



AWS VPC & Security Best Practices

OpsNow ArchOps 심선보(seonbo.shim@bespinglobal.com)

2023-08-04

AGENDA

1. Introduction
2. VPC
3. VPC 네트워크 보안



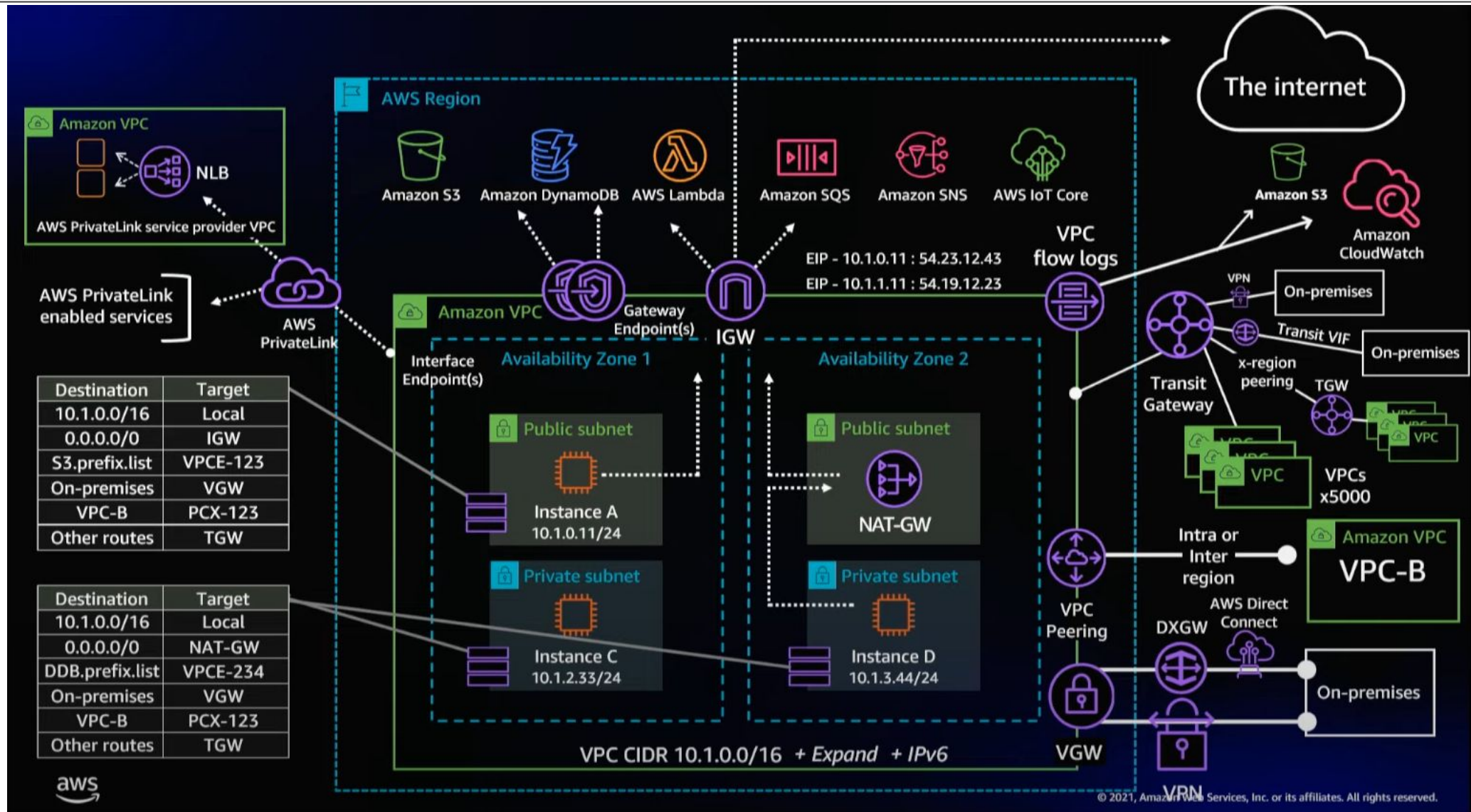
Introduction

AWS 클라우드의 근간이 되는 VPC 를 이해하고 운영 확장을 고려한 네트워킹 설계와 강화된 보안 정책을 적용함으로써 안전하고 확장 가능한 클라우드 아키텍처 설계 기법을 소개 합니다.

