iamneo

AWS VPC

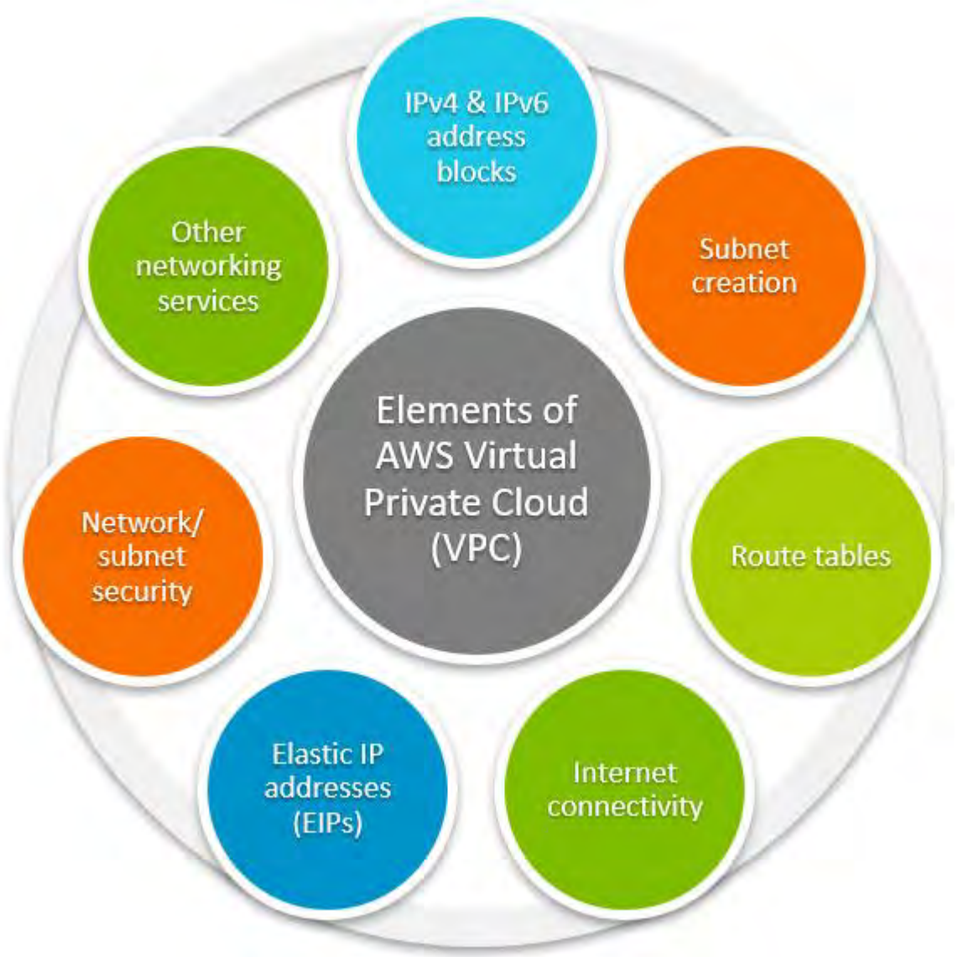
Introduction to AWS VPC

With Amazon Virtual Private Cloud (Amazon VPC), you can launch AWS resources in a logically isolated virtual network that you've defined. This virtual network closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of AWS.

Benefits of Using VPC

- **Improved Security**
- **Better Control**
- **Increased Flexibility**
- **Cost Savings**

