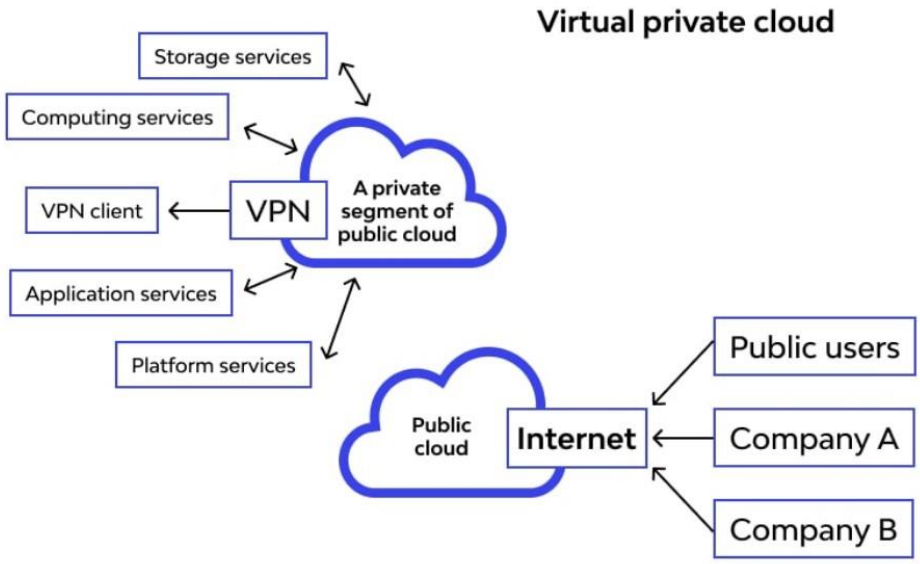
AWS VIRTUAL PRIVATE CLOUD (VPC)

1)What is VPC?

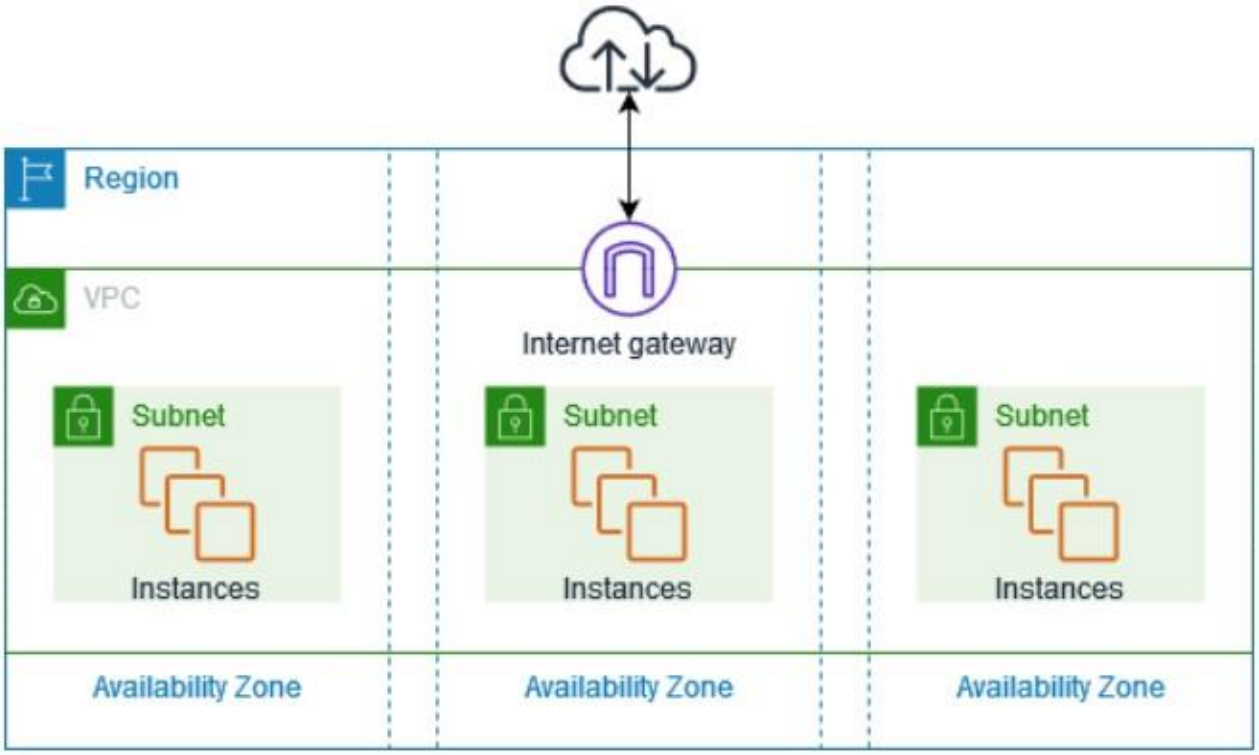
In Amazon Web Services (AWS), A VPC is a logically isolated network that you can create within the AWS cloud. It provides you with a level of control over your network environment that is similar to what you would have in your own on-premises data center.



