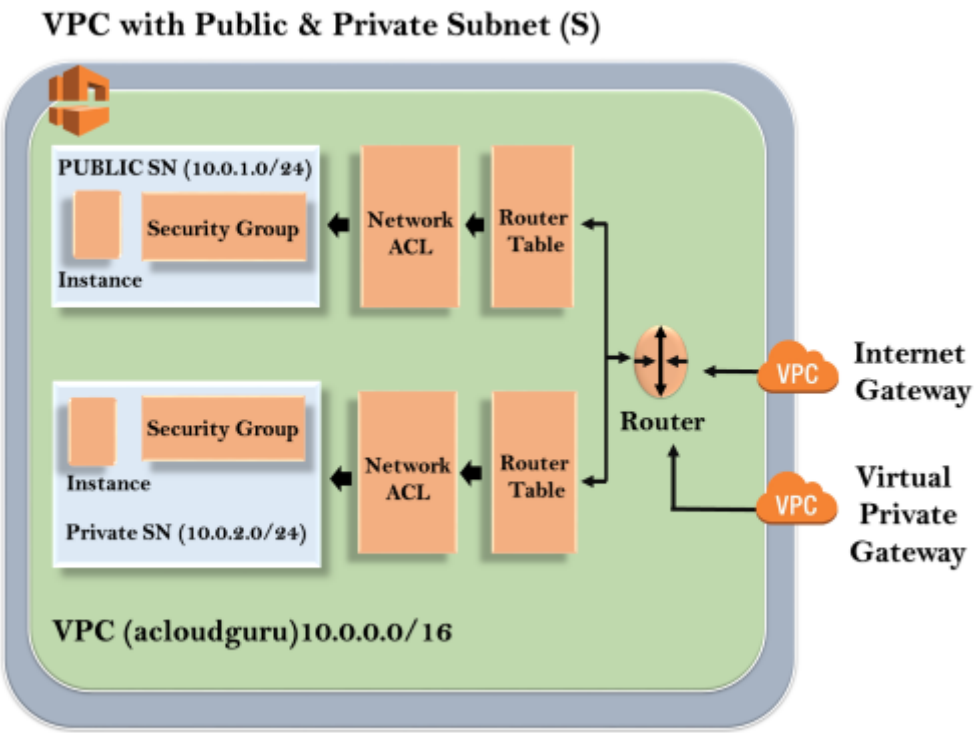
Amazon VPC

What is VPC

- VPC stands for Virtual Private Cloud.
- Amazon Virtual Private Cloud (Amazon VPC) provides a logically isolated area of the AWS cloud where you can launch AWS resources in a virtual network that you define.
- You have complete control over your virtual networking environment, including a selection of your IP address range, the 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 web servers that can access to the internet and can also place your backend system such as databases or application servers to a private-facing subnet.
- You can provide multiple layers of security, including security groups and network access control lists, to help control access to Amazon EC2 instances in each subnet.

Architecture of VPC



The outer line represents the region, and the region is us-east-1. Inside the region, we have VPC, and outside the VPC, we have internet gateway and virtual private gateway. Internet Gateway and Virtual Private Gateway are the ways of connecting to the VPC. Both these connections go to the router in a VPC and then router directs the traffic to the route table. Route table will then direct the traffic to Network ACL. Network ACL is the firewall or much like security groups. Network ACL are statelist which allows as well as deny the roles. You can also block the IP address on your Network ACL. Now,

move over to the security group that accesses another line against the EC2 instance. It has two subnets, i.e., Public and Private subnet. In public subnet, the internet is accessible by an EC2 instance, but in private subnet, an EC2 instance cannot access the internet on their own. We can connect the instances. To connect an instance, move over to the public subnet and then it SSH to the private subnet. This is known as jump boxes. In this way, we can connect an instance in public subnet to an instance in private subnet.

Some ranges are reserved for private subnet:

- 10.0.0.0 - 10.255.255.255 (10/8 prefix)
- 172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
- 192.168.0.0 - 192.168.255.255 (192.108/16 prefix)

What can we do with a VPC?

- Launch instances in a subnet of your choosing. We can choose our own subnet addressing.
- We can assign custom IP address ranges in each subnet.
- We can configure route tables between subnets.
- We can create an internet gateway and attach it to our VPC.
- It provides much better security control over your AWS resources.
- We can assign security groups to individual instances.
- We also have subnet network access control lists (ACLS).

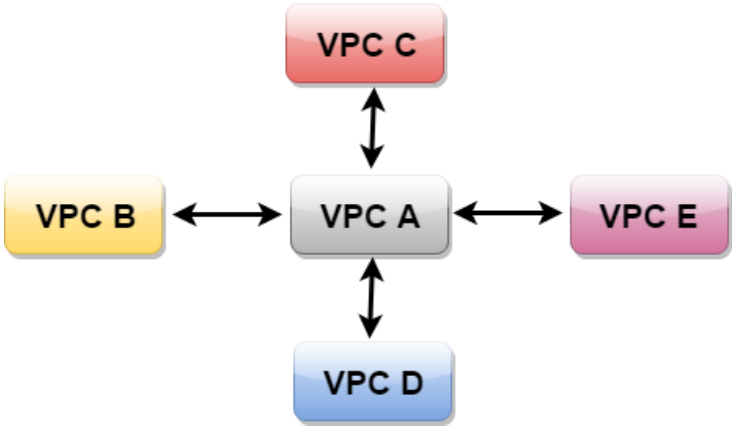
VPC Peering

- VPC Peering is a networking connection that allows you to connect one VPC with another VPC through a direct network route using private IP addresses.
- Instances behave as if they were on the same private network.
- You can peer VPC's with other AWS accounts as well as other VPCs in the same account.
- Peering is in a star configuration, i.e., 1 VPC peers other 4 VPCs.
- It has no **Transitive Peering!!**.

Note: Non-Transitive Peering means the networks that you want to connect are directly linked.

- You can peer between regions. Suppose you have one VPC in one region and other VPC in another region, then you can peer the VPCs between different regions.

Let's understand the example of non-transitive peering through an example.



The above figure shows that VPC B has peered to the VPC A, so instance in VPC B can talk to VPC A. However, VPC B cannot talk to VPC C through VPC A. This is known as Non-Transitive Peering, i.e., both VPC C and VPC B are not directly linked so they cannot talk to each other.