BATCH : 149

LESSON : AWS

DATE : 28.08.2023

SUBJECT : AWS VPC-3

techproeducation

techproeducation

techproeducation

techproeducation

techproedu

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.

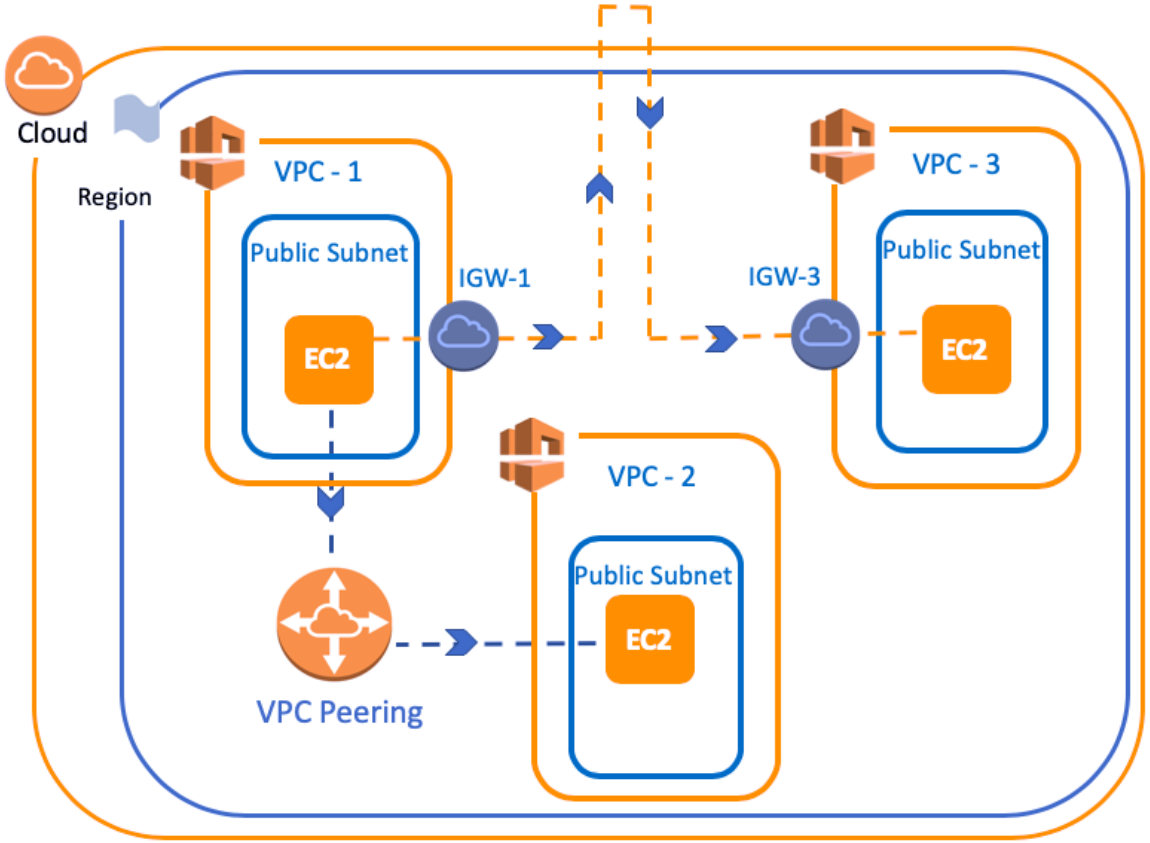
- ✔ **Elastic IP**
- ✔ **Bastion Host/ Jump Box**
- ✔ **NAT Gateway/ NAT Instance**

