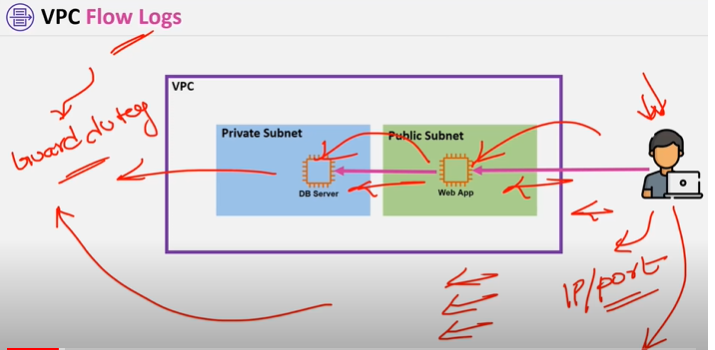
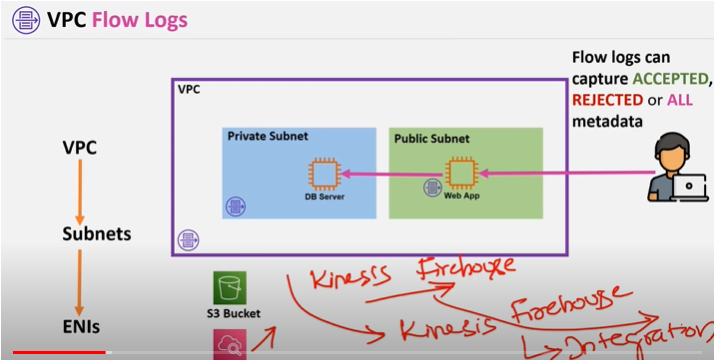
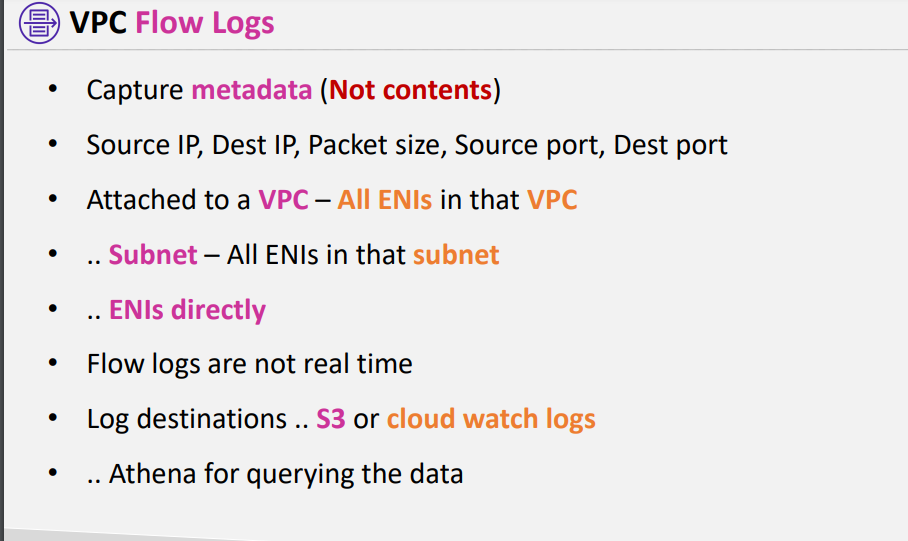
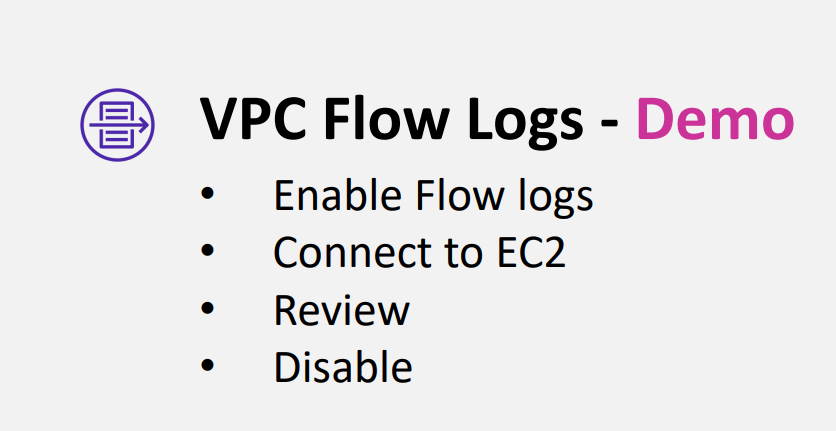