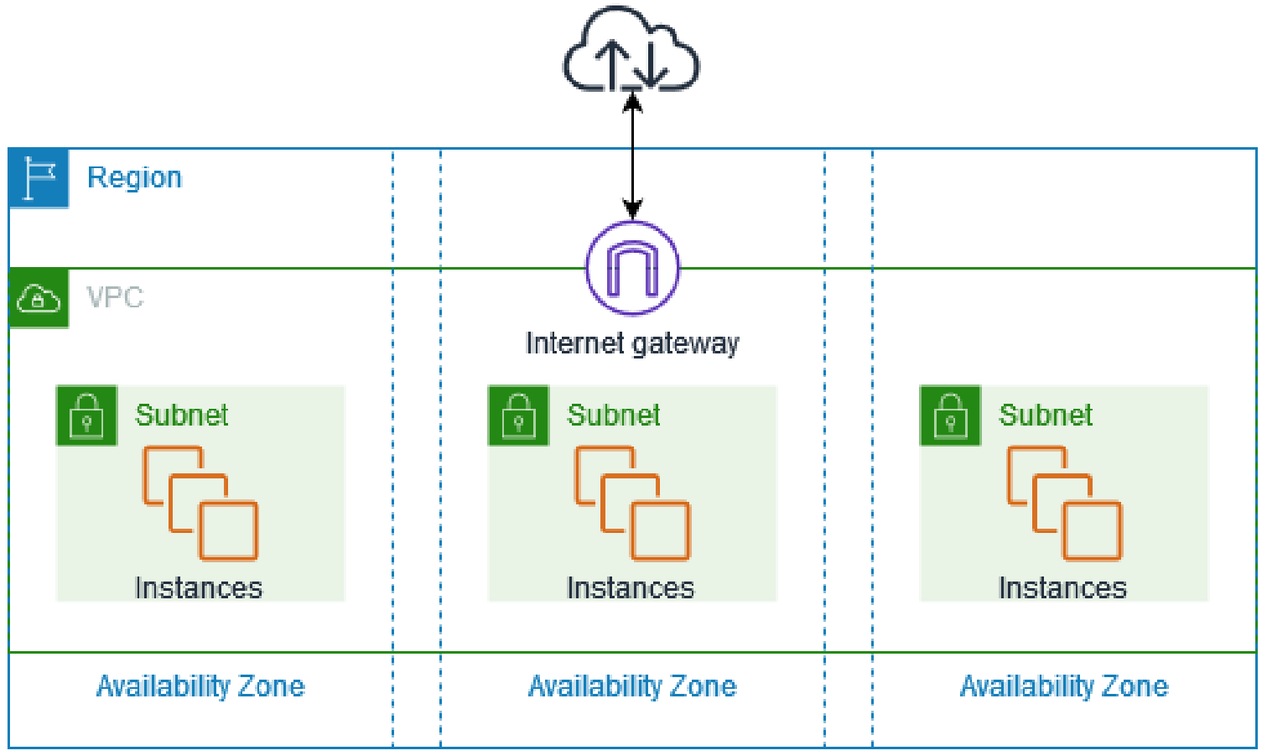
Elements of AWS VPC



Major components of a VPC

The following diagram shows an example VPC. The VPC has one subnet in each of the Availability Zones in the Region, EC2 instances in each subnet, and an internet gateway to allow communication between the resources in your VPC and the internet.

- **VPC CIDR blocks**
- **Subnet CIDR blocks**
- **Route Table**
- **Internet Gateway**

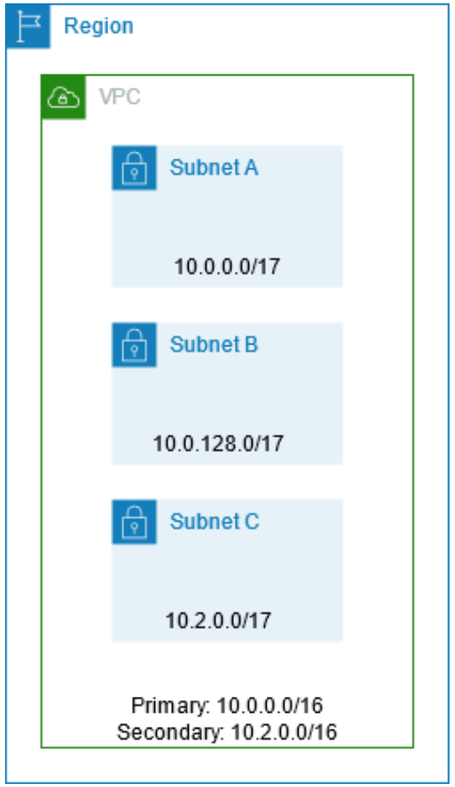


VPC CIDR blocks

Amazon VPC supports IPv4 and IPv6 addressing. A VPC must have an IPv4 CIDR block associated with it. You can optionally associate multiple IPv4 CIDR blocks and multiple IPv6 CIDR blocks to your VPC.

