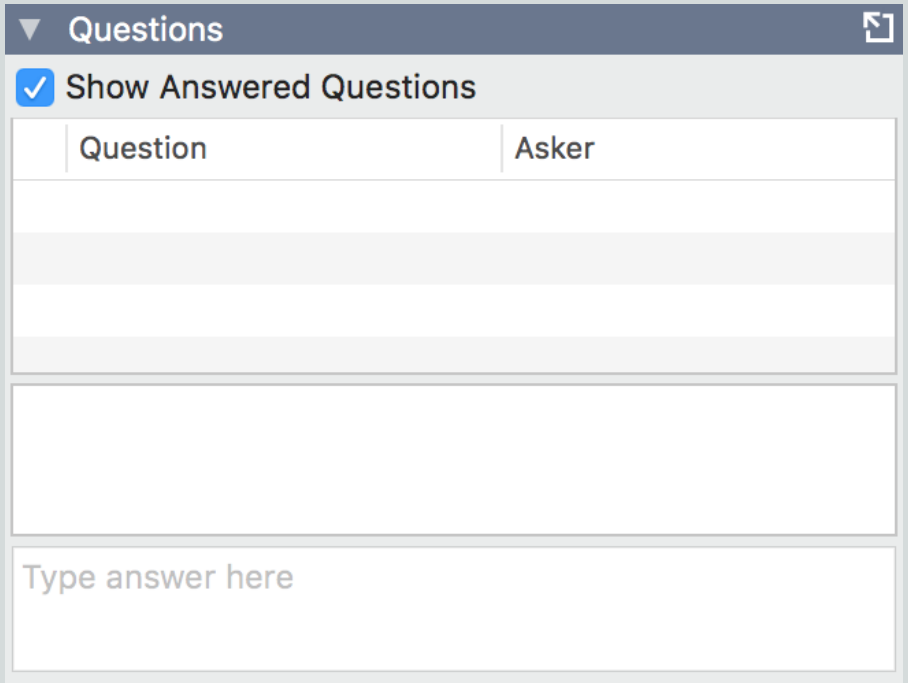
AWS Builders Program 300 – Advanced AWS Networking Design

" TransitGateway, NetworkFirewall, GWLB 디자인 심화학습 "

최 우 형 (whchoi@amazon.com) | Solutions Architect

강연 중 질문하는 방법



Go to Webinar “Questions” 창에 자신이 질문한 내역이 표시됩니다. 기본적으로 모든 질문은 공개로 답변 됩니다만 본인만 답변을 받고 싶으면 (비공개)라고 하고 질문해 주시면 됩니다.

고지 사항(Disclaimer)

본 컨텐츠는 고객의 편의를 위해 AWS 서비스 설명을 위해 온라인 세미나용으로 별도로 제작, 제공된 것입니다. 만약 AWS 사이트와 컨텐츠 상에서 차이나 불일치가 있을 경우, AWS 사이트(aws.amazon.com)가 우선합니다. 또한 AWS 사이트 상에서 한글 번역문과 영어 원문에 차이나 불일치가 있을 경우(번역의 지체로 인한 경우 등 포함), 영어 원문이 우선합니다.

Agenda

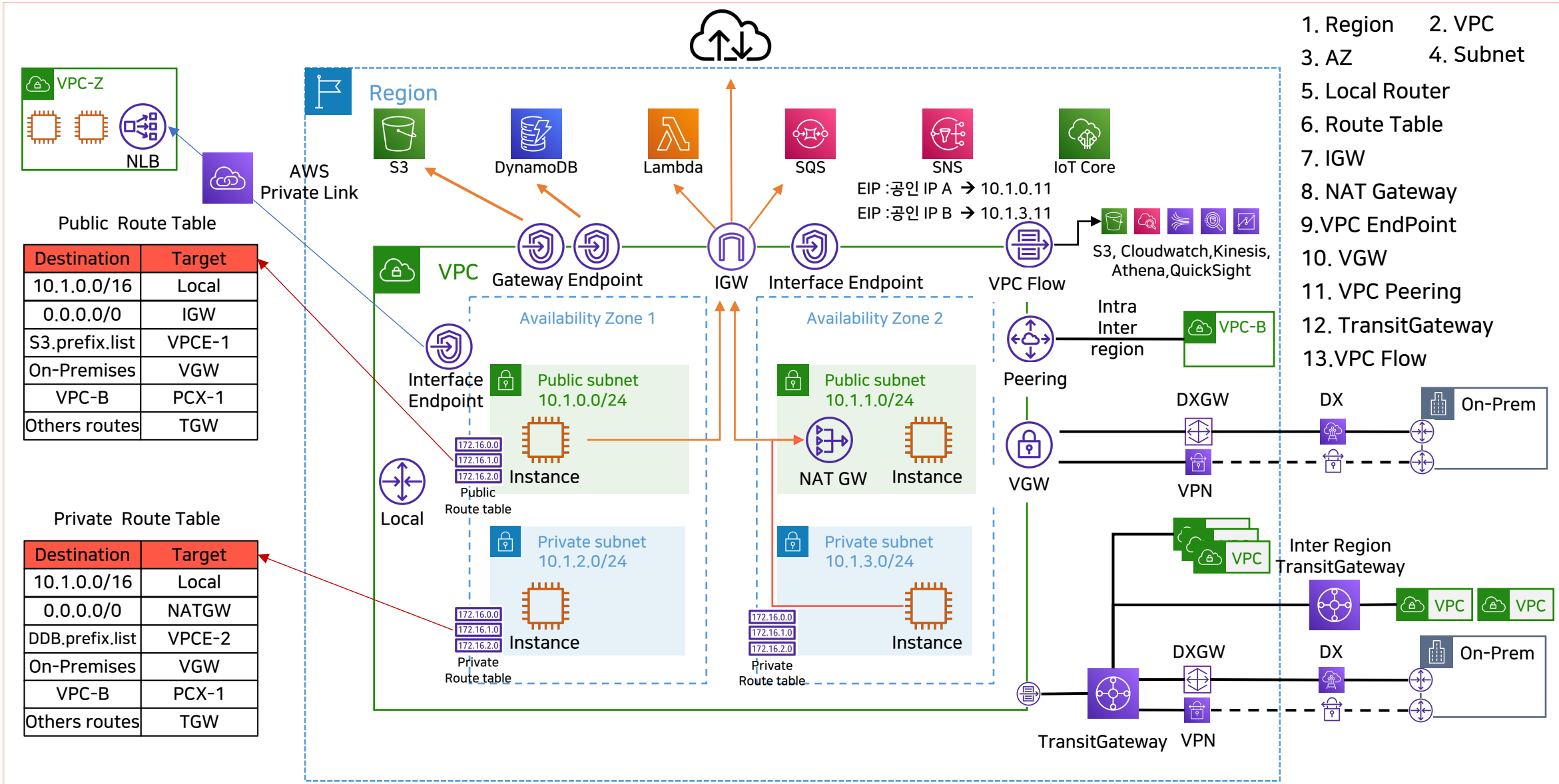
- ❑ VPC Networking Re:Cap
- ❑ AWS TransitGateway
- ❑ AWS GWLB
- ❑ AWS Network Firewall

AWS Builders - Program 300

VPC Networking Re:Cap

VPC Networking Re:Cap –VPC 트래픽 흐름 알아보기

AWS Builders - Program 300



Public Route Table

Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	IGW
S3.prefix.list	VPCE-1
On-Premises	VGW
VPC-B	PCX-1
Others routes	TGW

Private Route Table

Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	NATGW
DDB.prefix.list	VPCE-2
On-Premises	VGW
VPC-B	PCX-1
Others routes	TGW

VPC Networking Re:Cap –VPC 트래픽 흐름 알아보기

AWS Builders - Program 300

14. Ingress Routing
15. GWLB & NWFW
16. VPC Traffic Mirroring

VPC Ingress Route Table

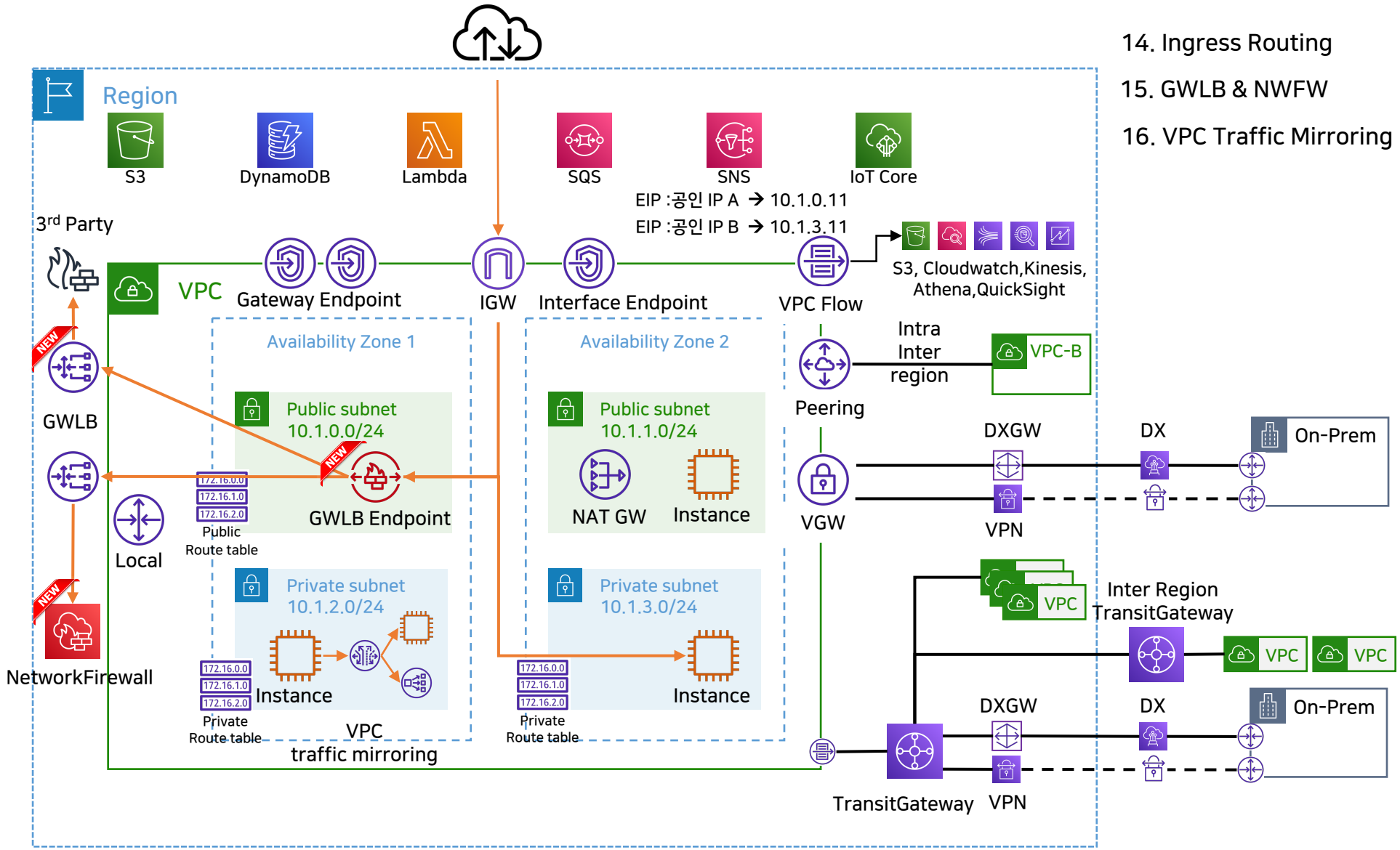
Destination	Target
10.1.0.0/16	Local
10.1.3.0/24	GWLBE-1

Public Route Table

Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	IGW
S3.prefix.list	VPCE-1
On-Premises	VGW
VPC-B	PCX-1
Others routes	TGW

Private Route Table

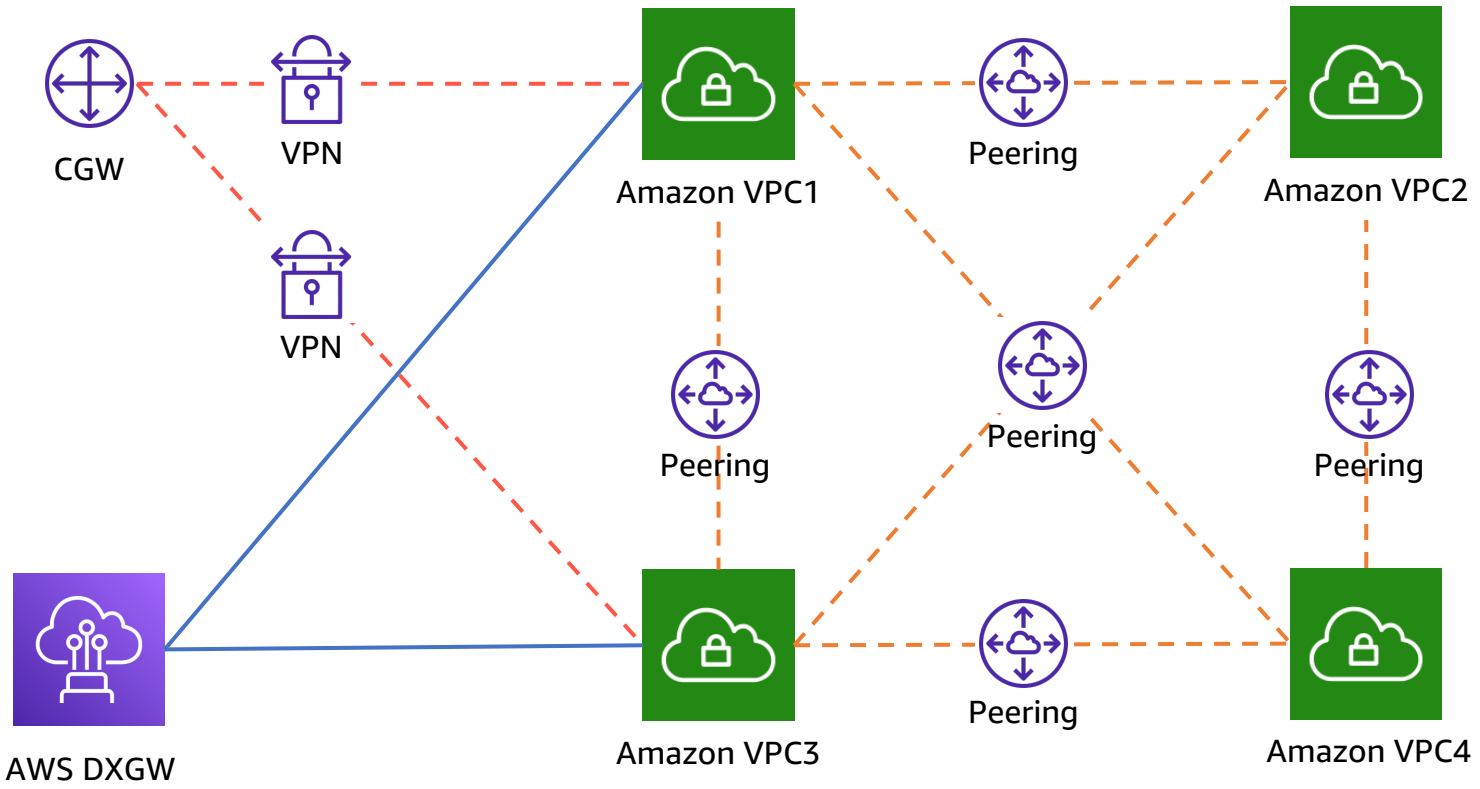
Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	GWLBE-1
DDB.prefix.list	VPCE-2
On-Premises	VGW
VPC-B	PCX-1
Others routes	TGW



AWS Builders - Program 300

TransitGateway Design

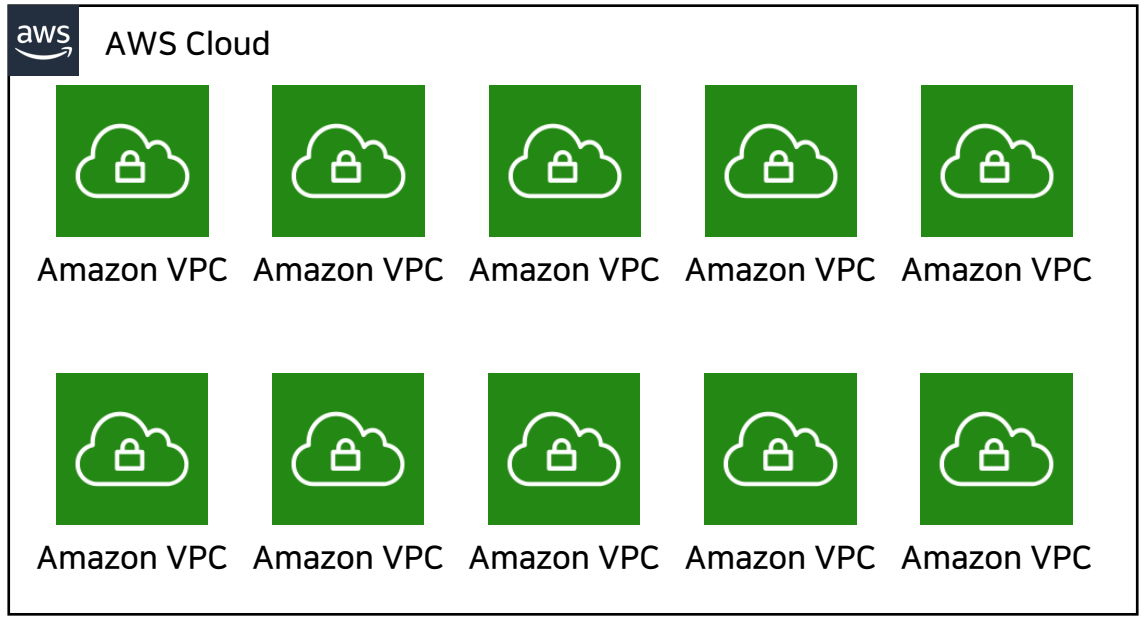
AWS TransitGateway 이전의 모습



- VPC Full Mesh 연결 기반의 관리
- VPN 연결 관리의 어려움
- DX 회선 연결 관리의 어려움

VPC Peering 의 관리적 부담

10개의 VPC가 있고, 상호간에 연결해야 한다면???



$$\frac{10(10-1)}{2}$$

45개 Peering

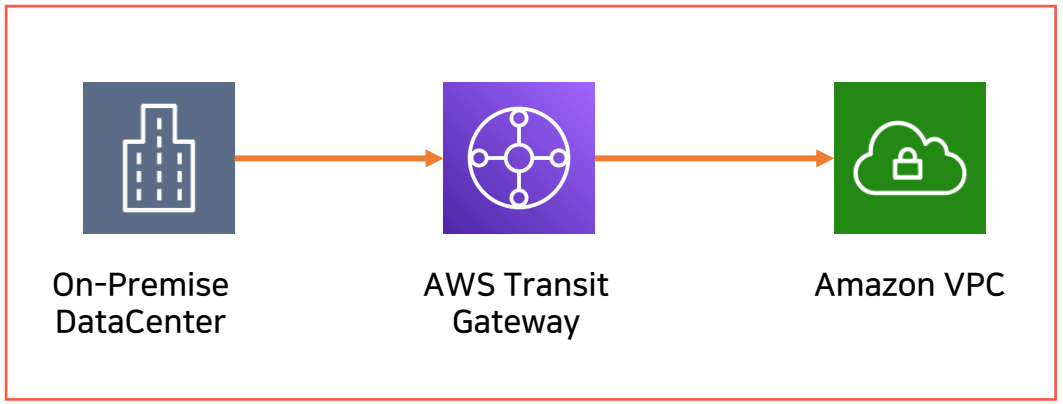
100개의 VPC가 있고, 상호간에 연결해야 한다면???

