**What is VPC**

To host or server any resource / service we definitely need a network.

Whenever we launch a service, AWS will take care of creating network setup like subnets, route tables, ip address, internet gateway, and so on which are needed to access that service. Through this network we can access the services.

So instead of using AWS default network setup we want to use our own private network setup. Instead of launching AWS services in the default network setup we want to launch AWS resources in our custom/private network setup. VPC will help us to do this.

Amazon Virtual Private Cloud (Amazon VPC) enables you to launch AWS resources into a virtual network that you've defined. It is logically isolated from other virtual networks in the AWS Cloud.

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.

VPC will help us to customize the network setup, we can select ip address range, launching subnets in VPC as public or private, configuring route tables, setup internet gateways, define security groups and network access control list etc.

**Note:** VPC is Region specific service. A VPC spans all of the Availability Zones in the Region. This means if we create a custom VPC in a region then the VPC is accessible in all Available Zones of that Region.


    VPC with the main route table
   

Core and important concepts in VPC are.

1. Subnets

2. Route table

3. NACL (network access control list) know as Security groups

4. Internet gateway

5. NAT gateway

**Subnet**

Networks become more complicate to manage when the size in increasing. Subnets are used to make management of complex networks easy by breaking into smaller manageable sub networks. This is why we call it as Subnet.

Subnet is nothing but a logical sub division of the bigger network.

Let’s see subnetting in real life examples. Let assume we have ordered a pizza, it is hard to eat pizza as it is, so we will make it into smaller slices to eat easily. Similarly, it is difficult to manage the whole network as it is, so we will make it into smaller sub-networks called as subnets.

**Note:** subnet is Zone specific. Each subnet must reside entirely within one Availability Zone and cannot span across multiple zones.

We will look deep into subnets in subnet section.

**Route table**

A Router is a networking device that forwards the information in form of data packets between computer network. When a data packet comes to a router port, the router reads address information in packet to determine out which port the packet will be sent.

When a packet arrives at a Router, it examines destination IP address of a received packet and make routing decisions accordingly. Routers use *Routing Tables* to determine out which interface the packet will be sent.

A routing table is a set of rules, called **routes**, that are used to determine where network traffic from your subnet or gateway is directed. Route table mainly have two columns in it.

1. Destination
2. Target

**Destination**—The range of IP addresses where you want traffic to go (destination CIDR). For example, an external corporate network with a 172.16.0.0/12 CIDR.

**Target**—The gateway, network interface, or connection through which to send the destination traffic; for example, an internet gateway.

We will study route table more in depth in route table section.

**Security groups**

A security group acts as a virtual firewall for our AWS resources (i.e. instance) to control inbound and outbound traffic.

Security groups act at the Resource (i.e. Instance) level, not the subnet level. Therefore, each resource/instance in a subnet in your VPC can be assigned to a different set of security groups.

When you launch an instance in a VPC, you can assign up to five security groups to the instance.

Will study about security groups more detail in further sessions.

**NACL (Network access control list)**

A network access control list(ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets.

NACL contains set of rules similar to our security groups. The difference between ACL and Security groups is, ACL will have two actions on a rule ALLOW/DENY, where as Security group will have only ALLOW action on a rule.

This means we can define ALLOW traffic and DENY traffic in ACL, but in Security groups we only define ALLOW traffic. Any traffic other than ALLOW will automatically become DENY traffic in Security groups.

Will see more about NACL in further sections.

**NAT Gateway**

NAT stands for Network Address Translator.

NAT Gateway will be used when we are working with subnets. There are 2 types of subnets.

1. Public subnet

2. Private subnet

When the subnet is connected to an internet gateway then it will become public subnet. If the internet gateway is not connected to the subnet then it will become private subnet.

But if we want to make some updates in our instance which is launched in private subnet, we need internet. To provide internet connectivity to private subnet we will use NAT Gateway.

**Note:**

When we created our own VPC it will create a Route Table and Network ACL automatically and attach them to the VPC.

After creating VPC we need to create an Internet Gateway and attach it to the VPC.