Example VPC CIDR blocks – IPv4

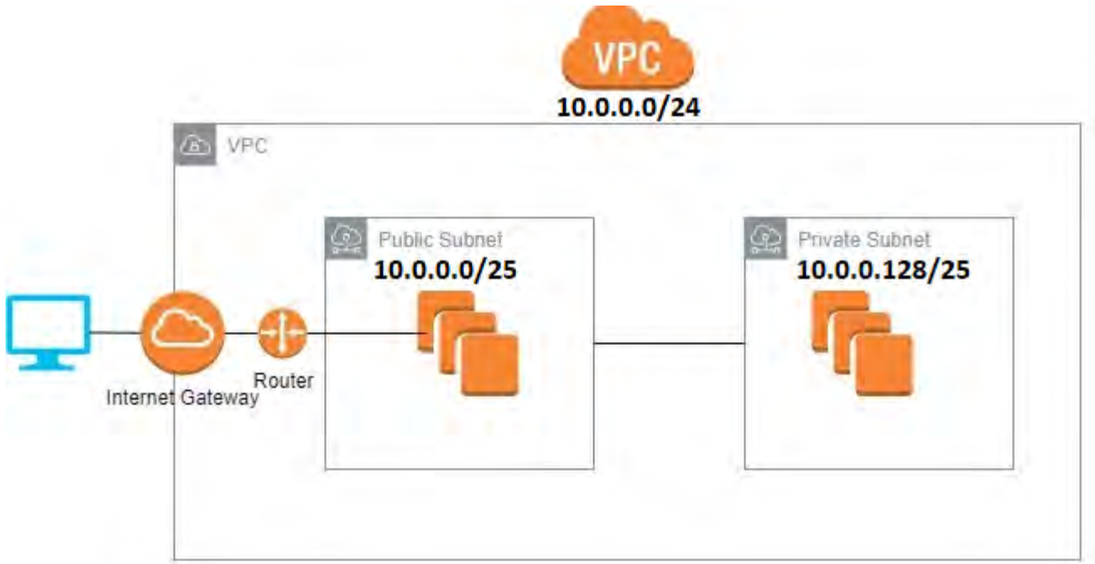
RFC 1918 range	Example CIDR block
10.0.0.0 - 10.255.255.255 (10/8 prefix)	10.0.0.0/16
172.16.0.0 - 172.31.255.255 (172.16/12 prefix)	172.31.0.0/16
192.168.0.0 - 192.168.255.255 (192.168/16 prefix)	192.168.0.0/20



Subnet CIDR blocks

The CIDR block of a subnet can be the same as the CIDR block for the VPC (for a single subnet in the VPC), or a subset of the CIDR block for the VPC (to create multiple subnets in the VPC). The allowed block size is between a /28 netmask and /16 netmask. If you create more than one subnet in a VPC, the CIDR blocks of the subnets cannot overlap.

Example: if you create a VPC with CIDR block 10.0.0.0/24, it supports 256 IP addresses. You can break this CIDR block into two subnets, each supporting 128 IP addresses. One subnet uses CIDR block 10.0.0.0/25 (for addresses 10.0.0.0 - 10.0.0.127) and the other uses CIDR block 10.0.0.128/25 (for addresses 10.0.0.128 - 10.0.0.255).



