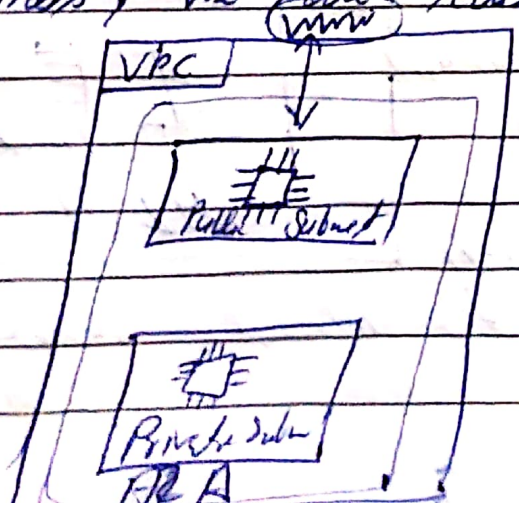
Day 23/100 Date → 30/12/2021

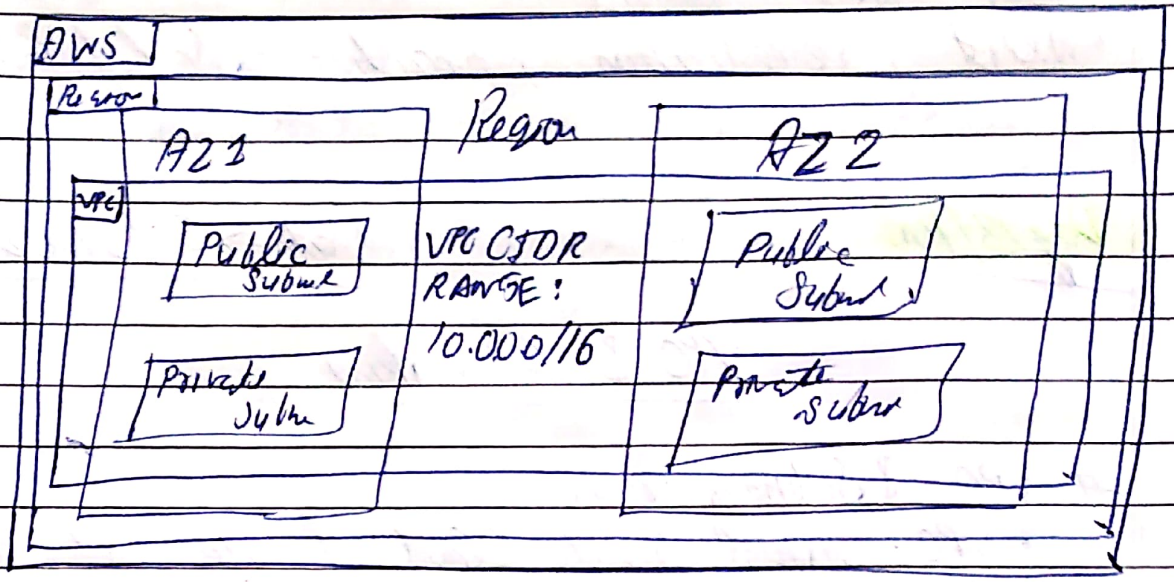
VPC & Networking

VPC & Subnets Primer

- VPC - Virtual Private Cloud: private network to deploy your resources [regional resource]
- Subnets - allow you to partition your network inside your VPC [AZ resource]
- A public subnet is a subnet that is accessible from the internet
- A private subnet is a subnet that is not accessible from the internet.
- To define access to your internet & b/w subnets, we use Route Tables

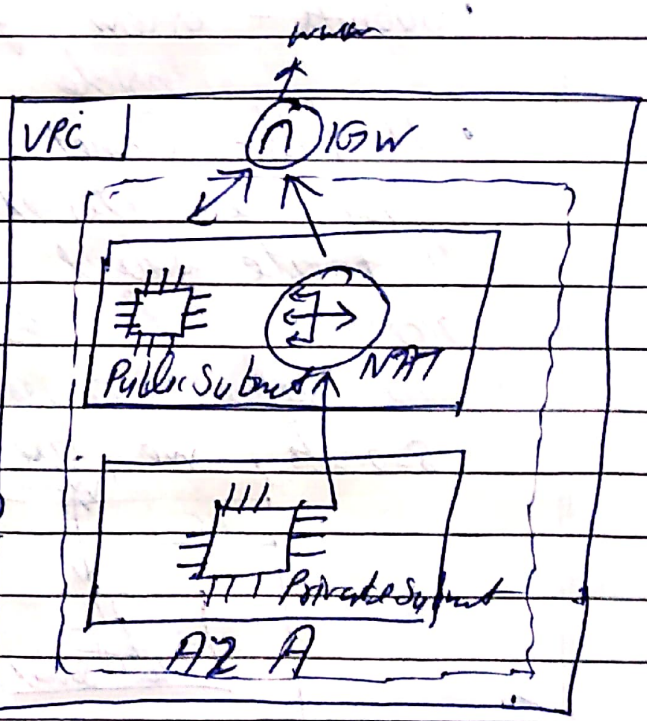


VPC Diagram →



Internet Gateway & NAT Gateways

- Internet Gateways helps our VPC instances connect with the internet
- Public Subnet have a route to the internet gateway
- NAT Gateways (AWS-managed) & NAT instance (self-managed) allow your instances in your Private Subnets to access the internet while remaining private

