**Assignment-17-May-22**

1. **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.

1. **What is Subnet?**

A subnet, or subnetwork, is a [network](https://www.cloudflare.com/learning/network-layer/what-is-the-network-layer/) inside a network. Subnets make networks more efficient. Through subnetting, network traffic can travel a shorter distance without passing through unnecessary [routers](https://www.cloudflare.com/learning/network-layer/what-is-routing/) to reach its destination.

**3. What is Internet Gateway?**

An internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between your VPC and the internet. An internet gateway enables resources (like EC2 instances) in your public subnets to connect to the internet if the resource has a public IPv4 address or an IPv6 address. Similarly, resources on the internet can initiate a connection to resources in your subnet using the public IPv4 address or IPv6 address. For example, an internet gateway enables you to connect to an EC2 instance in AWS using your local computer.

An internet gateway serves two purposes: to provide a target in your VPC route tables for internet-routable traffic, and to perform network address translation (NAT) for instances that have been assigned public IPv4 addresses.

**4.What is Router?**

Each AWS VPC has a VPC router. The primary function of this VPC router is to take all of the route tables defined within that VPC, and then direct the traffic flow within that VPC, as well as to subnets outside of the VPC, based on the rules defined within those tables.

**5. What is Peering Connection?**

* 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!!****.

1. **What is VPC endpoints?**

* A VPC endpoint allows you to privately connect your VPC to supported AWS services and VPC endpoint services powered by ****PrivateLink**** without requiring an internet gateway, NAT device, VPN Connection, or AWS Direct Connect connection.
* Instances in your VPC do not require public addresses to communicate with the resources in the service. Traffic between your VPC and the other service does not leave the Amazon network.
* VPC endpoints are virtual devices.
* VPC Endpoints are horizontally scaled, redundant and highly available VPC components that allow communication between instances in your VPC and services without imposing availability risks or bandwidth constraints on your network traffic.

**7. What is NAT instance?**

A NAT (Network Address Translation) instance is, like a bastion host, an EC2 instance that lives in your public subnet. A NAT instance, however, allows your private instances outgoing connectivity to the internet while at the same time blocking inbound traffic from the internet.

**8. What is NAT gateway?**

* NAT stands for ****Network Address Translation****.
* If you want your EC2 instance in a private subnet can access the internet, this can be achieved only when it can communicate to the internet. However, we do not want to make a subnet public as we want to maintain the degree of control. To overcome the problem, we need to create either NAT Gateways or NAT Instances.
* In real time, NAT Gateways are highly used than NAT instances as NAT instances are an individual EC2 instances, and NAT Gateways are highly available across multiple availability zones, and they are not on a single EC2 instance.

1. **What is Virtual Private Gateway?**

A virtual private gateway is a logical, fully redundant distributed edge routing function that sits at the edge of your VPC. As it is capable of terminating VPN connections from your on-prem or customer environments, the VPG is the VPN concentrator on the Amazon side of the Site-to-Site VPN connection.

1. **What is Customer Gateway?**

A customer gateway is a resource that you create in AWS that represents the customer gateway device in your on-premises network. When you create a customer gateway, you provide information about your device to AWS.

**11. What is AWS direct Connect ?**

* AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network solution from your premises to AWS.
* Using AWS Direct Connect, you can establish private connectivity between AWS and your datacenter, office environment, which can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.
* Direct Connect is a direct connection which is available on a dedicated line.

**12. What is Security Group?**

It adds a security layer to EC2 instances that control both inbound and outbound traffic at the instance level.

**13. What is Network ACL?**

* NACL stands for Network Access Control Lists.
* It is a security layer for your VPC that controls the traffic in and out of one or more subnets.
* It is an optional layer for your VPC.
* You can set up a Network ACL similar to the security group that adds an additional layer of security to your VPC.

1. **What is CIDR?**

Classless Inter-Domain Routing (CIDR) is a group of IP addresses that are allocated to the customer when they demand a fixed number of IP addresses.

In CIDR there is no wastage of IP addresses as compared to classful addressing because only the numbers of IP addresses that are demanded by the customer are allocated to the customer.

The group of IP addresses is called Block in Classless Inter - Domain (CIDR).

CIDR follows CIDR notation or Slash notation. The representation of CIDR notation is x.y.z.w /n the x.y.z.w is IP address and n is called mask or number of bits that are used in network id.