Amazon Virtual Private Cloud (Amazon VPC) enables you to launch AWS resources into a virtual network that you've defined and it is Amazon VPC is the networking layer for Amazon EC2.

The following are the key concepts for VPCs:

* **Virtual private cloud (VPC)** — A virtual network dedicated to your AWS account.
* **Subnet** — A range of IP addresses in your VPC.
* **Route table** — A set of rules, called routes, that are used to determine where network traffic is directed.
* **Internet gateway** — A gateway that you attach to your VPC to enable communication between resources in your VPC and the internet.
* **VPC endpoint** — Enables 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 IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network.
  1. ELASTIC IP ADDRESS:

Allocare new Address 🡪 need to associate Nate gate way to use

Subnet 🡪Ranger of IP address

Subnest Ranger 0 to 20 which provides 4096 address

(172.31.0.0/20,172.32.0.0/20)

* 1. Subnet to single availability zone

2 types private and public

Public connect to internet through route table

Private subnet no need of network

Creation

VPC dashboard🡪create Subnet 🡪

gave name ( US east-1-avialbe )

VPC name :select VPC

Avialblity zone: easet 1b,1c,1d,1e

CIDR block 10.0.1.0/24 (251 ranges) 🡪click create

* 1. Internet gate way:

To access internet integrate way (1 per pvc)

EC2 from internet

integrate way need to attach VPC

All instance in your subnets must have either a public ip addrss or Elastic IP

subnet rout table must point to internetgate way

and ALL SG groups should allow the required trafic

VPC 🡪internetgate ways 🡪create new interget gatreway

Name tag: aaaa 🡪create click

Once create 🡪 attach to VPC🡪

* 1. Route tables:

Network traffic direct 🡪

setsubnet 🡪one route table

routetable 🡪 subnet1 subnet2

VPC 🡪route table🡪create route table

Name of tag: \*\*\*\*

VPC :\*\*\*\*

Validate it in routes tab

Default of which is your CIDR range add another rout table

Desatination :0.0.0.0/0

Target :internet gate way name

And Save

Then go to the subnet Association 🡪 try to associate the subnet 🡪so it will be become public subnet

* 1. NAT

NAT device :🡪 allows you to enable to private subnets to connect internewt

Network address translation device 2m kinds of devices

1) NAT gate way (specific availability zone and it should lanched to public subnets)

2) NAT instance (ec2 instance under VPC).

Update ROUTE table private subnet so that it can connect to internet

VPC🡪NAT GATE WAY🡪New NAT gate wat

Subnet: create the subnet id private id

Elastic IP allocation ID: 🡪allocate if you already have else create new

Create new NAT gateway

🡪EDIT route table and 🡪go to the main route table🡪 edit🡪

Destination: 0.0.0.0/0

target is NAT id

* 1. SG

SG are state full and it will follow the inbound rules:

Inbound and outbound security groups

Type:

Protocol

Portrange

source

VPC🡪SG🡪

Name:

Group name

Description

VPC

Go to the inbound Rules and outbound rules and define

RDP 3389

* 1. Network ACL

It is optional Layer for VPC acts as firewall for controlling traffic in and out of one or more subnets

Between route table and subnets

Default NACLS all trafice.

Each subnet in your VPC must associated with an ACL ,if you wont define any new then it is defauls

A subnet can only associate to with one ACL and ACL can be associate to multiple ACL

Cotains lsit of numberd rules with are evaluated in order starting with lowest

ACLS are statless responses to allowed inbound traffic are subject to the rules for outbound trafice

VPC 🡪NACL

Create network ACL-🡪

Inbound Rules section

Roles#:100 ,\*

Types : all traffic

Protocol :All

Port Range: All

Destination :0.0.0.0/0

Allow/Deny :

Subnet Associations: associate to it

VPC Limits

5 VPCS per region

200 subnets per VPC

200 route tables per VPC

500 security groups per VPC

50 inbound out outbound rules per VPC