Cloud security idioms:-

An isolated system is never a problem beyond direct user access.

A network of computers identified by end points identified by IP addresses needs integrated security on each layer of networks and applications.

Followings are the cloud idioms extracted from AWS infrastructure build –

1) VPC – Virtual Private Cloud
   It is for provisioning of a logically isolated section of cloud.
   It is a virtual network (VPN) dedicated to your AWS account.
   Define the IP ranges by providing CIDR.
   Followings are the internal components
   a. Subnets –
      A *subnet* is a range of IP addresses in your VPC.
   b. Route table –
      A *route table* contains a set of rules, called routes, that are used to determine where network traffic is directed.
   c. Internet gateway –
      An *internet gateway* is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the internet. It therefore imposes no availability risks or bandwidth constraints on your network traffic.
   d. VPC endpoint –
      A *VPC endpoint* enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network.

   Ref:-

   https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html

   https://cidr.xyz/ <- to calculate cidr ranges

2) Availability Zones
   Availability zones (AZs) are isolated locations within data center regions from which public **cloud** services originate and operate. Regions are geographic locations in which public **cloud** service providers' data centers reside.
   a. Regions
      Your account determines the Regions that are available to you.
      For example, AWS US account will have regions like this

`us-east-2`	US East (Ohio)
`us-east-1`	US East (N. Virginia)

`us-west-1`	US West (N. California)
`us-west-2`	US West (Oregon)

b. Availability zones

If you distribute your instances across multiple Availability Zones and one instance fails, you can design your application so that an instance in another Availability Zone can handle requests.

An Availability Zone is represented by a Region code followed by a letter identifier; for example, `us-east-1a, us-east-1b, us-east-1c`.

Ref:-

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html

3) Security groups

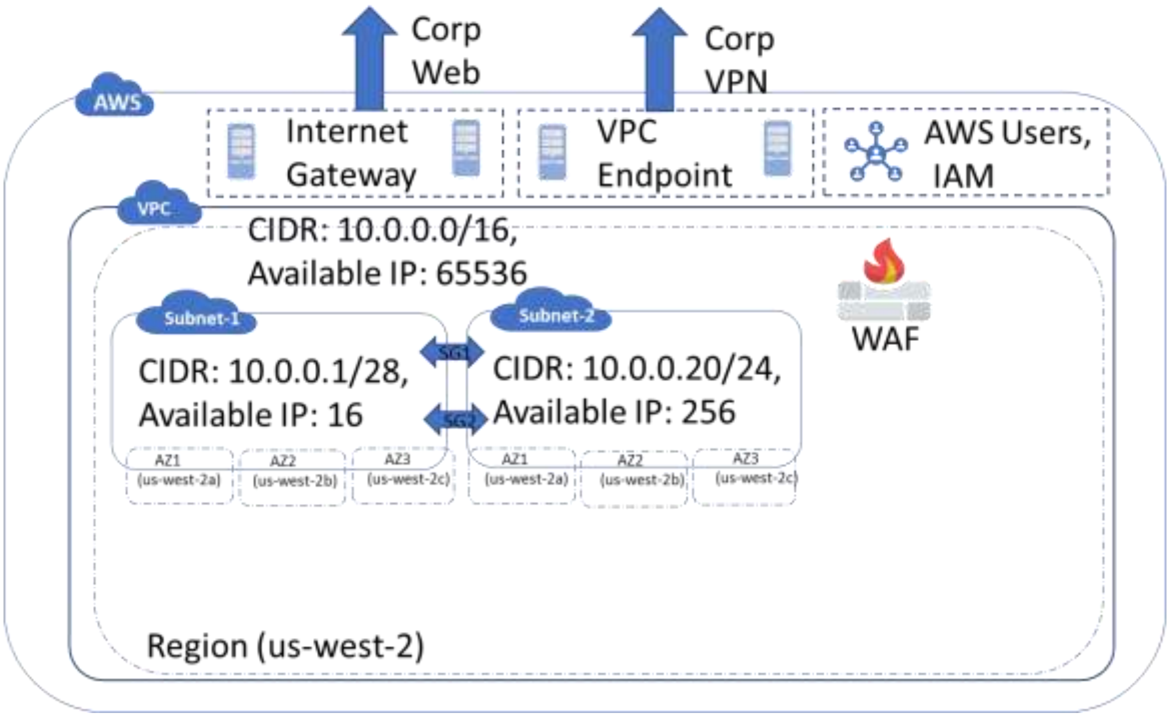
A *security group* acts as a virtual firewall that controls the traffic for one or more instances.

