Nội dung

CloudNut
Learn Clouds in a Nutshell

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

CloudNut
Learn Clouds in a Nutshell

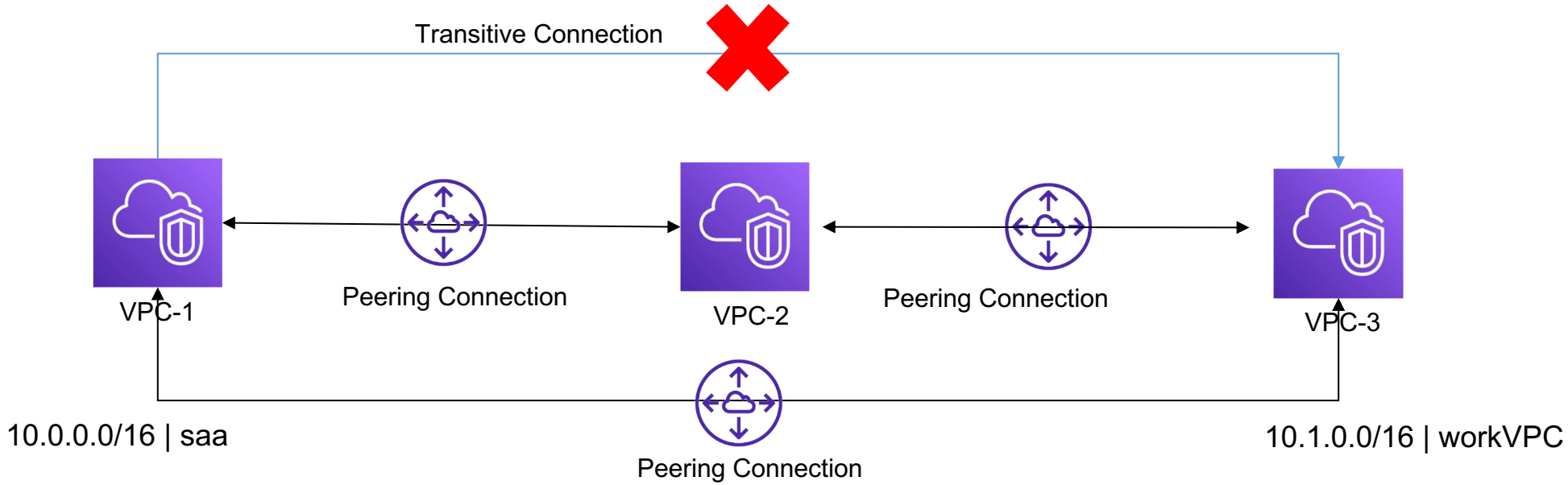
VPC peering

VPC peering

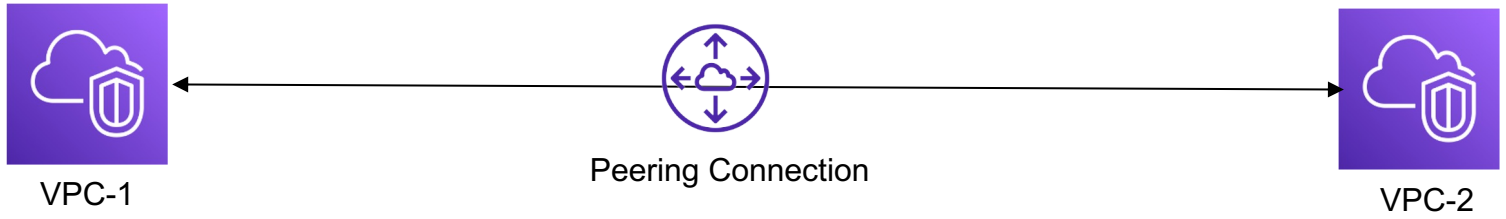
CloudNut
Learn Clouds in a Nutshell

- Cho phép kết nối các VPC với nhau theo đường kết nối Private của AWS
- Tài nguyên trong các VPC này giao tiếp với nhau như trong cùng một Network, sử dụng Private IP
- Yêu cầu VPC CIDR giữa các VPC cần Peering không được overlap (trùng hoặc đè nhau)
- Kết nối Peering không có tính bắc cầu (Transitive Peering)
- Kết nối Peering có thể setup giữa các VPC cùng hoặc khác Region hoặc khác AWS account

VPC peering (cont.)



VPC peering - Network topology



10.0.0.0/16 | VPC-1

Route Table
10.1.0.0/16 => VPCPeering

Public subnet (10.0.1.0/24)

10.0.1.10

10.1.0.0/16 | VPC-2

Route Table
10.0.0.0/16 => VPCPeering

Public subnet (10.1.1.0/24)