We can store logs to vpc level or subnet level or Eni’s level

Logs will be either stored in s3 or cloud watch logs

* Logs are nothing but the traffic or requests which wants to connect to thevpc
* For big projects will enble vc flow logs for more security
* 
* Guard duty will analyse the logs who is requesting on which port
* Guard duty will analyse the malware ip’s
* Kinesis fire house is also a service to store the logs
* Kinesis fire house is only pushes the logs
* If we want to integrate these logs with 3rd party tools there wont be any integration directly to aws
* So kinesis firewall helps in integrating
* 
* 
* 

Demo

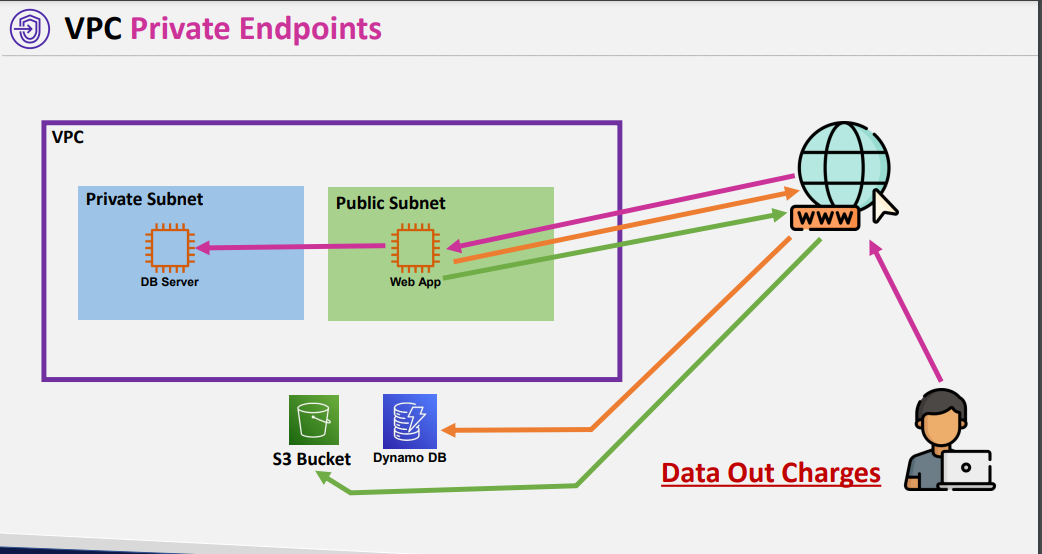
Create flowlog under vpc and create role

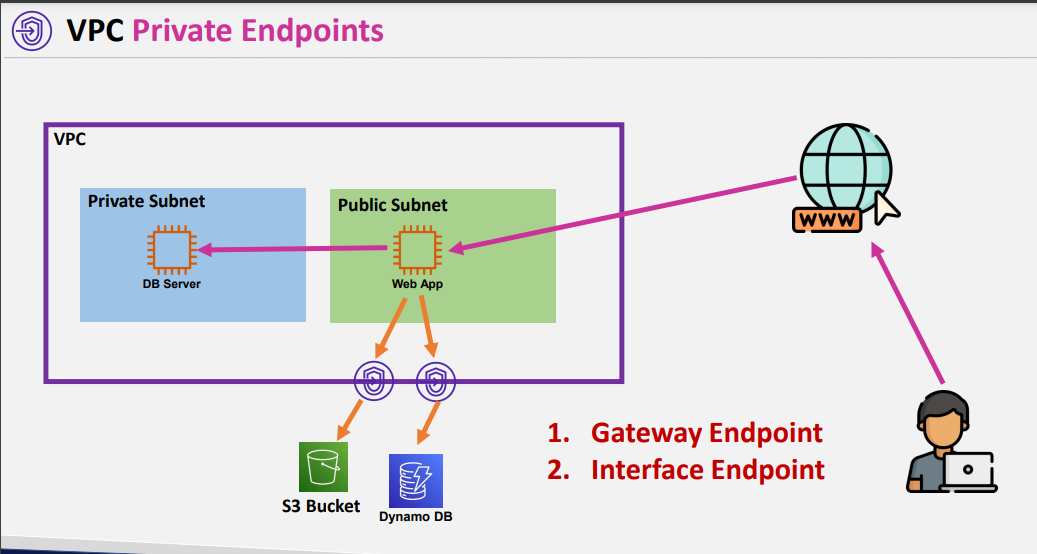
2. create ec2 instance and install apache tomcat yum install httpd -y

