Contents

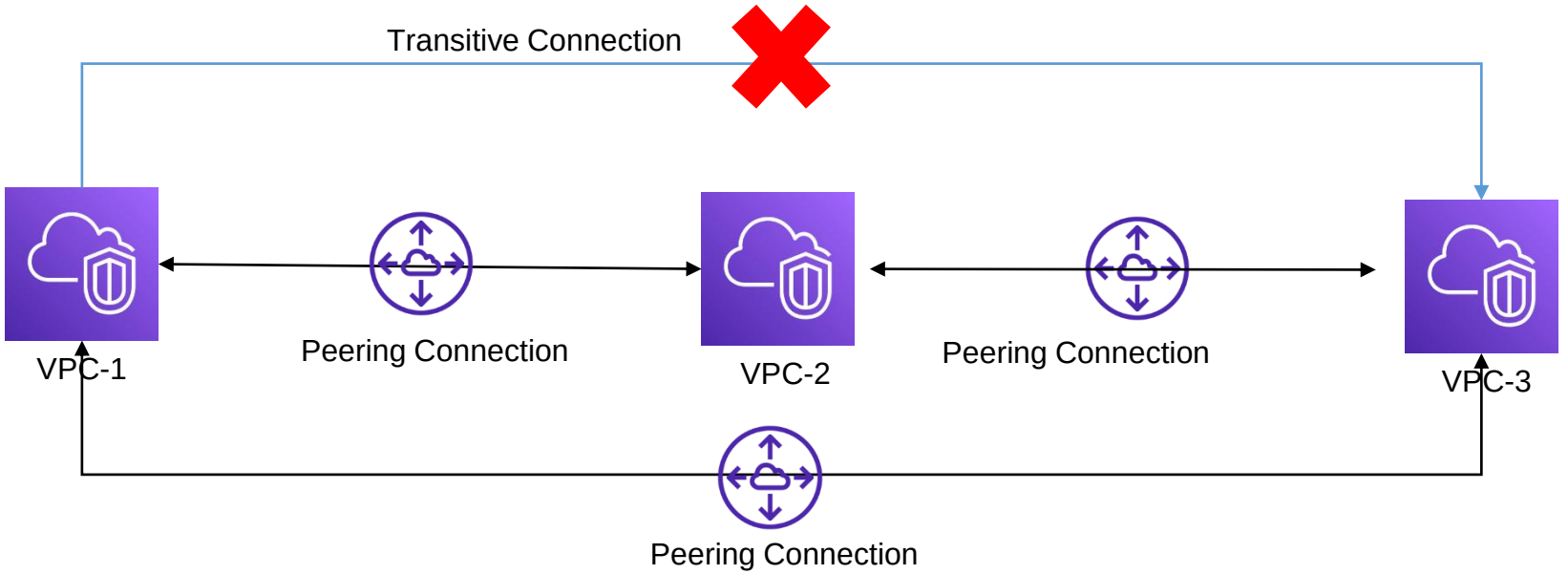
- VPC Peering
- VPC Endpoint
- AWS Privatelink
- VPN, VPN CLoudHub, Direct Connect (DX)
- Transit Gateway
- Global Accelerator
- Data Transfer Cost in AWS

VPC peering

VPC peering

- Connect two VPCs based on AWS network (privately)
- Resources in these VPCs communicate with others as same network (Using private IP)
- VPC CIDR is not overlapped
- Peering connection is not transitive
- Peering connection can setup with the VPC in difference regions, AWS account

VPC peering (cont.)

