Subnets

As discussed before, VPCs (Virtual Private Clouds), i.e. the virtual boxes into which we place our AWS resources are an integral component of any cloud environment/architecture that is even remotely complex.

Well, to take the box analogy one step further, when placing a vast array of things into boxes, is it not so much easier and neater if we were to group all the similar items together? Such as putting all the toys in one compartment and all the books in another. Makes things a whole lot easier right? Subnets in AWS are similar to those compartments except for VPCs. They allow us to logically separate different types of resources within your VPC.

So one could for example, have a VPC containing both the web server EC2 instances as well as say, RDS database instances. Subnets allow us to segment portions of a VPC allowing us to logically isolate our EC2 instances from the RDS database instances. They allow us to allocate IP addresses to resources (like EC2 instances) and enforce network access controls through Network Access Control Lists (ACLs) and Security Groups (Will be discussed in later chapters) therefore playing a crucial role in organizing and securing your AWS resources within a VPC environment.

Let us illustrate the logical segmentation performed by the VPC using the aforementioned scenario as an example, utilizing CIDR blocks:

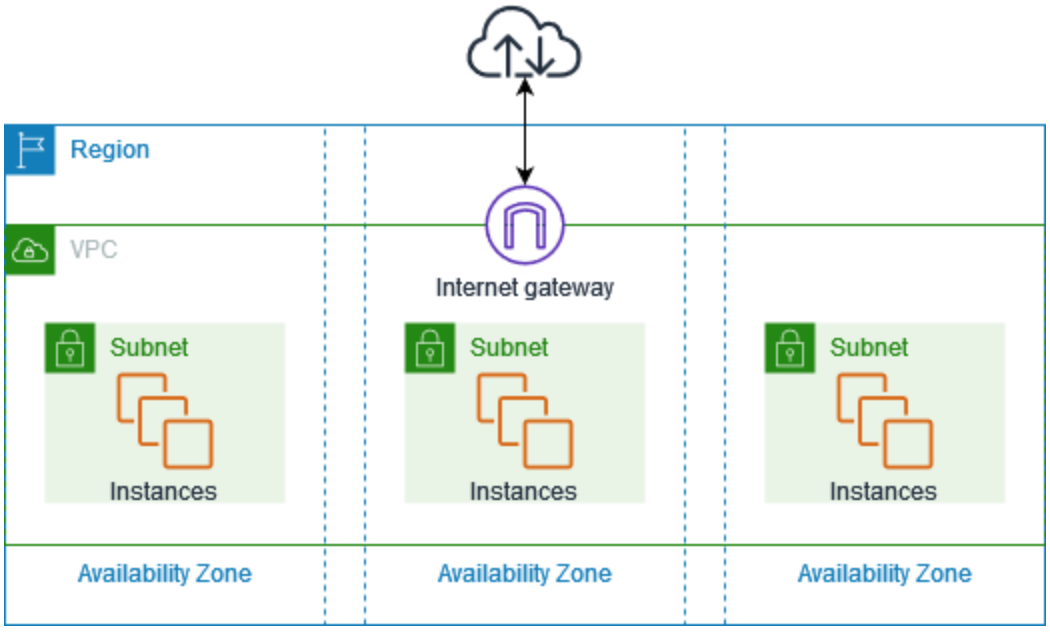
Imagine the hypothetical VPC CIDR block to be of the range: `0.0.0.0/16`

- This gives us a total of 65,536 IP addresses (from `10.0.0.0` to `10.0.255.255`)

Then, we can design the Subnet to be as follows:

- **Public Subnet for Web Servers**
  - **CIDR Block**: `10.0.1.0/24`
  - **IP Address Range**: `10.0.1.1` to `10.0.1.254`
  - **Purpose**: This subnet will host the EC2 instances that run the web servers, allowing them to be accessible from the internet.
- **Private Subnet for RDS Database Instances**
  - **CIDR Block**: `10.0.2.0/24`
  - **IP Address Range**: `10.0.2.1` to `10.0.2.254`
  - **Purpose**: This subnet will host the RDS instances. It is private, meaning the RDS instances are not directly accessible from the internet.

Note however that subnets are afflicted by a restriction which are not applicable to VPCs, as each subnet created by us is mapped to a single Availability Zone while VPCs have the capability to span across multiple availability zones.



Architecture of a VPC with 3 Subnets (Source: AWS)