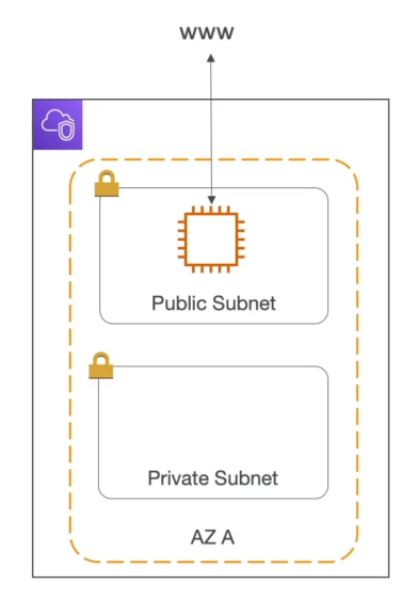
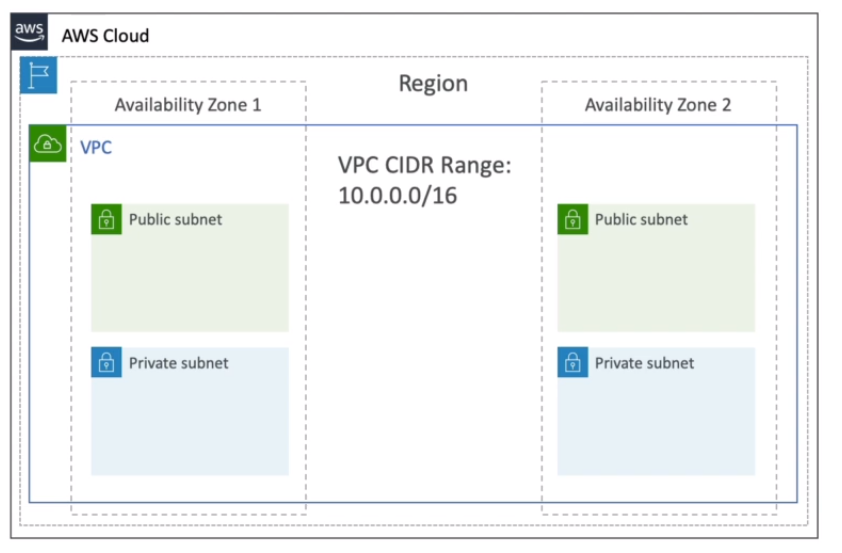
**Amazon VPC**

* VPC
* Subnets
* Internet gateway
* NAT Gateway
* Security Group
* Network ACL
* VPC FLow logs
* VPC peering
* VPC Endpoints
* Site to site VPN
* Direct Connect

**VPC and subnets Primer**

* VPC - virtual private cloud
* Deploy resources on VPC
* Subnets used to partition VPC
  + Public subnet - access from internet
  + Private subnet - cannot access from internet
* **Route table -** defines access to internet and between subnet





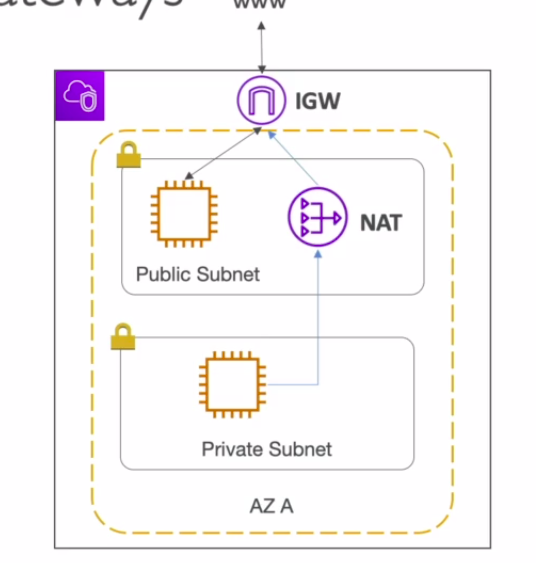
**Vopc that is created for you has only public subnets (one per az)**

**Internet gateway**

* Connects VPC instances to the internet.
* Internet gateway know how to connect to the internet, and public subnet knows how to connect to the internet gateway

**NAT Gateway**

* Used for only one way traffic to the internet. EC2 instance in private subnet can access the internet but the ec2 instance will not be accessible from the internet.