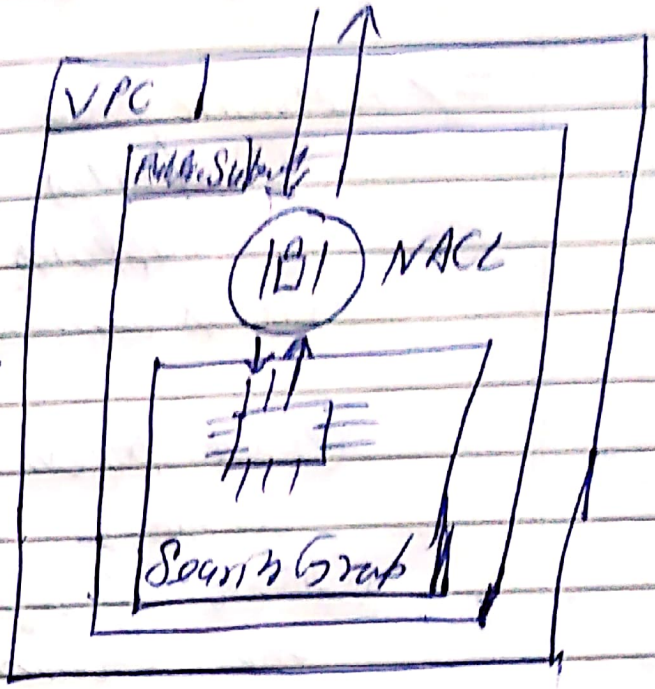


PAGE 1 | 8 | 21

DATE 30/10/21

Network ACL & Security Groups

- NACL (Network ACL)
  - A Firewall which Control traffic from and to Subnet.
  - Can have Allow and DENY rules
  - Are attached at the Subnet level
  - Rule only include IP addresses.



- Security Groups
  - A Firewall that Control traffic to and from an ENI / an EC2 instances
  - Can have only Allow rules.
  - Rules include IP addresses & other security groups.

⇒ Network ACLs vs Security Groups

- Security Group ⇒
  1. operates at the instances level
  2. Supports allow rules only
  3. Is Stateful: Return is automatically allowed regardless of your rules
  4. We evaluate all rules before deciding whether to allow traffic.
  5. Applies to an instance only if someone specifies the security group when launching the

instance, or associate the security group with the instance later on.

=> Network ACL

① Operates at the Subnet level
② Supports allow rules and deny rules
③ Is Stateless: Return traffic must be explicitly allow by rules
④ We process rules in number order when deciding whether to allow traffic.
⑤ Automatically applies to all instances in the Subnets it's associated with (therefore you don't have to rely on users to specify the security group).

VPC Flow Logs

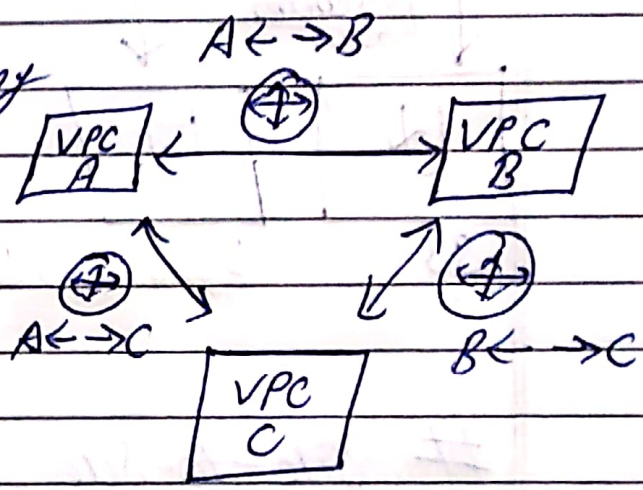
- Capture information about IP traffic going into your interfaces:
  - VPC Flow Logs.
  - Subnet Flow Logs.
  - Elastic Network Interface Flow Logs.

- Helps to monitor & troubleshoot connectivity issues. Example
  - Subnets to internet
  - Subnet to subnet
  - Internet to subnet

- Captures network information from AWS managed interfaces too: Elastic Load Balancers, ElastiCache RDS, Aurora etc---
- VPC Flow logs data can go to S3/CloudWatch Logs.