10.1.1.20

CloudNut
Learn Clouds in a Nutshell

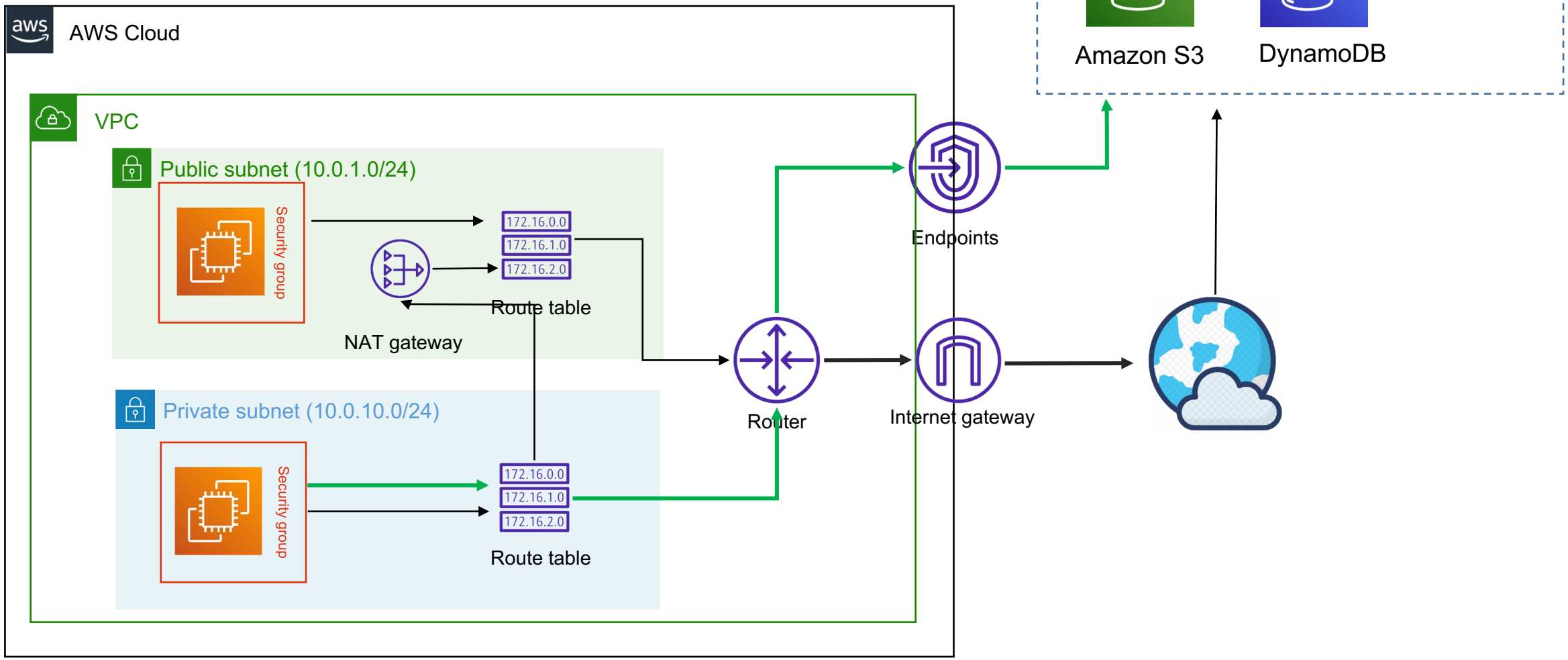
VPC endpoint

VPC endpoint

CloudNut
Learn Clouds in a Nutshell

- **VPC Endpoint** cho phép tạo kết nối private (sử dụng hạ tầng của AWS) tới các dịch vụ của AWS thay vì đi qua kết nối Internet
- Auto Scalling và HA
- Không cần NAT Gateway, IGW, Public IP

VPC endpoint (cont.)



VPC Endpoint Type

CloudNut
Learn Clouds in a Nutshell

- **Gateway Endpoint**
  - Sử dụng để kết nối tới dịch vụ DynamoDB và S3
  - Cần phải cấu hình trong Route Table
- **Interface Endpoint**
  - Sử dụng để kết nối tới các dịch vụ được hỗ trợ bởi AWS Private Link
  - Interface Endpoint sẽ được cấp 1 Private IP (lấy từ Subnet tạo Interface này) hoạt động như là Entry Point
- **Gateway Load Balancer Endpoint**
  - Dùng cho Gateway Load Balancer

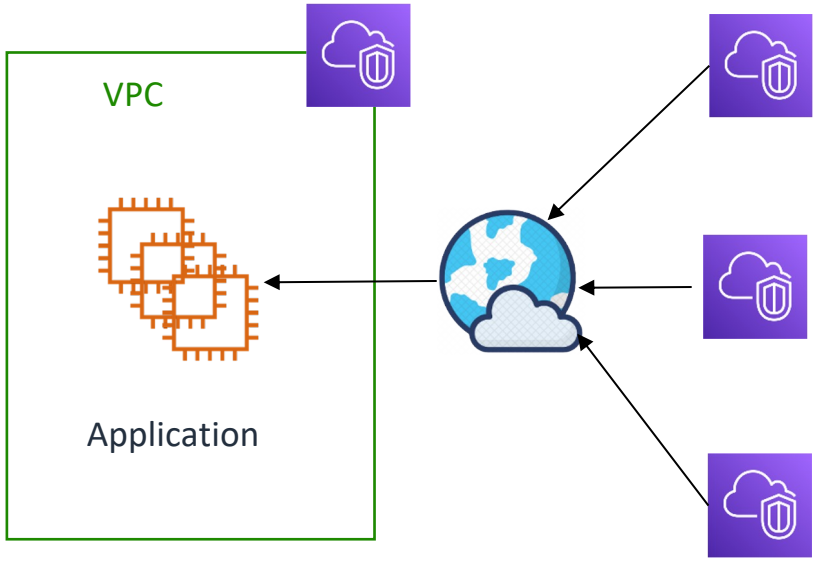
CloudNut
Learn Clouds in a Nutshell

AWS Privatelink

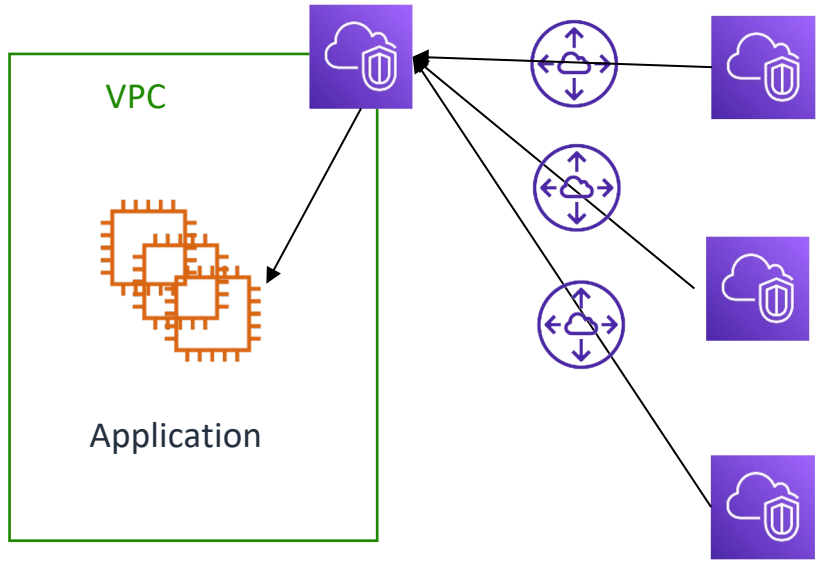
Expose Service cho VPC khác?