Amazon VPC-3

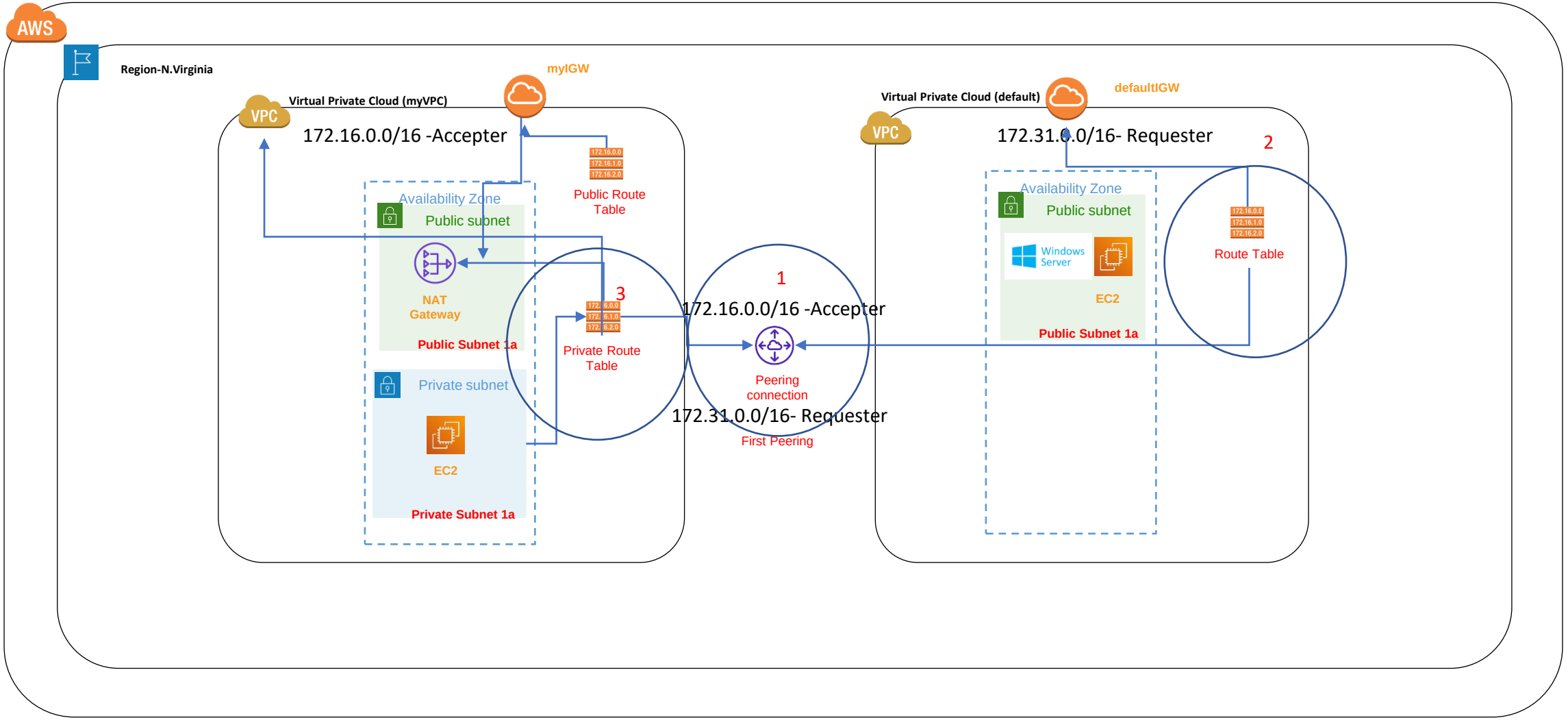
VPC - Endpoints, Peering Connection

VPC Peering

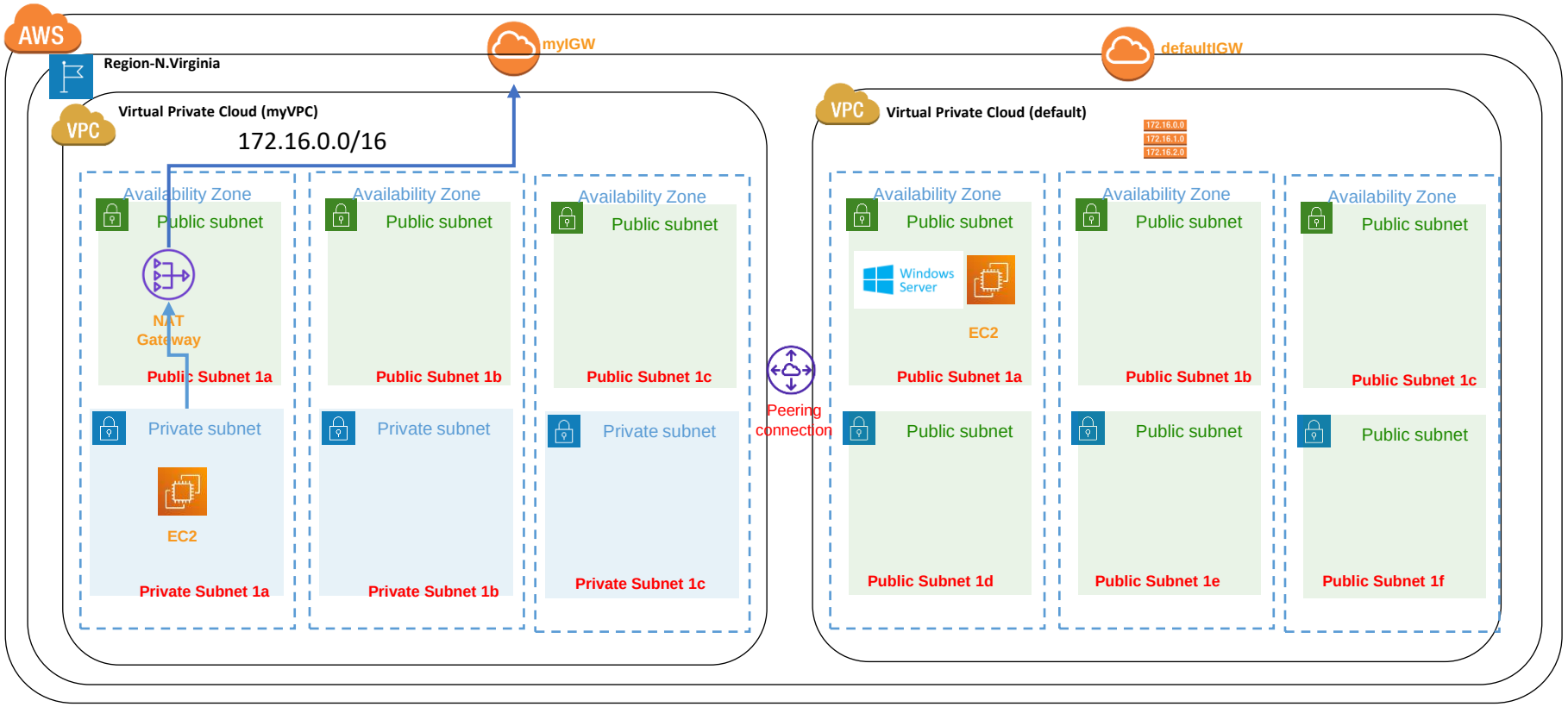
- ✓ A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection 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).