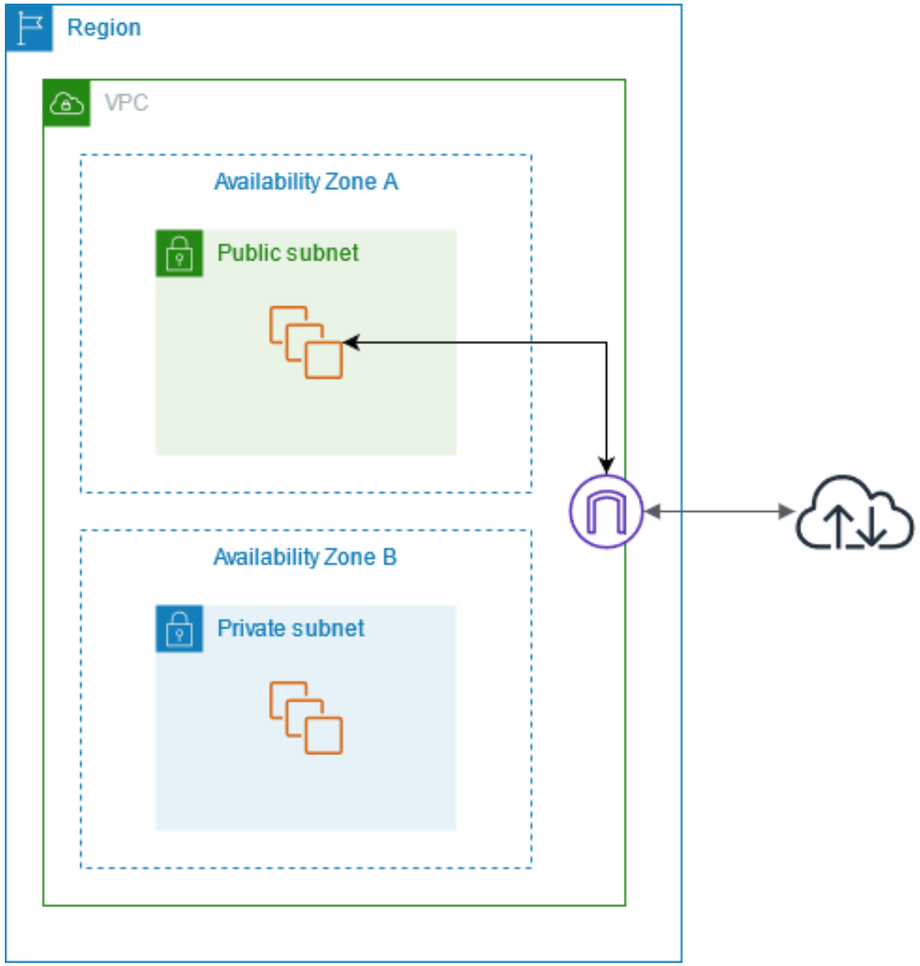
VPC Internet Gateways

Why use it?

With an Internet Gateway, you can enable communication between the instances in your VPC and the internet while keeping them secure.

How to configure?

Create an Internet Gateway, Attach the internet gateway to a VPC, and then update the route table of the VPC subnet to point traffic to the internet gateway.



