AWS Solution Architect Associate

Version : C03

Domain 1

Task 2

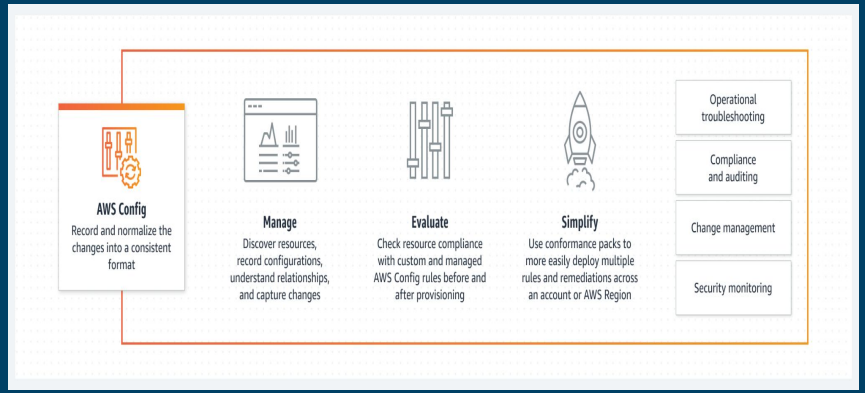
Design Secure Workloads and Applications

AWS Config

- Provides a detailed view of the configuration of AWS resources in the AWS account
- It helps to oversee the application resources
- AWS Resource is an entity in AWS. Example - EC2 instance,EBS etc
- **Resource Discovery**
  - As a very first step, supported AWS resources are discovered in the AWS account and a configuration item is generated for each of them
- **Resource Tracking**
  - AWS Config keeps track of all changes to the resources by invoking the list API call for each resource in the account

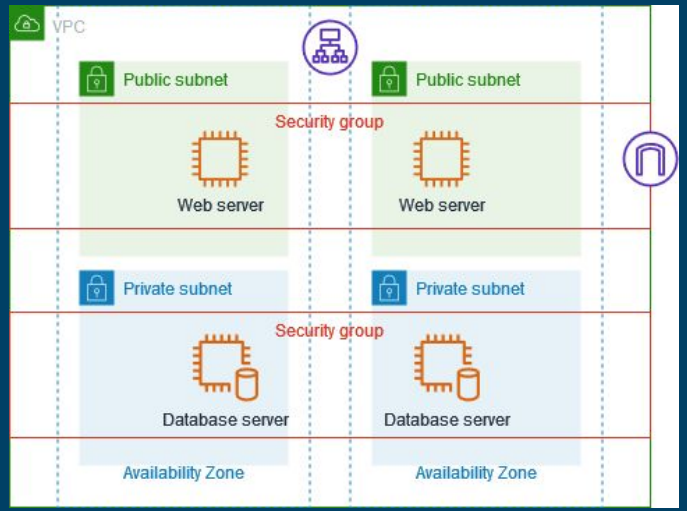
AWS Config

- AWS Config can deliver configuration items through one of the below channel
  - Amazon S3 bucket
  - Amazon SNS Topic



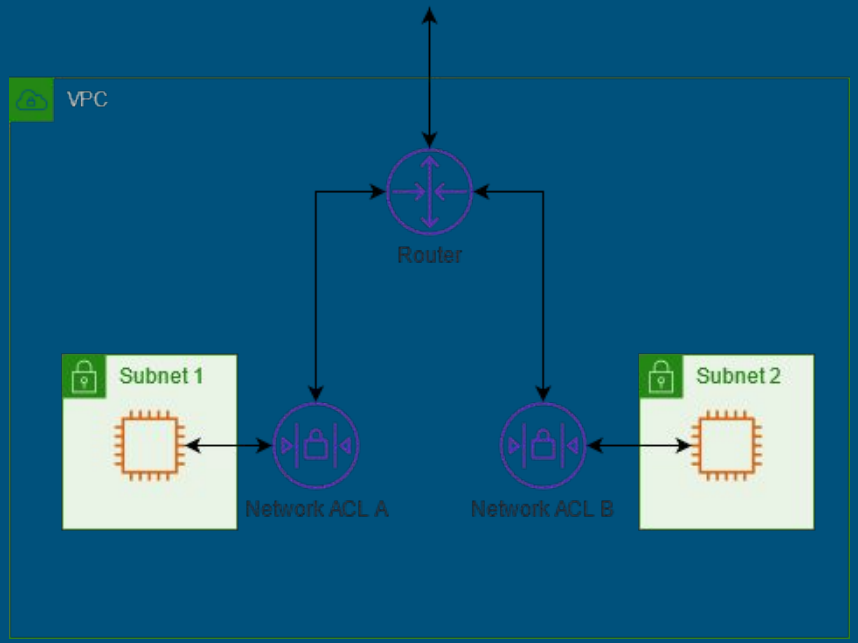
Security Group

- ➔ It controls the inbound and outbound traffic at the resource level
- ➔ A VPC or an EC2 comes with a default security group
- ➔ Multiple security groups can be assigned to a resource