1. ***Isolation and Security****: VPC allows you to create a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define. This means you can define your network topology and control over IP addressing, subnets, routing tables, and network gateways. This isolation enhances security by ensuring that your resources are not directly accessible from the internet.*
2. ***Connectivity Options****: AWS provides various connectivity options to establish connections between your on-premises data centers and the VPC in AWS. This includes AWS Direct Connect, VPN connections, or AWS Transit Gateway. These options allow you to extend your corporate network into the cloud securely and privately.*

3. ***Hybrid Cloud Deployments****: Many organizations operate in hybrid cloud environments, where they have some resources in their data centers and some in the cloud. VPC allows for seamless integration between on-premises infrastructure and cloud resources, enabling hybrid cloud deployments without compromising security or performance.*
4. ***Scalability and Flexibility****: With VPC, you have the flexibility to scale your resources up or down as needed. You can easily add or remove instances, subnets, and other resources within your VPC without affecting your on-premises infrastructure.*
5. ***Resource Management****: VPC enables centralized management of network resources, allowing you to define and enforce network access controls, route traffic, and monitor network activity from a single console.*
6. ***Vpc diagram 1a:-***

Vpc diagram 1b:-



2)COMPONENTS OF VIRTUAL PRIVATE CLOUD:-

The diagram shows the following components of a VPC:

Region: *An AWS region is a geographical area where AWS resources are located. Regions are physically separate from each other, and they have independent power, cooling, and security controls.*

VPC: The VPC itself is represented by the blue box in the diagram. It is the container for all of the other resources in your VPC network.

Internet Gateway: *The internet gateway (orange rectangle) is a highly available resource that allows traffic to flow between your VPC and the internet. You can attach an internet gateway to your VPC to enable resources in your VPC to communicate with the internet.*

Subnet: *A subnet (blue rectangles) is a range of IP addresses within a VPC. You can create multiple subnets in a VPC, and you can launch AWS resources in specific subnets. Subnets can be public or private. Public subnets have routes to the internet gateway, while private subnets do not.*

Availability Zone: *An Availability Zone (AZ) is a distinct location within a region. AZs are designed to be isolated from each other, so that a failure in one AZ does not affect the other AZs. The diagram shows three availability zones.*

3)VPC Route table:-

In a Virtual Private Cloud (VPC) on AWS, a route table acts like a traffic director. It's a set of rules that determines how network traffic gets routed within your VPC and to the internet.

Rules for Traffic Flow: Each route table contains entries called routes. These routes specify the destination (like an IP address or subnet) for a particular traffic flow and the next hop (like an internet gateway or another subnet) where the traffic should be directed.

Subnet Association: Every subnet in your VPC must be associated with one route table. This association defines which set of routing rules applies to the traffic originating from that subnet. A single route table can be associated with multiple subnets, allowing for different routing configurations for various parts of your VPC.

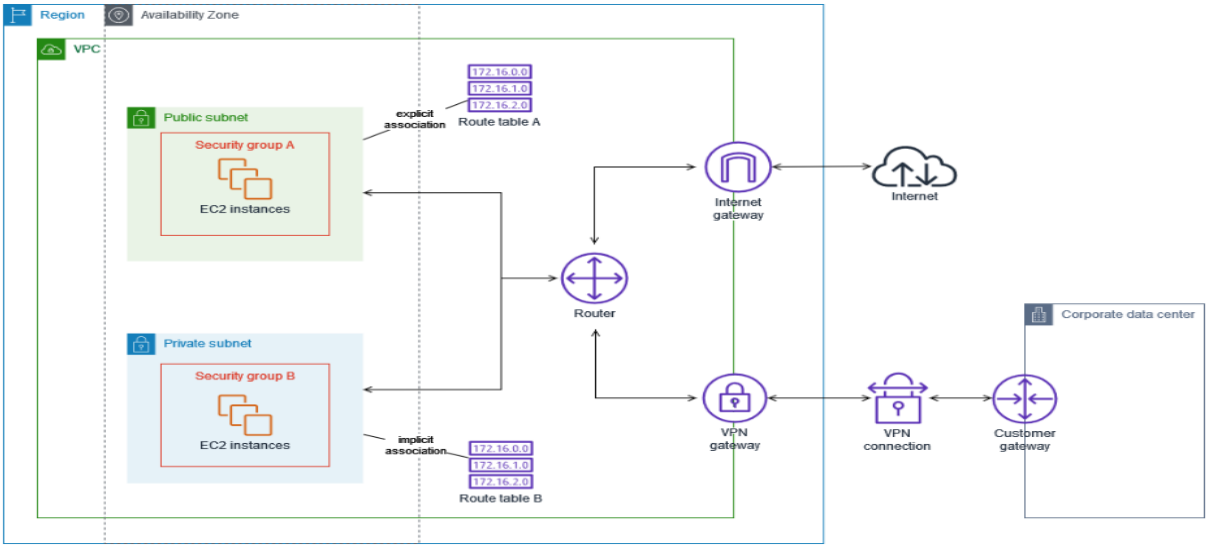
Default Local Route: By default, all route tables include a local route. This route ensures traffic destined for other resources within the same VPC stays within the VPC boundaries and doesn't go out to the internet.

