Networking

Traffic Control

Fire Wall

NACL

SG

Security

amazon web services™

Amazon Web Service - Training

NETWORKING
WITH AWS

TRAFFIC CONTROL

AWS VPC

In Bound

Fire Wall

Networking

Network Access Control List

Out Bound

Subnet

amazon web services™

AWS Solution Architect Associate - Training

NETWORK ACCESS CONTROL LIST

NACLs chứa các nhóm quy tắc **Outbound** và **Inbound.** **Inbound** xác thực các traffic đi vào trong Subnet, **Outbound** xác thực các traffic đi từ bên trong Subnet ra ngoài

Inbound rules (2)

Filter inbound rules

Default NACL

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

Outbound rules (2)

Filter outbound rules

Default NACL

Rule number	Type	Protocol	Port range	Destination	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

Các **kết nối** nằm bên **trong subnet** không bị ảnh hưởng bởi **NACLs**

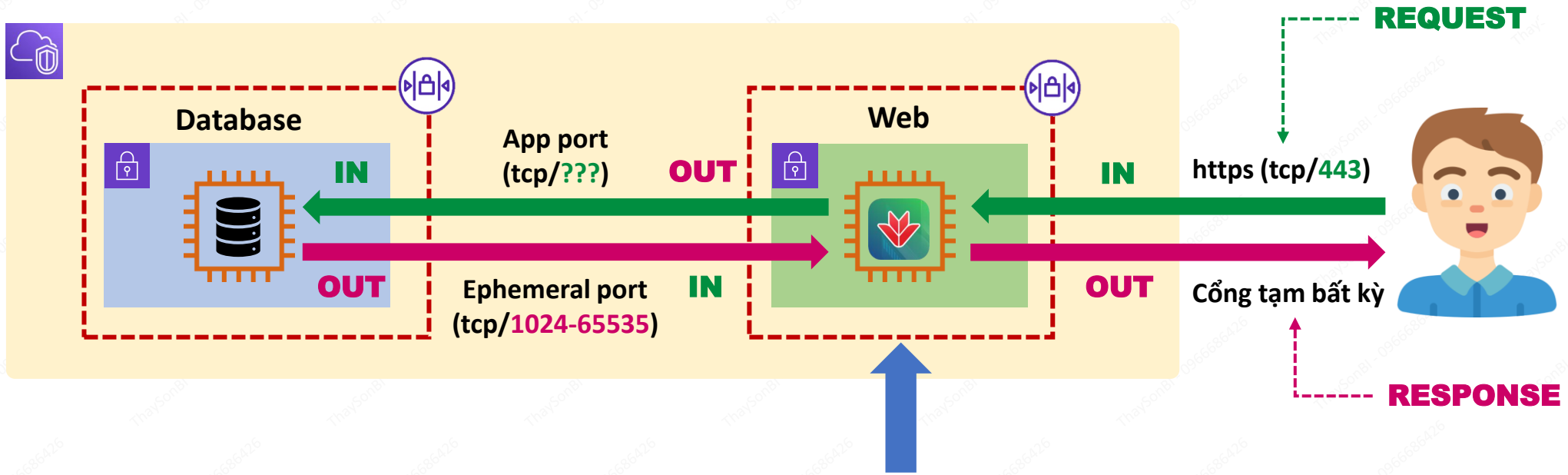
NACLs chỉ **lọc** các traffic **vào (Inbound)** và **ra (Outbound)**

NACL Rules xác thực **Destination IP, Range, Port, Protocol.** Sau đó, **ALLOW** hoặc **DENY** dựa trên sự trùng khớp

Traffic sẽ được kiểm tra qua các Rules **tuần tự** theo **Rule Number** từ **bé nhất** đến **lớn nhất.** Khi matched với 1 rule nào đó thì nó sẽ **STOP.**
* có nghĩa là nếu không match được với bất cứ rule nào sẽ bị **DENY**

NACL RULES

NACLs là **STATELESS**, cho nên các mối liên kết đều cần xác thực độc lập **REQUEST** và **RESPONSE.** Tương ứng với 1 x **INBOUND** và 1 x **OUTBOUND**



Những quy tắc ghép cặp **app port** và **ephemeral port** là cần thiết cho các mối liên kết **trong cùng** VPC, **vào** và **ra** VPC

INBOUND

Rule number	Type	Protocol	Port range	Source	Allow/Deny
110	HTTPS (443)	TCP (6)	443	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

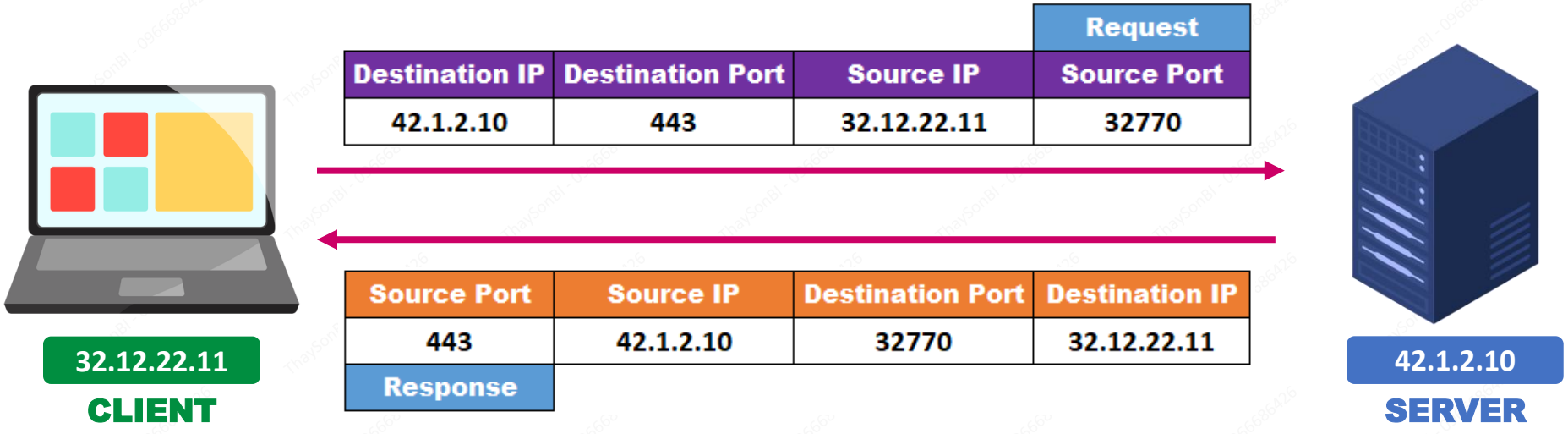
OUTBOUND

Rule number	Type	Protocol	Port range	Destination	Allow/Deny
120	Custom TCP	TCP (6)	1024 - 65535	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