VPC

VPC 구성 요소 및 네트워크 구성

VPC Architecture



VPC - CIDR

클래스 A Private 서브넷 대역: 10.0.0.0 - 10.255.255.255 CIDR: 10.0.0.0/8 - 16,777,216

클래스 B Private 서브넷 대역: 172.16.0.0 - 172.31.255.255 CIDR: 172.16.0.0/12 - 1,048,576

클래스 C Private 서브넷 대역: 192.168.0.0 - 192.168.255.255 CIDR: 192.168.0.0/16 - 65,535

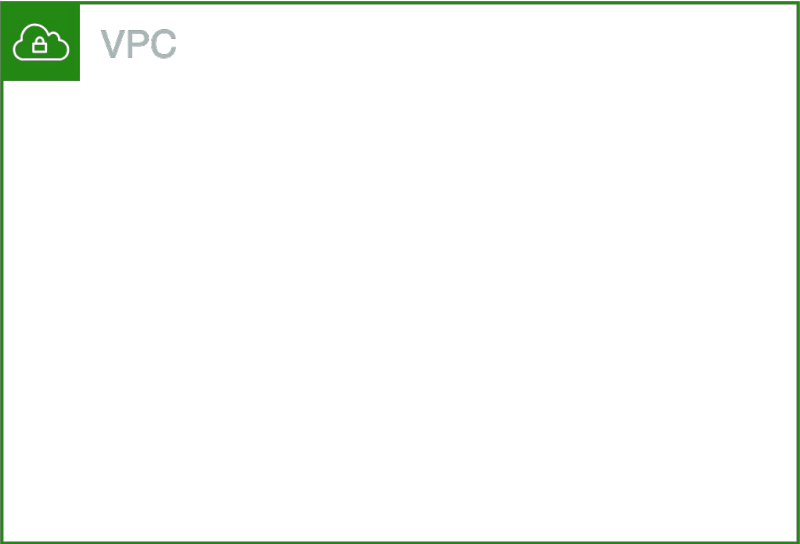
0.0.0.0 => 현재의 네트워크

127.0.0.0 => 호스트 자기 자신을 가리키는 Loop Back

172.16.0.0 인 경우 local => VPC 자신을 가리키는 Loop Back

VPC (Virtual Private Cloud)

AWS에서 제공하는 가상 네트워킹 환경으로, 고객이 원하는 전용 네트워크를 **AWS** 클라우드 위에 구축할 수 있도록 해주는 서비스입니다.



VPCs See all regions ▼	Asia Pacific 1	NAT Gateways See all regions ▼	Asia Pacific 2
Subnets See all regions ▼	Asia Pacific 38	VPC Peering Connections See all regions ▼	Asia Pacific 10
Route Tables See all regions ▼	Asia Pacific 9	Network ACLs See all regions ▼	Asia Pacific 1
Internet Gateways See all regions ▼	Asia Pacific 1	Security Groups See all regions ▼	Asia Pacific 199
Egress-only Internet Gateways See all regions ▼	Asia Pacific 0	Customer Gateways See all regions ▼	Asia Pacific 4
DHCP option sets See all regions ▼	Asia Pacific 1	Virtual Private Gateways See all regions ▼	Asia Pacific 2
Elastic IPs See all regions ▼	Asia Pacific 6	Site-to-Site VPN Connections See all regions ▼	Asia Pacific 3
Endpoints See all regions ▼	Asia Pacific 2	Running Instances See all regions ▼	Asia Pacific 11
Endpoint Services See all regions ▼	Asia Pacific 1		

VPC - Subnets

Subnets

See all regions ▼

Asia Pacific 38

하나의 독립적인 네트워크 공간을 구축하는 네트워크(Subnet)를 정의하고 그 안에 WEB, API, 데이터베이스, Serverless Lambda 등 컴퓨팅 인스턴스를 배치할 수 있습니다.



VPC - Route Table

Route Tables

See all regions ▼

Asia Pacific 9

목적지에 정의된 트래픽은 **Target** 으로 라우팅 되도록 규칙을 정의 합니다.

연결된 서브넷 “**WEB**” 은 여기에 정의된 라우팅 규칙을 따릅니다.