There are two main types of route tables:

Main Route Table (Default): When you create a VPC with a public subnet, AWS creates a default route table with a route pointing to the internet gateway. This allows internet access for resources in the public subnet. It's recommended to keep this main route table mostly untouched for security reasons.

Custom Route Tables: You can create custom route tables with specific routing rules. These are useful for scenarios where you want more granular control: over traffic flow. For example, you might create a custom route table for a private subnet that doesn't have internet access by default.

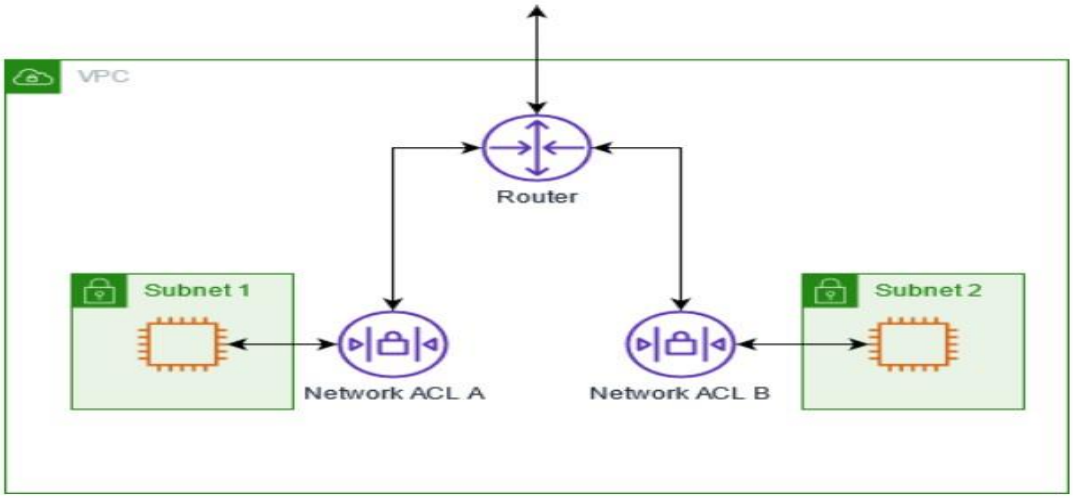
Vpc diagram 1c:-



ROUTE TABLE Diagram

4)NACL (NETWORK ACCESS CONTROL LIST):-

NACL DIAGRAM



NACL:-*A VPC is a logically isolated network that you can create within the AWS cloud. NACLs act as firewalls that control inbound and outbound traffic within your VPC.*

Network ACL A & B*: The two orange rectangles labelled "Network ACL A" and "Network ACL B" represent Network Access Control Lists (NACLs). NACLs are firewall rules that control inbound and outbound traffic at the subnet level. You can associate one or more NACLs with a subnet.*

Here are some key points about NACLs:

Filtering Rules: *NACLs contain rules that allow or deny traffic based on various criteria, including source and destination IP address, port number, and protocol (e.g., TCP, UDP).*

Subnet Level Security: *NACLs are attached to subnets, so they filter traffic entering or leaving the subnet. This provides granular control over traffic flow within your VPC.*

Inbound and Outbound Rules: NACLs can have separate rules for inbound and outbound traffic. This allows you to control what kind of traffic can enter a subnet and what kind of traffic can leave a subnet.

Default Deny All: NACLs follow a default deny-all rule. This means that only traffic explicitly allowed by a rule in the NACL is permitted.

DEFAULT NACL:-

The default network ACL is configured to allow all traffic to flow in and out of the subnets with which it is associated. Each network ACL also includes a rule whose rule number is an asterisk (*). This rule ensures that if a packet doesn't match any of the other numbered rules, it's denied. You can't modify or remove this rule.

The following is an example default network ACL for a VPC that supports IPv4 only.