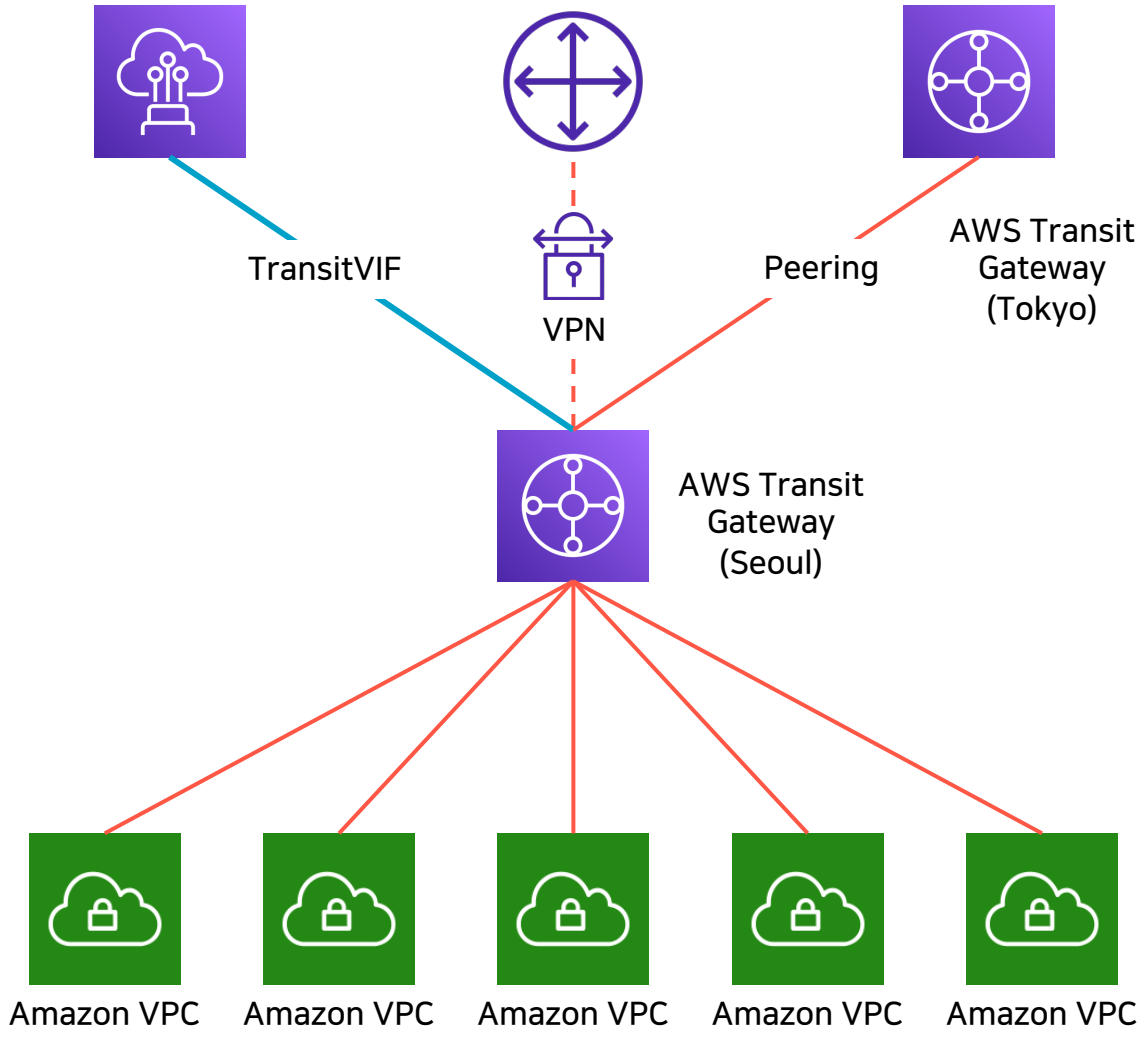
$$\frac{100(100-1)}{2}$$

4500개 Peering

TransitGateway 장점

TransitGateway 기반의 간편한 연결



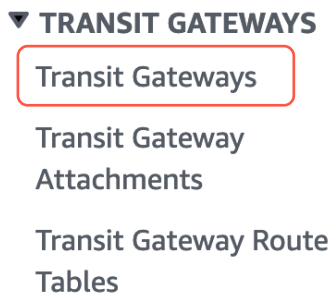


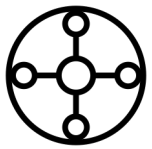
- 간편한 연결
- 가시성 및 제어성 향상
- 향상된 보안
- 유연한 멀티캐스트

TransitGateway 핵심컨셉 이해하기

AWS TransitGateway

- Attachment
- RouteTable
  - ❑ Association
  - ❑ Propagation





AWS TransitGateway

Attachment

RouteTable - Association

- Propagation

- Route

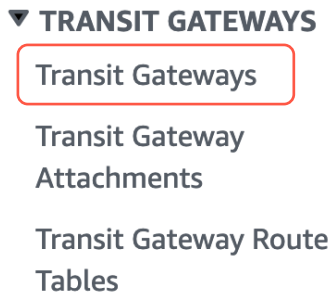
aws

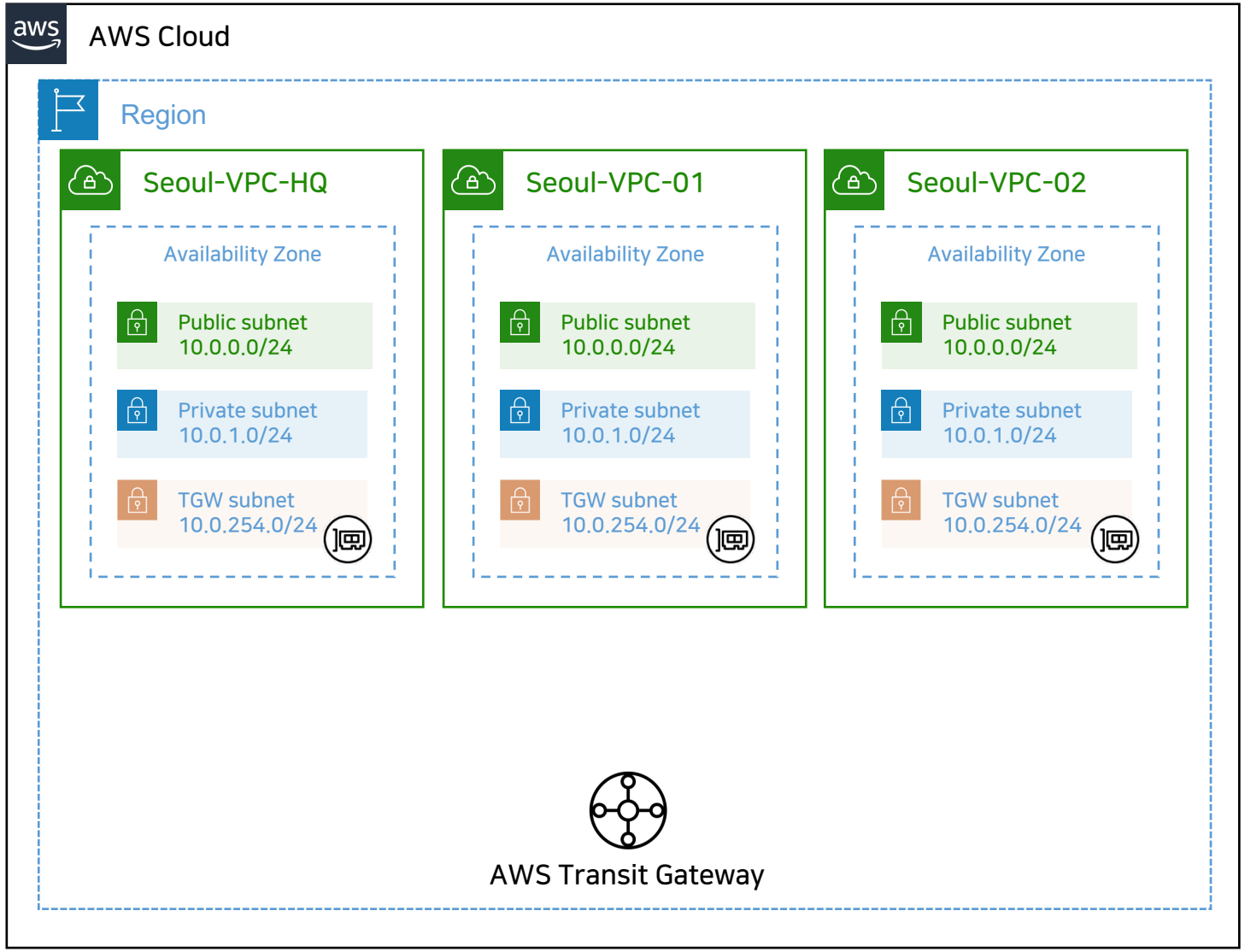
TransitGateway 핵심컨셉 이해하기

TransitGateway

AWS TransitGateway

- Attachment
- RouteTable
  - ❑ Association
  - ❑ Propagation
  - ❑ Route

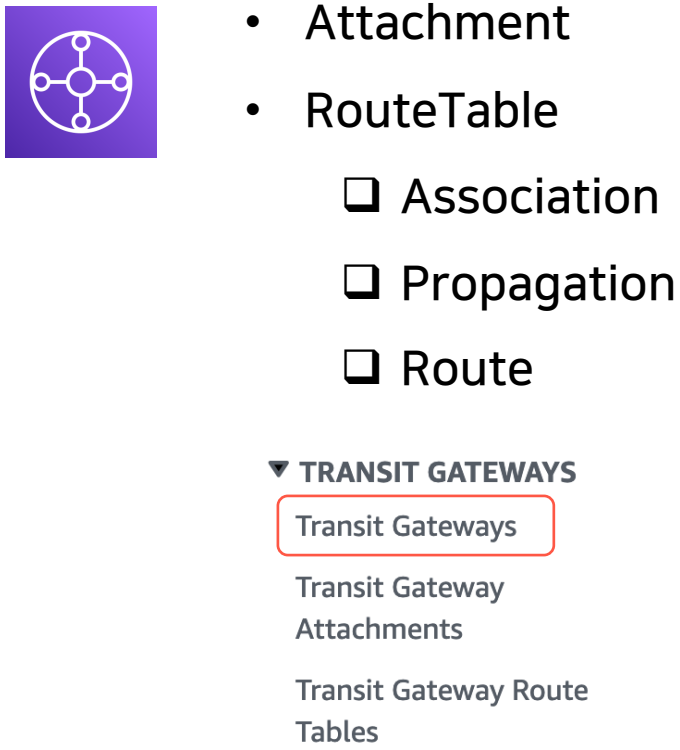




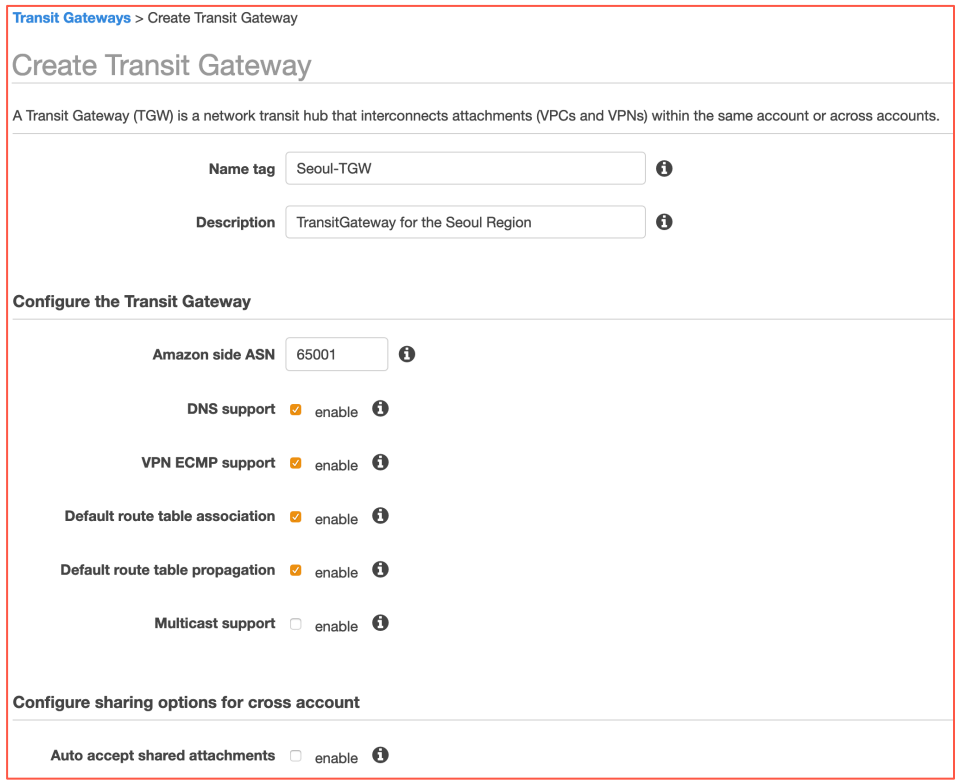
TransitGateway 핵심컨셉 이해하기
TransitGateway

AWS TransitGateway

- Attachment
- RouteTable
  - ❑ Association
  - ❑ Propagation
  - ❑ Route



VPC – Transit Gateway – Create Transit Gateway



TransitGateway 핵심컨셉 이해하기
Attachment

AWS TransitGateway

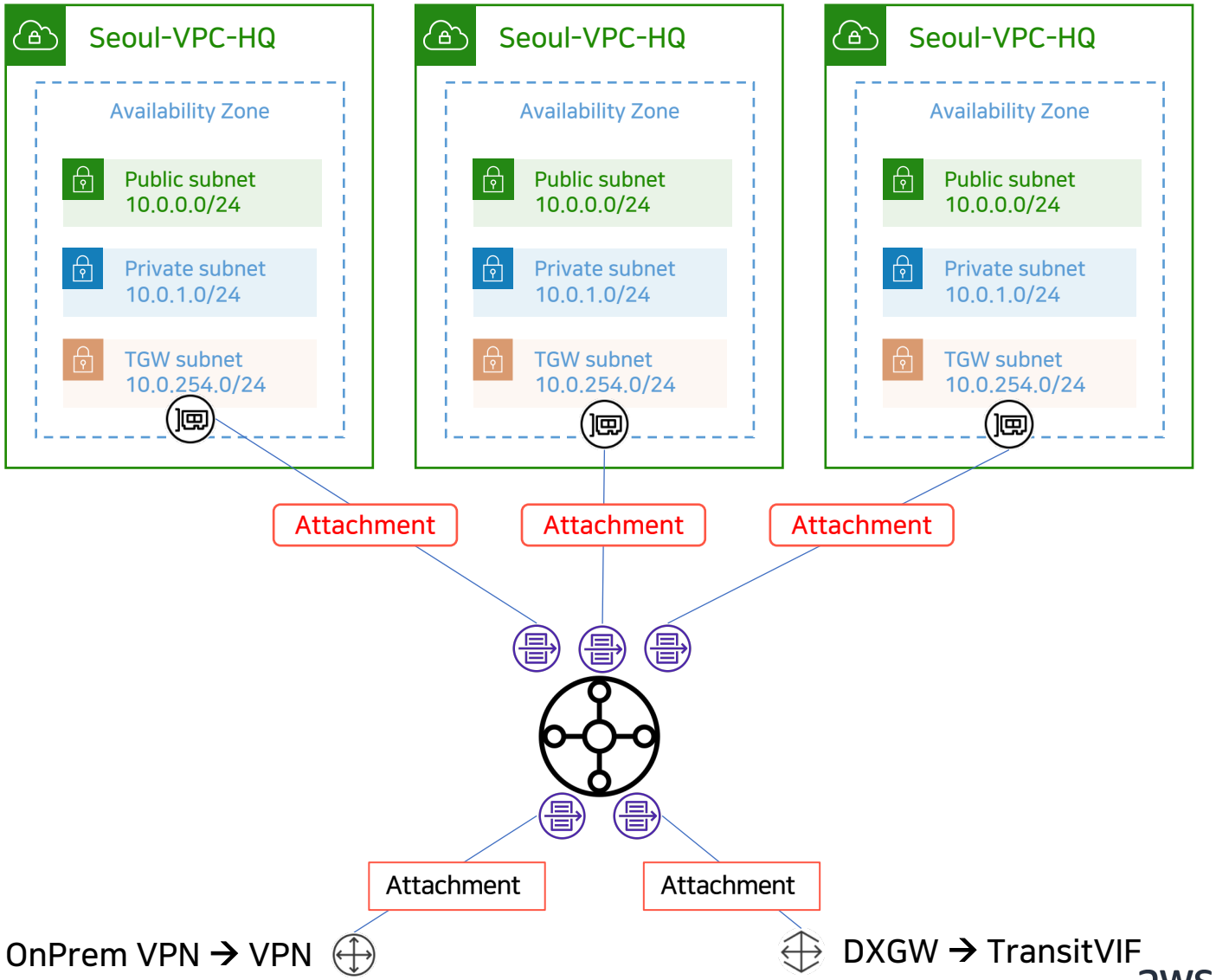
- Attachment
- RouteTable
  - ❑ Association
  - ❑ Propagation
  - ❑ Route

▼ TRANSIT GATEWAYS

Transit Gateways

Transit Gateway Attachments

Transit Gateway Route Tables



TransitGateway 핵심컨셉 이해하기
Attachment

AWS TransitGateway

- Attachment
- RouteTable
  - ❑ Association
  - ❑ Propagation
  - ❑ Route

▼ TRANSIT GATEWAYS

Transit Gateways

Transit Gateway Attachments

Transit Gateway Route Tables

VPC – Transit Gateway – Create Transit Gateway

Transit Gateway Attachments > Create Transit Gateway Attachment

Create Transit Gateway Attachment

Select a Transit Gateway and the type of attachment you would like to create.

