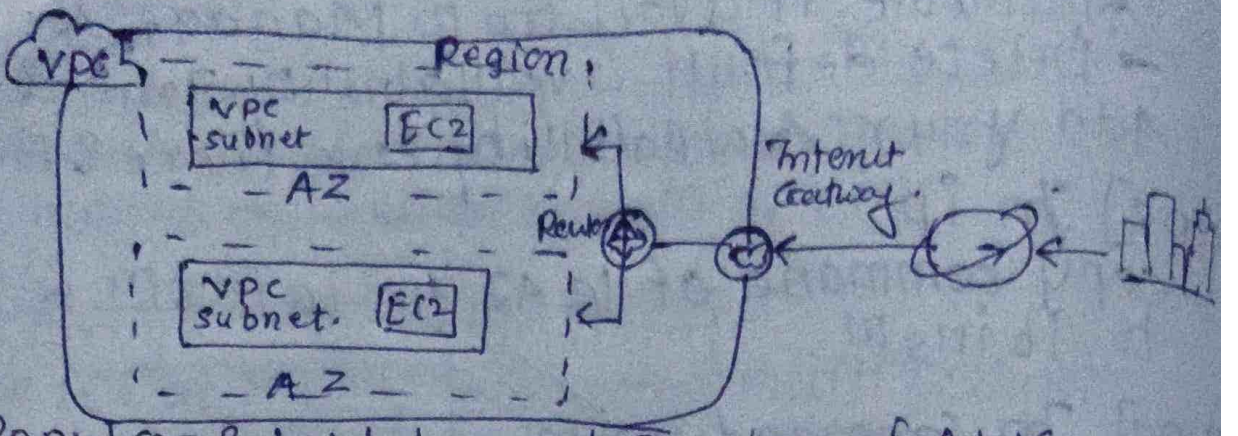
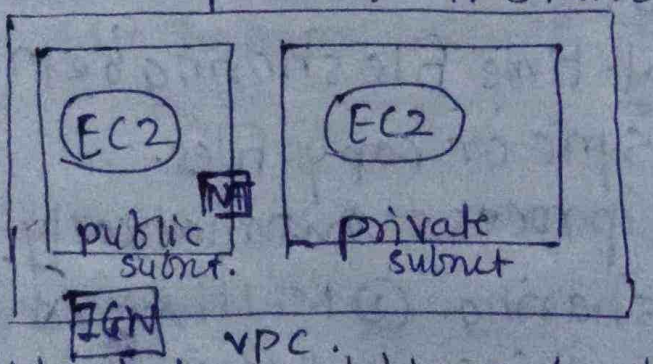
AWS VPC (Virtual Private Cloud).



Most Popular & Widely used services of AWS.
releated to security concepts in cloud & access to data inside third party data centre.
VPC is logically isolated network from another virtual network,
Max 5 VPC per region.
200 subnet per region.
It is used for balancing the traffic.
We can Access private instance from the public in



NAT is attach to public subnet & configure in privat
and Intenet gateway directly attach to the VPC.

Components of VPC:

① VPC: own isolated network in AWS.
② Subnet: small block inside VPC CIDR
two types: ① public: connect to Intenet gatew
② private: no intnt access
③ Intenet Gateway. All instn in public subnt to connect to intent must attach to VPC.
④ Route table: contain rules for directing network traffic. associate with subnt

⑤ NAT Gateway: private subnet instn access internet. outbound only.

⑥ Security Group Act as firewall for EC2 instn.

⑦ Network ACL Firewall for subnet.

⑧ DHCP opn set Manage domain name resolutn.

⑨ VPC peering connect two VPC so they can communicate privately.

Steps for Accessing Private instn within the public instn.

Step ① Make Outlayer.

Create VPC.

go to vpc only. (IPV4 CIDR manual i/p)

CIDR 192.168.1.0/24.

Create it.

Step ② Create Subnet.

for choose our VPC.

VPC name → public → subnet.

Availability zone 1a.

IPV4 CIDR 192.168.1.0/25.

Add new subnet:

create private subnet:

AZ 1b. CIDR: 192.168.1.128/25.