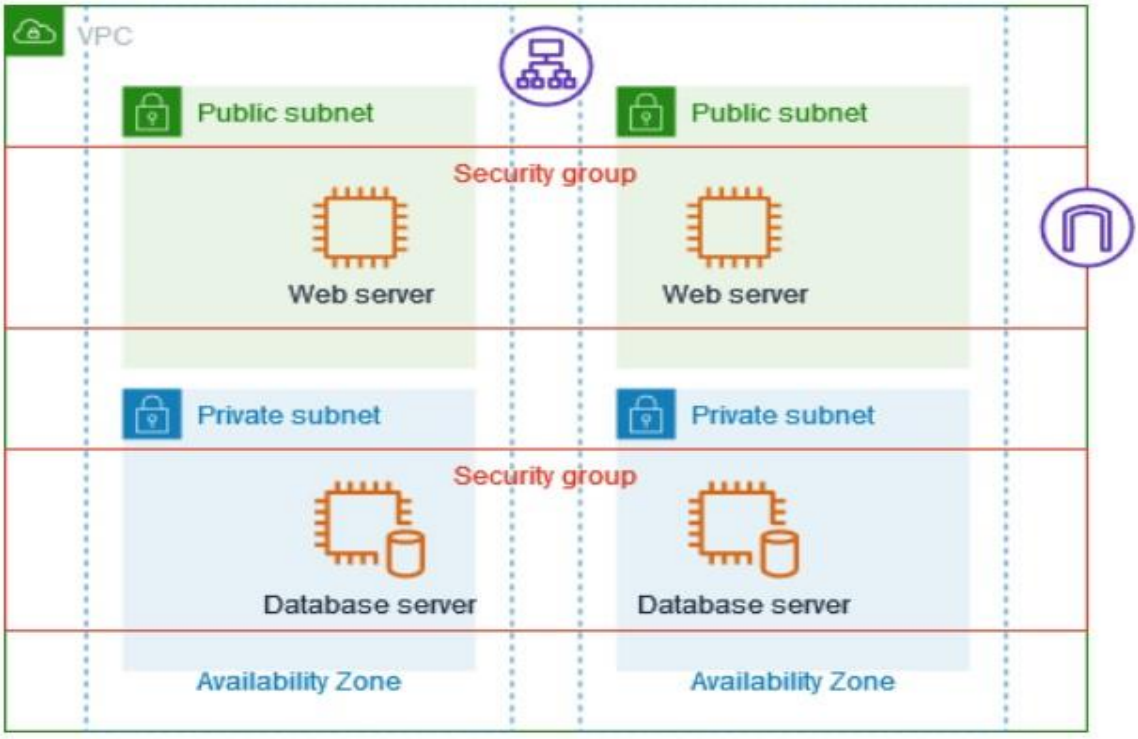
Inbound

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

5) SECURITY GROUP:-



Security group diagram

WHAT IS SECURITY GROUP ?

Security groups are a firewall service offered by AWS that acts as a stateful firewall to control inbound and outbound traffic to your VPC resources.

Here are the key points about security groups:

Control traffic to VPC resources: *Security groups act as virtual firewalls, controlling inbound and outbound traffic to your Amazon EC2 instances within a VPC [1]. They filter traffic at the instance level, unlike Network Access Control Lists (NACLs) that filter traffic at the subnet level [1].*

Inbound and outbound rules: *Security groups consist of rules that define the flow of traffic. You can create rules to allow specific types of traffic to enter or leave your VPC resources. Each rule specifies a*

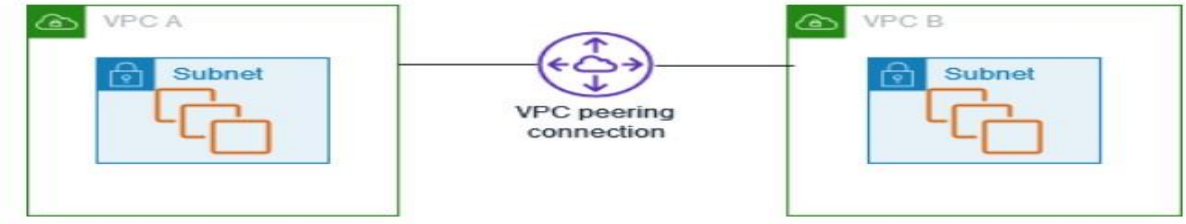
protocol (e.g., TCP, UDP), port range, and source (IP address or security group).

Stateful inspection: Security groups perform stateful inspection, meaning they keep track of the connection state and allow return traffic for permitted inbound connections.