Network ACL

- ➔ It allows or denies specific inbound or outbound traffic at the subnet level
- ➔ Default network ACL or custom network ACL with rules can be used
- ➔ It adds an additional layer of security to the VPC
- ➔ No additional charges for using the network ACL's
- ➔ Default network ACL is configured to allow all traffic to flow in and out of the subnets with which it is associated.



Network ACL

➔ It includes a rule which ensures that if a packet doesn't match any of the numbered rules , it's denied.

Default Network ACL rules :

Inbound

Rule #	Type	Protocol	Port range	Source	Allow/Deny
100	All IPv4 traffic	All	All	0.0.0.0/0	ALLOW
*	All IPv4 traffic	All	All	0.0.0.0/0	DENY

Outbound

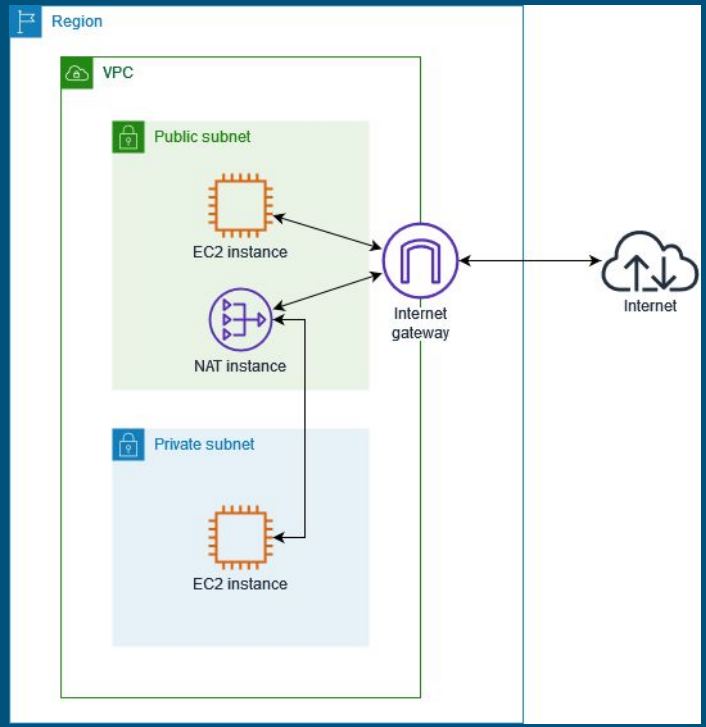
Rule #	Type	Protocol	Port range	Destination	Allow/Deny
100	All IPv4 traffic	All	All	0.0.0.0/0	ALLOW
*	All IPv4 traffic	All	All	0.0.0.0/0	DENY

NAT Gateway

- A Network Address translation service
- It can be used for the instances in a private subnet to connect to services outside the VPC
- Using NAT gateway , external services cannot connect to the instances in the private subnet
- Created in a specific Availability Zone and implemented with redundancy in that zone
- There are 2 connection types
  - **Public** - Instances in the private subnets can connect to the internet through a public NAT gateway but cannot have unsolicited inbound connections from the internet.
  - **Private** - Instances in the private subnets can connect to other VPC's or on-premises network through a private NAT gateway.

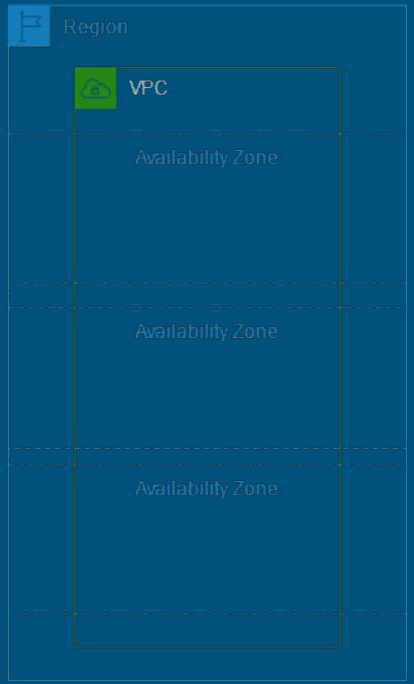
NAT Gateway

- When sending response traffic to the instances, whether it's a public or private NAT gateway, the NAT gateway translates the address back to the original source IP address.
- NAT gateway supports TCP, UDP and ICMP
- A security group cannot be associated with the NAT gateway