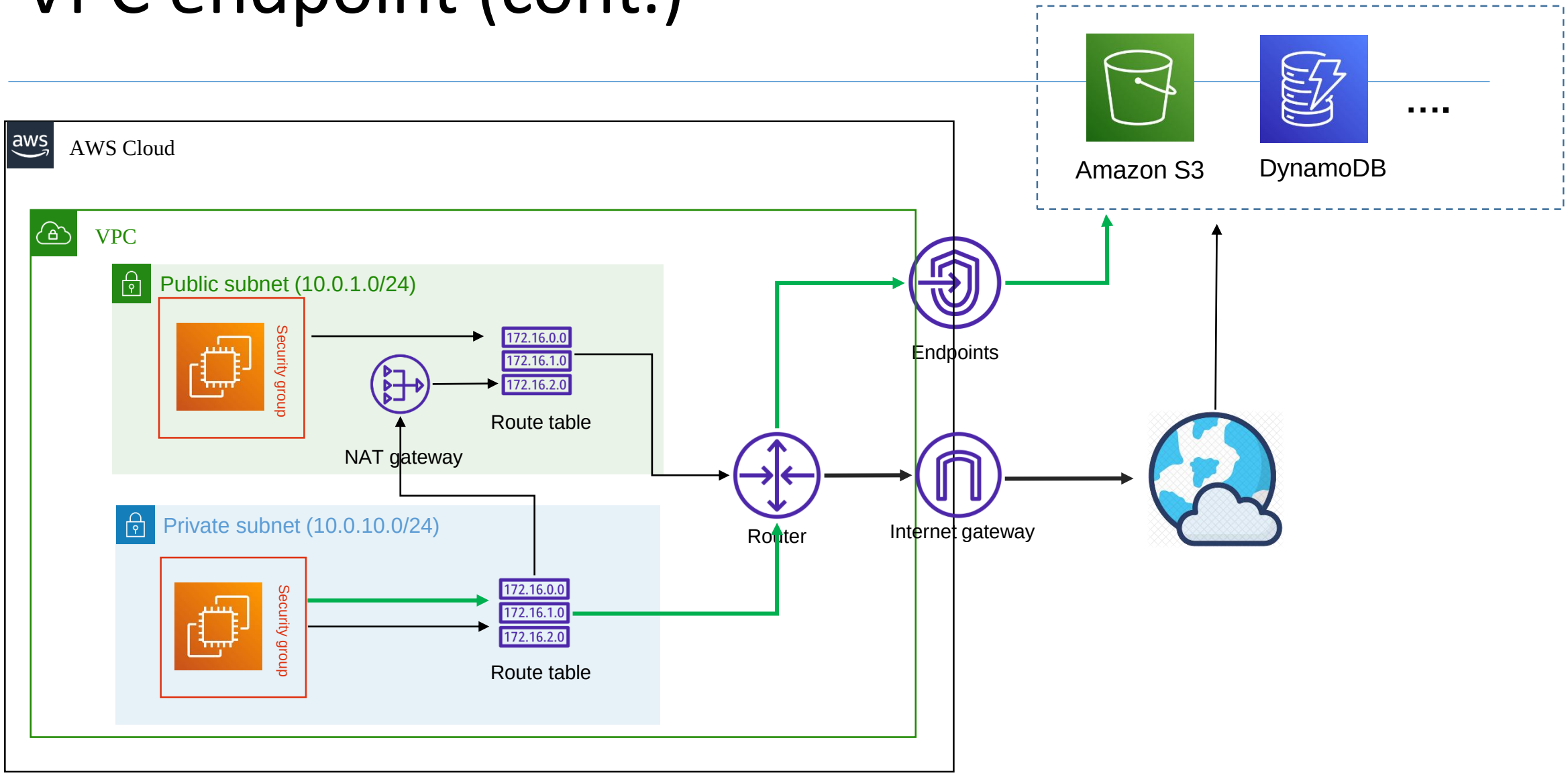


VPC endpoint

VPC endpoint

- Endpoints allow you to privately connect your VPC to supported AWS services using AWS network
- Auto scaling and high availability
- No need NAT gateway, IGW, Public IP… to access AWS services

VPC endpoint (cont.)



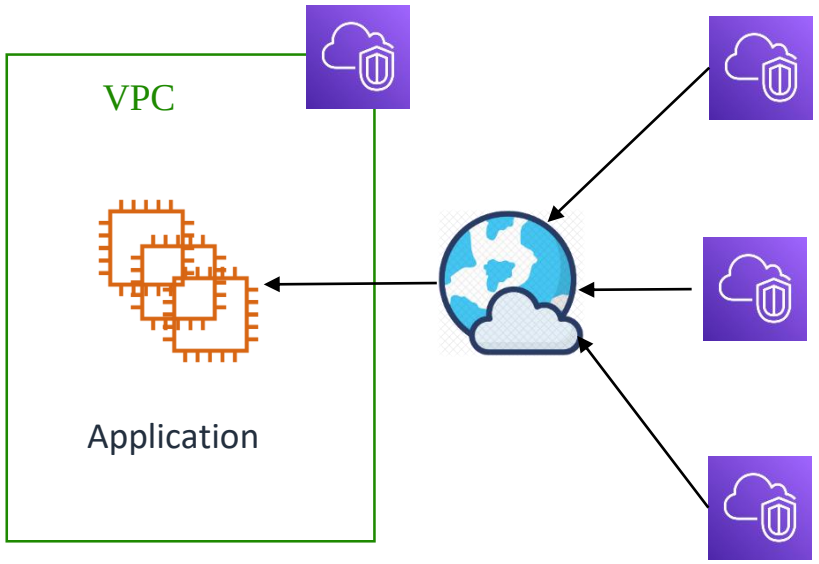
VPC endpoint type

- **Gateway endpoint**
  - Using for **DynamoDB and S3** only
  - Need to configure Route Table
- **Interface Endpoint**
  - For the rest supported services
  - Provision ENI with private IP address as an entry point for services

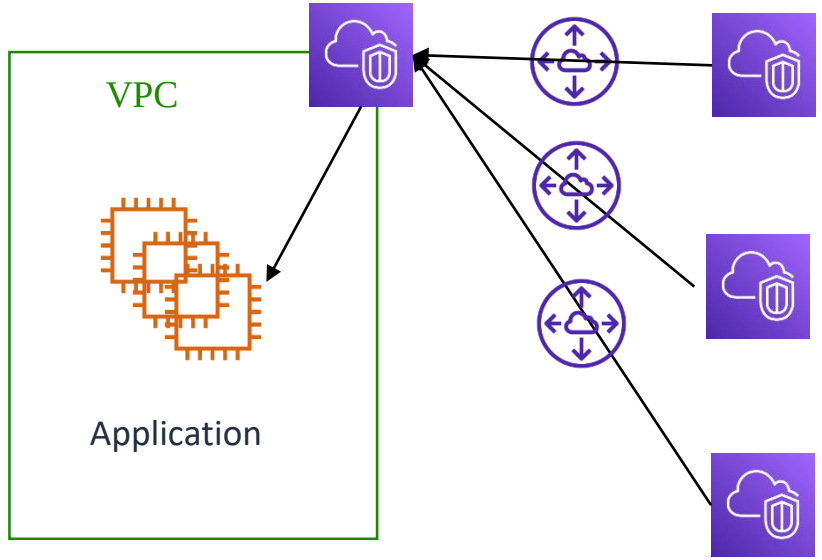
AWS Privatelink

How to expose service to another VPC

- **Option 1**: Via internet
  - Unsercure
  - Need to manage many things (Firewall, DDoS…)