VPC Peering

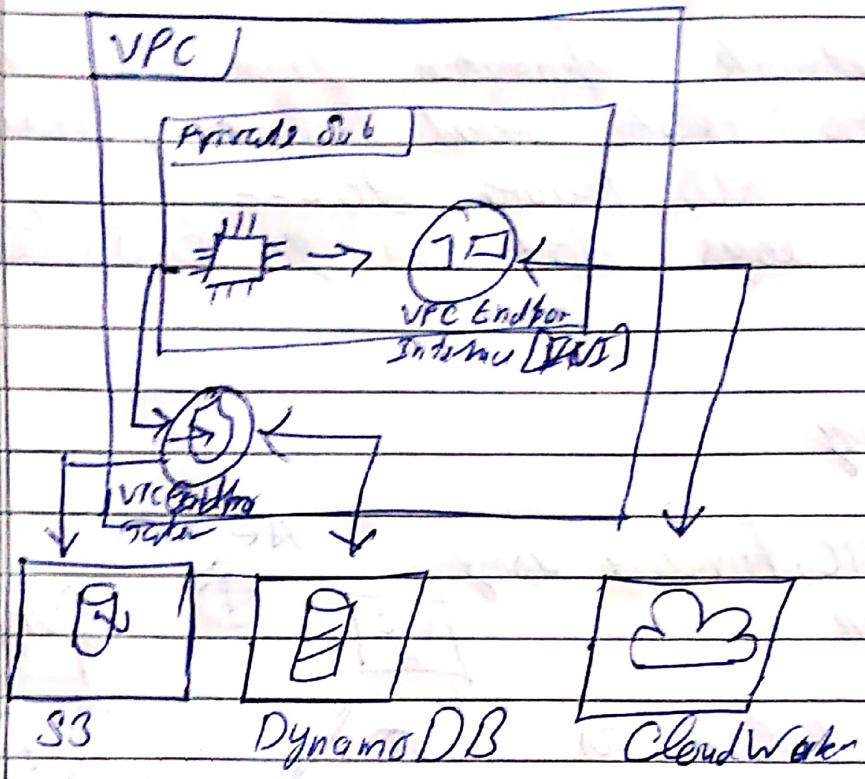
- Connect two VPC, privately using AWS network
- Make them behave as if they were in the same network.
- Must not have overlapping CIDR (IP address range)
- VPC Peering Connection is not transitive (must be established for each VPC that need to communicated with one another.



VPC Endpoint.

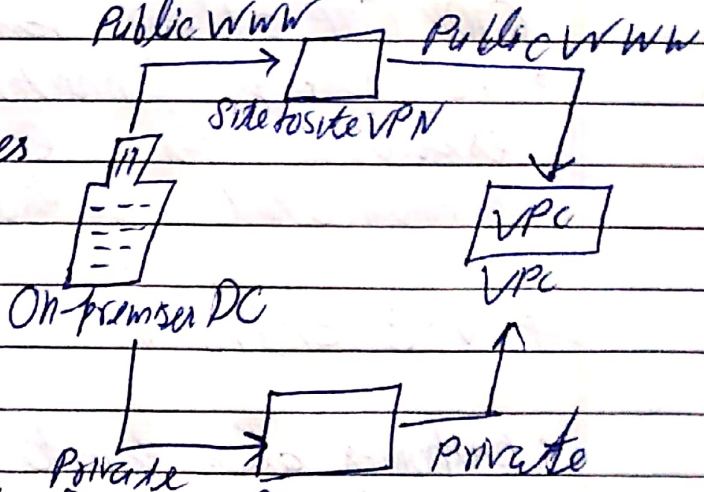
- Endpoints allow you to connect to AWS Services using a private network instead of the public internet
- This gives you enhanced security & lower latency to access AWS services
- VPC Endpoint Gateway: S3 & DynamoDB.
- VPC Endpoint Interface: the rest

PAGE 101 DATE 30/12/21

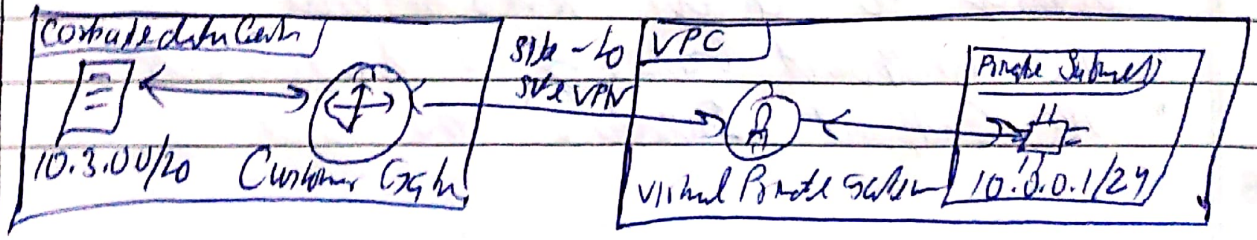


Site-to-Site VPN & Direct Connect

- Site to Site VPN
  - Connect an on-premises VPN to AWS
  - The Connection is automatically
  - Goes Over the Public Subnet



- On premises: must use Customer Gateway [CGW]
- AWS: must use a Virtual Private Gateway [VPG]



EKS

DATE 30/12/21

- Direct Connect (DX)
  - Establish a physical Connection b/w On-premises & AWS
  - The Connection is private, secure & fast
  - Goes over a private network
  - Takes at least month to establish

Transit Gateway

- For having transitive peering b/w thousands of VPC and on-premises, hub & spoke (star) Connection
- One single Gateway to provide this functionality
- Works with direct Connect Gateway, VPN Connections