Virtual private cloud

1. Created virtual private cloud.
2. Created subnet and added subnets to existing virtual private cloud. With all proper CIDR value so that it does not overlap.
3. 2 subnet for public and 2 subnet for private.
4. Created internet gateway and attached to vpc.
5. Edited route table setting for public subnet and allow all ip address to internet gateway.
6. Does not set private route table setting.

Bastion host. Created ec2 instance in public subnet and established connection to ec2 instance in private subnet through ssh.

Nat gateway – created nat gateway in public subnet and edited route table setting of private subnet. Allowing all ips of private subnet to directed to nat gateway.

Thus we can access the ec2 instance in private subnet through nat gateway which is in public subnet which is connected to internet gateway.

NACL- network access control list. It is additional layer of security for subnet that control the traffic in and out of subnet.

There is NACL rules- rules are number, higher procedure with a lower number .

We can block specific ip address.