VPC & Networking

→ VPC is something you should know in depth for AWS certified Solutions Architech Associate & AWS certified sysOps Administrator.

→ At the AWS Certified Cloud Practitioner level, you know about:

① VPC, subnets. Internet Gateways & NAT gateways.

② Security Groups, N/w ACL (NACL), VPC flow logs

③ VPC Peering, VPC endpoints

④ site to site VPN & Direct Connect

⑤ Transit Gateway

1/2 questions are expected. in exam.

IP Address in AWS:-

IPV4 - Internet Protocol Version 4 (4.3 billion addresses)

+ Public IPV4 - can be used on the internet.

+ EC2 instance gets a new a public IP address every time you stop then start it (default).

+ Private IPV4 - can be used on private networks (LAN) such as internal AWS networking (e.g., 192.168.1.1)

+ Private IPV4 is fixed for EC2 instances even if you start/stop them.

⇒ Elastic IP - allows you to attach a fixed public IPV4 address to EC2 instance.

- Note - all public IPV4 on AWS will be charged $0.005 per hour (including EIP)
  - free tier: 750 hours usage per month.

→ free

° IPV6 - Internet Protocol Version 6 (3.4x10^{38} add)

- Every IP address is public in AWS (No private range)
- Example - 2001:db8:3333:4444:cccc:dddd:eeee:ffff

VPC & Subnets Primer:-

① VPC (Virtual Private Cloud): Private network to deploy your resources (regional resource)

② Subnets allows you to partition your n/w inside your VPC (Availability zone resource)

③ A Public subnet is a subnet that is accessible from the internet.

④ A Private subnet is a subnet that is not accessible from the internet

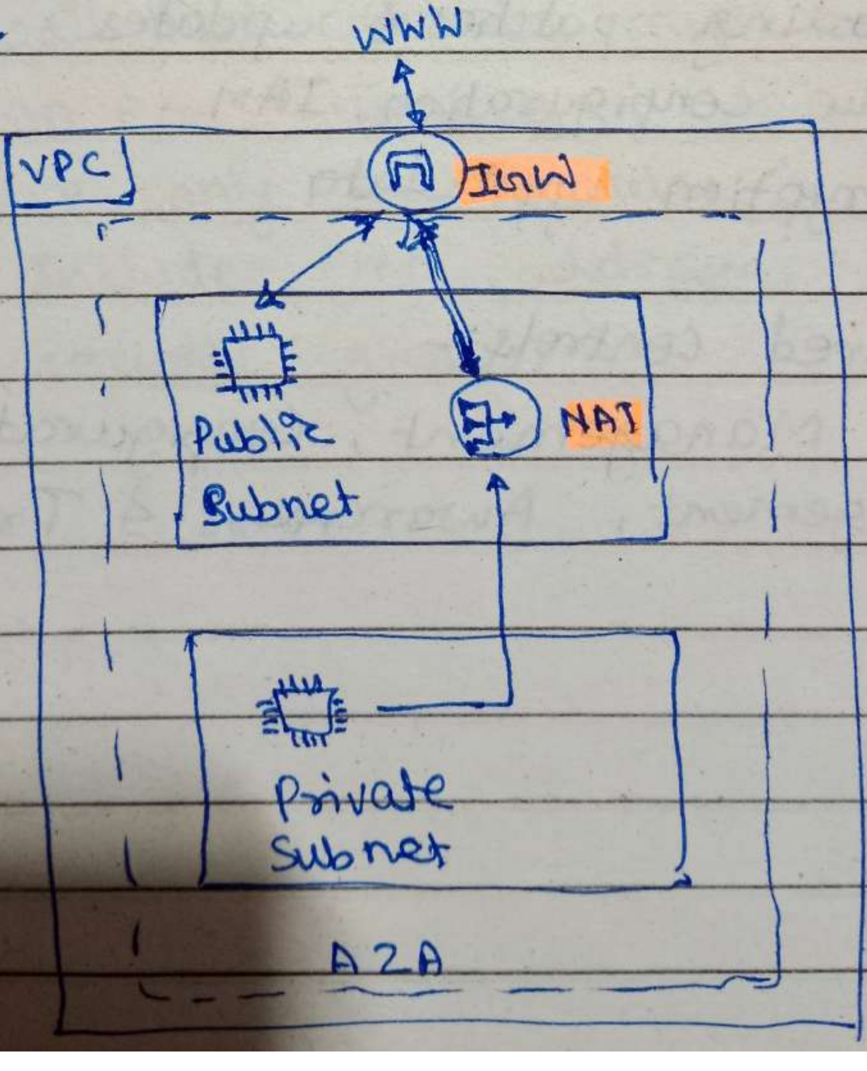
⑤ To depine access to the internet & between subnets, we use Route tables.

