BATCH : B107 AWS-DevOps

LESSON : **AWS**

DATE : 08.03.2023

SUBJECT : **VPC-3**

ZOOM GİRİŞLERİNİZİ LÜTFEN **LMS** SİSTEMİ ÜZERİNDEN YAPINIZ

VPC - Endpoints, Peering Connection

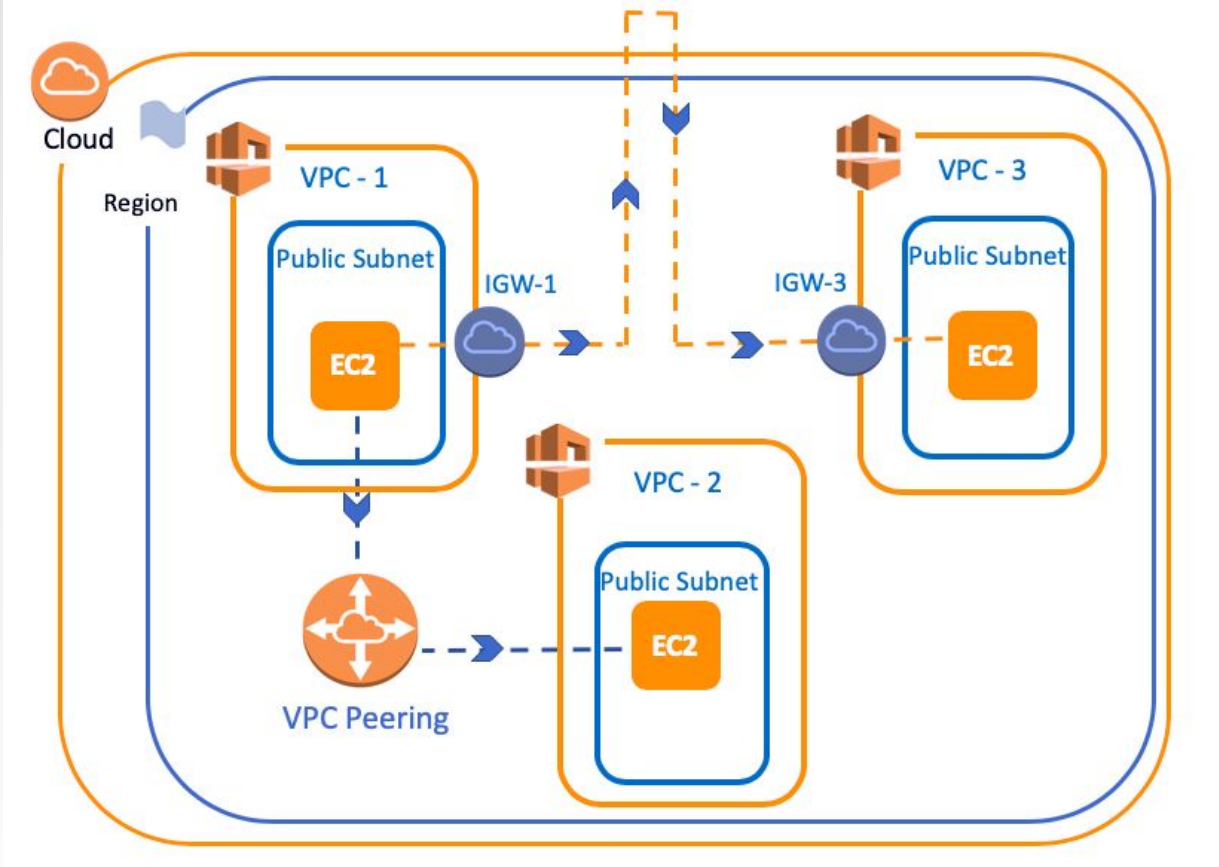
VPC Components

- ✔ **Subnet** — A segment of VPC's IP address range.
- ✔ **Route table** — A set of rules, called routes, that are used to determine where network traffic is directed.
- ✔ **Internet gateway** — A gateway that you attach to your VPC to enable communication between resources in your VPC and the internet.
- ✔ **Egress only Internet Gateway** — Internet Gateway for IPv6
- ✔ **CIDR block** — Classless Inter-Domain Routing.

