VIRTUAL PRIVATE CLOUD

→ A virtual private cloud is a virtual Network that closely Resembles a ~~trans~~ traditional Networking that you Operate in your own ~~risk~~ data centre with the Benifits of using the scalable Infra-structure of AWS.

OR

VPC is a virtual Network or Datacentre inside AWS for one client.

→ It is logically isolated from other virtual Network in the AWS cloud.

→ Max. 5 VPC can be created and 200 subnets in 1 VPC.

→ we can allocate max. 5 elastic Ip.

→ Once we created a VPC, DHCP, NACL and security group will be automatically created.

→ A VPC is confined to on AWS Region and does not extend Between Regions.

DHCP → Dynamic Host configuration protocol
NACL → Network Access controll List.

→ Once the VPC is created, you cannot change its CIDR, Block Range.

→ If you need a different CIDR size, create a new vpc.

→ The different subnets within a vpc cannot overlap.

→ You can however expand your vpc CIDR By adding New/extra Ip address Ranges (except Govcloud & Aws china).

Component of vpc :-

CIDR & Ip Address, subnets.

→ Implied Router & Routing table

→ Internet Gateway

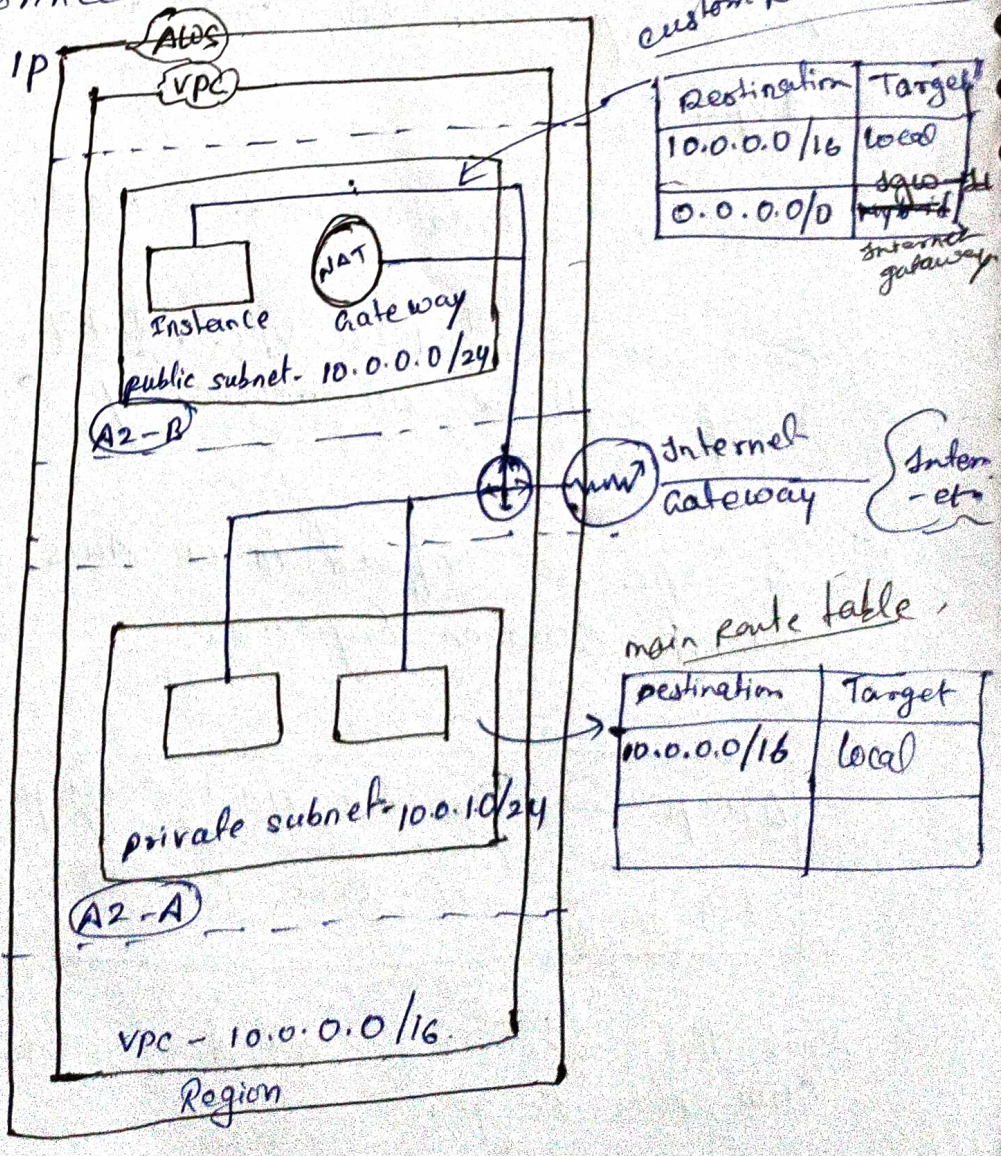
→ security groups

→ Network ACL

→ virtual private gateway

→ peering connections

→ Elastic Ip



VPC TYPES :→

* Default VPC :→

→ Created in each Region when an AWS Account is created.

→ Has default CIDR, security group, NACL and Route Table setting.

→ Has an Internet gateway by default.

* Custom VPC :→

→ It Is a vpc on AWS Account owner creates.

→ AWS user creation the custom vpc can decide the CIDR.

→ Has its own default Security group, Network ACL and Route Tables.

→ Does not have an Internet gateway by default, one need to be created if needed.

Public subnet :→ If a subnet's traffic is Routed to an Internet Gateway, the subnet is known as a ~~Route~~ public subnet. If you want your instance in a public subnet to communicate with the internet over Ipv4, it must have a public Ipv4 address or an elastic Ip address.

Private subnet :→ If a subnet does not have a route to the internet gateway, the subnet is known as a privat subnet.

VPC TYPES :→

* Default VPC :→

→ Created in each Region when an AWS Account is created.