CloudNut
Learn Clouds in a Nutshell

- **Option 1**: Expose Service qua Internet
  - Không an toàn
  - Cần phải quản lý Firewall, chống DDoS…



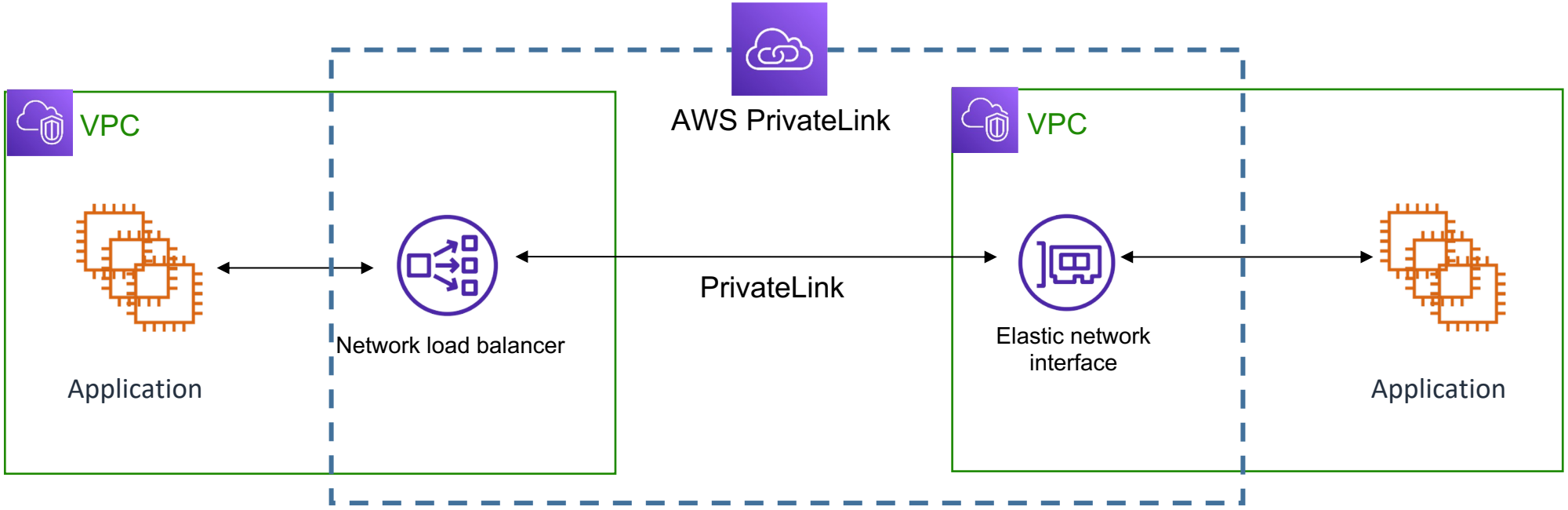
- **Option 2**: Qua Peering Connection
  - Cần phải quản lý nhiều Peering Connection
  - Expose tất cả resources thay vì chỉ riêng Service



Expose Service cho VPC khác?

CloudNut
Learn Clouds in a Nutshell

- **Option 3**: Qua AWS privatelink
  - An toàn, bảo mật
  - Không cần phải quản lý VPC Peering, IGW, Route Table…
  - Cần phải tạo Network Load Balancer và ENI



Exam Tips

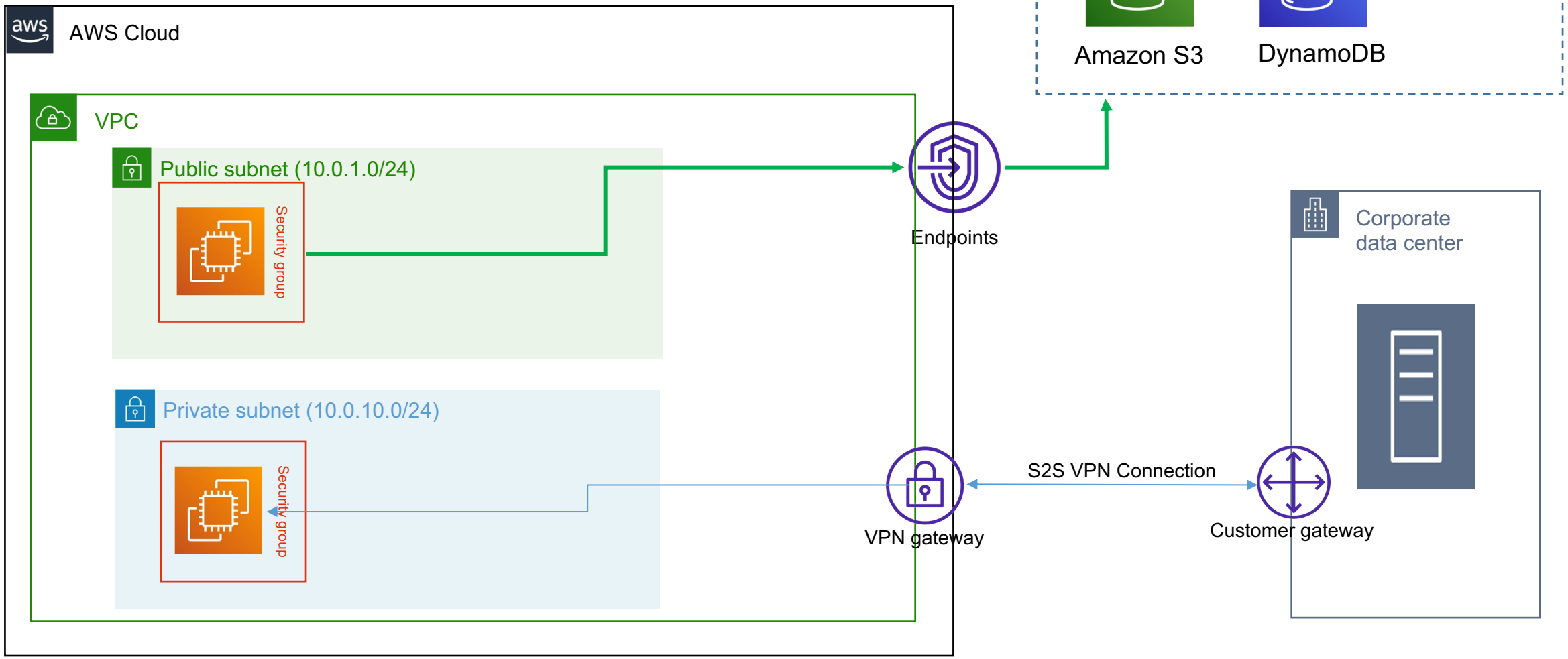
CloudNut
Learn Clouds in a Nutshell

- Expose Service cho hàng trăm, nghìn VPC => Sử dụng AWS PrivateLink
- Sử dụng AWS PrivateLink không cần phải quản lý Peering Connection, Route Table, NAT, IGW…
- Cần phải Setup một Network Load Balancer (NLB) và một ENI tại VPC của khách hàng

CloudNut
Learn Clouds in a Nutshell

VPN, VPN Cloud Hub

VPN (Virtual Private Network)