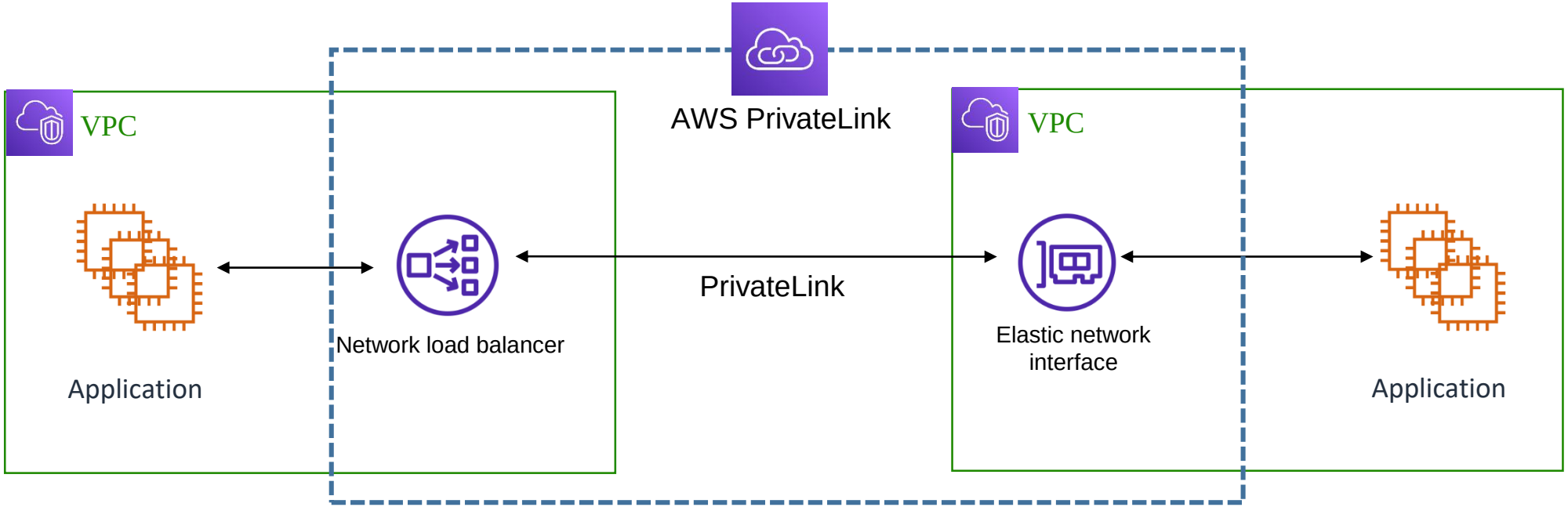


- **Option 2**: Via Peering connection
  - Need to many peering connections
  - Expose all resources, not only application service



How to expose service to another VPC (cont.)

- **Option 3**: Via AWS privatelink
  - Sercure, Private
  - No need to manage many things (VPC peering, IGW, Route Table…)
  - Need to create Network Load Balancer and ENI

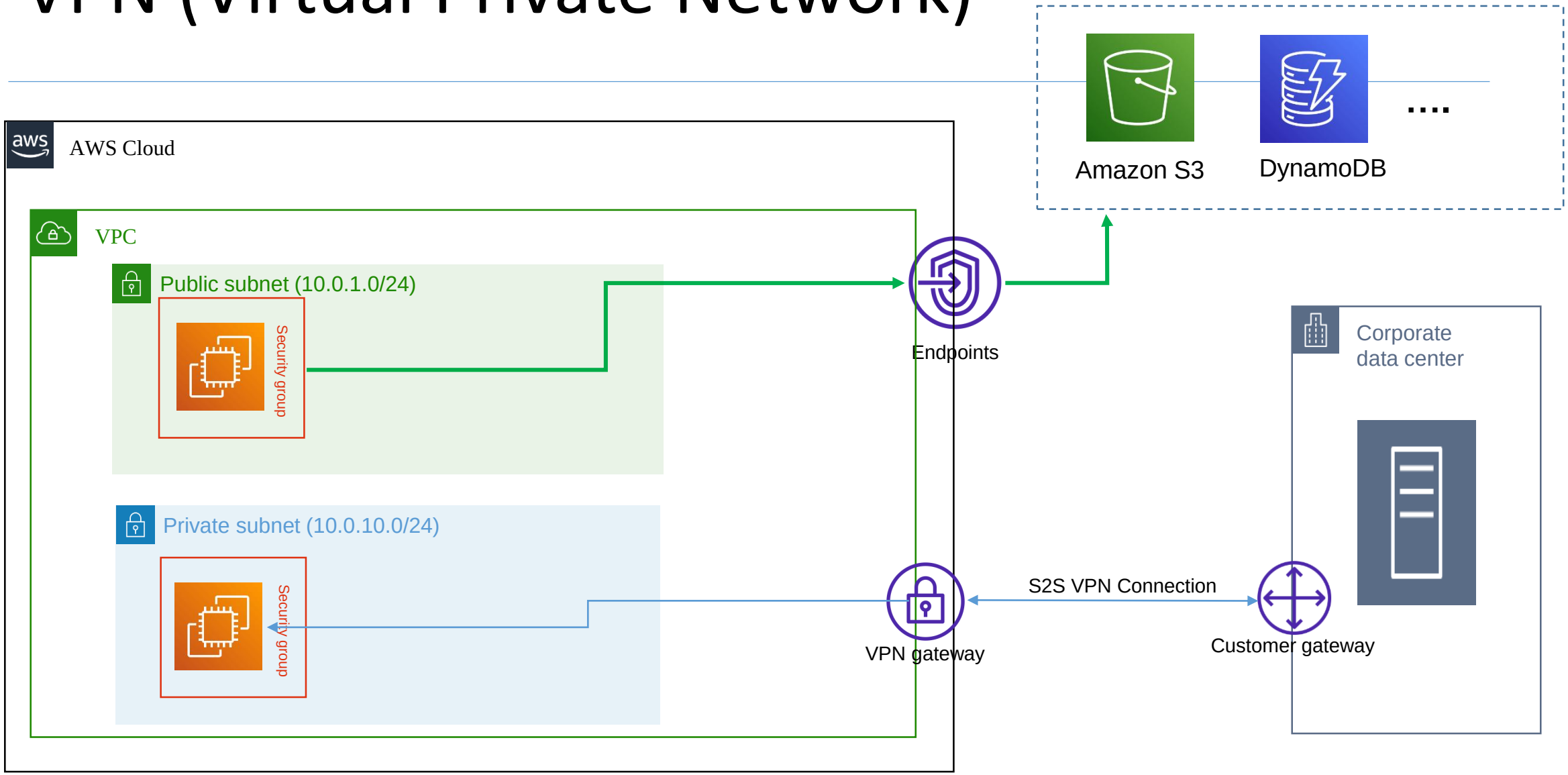


Exam Tips

- Expose services to thousand of VPC => AWS privatelink
- No need VPC peering, no Route Table, NAT, IGW, etc.
- Need Network Load Balancer (NLB) and ENI in the customer VPC