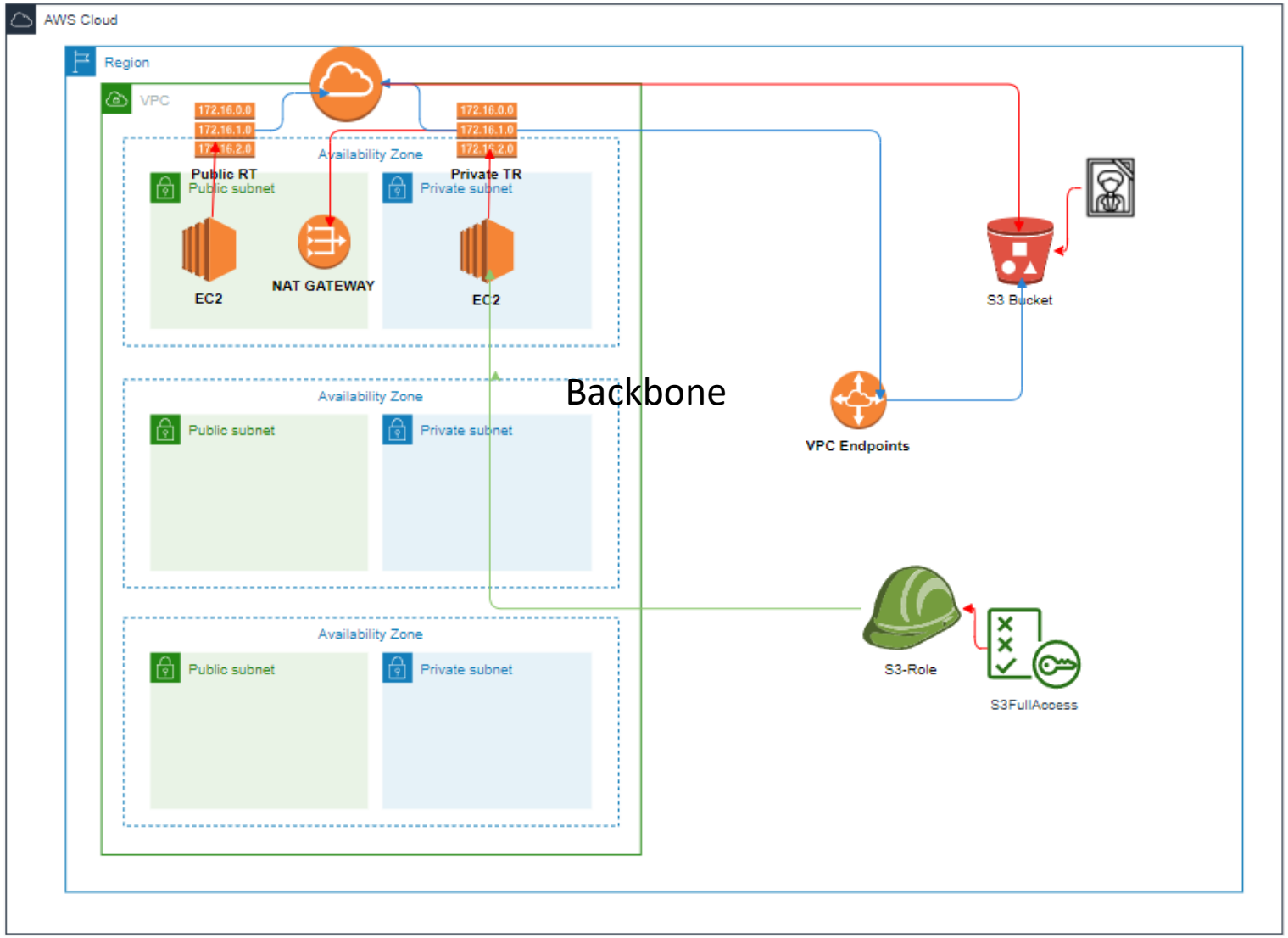
VPC Peering


AWS
Region-N.Virginia
myIGW
Virtual Private Cloud (myVPC)
VPC
172.16.0.0/16 -Accepter
Public Route Table
Availability Zone
Public subnet
NAT Gateway
Public Subnet 1a
Private Route Table
Private subnet
EC2
Private Subnet 1a
3
1
172.16.0.0/16 -Accepter
Peering connection
172.31.0.0/16- Requester
First Peering
Virtual Private Cloud (default)
defaultIGW
VPC
172.31.0.0/16- Requester
2
Availability Zone
Public subnet