VPC

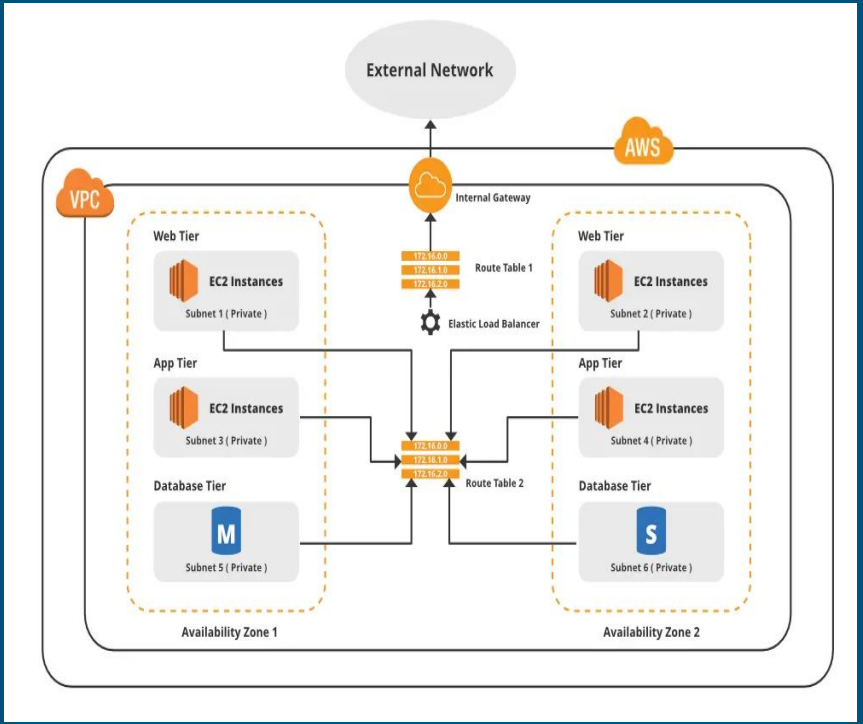
- VPC aka virtual private cloud (VPC)
- Virtual network dedicated to an AWS account.
- Logically isolated from other virtual networks in the AWS Cloud.
- An IP address range can be specified for the VPC,
- VPC can span across Availability Zones in a Region
- Every region has a default VPC which includes public subnet , an internet gateway and settings to enable DNS resolution
- Types of VPC
  - **Default VPC**
  - **Custom VPC**
- Supports tagging, allowing you to categorize and manage your resources more effectively.
- It supports IPv4 and IPv6 addressing for your resources
- VPC Endpoints allow you to privately connect your VPC to supported AWS services without requiring internet gateways or NAT instances
- VPC Peering enables you to connect one VPC with another VPC within the same AWS region, allowing for inter-VPC communication.



VPC Architecture

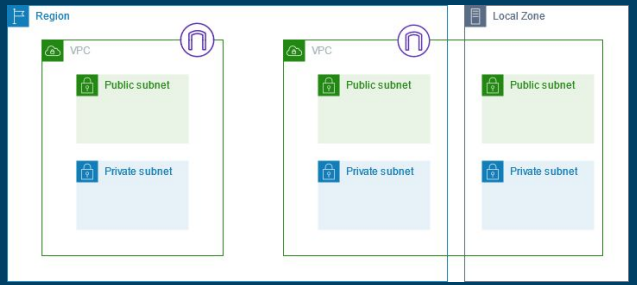
- Main components of AWS VPC are
  - **Subnets**
  - **Internet Gateway**
  - **VPC Peering**
- When a request is made to an application which is hosted in a particular region in a VPC, it is served following the below steps :

  User Request -> VPC routing -> Subnet routing -> Security Group Evaluation -> Directed to load balancer -> Received and processed at web server -> Response Generation -> Security Group Evaluation -> Directed by load balancer -> Subnet Routing -> VPC Routing -> **User Response**



