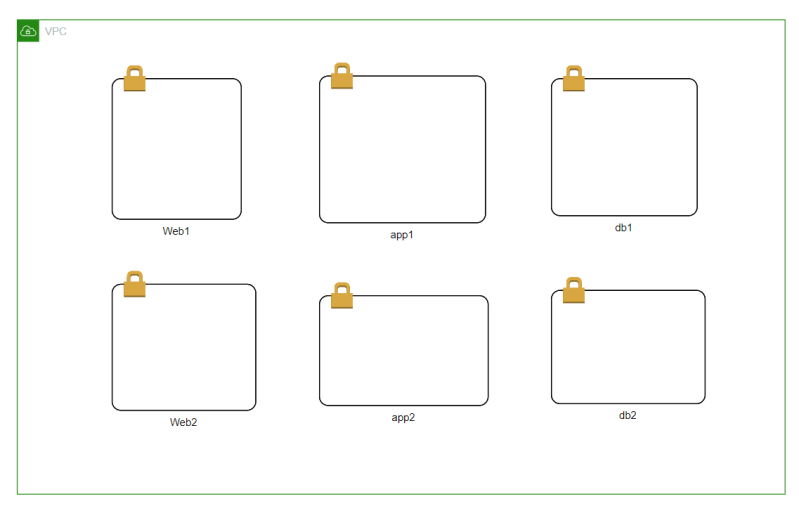
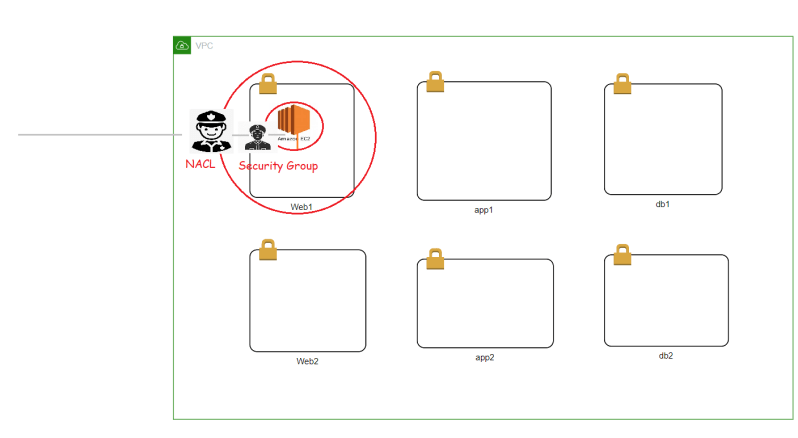
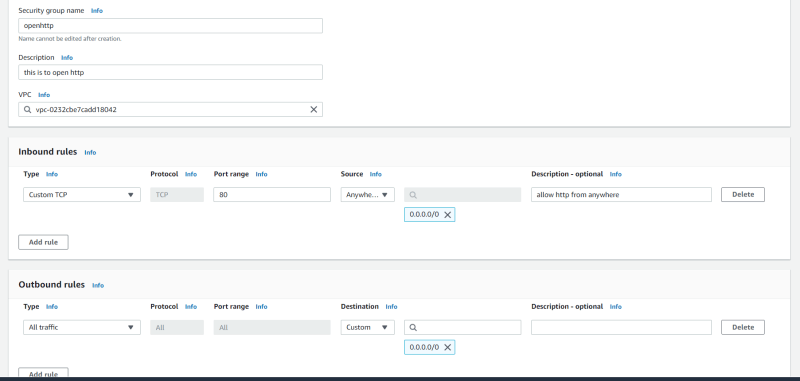
**Scenario**

* Create an AWS VPC with the following requirements 
* Requirements:
  + All the subnets should be private and they should be able to access internet
* Solution:
  + AWS has egress only internet gateway for these kinds of scenarios.
* To the ec2 instance in web subnet (which is public and has public ip) allow only http connections.
  + http => TCP 80
* EC2 instance get private ip from elastic network interface.
* In AWS at the elastic network interface level, we have a kind of a network filter (acts as firewall) where we can write only allow rules because if there is no rule it is denied.
* And at subnet level we have Network ACL 
* When we create AWS VPC, we get a default Network ACL which allows all incoming and outgoing traffic.
* Let’s look at security group: Here we define rule for incoming and outgoing traffic.

**Configuring AWS CLI**

* We need to create an IAM user and configure the user credentials to AWS CLI
* Now configure aws cli

aws configure

aws s3 ls

* Note:
  + Try to delete security credentials everytime after practice (atleast make them inactive when you are not using it)
  + Link: <https://serverless-stack.com/chapters/create-an-iam-user.html>