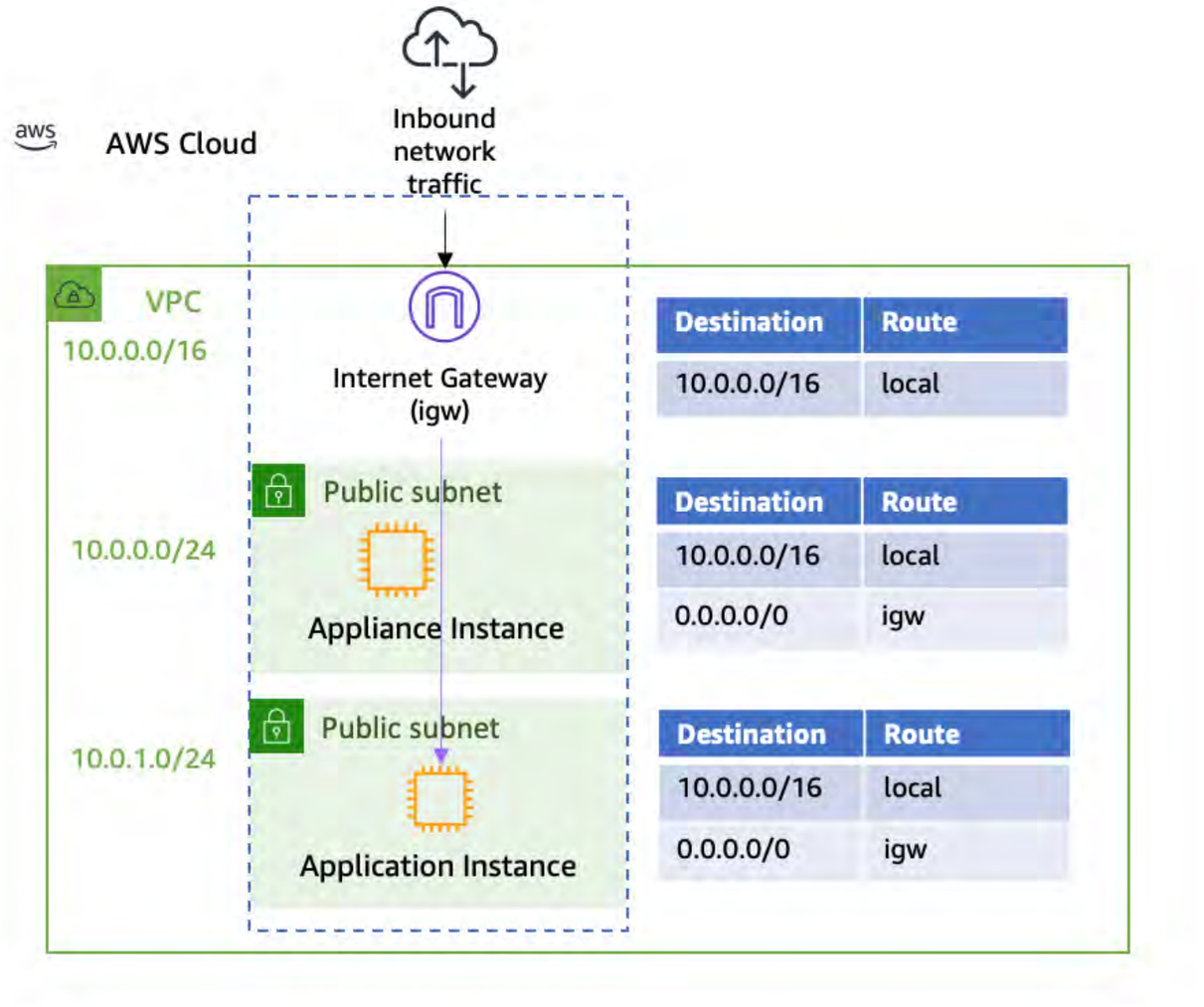
VPC Route tables

Subnets

Divide a VPC's IP address range into smaller CIDR blocks to utilize resources more efficiently.

