Amazon Virtual Private Cloud

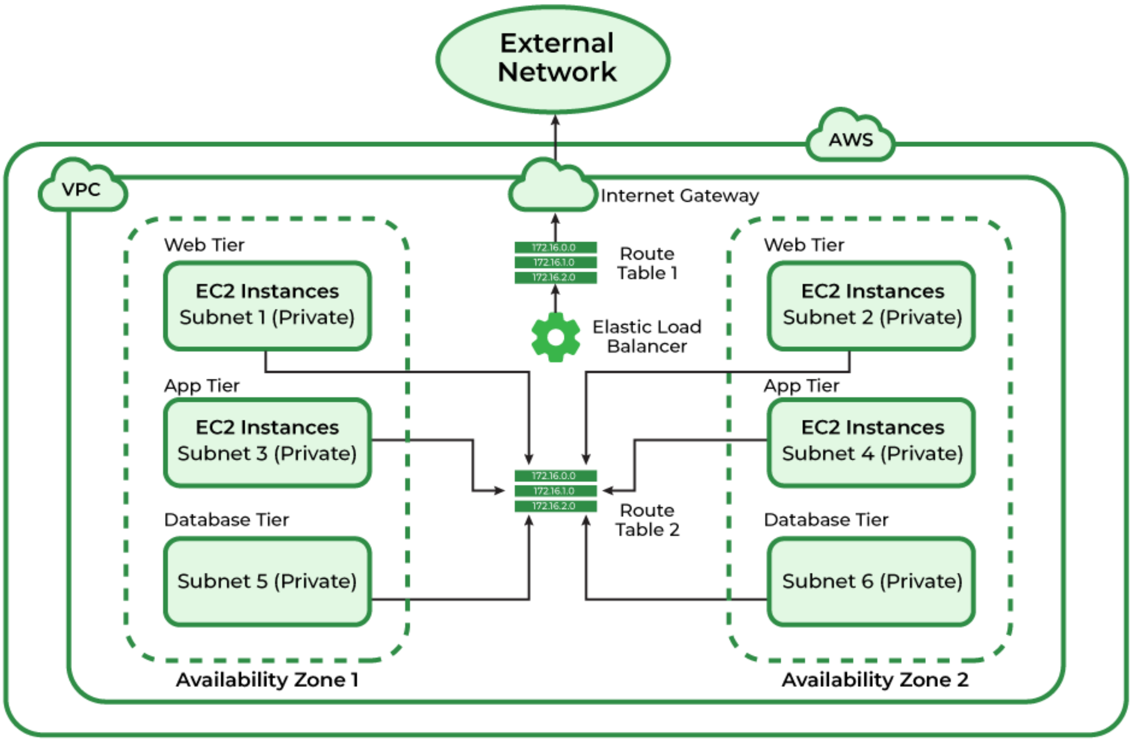
Amazon VPC or **Amazon Virtual Private Cloud** is a service that allows its users to launch their virtual machines in a protected as well as isolated virtual environment defined by them. You have complete control over your VPC, from creation to customization and even deletion. It's applicable to organizations where the data is scattered and needs to be managed well. In other words, VPC enables us to select the virtual address of our private cloud and we can also define all the sub-constituents of the VPC like subnet, subnet mask, availability zone, etc on our own.

- We can place the necessary resources and manage access to those resources in the VPC, a private area of Amazon that we control.
- A default "VPC" will be generated when we register an AWS account, allowing us to manage the virtual networking environment, the IP address, the construction of subnets, route tables, and gateways.

The Architecture of Amazon VPC

The basic architecture of a properly functioning VPC consists of many distinct services such as Gateway, Load Balancer, Subnets, etc. Altogether, these resources are clubbed under a VPC to create an isolated virtual environment. Along with these services, there are also security checks on multiple levels.

It is initially divided into subnets, connected with each other via route tables along with a load balancer.



VPC Components

- **VPC:** You can launch AWS resources into a defined virtual network using Amazon Virtual Private Cloud (Amazon VPC). With the advantages of utilizing the scalable infrastructure of AWS, this virtual network closely mimics a conventional network that you would operate in your own data center. /16 user-defined address space maximum (65,536 addresses)

- **Subnetes:** To reduce traffic, the subnet will divide the big network into smaller, connected networks. Up to /16, 200 user-defined subnets.
- **Route Tables:** Route Tables are mainly used to Define the protocol for traffic routing between the subnets.
- **Network Access Control Lists:** Network Access Control Lists (NACL) for VPC serve as a firewall by managing both inbound and outbound rules. There will be a default NACL for each VPC that cannot be deleted.
- **Internet Gateway(IGW):** The Internet Gateway (IGW) will make it possible to link the resources in the VPC to the Internet.
- **Network Address Translation (NAT):** Network Address Translation (NAT) will enable the connection between the private subnet and the internet.

VPC Fundamentals

- If the subnet has internet access then it is called PublicSubnet.
- If the subnet doesn’t have internet access then it is called PrivateSubnet.
- A subnet must reside entirely within one Availability Zone.
- An entire subnet must be contained within a single Availability Zone.
- Access between instances is managed by VPC Security Groups for both inbound and outgoing traffic (EC2 Security Groups can only define inbound rules).
- We can specify Subnet IP Routing with the aid of the Route Table.
- If a server/instance which is in a private subnet wants to reach the internet then it must have NAT in a public subnet.