AWS Site-to-Site (S2S) VPN

CloudNut
Learn Clouds in a Nutshell

- Virtual Private Gateway (VPG)
  - Đầu kết nối của VPN connection ở phía đầu AWS
  - VPG được gắn vào VPC muốn tạo kết nối S2S VPN

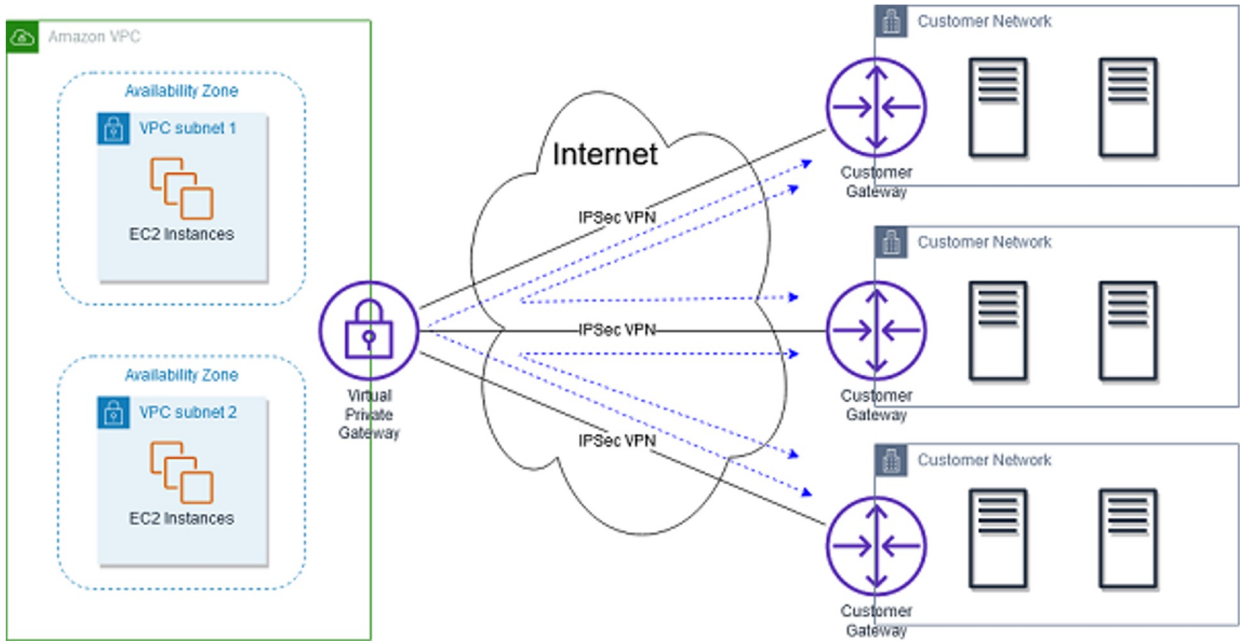
AWS Site-to-Site VPN

- Customer Gateway (CGW)
  - Phần mềm hoặc phần cứng đóng vai trò Gateway của VPN connection ở phía hạ tầng On-Premise hoặc VPC

VPN Cloudhub

CloudNut
Learn Clouds in a Nutshell

- Cung cấp kết nối VPN giữa các Branch, Remote Office
- Sử dụng mô hình Hub-and-Spoke
- Sử dụng kết nối VPN qua public Internet



CloudNut
Learn Clouds in a Nutshell

Direct Connect (DX)

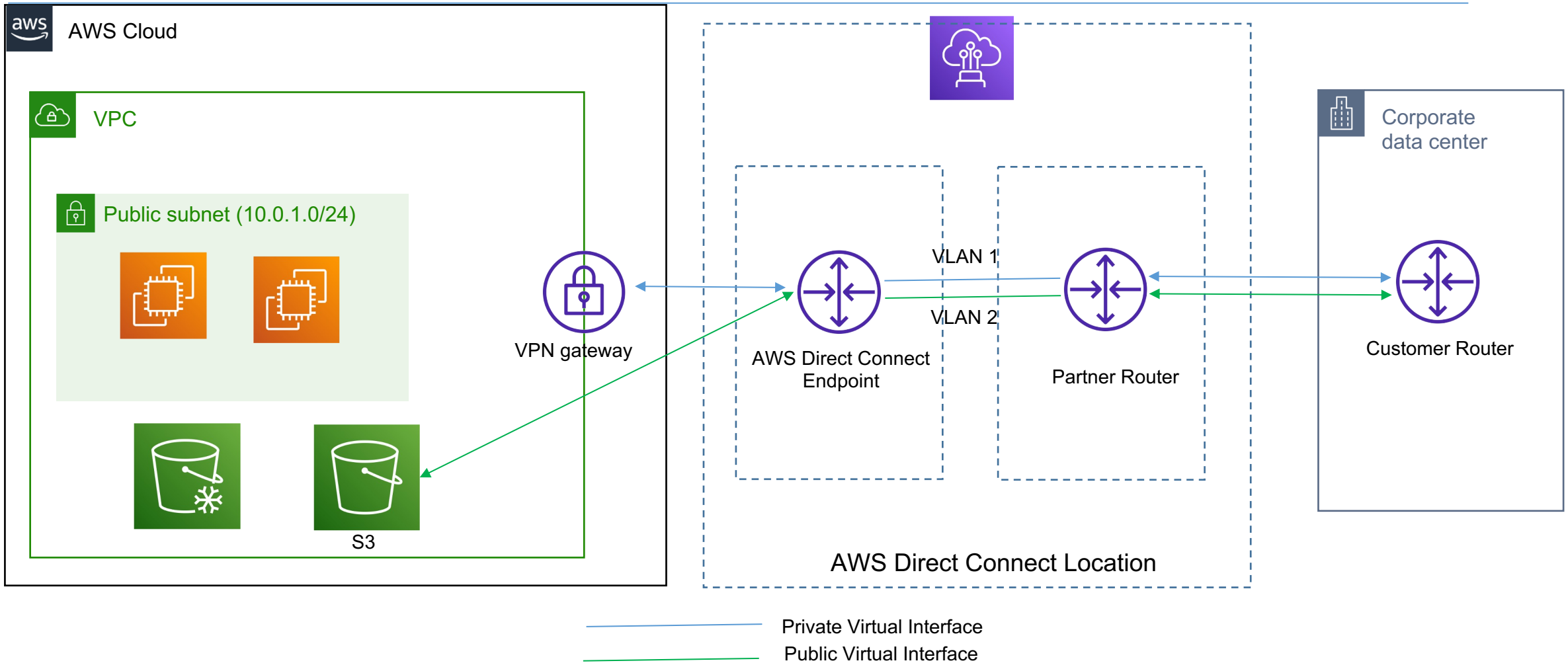
Direct Connect (DX)