EPHEMERAL PORT

Một Ephemeral Port là một cổng dùng để truyền tin tạm thời cho mạng **Internet Protocol (IP)**.
Nó được tạo ra từ **một tập hợp các số cổng** bằng **phần mềm IP.**

- Amazon linux kernel: **32768 - 61000**
- Elastic Load Balancing: **1024 – 65535**
- Windows Server 2008 và Version mới nhất: **49152 - 65535**
- NAT Gateway: **1024 - 65535**
- AWS Lambda: **1024 - 65535**



CUSTOM NACL

Inbound rules (1)

Filter inbound rules

Rule number	Type	Protocol	Port range	Source	Allow/Deny
*	All traffic	All	All	0.0.0.0/0	Deny

Chúng chỉ có duy nhất **1** **INBOUND** rule dùng để loại trừ tất cả traffic đi **VÀO**

Custom NACLs có thể được được tạo trong 1 **VPC** mà không gán vào bất cứ **Subnet** nào

ALL TRAFFIC → DENY

Outbound rules (1)

Filter outbound rules

Rule number	Type	Protocol	Port range	Destination	Allow/Deny
*	All traffic	All	All	0.0.0.0/0	Deny

Chúng chỉ có duy nhất **1** **OUTBOUND** rule dùng để loại trừ tất cả traffic đi **RA**

CUSTOM NACL

INBOUND					
Rule #	**Type**	**Protocol**	**Port Range**	**Source**	**Allow/Deny**
100	HTTP	TCP	80	0.0.0.0/0	ALLOW
110	HTTPS	TCP	443	0.0.0.0/0	ALLOW
120	SSH	TCP	22	192.0.2.0/24	ALLOW
130	RDP	TCP	3389	192.0.2.0/24	ALLOW
140	Custom TCP	TCP	32768-65535	0.0.0.0/0	ALLOW
*	All Traffic	All	All	0.0.0.0/0	DENY
OUTBOUND					
Rule #	**Type**	**Protocol**	**Port Range**	**Source**	**Allow/Deny**
100	HTTP	TCP	80	0.0.0.0/0	ALLOW
110	HTTPS	TCP	443	0.0.0.0/0	ALLOW
120	Custom TCP	TCP	32768-65535	0.0.0.0/0	ALLOW
*	All Traffic	All	All	0.0.0.0/0	DENY

HTTPS REQUEST (443)

NO MATCH

MATCHED

EPHEMERAL

NO MATCH

MATCH 443

EPHEMERAL

NACL SUMMARY

STATELESS – Kiểm tra cả **REQUEST** và **RESPONSE**

Chỉ ảnh hưởng đến dữ liệu **vào/ra**

NACLs dùng **Ips/CIDR, Ports, Protocol** để xác định **ALLOW** và **DENY**

NACLs chỉ được gắn vào **Subnet**, không dành cho đối tượng khác

Kết hợp với **Security Group (SG)** để **DENY** Ips/Nets không phù hợp

Mỗi Subnet chỉ có thể có **1 NACL** (Default hoặc Custom)

1 NACL có thể được gắn cho **nhiều Subnet**

ENJ

Reference

Networking

Security Group

Traffic Control

Stateful

amazon web services™

Amazon Web Service - Training

SG OVERVIEW

STATEFUL – Tự động tìm **RESPONSE** traffic

Allowed (vào hoặc ra) **request** = **allowed response**

Không thể ngăn chặn một cách **cụ thể** các tác nhân xấu

Hỗ trợ Ips/CIDR… và cả **logical resources** (SG khác và chính nó)

Được gắn vào **ENI** (Elastic Network Interface) theo quan hệ **N-N**

… chứ **SG** không gắn vào **Instance**

NACLs → Subnets còn **SG → ENI → Instance**

SG WORKING

Không thể ghi đè một rule đã được xác thực **(IN tcp/443)**

Chấp thuận cho **tất cả** traffic **đi vào** hoặc **đi ra khỏi ENI**

Database Instance

Elastic Network Interface

SG được gắn với một **primary ENI** của instance

REQUEST

https (tcp/443)

SG là **stateful** - **Response** luôn **tự động** được thông qua nếu **Request** được cho phép