Create those subnet.

step ③. Make Internet Gateway.

Create → name → create.

Attach to VPC.

Go to Actn attach to VPC. Attach Intent.

step ④ NAT Gateway.

create → name → subnet (publicsubnet).

Allocate Elasticip.

step ⑤ Create Route table.

① public-rt

② private-rt.

Go to public → Routes → edit Routes Add.

Add Route 0.0.0.0/0. & Internet gateway.
Subnet Associat^n save. For private add NAT Gateway.

step ⑥. Make 2 Instance Public & Private.
imp role of key pair.
choose = our vpc.
subnet public.
select security group.
For private Instance.
Disable auto assign IP.
In Security Group. Must add All Traffic.

step ⑦. Open key file. & copy the content.

step ⑧ Goo to Public Instance & Run.
~~nano~~ make file same name as key name
nano stock.pem.
paste the content here.
give permission.
chmod 400 stock.pem.

step ⑨ In Private Instance go to SSH client.
copy example.
& paste it to the public Instance.

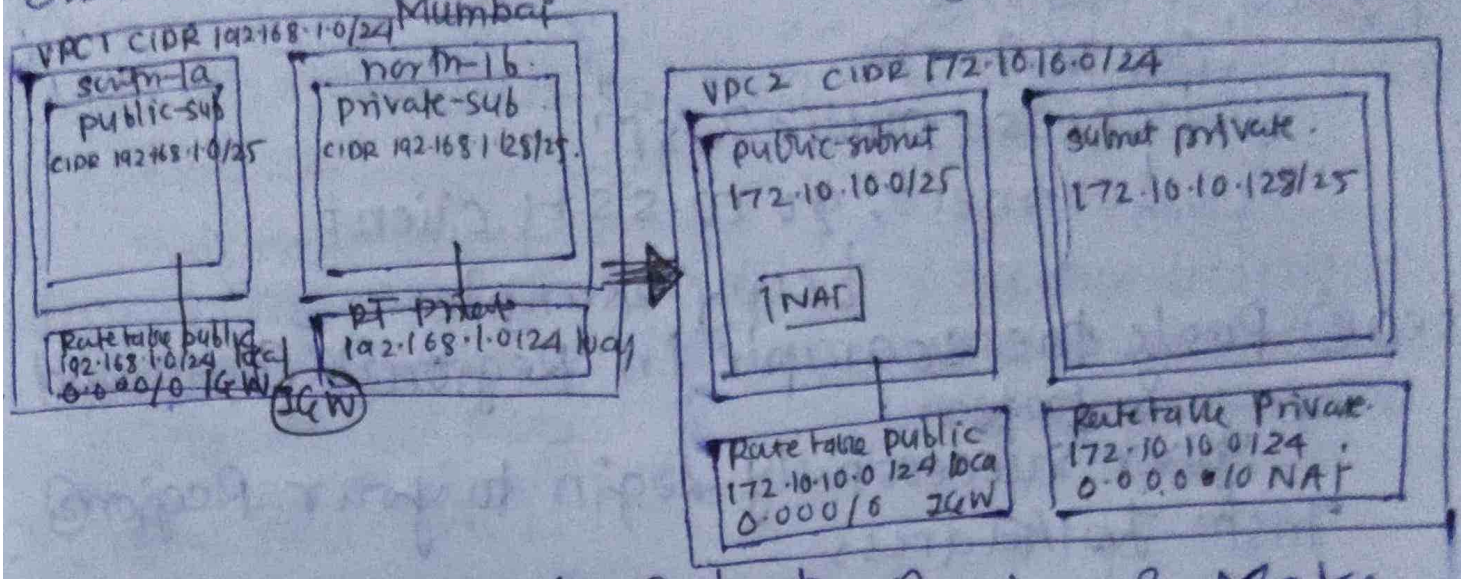
step ⑩ Check if ip change then it consider as you go in private Instance directly from public Inst^n.

step ⑪ Run.
ping IP_add.
If it run successfully it shows like.
process done good.

chmod 400 stock.pem.
ping public_IP.