→ Has default CIDR, security group, NACL and Route Table setting.

→ Has an Internet Gateway by default.

* Custom VPC :→

→ It Is a VPC on AWS Account owner creates.

→ AWS user creation the custom VPC can decide the CIDR.

→ Has its own default Security group, Network ACL and Route Tables.

→ Does not have an internet gateway by default; one need to be created if needed.

Public subnet :→ If a subnet's traffic is Routed to an Internet Gateway, the subnet is known as a ~~route~~ public subnet. If you want your instance in a public subnet to communicate with the internet over Ipv4, it must have a public Ipv4 address or an elastic Ip address.

Private subnet :→ If a subnet does not have a route to the internet gateway, the subnet is known as a privat subnet.

VPC TYPES :→

* Default VPC :→

→ Created in each Region when an AWS Account is created.

→ Has default CIDR, security group, NACL and Route Table setting.

→ Has an Internet Gateway by default.

* Custom VPC :→

→ It Is a VPC on AWS Account owner creates.

→ AWS user creation the custom VPC can decide the CIDR.

→ Has its own default Security group, Network ACL and Route Tables.

→ Does not have an internet gateway by default, one need to be created if needed.

public subnet :→ If a subnet's traffic is Routed to an Internet Gateway, the subnet is known as a ~~route~~ public subnet. If you want your instance in a public subnet to communicate with the internet over Ipv4, it must have a public Ipv4 address or an Elastic Ip address.

Private subnet :→ If a subnet does not have a route to the internet gateway, the subnet is known as a privat subnet.

→ when you create a vpc, you must specify an IPv4 CIDR block for the vpc. The allowed block size is between /16 to /28 netmask.

→ The first four & last Ip address of subnet cannot be assigned.

for eg:- 10.0.0.0/24.

10.0.0.0 → Network address.

10.0.0.1 → Reserved by AWS for the vpc Router.

10.0.0.2 → Reserved by AWS for the Ip address of DNS server.

10.0.0.3 → Reserved for future use.

10.0.0.255 → Broadcast address.

Note :→ AWS do not support broadcast in a vpc but reserved this address.

Implied Router & Routing Route Table :→

→ It is the central Routing function.