Route Tables

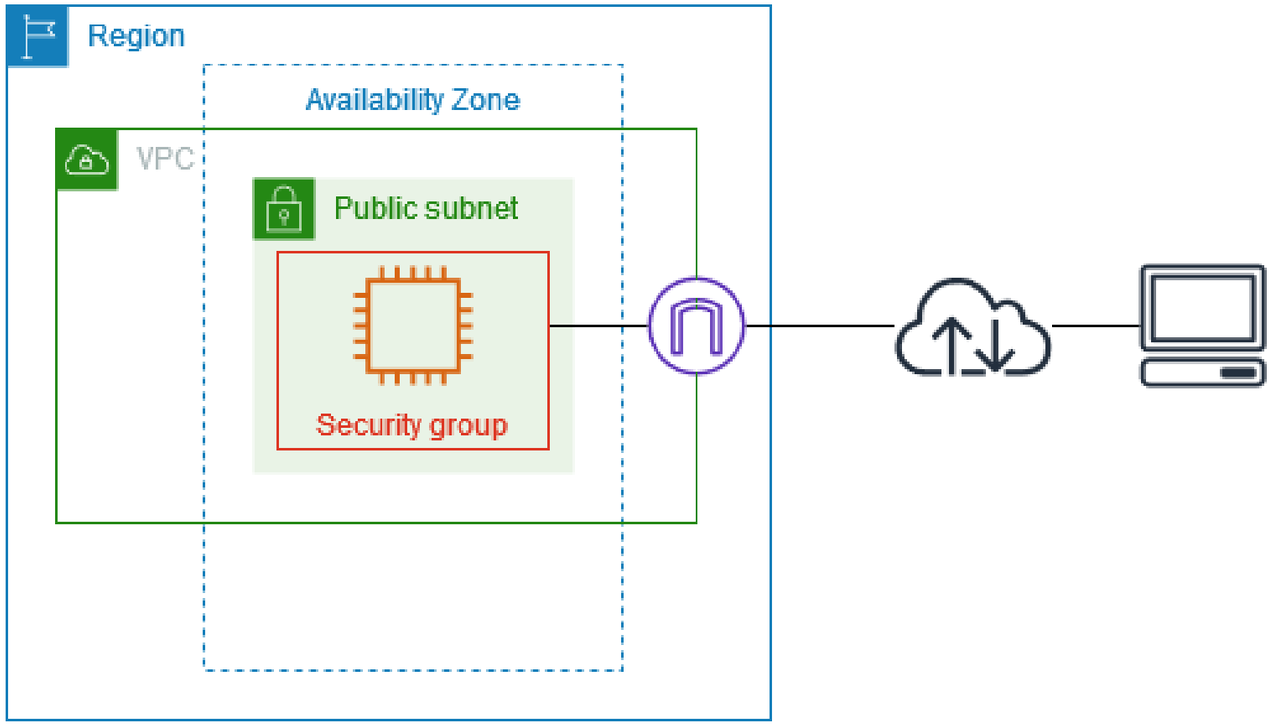
Define how traffic should be directed between subnets and to the internet. Routing can be customized based on the destination IP address.



VPC with Public Subnet

Public Subnet

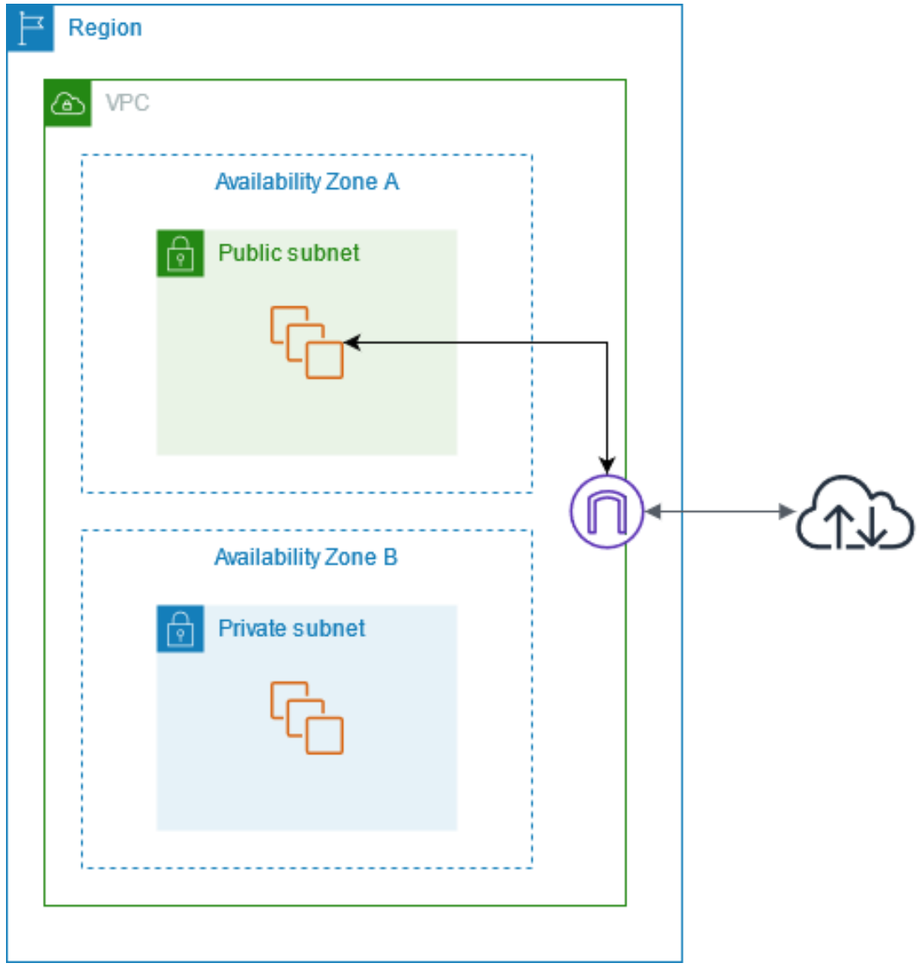
A public subnet is a subnet that is associated with a Route Table that has a route to an Internet Gateway (Igw). This route allows access from the Public Internet to the subnet.