Transit Gateway ID* tgw-08d037f95bb3ebee7 — Transit Gateway ID

Attachment type VPC — Attachment 타입 (VPC,VPN,TGW Peering)

VPC Attachment

Select and configure your VPC attachment.

Attachment name tag Seoul-TGW-Attach-Seoul-VPC-HQ

DNS support ☑ enable

IPv6 support ☐ enable

VPC ID* vpc-0c52b711f5af2ab79 — 연결할 VPC 선택

Subnet IDs* subnet-04880c777d61ce86c, subnet-055029784c028f5a7

	Availability Zone	Subnet ID
☑	ap-northeast-2a	subnet-04880c777d61ce86c (Seoul-VPC-HQ-TGWSubnetA)
☑	ap-northeast-2b	subnet-055029784c028f5a7 (Seoul-VPC-HQ-TGWSubnetB)
☐	ap-northeast-2c	No subnet available
☐	ap-northeast-2d	No subnet available

TGW와 연결할 Subnet 선택

TransitGateway 핵심컨셉 이해하기
Attachment

AWS TransitGateway

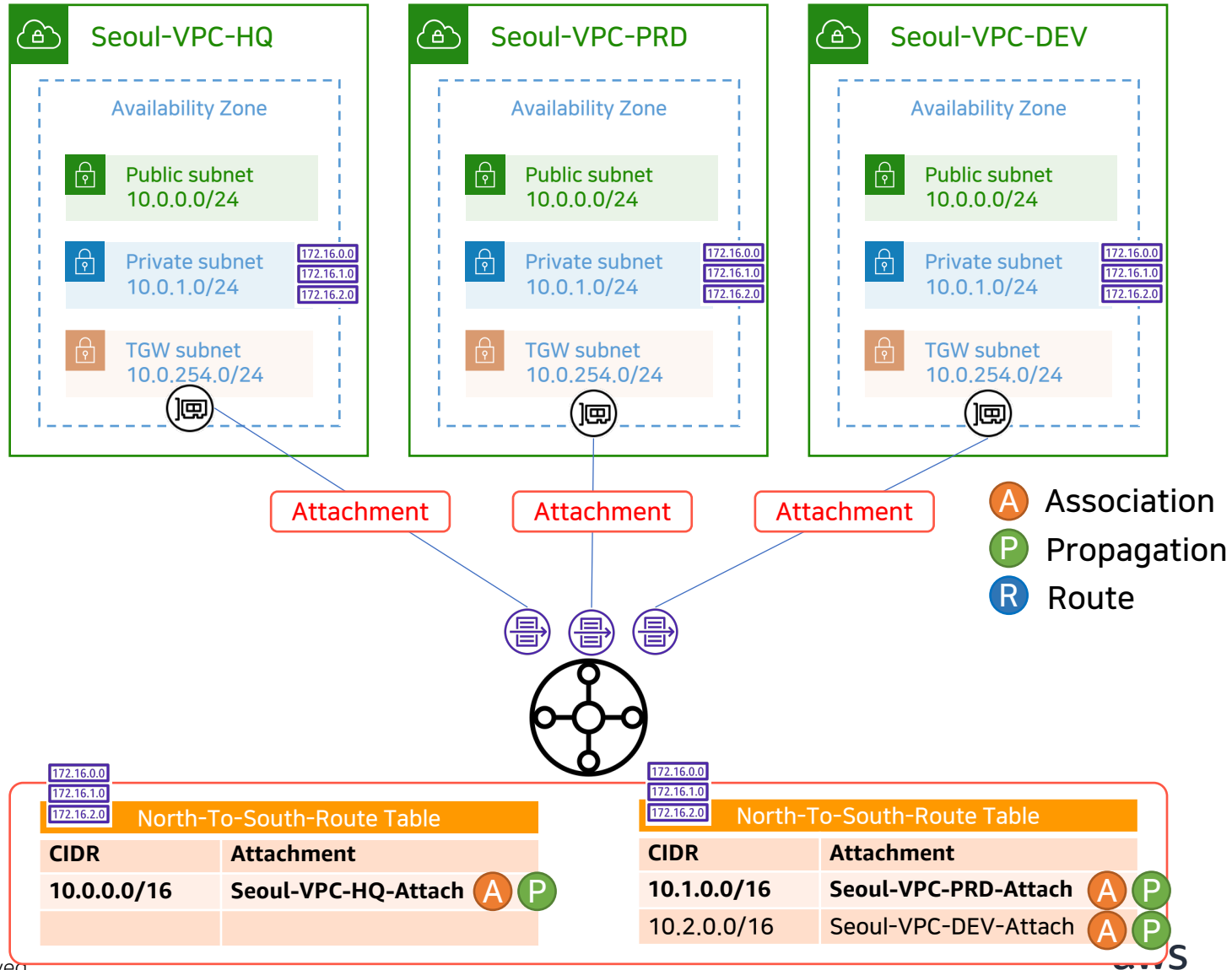
- Attachment
- RouteTable
  - ❑ Association
  - ❑ Propagation
  - ❑ Route

▼ TRANSIT GATEWAYS

Transit Gateways

Transit Gateway Attachments

Transit Gateway Route Tables



TransitGateway 핵심컨셉 이해하기
Attachment

AWS TransitGateway

- Attachment
- RouteTable
  - ❑ Association
  - ❑ Propagation
  - ❑ Route

▼ TRANSIT GATEWAYS

Transit Gateways

Transit Gateway Attachments

Transit Gateway Route Tables

VPC – Transit Gateway – Create Transit Gateway

Name	Transit Gateway attachment ID	Transit Gateway ID	Resource type	Resource ID	State	Associated route table ID	Association state
Seoul-TGW-Attach-Seoul-VPC-STG	tgw-attach-0fb774b4b27f1e4d8	tgw-08d037f95bb3ebee7	VPC	vpc-0e728bf16015c7a9b	available	tgw-rtb-00c28abe36e2d79ef	associated
Seoul-TGW-Attach-Seoul-VPC-PRD	tgw-attach-01a6c52c410fd777b	tgw-08d037f95bb3ebee7	VPC	vpc-03b612e4a3af6f0b1	available	tgw-rtb-00c28abe36e2d79ef	associated
Seoul-TGW-Attach-Seoul-VPC-HQ	tgw-attach-06ba039ae3ec2940f	tgw-08d037f95bb3ebee7	VPC	vpc-0c52b711f5af2ab79	available	tgw-rtb-0731dd0c6b867836d	associated
Seoul-TGW-Attach-Seoul-VPC-DEV	tgw-attach-0d639b47c3b5a6ea9	tgw-08d037f95bb3ebee7	VPC	vpc-0d242d945209a2056	available	tgw-rtb-00c28abe36e2d79ef	associated

Transit Gateway Attachment: tgw-attach-06ba039ae3ec2940f

Details | Tags

Transit Gateway attachment ID	tgw-attach-06ba039ae3ec2940f	**Transit Gateway owner ID**	606879168280
Transit Gateway ID	tgw-08d037f95bb3ebee7	**Resource owner account ID**	606879168280
Resource type	VPC	**State**	available
Resource ID	vpc-0c52b711f5af2ab79	**Associated route table**	tgw-rtb-0731dd0c6b867836d
Association state	associated	**DNS support**	enable
IPv6 support	disable	**Subnet IDs**	subnet-04880c777d61ce86c subnet-055029784c028f5a7

- Attachment 연결을 위해서 VPC 각 가용 영역별 서브넷 지정 필요
- 별도의 서브넷 지정을 권고 (TGW-Attachment Subnet)
- VPC 서브넷에서 라우팅 테이블 경로가 있어야 트래픽 전송

TransitGateway 핵심컨셉 이해하기
RouteTable - Assocation

AWS TransitGateway

- Attachment
- RouteTable
  - ❑ Association
  - ❑ Propagation
  - ❑ Route

▼ TRANSIT GATEWAYS

Transit Gateways

Transit Gateway Attachments

Transit Gateway Route Tables

172.16.0.0 / 172.16.1.0 / 172.16.2.0 VPC – Transit Gateway – Transit Gateway Route Table - Create Transit Gateway Route Table

Transit Gateway Route Tables > Create Transit Gateway Route Table

Create Transit Gateway Route Table

A route table controls how traffic flows for all associated attachments.

Name tag Seoul-TGW-RT-East-To-West

Transit Gateway ID* tgw-08d037f95bb3ebee7

Transit Gateway Route Tables > Create association

Create association

Associating an attachment to a route table allows traffic to be sent from the attachment to the target route table. An attachment can only be associated to one route table.

Transit Gateway ID tgw-08d037f95bb3ebee7

Transit Gateway route table ID tgw-rtb-00c28abe36e2d79ef

Choose attachment to associate* tgw-attach-06ba039ae3ec2940f

TGW Route Table과 Attachment ID 연결

* 필수 사항

속성별 필터

Attachment ID	Name tag	Resource ID	Resource Type	Resource owner ID	Association route table
tgw-attach-01a6c52c410fd777b	Seoul-TGW-Attach-Seoul-VPC-PRD	vpc-03b612e4a3af6f0b1	vpc	606879168280	tgw-rtb-00c28abe36e2d79ef
tgw-attach-06ba039ae3ec2940f	Seoul-TGW-Attach-Seoul-VPC-HQ	vpc-0c52b711f5af2ab79	vpc	606879168280	tgw-rtb-0731dd0c6b867836d
tgw-attach-0d639b47c3b5a6ea9	Seoul-TGW-Attach-Seoul-VPC-DEV	vpc-0d242d945209a2056	vpc	606879168280	tgw-rtb-00c28abe36e2d79ef
tgw-attach-0fb774b4b27f1e4d8	Seoul-TGW-Attach-Seoul-VPC-STG	vpc-0e728bf16015c7a9b	vpc	606879168280	tgw-rtb-00c28abe36e2d79ef

TransitGateway 핵심컨셉 이해하기
RouteTable - Propagation

AWS TransitGateway

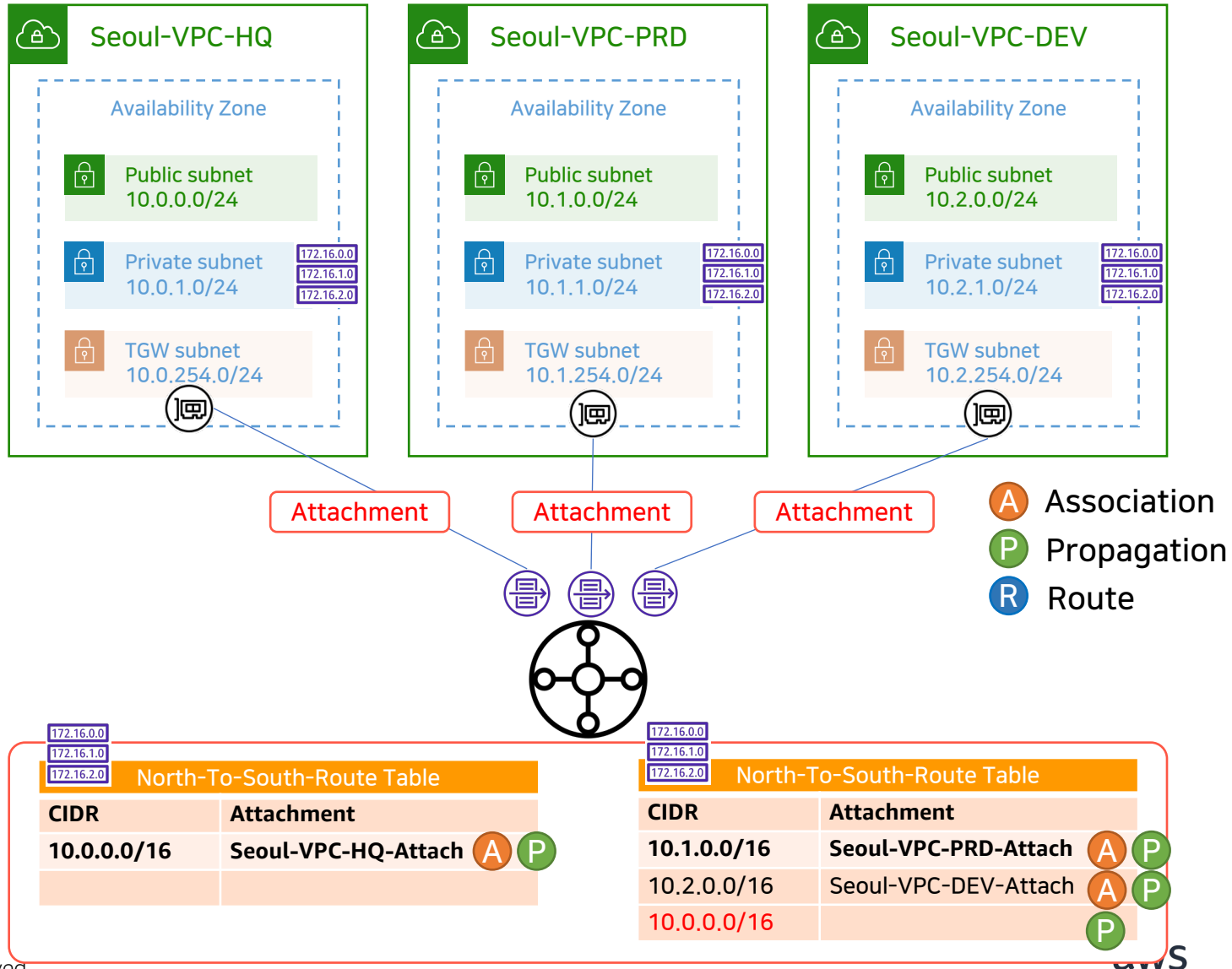
- Attachment
- RouteTable
  - ❑ Association
  - ❑ Propagation
  - ❑ Route

▼ TRANSIT GATEWAYS

Transit Gateways

Transit Gateway Attachments

Transit Gateway Route Tables



TransitGateway 핵심컨셉 이해하기
RouteTable - Route

AWS TransitGateway

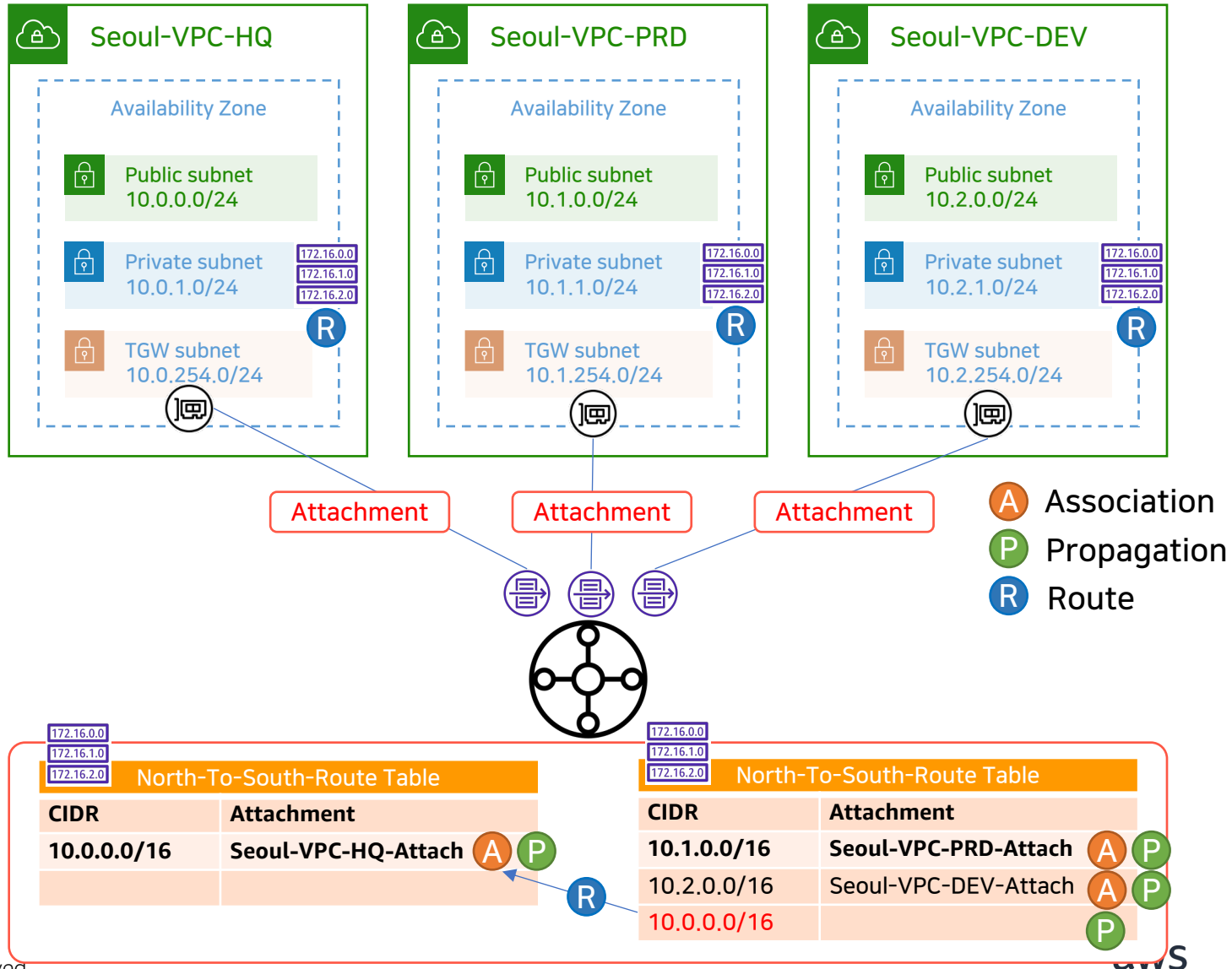
- Attachment
- RouteTable
  - ❑ Association
  - ❑ Propagation
  - ❑ Route

▼ TRANSIT GATEWAYS

Transit Gateways

Transit Gateway Attachments

Transit Gateway Route Tables



TransitGateway 핵심컨셉 이해하기
RouteTable - Route

AWS TransitGateway

- Attachment
- RouteTable
  - ❑ Association
  - ❑ Propagation
  - ❑ Route

▼ TRANSIT GATEWAYS

Transit Gateways

Transit Gateway Attachments

Transit Gateway Route Tables

172.16.0.0 / 172.16.1.0 / 172.16.2.0 VPC – Transit Gateway – Transit Gateway Route Table - Create Static Route

Transit Gateway Route Tables > Create static route

Create static route

Add a static route to your Transit Gateway route table.