VPN, VPN Cloud Hub

VPN (Virtual Private Network)



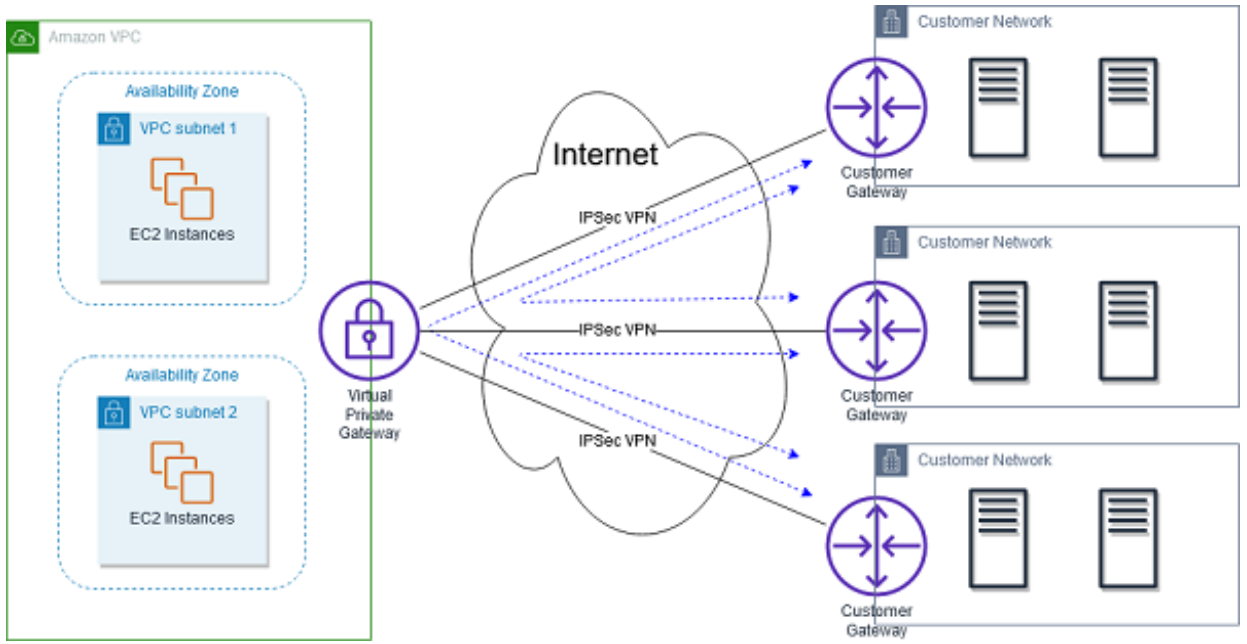
AWS Site-to-Site VPN

- Virtual Private Gateway (VPG)
  - VPN concentrator on the AWS side of VPN connection
  - VGP is attached to VPC from which you wanna create a Site-to-Site VPN connection
- Customer Gateway (CGW)
  - Software application or physical device on the customer side of S2S VPN connection

AWS Site-to-Site VPN

VPN Cloudhub

- Provide secure connection between sites (On-Premise and VPC)
- Using hub-and-spoke model
- Using VPN connection via public internet