Windows Server
EC2
Public Subnet 1a
Route Table

VPC Peering

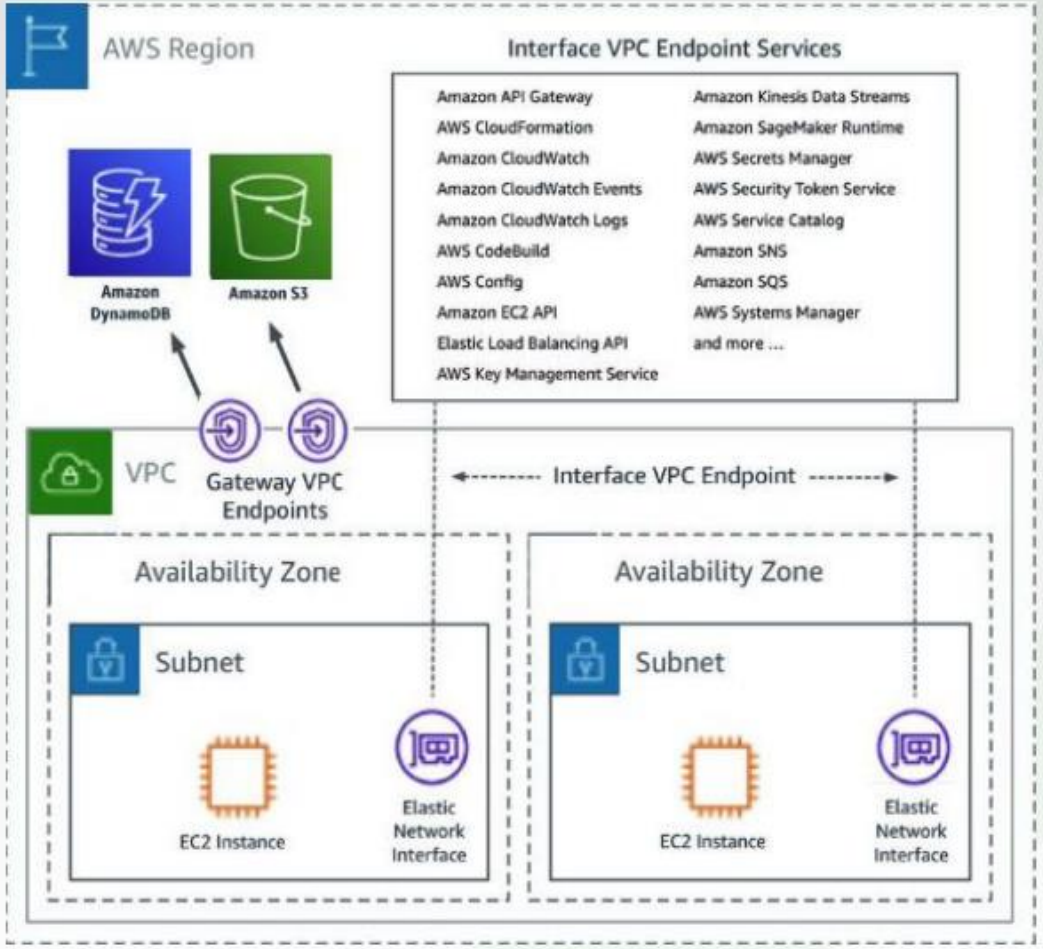

AWS
Region-N.Virginia
myIGW
defaultIGW
VPC
Virtual Private Cloud (myVPC)
172.16.0.0/16
VPC
Virtual Private Cloud (default)
172.16.0.0
172.16.1.0
172.16.2.0
Availability Zone
Public subnet
NAT Gateway
Public Subnet 1a
Public Subnet 1b
Public Subnet 1c
Private subnet
EC2
Private Subnet 1a
Private Subnet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