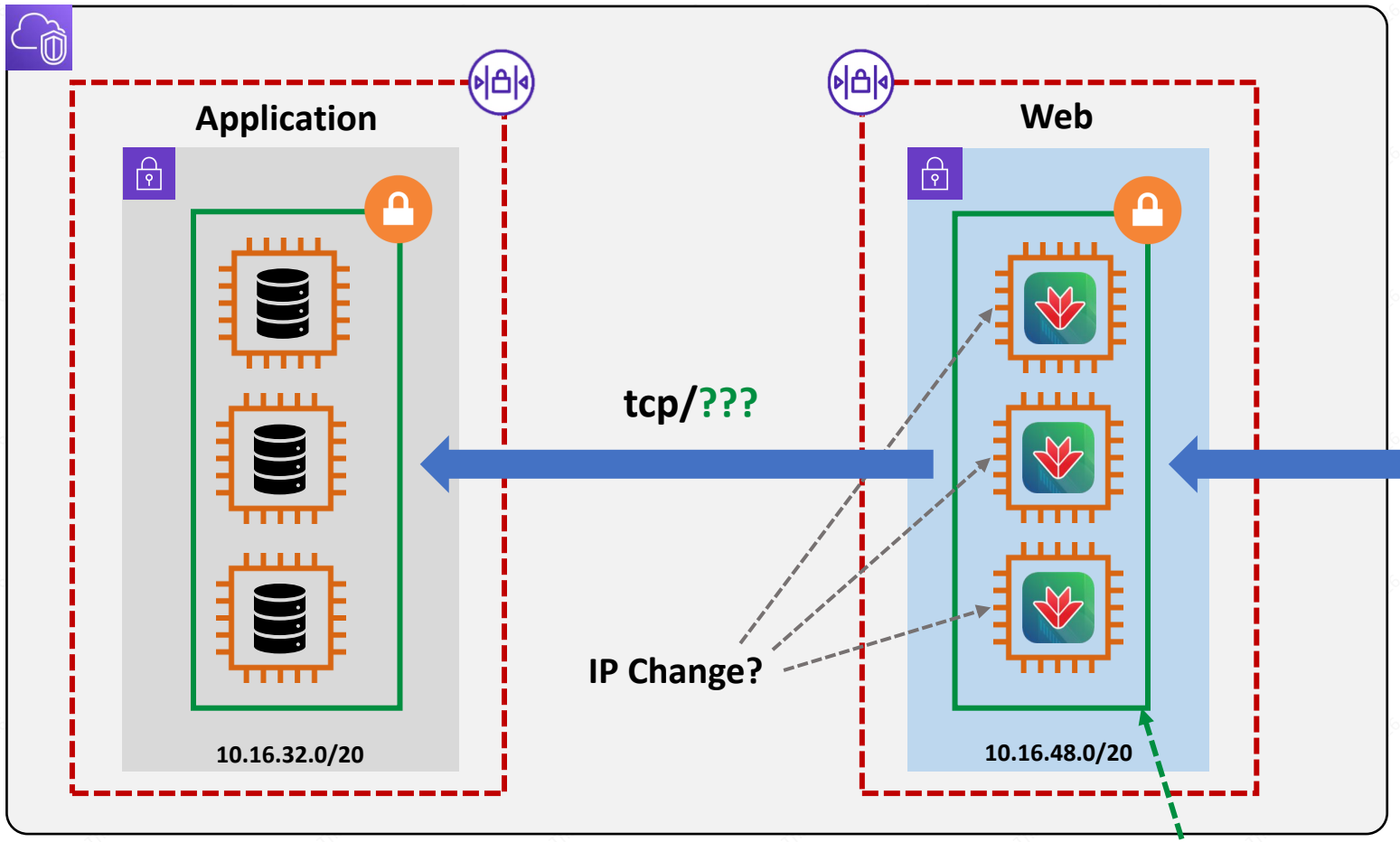
RESPONSE

Không có rule **DENY** rõ ràng

Inbound rules (1)

Type	Protocol	Port range	Source	Description - optional
HTTPS	TCP	443	0.0.0.0/0	inbound HTTPS

SG LOGICAL REFERENCE



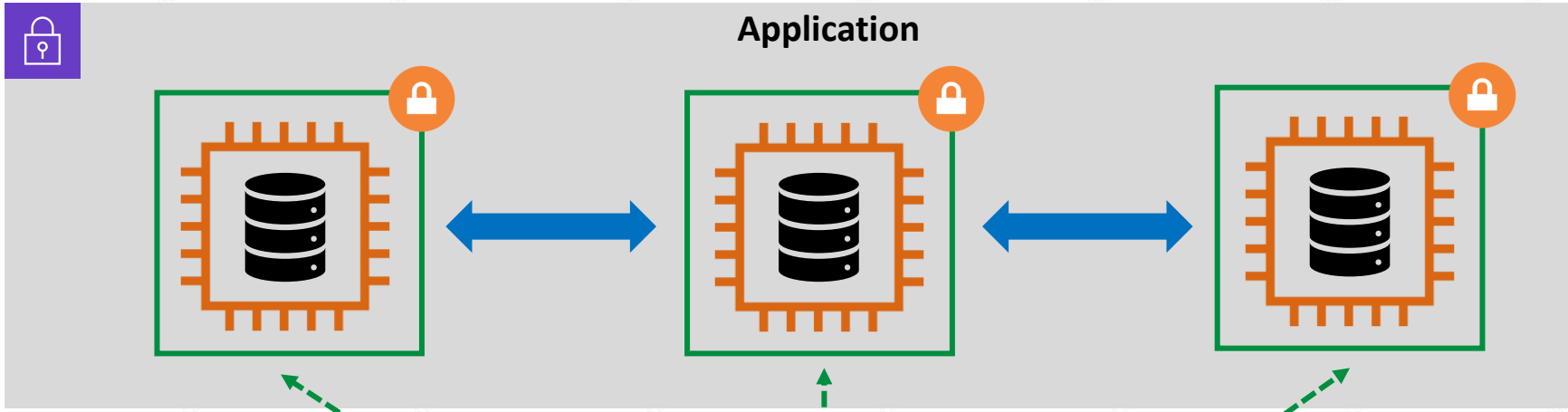
References

Security group rule ID	Type	Protocol	Port range	Source
sgr-0aac44e1665fb3a8e	Custom TCP	TCP	1337	sg-045d0c9d84d5f5455 / tsbi-sg-ec2-web-01

Security group rule ID	Type	Protocol	Port range	Source
sgr-03a3b0f2d766f1c59	HTTPS	TCP	443	0.0.0.0/0

SG SELF REFERENCE

Self reference có nghĩa là **bất cứ thứ gì** được gắn bởi **SG** này đều có thể tương tác với nhau



Nếu có bất cứ **thay đổi về IP** sẽ đều **không ảnh hưởng**

Security group rule ID	Type	Protocol	Port range	Source
sgr-0aac44e1665fb3a8e	Custom TCP	TCP	1337	sg-045d0c9d84d5f5455 / tsbi-sg-ec2-web-01
sgr-0db3ffaaf778ce1f9	All traffic	All	All	sg-0458cb0e59afdb1b0 / tsbi-sg-ec2-app-01

References chính nó

Step by Step

Easily

Hands On

Setup NACL & SG Custom

Practice

Explain

amazon web services™

Amazon Web Service - Training

NETWORKING WITH AWS

PRACTICE ARCHITECTURE

AWS ap-southeast-1

VPC – tsbi-vpc-study-01 (10.16.0.0/16)

Web

tsbi-sg-ssh-01

A

Database

Application

tsbi-sub-web-01

tsbi-ec2-web-01

10.16.48.0/20

tsbi-nacl-ssh-01

B

Database

Application

tsbi-sub-web-02

tsbi-ec2-web-02

10.16.112.0/20

C

Database

Application

tsbi-sub-web-03

tsbi-ec2-web-03

10.16.176.0/20

tsbi-rtb-public

SSH (TCP/22)

