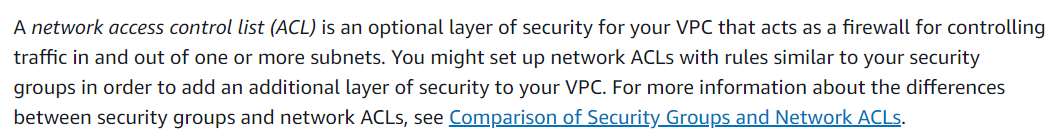
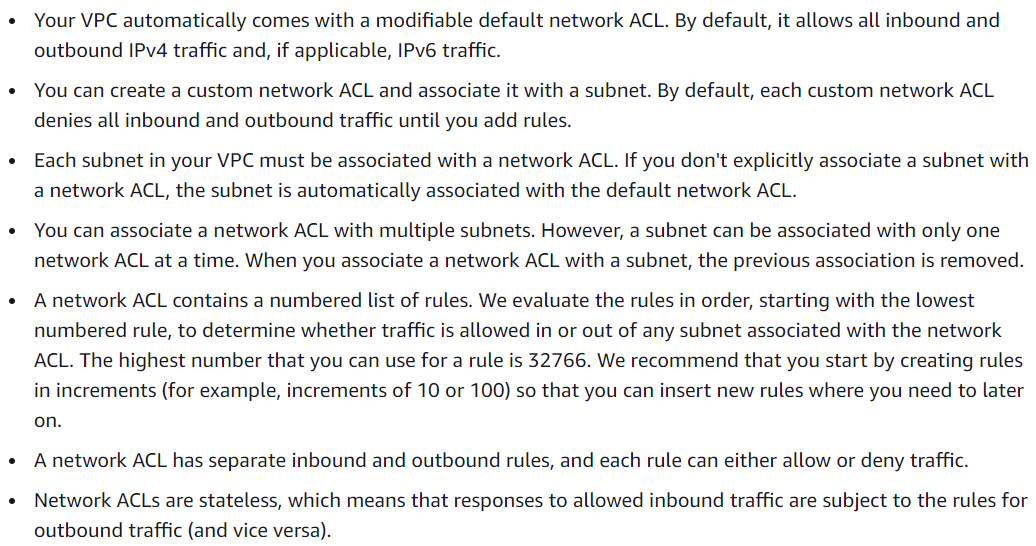
**Firewall:**

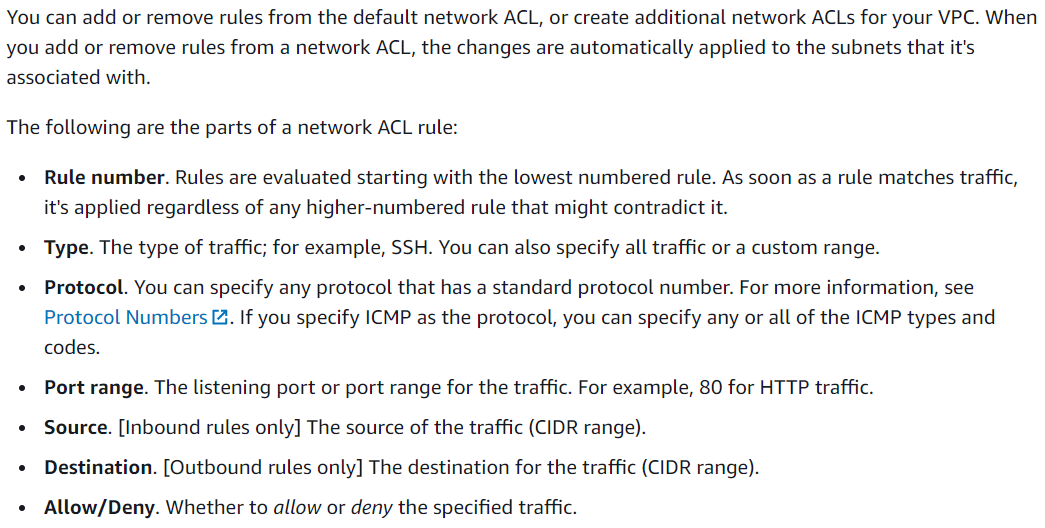
* The traffic comes and goes through the firewall and if any unwanted comes in then firewall will avoid it

**Introduction: (Network Access Control Lists)**





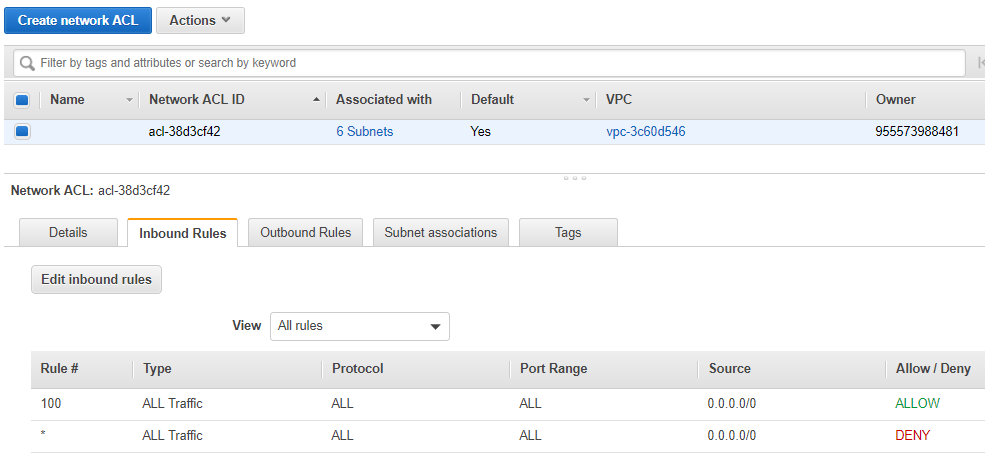
**Rules:**



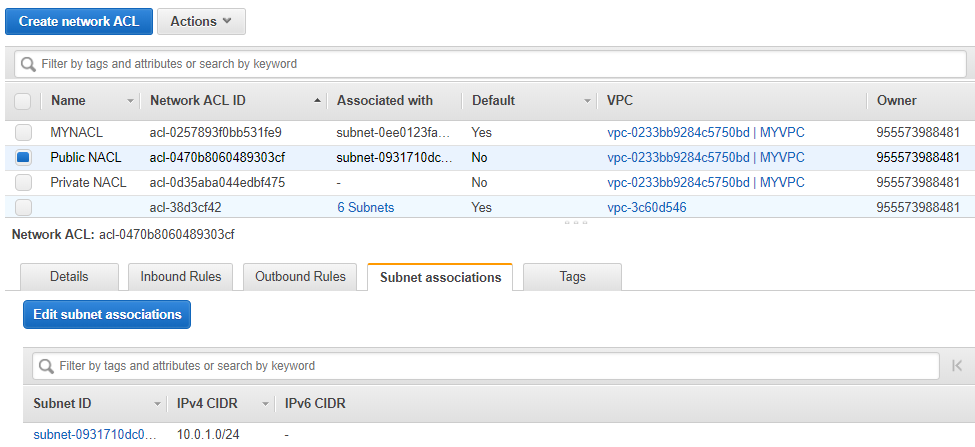
**Practical:**

* NACL acts as a firewall at the subnet level where we can restrict inbound and outbound traffic
* We need to write two rules for the traffic that inbound to the subnet and the traffic that outbound from the subnet
* Whenever we create VPC, we will get NACL created automatically for the subnets under VPC
* **We can create a NACL for a VPC, once created, we can add as many subnets as we want under subnet association section of NACL.**

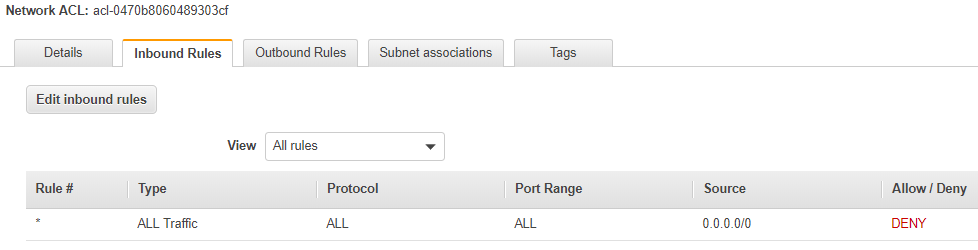


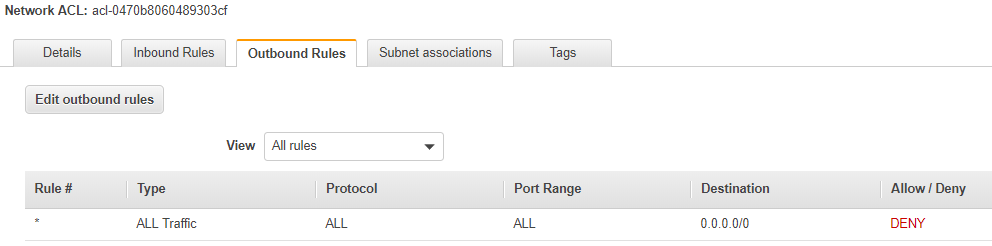


* We can see the inbound and outbound rules of NACL as above
* So, create two NACL for public and private. If we create VPC from wizards, the NACLs also gets created by default. We can edit them later