VPC with Private Subnet

Private Subnet

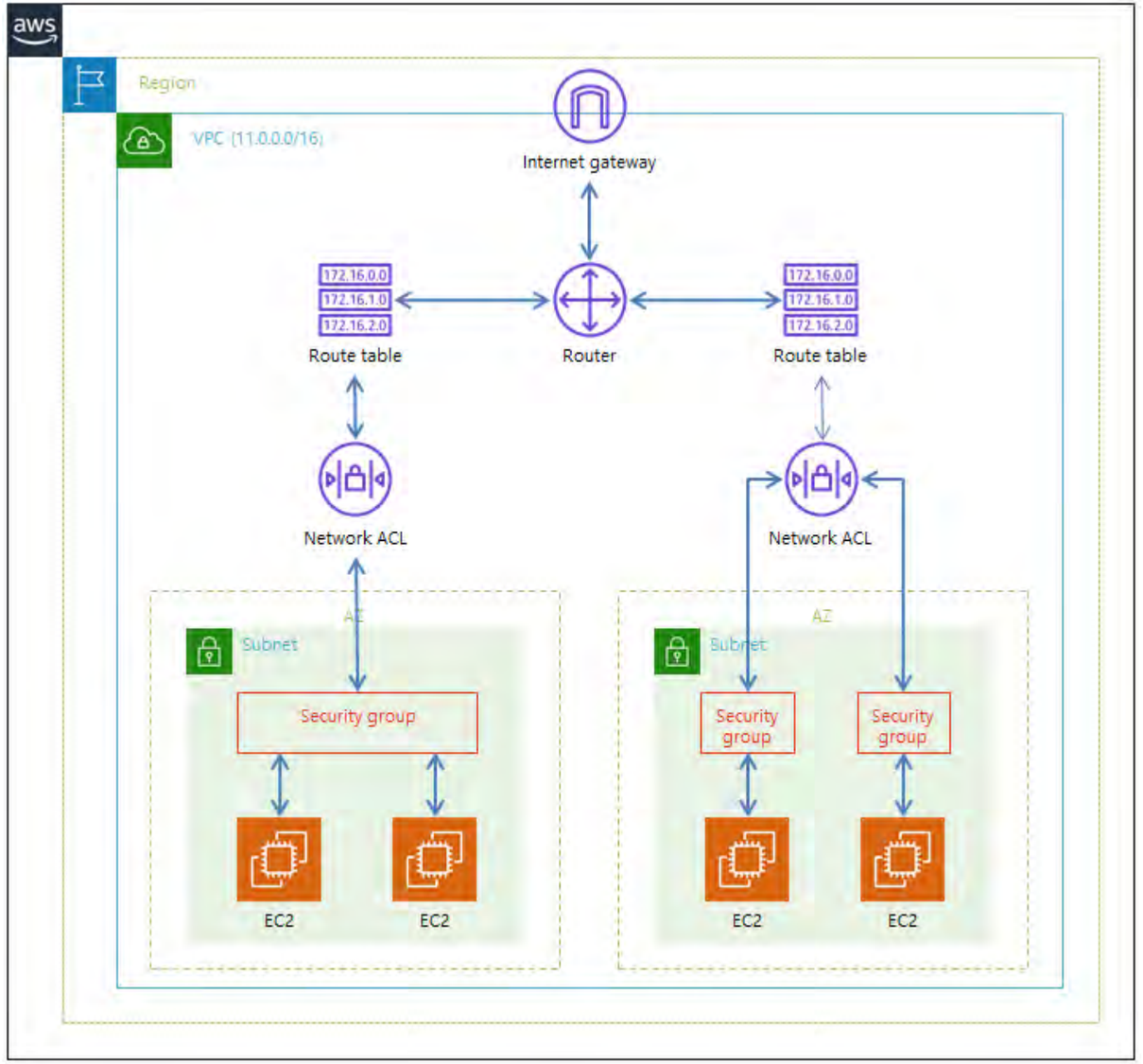
- A private subnet is a subnet that is associated with a route table that doesn't have a route to an internet gateway.
- Resources in private subnets cannot communicate with the public internet.
- AWS resources within the same VPC CIDR can communicate via their private IP addresses.