Internet Gateway

tsbi-igw-01

Internet

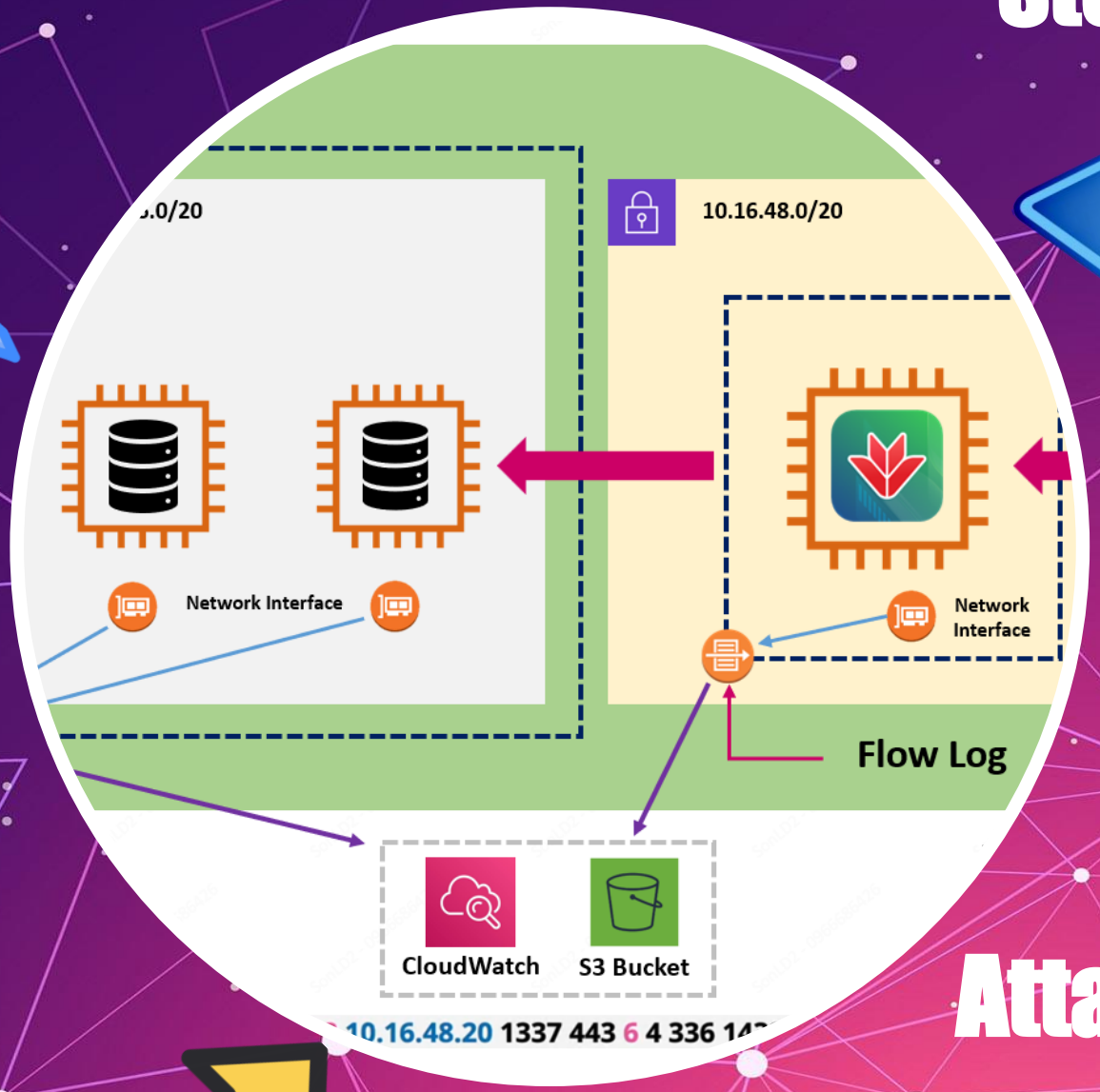
AWS Public Zone

Storage

Loging

Networking

AWS Flow Logs



Attach

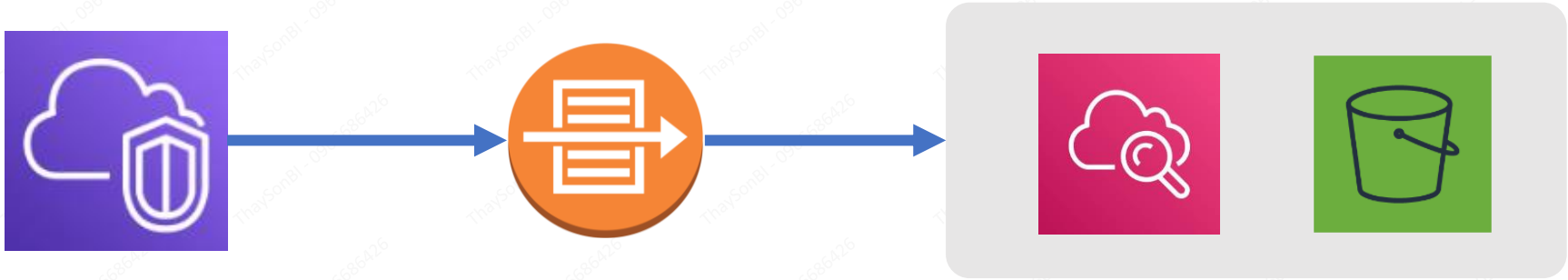
ENJ

amazon web services™

Amazon Web Service - Training

OVERVIEW

VPC Flow log là một tính năng được bật để ghi lại thông tin về các traffic **đi vào và đi ra** khỏi **network interface** nằm trong VPC của bạn



1. **Mornitoring** traffic mà tương tác với **instance** của bạn
2. Đóng vai trò **chuẩn đoán,** điều mà ở **security group** bị hạn chế
3. **Xác định** hướng của traffic **đến và đi** khỏi network interface

