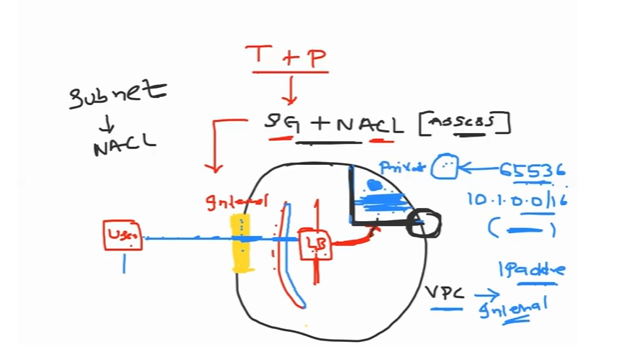
Without vpc, it is impossible to provide security in AWS as good…

Vpc introduces private cloud in the field of public cloud..

Subnet: when we define a vpc, we need to define a ip range ….means what is the size of vpc



When any user wants to access this internet gateway…user eventually goes into this internet gateway ..within this public subnet… DevOps engineer usually place a load balancer…Load balancer can be accessed by the outside world ..This load balancer will take to this private subnet…load balancer is the one ..it has access to private subnet ..and this user has the access the load balancer ..within the load balancer also we can do lot of configurations…we can more secure with load balancer..

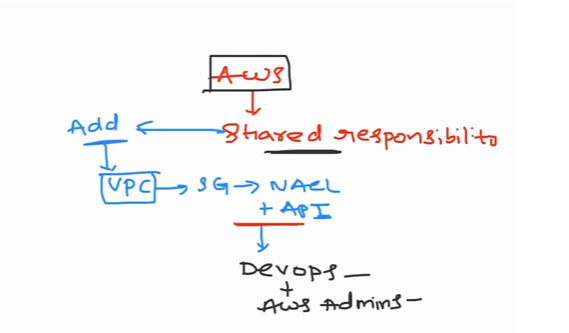
As a devops engineer or application owner we can add more security at ec2 instance

We can add additional security at the layer at the subnet..

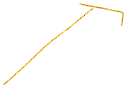
Technically we can use 65536 components in that particular vpc…

In aws we can add security at multiple levels

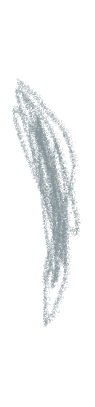
In aws, security is always a shared responsibility

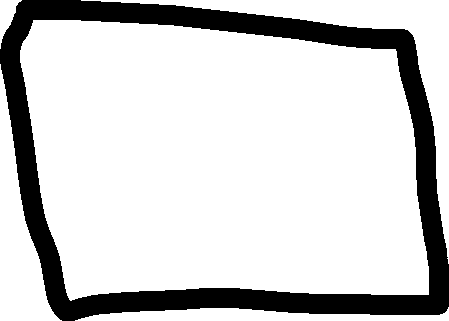
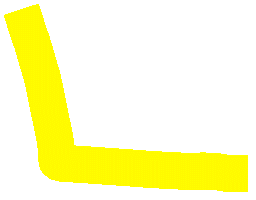


AWS says that we can add more security at subnet level…









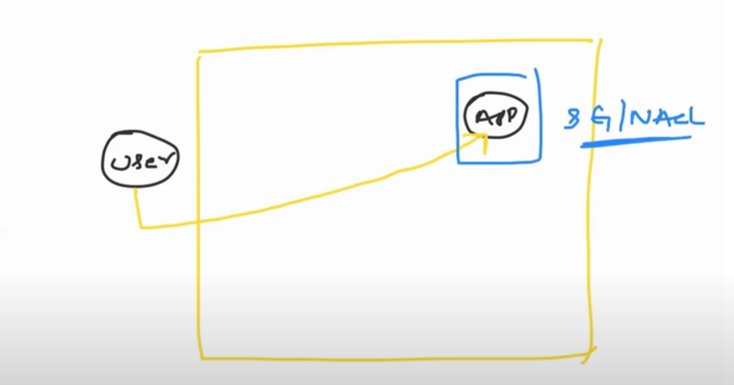
IP ADDRESS RANGE means how many ip addresses you want in this vpc

Anyone can access public subnet

At the EC2 level, if we add security then it is called security groups.

Using security groups, we can add more security to the EC2 level.

If we want more security at the subnet level, then we use NACL (Network Access



A security group is used at the instance level