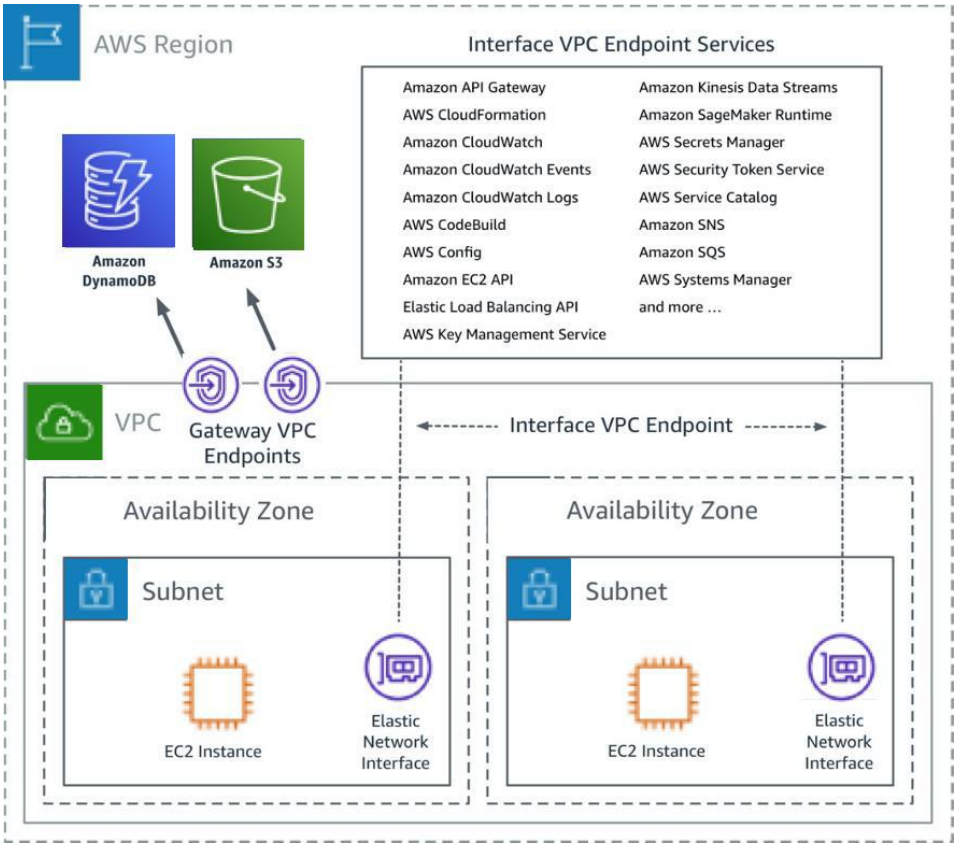
The diagram shows a VPC with two public subnets and two private subnets. Each subnet has a security group associated with it. The security groups control the traffic flow to the resources in the subnets. For example, the security group for the web servers in the public subnet might allow inbound SSH traffic on port 22 and HTTP traffic on port 80, while the security group for the database server in the private subnet might only allow inbound traffic from the web servers in the public subnet.

VPC PEERING:-

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them privately. Resources in peered VPCs can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, with a VPC in another AWS account, or with a VPC in a different AWS Region. Traffic between peered VPCs never traverses the public internet.



Vpc endpoint :-Diagram:



A VPC endpoint enables private connectivity between your VPC and supported AWS services or VPC endpoint services powered by AWS PrivateLink .This means that traffic between your VPC resources and the AWS service doesn't leave the AWS network, improving security and potentially reducing network latency.

There are two main types of VPC endpoints depicted in the image ***Interface VPC Endpoint****: This type of endpoint creates an elastic*

network interface (ENI) within your VPC subnet. The ENI serves as an entry point for traffic destined to the chosen AWS service. Traffic is routed to the service using DNS resolution .

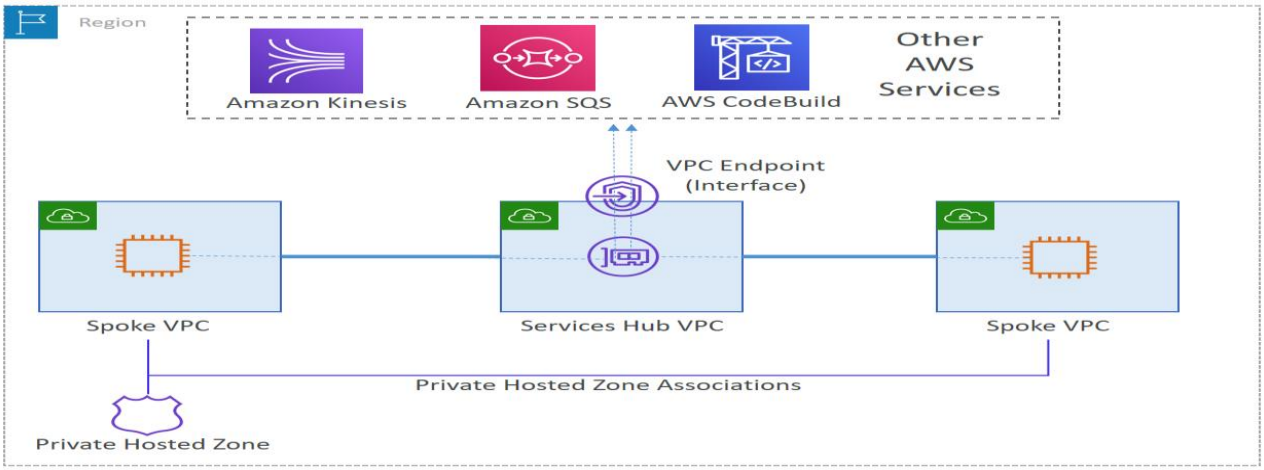
Gateway VPC Endpoint*: This type of endpoint routes traffic to the AWS service through a VPC gateway attached to your VPC. VPC gateway routes traffic to the AWS service endpoint in the AWS region.Here are some of the benefits of using VPC endpoints:*