라우팅 서브넷 연결 엣지 연결 라우팅 전파 태그

라우팅 (3)

라우팅 필터링

대상	대상	상태	전파됨
pl-78a54011	vpce-035667eb597e0545d	🟢 활성	아니요
0.0.0.0/0	igw-0ce8164d7170e7ecf	🟢 활성	아니요
172.10.0.0/16	local	🟢 활성	아니요

10.251.0.0/16	local
192.168.117.0/23	pcx-06cfeff04391eaf97
10.223.0.0/16	tgw-0f6a06a8748da3dac
pl-04fcd92a958c7ee66	vgw-8fdc53bf
0.0.0.0/0	igw-def632b7
0.0.0.0/0	nat-07a7e210196deaaf2

aws Services Search [Option+S]

Route 53 EC2 IAM Elastic Container Service VPC Amazon MQ AWS AppConfig AWS Cloud Map

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (4/22)

Filter subnet associations

	Name	Subnet ID	IPv4 CIDR
<input type="checkbox"/>	C	subnet-0e80caf12679d8436	10.251.151.0/24
<input type="checkbox"/>	A	subnet-0653eaa65231afdde	10.251.150.0/24
<input checked="" type="checkbox"/>	-WEB--C2	subnet-0d87f7e78b71b39d8	10.251.147.0/24
<input checked="" type="checkbox"/>	-WEB--C1	subnet-01fac353d60b7fd2b	10.251.158.0/24
<input checked="" type="checkbox"/>	-WEB--A2	subnet-0354ef3c528c91176	10.251.146.0/24
<input checked="" type="checkbox"/>	-WEB--A1	subnet-060c47eb1f7fadceb	10.251.157.0/24
<input type="checkbox"/>	-DB--C	subnet-0509fa3c8dd7c0246	10.251.155.0/24
<input type="checkbox"/>	-DB--A	subnet-04ba46076ecbbfb85	10.251.154.0/24

VPC - Route Table



네트워크 연결 포인트를 통해 Subnet 의 라우팅 연결을 제어 합니다.

Route Table 은 Destination 과 Target 으로 정의 하며, 전파할 서브넷을 연결 하여야 합니다.

Destination 유형

- IP CIDR 대역(10.10.10.0/24)
- Managed Prefix (IP 그룹)

Target 유형

- Egress Only Internet Gateway
- Instance (EC2 ...)
- Internet Gateway
- local (internal VPC)
- NAT Gateway
- Outpost Local Gateway
- Peering Connection
- Transit Gateway
- Virtual Private Gateway

Destination Type	Destination	Target	Target Type	Description
CIDR	0.0.0.0/0	igw-def632b7	Internet Gateway	모든 대역은 Internet Gateway 에 전파
CIDR	0.0.0.0/0	nat-07a7e210196d	Nat Gateway	모든 대역은 NAT Gateway 에 전파
CIDR	10.251.0.0/16	local	local	10.251.0.0/16 VPC 대역은 local 에 전파
CIDR	192.168.117.0/23	pcx-06cfe391eaf97	Peering Connection	192.168.117.0/23 대역은 VPC 피어링에 전파
CIDR	10.223.0.0/16	tgw-eff04391e	Transit Gateway	10.223.0.0/16 대역은 TGW 에 전파
Managed Prefix	pl-04fcd92a95	vgw-8fdc53bf	Virtual Private Gateway	pl-04fcd92a95 아이피 그룹은 VPN 에 전파

VPC (Virtual Private Cloud)

Route Tables

See all regions ▼

Asia Pacific 9

목적지에 정의된 트래픽은 **Target** 으로 라우팅 되도록 규칙을 정의 합니다.

연결된 서브넷 “**WEB**” 은 여기에 정의된 라우팅 규칙을 따릅니다.

Destination	Target
0.0.0.0/0	igw-def632b7
0.0.0.0/0	nat-07a7e210196d
10.251.0.0/16	local
192.168.117.0/23	pcx-06cfe391eaf97
10.223.0.0/16	tgw-eff04391e
pl-04fcd92a95	vgw-8fdc53bf

aws

Services

Search

[Option+S]

Route 53

EC2

IAM

Elastic Container Service

VPC

Amazon MQ

AWS AppConfig

AWS Cloud Map

Edit subnet associations

Change which subnets are associated with this route table.

