e performance and
rvices underlying
ation.

irectly impact you
e, scheduled

nce of AWS
, perform EC2
metric.
2 instances,

nts in AWS,

le within

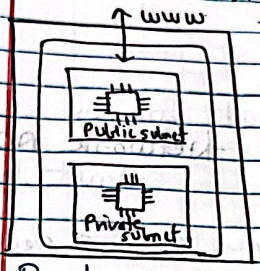
nalysis of

ough your

application performance recommendations.

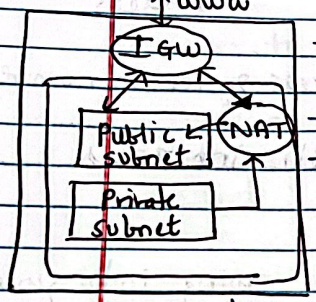
→ VPC (Virtual Private Cloud).

→ VPC & Subnets Primer



- VPC: Private network to deploy your resources.
- Subnets: Partition network inside VPC
- Public subnet: Accessible from the internet
- Private subnet: Not accessible from the internet

– Route Table - Access to the internet and between subnets



- Internet Gateways helps VPC instances connect with the Internet
- Public Subnets have route to IGW.
- NAT Gateways (AWS-managed) & NAT Instances (self-managed) allow your instances in your Private Subnets to access the internet while remaining private.

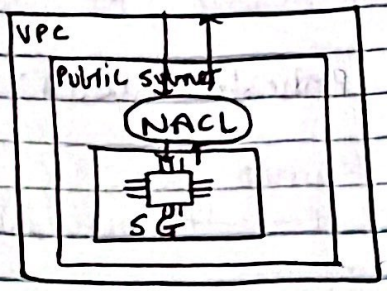
→ Network ACL & Security Group

1) Network (NACL):
– Firewall which controls traffic from and to subnet
– Can have Allow and Deny rules.
– Are attached at the Subnet level
– Rules only include IP addresses.

2)

Security Groups:
A firewall that controls traffic to and from an ENI / an EC2 instance

- Only ALLOW rules
- IP addresses, other security groups.



→ Network ACLs vs Security Groups.

	Security Group	Network ACL
Instance level	Instance level	Subnet level
Allow rules	Allow rules	Allow & Deny
Stateful	Stateful	Stateless
Evaluate	all rules	Process rules in numbers
Instance	specific	All instances

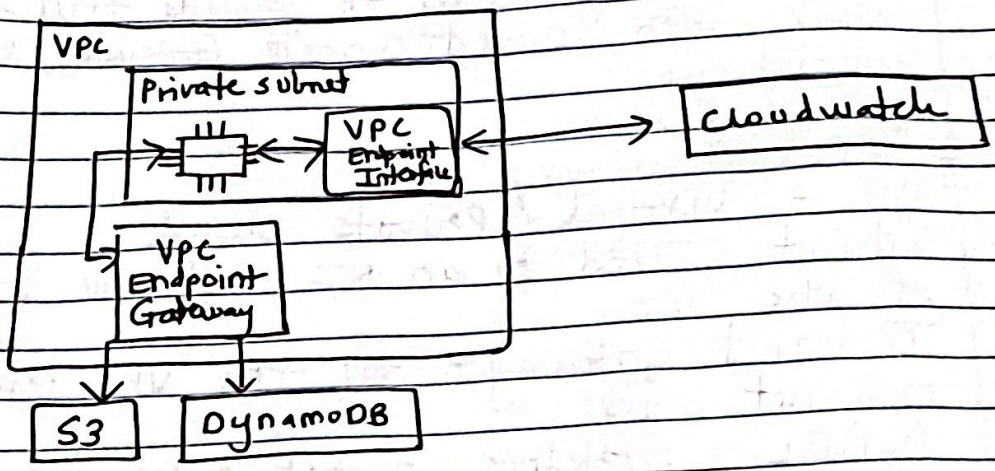
→ VPC Flow logs
- Capture info about IP traffic going into your interface: VPC, subnet, ENI flowlogs
- Helps to monitor & troubleshoot connectivity
- Captures network info from AWS managed interfaces.
- Can go to S3 / CloudWatch logs.

→ VPC Peering:
- Connect two VPC, privately using AWS network

- Must not have overlapping CIDR
- Not transitive.

→ VPC Endpoints

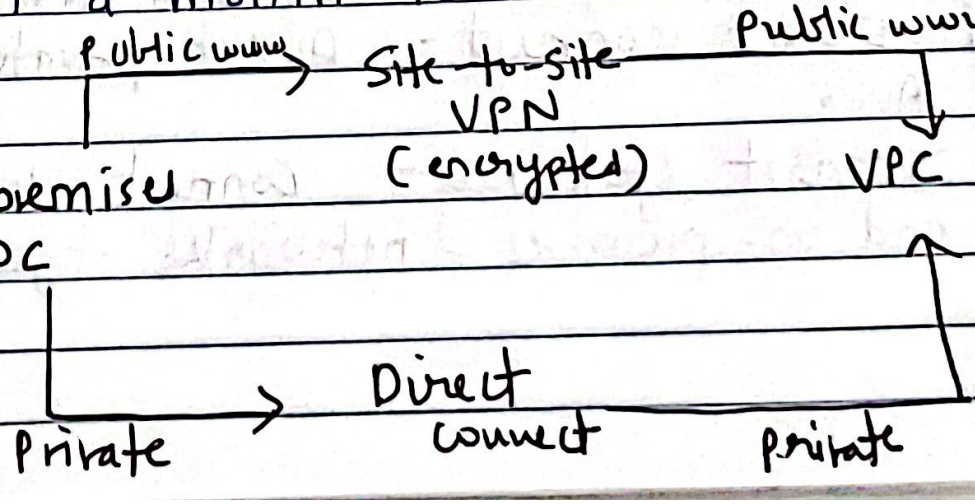
- Connect to AWS services using a private network.
- Enhanced security and lower latency to access AWS services
- VPC Endpoint Gateway: S3 & DynamoDB
- VPC Endpoint Interface: the rest



→ Site-to-site & Direct Connect.

1) Site-to-site.
- On premise VPN to AWS
- Automatically encrypted
- Goes over the public internet.

2) Direct Connect (DX).
- Physical connection between on-premises and
- Private, secure, fast
- Goes over the private network
- Atleast a month to establish.



Site-to-site VPN:
On premises: must we a customer Gateway (CGW)
AWS: must we a virtual private Gateway (VGW)

Transit Gateway:
For having transitive peering between thousands of VPC and on-premises, hub-and-spoke (star) connection.
One single gateway to provide this functionality.
Works with Direct Connect Gateway, VPN connections.

* VPC Summary *
VPC - Virtual Private cloud.
Subnets - Tied to an AZ, network partition of the VPC.
Internet Gateway - At the VPC level, provide Internet access.
NACL - Stateless, subnet rules for inbound and outbound
Security Groups - Stateful, operate at the EC2 instance level or ENI.
VPC Peering - Connect two VPC with non-overlapping IP ranges, nontransitive.
VPC Endpoints - Provide private access to AWS services within VPC.
VPC flow logs - Network Traffic logs.
Site-to-site VPN - VPN over public internet between on-premises DC and AWS.
Direct connect - Direct private connection to AWS.
Transit Gateway - Connect thousands of VPC and on-premises networks together.