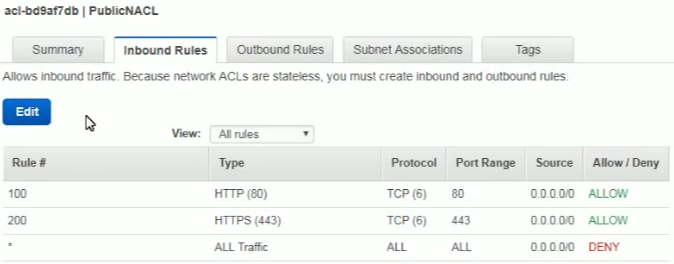


* After creating it, we need to associate the subnets

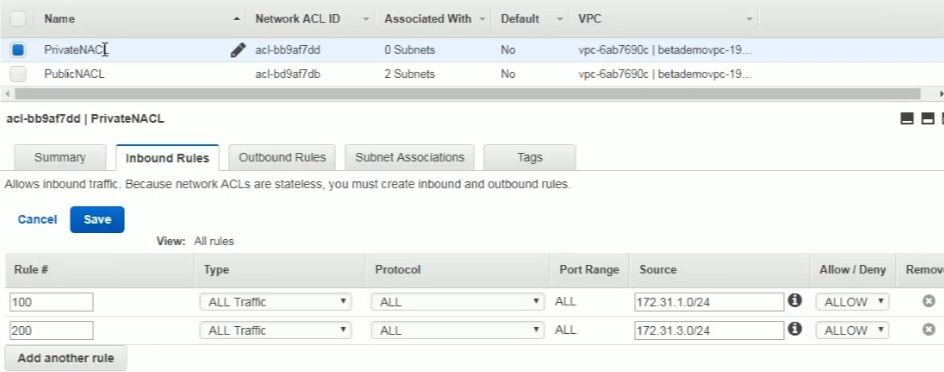




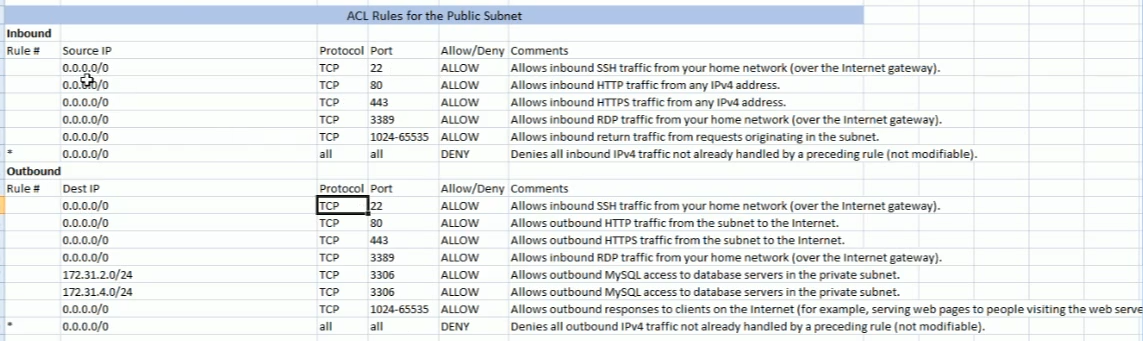
* After creating, by default the all inbound and outbound ports won’t be allowed
* We have to go and allow them whatever the ports required
* So, we got to edit them
* The default NACL & the NACL created by wizard will by default allow all the traffic in and out bound
* Whereas the custom NACL won’t. we need to edit them as below

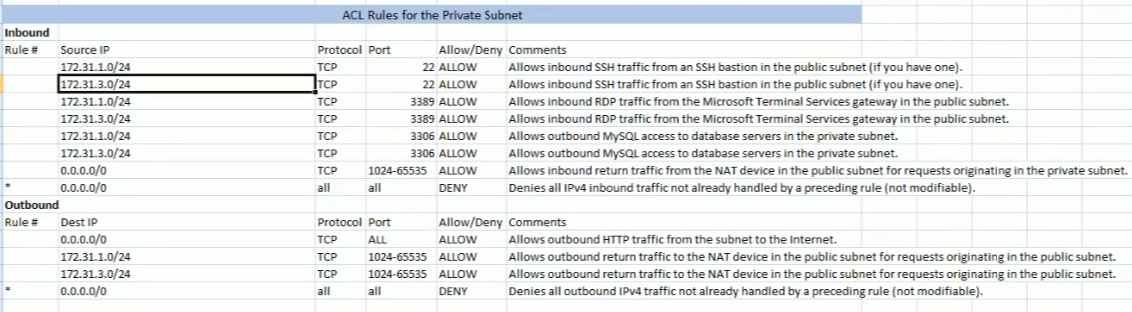


* Rule# number we can give any random number
* We can assign only one NACL per subnet
* If we have given inbound rules, then we need to allow outbound as well to access that

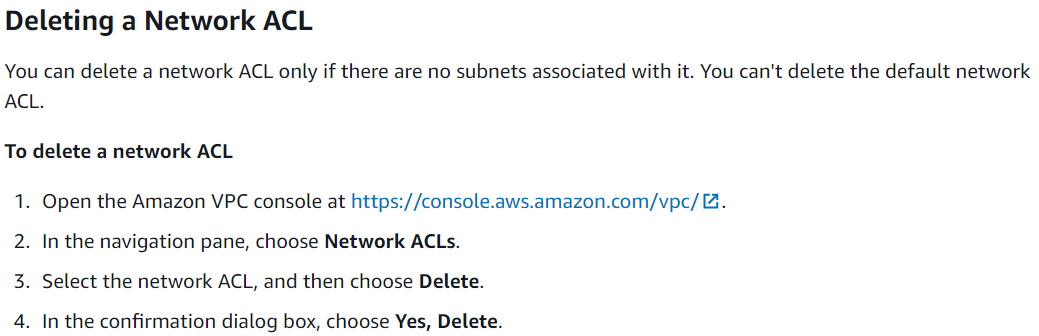


* We can allow the rules as above for private NACL for private subnets. We need to give the same rules in outbound as well





**Deleting a NACL:**



**Difference between security group & NACL:**

