**Virtual Private Cloud (Amazon VPC)**

The Amazon Virtual Private Cloud (Amazon VPC) is a custom-defined virtual network within the AWS Cloud. You can provision your own logically isolated section of A WS, similar to designing and implementing a separate independent network that would operate in an on premises data center.

Amazon VPC is the networking layer for Amazon Elastic Compute Cloud (Amazon EC2), and it allows you to build your own virtual network within AWS.

You will have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways.

You can easily customize the network configuration for your Amazon Virtual Private Cloud.

For example, you can create a public-facing subnet for your webservers that has access to the Internet, and place your backend systems such as databases or application servers in a private facing subnet with no Internet access.

VPCs also have a few limits set on them by default. For example, you can have a maximum of five VPCs per region. Each VPC can have a max of one Internet gateway as well as one virtual private gateway. Also, each VPC has a limit of hosting a maximum of up to 200 subnets per VPC. You can increase these limit by simply requesting AWS to do so.

An Amazon VPC consists of the following components:

* Security groups
* Subnets
* Network Access Control Lists (ACLs)
* Route tables
* Dynamic Host Configuration Protocol (DHCP) option sets

An Amazon VPC has the following optional components:

* Internet Gateways (IGWs)
* Elastic IP (EIP) addresses
* Elastic Network Interfaces (ENis)
* Endpoints
* Peering
* Network Address Translation (NATs) instances and NAT gateways
* Virtual Private Gateway (VPG), Customer Gateways (CGW.s), and Virtual Private Networks (VPNs).

By default, AWS will create a VPC for you in your particular region the first time you sign up for the service. This is called as the default VPC. The default VPC comes preconfigured with the following set of configurations:

The default VPC is always created with a CIDR block of/ 16, which means it supports 65,536 IP addresses in it.

A default subnet is created in each AZ of your selected region. Instances launched in these default subnets have both a public and a private IP address by default as well.

An Internet Gateway is provided to the default VPC for instances to have Internet connectivity.

A few necessary route tables, security groups, and ACLs are also created by default that enable the instance traffic to pass through to the Internet.

Classless Inter-Domain Routing (CIDR): When you create an Amazon VPC, you must specify the 1Pv4 address range by choosing a Classless Inter-Domain Routing (CIDR) block, such as 10.0.0.0/ 16. The address range of the Amazon VPC cannot be changed after the Amazon VPC is created. An Amazon VPC address range may be as large as / 16 (65,536 available addresses) or as small as / 28 ( 16 available addresses) and should not overlap other network with which they are to be connected.

**Subnets:** A subnet is a segment of an Amazon VPC's IP address range where you can launch Amazon EC2 instances, Amazon Relational Database Service {Amazon RDS) databases, and other AWS resources.

After creating an Amazon VPC, you can add one or more subnets in .each Availability Zone. Subnets reside within one Availability Zone and cannot span zones.

Remember that by default one subnet created in one Availability Zone. You can, however, have multiple subnets in one Availability Zone.

Subnets can be classified as public, private, or VPN-only.

A public subnet is one in which the associated route table directs the subnet's traffic to the Amazon VPC's IGW.

A private subnet is one in which the associated route table does not direct the subnet's traffic to the Amazon VPC's IGW.

A VPN-only subnet is one in which the associated route table directs the subnet's traffic to the Amazon VPC's VPG and does not have a route to the IGW.

**Route Tables:**

A route table is a logical construct within an Amazon VPC that contains a set of rules (called routes) that are applied to the subnet and used to determine where network traffic is directed.

You can modify route tables and add your own custom routes.

You can also use route tables to specify which subnets are. public (by directing Internet traffic to the IGW) and which subnets are private {by not having a route that directs traffic to the IGW).

Each route table contains a default route called the local route, which enables communication within the Amazon VPC, and this route cannot be modified or removed.

Additional routes can be added to direct traffic to exit the Amazon VPC via the IGW, the VPG, or the NAT instance.

You should remember the following points about route tables: