AWS Lab 23

VPC Peering

Overview of the lab

In this lab you will learn to how to create VPC peering between two VPC in two different regions(Inter Region VPC Peering)

VPC Peering

It is a network connection between two VPC's , where instance(s) in either VPC can communicate between each other using private IP addresses

It improves security and latency(since it uses amazon private link)

Types

- Inter region VPC (same or different account)

VPC peering between two VPC in different region in same or different aws account

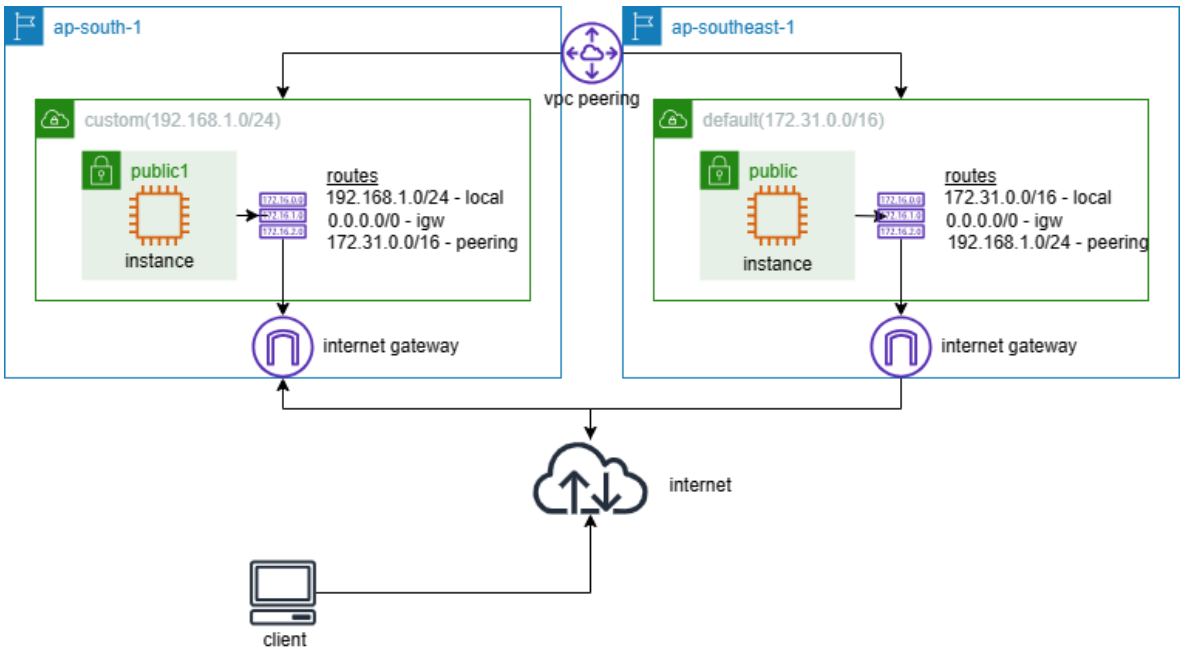
- Intra region VPC(same or different account)

VPC peering between two VPC in same region in same or different aws account

Limitations

VPC should not have same CIDR

Architecture



Step by Step Lab

Launch instance in custom-vpc in ap-south-1(mumbai) region

1. In EC2 management console, click on launch instance
    a. Name and tag – windows-mumbai
    b. Application and OS Images – Windows
    c. Instance type - t2.micro
    d. Key pair – select the existing keypair
    e. Edit Network settings
        a. VPC - custom-vpc
        b. Subnet – custom-vpc-public1
        c. Auto-assign public IP - Enable
        d. Firewall – Select existing security group

e. Common security groups - custom-vpc-demo-sg
f. Click on launch instance

(while it is getting launched)

Launch instance in default-vpc in ap-southeast-1(singapore) region

2. In EC2 management console, click on launch instance
    a. Name and tag – windows-singapore
    b. Application and OS Images – Windows
    c. Instance type - t2.micro
    d. Key pair – Create new key pair
        i. Key pair name - awsclass-singapore-kp
        ii. Click on Create key pair
    e. Edit Network settings
        f. VPC - default-vpc
        g. Subnet – No preference
        h. Auto-assign public IP - Enable
        i. Firewall – Create security group
        j. Security group name - default-vpc-demo-sg

(leave all other settings as default)

f. Click on launch instance

Connect(Login) to both instances(ap-south-1 & ap-southeast-1) instances from local computer(since both are launched in public subnet with public IP address enabled)

Connect to ap-southeast-1 region instance from ap-south-1 region instance using public IP address (It will work)

Connect to ap-southeast-1 region instance from ap-south-1 region instance using private IP address (It will not work)

Create vpc peering (from ap-south-1)

3. In VPC Management Console - Click on Peering connections
4. Click on Create peering connection
    a. Name - demo-peer
    b. VPC ID - custom-vpc
    c. Account - My account
    d. Region - Another Region(singapore)
    e. VPC ID - vpc-xxx (copy from singapore vpc console)
5. Click on Create peering connection

Accept peering connection (from ap-southeast-1)

6. In VPC Management Console - Click on Peering connections
7. Select the peering connection - Actions - Click on Accept request

8. Again click on - Accept request

Manage route table (ap-southeast-1)

9. Click on Route tables and select the default vpc - route table
10. Click on Actions and click on Edit routes
11. Click on Add route
    a. Destination - 192.168.1.0/24 (VPC CIDR ap-south-1)
    b. Target - peering connection
12. Click on Save changes

Manage route table (ap-south-1)

13. Click on Route tables and select the custom-vpc-main-rt
14. Click on Actions and click on Edit routes
15. Click on Add route
    a. Destination - 172.31.0.0/16 (VPC CIDR ap-southeast-1)
    b. Target - peering connection
16. Click on Save changes

Connect to ap-southeast-1 region instance from ap-south-1 region instance using private IP address (It will work)

Clean Up Step

1. In EC2 Management console - Select the instance in ap-south-1 and ap-southeast-1 and terminate it

2. In VPC Management console - Select the peering connection and delete the peering connection & related routes