a. WAF – Web Application Firewall
b. Corporate firewall rules

Ref:-

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-security-groups.html

https://aws.amazon.com/waf/



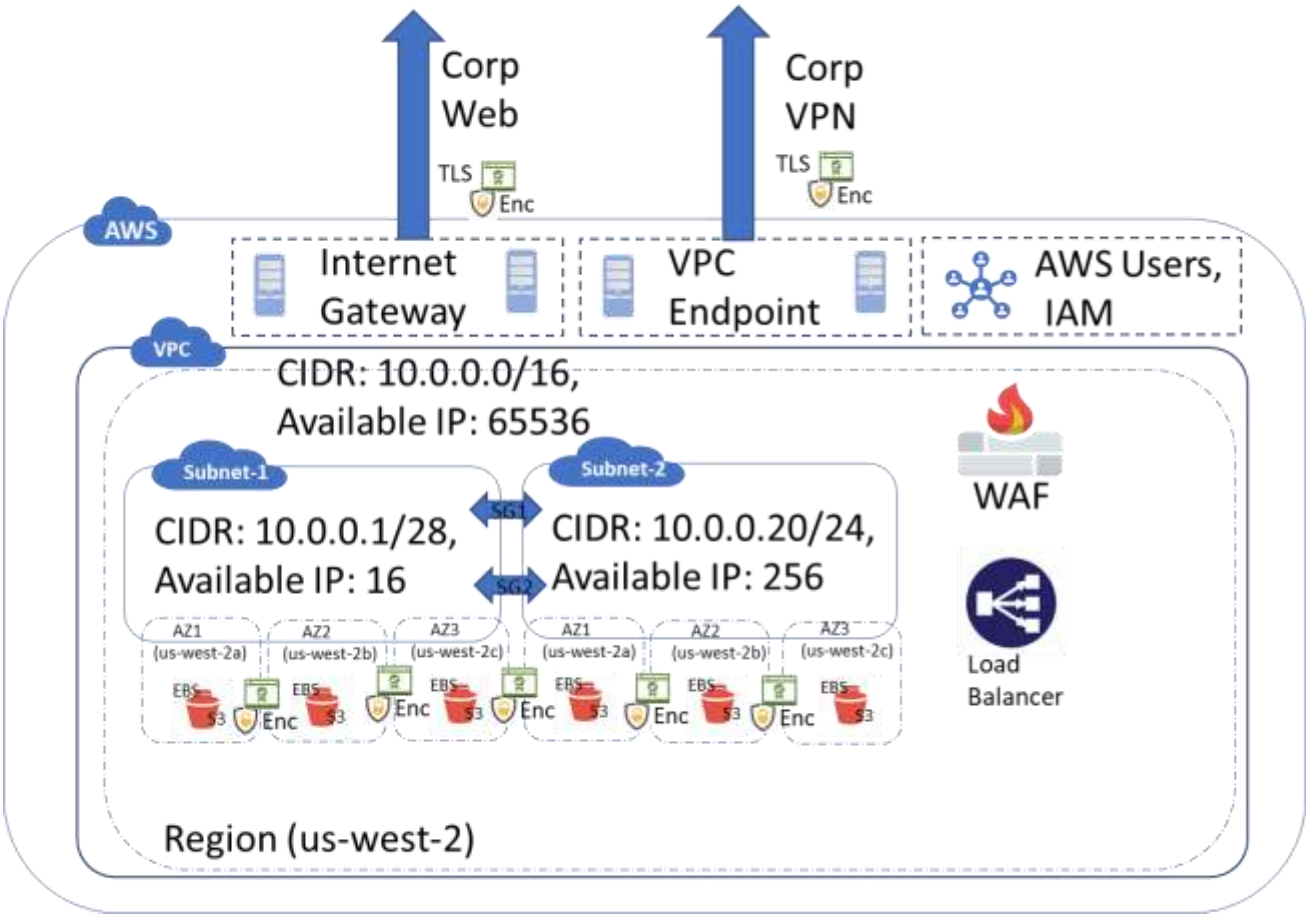
Security around these –

A must in security is zero trust policy.

1) Identity management
    a. IAM
        i. AWS roles and groups
    b. Multi-level user authentication like Okta
    c. SSO (single sign-on) using OAuth

2) Data in transit security
    a. AWS Certificate management
    b. TLS 1.2 algorithms with Java and others

3) Data at rest security
    a. Encryption zones and encryption key management
    b. Scrubbing of unused volumes, AWS promises to scrub before new use but always good to do it custom then release the storage


Corp Web
TLS
Enc
Corp VPN
TLS
Enc
AWS
Internet Gateway
VPC Endpoint
AWS Users, IAM
VPC
CIDR: 10.0.0.0/16,
Available IP: 65536
Subnet-1
CIDR: 10.0.0.1/28,
Available IP: 16
SG1
SG2
Subnet-2
CIDR: 10.0.0.20/24,
Available IP: 256
WAF
Load Balancer
AZ1 (us-west-2a)
AZ2 (us-west-2b)
AZ3 (us-west-2c)
AZ1 (us-west-2a)
AZ2 (us-west-2b)
AZ3 (us-west-2c)
EBS
S3
Enc
Region (us-west-2)