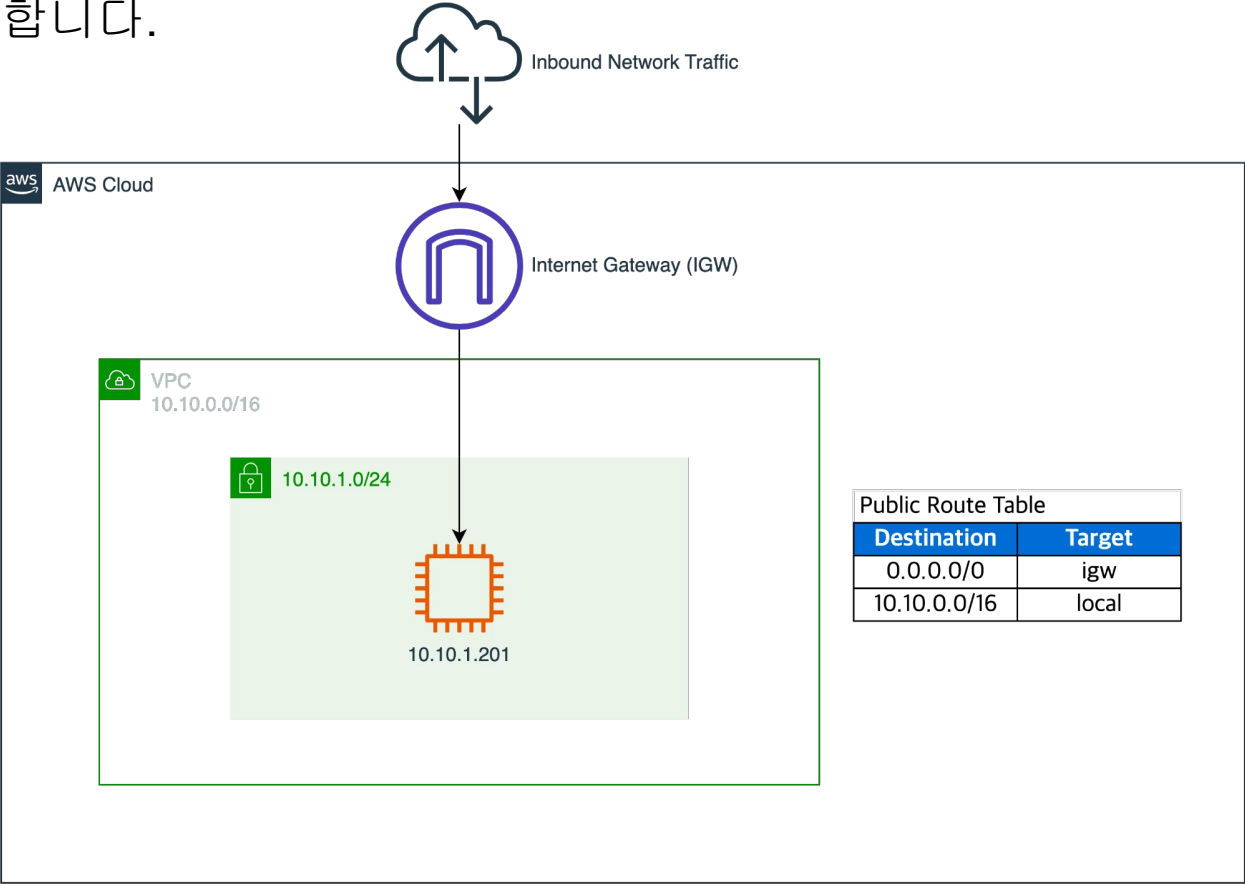
Available subnets (4/22)

Filter subnet associations

	Name	Subnet ID	IPv4 CIDR
<input type="checkbox"/>	C	subnet-Oe80caf12679d8436	10.251.151.0/24
<input type="checkbox"/>	A	subnet-0653eaa65231afdde	10.251.150.0/24
<input checked="" type="checkbox"/>	-WEB--C2	subnet-0d87f7e78b71b39d8	10.251.147.0/24
<input checked="" type="checkbox"/>	-WEB--C1	subnet-01fac353d60b7fd2b	10.251.158.0/24
<input checked="" type="checkbox"/>	-WEB--A2	subnet-0354ef3c528c91176	10.251.146.0/24
<input checked="" type="checkbox"/>	-WEB--A1	subnet-060c47eb1f7fadceb	10.251.157.0/24
<input type="checkbox"/>	-DB--C	subnet-0509fa3c8dd7c0246	10.251.155.0/24
<input type="checkbox"/>	-DB--A	subnet-04ba46076ecbbfb85	10.251.154.0/24