Transit Gateway ID tgw-08d037f95bb3ebee7

Transit Gateway route table ID tgw-rtb-00c28abe36e2d79ef

CIDR* 0.0.0.0/0 — CIDR 주소

Blackhole

Choose attachment

* 필수 사항

속성별 필터

Attachment ID	Name tag	Resource ID	Resource Type	Resource owner ID	Association route table
tgw-attach-01a6c52c410fd777b	Seoul-TGW-Attach-Seoul-VPC-PRD	vpc-03b612e4a3af6f0b1	vpc	606879168280	tgw-rtb-00c28abe36e2d79ef
tgw-attach-06ba039ae3ec2940f	Seoul-TGW-Attach-Seoul-VPC-HQ	vpc-0c52b711f5af2ab79	vpc	606879168280	tgw-rtb-0731dd0c6b867836d
tgw-attach-0d639b47c3b5a6ea9	Seoul-TGW-Attach-Seoul-VPC-DEV	vpc-0d242d945209a2056	vpc	606879168280	tgw-rtb-00c28abe36e2d79ef
tgw-attach-0fb774b4b27f1e4d8	Seoul-TGW-Attach-Seoul-VPC-STG	vpc-0e728bf16015c7a9b	vpc	606879168280	tgw-rtb-00c28abe36e2d79ef

원하는 CIDR 주소로 향할 목적지 Attachment 선택

TransitGateway 핵심컨셉 이해하기
RouteTable - Route

AWS TransitGateway

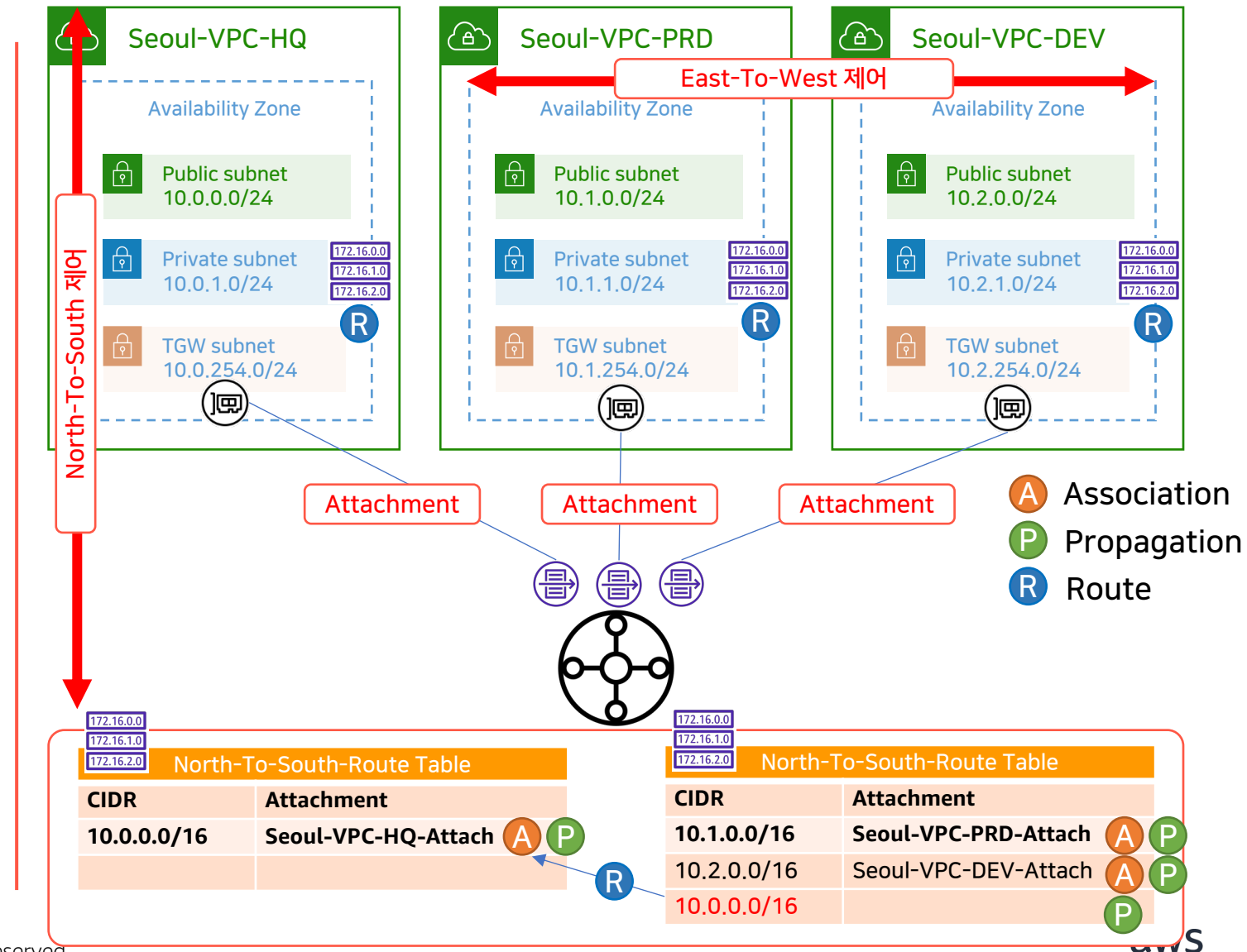
- Attachment
- RouteTable
  - ❑ Association
  - ❑ Propagation
  - ❑ Route

▼ TRANSIT GATEWAYS

Transit Gateways

Transit Gateway Attachments

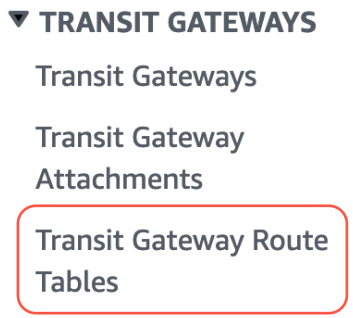
Transit Gateway Route Tables



TransitGateway 핵심컨셉 이해하기
RouteTable - Route

AWS TransitGateway

- Attachment
- RouteTable
  - ❑ Association
  - ❑ Propagation
  - ❑ Route



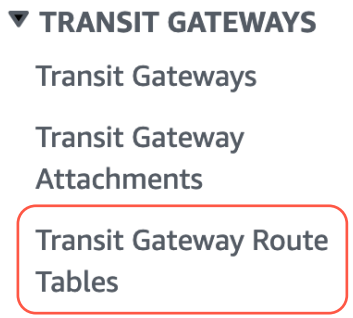
AWS TransitGateway RouteTable Tip !!!

- Routing Table 도메인 분리
- Blackhole Routing 을 통한 보안 강화
- Routing Table의 Static을 통한 TGW 기반 흐름 제어

TransitGateway 핵심컨셉 이해하기
RouteTable - Route

AWS TransitGateway

- Attachment
- RouteTable
  - ❑ Association
  - ❑ Propagation
  - ❑ Route



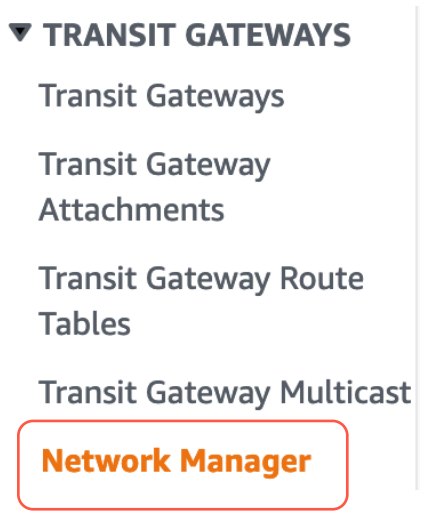
AWS TransitGateway RouteTable Tip !!!

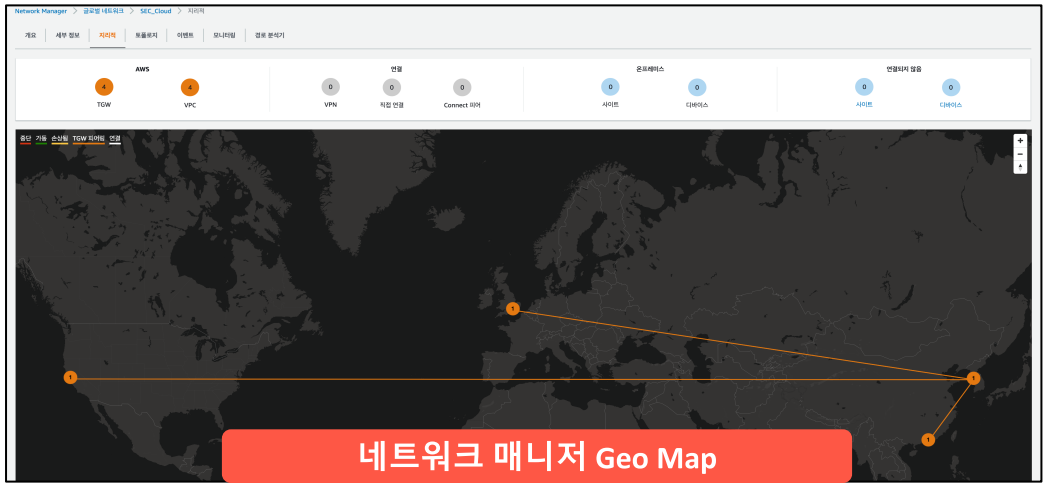
- Routing Table 도메인 분리
- Blackhole Routing 을 통한 보안 강화
- Routing Table의 Static을 통한 TGW 기반 흐름 제어

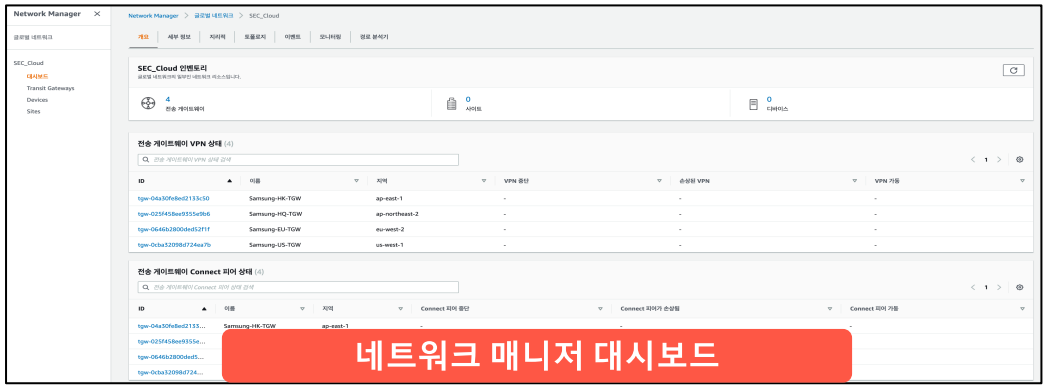
TransitGateway 를 위한 도구들
Network

AWS TransitGateway

- Network Manager
- 경로 분석기





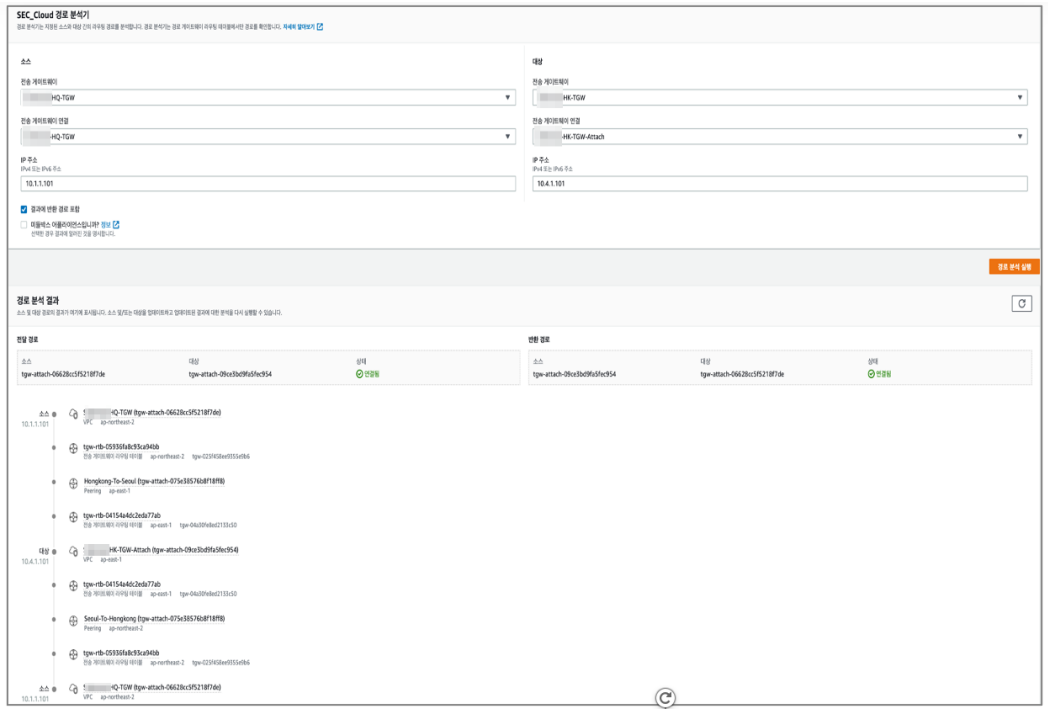


- 대시보드에서 단독으로 글로벌 네트워크를 시각화하고 모니터링
- 네트워크 리소스 및 연결에 대한 목록 보기, 논리적 보기 및 맵 보기를 확인
- 비정상적 연결, AWS 리전 및 온프레미스 사이트 전반의 가용성 및 성능 변경에 대한 알림을 제공

TransitGateway 를 위한 도구들
경로 분석기

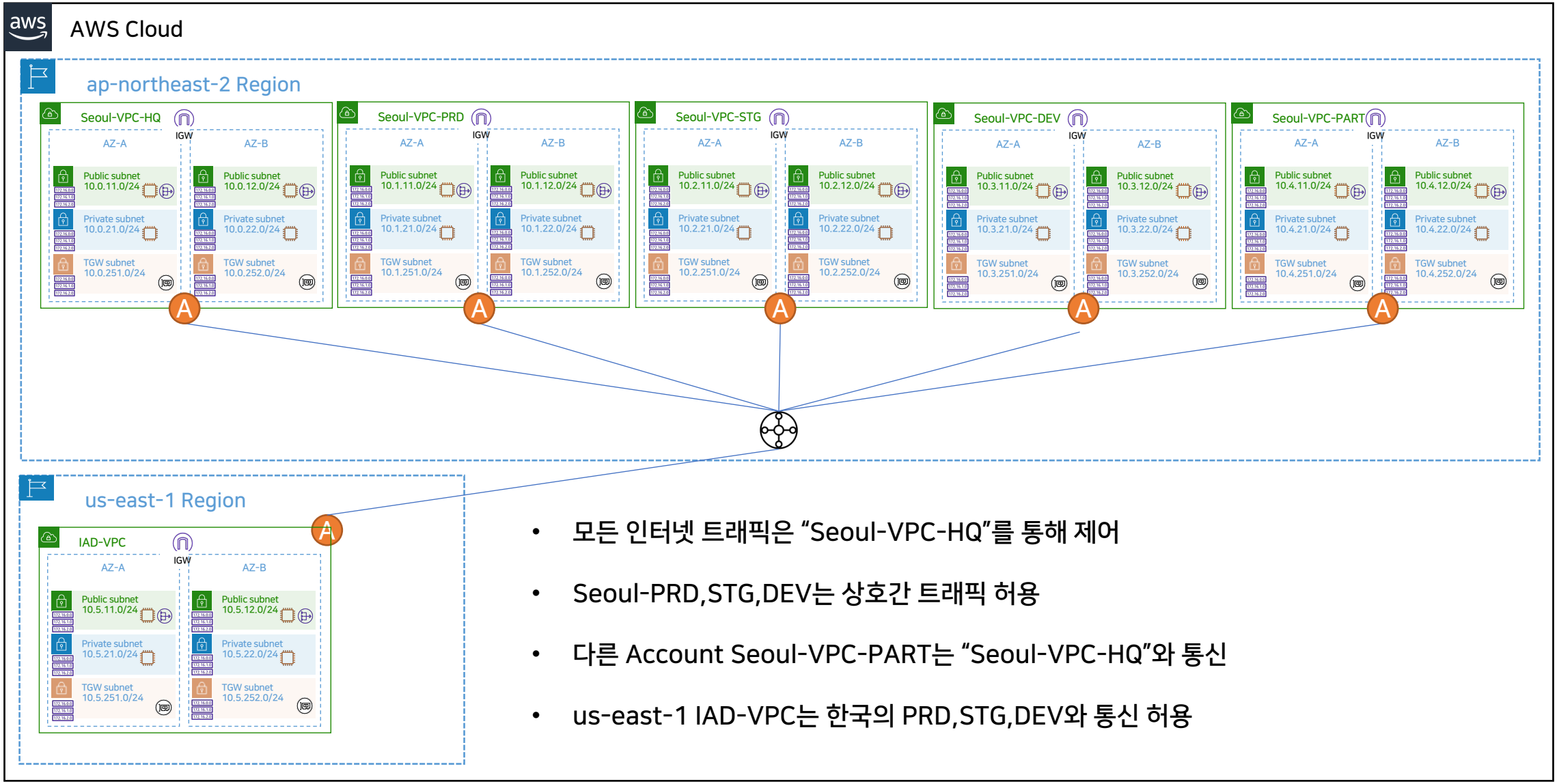
AWS TransitGateway

- Network Manager
- 경로 분석기



- 분석 - Route Analyzer를 사용하여 전송 게이트웨이 라우팅 테이블의 라우팅 분석
- 분석 시각화 - 지정된 소스와 대상 간의 라우팅 경로를 분석
- 사전 검증 - 전송 게이트웨이 라우팅 테이블 구성이 예상대로 작동하는지 확인
- 유효성 점검 - 기존 라우팅 구성의 유효성을 검사
- 라우팅 문제 진단 - 글로벌 네트워크에서 트래픽 중단을 일으키는 라우팅 문제 진단