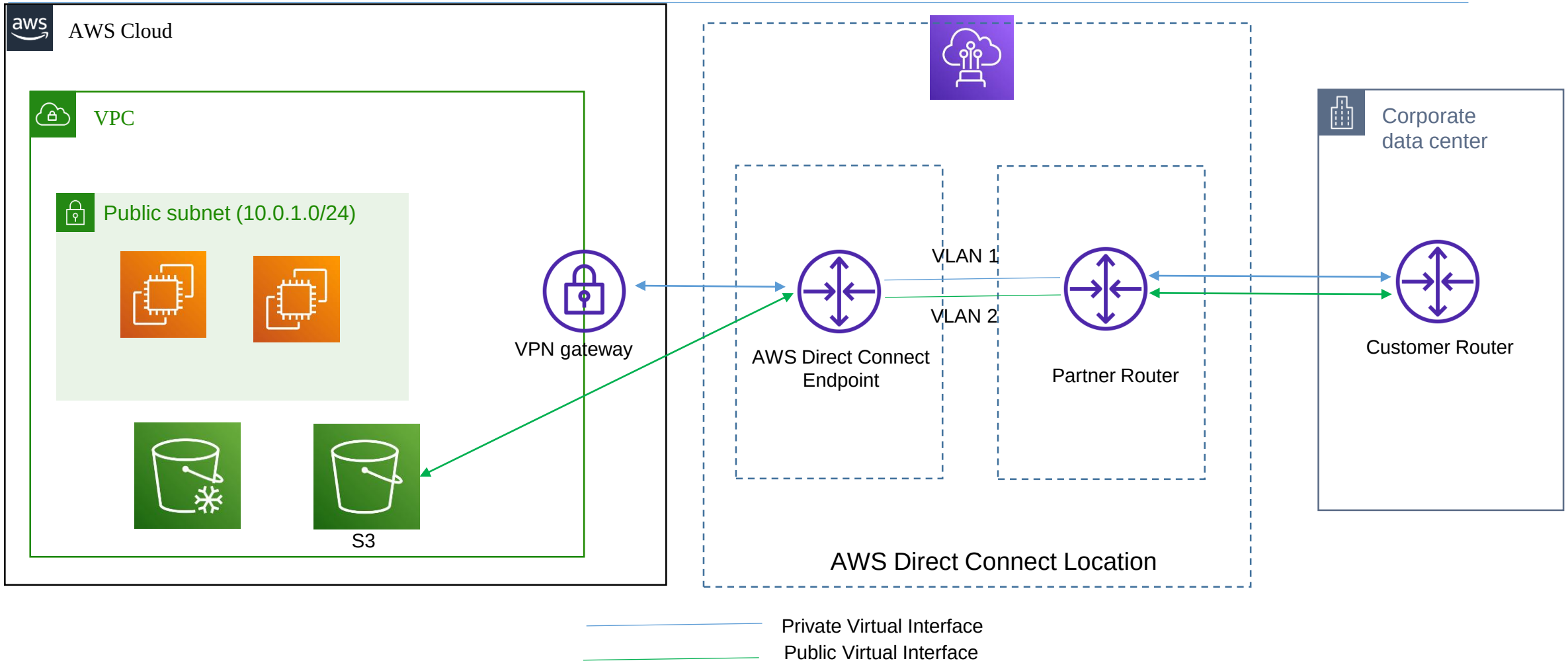


Direct Connect (DX)

Direct Connect (DX)

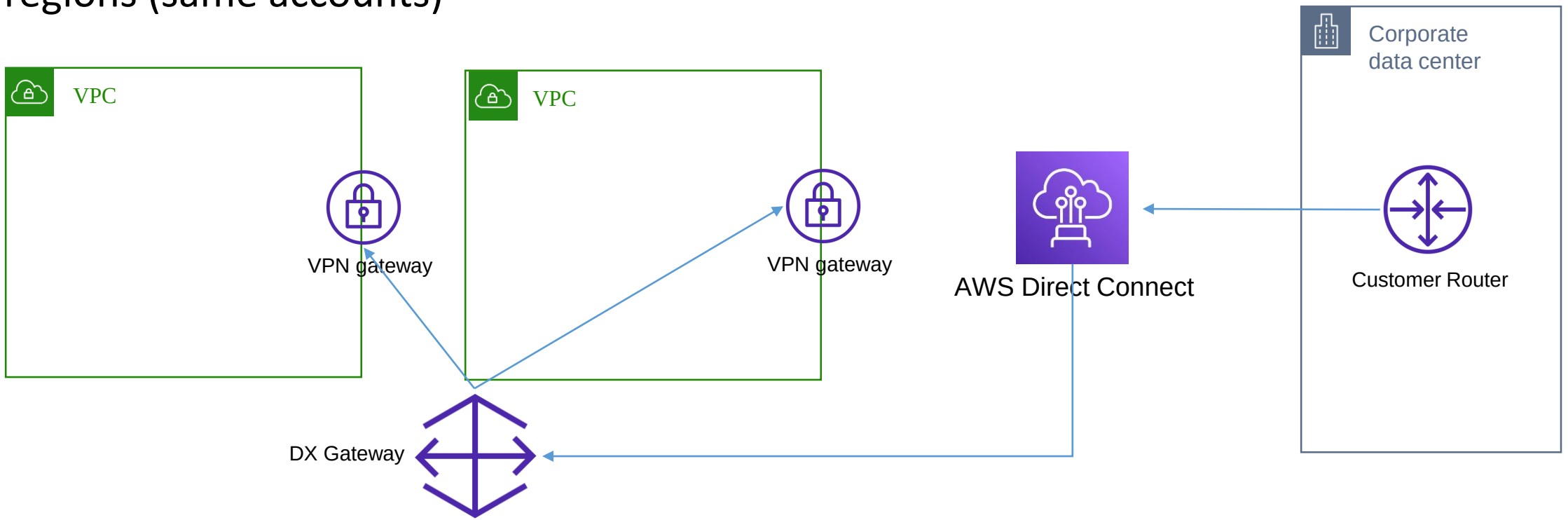
- Provides a dedicated private connection from corporate network to VPCs
- Dedicated connection must be setup between corporate network and DX location
- Need to setup VPG on VPC
- Use cases:
  - Increase bandwidth throughput – transfer large datasets at low cost
  - Consistent network experience

Direct Connect (DX)



Direct Connect Gateway

- Using DX Gateway if you wanna setup DX to one or more VPC in difference regions (same accounts)