Internet Gateway & NAT Gateways

① Internet Gateways helps our VPC instances connect with the internet.

② Public subnets have a route to the internet gateway

③ NAT gateways (AWS - managed) & NAT instances (self-managed) allow your instance in your Private subnets to access the internet while remaining private



Network ACL & Security Group

① NACL (Network ACL) [Subnet Level]

+ A firewall which controls traffic from & to ~~to~~ subnet
+ Can have ALLOW and DENY rules
+ Are attached at the subnet level
+ Rules only include IP address.

② Security Groups :- [EC2 instance level]

+ A firewall that controls traffic to and from an EC2 Instance
+ Can have only ALLOW rules
+ Rules Includes IP addresses & other security groups.

VPC Flow Logs

① Capture info about IP traffic going into interfaces:
+ VPC flow Logs
+ Subnet flow Logs
+ Elastic N/w Interface flowLogs

② Helps to monitor & troubleshoot connectivity issues. Example:
+ subnet to internet
+ subnet to subnet
+ Internet to Subnet

③ Captures n/w information from AWS managed interfaces too: Elastic Load Balancers, Elastic Cache, RDS, Aurora, etc --

④ VPC flow logs data can go to S3, CloudWatch Logs, & Kinesis Data firehose

#VPC Peering:-

① Connect two VPC, privately using AWS n/w.

② Make them behave as if they were in the same n/w.

③ Must not have overlapping CIDR (IP address range)

④ VPC peering connection is not transitive (must be established for each VPC that need to communicate with one another).

[If VPC A and VPC B are connected with VPC Peering & VPC A is also connected with VPC C then VPC C & VPC B are not connected. If VPC B or VPC C wants to connect with each other then they have to create new connection using VPC peering.]

#VPC Endpoints :

① Endpoints allow you to connect to AWS services using a private ntw instead of the public www network.

② This gives you enhanced security & lower latency to access AWS services.