VPC Endpoint

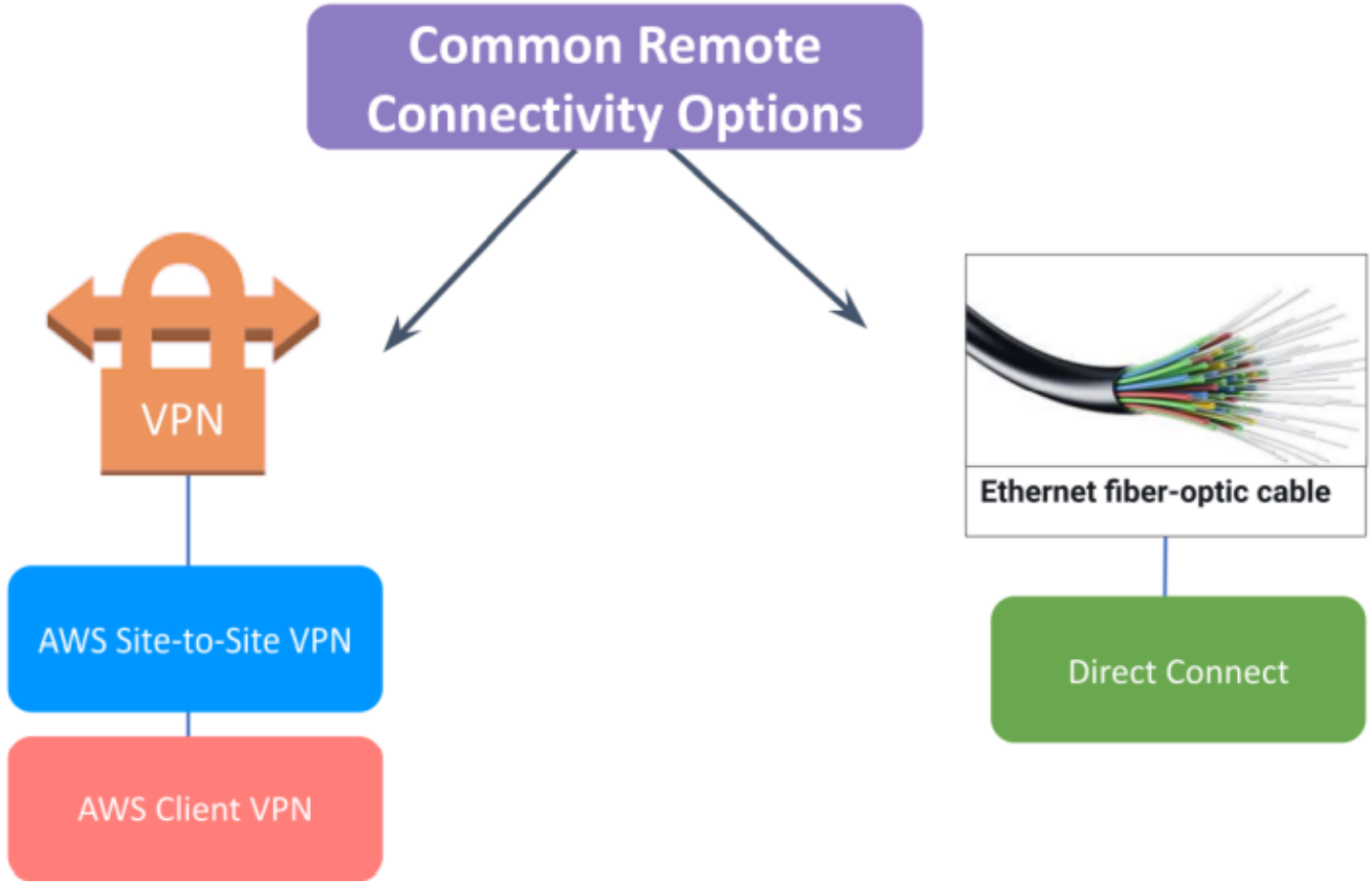


VPC Endpoint

- 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



VPN & Direct Connect



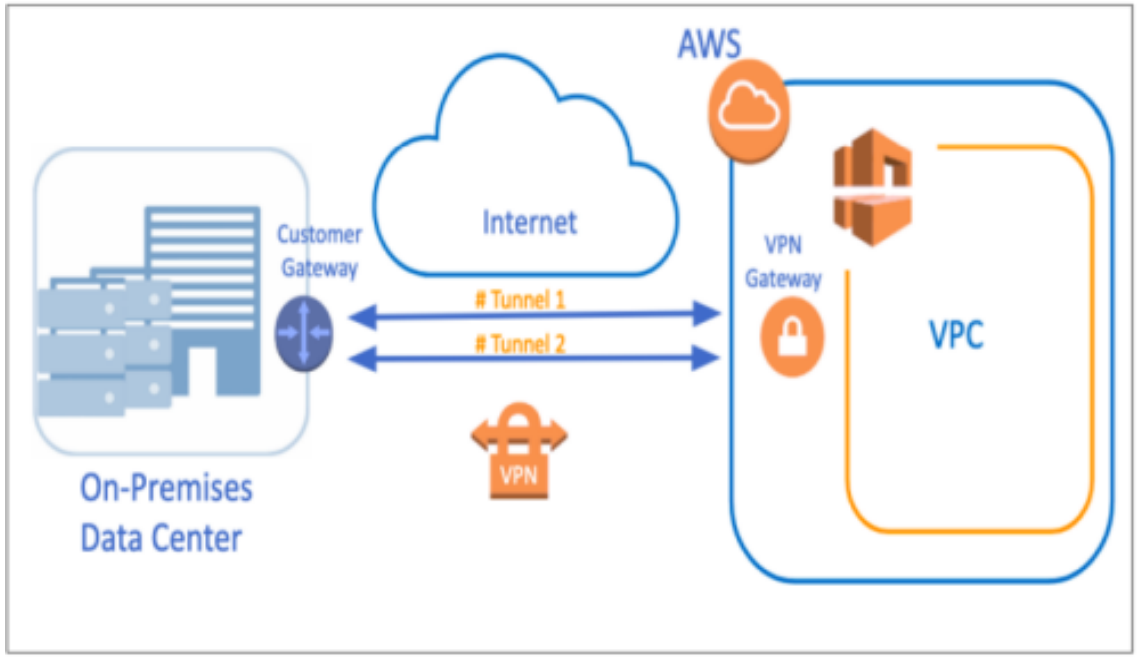
VPN & Direct Connect

- **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

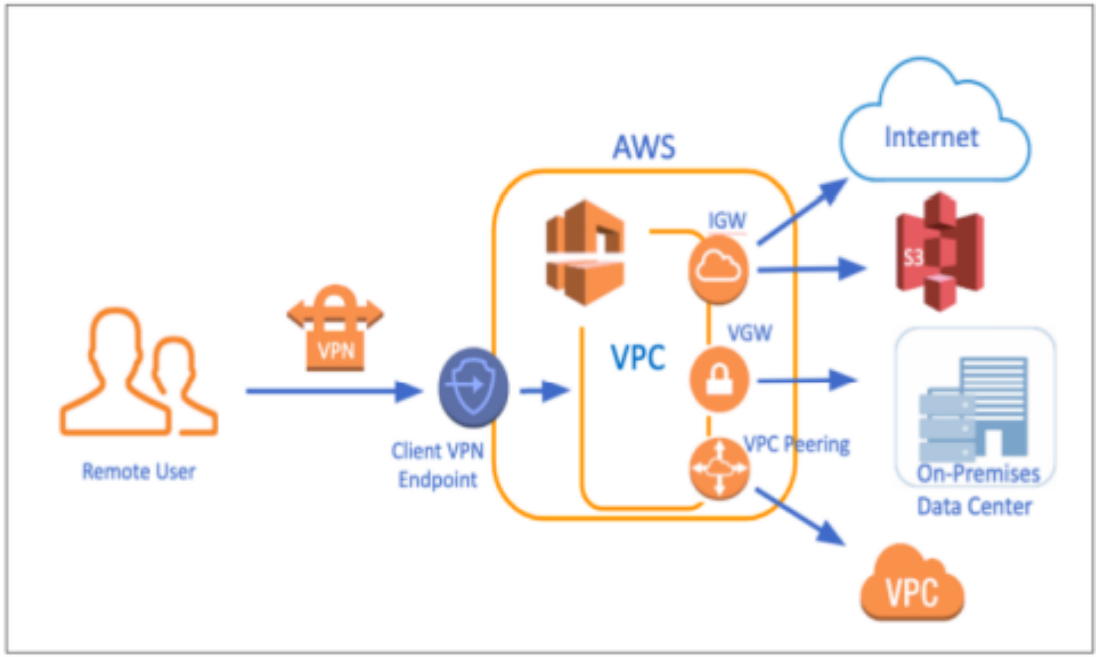
VPN

VPN Connections