***Improved Security**: Traffic between your VPC resources and AWS services doesn't travel over the public internet, reducing the attack surface for malicious actors.*

***Reduced Costs**: Depending on your data transfer usage, you might see reduced costs by using VPC endpoints instead of internet gateways.*

***Amazon PrivateLink Integration:** VPC endpoints work seamlessly with AWS PrivateLink, a service that enables you to privately connect your VPC to services offered by other AWS accounts and service providers.*

vpc endpoint to other service aws



What is AWS Site-to-Site VPN?

The VPN connection offers two VPN tunnels between a virtual private gateway or transit gateway on the AWS side and a customer gateway on the on-premises side.

This allows you to extend your on-premises network to the AWS cloud, enabling communication between your resources in the cloud and your on-premises servers.

A Site-to-Site VPN connection consists of the following components:-

***1)A virtual private gateway or a transit gateway:-** A virtual private gateway is the VPN concentrator on the Amazon side of the Site-to-Site VPN connection. You create a virtual private gateway and attach it to a virtual private cloud (VPC) with resources that must access the Site-to-Site VPN connection.*

diagram of a virtual private gateway (VGW) in the context of AWS Site-to-Site VPN. Let's break down the different components:

Region: *This refers to the AWS region where your VPC resides.*

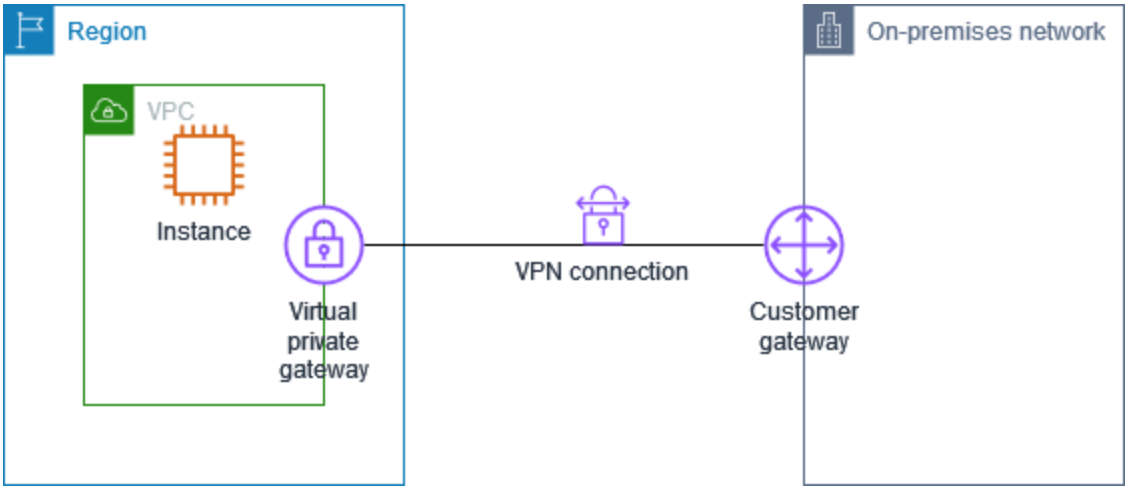
VPC: *Virtual Private Cloud is a private network that you create within the AWS cloud. It logically isolates your AWS resources from the public internet.*

Instance: *This represents an Amazon EC2 instance which is a virtual server in the AWS cloud.*