Network ACL in AWS VPC

Network ACL

- A network access control list (ACL) allows or denies specific inbound or outbound traffic at the subnet level.
- You can use the default network ACL for each VPC, or you can create a custom network ACLs for your VPCs, with rules that are similar to the rules for your security groups.
- This provides an additional layer of security to your VPC.
- There is no additional charge for using default network ACLs.



Elastic IP Addresses

1 What are they?

Elastic IP addresses are static IPv4 addresses that you can allocate and associate with your AWS account. They allow you to mask the failure of an instance or software.

2 Why use them?

They provide the flexibility to mask an instance or software failure by quickly remapping the address to another instance in your account.

3 How to configure?

Allocate an elastic IP address, associate the IP address with your instances or network interfaces, and then update your domain name service (DNS) records.

Use Cases for VPC

Development and Testing	VPC allows you to create a sandbox environment for development and testing without affecting your production environment. You can easily create and destroy instances to test your applications.
Web Hosting	VPC provides a scalable and secure environment for hosting your websites. It allows you to easily configure load balancing, auto scaling, and high availability for your applications.
Big Data Analytics	VPC allows you to easily deploy and scale your big data analytics applications. You can securely connect to data sources and use AWS EMR and other tools to process and analyze your data.

Introduction to AWS VPC Creation

Learn how to create a Virtual Private Cloud in AWS with this step-by-step guide. We'll cover everything from IP address ranges to VPC security best practices.

Creating a VPC in AWS

Pre-Setup

1. AWS Account Registration and Setup
2. AWS Console Access
3. Acquiring AWS Credentials

Setup

1. VPC Creation
2. Creation of DHCP Options Sets
3. Creation of Subnets
4. Create Internet Gateway
5. Attach the Internet Gateway to VPC

Post Setup

1. Launch an EC2 Instance within VPC
2. Assign Static IPs
3. Configuring Elastic IP Addresses
4. Configure Security Groups and Firewalls

Enabling Internet Connectivity within VPC

- **Create a Public Subnet**

  You can create a public subnet that has a route table entry that points to an Internet Gateway.

- **Create a Private Subnet**

  Create a private subnet that has a route table entry that points to a NAT gateway.

- **Configure Security Groups**

  Add an inbound rule to the instance to allow HTTP traffic and add an outbound rule to allow all traffic.

iamneo

Thankyou