Direct Connect (DX) – Connection Type

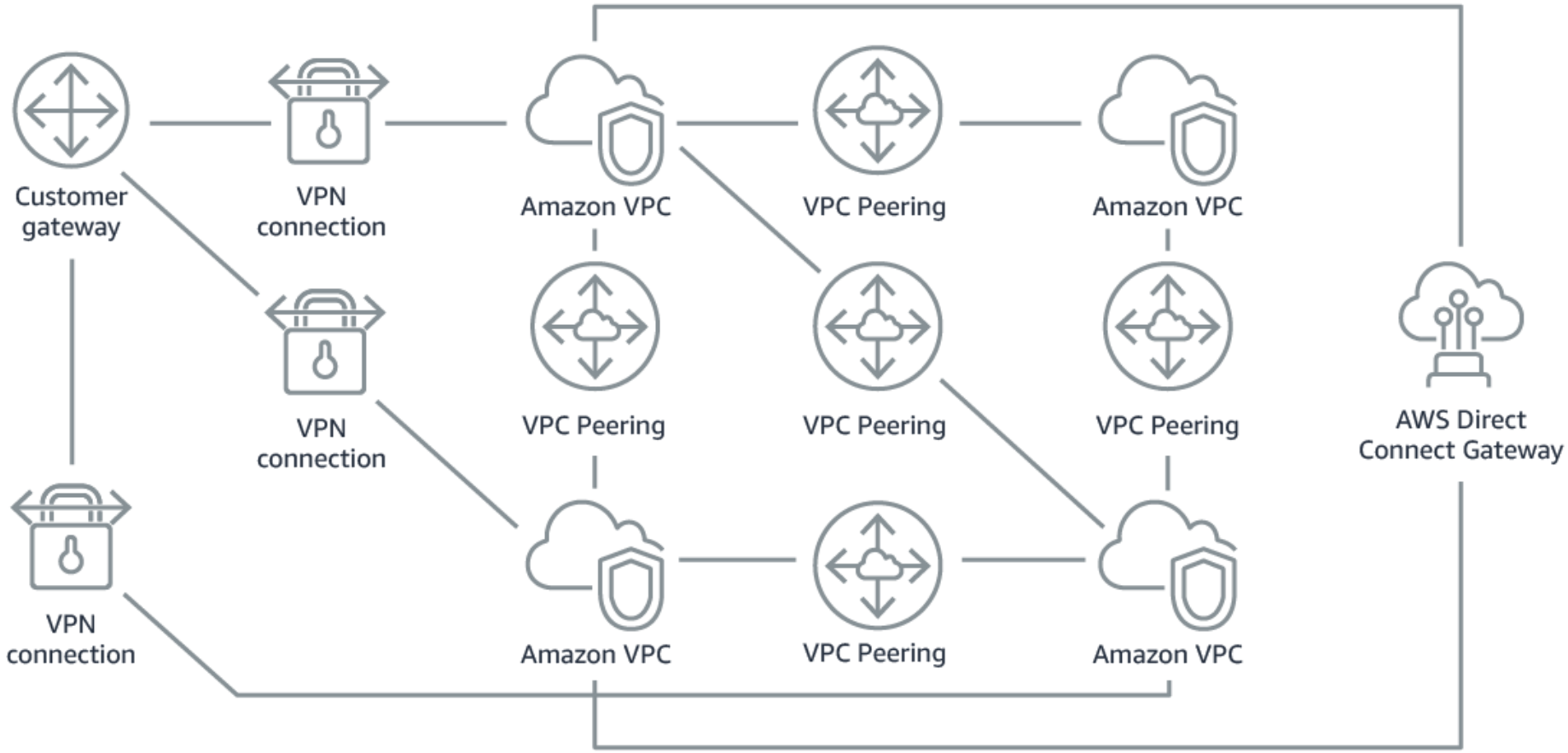
- **Dedicated Connection**
  - 1Gbps or 10Gbps capacity
  - Request to AWS first then AWS Direct Connect parter
- **Hosted Connection**
  - Request is made via AWS Direct Connect parter
  - Capacity can be added or removed on demand
  - 1, 2, 5, 10 Gbps available at AWS DX parter

Direct Connect (DX) – Encryption

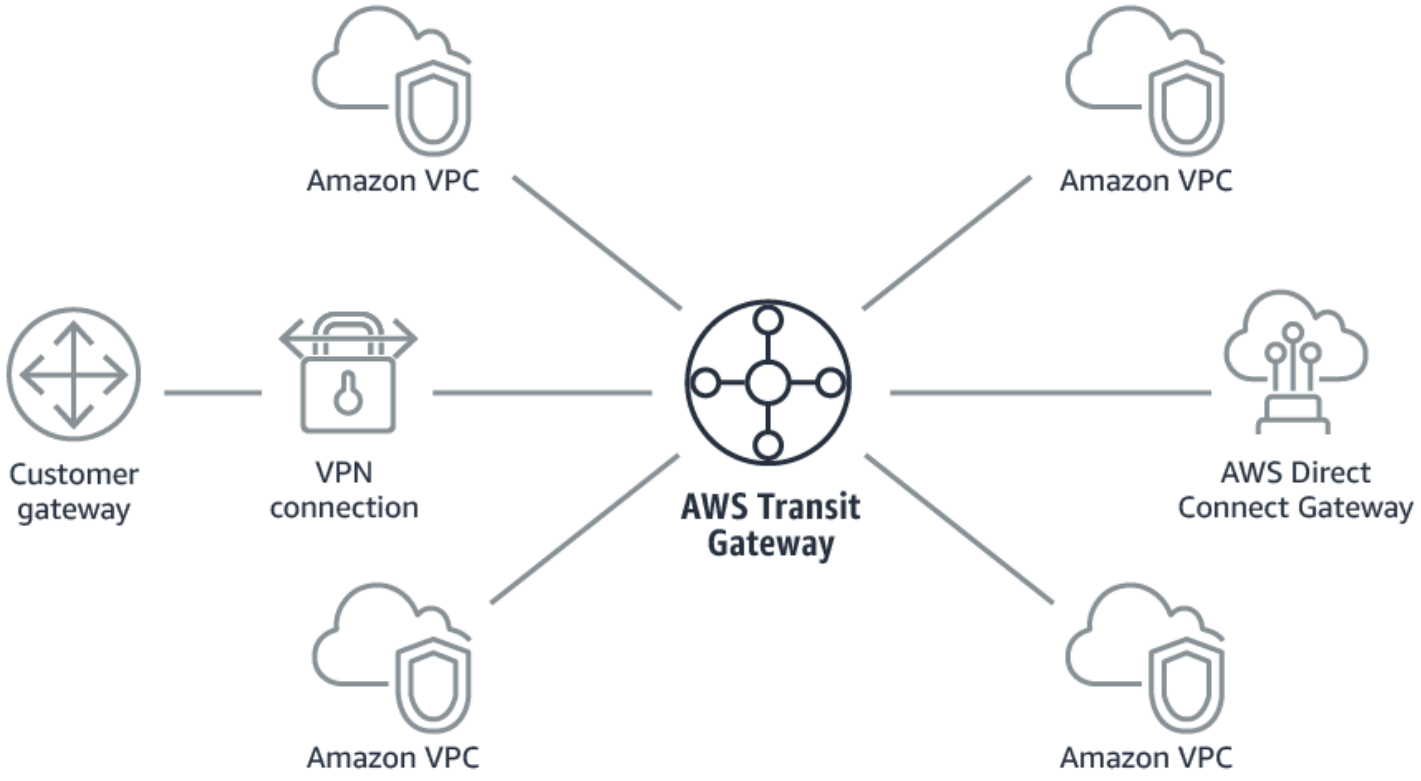
- Data in transit is **not encrypted** but it is private
- Using VPN over DX for extra layer security (but it is complex)