CHARACTERISTICS

Metadata được lưu trữ, **không phải** nội dung của gói tin

Gắn vào **VPC** – **Toàn bộ ENIs** của VPC đó

Gắn vào **Subnet** – **Toàn bộ ENIs** của Subnet đó

Flow Log không real-time

Log có thể được lưu trữ trong **S3** hoặc **CloudWatch logs**

… cũng có thể là **Athena** để query trực tiếp

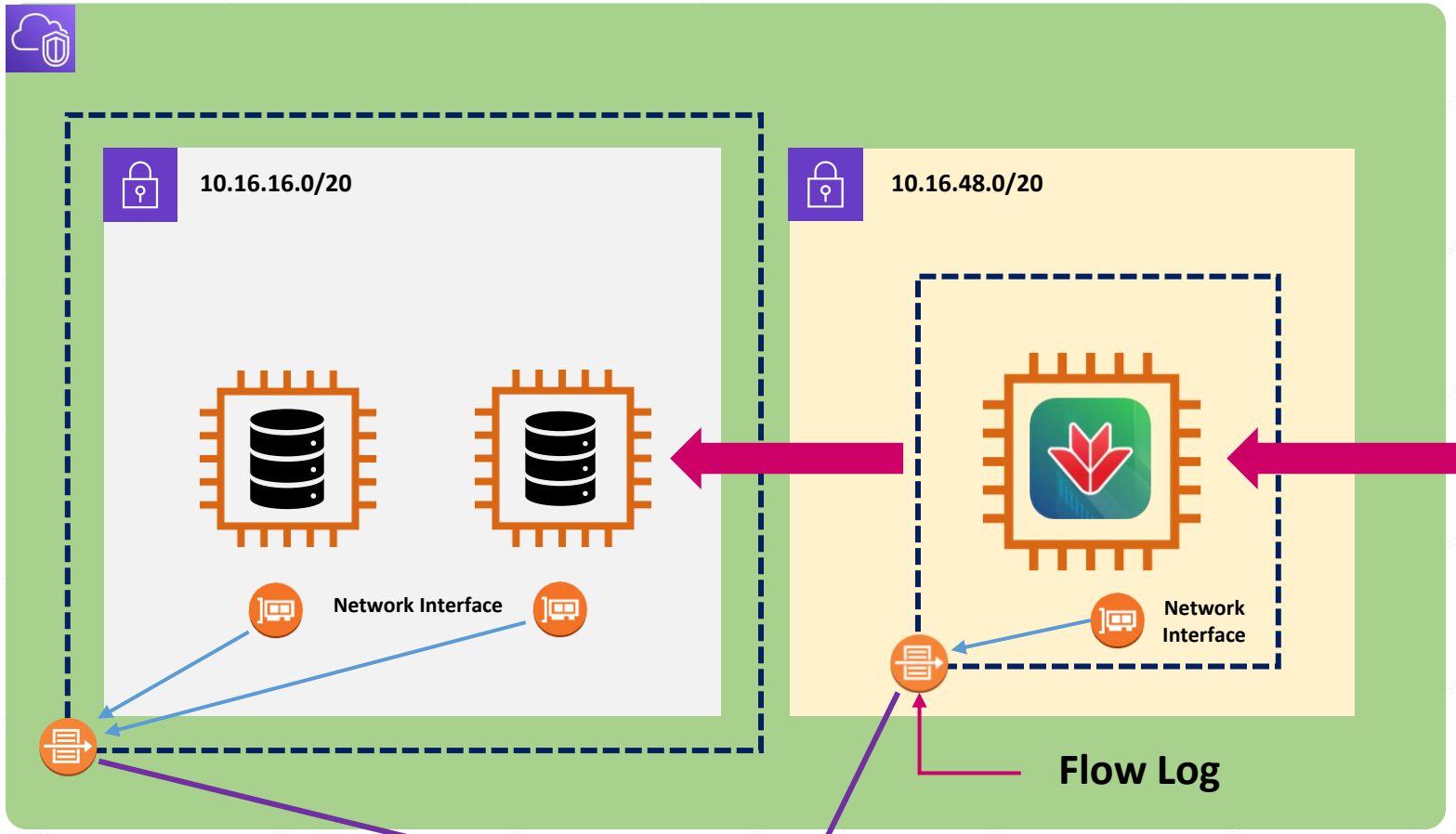
FLOW LOG WORKING

Flow Logs có thể cấu hình **lên nhiều tầng**

VPC

Subnet

Interface



Flow Logs có thể ghi lại các trạng thái **ACCEPTED, REJECTED** hoặc **ALL** metadata