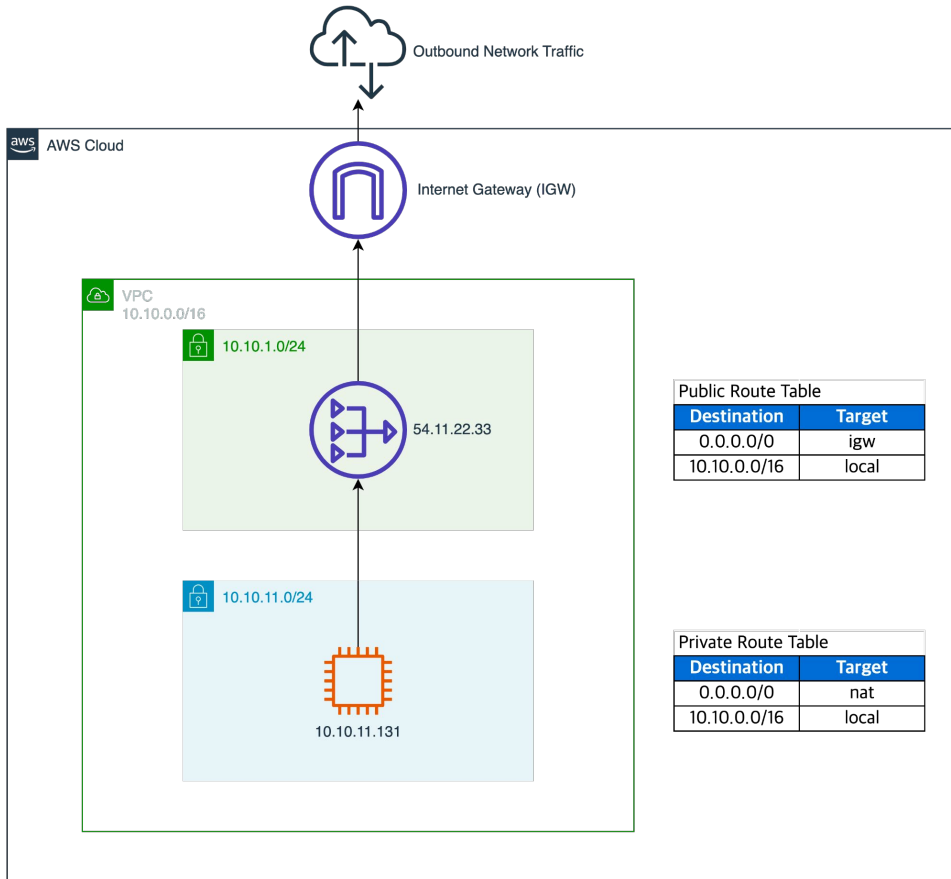
VPC - Internet Gateway

인터넷의 클라이언트(브라우저 및 앱)가 VPC 의 리소스를 액세스 하기 위해선 **Internet Gateway** 와 구성 되어야 합니다. **Internet Gateway** 가 **Subnet** 에 연결되어 있으면 해당 **Subnet** 은 인터넷과 연결 되므로 **Public Subnet** 이라고 합니다.



VPC - NAT(Network Address Translation) Gateway

프라이빗 서브넷의 인스턴스가 인터넷에 접속하거나 인터넷에서 프라이빗 서브넷의 인스턴스 접속을 가능하게 합니다. 이를 위해 **Private / Public** 네트워크 연결을 위해 **IP** 주소를 변환합니다.



Private 서브넷의 10.10.11.131 인스턴스가 인터넷 리소스를 액세스 하기 위해 NAT 를 거치는 과정은 다음과 같습니다.

1. EC2(10.10.11.131) 는 인터넷으로 트래픽을 전송하기 위해 목적지 IP 주소 (3.228.146.75)를 가지는 패킷을 생성 합니다.
2. EC2 는 라우팅테이블 규칙에 의해 NAT Gateway(10.10.1.1) 으로 라우팅 됩니다.
3. NAT 로 전달된 패킷은 NAT 에 의해 출발지 IP 주소를 NAT 의 Public IP(54.11.22.33) 주소로 변환 합니다.
4. Public IP 로 변환된 패킷은 Public 서브넷으로 라우팅 되며, Public 라우팅테이블 규칙에 의해 IGW 를 거쳐 인터넷 목적지로 연결 됩니다.
5. 인터넷 목적지 3.228.146.75 에 연결 및 응답 패킷을 받고, Public 서브넷의 라우팅 테이블의 의해 NAT 로 전달 됩니다
6. Public 서브넷의 응답 패킷을 수신한 NAT는, 이번에는 출발지를 Private IP(10.10.1.1) 로 변환 하여 Private Subnet 으로 라우팅 합니다.
7. Private Subnet 의 EC2(10.10.11.131) 는 응답 패킷을 받아 처리합니다.