AWS Site-to-Site VPN

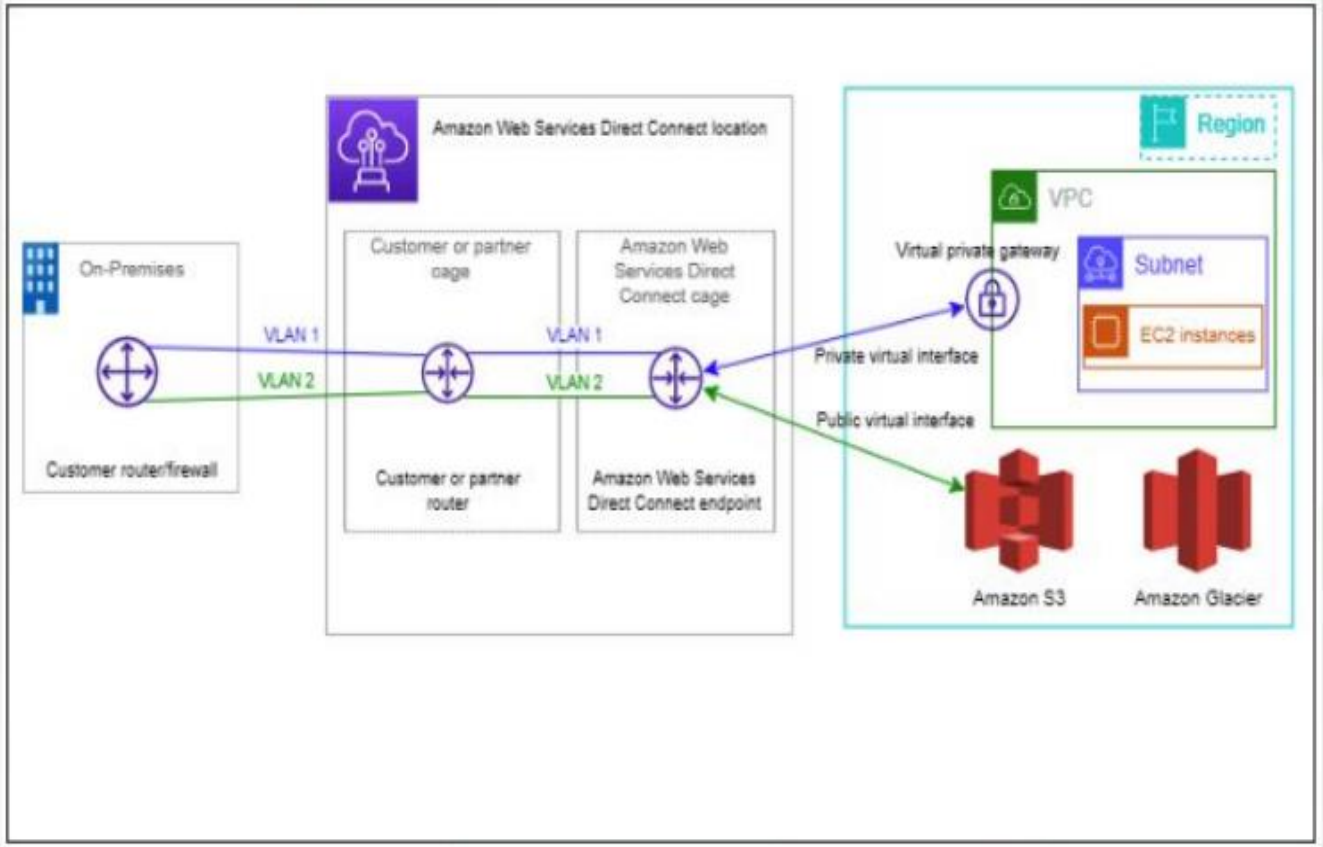


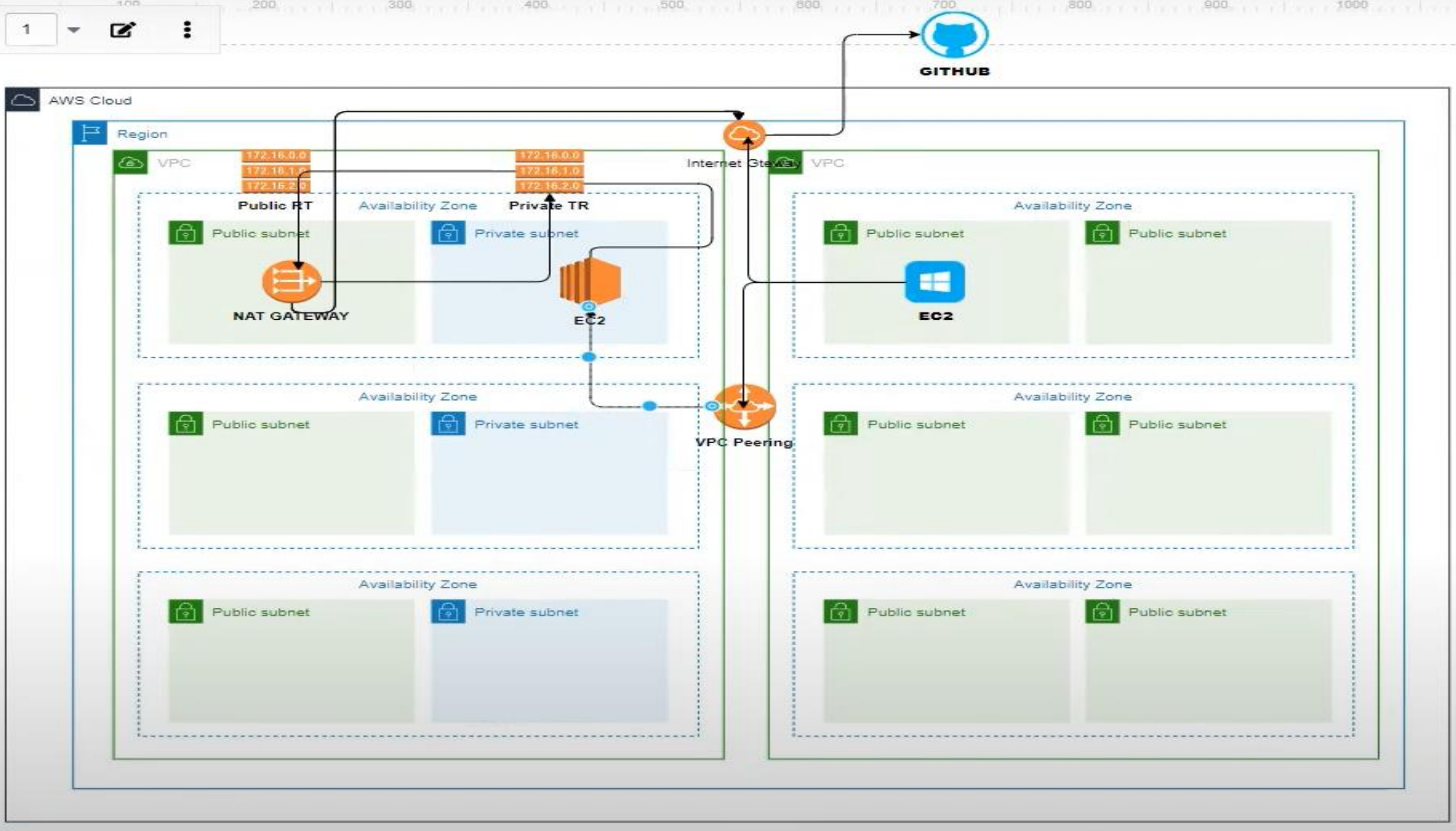
AWS Client VPN



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




GITHUB
AWS Cloud
Region
VPC
172.16.0.0
172.16.1.0
172.16.2.0
Public RT
Availability Zone
Public subnet
Private subnet
NAT GATEWAY
EC2
Private TR
Internet Gateway
VPC