CloudNut
Learn Clouds in a Nutshell

- DX cung cấp đường truyền chuyên biệt (Dedicated Connection) giữa hạ tầng On-Premise (Corperate Network) với AWS
- Đường truyền này phải được thiết lập giữa hạ tầng On-Premise và DX Location
- Cần phải setup VPG (Virtual Private Gateway) ở VPC
- Use cases:
  - Tăng băng thông đường truyền. Giảm chi phí khi truyền tải khối lượng lớn dữ liệu lên AWS
  - Hiệu năng của đường truyền ổn định

Direct Connect (DX)

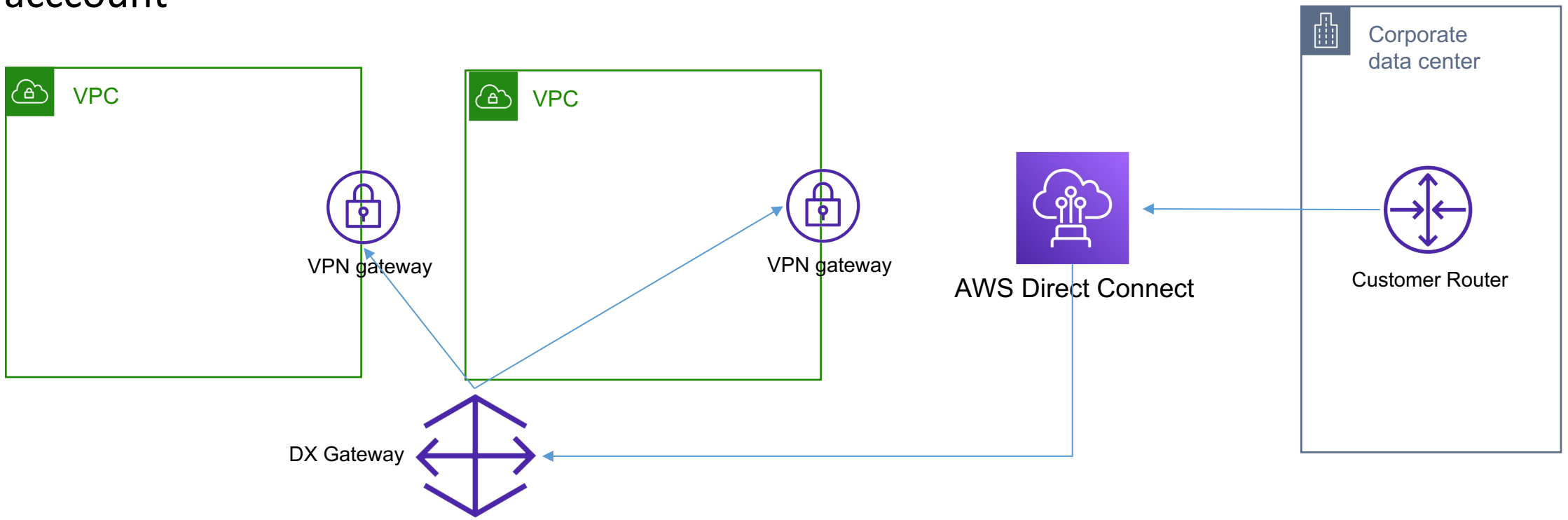
CloudNut
Learn Clouds in a Nutshell



Direct Connect Gateway

CloudNut
Learn Clouds in a Nutshell

- DX Gateway cho phép tạo DX connection tới nhiều VPC khác nhau trong cùng acccount



Direct Connect (DX) – Connection Type

CloudNut
Learn Clouds in a Nutshell

- **Dedicated Connection**
  - Băng thông 1Gbps or 10Gbps
  - Request được gửi cho AWS, sau đó là DX Partner của AWS
- **Hosted Connection**
  - Request được gửi qua AWS DX partner
  - Băng thông có thể thay đổi tuỳ thuộc theo nhu cầu (On-Demand)
  - Băng thông có thể 1, 2, 5, 10 Gbps

Direct Connect (DX) – Encryption

CloudNut
Learn Clouds in a Nutshell

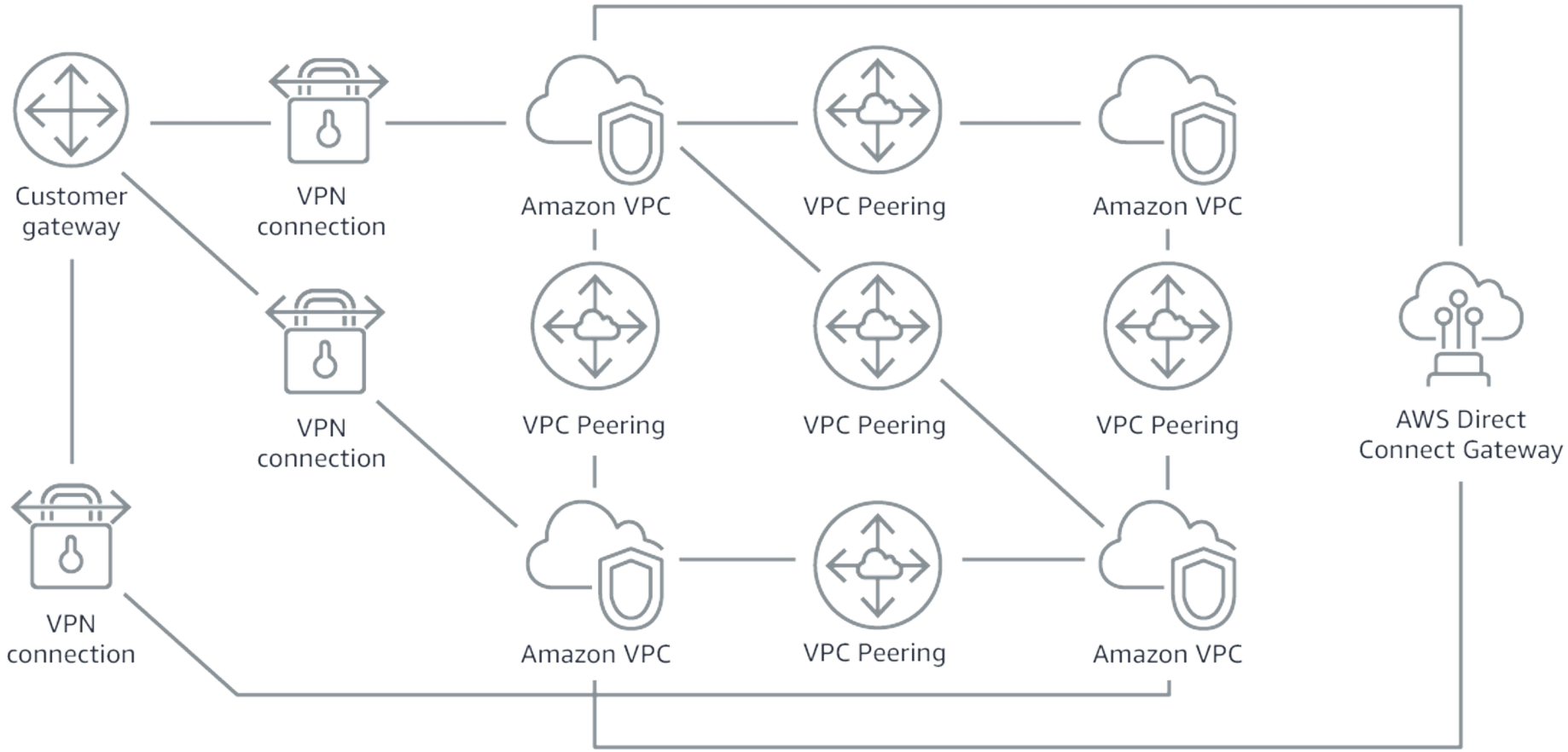
- Dữ liệu sẽ không được mã hoá (Not Encrypted) giống VPN nhưng sẽ riêng tư (Private) vì dùng đường kết nối chuyên biệt (Dedicated Line)
- Có thể sử dụng VPN dựa trên kết nối DX. Tuy nhiên tương đối phức tạp