VPC - VPC Gateway Endpoint (S3, DynamoDB)

The screenshot displays the AWS Management Console interface for a VPC Gateway Endpoint. The left sidebar shows navigation options under 'Virtual private cloud', 'Security', and 'Network Firewall'. The main content area shows the details for the endpoint `vpce-04cc0f8c839860e3e / mea-mc1p-s3-vpce`.

Details

Endpoint ID vpce-04cc0f8c839860e3e	Status Available	Endpoint type Gateway
VPC ID mea-mc1p-vpc	Status message -	Private DNS names enabled No
Service name com.amazonaws.me-central-1.s3		

Route tables (3)

Name	Route Table ID	Main
mea-mc1p-public-rt	rtb-0a1b2c3d4e5f6g7h8i9j (mea-mc1p-public-rt)	No
mea-mc1p-blb-b1-rt	rtb-0a1b2c3d4e5f6g7h8i9j (mea-mc1p-blb-b1-rt)	No
mea-mc1p-blb-a1-rt	rtb-0a1b2c3d4e5f6g7h8i9j (mea-mc1p-blb-a1-rt)	No

VPC - VPC Interface Endpoint

The screenshot displays the AWS Management Console interface for a VPC Interface Endpoint. The breadcrumb navigation shows 'VPC > Endpoint services > vpce-svc-05a2b5980f9203197'. The endpoint name 'vpce-svc-05a2b5980f9203197' is prominently displayed at the top. Below this, the 'Details' section provides various attributes:

- Service ID:** vpce-svc-05a2b5980f9203197
- Types:** Interface (highlighted with an orange box)
- Service name:** com.amazonaws.vpce.me-central-1.vpce-svc-05a2b5980f9203197
- State:** Available (indicated by a green checkmark)
- Network Load Balancers ARNs:** arn:aws:elasticloadbalancing:me-central-1:aws:vpce-svc-05a2b5980f9203197:nlb/me-central-1a
- DNS names:** vpce-svc-05a2b5980f9203197.me-central-1.vpce.amazonaws.com (highlighted with an orange box)
- Domain verification type:** Info
- Gateway Load Balancers ARNs:** -
- Private DNS name:** -
- Domain verification value:** Info
- Availability Zones:** 2 Availability Zones
- Domain verification status:** Info
- Supported IP address type:** ipv4
- Acceptance required:** No
- Domain verification name:** Info

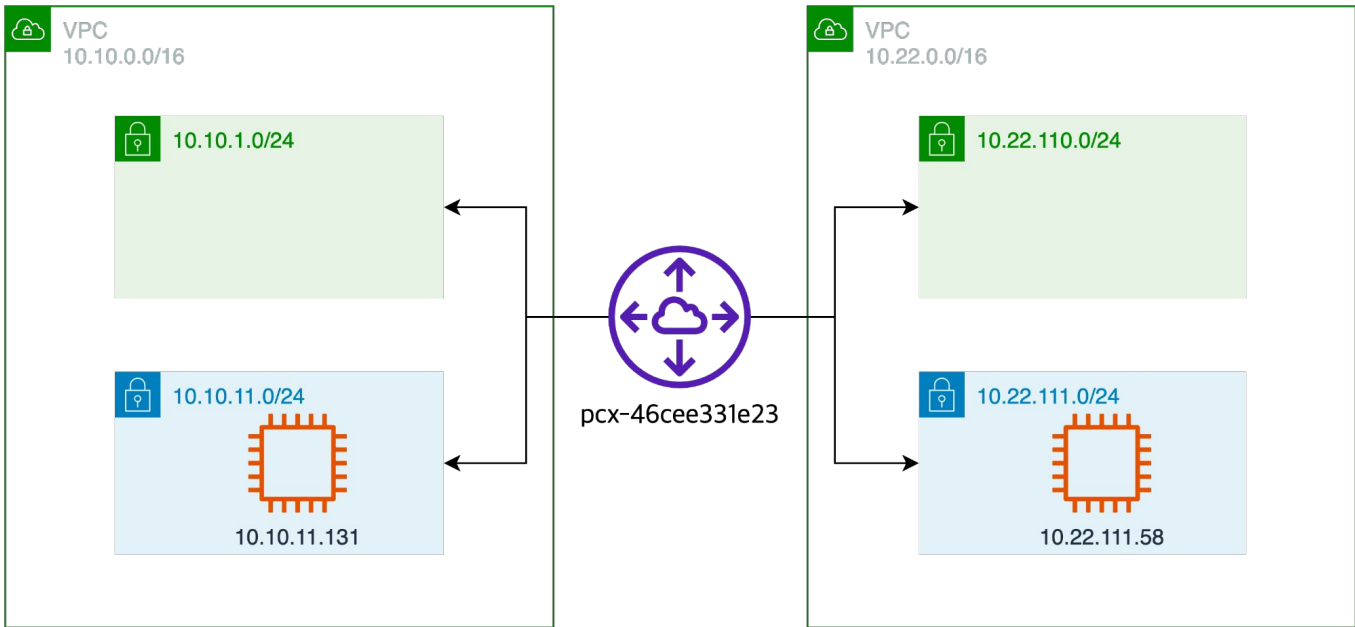
Below the details, there are tabs for 'Load balancers', 'Allow principals', 'Endpoint connections', 'Notifications', 'Monitoring', 'Contributor Insights', and 'Tags'. The 'Load balancers' tab is active, showing a list of two load balancers:

