AWS

1. VPC :

Amazon virtual private cloud is a servuie that let's you launch AWS resources in a logically isolated virtual n/w that you define. You have complete control over your virtual networking environment, including selection of your own IP addr range, creation of subnets & configuration of route tables & n/w gateways. You can use both IP4 & IP6 for most resources in your virtual private cloud.

2) Subnets :

It is a range of IP address in your VPC. After creating a VPC, you can add one or more subnets in each availability zone. It is a key component in VPC. A VPC can contain all public subnets or public/private subnet combination. Private subnet is a subnet which doesnt have a route to the internet gateway. A subnet can be configured as a VPN-only subnet by routing traffic via virtual private gateway, it is part of the network.

3) Route tables :

Your VPC has a route table with a set of rules called, routes, that are used to determine where n/w traffic from your subnet or gateway is directed. You can use route tables to control where n/w traffic is directed. Each subnet in your VPC must be associated with a route table, which controls the routing for the subnets you can explicitly associate a subnet with a particular route table. Otherwise the subnet is implicitly associated with the main route table. A subnet can only be associated with one route table

at a time. But you can associate multiple subnets with the same subnet route table.

4) Internet gateway:

It is a horizontally scaled, redudant & highly available VPC component that allows communication b/w your VPC & the internet.

It serve 2 purpose: to provide a target in your VPC route table for internet-routable traffic & to perform n/w address translation (NAT) for instances that have been assigned IPV4 address.

5) Security Groups:

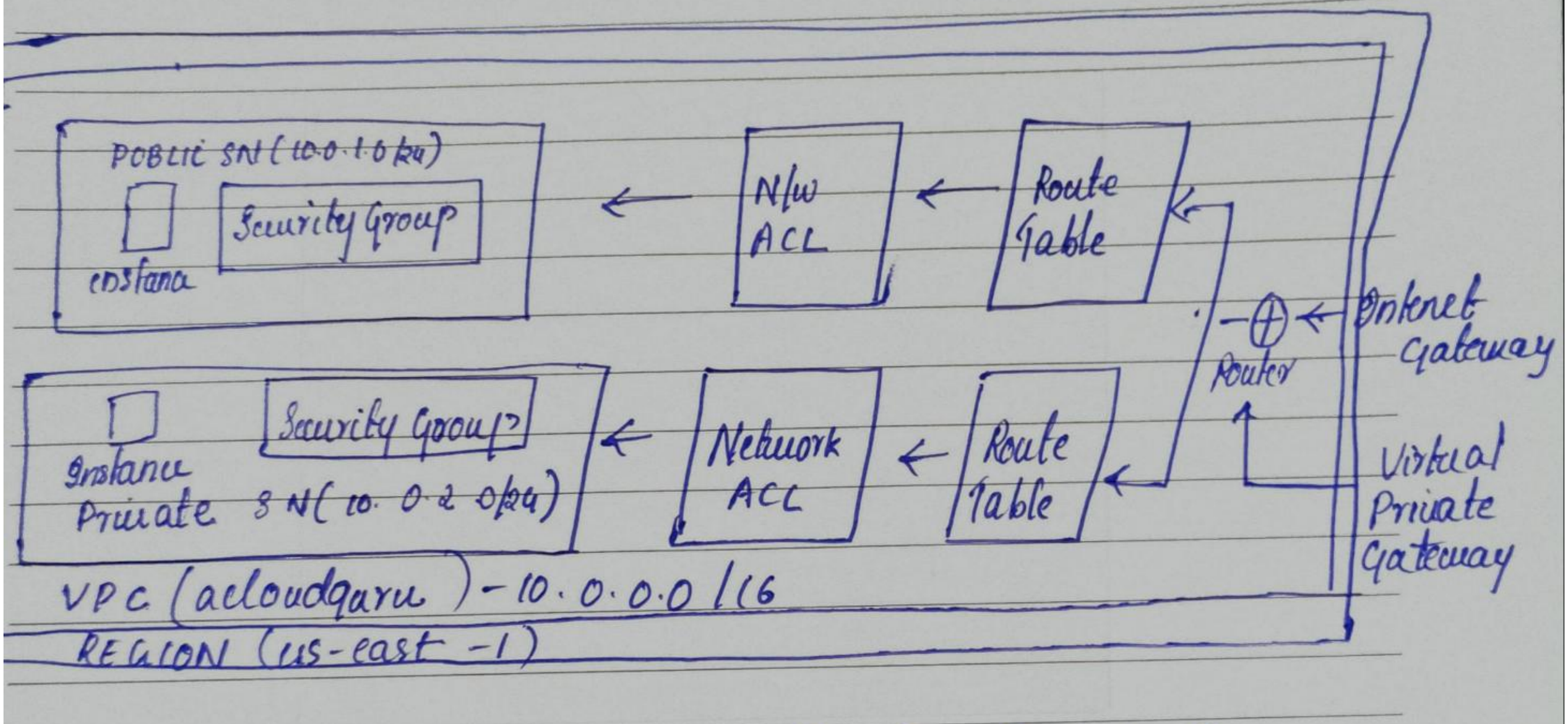
It acts as a virtual firewall for your EC2 instances to control incoming & outgoing traffic: Inbound rules control the incomming traffic to your instances & outbound rules control the off & outgoing traffic from your instance. When you launch an instance you can specify one or more security groups.

If you dont specify a security group. You can add rules to each security that allow traffic to or from its associated instances. You can modify the rules for a security group at any time. New & modified rules are automatically applied to all instances that are associated with the group.

6) Network ACL's:

A network access control list is an optional layer for security for your VPC that acts as a firewall for controlling traffic in & out of one or more subnets. You might set up network ACL's with

rules similar to your security groups in order to add an additional layer of security to your VPC



VPC with Public & Private Subnets