CloudNut
Learn Clouds in a Nutshell

Transit Gateway

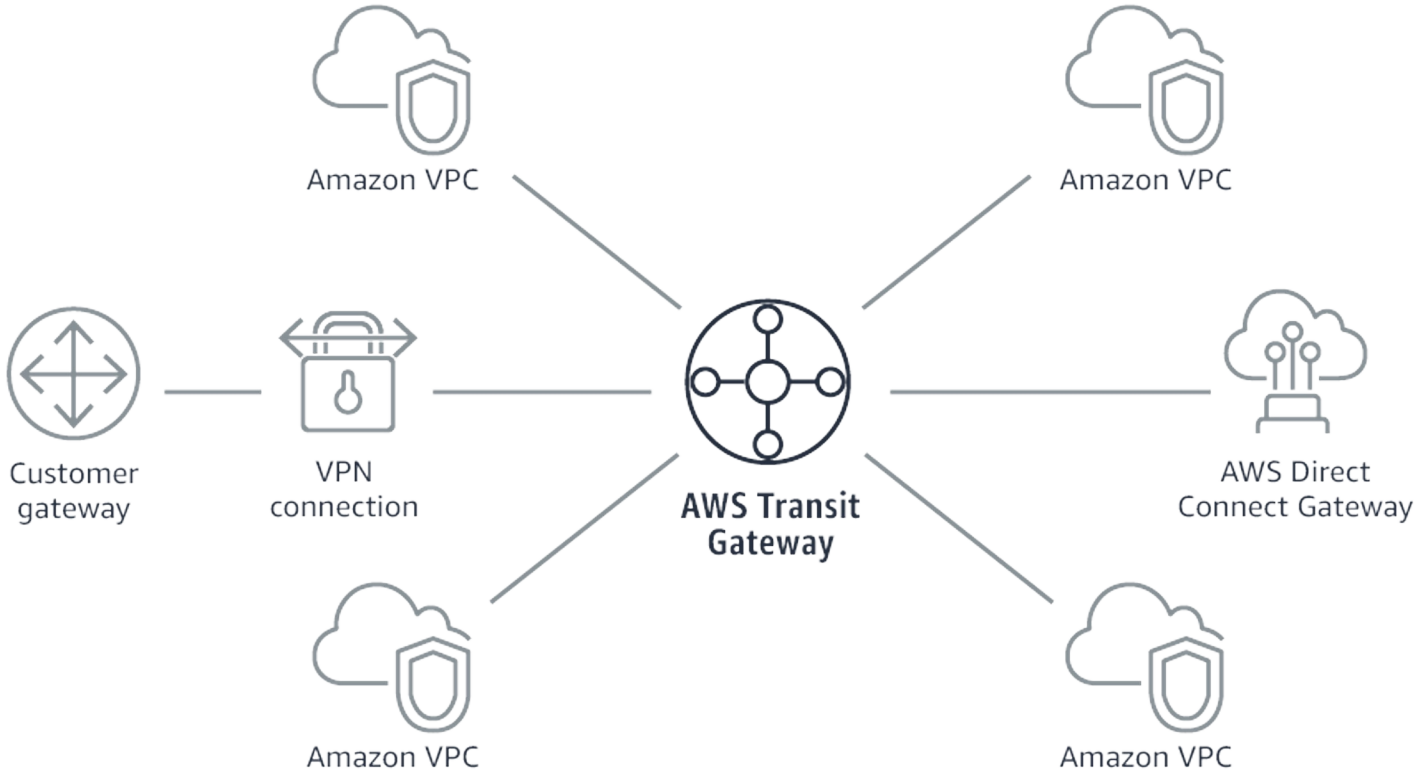
Tính phức tạp của một Network?