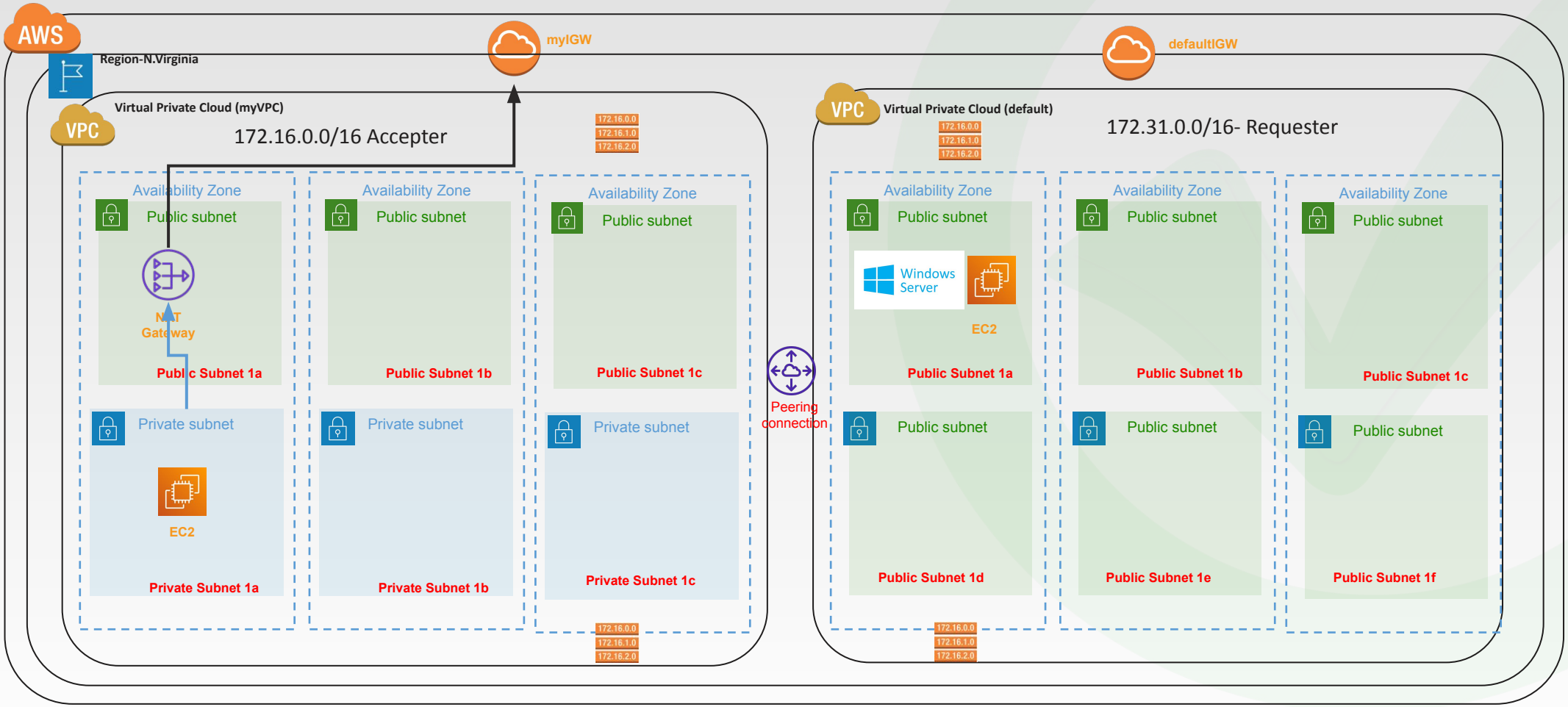
- ✔ **Elastic IP**
- ✔ **Bastion Host/ Jump Box**
- ✔ **NAT Gateway/ NAT Instance**

VPC Peering

- A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses.
- Instances in either VPC can communicate with each other as if they are within the same network.
- You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account. The VPCs can be in different regions (also known as an inter-region VPC peering connection).