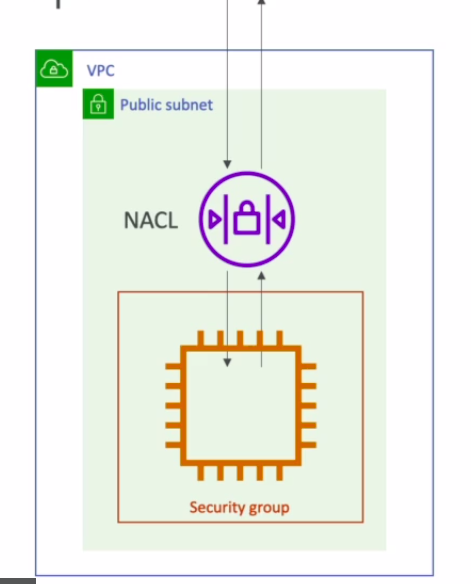


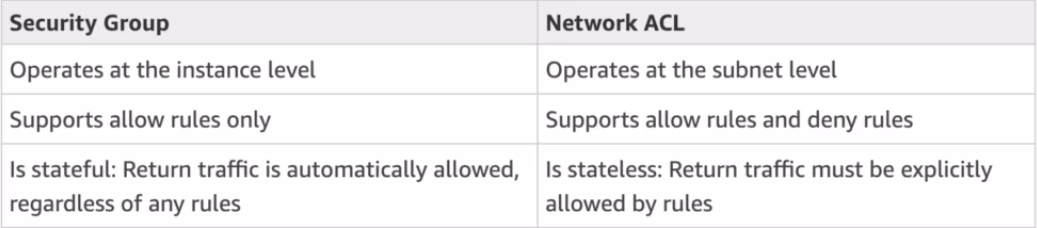
**Network ACL(NACL)**

* Firewall that controls traffic from and to **subnet**
* Has allow and deny rules
* Attached at subnet level
* Rules include only ip address
* Default NACL allows everything in and out of the subnet

**Security Group**

* FIrewall that controls traffic from and to **ENI(SSL certificate manager)/ EC2 instances**
* Only has allow rules
* Rules include ip address and other security groups





**VPC flow logs**

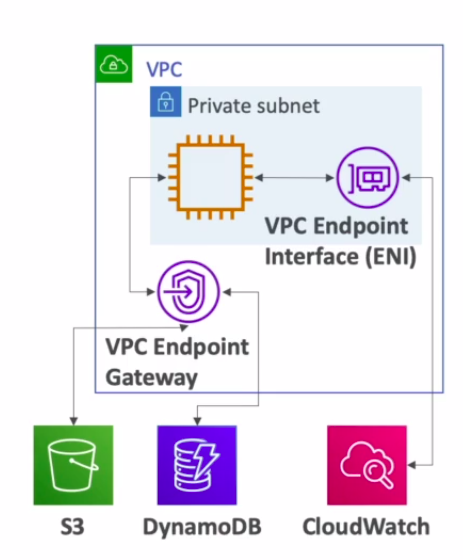
* Info about traffic going into your interfaces
  + VPC flow logs
  + Subnet flow logs
  + ENI flow logs
  + ELB,Elasticache,RDS,Aurora.
* Helps monitor and troubleshoot connectivity issues.
  + Subnets to internet
  + Subnets to subnets
  + Internet to subnets
* Log data can be stored into s3 or cloudwatch logs

**VPC peering**

* **Privately** connect two VPC’s
* Makes the two vpc’s behave as if they were from the same network
* Must not have overlapping IP ranges
* Connection not transitive. (A connected to B, B connected to C, does not mean A is connected to C, new vpc peering connection must be established

**VPC Endpoints**

* Endpoints allow you to connect to AWS services from private network instead of the internet (security and speed increased)
* VPC endpoint gateway: s3 and dynamodb
* Vpc endpoint interface: rest of the service



**To** Connect an on-premise VPN to AWS:-

**1)Site to site VPN**

* Automatically encrypted
* Goes over public internet

**2)Direct connect (DX)**

* Connection is private, secure and fast
* Private network
* Takes at least a month to establish

***Site to site VPN and direct connect cannot access VPC endpoint***