Flow Log Records

2 ACC-ID eni-ID 119.18.34.78 10.16.48.20 1337 443 6 4 336 1432917027 1432917142 ACCEPT OK

Easily

Step by Step

Hands On

Setup Flow Logs

Practice

Explain

amazon web services™

Amazon Web Service - Training

MAIN STEPS

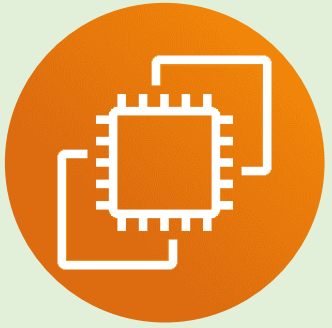
1 STEP

Setup **Flow Log** in VPC

2 STEP

Setup **Flowlog** in Subnet

3 STEP



Create **EC2** and setup **Flowlog**

4 STEP

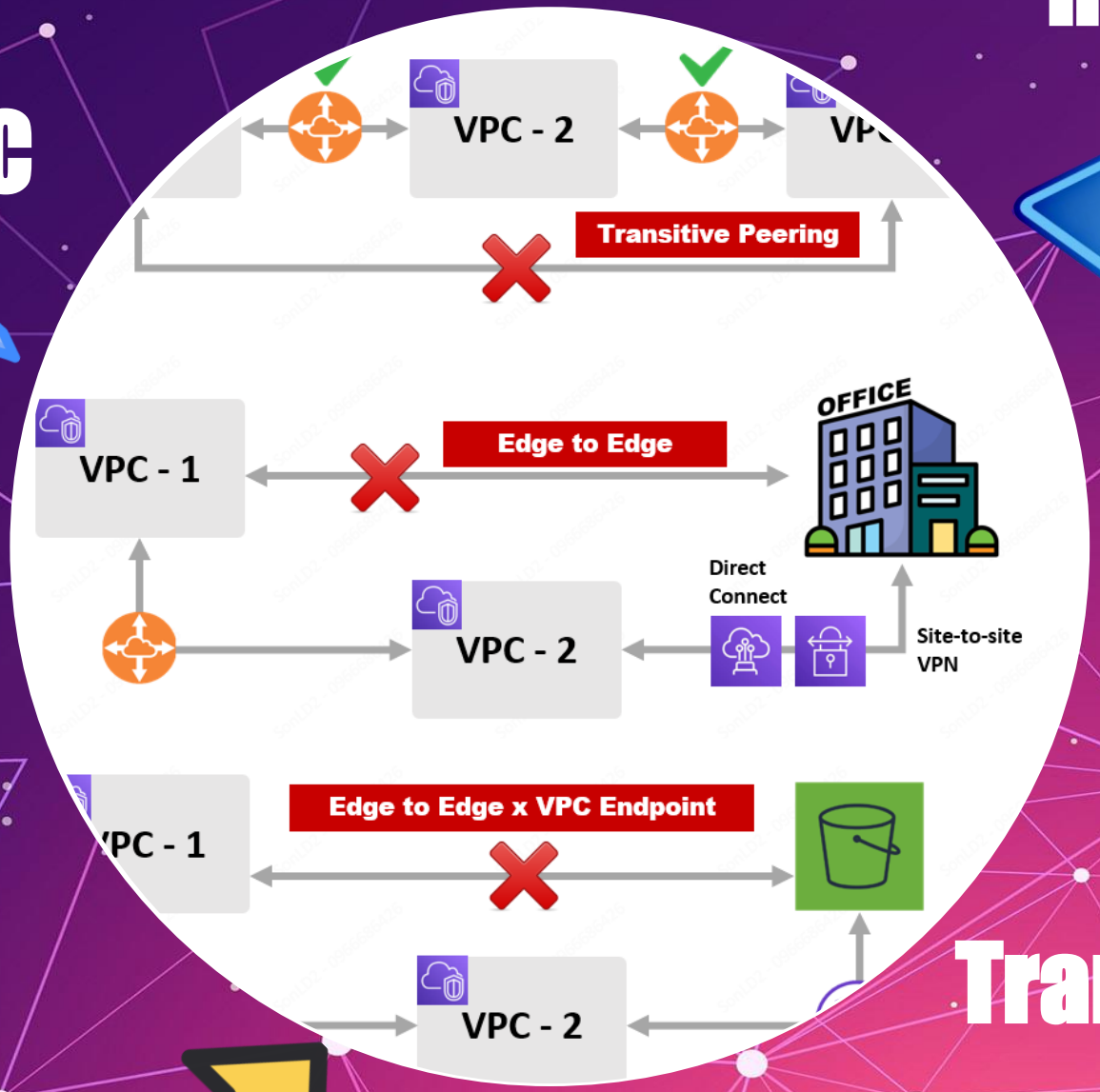
Delete all resouce **EC2** instance

Region

VPC-VPC

Networking

Peering Connection



Transfer

AZ

amazon web services™

Amazon Web Service - Training

NETWORKING WITH AWS

PEERING CONNECTION

AWS VPC Peering

Chỉ với 2 VPC độc lập không thể kết nối với nhau **trực tiếp**

ap-southeast-1

tsbi-vpc-study-02
10.17.0.0/16

sub-A
10.17.32.0/20

sub-B
10.17.48.0/20

tsbi-vpc-study-03
10.18.0.0/16

sub-A
10.18.32.0/20

sub-B
10.18.48.0/20

VPC Peering

Phương thức cho phép **2 network** kết nối **trực tiếp** với nhau

us-east-1

10.19.48.0/20

us-west-2

10.20.48.0/20

Không thể kết nối **3 VPC** với nhau

CHARACTERISTICS

Chỉ kết nối được **2 VPC** với nhau (encrypted connect)

Một VPC chỉ có **tối đa 125** peering connection (**mặc định**: **50**)

Chia sẻ dữ liệu **cùng/khác** account, region

Sử dụng **private IPv4** hoặc **IPv6** để giao tiếp với nhau

Cần phải thiết lập **Routing**, dùng **SGs, NACLs** để lọc traffic

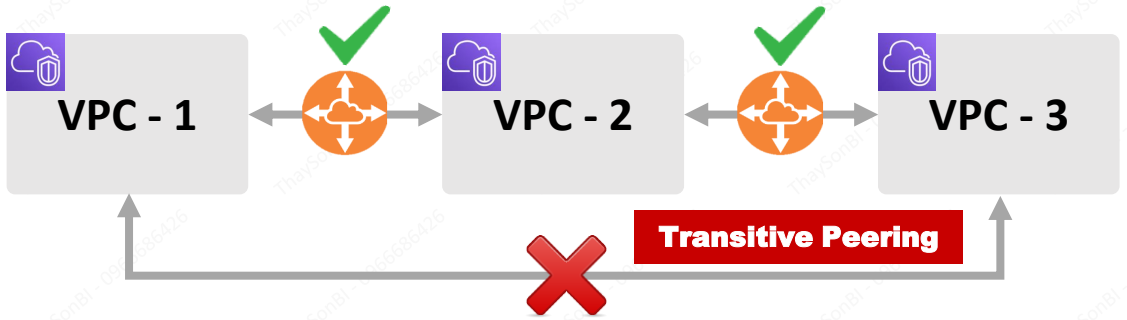
KHÔNG hỗ trợ **bắc cầu peering, overlap CIDR Block**

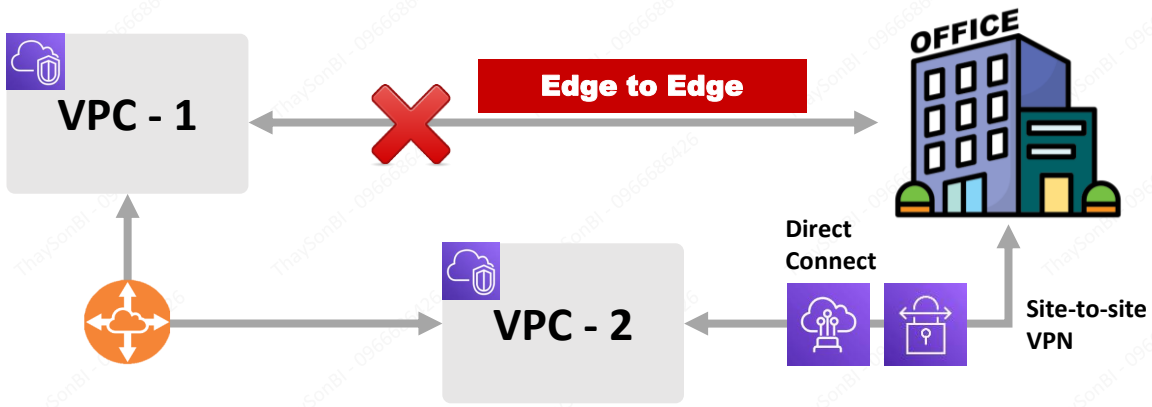
Nếu 2 VPC **chung Region** → **SG** có thể dùng **Peering**