→ It connect the different AZ together and connects the ~~different~~ vpc to the Internet gateway.

→ you can have upto 200 Route table per vpc.

→ you can have upto 50 Route entries per Route Table.

→ Each subnet must ~~have~~ be associated with only one Route table at any given time.

→ If you do not specify a subnet to Route table association, the subnet will be associated with the default vpc Route table.

→ you can also edit the main Route table if you need, but you cannot delete main Route table.

→ However you can make a custom Route table manually become the main Route Table then you can delete the former main, as it is no longer a main Route table.

→ you can associate multiple subnets with the same Route table.

Internet gateway :→

→ An Internet gateway is a virtual Router that connects a vpc to the internet. ~~gateway~~

→ Default vpc is already attached with an internet gateway.

→ If you create a new vpc then you must attach the internet gateway in order to access the internet.

→ Ensure that your subnet's Route table points to the internet gateway.

→ It performs NAT between your private and public Ipv4 address.

→ Its support both Ipv4 & IPv6.

NAT Gateway :→

You can use a network address translation Gateway to enable instance in a private Subnet to the internet from initiating a connection with those instances.

→ You are charged for creating and using a NAT gateway in your account NAT gateway hourly usage and data processing rates apply Amazon Ec2 charges for data transfer also apply.

→ To create a NAT gateway, you must specify the public subnet in which the Nat gateway should Reside.

→ You must also specify an elastic address to associate with NAT gateway when you create it.

→ No need to assign public Ip address to your private instance.

→ After you have created a NAT gateway you must update the Route table associated with one or more of your private Subnet to point Internet Bound traffic to the NAT gateway.

This enables instance in you private Subnet to Communicate with the internet.

→ Deleting a NAT gateway, disassociates its elastic Ip address but doesn't release the address from your

account.

Security Groups

→ It is a virtual firewall works at ENI Level.

→ Upto 5 security group ~~can be applied~~ per ~~security~~ EC2 instance interface can be applied.

→ Can only have permit Rules, cannot have deny Role.

→ Stateful, Return traffic of allowed inbound traffic is allowed even if there are no rules to allow it.

Network ACL (Access control List)

→ It is a function performed on the implied Router.

→ NACL is an optional layer of security for VPC that acts as a firewall for controlling traffic in ~~and~~ and out of one or more subnets.

→ your vpc automatically comes with a modifiable default Network ACL By default, It allows all inbound & outbound IPv4 traffic and if applicable IPv6 traffic.

→ You can create a custom network, ACL and associate it with a subnet ~~by default~~
By default, each custom NACL denies all inbound & outbound traffic until you add rules.

→ Each subnet in your vpc must be associated with a NACL. ~~the~~ If you don't explicitly associate a subnet with a NACL, the subnet is automatically associated with the default NACL.

→ You can associate a NACL with multiple subnet, however a subnet can be associated with only one network ACL at a time. When you associate a Network ACL with a subnet, the previous association is Removed.

→ A NACL contains a numbered list of Rules that we evaluate in order, starting with the lowest numbered Rule.

→ The highest no. that you can use for a Rule is 32766. Recommended that you start by creating Rules with Rule numbers that a multiple of 100, so that you can insert new Rules where you need later.

→ It functions at the subnet level.

→ NAcl are stateless, outbonds traffic for an allowed inbound traffic, must be explicitly allowed too.

→ You can have permit and ~~deny~~ deny Rules in a NACL.

Security group	NACL
→ Operate at instance Level	→ Operate at the subnet level.
→ Support allows rules only	→ It permits allow as well as Deny Rules.
→ stateful, Return traffic is automatically allowed	→ stateless, Return traffic must be explicitly allowed by rules.
→ Applies to an instance only.	→ Applies to all instances in the subnet.

VPC PEERING :→

A vpc peering connection is a Networking connection between two vpc that enables you to route traffic b/w them using private IPv4 addresses or IPv6 addresses.

→ Instance in either vpc can communicate with each other as if they are within the same Network.

→ You can create a vpc peering connection between your own vpc or with a vpc in another Aws Account. The vpc can be in different Region.