Network Segmentation Strategies

- Subnets is a range of IP addresses in the VPC
- Each subnet must reside entirely within 1 AZ and cannot span across zones
- Subnet Types
  - **Private Subnet**
  - **Public Subnet**
- Each subnet must be associated with a route table, which specifies the allowed routes for outbound traffic leaving the subnet
- By default every subnet is automatically associated with the main route table for the VPC
- Network ACL' are used to allow or deny inbound/outbound traffic at the subnet level



Securing Application using AWS services

- **AWS Shield**
  - A managed DDoS protection service that safeguards applications running on AWS
  - Works at OSI layer 3,4 and 7
  - Shield Types
    - **Shield Standard - Free**
    - **Shield Advanced - Paid**
  - It detects and mitigates the coverage against threats even if they are not explicitly known
- **AWS WAF**
  - Helps secure the web applications
  - Protect against common web exploits and bots
  - Controls access to content by allowing/blocking web requests based on the specified criteria
  - Protects CloudFront distributions and origin servers

Securing Application using AWS services

- **AWS SSO**
  - AWS Single Sign-On (AWS SSO) is now AWS IAM Identity Center
  - Used to create, connect the workforce users once and centrally manage their access to multiple AWS accounts and applications
  - Supports various security standards and compliance certifications
  - Available in 21 regions globally
- **AWS Secret Manager**
  - Helps to manage, retrieve and rotate database credentials, application credentials, OAuth tokens, API keys and other secrets throughout their life cycles.
  - Used by many AWS services
  - Helps in improving the security posture
  - Provides automatic rotation schedule
  - In Secrets Manager, a secret consists of secret information, the secret value, plus metadata about the secret.

AWS Service Endpoints

- An endpoint is the URL of the entry point for an AWS web service
- It is used to connect to an AWS service programmatically
- Types of Endpoints
  - **Regional Endpoints**
  - **Global Endpoints**
- Most Amazon Web services offer a regional endpoint that can be used to make requests
- Following services support both endpoints
  - Amazon EC2
  - Amazon EC2 Auto Scaling
  - Amazon EMR

VPN

- VPN or Virtual Private Network creates a private network connection between devices through the internet.
- Used to safely and anonymously transmit data over public networks.
- It masks the user IP addresses and encrypt data so it's unreadable by unauthorized entities
- Three main functions of VPN are
  - **Privacy** - Use encryption to keep the confidential information private , especially when connecting over public networks
  - **Anonymity** - It hides the IP address so that the user remains anonymous on the internet
  - **Security** - Uses cryptography to protect the internet connection from unauthorized access
- AWS VPN offers 2 valuable services
  - **AWS Site to Site VPN** - Enables to securely connect on-premise network or branch office site to Amazon VPC
  - **AWS Client VPN** - Allows to securely connect users to AWS or on-premise networks

