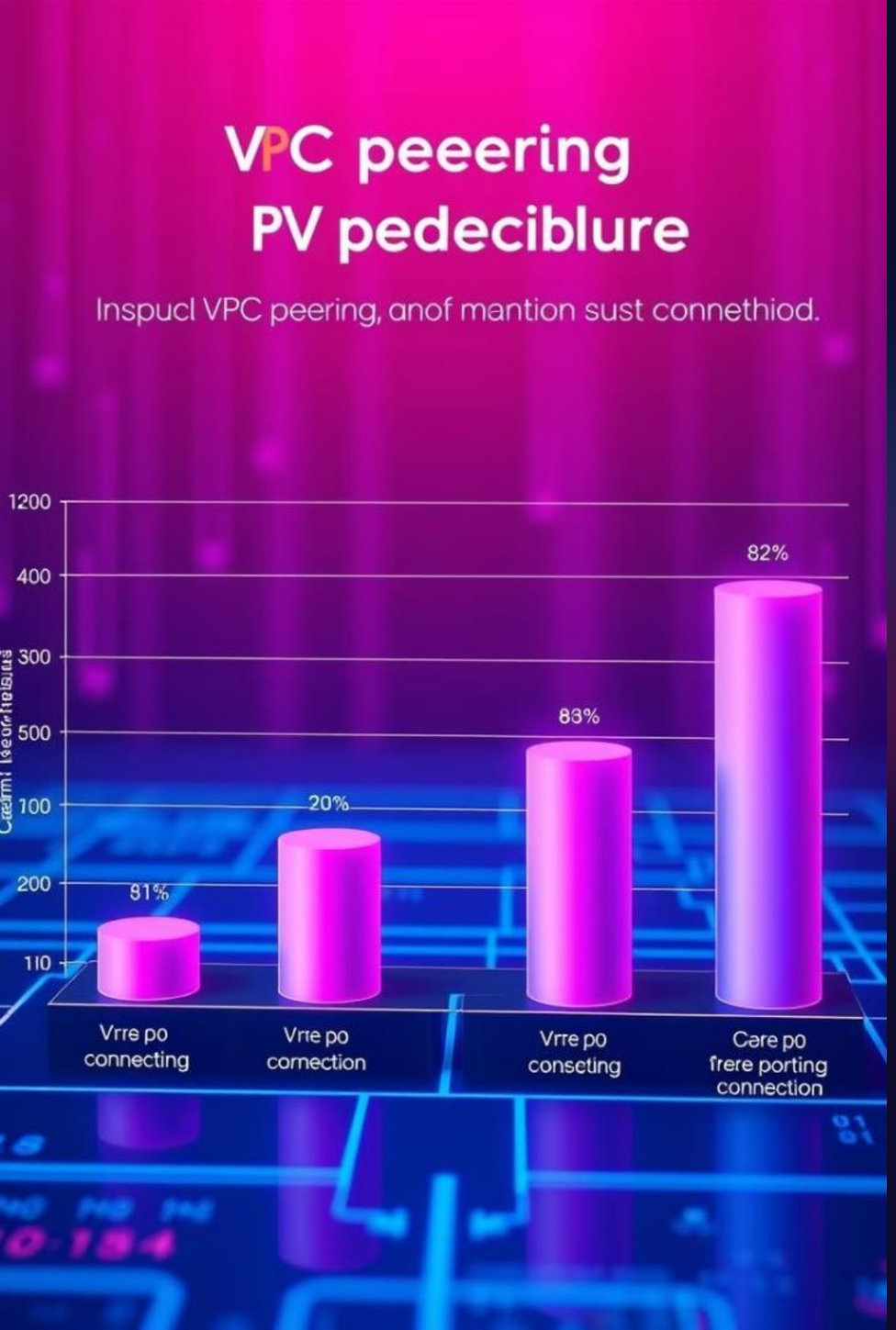
VPC peering connects two VPCs, enabling communication between instances.

No Internet Gateway

Communication occurs directly between the VPCs, bypassing the internet gateway.

Networking Benefit

It's cost-effective and improves the overall network efficiency.



Benefits of VPC Peering

1 **Cost Savings**

Reduces data transfer costs and improves efficiency.

2 **Improved Security**

Data remains within the AWS infrastructure, improving security.

3 **Simplified Management**

It simplifies network management and improves organization.

4 **Enhanced Performance**

Low latency communication between VPCs improves performance.

VPC Peering Requirements

Account Ownership

VPCs must belong to the same AWS account, or different accounts that have enabled resource sharing.

IP Address Space

The IP address ranges of both VPCs must not overlap.

State of VPCs

Both VPCs must be in a healthy state. Check for any errors or issues.

Steps to Establish VPC Peering

1

Request Peering Connection

Initiate the peering connection request from one VPC.