Transit Gateway

Network topology complexity increases with scale



Simplify your network with Transit Gateway



Transit Gateway

- Allows transitive peering connection between thousand of VPCs and On-Premise Data Center
- Work in Hub-and-Spoke model (Star connection)
- Work in regional scope but can across regions
- Can share across multiple AWS accounts using Resource Access Manager service (RAM)
- Route Tables: Control how VPC can talk with others
- Work with Direct Connect Gateway, VPN connections
- Support IP Multicast (Not supported by any other services)

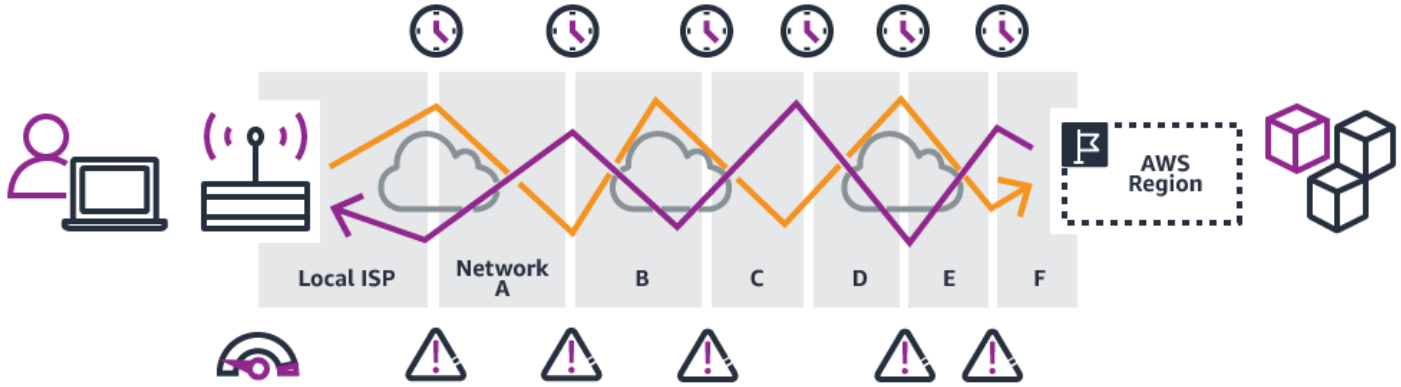
Exam Tips

- Simplify Network topology with hunders of VPC peering, VPN connection, DX => Transit Gateway
- Support IP multicast => Transit Gateway

Global Accelerator

How users connect to your application

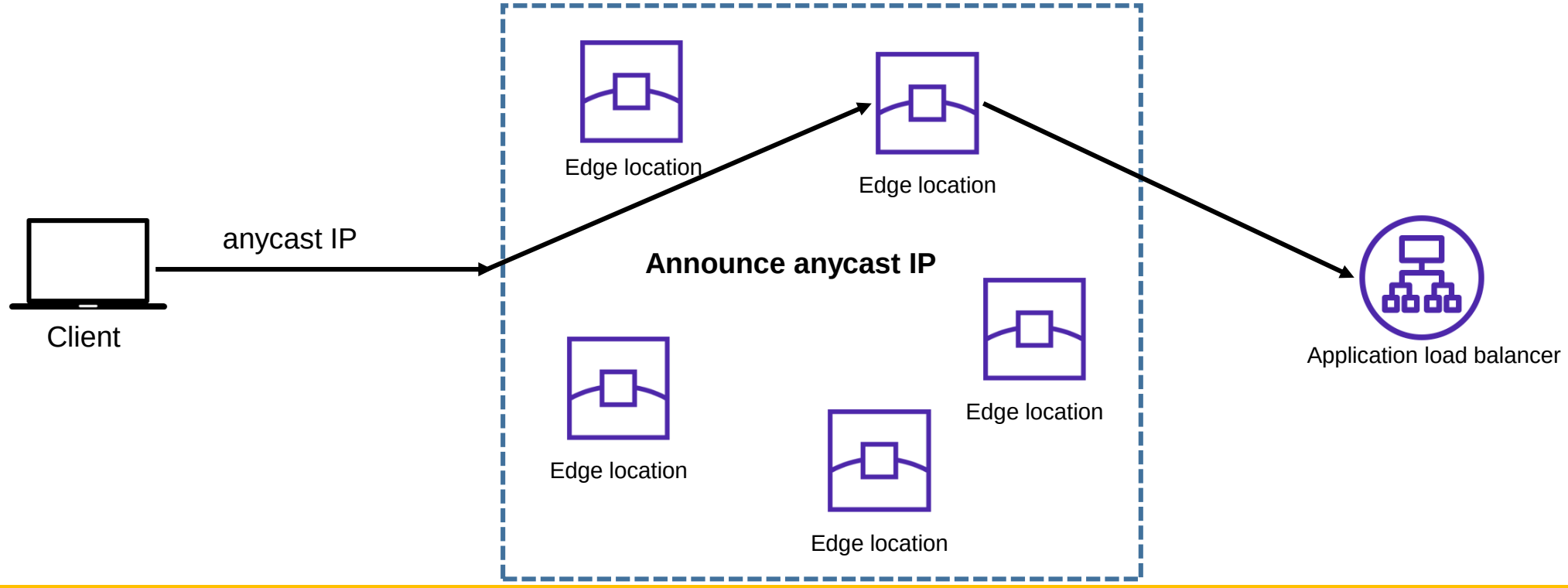
Without Global Accelerator



With Global Accelerator

Global Accelerator

- Using AWS internal network to route to the application
- 2 static anycast IPs created for Global Accelerator as entry point for your application



