# AWS VPC

## VPC

* VPC is a virtual N/W
* Types:
  + Default VPC :
    - Should have default public subnet in each AZ.
    - Should have IG
    - For each instance should have Public & Private IPV4 addresss.
  + Non-Default VPC:
    - They are custom VPC
    - By default, if any instances falls into the non default VPC, non-default subnet, they only have private IPV4 address.
    - You need to specify “Assign Public IP address” at instance launch time to get the public IP.

## Subnet:

* Subnet is a range of ip-address in VPC
* Types
  + Public: Which have access to the internet.
    - AWS will check corresponding route table have attached with IG.
  + Private: Which don’t have access to the internet.
    - If you want to access outbound internet and restrict unsolicited access from internet , use NAT. But it only support IPV4 address.
    - For IPV6, you should use egress only gateway.

## Security

### Security Group

* A security group acts as a virtual firewall for your instance
* You can specify allow rules, but not deny rules.
* You can specify separate rules for inbound and outbound traffic.
* **By default, it denies all inbound and allows all outbound**
* For **Custom** security group**, it has no inbound rules** **and allows all outbound**
* Security groups are stateful
* Security groups are associated with network interfaces.
* Instances attached with **Default** **SG can talk** to each other but for custom S.G we have to add new Rules.

### NACL

* Acts as a firewall for controlling traffic in and out of one or more subnets.
* Your VPC automatically comes with a modifiable default network ACL.
* **By default, it allows all inbound and outbound** IPv4 traffic and, if applicable, IPv6 traffic.
* By default, each **custom network ACL denies all inbound and outbound** traffic until you add rules.
* Each subnet in your VPC must be associated with a network ACL
* A network ACL has separate inbound and outbound rules, and each rule can either allow or deny traffic.
* Network ACLs are stateless

## DNS

* Domain Name System (DNS) is a standard by which names used on the Internet are resolved to their corresponding IP addresses.
* it's composed of a host name and a domain name
* DNS servers resolve DNS hostnames to their corresponding IP addresses.
* Public IPv4 addresses enable communication over the Internet, while private IPv4 addresses enable communication within the network of the instance

## VPC Peering

* A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them privately.
* You can create a VPC peering connection between
  + Own VPCs
  + VPC in another AWS account
  + VPC in a different AWS Region.

## VPC PrivateLink

* Enables you to privately connect your vpc to following things:
  + AWS services
  + Aws services hosted by other AWS A/c (VPC endpoint services)
  + AWS Marketplace partner services.
* PrivateLink creates an ENI in the subnet with private IP address.

## VPC Endpoints

* A VPC endpoint allows you to securely connect your VPC to another service.
* PrivateLink is a highly available, scalable technology that enables private access to services.
* If any instance inside the private subnet wants to communicate with the S3 bucket, it needs to create an IAM role and communication goes through Nat gateway. But it will use public connection. So Is there any other mechanism to access Aws resources privately?? Now it’s time to learn VPC end points ☺
* Enables you to privately connect VPC to
  + AWS services
  + VPC end points.
  + Without requiring IG, NAT device, VPN Connection, AWS Direct Connection.
* Not require Public IP address.
* Types:
  + Interface Endpoints
    - An interface endpoint is powered by [PrivateLink](https://docs.aws.amazon.com/console/vpc/endpoints/privatelink" \t "_blank), and uses an elastic network interface (ENI) as an entry point for traffic destined to the service.
      * AWS Service
      * End-point Service
      * Market Place Service
    - Once Service, VPC and Subnet are selected, AWS will create an ENI inside this subnet.
    - To use private DNS names, ensure that the attributes 'Enable DNS hostnames' and 'Enable DNS Support' are set to 'true' for your VPC
    - Interface endpoint can be accessed through
      * AWS VPN connection
      * Direct Connect
      * VPC peering
    - While creating Interface Endpoints, you can choose only one subnet/AZ.
    - An interface endpoint supports TCP traffic and IPv4 address only.
  + Gateway Endpoints
    - A gateway endpoint serves as a target for a route in your route table for traffic destined for the service.

## VPC Endpoint Service

* You can create your own application in your VPC and configure it as an AWS PrivateLink-powered service (referred to as an *endpoint service*)
* We are using interface VPC endpoint

## ClassicLink

* Allows you to link classic-Ec2 instance to VPC.
* Steps
  + Must enable ClassicLink for VPC
  + Add Security Groups

## VPN

### Site-to-Site VPN

* Used to enable remote N/W access.
* Types:
  + AWS Classic VPN
  + AWS VPN
* Components:
  + Virtual Private Gateway: Will create two VPC end points to manage failover mechanism.
  + Customer Gateway:

### Client VPN

* Types of users interact with client VPN
  + Administrator: responsible to set-up this service.
  + Client: Will establish the connection to VPC endpoints.

### AWS VPN CloudHub

* Create a virtual private gateway with multiple customer gateways.

### Third Party Software VPN:

* Use Ec2 instance and run third party VPN appliances