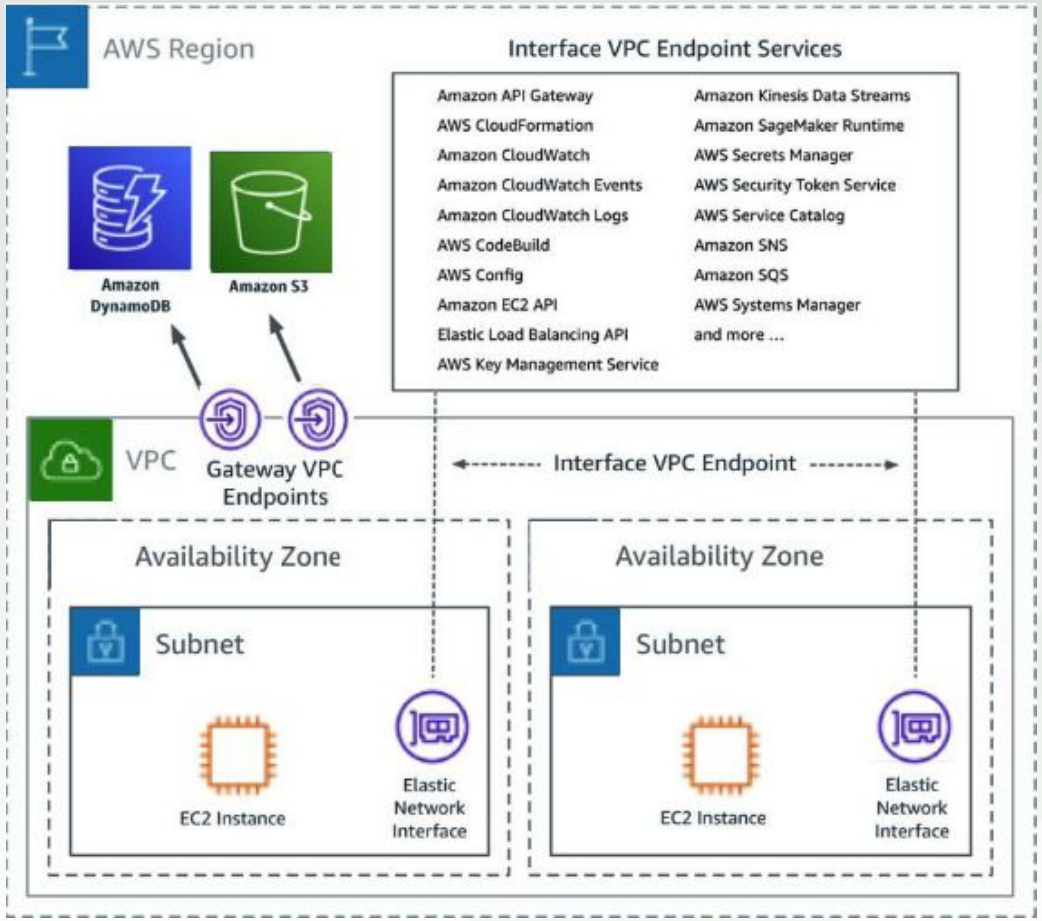


VPC Peering

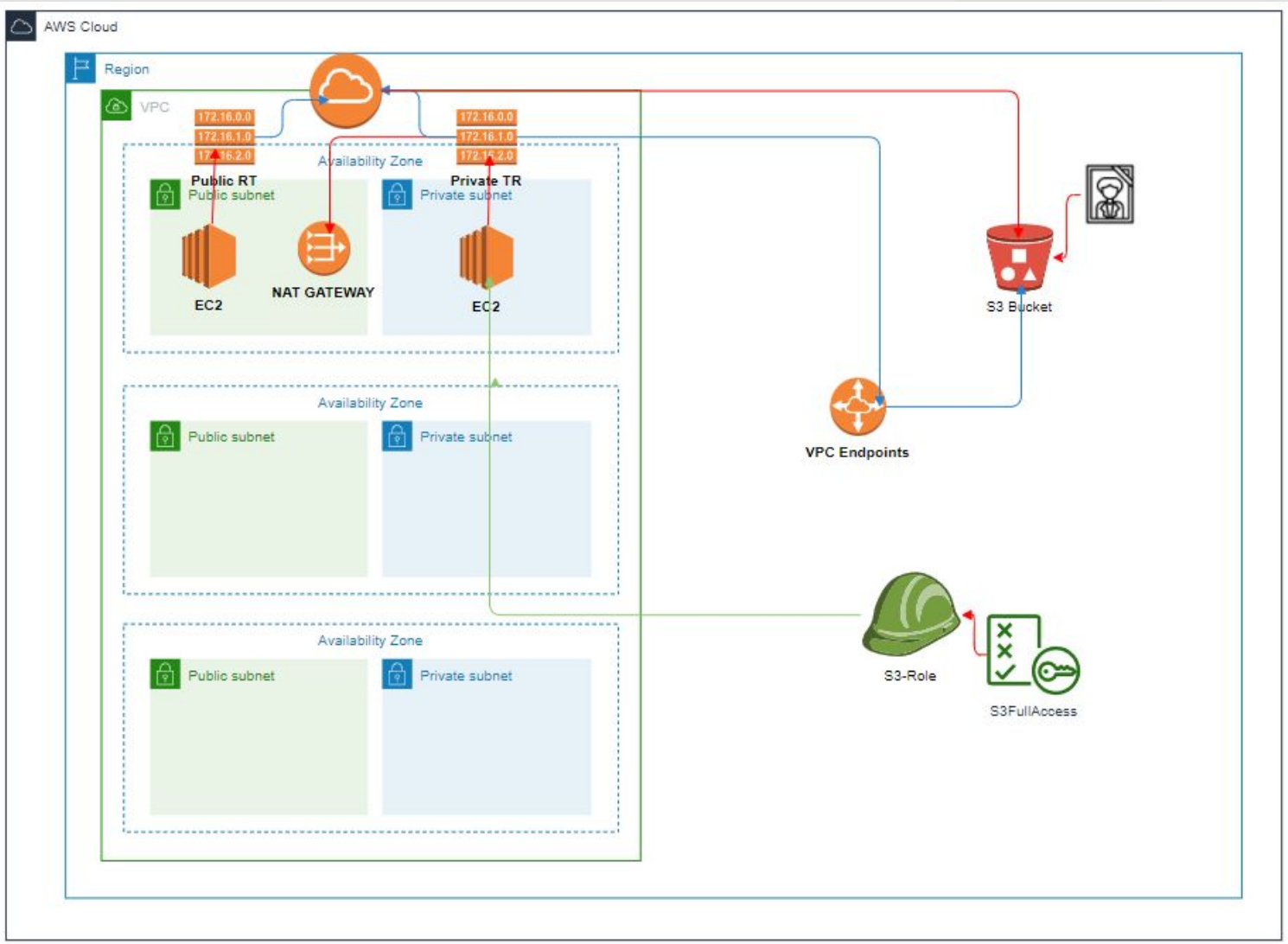

AWS
Region-N.Virginia
myIGW
defaultIGW
Virtual Private Cloud (myVPC)
VPC
172.16.0.0/16 Accepter
172.16.0.0
172.16.1.0
172.16.2.0
Availability Zone
Public subnet
NAT Gateway
Public Subnet 1a
Public Subnet 1b
Public Subnet 1c
Private subnet
EC2
Private Subnet 1a
Private Subnet 1b
Private Subnet 1c
Peering connection
Virtual Private Cloud (default)
172.31.0.0/16- Requester
Windows Server
EC2
Public Subnet 1d
Public Subnet 1e
Public Subnet 1f