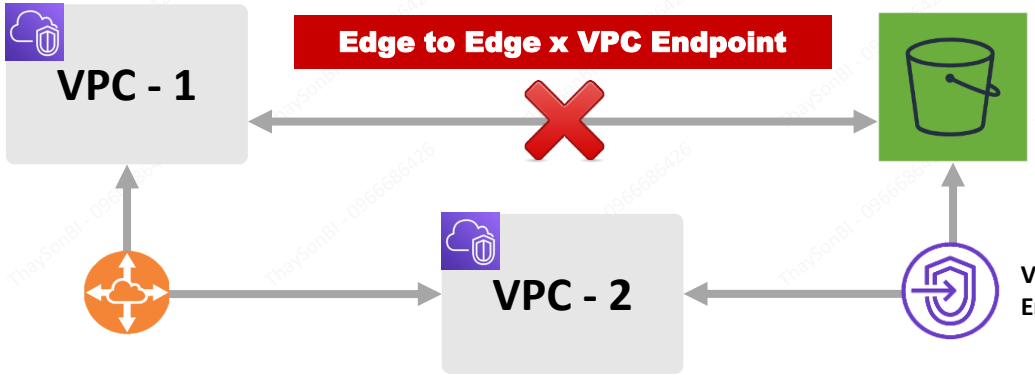
NETWORKING WITH AWS

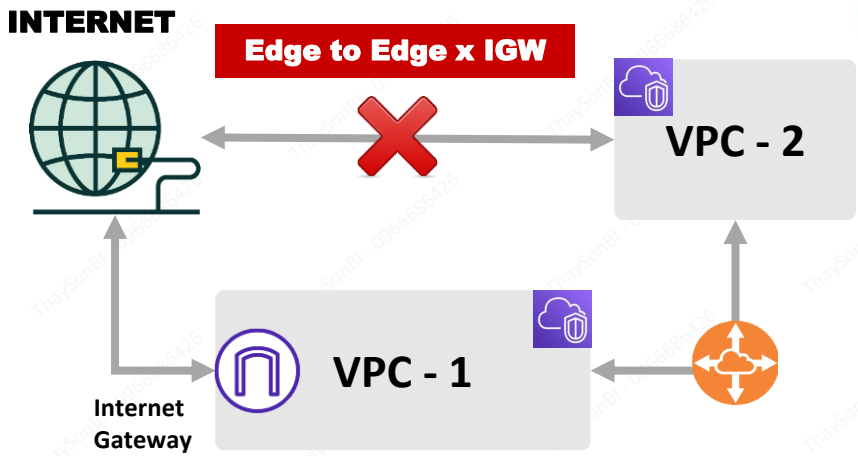
PEERING NOT SUPPORT

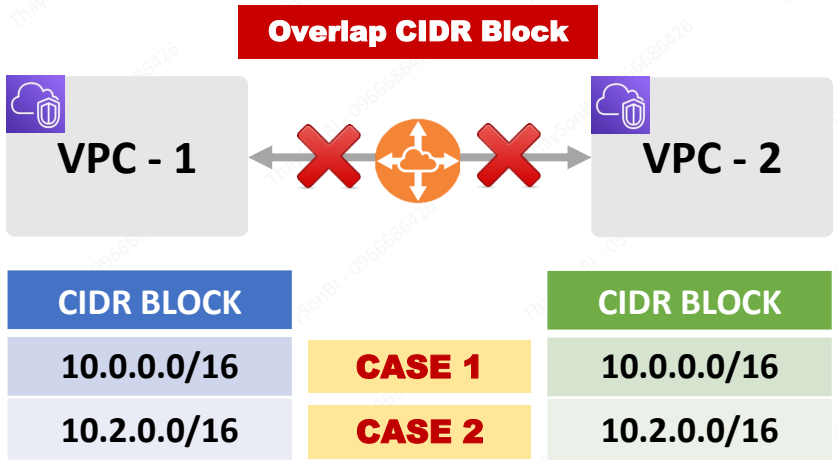
AWS VPC Peering











CIDR BLOCK		CIDR BLOCK
10.0.0.0/16	CASE 1	10.0.0.0/16
10.2.0.0/16	CASE 2	10.2.0.0/16

ESTABLISH A PEERING

AWS
VPC Peering

VPC - A

VPC - B

Maximum 25 req

Gửi yêu cầu để tạo VPC Peering

Chấp nhận yêu cầu VPC Peering

2 bên (VPC) thêm Routes vào Route Table

Cập nhật SG hoặc DNS Resolution nếu cần

REQUESTER

ACCEPTER

VPC PEERING LIFECYCLE

Request

Pending Accept

Provisioning

Active

Nếu không xác nhận (accepted) trong vòng **7 ngày**

Deleting

Quy trình thực thi áp dụng cho kết nối giữa các **Region khác nhau**. Và **yêu cầu xóa** đến từ 1 bên trong party

Failed

Expried

Rejected

Deleted

Hiển thị trong vòng **2 giờ** đối với **requester**

Hiển thị trong vòng **2 ngày** với cả **requester** và **accepter**

Hiển thị trong **2 ngày** với **requester** và **2 giờ** với **accepter**

Hiển thị trong **2 giờ** với **người muốn xóa** và **2 ngày** với **người kết hợp**