Cd var/www/html

Service httpd start

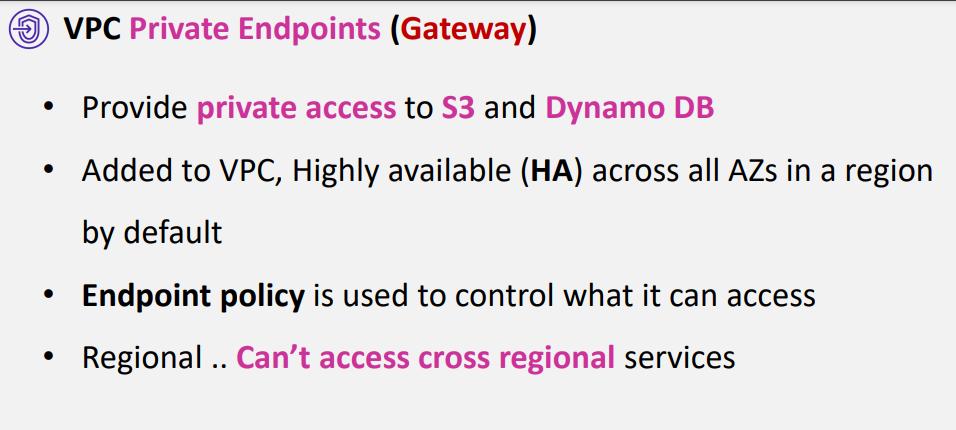
Iplookup site



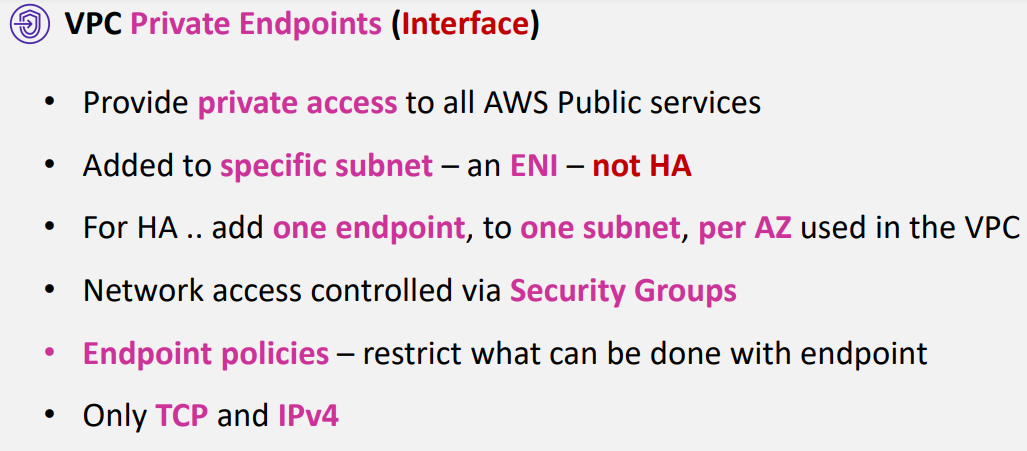


Advantage

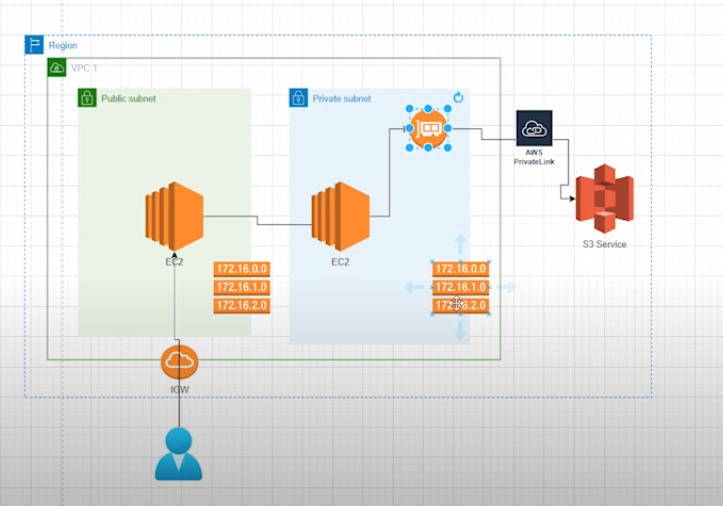
1. Your traffic wont be into the internet
2. And data out charges wont be there



Aws recently added s3 interface end point



demo



CREATE VPC

2 SERVERS 1) PUBLIC 2)PR

aws s3 ls --endpoint-url <https://bucket.vpce-00071a3cd47209efc-gv4vwcun.s3.ap-south-1.vpce.amazonaws.com> (endpointDNS) --region ap-south-1

aws s3 ls S3://BUCKETNAME --endpoint-url <https://bucket.vpce-00071a3cd47209efc-gv4vwcun.s3.ap-south-1.vpce.amazonaws.com> (endpointDNS) --region ap-south-1 (To acess bucket)