VPC Endpoint

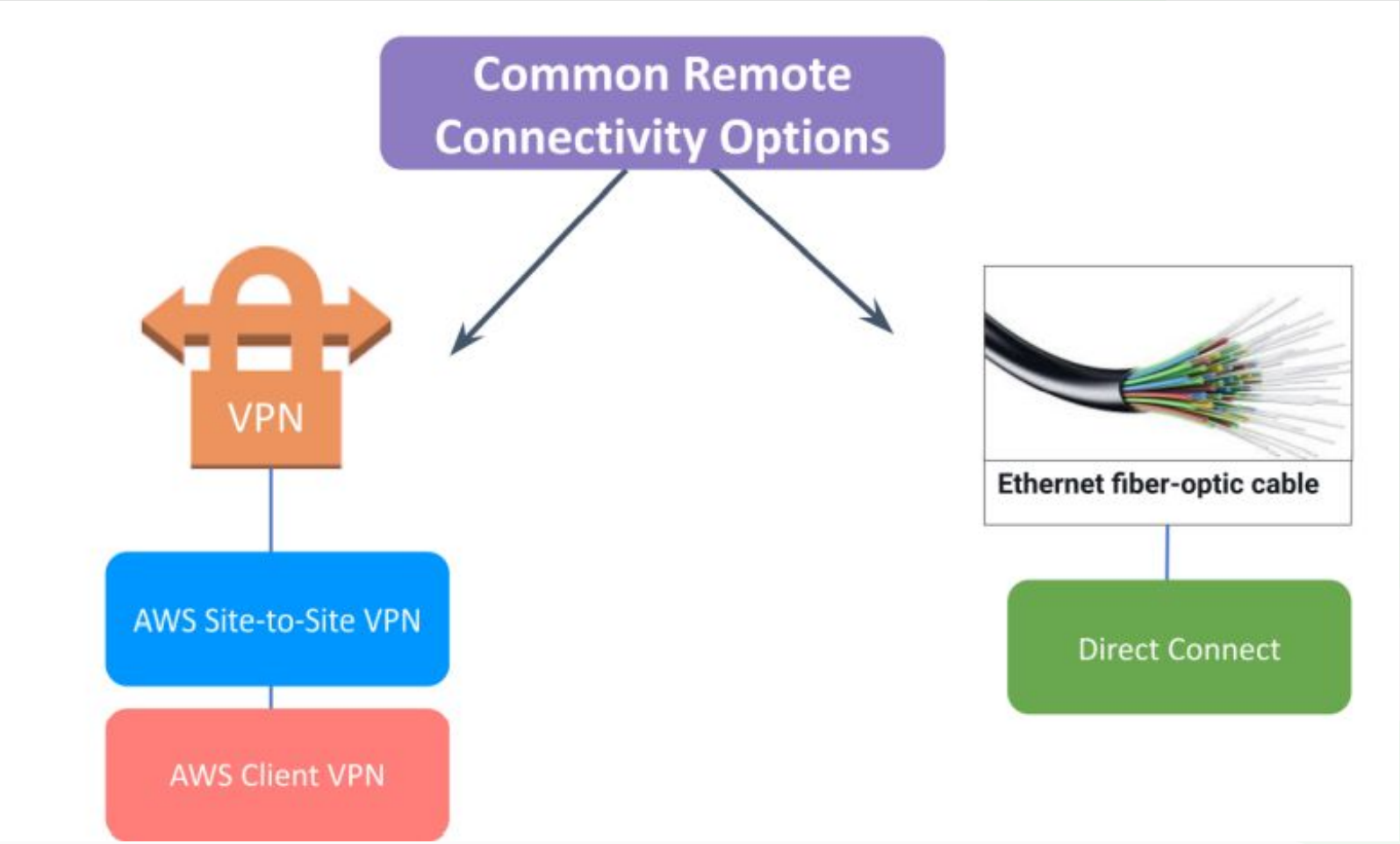
- A VPC endpoint enables customers to privately connect to supported AWS services. Amazon VPC instances do not require public IP addresses to communicate with resources of the service. **Traffic between an Amazon VPC and a service does not leave the Amazon network.**
- VPC endpoints are virtual devices. They are horizontally scaled, redundant, and highly available Amazon VPC components that allow communication between instances in an Amazon VPC and services. There are two types of VPC endpoints:
  a. Interface endpoints
     i. Connect to services over PrivateLink, uses private IP
     ii. Should attach Security Group
     iii. $ per hour + $ per GB of data processed
  b. Gateway endpoints
     i. Targets routes on route tables
     ii. Supports S3, DynamoDB
     iii. Free