TransitGateway Demo



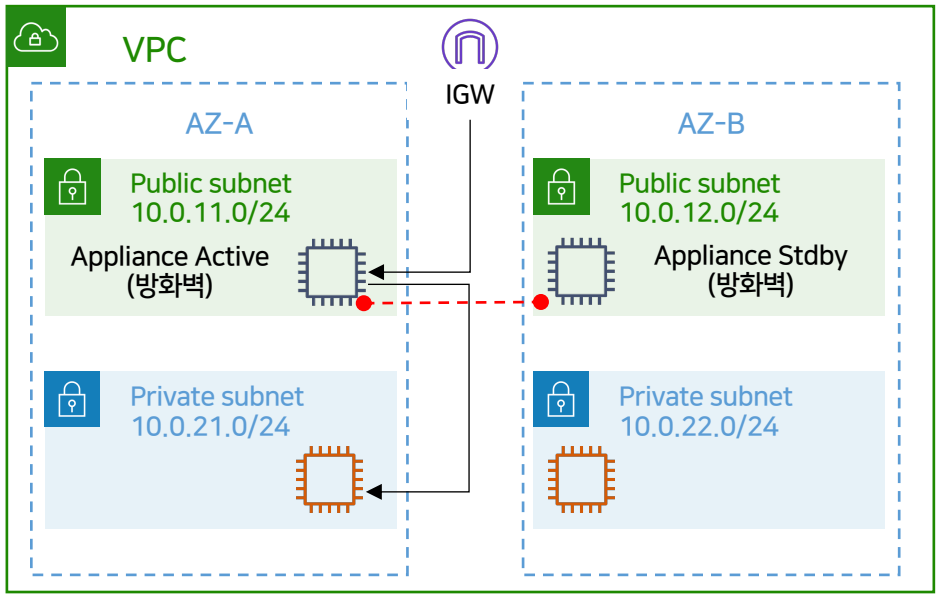
- 모든 인터넷 트래픽은 “Seoul-VPC-HQ”를 통해 제어
- Seoul-PRD,STG,DEV는 상호간 트래픽 허용
- 다른 Account Seoul-VPC-PART는 “Seoul-VPC-HQ”와 통신
- us-east-1 IAD-VPC는 한국의 PRD,STG,DEV와 통신 허용

AWS Builders - Program 300

GWLB Overview

Gateway Load Balancer 소개

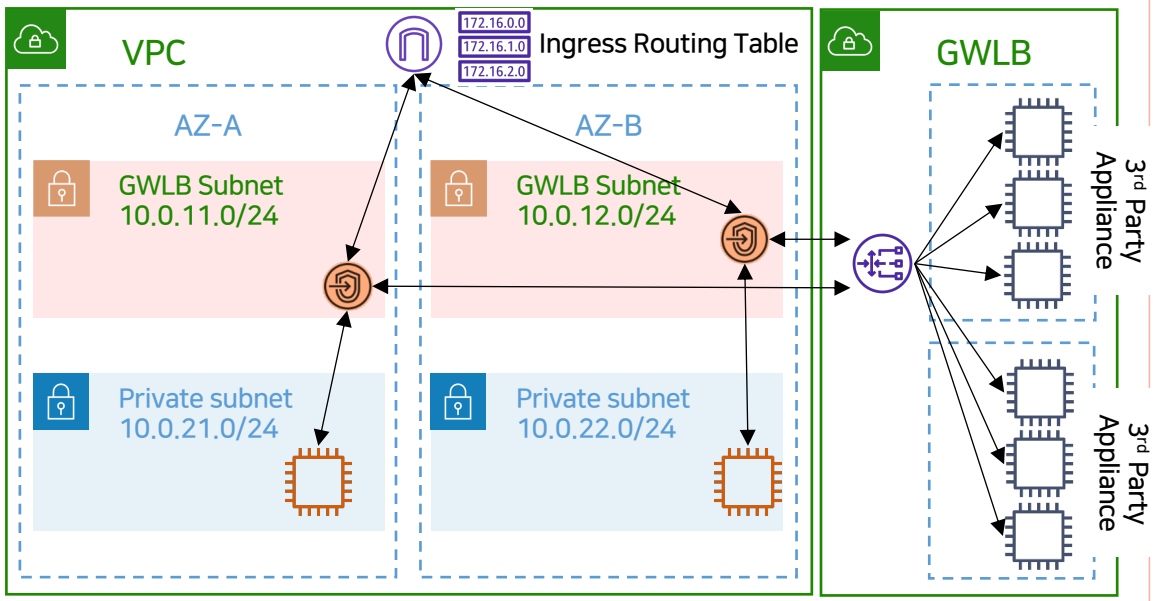
AS-IS : 기존 Appliance 디자인 문제점



- HA 구성의 어려움
- 확장성의 한계와 Passive 장비 활용도 문제
- 관리 포인트 증가

Gateway Load Balancer 서비스 제공

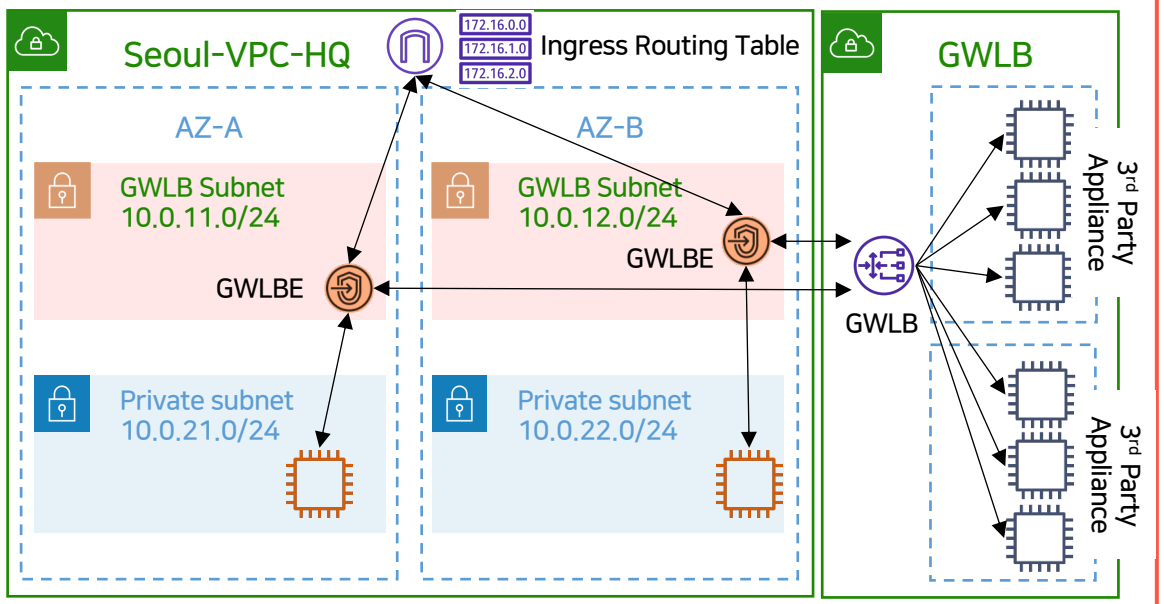
Seoul Region
COMING SOON



- 3rd Party 제품에 높은 고가용성 기반 설계
- 수평적 확장 가능
- BYOL, On-Demand 기반의 비용 고려 설계
- 지속적인 상태 및 성능 지표 모니터링

Gateway Load Balancer 소개

Gateway Load Balancer 서비스 제공



- L3 Gateway (Next-Hop ,No Packet rewrite)
- L4 LB – Scaling, Flow Stickness, Health Checks, Flow rerouting

- 주요 구성 요소
  - ❑ Gateway LB Endpoint (GWLBE) – VPC Endpoint
  - ❑ GWLB – L3 GW + L4 LB 역할 수행
  - ❑ AWS Hyperplane 기반 처리
- 장점
  - ❑ 어플라이언스의 수평적 확장 가능
  - ❑ 고가용성 설계 가능
  - ❑ 소스 트래픽의 변경 없이 처리
  - ❑ 엔터프라이즈급 보안 설계 가능 (Appliance-as-a-Service)
- 구성 방법
  - ❑ NLB & Private Link 구성방법과 유사
  - ❑ VPC Route Table에서 GWLBE에 대한 라우팅 처리

GWLB 구성을 위한 파트너 협력

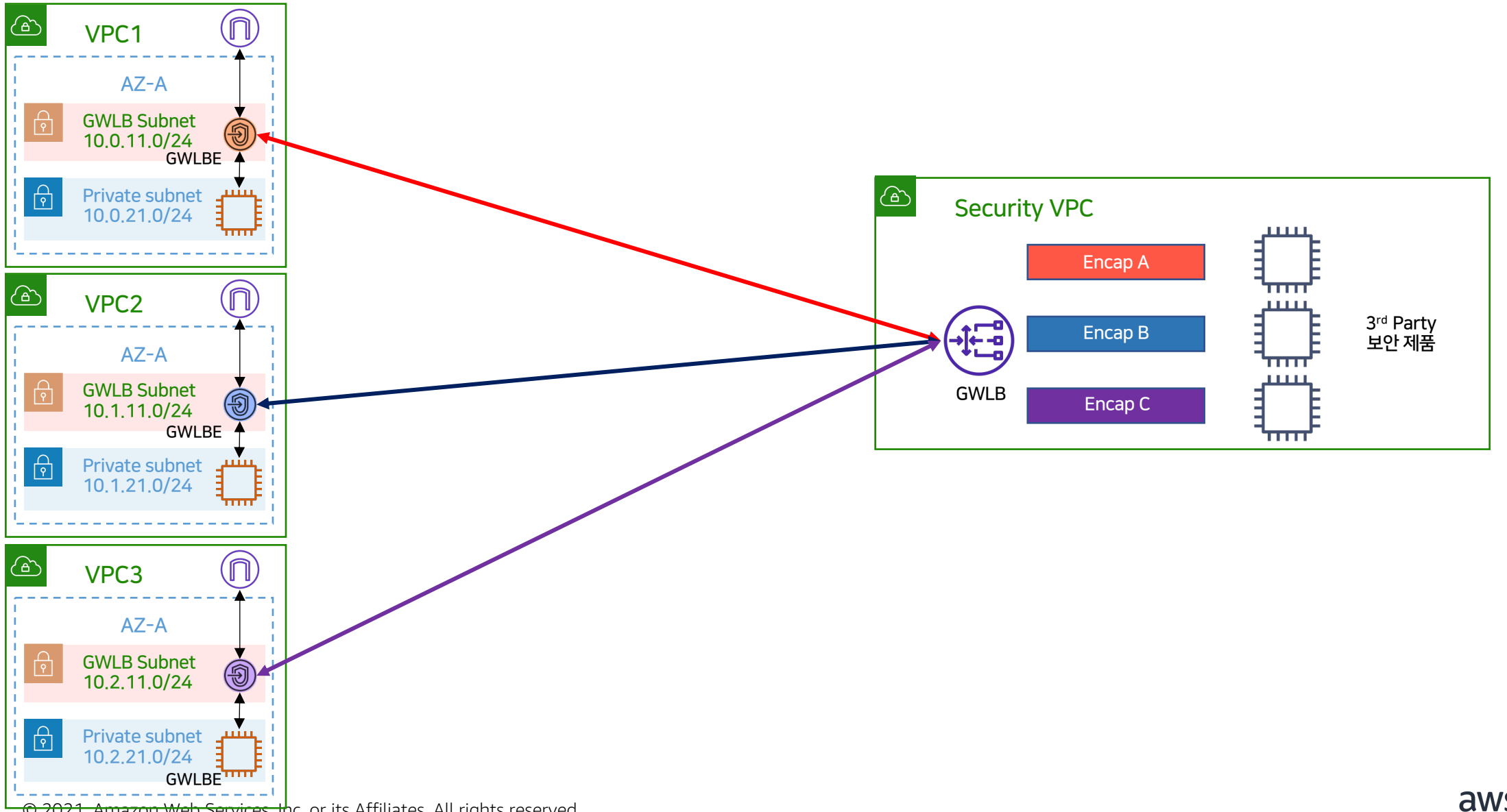
Security Appliance 파트너

네트워크 분석 파트너

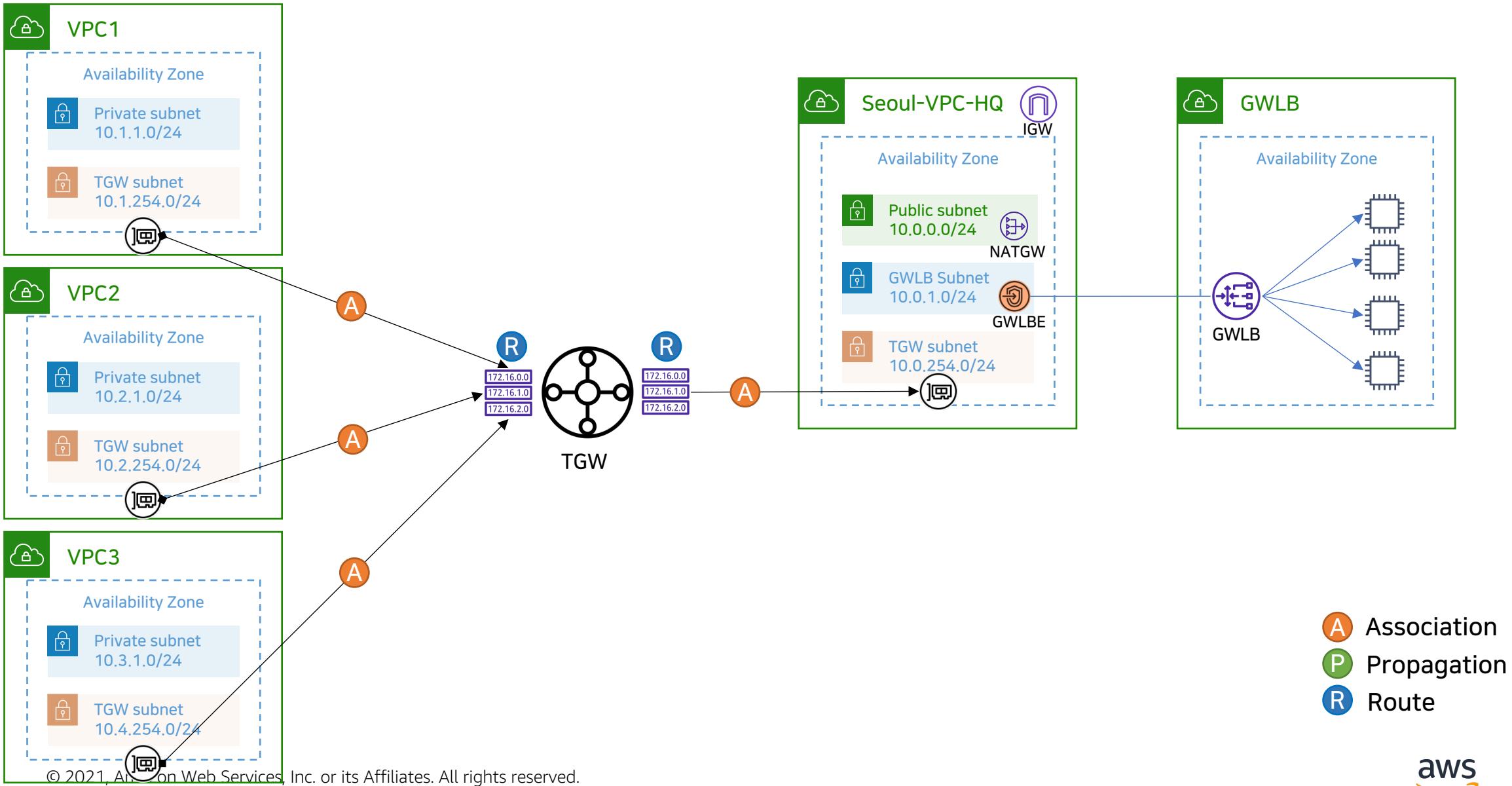
오케스트레이션 파트너

aws

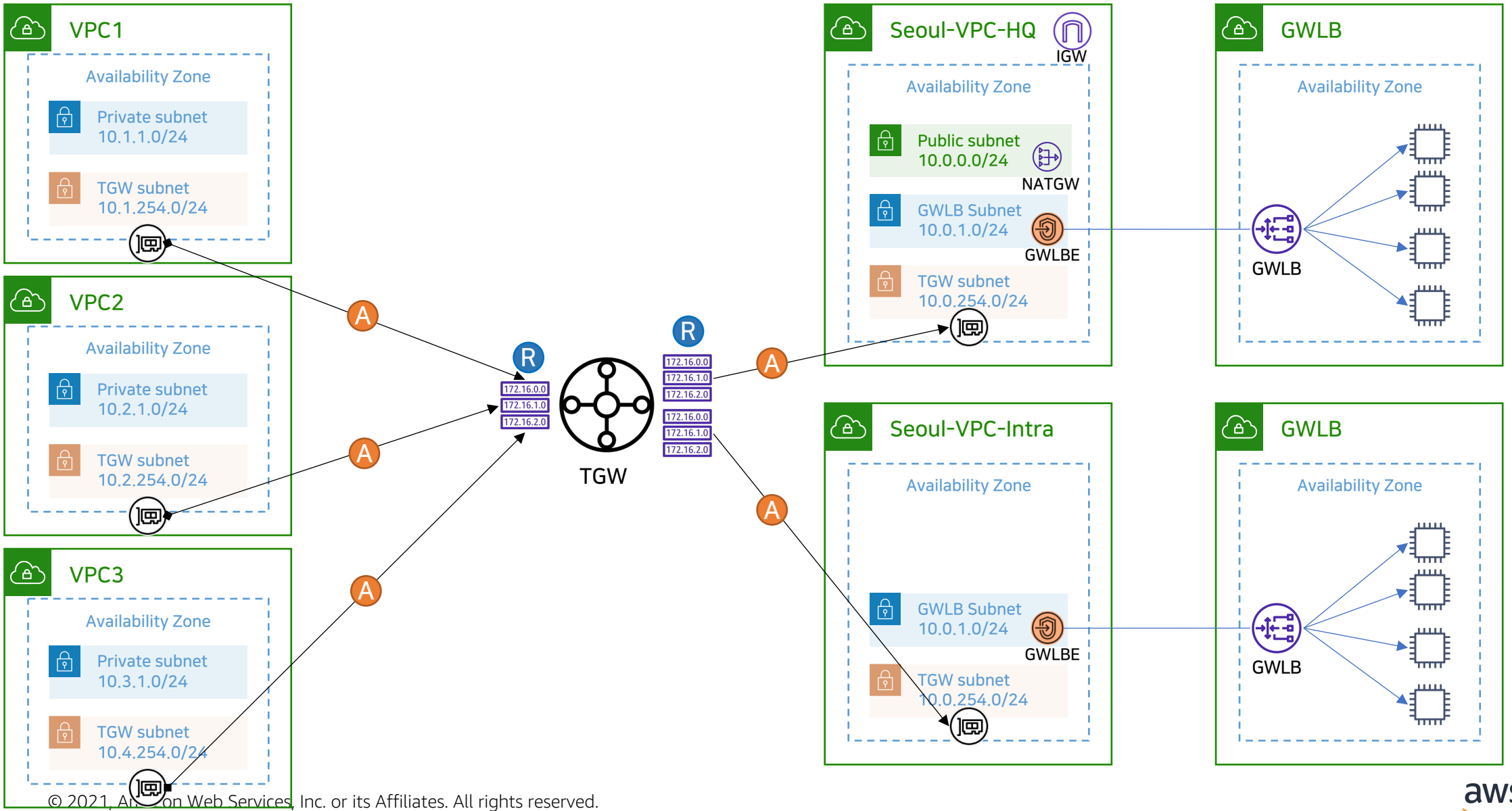
GWLB 기반의 다양한 디자인
1. GWLBE를 이용한 분산형 보안 탐지