2

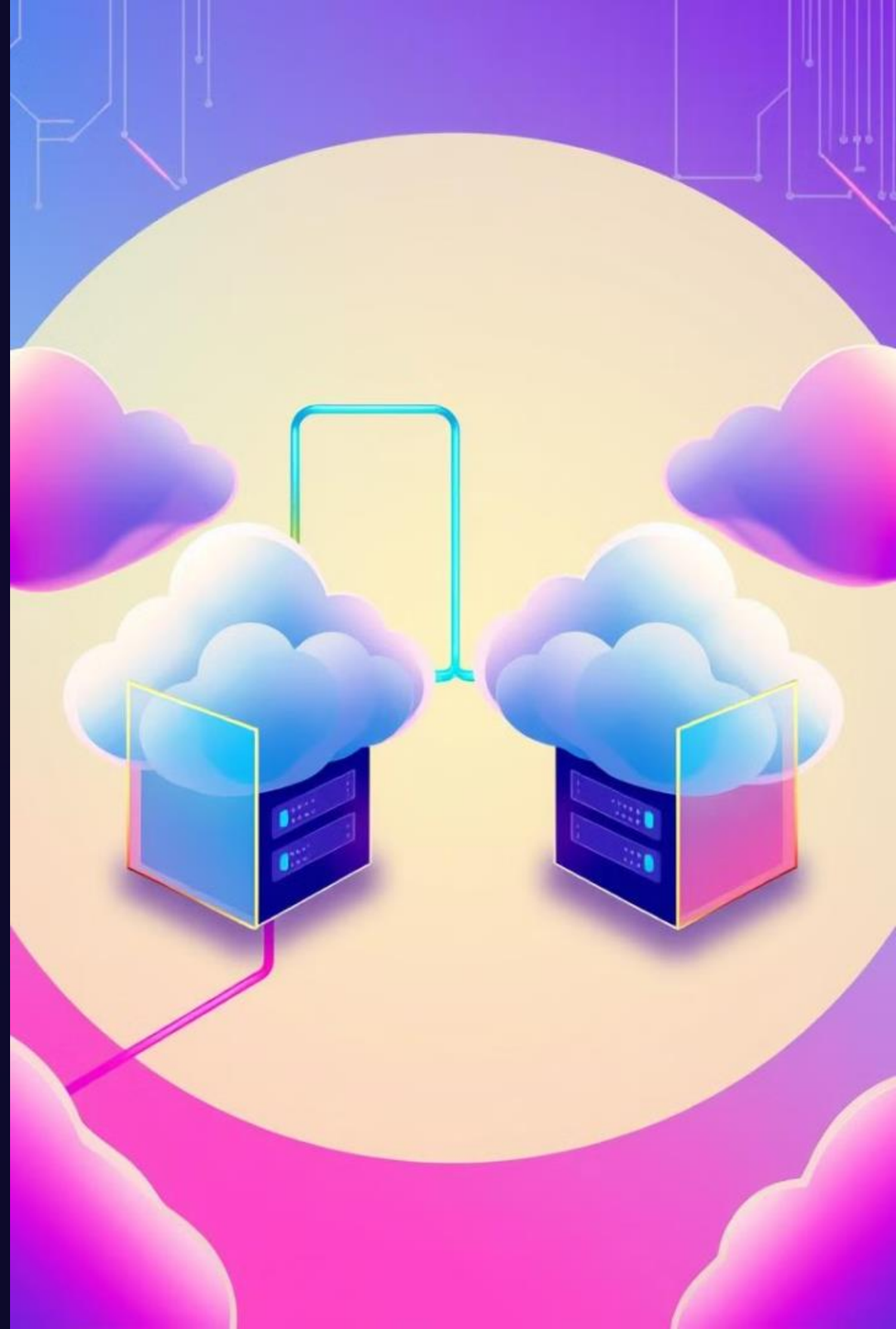
Accept Peering Connection

Accept the peering connection request from the target VPC.

3

Configure Route Tables

Configure route tables to enable traffic flow between the VPCs.



Configuring Route Tables

Route Table	Destination CIDR Block	Target
VPC A	VPC B CIDR	VPC Peering Connection ID
VPC B	VPC A CIDR	VPC Peering Connection ID

Security Considerations

Security Groups

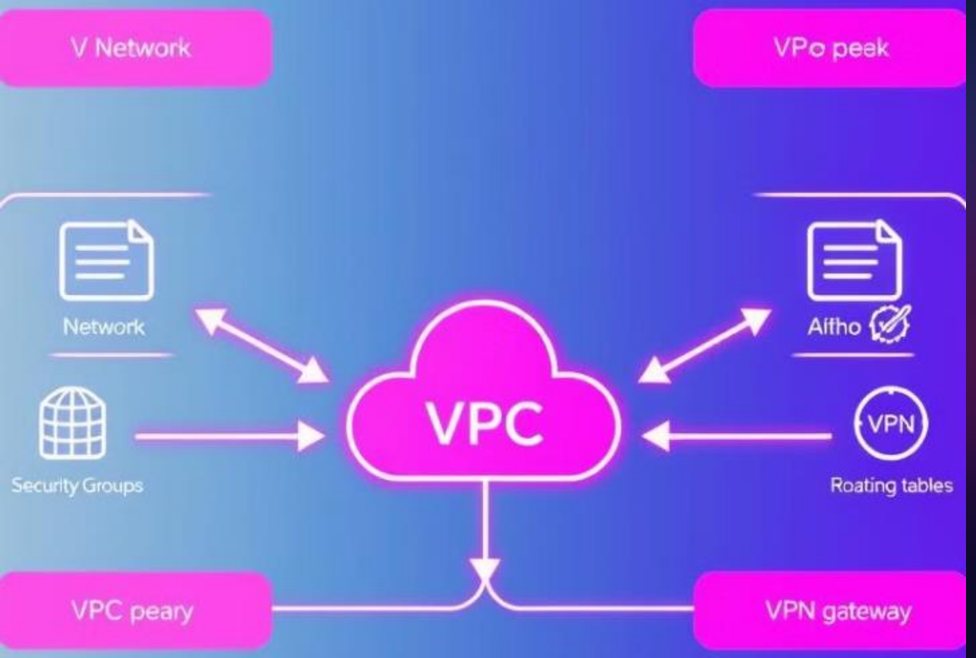
Configure security groups to control traffic flow.

Network ACLs

Use Network ACLs for additional filtering of traffic.

IAM Roles

Restrict access using appropriate IAM roles.



Best Practices and Troubleshooting

1

Regular Monitoring

Monitor peering connection status and health.

2

Testing Connectivity

Test connectivity between instances in both VPCs.

3

Documentation

Maintain accurate documentation of the setup.