VPC

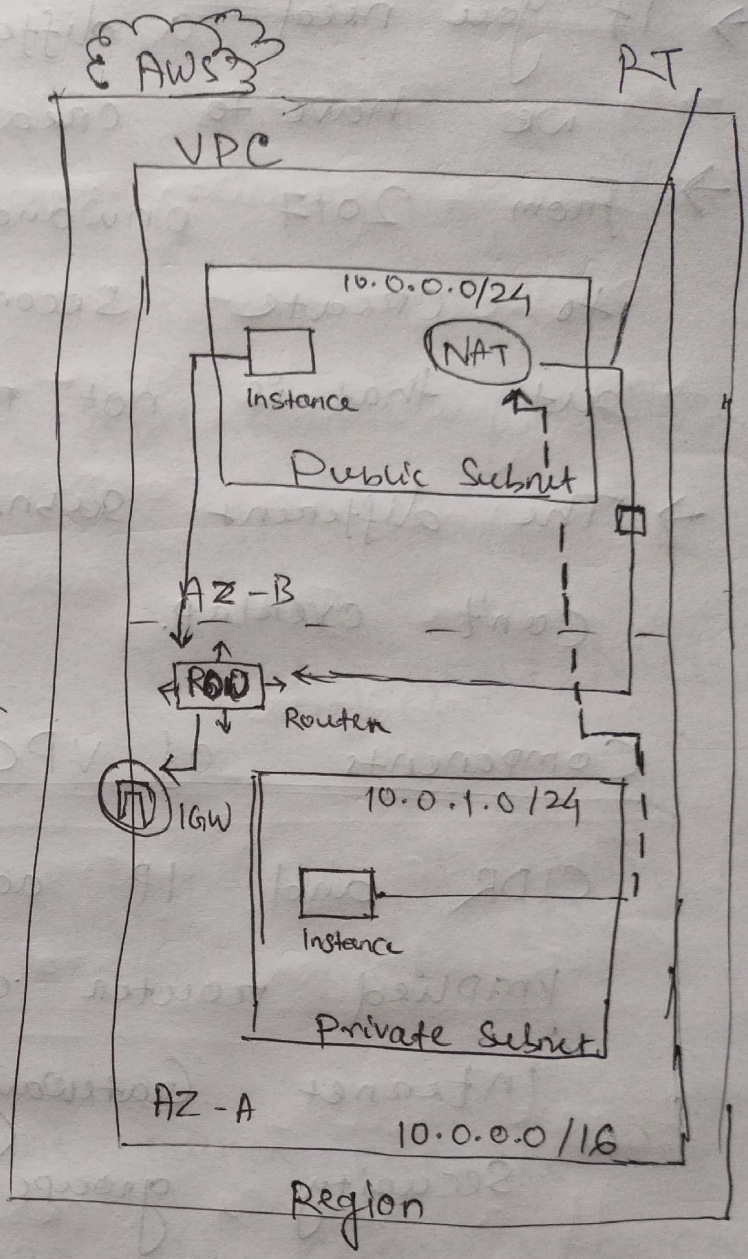
Virtual Private Cloud

A VPC is a virtual network inside AWS for one client.

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

→ Max 5 VPCs and 200 subnets in a VPC.

→ We can allocate max 5 elastic IPs



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

→ A VPC is confined to an AWS Region and doesnot extend between regions.

→ once the VPC is created, you can't change it's CIDR.

→ If you need a different CIDR -size, we have to create a new VPC.

→ From 2017 onwards we have the option to create secondary CIDR range. but that is not recommended.

→ The different subnets within a VPC can't overlap.

Components of VPC –

CIDR and IP address
Subnets
Implied router and Routing table
Internet Gateway
Security groups
NACL
Virtual private Gateway
Peering Connections
Elastic IPs.

VPC types

→ Default VPC

→ Custom VPC

Default VPC

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

→ It has default CIDR, security group, NACL and route table settings.

→ It has an Internet gateway by default.

Custom VPC

VPC on AWS account owner creates

→ AWS user creating the custom VPC can decide it's CIDR

→ It has it's own default security group, NACL and route table.

→ Doesn't have the IGW by default, one needs to be created if needed.

Public Subnet

→ If a subnet is traffic is routed to an Internet gateway, the subnet is known as Public Subnet.

→ If you want your instance in a public subnet to communicate with the internet over IPV4 address or an Elastic IP address.

> The starting 4 IPs and last IP is Reserved for internal purpose.

Private Subnet

If a subnet does not have a route to the internet gateway, the subnet is known as a private 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 and last IP address of subnet can't be assigned.

The starting 4 IPs and last IP is reserved for internal purpose.

e.g. 10.0.0.0/16

10.0.0.0 → Network address

10.0.0.1 → Reserved by AWS for the VPC router.

10.0.0.2 → Reserved by AWS 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 reserve this address.

Implied Router / Router

→ It is the central routing function

→ It connects the different AZ together and connects the VPC to the IGW.

→ You can have upto 200 route tables per VPC

→ You can have upto 50 routes Entries per route table.

→ Each subnet must be associated with only one route table at any given time.

→ If you don't specify a subnet to route table association, the subnet will be associated with the default VPC Route table.

→ You can also edit the main RT if you need, but you can't delete main RT.

→ 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 RT.

→ You can associate multiple subnets with the same route table.

Internet Gateway (IGW)

→ A Internet gateway is a virtual router that connects a VPC to the internet.

→ 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

→ It supports both IPV4 and IPV6.

NAT Gateway (Network Address Translation)

You can use a NAT gateway to enable instances in a private subnet to connect to the internet or other AWS services, but prevent 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~~ 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 IP 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 subnets to point internet bound traffic to the NAT gateway.

This enables instances in your private subnet to communicate with the internet.

→ Deleting a NAT gateway, dissassociates it's Elastic Ip address, but does not release the address from your account.

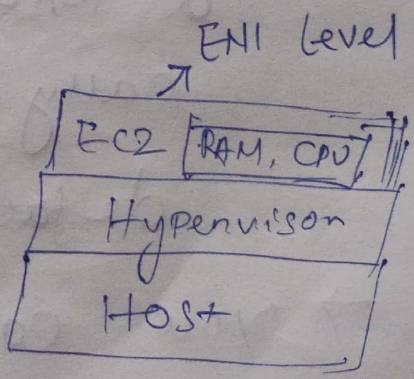
Security Groups

→ It is a virtual firewall works at ~~Subnet~~/Eni Level.

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

→ Can only have permit rules, can't have deny rules.

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



NACL [Network Accessed Control List]

→ It is a function performed on the implied router.

→ NACL is an optional layer of security for your VPC that act as a

firewall for controlling traffic in and out of one or more subnets.

→ Your VPC automatically comes with a modifiable default NACL - by-default it allows all inbound and outbound IPV4 traffic and if applicable IPV6 traffic.

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

→ Each subnet in your VPC must be associated with a NACL. 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 subnets, however a subnet can be

associated with only one NACL. at a time. When you associate a NACL with a subnet, the previous association is removed.

→ A ~~Ac~~ NACL contains a numbered list of rules that we evaluate in order, starting with the lowest numbered rule.

→ The highest number that you can use for a rule is 32766. Recommended that you start by creating rules with rule ~~Am~~ numbers that are multiple of 100, so that you can insert new rules where you need later.

→ It functions at the subnet level.

→ NACL are stateless, outbound traffic for an allowed inbound traffic, must be explicitly allowed ~~too~~.

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

VPC Peering

A VPC Peering connection is a networking connection between two VPC that enables you to route traffic between them using Private IPv4 addresses or IPv6 address.

→ Instances 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.