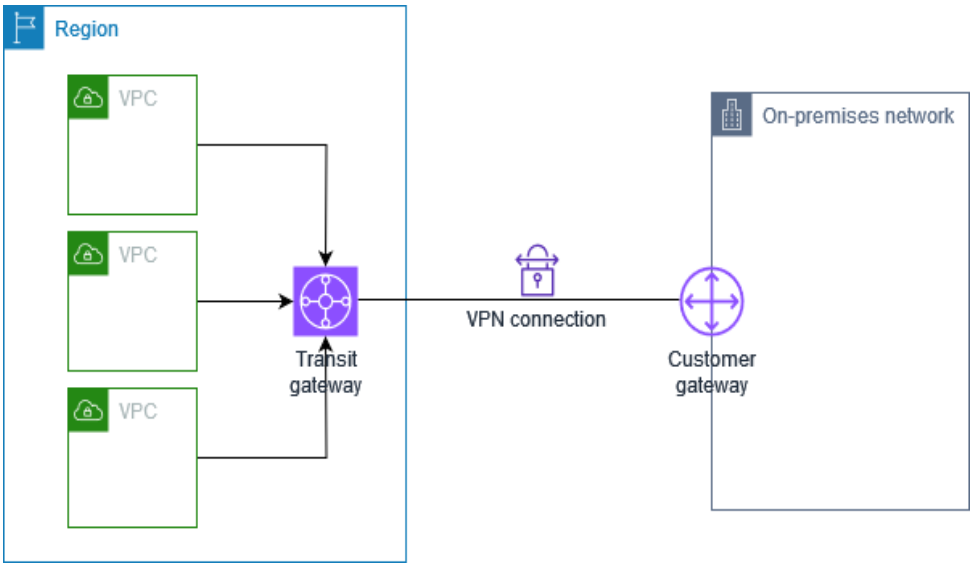
On-premises network: *This is your own network that exists outside of the AWS cloud.*

Customer Gateway: *this is a physical or virtual appliance located on your on-premises network that terminates the VPN tunnel on the customer side.*

Virtual Private Gateway: *This is the AWS component that terminates the VPN tunnel on the AWS side. It acts as a gateway or entry point for traffic moving between your VPC and your on-premises network.*

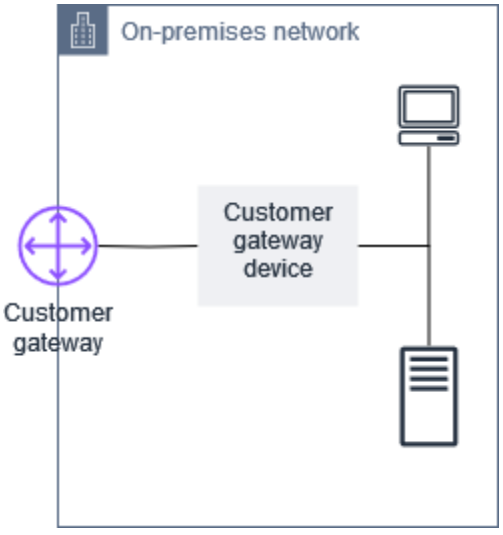


TRANSMIT GATEWAY:- *A transit gateway is a transit hub that you can use to interconnect your VPCs and your on-premises networks. The following diagram shows a VPN connection between multiple VPCs and your on-premises network using a transit gateway. The transit gateway has three VPC attachments and a VPN attachme*



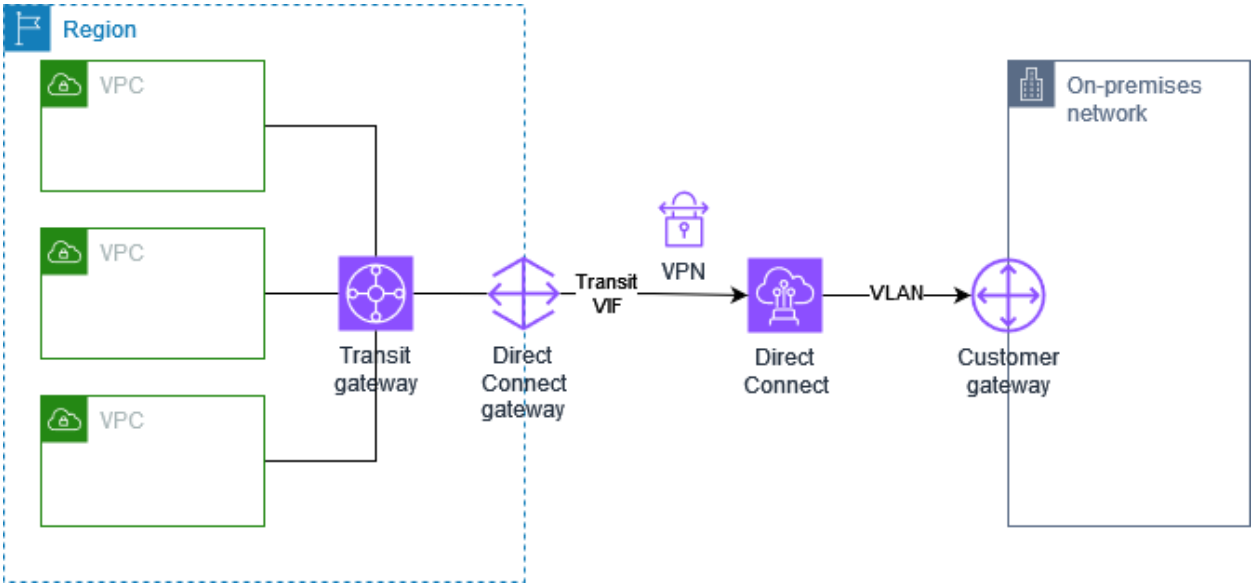
2)A customer gateway device:- *A customer gateway device is a physical device or software application on your side of the Site-to-Site VPN connection.*