VPC Endpoint



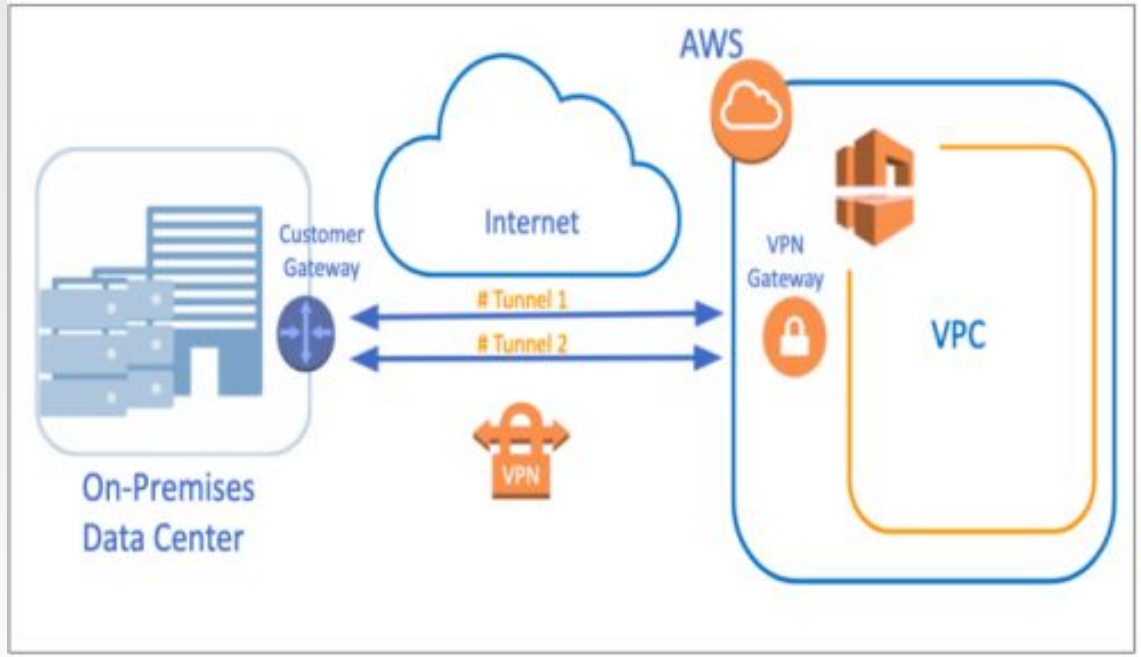
VPN & Direct Connect



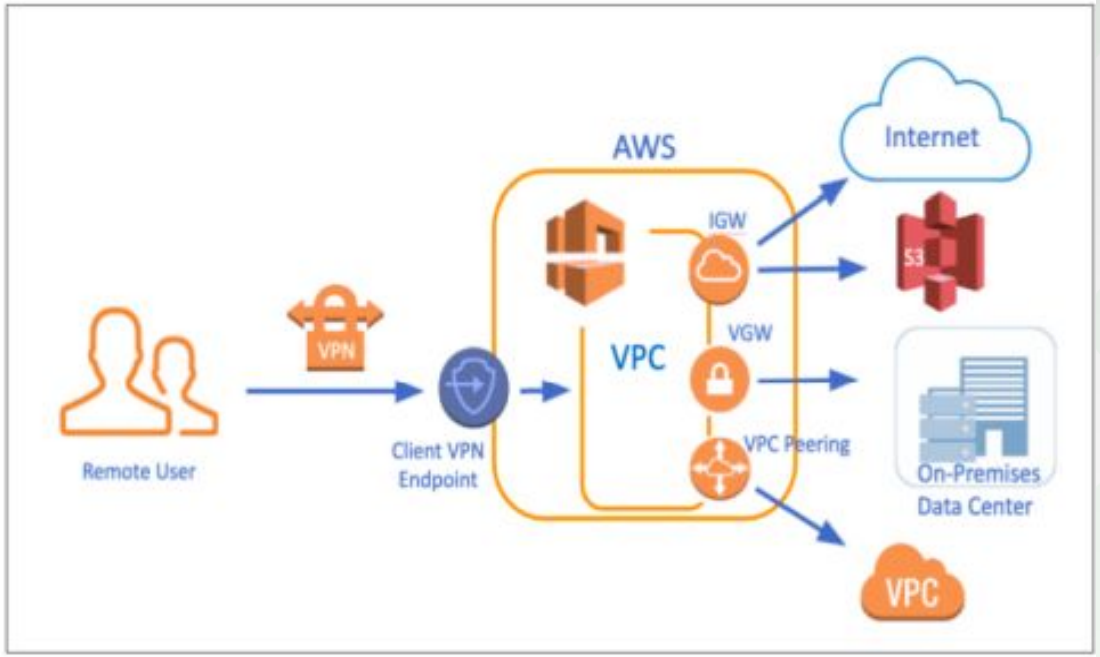
VPN & Direct Connect

VPN Connections

AWS Site-to-Site VPN

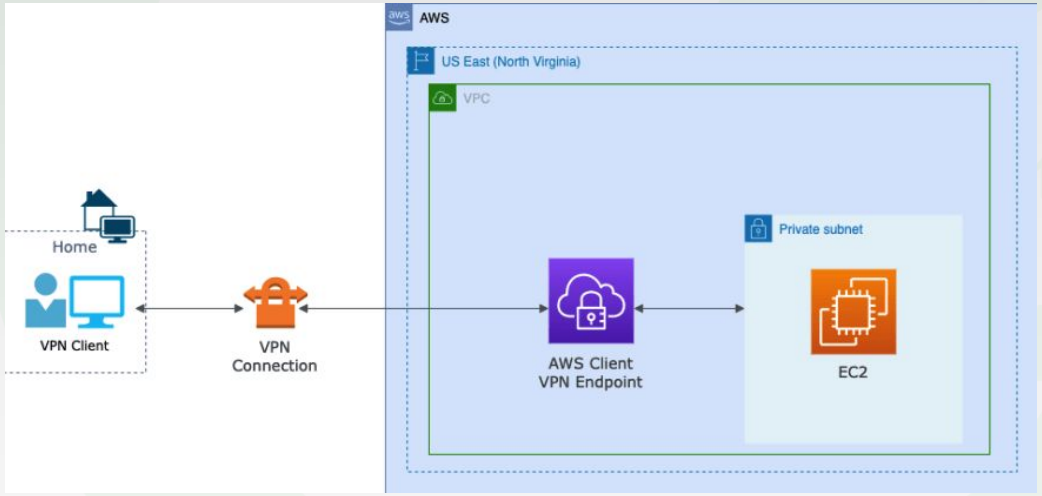


AWS Client VPN



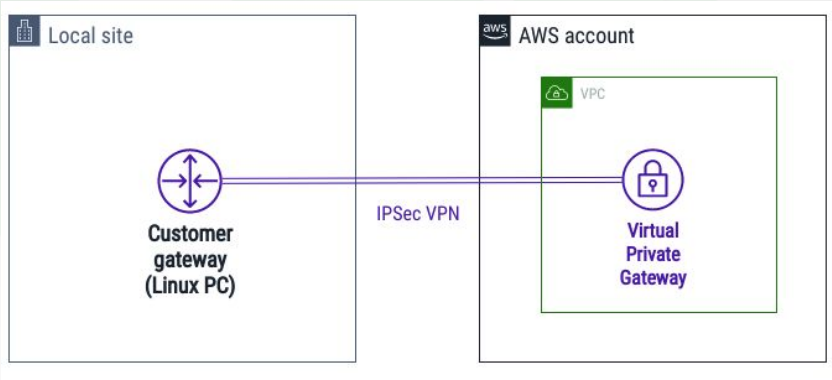
VPN & Direct Connect

- **AWS Client VPN**
- A managed client-based VPN service that enables you to securely access AWS resources and resources in your on-premises network.
- Key Components are
  a. Client VPN endpoint
  b. VPN client application
  c. Client VPN endpoint configuration file