GWLB 기반의 다양한 디자인
2. TransitGateway를 이용한 North-To-South 트래픽 제어



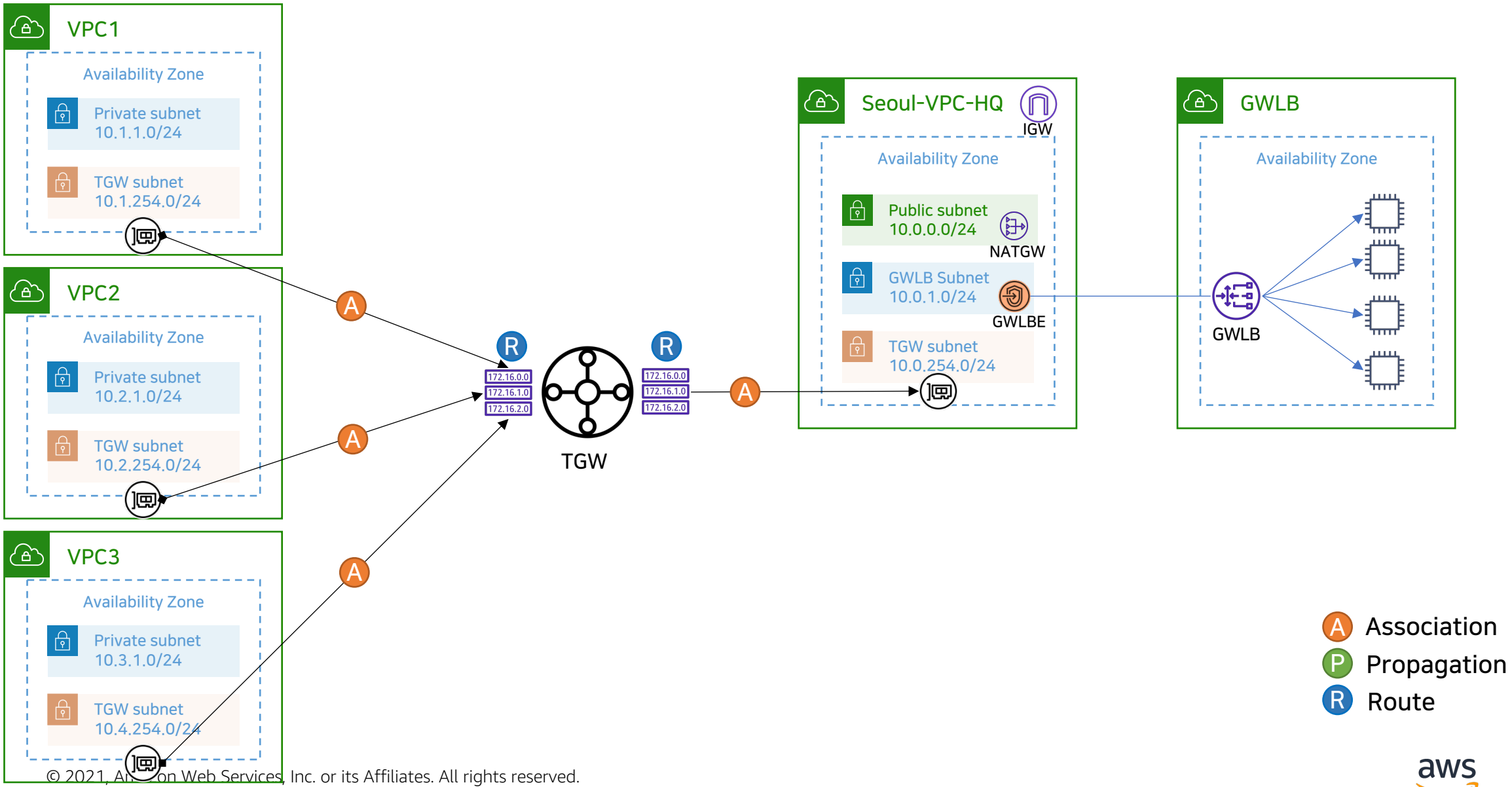
GWLB 기반의 다양한 디자인
3. TransitGateway를 이용한 VPC 트래픽 제어



GWLB Demo

TransitGateway를 이용한 North-To-South 트래픽 제어

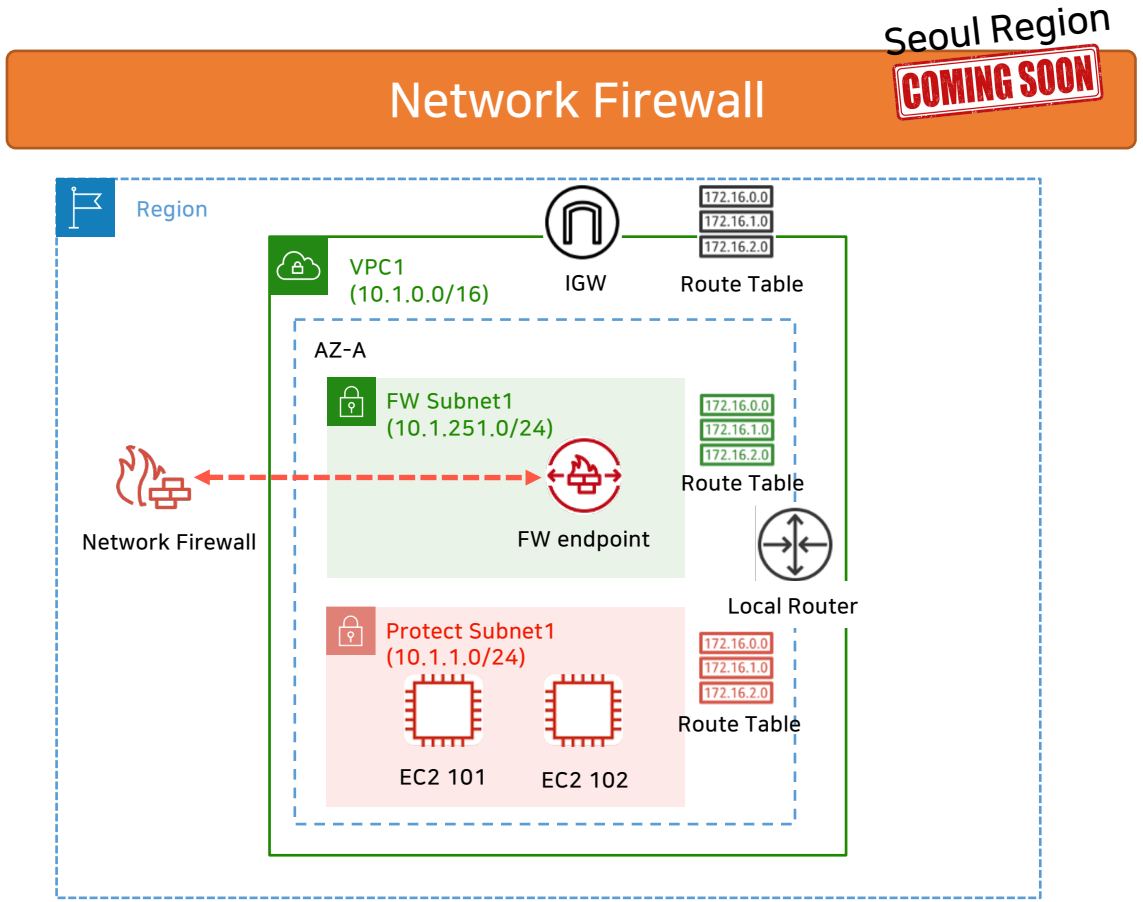
AWS Builders - Program 300



AWS Builders - Program 300

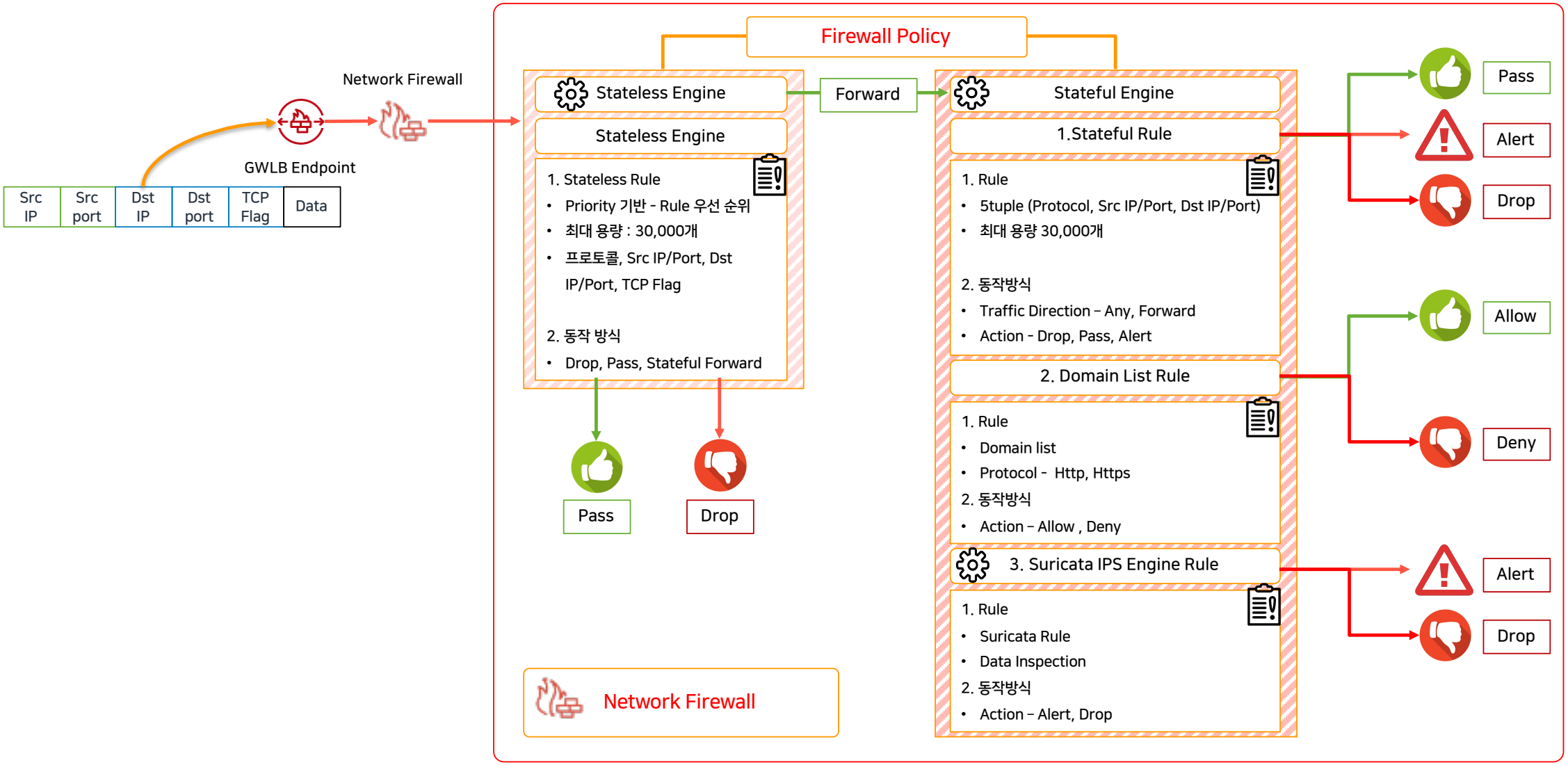
Network Firewall Overview

Network Firewall 소개

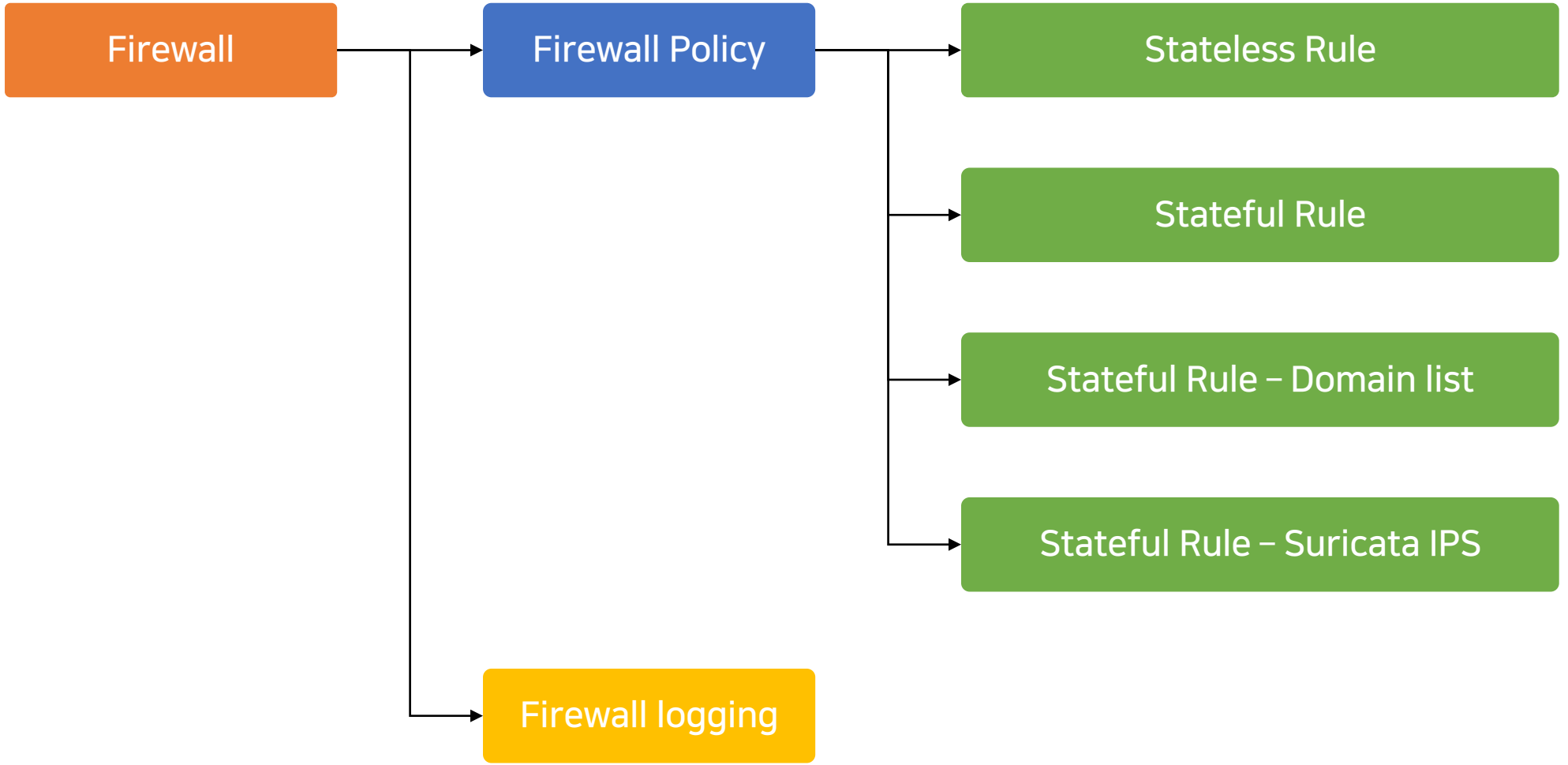


- 주요 구성 요소
  - ❑ Gateway LB Endpoint (GWLBE) – VPC Endpoint
  - ❑ Network Firewall
    - ➢ Stateless
    - ➢ Stateful
    - ➢ Stateful Domain 필터
    - ➢ Stateful Suricata 필터
- 장점
  - ❑ 고가용성을 위한 관리형 인프라
  - ❑ 세밀한 제어 기반의 유연한 보호
  - ❑ VPC 및 계정 전반에 걸친 일관성 있는 정책 관리
  - ❑ Firewall Manager 기반의 통합 관리
- 구성 방법
  - ❑ NLB & Private Link 구성방법과 유사
  - ❑ VPC Route Table에서 GWLBE에 대한 라우팅 처리