③ VPC Endpoint Gateway: to connect to S3 & DynamoDB

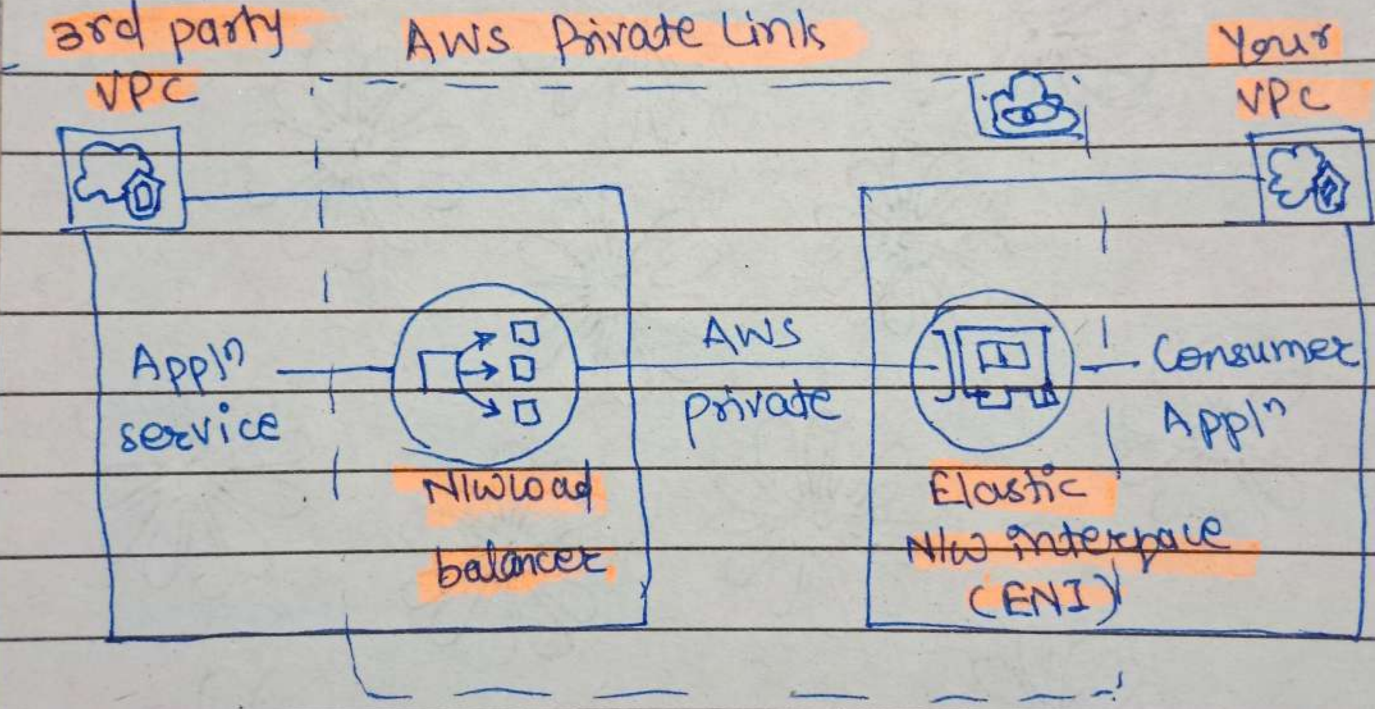
④ VPC Endpoint Interface : to connect with all other (Rest all services) ex:- Cloudwatch

#AWS Privatelinks (VPC Endpoint services)

① Most secure & scalable way to expose a service to 1000s to VPCs.

② Does not require VPC peering, internet gateway, NAT, route tables....

③ Requires a n/w load balancer (service VPC) & ENI (Customer VPC)



Site to Site ~~and~~ VPN & Direct Connect

- Site to Site VPN

① Connect an on-premises VPN to AWS.

② The connection is automatically encryp

③ Goes over the public internet.

- Direct Connect (DX)

① Establish a physical connection between on-premises & AWS.

② The connection is private, secure & fast.

③ Goes over the private n/w.

④ Takes at least a month to establish.

* Site to Site VPN

① On-premises: must be use a customer Gateway (CGW)