CloudNut
Learn Clouds in a Nutshell



Transit Gateway

CloudNut
Learn Clouds in a Nutshell



Transit Gateway

CloudNut
Learn Clouds in a Nutshell

- Cho phép Transitive Peering giữa các VPC
- Allows transitive peering connection between thousand of VPCs and On-Premise Data Center
- Hoạt động theo mô hình Hub-and-Spoke model (Star connection)
- Có thể chia sẻ với nhiều Account AWS sử dụng dịch vụ RAM (Resource Access Manager)
- Có thể làm việc với Direct Connect Gateway, VPN connections
- Hỗ trợ IP Multicast

Exam Tips

CloudNut
Learn Clouds in a Nutshell

- Các Network Topo với số lượng hàng trăm, hàng nghìn VPC, VPN connection và DX => Sử dụng Transit Gateway
- Hỗ trợ IP multicast => Transit Gateway

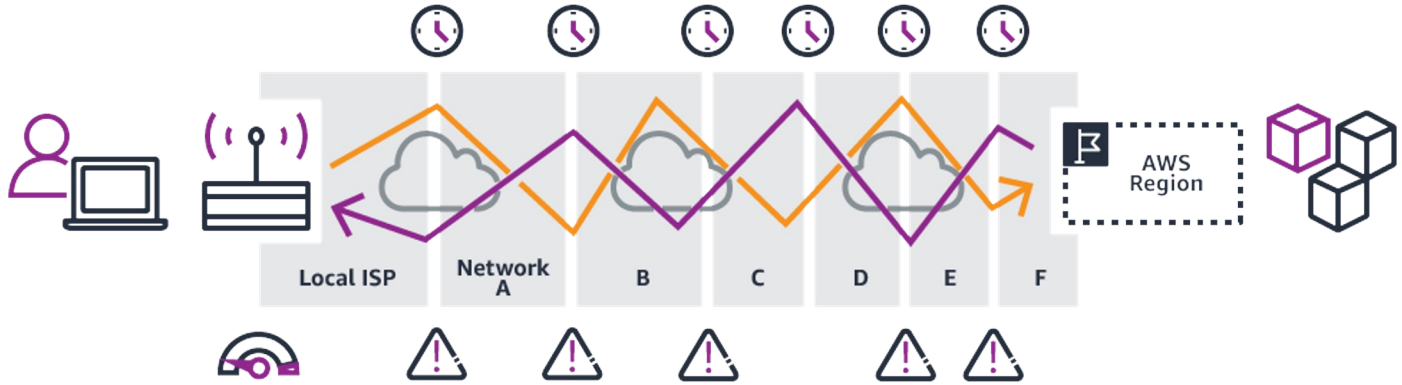
CloudNut
Learn Clouds in a Nutshell

Global Accelerator

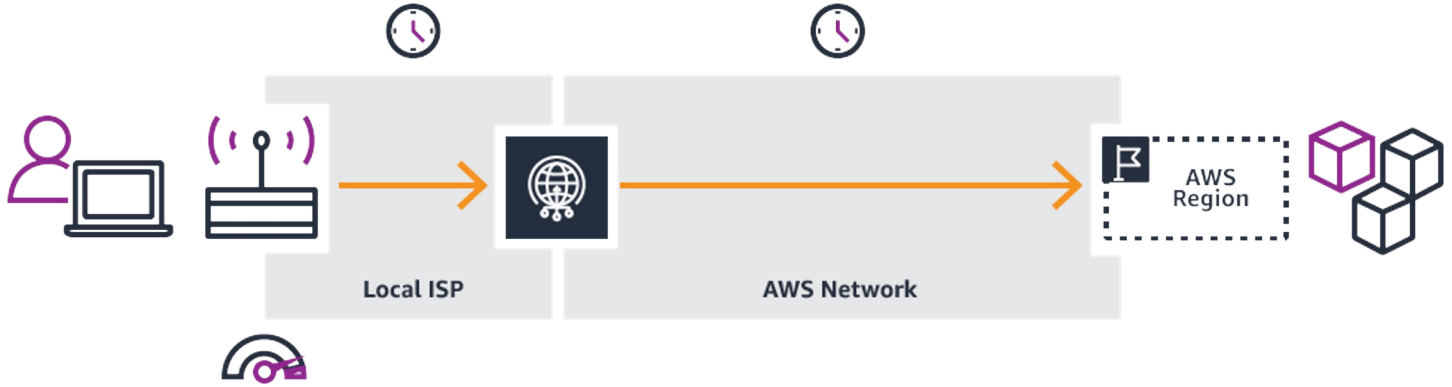
Cách user truy cập ứng dụng?

CloudNut
Learn Clouds in a Nutshell

Without Global Accelerator



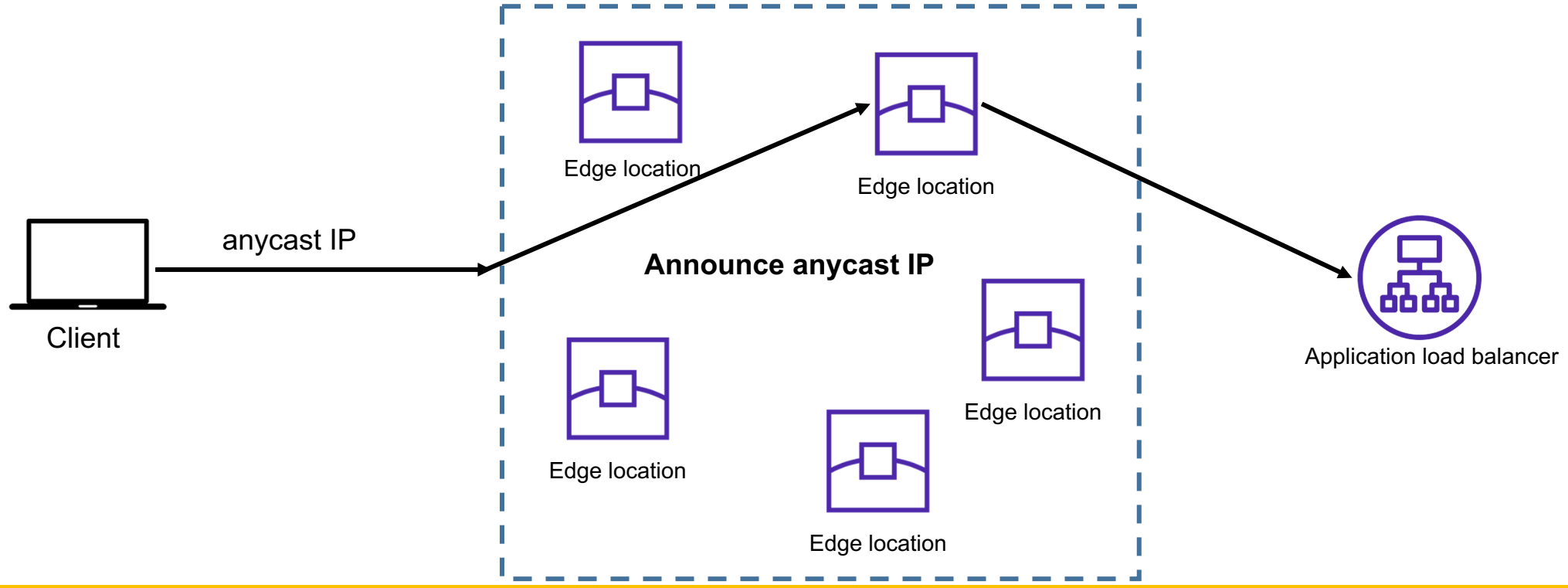
With Global Accelerator



Global Accelerator

CloudNut
Learn Clouds in a Nutshell

- Sử dụng AWS Internal Network để định tuyến tới ứng dụng (Hosted AWS)
- Sử dụng 2 anycast IP (Anycast của Edge Location) hoạt động như Entry Point cho ứng dụng