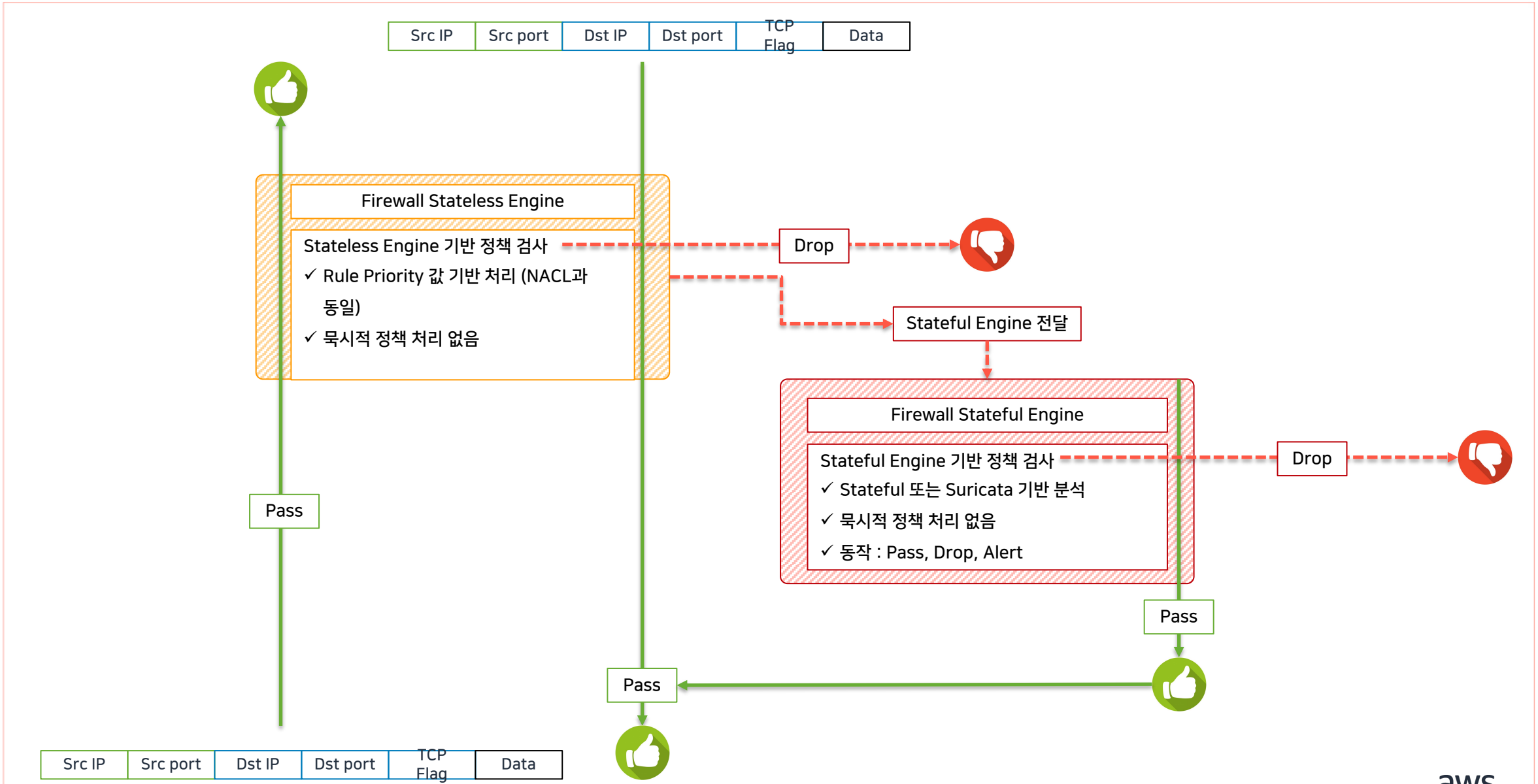
Network Firewall 구조 이해



Network Firewall Policy 구조

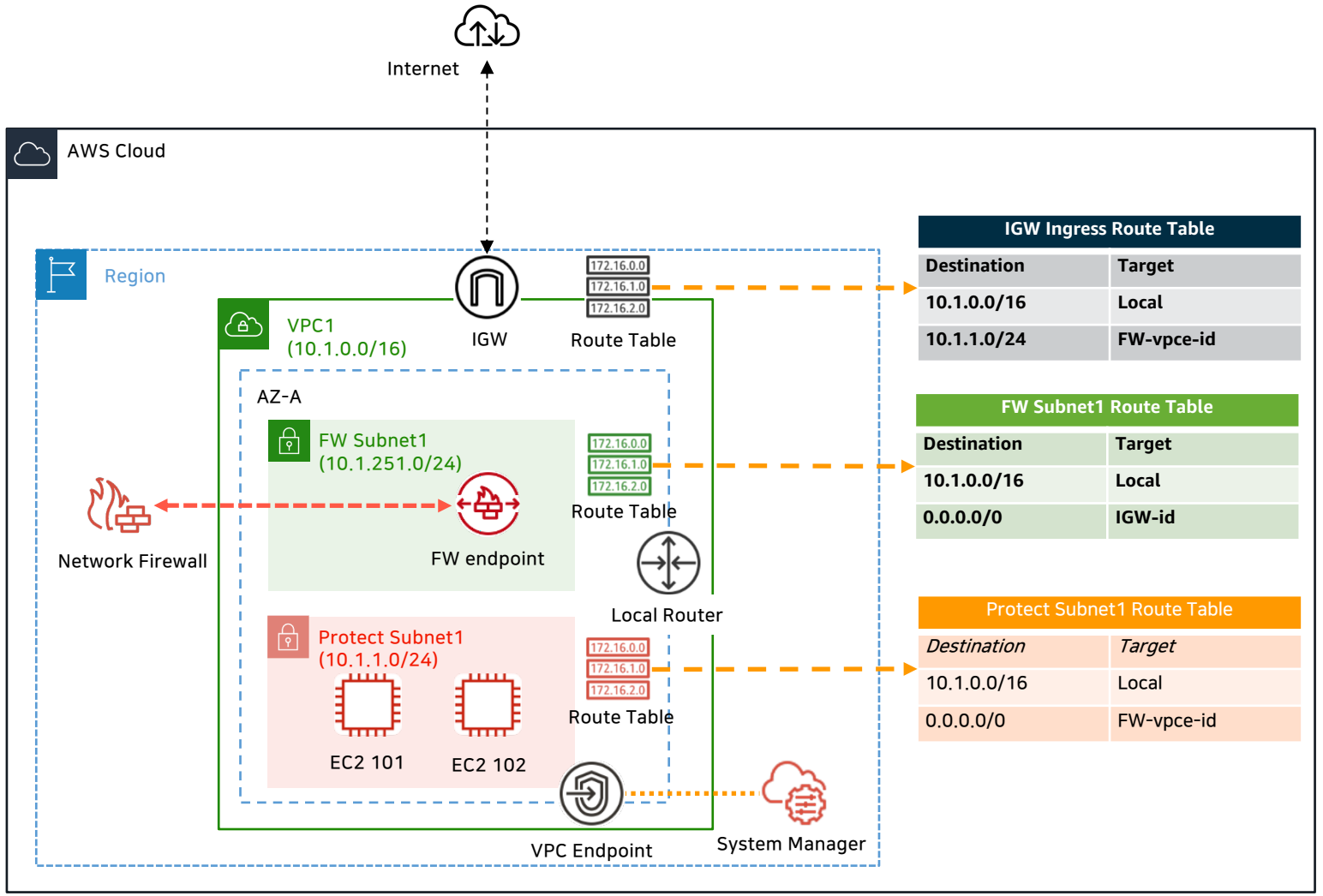


Network Firewall Packet Walk



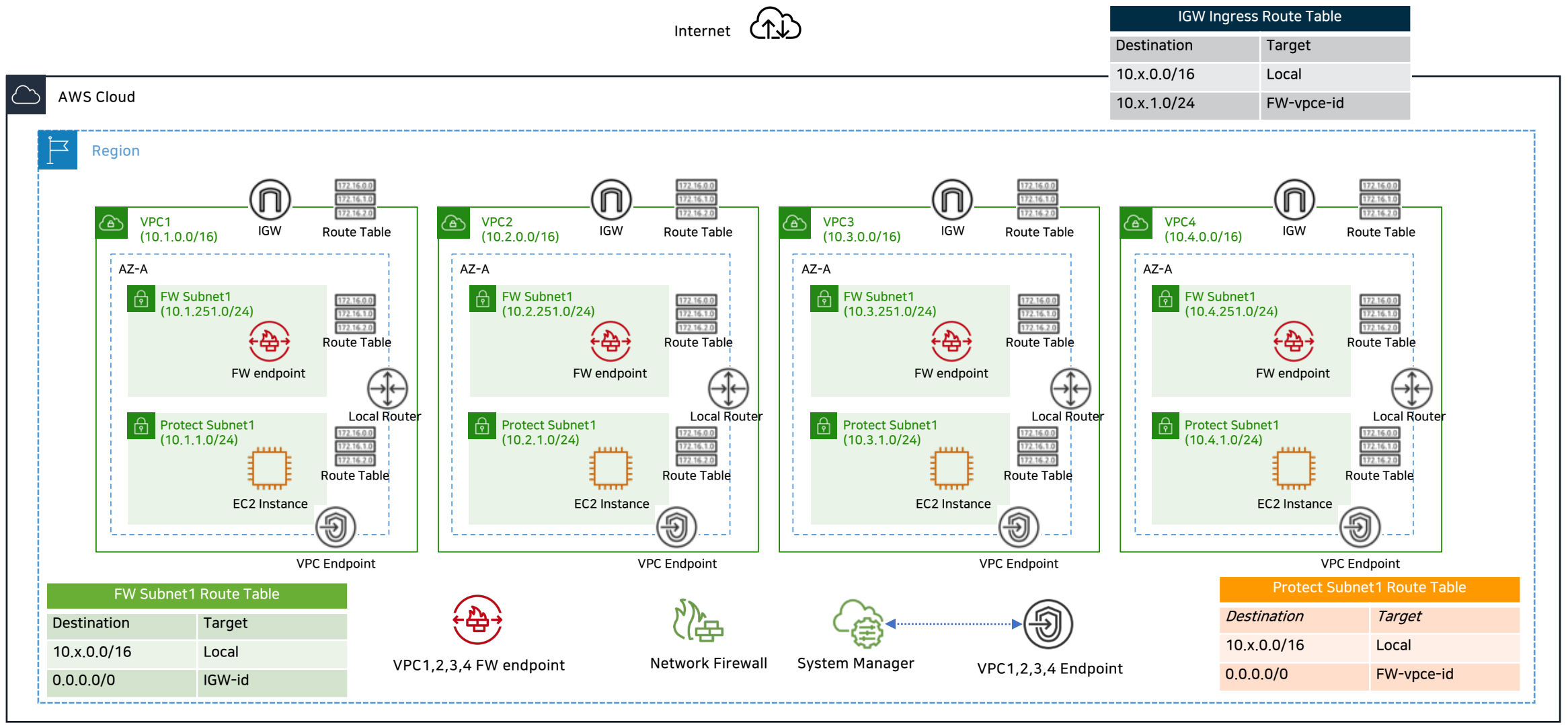
Network Firewall 디자인 1

AWS Network Firewall deployed in Single VPC (single AZ)



Network Firewall 디자인 2

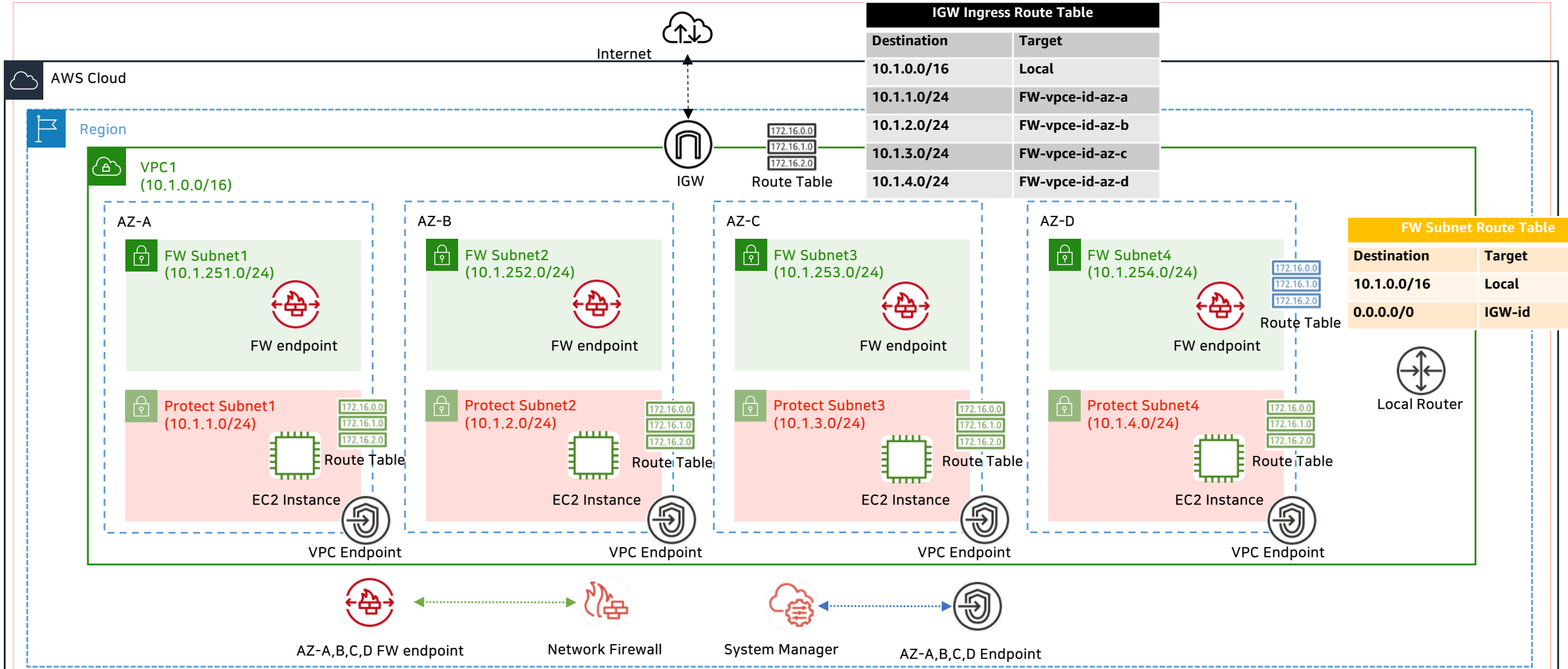
Distributed – AWS Network Firewall deployed in each VPC (single AZ)



Network Firewall 디자인 3

Distributed, multi-AZ protecting Public Subnets

AWS Builders - Program 300



IGW Ingress Route Table	
Destination	**Target**
10.1.0.0/16	Local
10.1.1.0/24	FW-vpce-id-az-a
10.1.2.0/24	FW-vpce-id-az-b
10.1.3.0/24	FW-vpce-id-az-c
10.1.4.0/24	FW-vpce-id-az-d

FW Subnet Route Table	
Destination	**Target**
10.1.0.0/16	Local
0.0.0.0/0	IGW-id

Protect Subnet1 Route Table	
Destination	*Target*
10.1.0.0/16	Local
0.0.0.0/0	FW-vpce-id-az-a

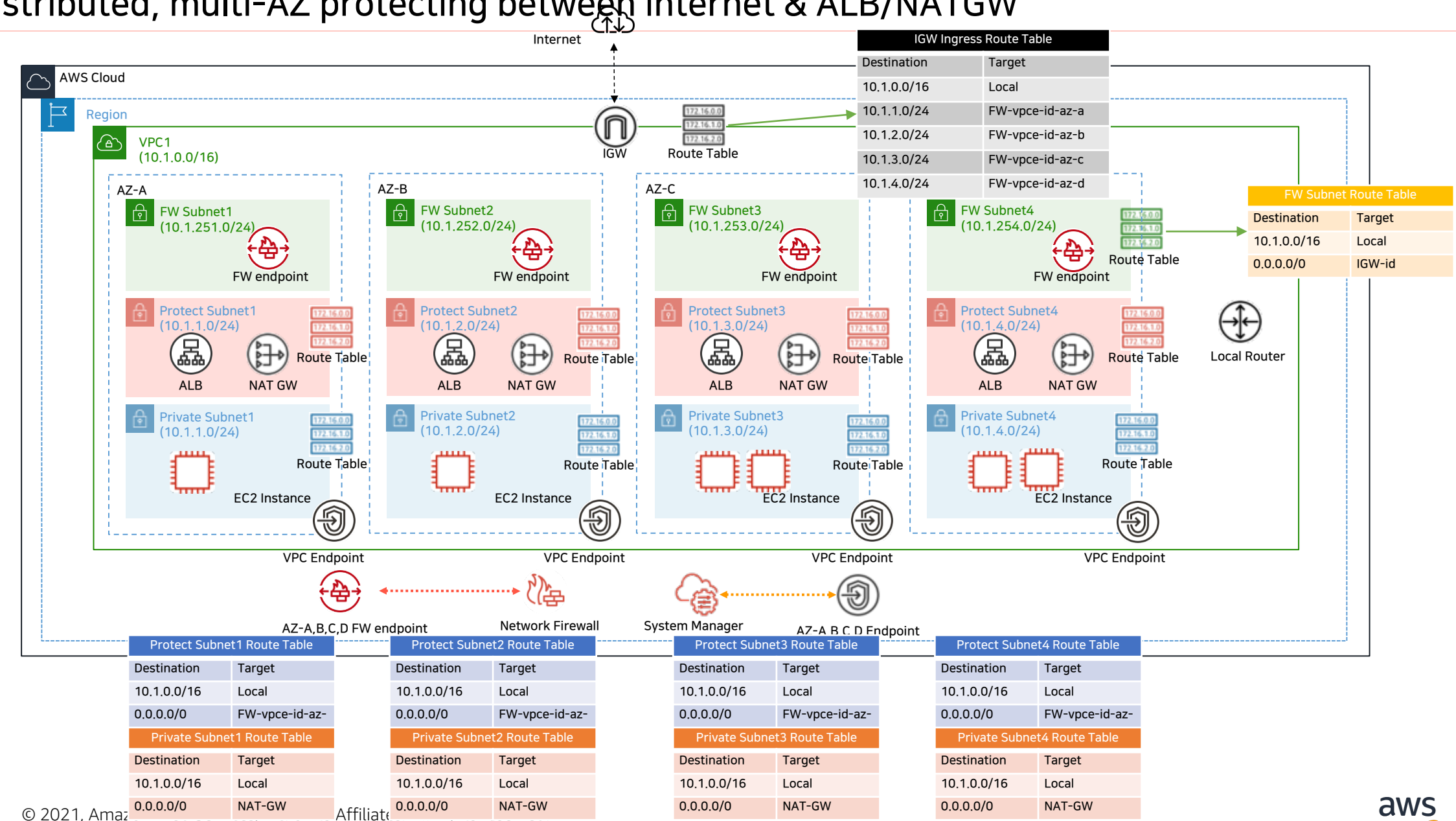
Protect Subnet2 Route Table	
Destination	*Target*
10.1.0.0/16	Local
0.0.0.0/0	FW-vpce-id-az-b