Availability Zone
Public subnet
Public subnet
EC2
Availability Zone
Public subnet
Private subnet
VPC Peering
Availability Zone
Public subnet
Public subnet
Availability Zone
Public subnet
Private subnet
Availability Zone
Public subnet
Public subnet

NAT Gateway

VPC Peering

Edit routes

Destination	Target	Status	Propagated
10.7.0.0/16	local	active	No
0.0.0.0/0	nat-0ded7d8a9439d336d	active	No
172.31.0.0/16	pcx-0ecbf98754b602517	active	No
0.0.0.0/0	igw-0416e7d5a8d836388		No

Add route

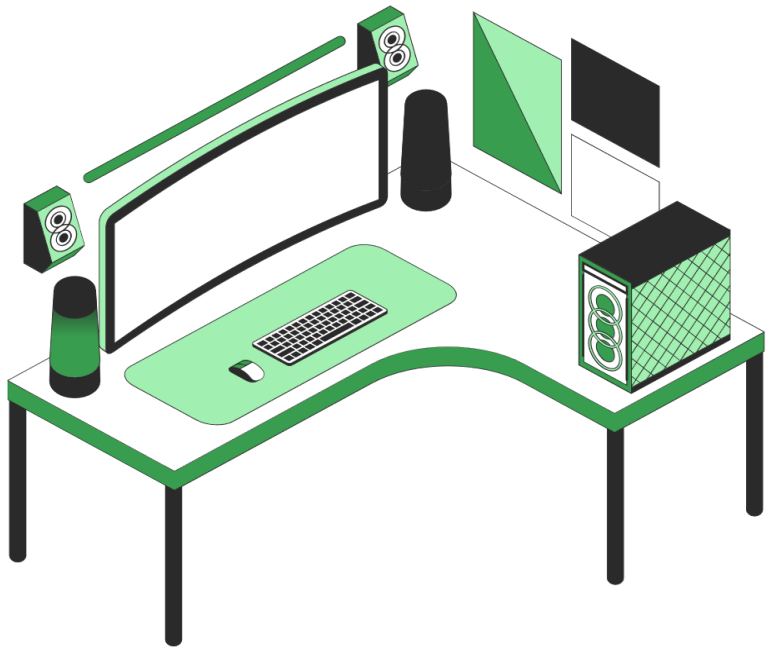
* Required

Cancel Save routes

Route Tables

Internet Gateway

VPC Endpoint



Do you have any questions?

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