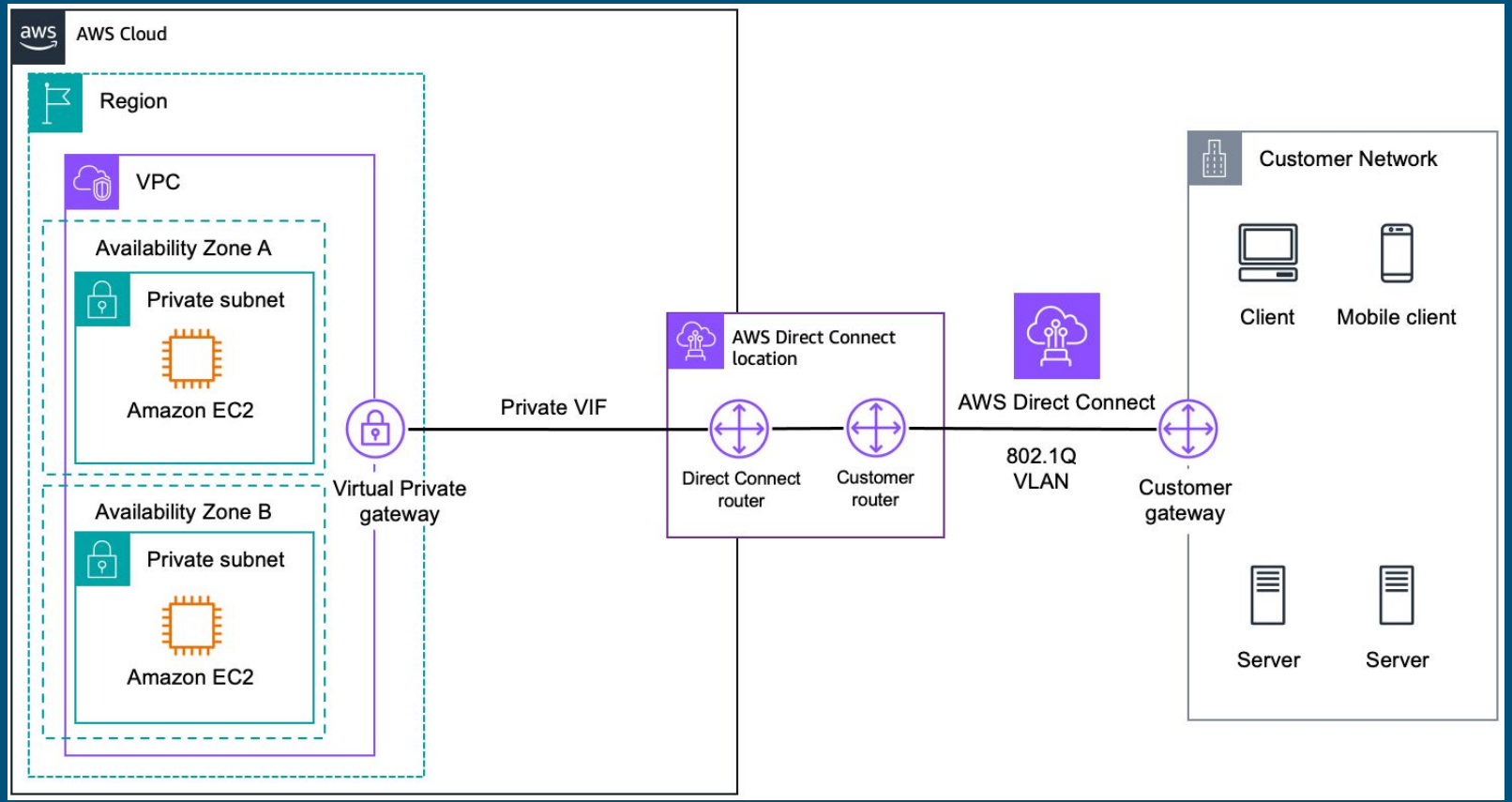
How does a VPN work ?

- VPN connection redirects data packets from the machine to another remote server before sending them to 3rd party over the internet
- Key principles behind VPN technology are
  - **Tunneling Protocol**
    - VPN creates a secure data tunnel between the local machine and another VPN server
    - Contents of the internet traffic is not visible to ISP and other 3rd parties
  - **Encryption**
    - VPN protocol - IPSec is a protocol suite for securing Internet Protocol(IP) communications by authenticating and encrypting each IP packet of a data stream
    - VPN service makes sure the data is unreadable and is decoded only at the other end to avoid data misuse

AWS Direct Connect

- Establishes a dedicated connection from an on-premises network to one or more VPCs
- It can reduce network costs , increase bandwidth throughput and provide a more consistent network experience than internet based connections
- Uses industry standard 802.1Q VLANs to connect to Amazon VPC using private IP addresses
- VLANs are configured using virtual interfaces (VIFs)
- Three different types of VIFs that can be configured are
  - **Public Virtual Interface**
  - **Transit Virtual Interface**
  - **Private Virtual Interface**
- AWS direct connect has two types of connections
  - **Dedicated connection** - A physical ethernet connection is associated with a single customer
  - **Hosted connection** - A physical ethernet connection is provisioned by an AWS Direct Connect Partner and is shared

AWS Direct Connect



Threat Vectors External to AWS

- **DDoS**
  - DDoS stands for Distributed Denial of Service
  - It is a malicious attempts to disrupt the normal traffic of a targeted server, service or network by overwhelming it with a flood of internet traffic.
  - If not mitigated effectively, It can lead to impaired availability or degraded response times for web applications
  - AWS services to protect from DDoS
    - AWS Shield - Standard / Advanced
    - Amazon CloudFront
    - Amazon Route53
    - AWS WAF
    - AWS Shield Advanced Global Accelerator

- **SQL Injection**
  - Type of cyber attack that involves injecting malicious code into an SQL statement allowing attackers to gain access to sensitive information stored in the database.
  - It can be devastating for the businesses and can result in the theft of valuable data , financial losses
  - AWS services to protect from SQL Injection
    - AWS WAF
    - AWS GuardDuty
    - AWS Inspector
    - AWS Cloudwatch

AWS Solution Architect Associate

Version : C03

Domain 1

Task 2

The END