Protect Subnet3 Route Table	
Destination	*Target*
10.1.0.0/16	Local
0.0.0.0/0	FW-vpce-id-az-c

Protect Subnet4 Route Table	
Destination	*Target*
10.1.0.0/16	Local
0.0.0.0/0	FW-vpce-id-az-d

Network Firewall 디자인 4

Distributed, multi-AZ protecting between internet & ALB/NATGW



IGW Ingress Route Table

Destination	Target
10.1.0.0/16	Local
10.1.1.0/24	FW-vpce-id-az-a
10.1.2.0/24	FW-vpce-id-az-b
10.1.3.0/24	FW-vpce-id-az-c
10.1.4.0/24	FW-vpce-id-az-d

FW Subnet Route Table

Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	IGW-id

Protect Subnet1 Route Table

Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	FW-vpce-id-az-

Private Subnet1 Route Table

Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	NAT-GW

Protect Subnet2 Route Table

Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	FW-vpce-id-az-

Private Subnet2 Route Table

Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	NAT-GW

Protect Subnet3 Route Table

Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	FW-vpce-id-az-

Private Subnet3 Route Table

Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	NAT-GW

Protect Subnet4 Route Table

Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	FW-vpce-id-az-

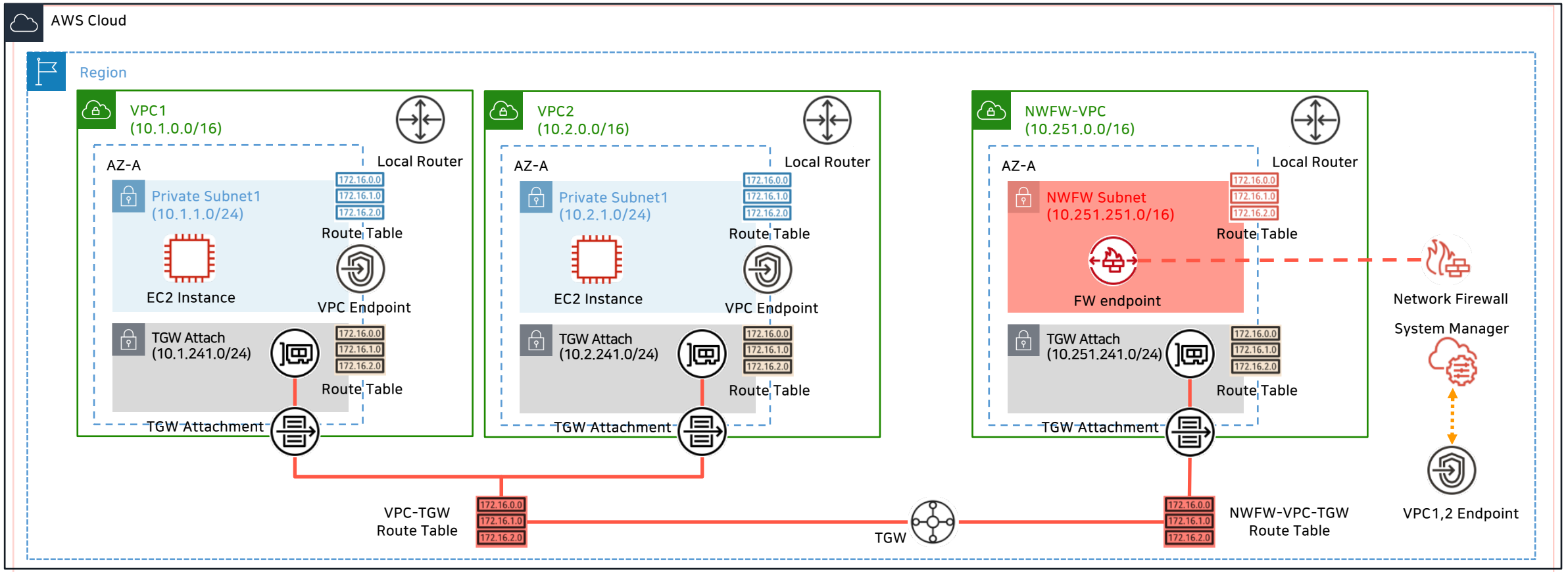
Private Subnet4 Route Table

Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	NAT-GW

Network Firewall 디자인 5

Centralized protecting East-West traffic (VPC to VPC)

AWS Builders - Program 300



VPC1 Private Subnet1 Route Table	
Destination	**Target**
10.1.0.0/16	Local
0.0.0.0/0	tgw-id

VPC2 Private Subnet1 Route Table	
Destination	**Target**
10.2.0.0/16	Local
0.0.0.0/0	tgw-id

VPC-TGW Route Table	
CIDR	**Attachment**
0.0.0.0/0	NWFW-TGW-Attach

Protect Subnet3 Route Table	
Destination	**Target**
10.1.0.0/16	Local
0.0.0.0/0	tgw-id

VPC1 TGW Attach Subnet RT	
Destination	**Target**
10.1.0.0/16	Local
0.0.0.0/0	tgw-id

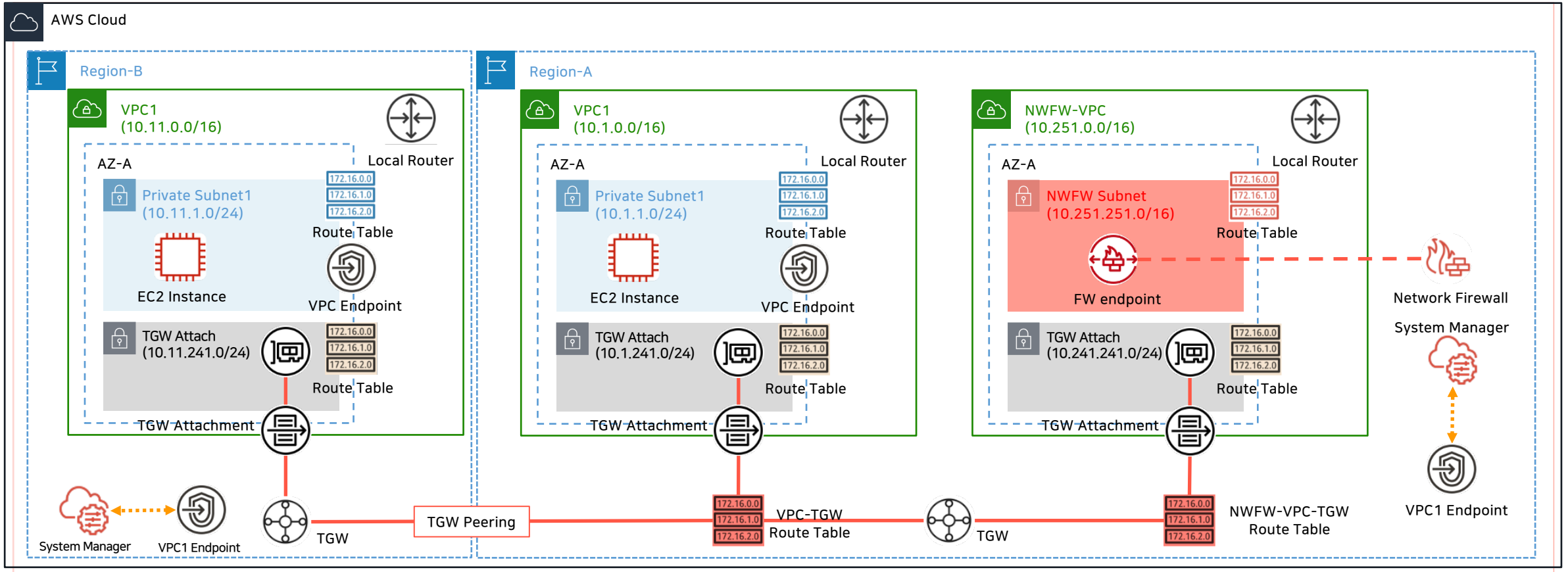
VPC2 TGW Attach Subnet RT	
Destination	**Target**
10.2.0.0/16	Local
0.0.0.0/0	tgw-id

NWFW TGW Route Table	
CIDR	**Attachment**
10.1.0.0/16	VPC1-TGW-Attach
10.2.0.0/16	VPC2-TGW-Attach

VPC2 TGW Attach Subnet RT	
Destination	**Target**
10.2.0.0/16	Local
0.0.0.0/0	FW-vpce-id-az-a

Network Firewall 디자인 6

Centralized protecting Cross-Region



Region-B-VPC1 Private Subnet1 RT	
Destination	Target
10.11.0.0/16	Local
0.0.0.0/0	tgw-id

Region-B VPC1 TGW Attach Subnet RT	
Destination	Target
10.11.0.0/16	Local
0.0.0.0/0	tgw-id

Region-A-VPC1 Private Subnet1 RT	
Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	tgw-id

Region-B VPC1 TGW Attach Subnet RT	
Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	tgw-id

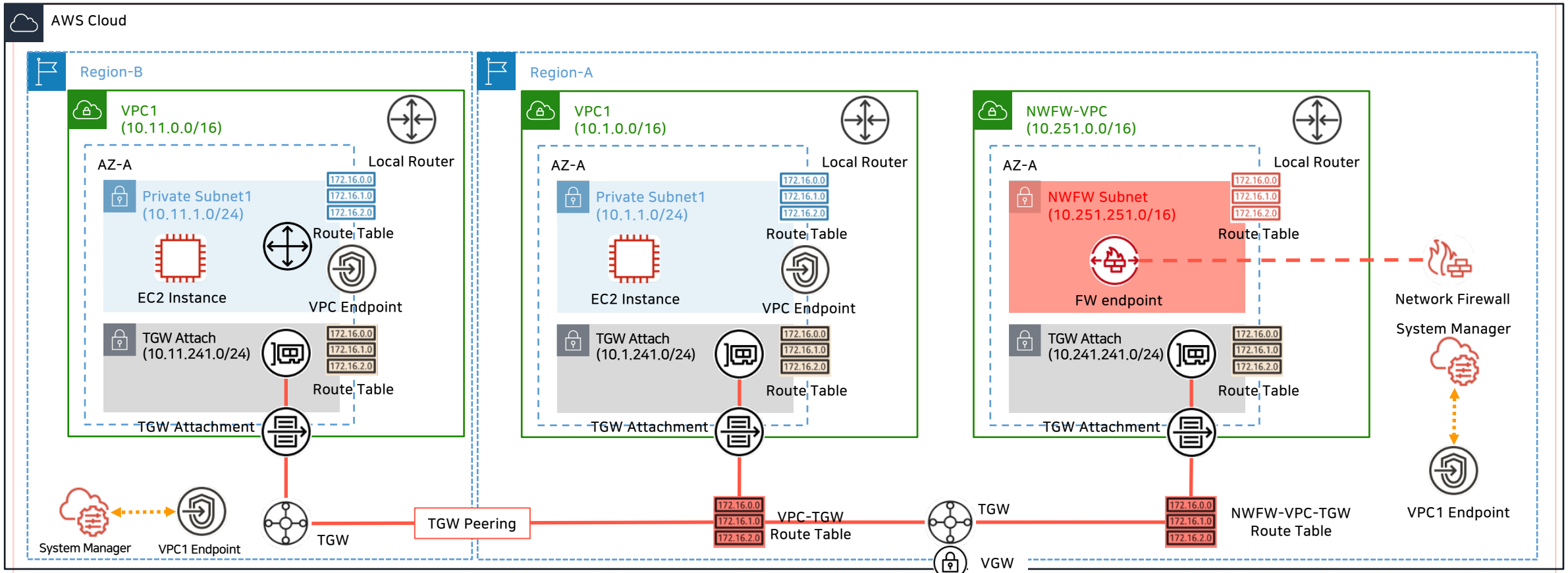
VPC-TGW Route Table	
CIDR	Attachment
0.0.0.0/0	NWFW-TGW-Attach

NWFW TGW Route Table	
CIDR	Attachment
10.1.0.0/16	R-A-VPC1-Attach
10.11.0.0/16	R-B-VPC1-Attach

NWFW Route Table	
Destination	Target
10.251.0.0/16	Local
0.0.0.0/0	tgw-id

NWFW VPC TGW Attach Subnet RT	
Destination	Target
10.251.0.0/16	Local
0.0.0.0/0	FW-vpce-id-az-a

Network Firewall 디자인 7
Scenario 7: Centralized with Transit VIF/DX/Site-to-Site VPN



Region-B-VPC1 Private Subnet1 RT

Destination	Target
10.11.0.0/16	Local
0.0.0.0/0	tgw-id

Region-B VPC1 TGW Attach Subnet RT

Destination	Target
10.11.0.0/16	Local
0.0.0.0/0	tgw-id

Region-A-VPC1 Private Subnet1 RT

Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	tgw-id

Region-B VPC1 TGW Attach Subnet RT

Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	tgw-id

VPC-TGW Route Table

CIDR	Attachment
0.0.0.0/0	NWFW-TGW-Attac

NWFW TGW Route Table

CIDR	Attachment
10.1.0.0/16	R-A-VPC1-Attach
10.11.0.0/16	R-B-VPC1-Attach
192.168.0.0/16	VPN-Attach

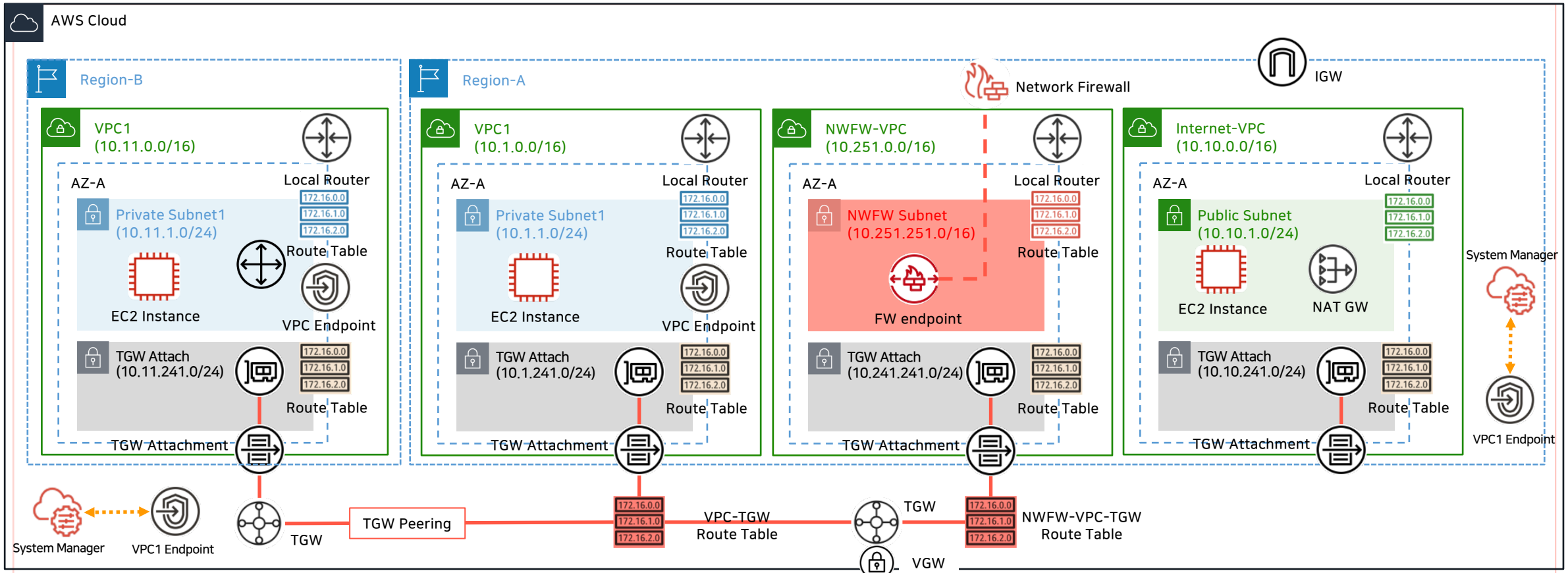
NWFW Route Table

Destination	Target
10.251.0.0/16	Local
0.0.0.0/0	tgw-id

NWFW VPC TGW Attach Subnet RT

Destination	Target
10.251.0.0/16	Local
0.0.0.0/0	FW-vpce-id-az-a

Network Firewall 디자인 8
Scenario 8: Centralized internet egress and NAT gateway



Region-A-VPC1 Private Subnet1 RT	
Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	tgw-id

Region-B VPC1 TGW Attach Subnet RT	
Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	tgw-id

VPC-TGW Route Table	
CIDR	Attachment
0.0.0.0/0	NWFW-TGW-Attach

NWFW TGW Route Table	
CIDR	Attachment
10.1.0.0/16	R-A-VPC1-Attach
10.11.0.0/16	R-B-VPC1-Attach
192.168.0.0/16	VPN-Attach
0.0.0.0/0	Internet-VPC-Attach

NWFW Route Table	
Destination	Target
10.251.0.0/16	Local
0.0.0.0/0	tgw-id

NWFW VPC TGW Attach Subnet RT	
Destination	Target
10.251.0.0/16	Local
0.0.0.0/0	FW-vpce-id-az-a

Public Route Table	
Destination	Target
10.10.0.0/16	Local
10.0.0.0/8	tgw-id
0.0.0.0/0	igw-id

Internet VPC TGW Attach Subnet RT	
Destination	Target
10.10.0.0/16	Local
10.0.0.0/8	tgw-id
0.0.0.0/0	igw-id

데모 실습 소개

LAB 가이드 URL

http://bit.ly/2NefEKW 또는 https://whchoi98.gitbook.io/builders-net/

Source & Shell , LAB 가이드 문서

https://github.com/whchoi98/builders20210312

LAB이 완료 된 이후에는 자원을 삭제하세요 !!!

해당 LAB에 대해서 추후에도 어드밴스드 네트워킹 LAB에 대해 계속 문의하고 싶어요.
Slack Channel - https://whchoi-hol.slack.com/archives/C01QM79Q4BD

더 나은 세미나를 위해
여러분의 의견을 남겨주세요!

▶ 질문에 대한 답변 드립니다.

AWS Builders Program 300 –

감사합니다.