Global Accelerator

CloudNut
Learn Clouds in a Nutshell

- Làm việc được với Elastic IP, EC2 instances, ALB, NLB
- Tăng hiệu năng của ứng dụng
  - Giảm Latency tới ứng dụng nhờ sử dụng AWS Network (sử dụng Edge Location và Anycast IPs)
- Health Check
  - Cho phép thực hiện Healthcheck tới ứng dụng
  - Cho phép nhanh chóng khôi phục ứng dụng khi có sự cố (Fast Failover)
- Security
  - Chỉ cần quản lý, tương tác với 2 Anycast IP
  - Có thể kết hợp với AWS Shield để ngăn chặn DDoS

Global Accelerator vs CloudFront

CloudNut
Learn Clouds in a Nutshell

Global Accelerator		CloudFront
Mục đích	Sử dụng Edge Location để tìm đường đi ngắn nhất truy cập tới ứng dụng (Lowest-Latency Path)	Sử dụng Edge Location để Cache các nội dung tĩnh (static content)
IP addresses	Sử dụng 2 IP Anycast	Dải địa chỉ IP thay đổi
Use case	Xử lý được cho HTTP và non-HTTP (UDP/TCP) và không Cache	Xử lý HTTP, có Cache
Giá	Số giờ sử dụng (Per hour) + Dữ liệu truyền tải (Data transfer)	Số lượng yêu cầu (Number of requests) + Dữ liệu truyền tải (Data transfer)

CloudNut
Learn Clouds in a Nutshell

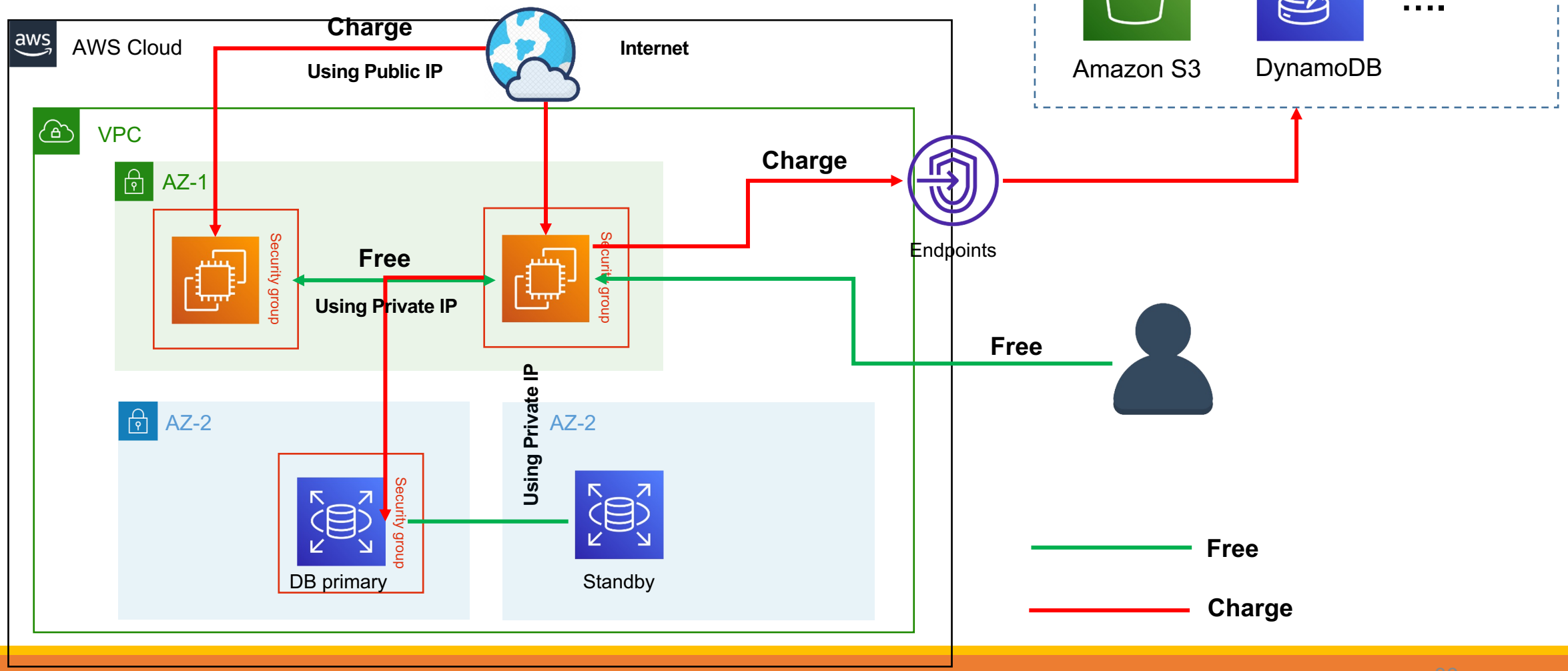
Data Transfer cost in AWS

Data Transfer cost in AWS

CloudNut
Learn Clouds in a Nutshell

- Traffic đi vào (Traffic In) là FREE
- Traffic đi ra (Traffic Out) => Charge phí với đơn giá các ngữ cảnh sau
  - Traffic Out ra Internet
  - Traffic Out ra các Resources nằm trên Availibility Zone khác
  - Traffic Out ra các AWS services

VPC diagram


CloudNut
Learn Clouds in a Nutshell
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
AZ-2
Security group
DB primary
Standby
Free
Charge

Exam Tips

CloudNut
Learn Clouds in a Nutshell

- Setup tất cả các Resources trong cùng một AZ sẽ tiết kiệm được phí truyền tải dữ liệu (Data Tranfer Cost). Tuy nhiên hệ thống sẽ giảm tính High Availibility khi AZ này gặp sự cố (Downtime)
- Tạo NAT Gateway trên mỗi AZ và sử dụng cho AZ này sẽ giảm được chi phí truyền tải dữ liệu giữa các AZ

Labs

- VPC Peering hands on Lab
- VPC Endpoint Lab