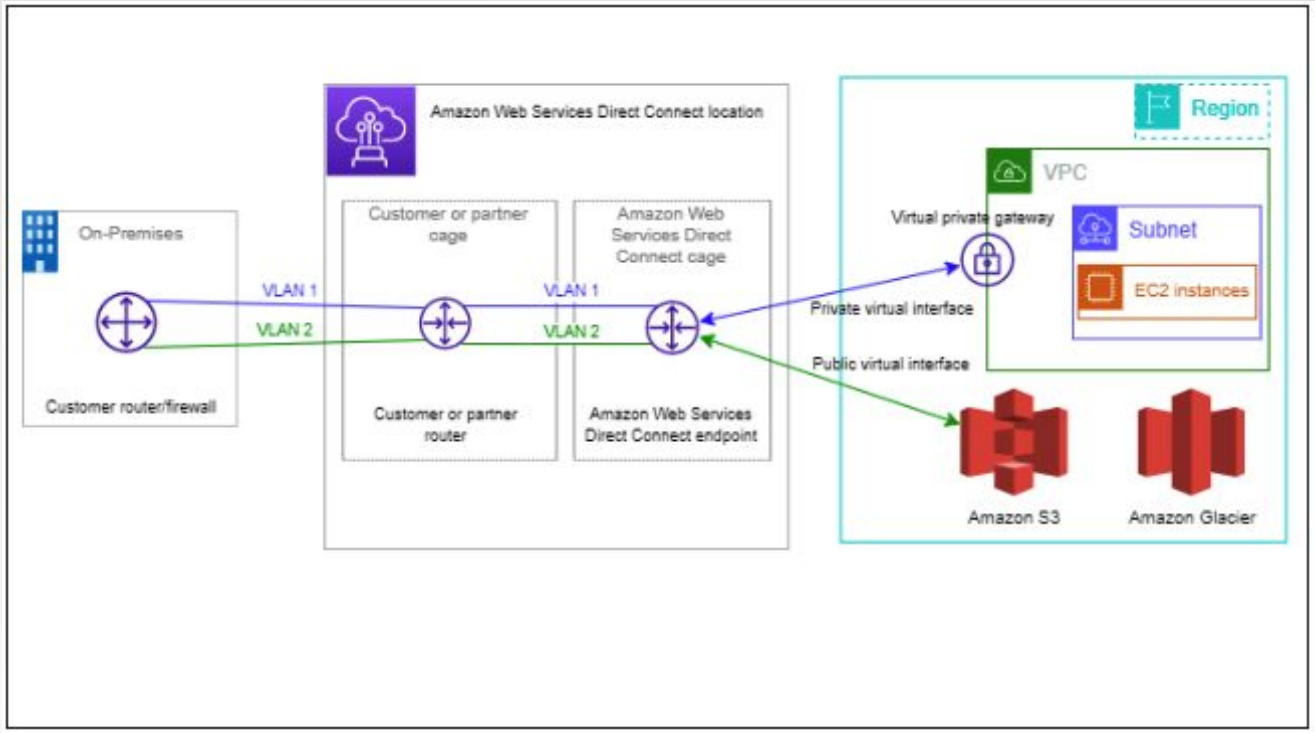
VPN & Direct Connect

- **AWS Site-to-Site VPN**
- By default, instances that you launch into an Amazon VPC can't communicate with your own (remote) network. You can enable access to your remote network from your VPC by creating an AWS Site-to-Site VPN (Site-to-Site VPN) connection, and configuring routing to pass traffic through the connection.
- Internet
- Encryption
- Key Concepts:
    a. VPN Tunnel
    b. Customer gateway
    c. Customer gateway device
    d. Virtual private gateway
    e. Transit gateway



VPN & Direct Connect

- **AWS Direct Connect**
- AWS Direct Connect links your internal network to an AWS Direct Connect location over a standard Ethernet fiber-optic cable. One end of the cable is connected to your router, the other to an AWS Direct Connect router. With this connection, you can create virtual interfaces directly to public AWS services (for example, to Amazon S3) or to Amazon VPC, **bypassing internet service providers** in your network path.
- Key Components:
    a. Connections
    b. Virtual Interfaces



Solution Architect Cases

1 Your organization has a pre-production VPC and production VPC. You need to be able to setup routing between these VPCs using private IP addresses.
What solution do you suggest?

Create VPC Peering between VPCs

2 Several remote office locations should be connected to an Amazon VPC over internet connection with full encryption. What do you suggest?

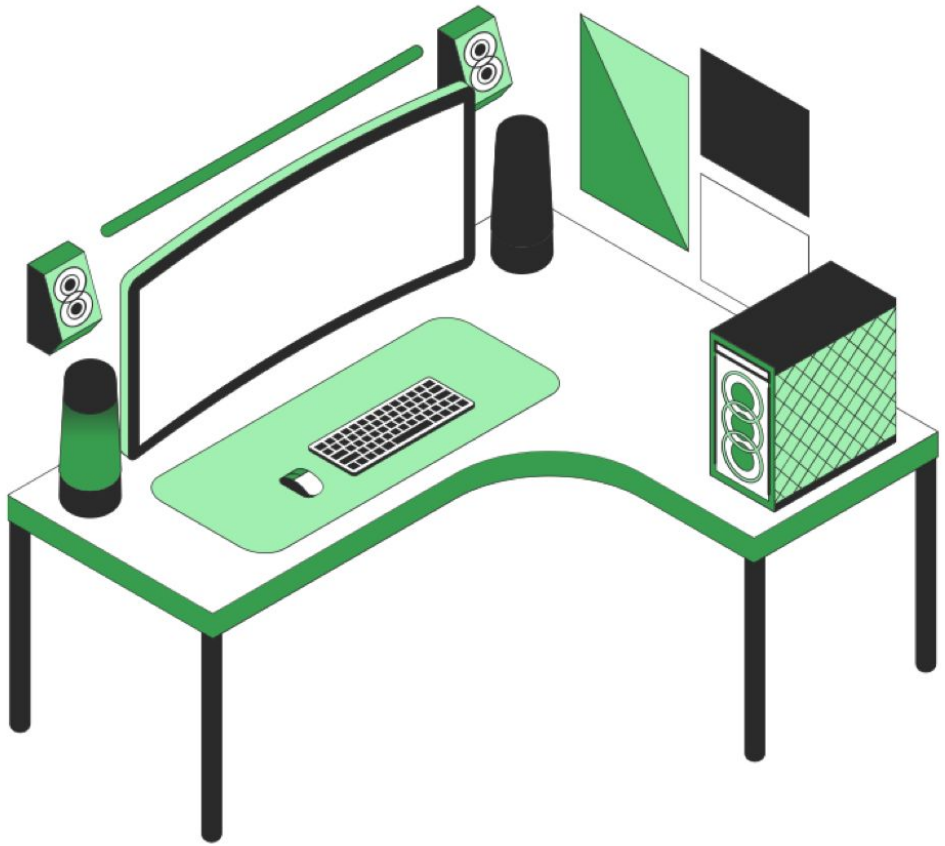
Create Site-to-Site VPN connection

3 You need to set up a dedicated connection between your on-premises corporate datacenter and AWS Cloud. This connection must be private, consistent, and traffic must not travel through the Internet. What do you suggest?

AWS Direct Connect

4 When using VPC Endpoints, what are the only two AWS services that have a Gateway Endpoint available?

S3 and DynamoDB



Do you have any questions?

Send it to us! We hope you learned something new.