**Experiment 4: Creating Virtual Private Cloud**

**Aim:** Create Virtual Private Cloud for the cloud-based application.

**Learning Objective**:

* Understand the fundamental concepts and benefits of a Virtual Private Cloud (VPC) within AWS.
* Learn how to design and configure a VPC to securely host and manage resources for a cloud-based application.

**Tools:** AWS, Git, GitHub

**Theory:**

To effectively deploy and manage a cloud-based application on AWS, it is essential to understand and configure several key components of the AWS networking infrastructure. This includes EC2 instances, Virtual Private Cloud (VPC), Internet Gateways, and Route Tables.

1. **EC2 Instances**:

Amazon Elastic Compute Cloud (EC2) provides scalable virtual servers, known as instances, in the AWS cloud. EC2 instances allow users to run applications on virtual machines with varying capacities based on their needs. Instances are available in different types and sizes to optimize cost and performance. You can launch instances from predefined Amazon Machine Images (AMIs) or custom AMIs to suit specific application requirements. EC2 instances can be configured with different amounts of CPU, memory, and storage resources, and can be managed using the AWS Management Console, CLI, or SDKs.

1. **Virtual Private Cloud (VPC)**:

A Virtual Private Cloud (VPC) is a logically isolated network within the AWS cloud. It enables you to define a custom network topology, including IP address ranges, subnets, and network gateways. A VPC provides a secure and controlled environment where you can deploy AWS resources like EC2 instances. You can configure VPC settings to control access to your resources and segment your network into public and private subnets.

1. **Internet Gateway**:

An Internet Gateway (IGW) is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the internet. It is used to enable internet access for resources within your VPC, such as EC2 instances. An IGW supports both inbound and outbound traffic, providing a bridge between the VPC and the external internet.

1. **Attaching an Internet Gateway to a VPC**:

To enable internet connectivity for your VPC, you need to attach an Internet Gateway to it. This process involves creating an IGW in the AWS Management Console and associating it with your VPC. Once attached, the IGW can be used to route internet-bound traffic to and from your VPC.

1. **Route Tables**:

Route Tables are used to control the traffic routing within a VPC. Each route table contains a set of rules, known as routes, that determine where network traffic is directed. A route table defines how packets are routed between subnets within the VPC, to the internet, or to other VPCs. For instance, to allow instances in a public subnet to access the internet, you must configure a route in the route table that directs traffic destined for the internet (0.0.0.0/0) to the Internet Gateway.

**Lab Outcome:**

* Successfully create and configure a VPC to host a cloud-based application, ensuring proper network isolation and security.
* Demonstrate the ability to manage network resources, including subnets, route tables, and security configurations, to support a scalable and secure application environment.

**Implementation:**