Global Accelerator

- Work with Elastic IP, EC2 instances, ALB, NLB
- Accelerate performance
  - Reduce latency by using AWS internal network
  - No issues with Client IP cache
- Health Check
  - Perform health check to application
  - Fastest failover
- Security
  - Only needs to whitelist 2 static anycast IPs
  - DDoS protection by AWS Shield

Global Accelerator vs CloudFront

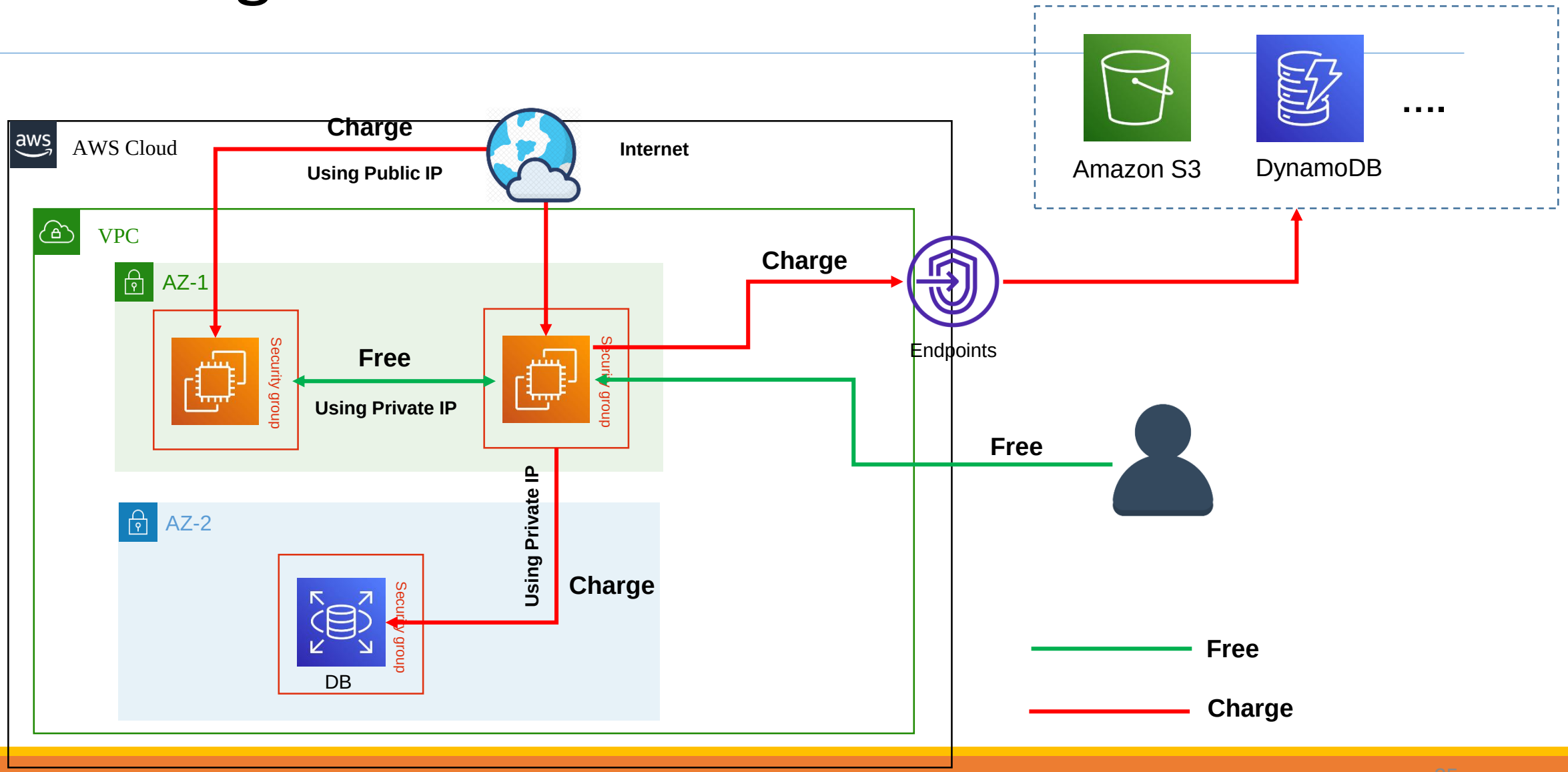
Global Accelerator		CloudFront
Purpose	Using Edge Location to find lowest-latency path to application	Using Edge Location to cache static contents
IP addresses	Using 2 static IP address as entry point of application	Using set of changing IP address
Use case	Handle HTTP and non-HTTP (UDP/TCP) application (**No cache**)	HTTP application (**Need cache**)
Price	Per hour + Data transfer	Number of requests + Data transfer

Data Transfer cost in AWS

Data Transfer cost in AWS

- Traffic in => Free
- Traffic Out => Charge
  - Out to the internet
  - Out to resources in difference AZs
  - Out to AWS services

VPC diagram


Amazon S3
DynamoDB
....
aws
AWS Cloud
Charge
Using Public IP
Internet
VPC
AZ-1
Security group
Free
Using Private IP
Security group
Charge
Endpoints
Free
Using Private IP
AZ-2
Charge
Security group
DB
Free
Charge

Exam Tips

- Setup all resources in one AZs can be free data transfer cost but it will be sufferd of Single Point of Failure (SPOF) when the AZ down
- Create each NAT gateway in each AZ and use for this AZ

Labs

- VPC Peering hands on Lab
- VPC Endpoint Lab