Availability Zone	Load balancer names
me-central-1b (mec1-az2)	mea-mc1p-openapi-nlb
me-central-1a (mec1-az1)	mea-mc1p-openapi-nlb

The footer of the console includes 'Feedback', 'Language', and copyright information for Amazon Web Services, Inc. or its affiliates, dated 2023.

VPC - Peering

2개의 VPC 서비스를 서로 네트워크로 연결하는 서비스 입니다. 두개의 VPC는 동일한 CIDR 대역으로 겹치지 않도록 합니다.



VPC-A Peering Route Table	
Destination	Target
10.22.0.0/16	pcx-46cee331e23

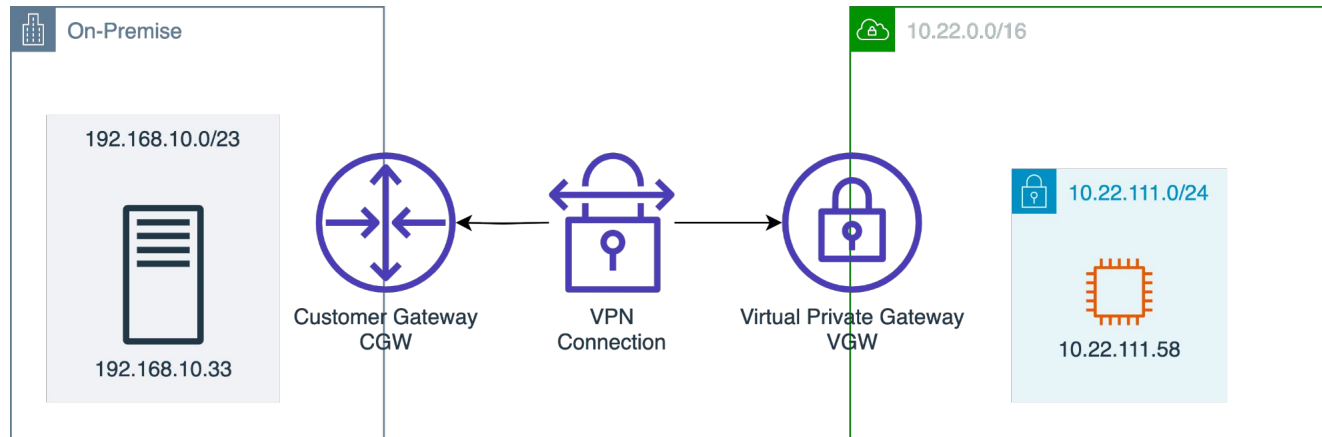
VPC-B Peering Route Table	
Destination	Target
10.10.0.0/16	pcx-46cee331e23

VPC Peering 연결은 하나의 VPC 에서 요청을, 다른 하나는 수락 을 통해서 상호간에 연결이 이루어 집니다.

1. “A” VPC 는 “B” VPC 를 대상으로 라우팅 테이블을 구성 합니다.
2. “B” VPC 는 “A” VPC 를 대상으로 라우팅 테이블을 구성 합니다.
3. VPC Peering은 별도의 보안 그룹 및 NACL 을 통해 액세스 제어를 할 수 있습니다.
4. 만약 VPC “B” 가 `bvpc.local` 과 같은 Private 도메인을 설정했고 VPC “A” 에서 이 도메인을 해석 할수 있습니다.
 - a. VPC A 및 B 에서 DNS Resolution 구성을 설정
 - b. Route 53 Resolver를 사용하여 VPC A에서 VPC B의 Private 도메인(`bvpc.local`)을 해석하도록 규칙 생성
 - c. Route 53 Resolver 규칙을 VPC A 에 연결

VPC - Virtual Private Gateway

Virtual Private Gateway(VGW)는 온프레미스 네트워크 또는 다른 클라우드 환경과 네트워크 연결을 제공하는 서비스입니다. VGW는 VPC와 외부 네트워크 간의 트래픽을 안전하게 라우팅하고, 보안적으로 격리된 통신을 지원합니다.