3) A customer gateway:- *A customer gateway is a resource that you create in AWS that represents the customer gateway device in your on-premises network*



Private IP Site-to-Site VPN connection with AWS Direct Connect:-

With a private IP Site-to-Site VPN you can encrypt AWS Direct Connect traffic between your on-premises network and AWS without the use of public IP addresses. Private IP VPN over AWS Direct Connect ensures that traffic between AWS and on-premises networks is both secure and private, allowing customers to comply with regulatory and security mandates.



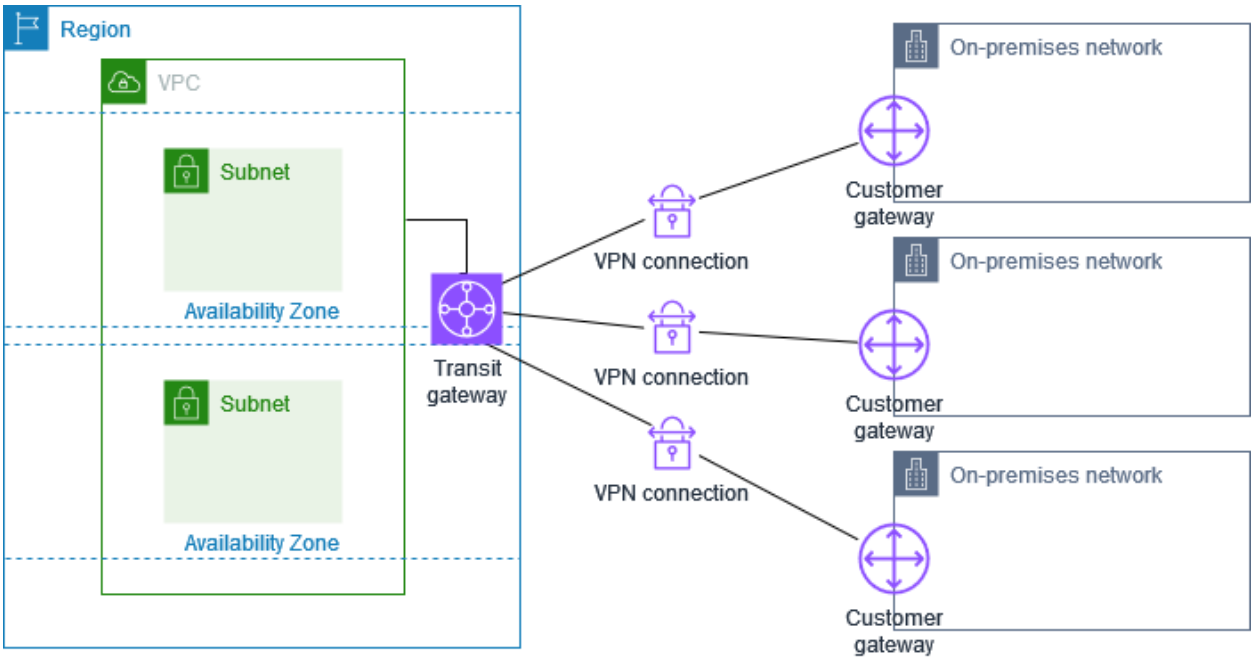
Benefits of Private IP Site-to-Site VPN:

Enhanced Security: Encrypts traffic between your on-premises network and AWS using private IP addresses, adhering to stricter security and regulatory compliance requirements.

Centralized Management: Transit Gateway simplifies managing multiple VPN and Direct Connect connections.

Multiple Site-to-Site VPN connections with a transit gateway:-

The VPC has an attached transit gateway, and you have multiple Site-to-Site VPN connections to multiple on-premises locations



When you create multiple Site-to-Site VPN connections to a single transit gateway, you can configure a second customer gateway to create a redundant connection to the same external location.You can also use this scenario to create Site-to-Site VPN connections to multiple geographic locations and provide secure communication between sites.