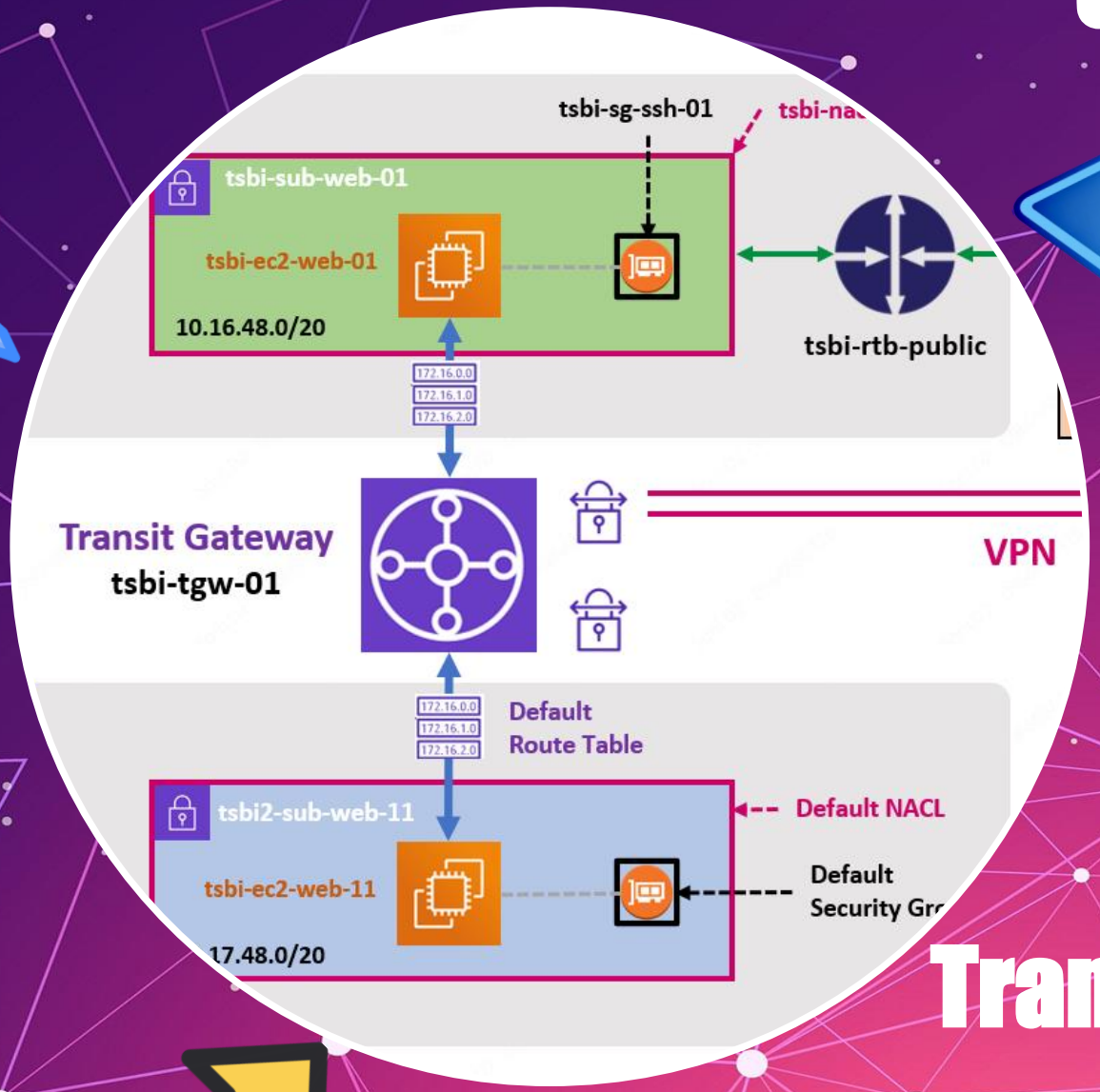
No longer visible

Networking

Transit Gateway

Hub

Global



Transitive

On-Prem

amazon web services™

Amazon Web Service - Training

OVERVIEW

AWS Transit Gateway

Network Transit Hub để **VPC** kết nối với **On-Premise**

Giảm thiểu độ **phức tạp** khi thiết kế mạng

Luôn sẵn sàng **(High Availability)** và dễ mở rộng **(Scalable)**

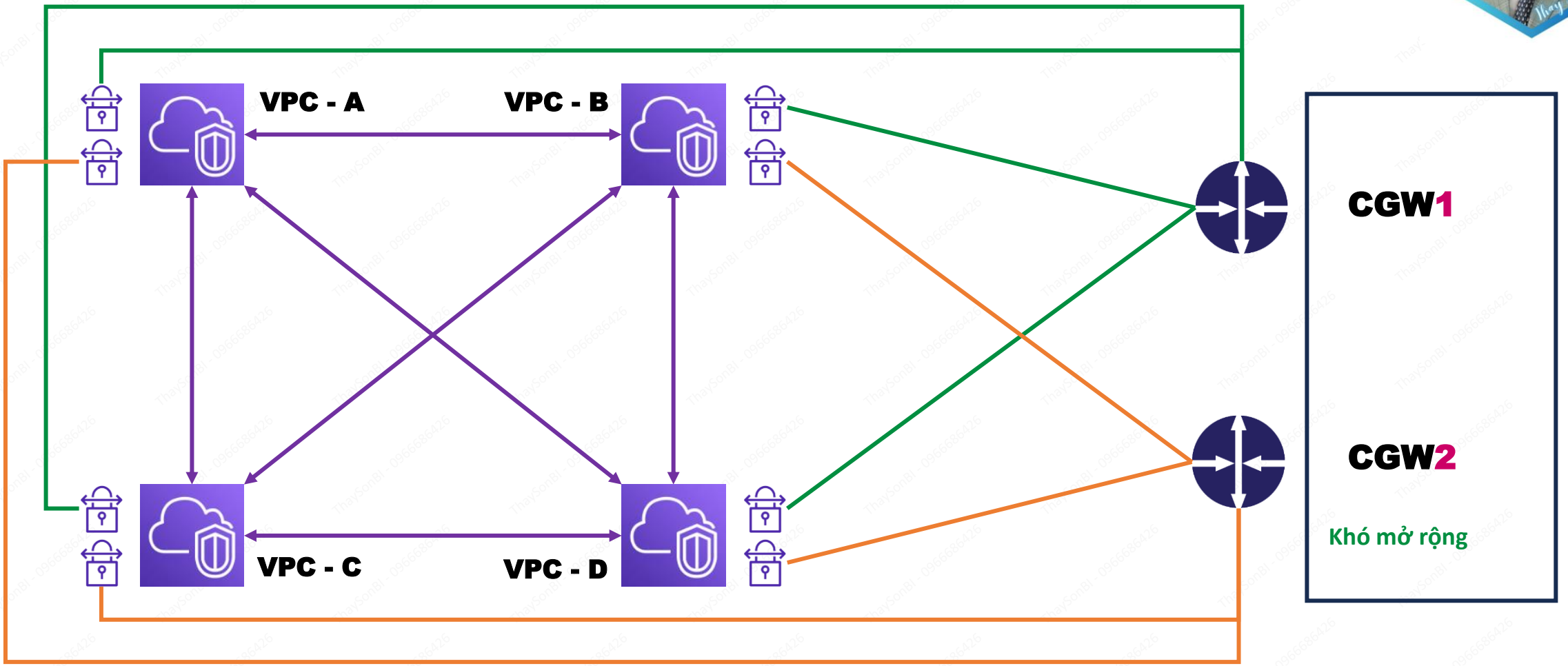
Gắn vào được nhiều mạng khác nhau

VPC, Site-to-Site VPN và **Direct Connect Gateway**

NETWORKING
WITH AWS

W/O TRANSIT GATEWAY

AWS
Transit Gateway



NETWORKING WITH AWS

WITH TRANSIT GATEWAY

AWS Transit Gateway

Direct Connect Gateway

VPC - A

VPC - B

TGW có thể tích hợp trực tiếp cùng với Direct Connect để truyền VIF

VPC Attachments được cấu hình cùng với subnet trong mỗi AZ , nơi chứa dịch vụ được gọi đến

CGW1

CGW2

VPC - C

VPC - D

Peering Attachment
Cross-Region
Same/Cross Account

TG CONSIDERATIONS

Hỗ trợ **transitive routing**

Có thể được sử dụng để tạo ra **Global Networks**

Có thể chia sẻ **giữa các account** sử dụng **AWS RAM**

Peer với những **region khác nhau…**
same hoặc **cross account**

Giảm sự **phức tạp** so với việc **không** sử dụng **TGW**

Easily

Step by Step

Hands On

Using Transit Gateway

Practice

Explain

amazon web services™

Amazon Web Service - Training

PRACTICE

AWS Transit Gateway