VPC peering from One Region to Another Region.

CIDR : classless Inter Domain Range.



First Connect Instn of both Region & Make sure that you complete the Above process (~~Access~~ Make VPC & Instances in both diff Region).

step① In Region① go to peering connection.
- create peering connn
- name. - choose Requestor VPC.
- choose options
Apply Acceptor & VPC ~~Re~~ ID's (Region②)
& Create peering. (send Req to Region②)

step② In Region② Go peering connn & Accept the peering Request.

step③ In Region① Go to Route table.
Select public route table.
Edit Route
Apply the CIDR of VPC in it
choose peering connection. & save changes.

step④ In this Region① Go to EC2.
Connect public instn. ~~sudo -i, nano~~
sudo -i
nano (key name of Region②)
paste the content in this.

chmod 400 key.pem

step ⑤ Go to Region ②
L Go to Instn
L choose public Ip of Instn
L connect, go to SSH client
L copy example.

step ⑥ Paste the example in Region ② Command & Enter.
your successfully login to your Region ② Instn Ip Address.

step ⑦ Likewise you can access Region ② private Instance also.

To Ensure that process is done check Ip current old if change it done.

Likewise We can Access Another PC @ Instance on our Instn.

For that

step ① When you select peering connection in downword choose ~~another~~
→ Another account.
L Place account Id of that user.
L And Make sure that you select correct Region.

While writing Account Id don't use (-) It will gives you error.

step ② further processes are same.

In VPC.

↳ NACL (Network Access Control List).

this stateless firewall at subnet level in your VPC that controls inbound & outbound traffic.

NACL	Security Group
Subnet level	Instance level.
Separate Inbound & Outbound	one set for both dir.
Evaluate in order (low to high)	all rules evaluated.
Can Allow / Deny.	only support allow.

Creat new NACL.

step① Create new ACL
- fill details
  - Name:
  - VPC - select vpc.
- click to create network ACL.

step② Add Inbound & Outbound Rule.
* After creating NACL.

→ Inbound Rule:
- select your NACl
- Go to Inbound rule → edit inbound rule.
- Add Rules like
  - Rule 1 Allow TCP 22 SSH from 0.0.0.0/0.

save changes.

~~st~~ → outbound rules.
go to outbound → click edit.
- Add rules
  - rule 1 Allow TCP 80 HTTP 0.0.0.0/0.

step③ Associate Subnet with NACL
select NACL
Go to subnet association → edit subnet association.
choose subnet you want to apply NACL

Jai

Elastic IP

They are static, public IPv4 address provided by AWS you can allocate to your acc & assign to any EC2 ins

How to create Elastic IP

Go to EC2 dash.
left hand → click Elastic IP.
Allocate Elastic IP.
leave def setting or select.
Scope: Region
NBG: auto select.
click Allocate

- To associate with EC2.

① select newly create Elastic IP.
② Click Actn → Associate Elastic IP.
choose: Res type: Instn.
select Instn ID
click Associate

Now Normal IP assigned when you launch EC2 instn, AWS auto assign IPv4
→ subnet has Auto assign public IP" enabled
you choose Enable while lau

Elastic IP	Normal IP
Static	Dynamic
Remain same if we stop/start	change if we stop/strt.
Manually Assigned.	AWS assign auto.
eg long lived app, DNS mapping	eg. temporary test or setup.

Internet network of networks.

Internet Proto: criq no. assign to every device.

IPV4	IPV6
32 bit IP	128 bit IP
seprate by dot (.)	seprate by (:)
support broadcast	doesnt support broadcast.
12 header field	8 header field.

Classes of IP

class A	1.0.0.0	to 126.255.255.255
class B	128.0.0.0	to 191.255.255.255
class C	192.0.0.0	to 223.255.255.255
class D.	224.0.0.0	to 239.255.255.255
E	224.0.0.0	to 254.255.255.255

How IP Add. Provided

IANA Internet Assign no Authority.

→ RIR Regional Registry Internet.

→ ISP Internet servia provider.

Network ID Identify specific network on which device

Host ID Identify specific device on network. local

Broadcast IP: one to all