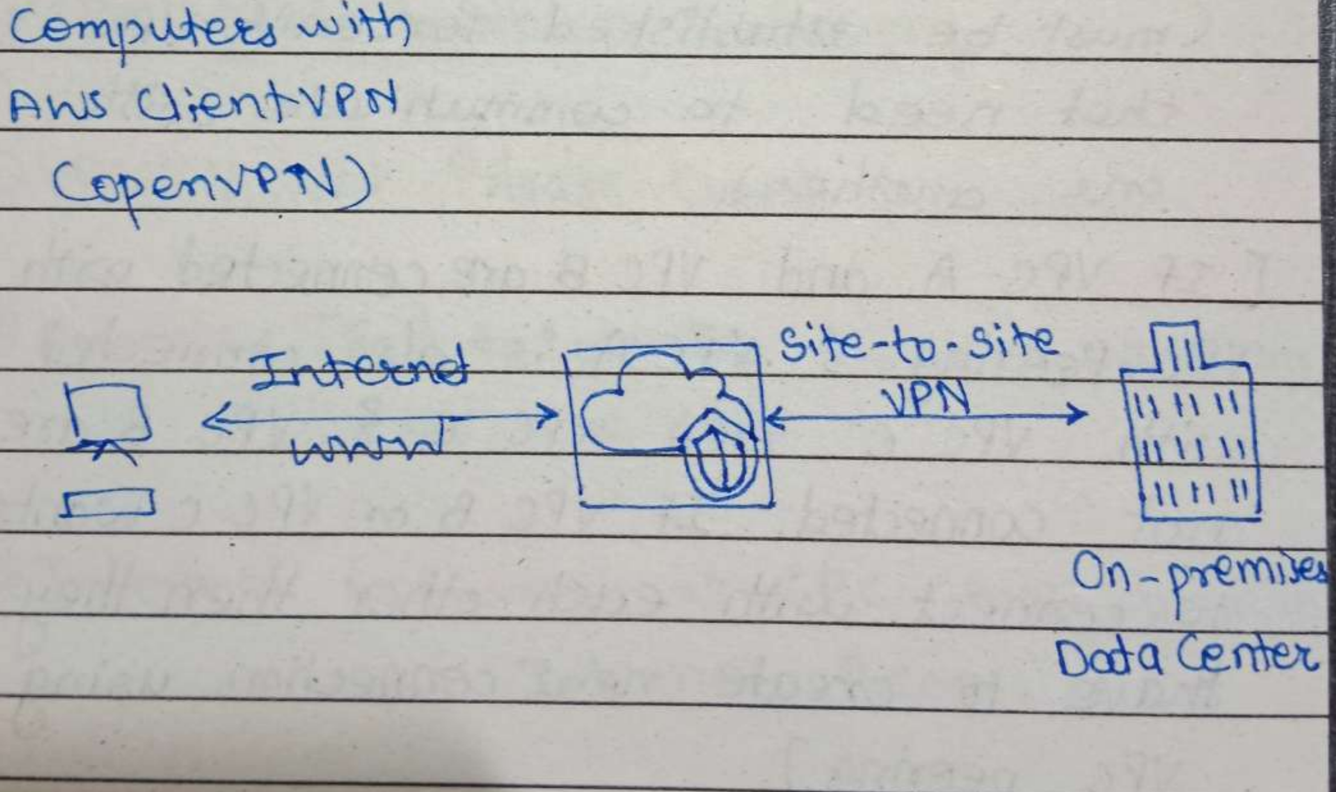
② on AWS side:- must use a Virtual Private Gateway ~~(VPG~~ (VGW)

AWS Client VPN :-

① Connect from your computer using openVPV to your private network in AWS & on-premises.

② Allow you to connect to your EC2 instance over a private IP (just as if you were in the private VPC network)

③ Goes over public Internet.



Transit Gateway :-

① for having transitive peering between thousands op VPC & on-premises; hub & spoke (star) connection

② One single gateway to provide this functionidity.

③ Works with Direct connect Gateway, VPN connections.

VPC & Networking Summary

① VPC : Virtual Private Cloud

② Subnets : Tied to an AZ, network partition op the VPC.

③ Internet Gateway : at VPC level, provide Internet Access

④ NAT Gateway/Instances : gives internet access to private subnets

⑤ NACL : Stateless , subnet rules ^for Inbound & Outbound.

⑥ security group : stateful, operate at the EC2 instance level or ENI

⑦ VPC Peering: Connect twoVPC with non-overlapping IP ranges, nontransitive

⑧ Elastic IP: fixed public IPV4, ongoing cost if not in-use.

⑨ VPC Endpoints: Provide private access to AWS Services within VPC

⑩ Private Link: Privately connect to a service in a 3rd party VPC

⑪ VPC Flow Logs: network traffic logs

⑫ site to Site VPN: VPN over public internet between on-premises DC & AWS.

⑬ Client VPN : Open VPN connection from your computer into your VPC

⑭ Direct Connect : direct private connection to AWS.

⑮ Transit Gateway : Connect thousands of VPC & on-premises networks together.