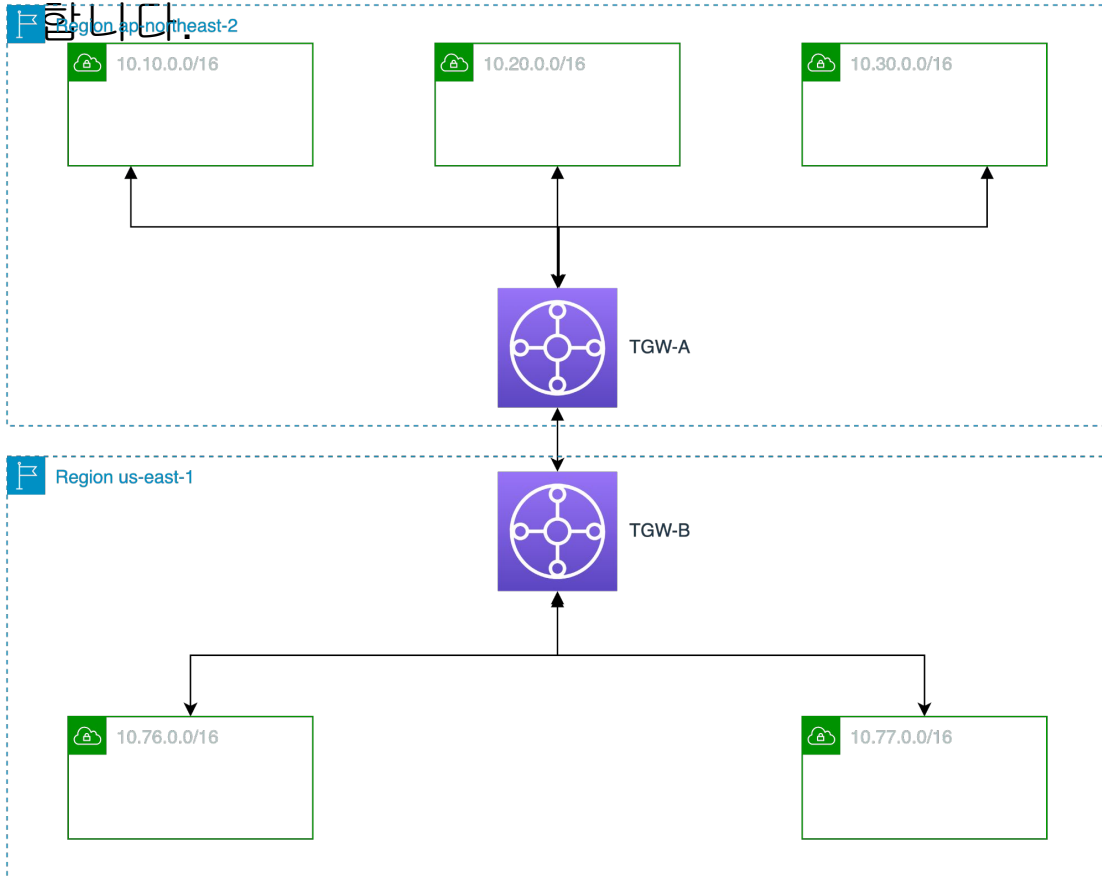
Virtual Private Gateway Route Table	
Destination	Target
192.168.10.0/23	vgw-8fdc53bf

Virtual Private Gateway 연결은 VPC와 On-Premise 네트워크 연결을 지원 하는 서비스 입니다. **Static** 및 **BGP** 기반의 동적 라우팅 방식이 있습니다.

1. CGW(고객 게이트웨이)를 구성 합니다. VPN 연결을 위한 Public IP 와 Static 라우팅을 설정 합니다.
2. VGW(가상 사설 게이트웨이)를 생성하고 VPC 를 추가 합니다.
3. VPN Connection(Site to Site) 을 구성 합니다. 앞서 생성한 VGW 와 CGW 를 바인딩 합니다. Static 라우팅 설정으로 구성 하며, OnPremise 와 VPC CIDR 대역을 추가 하여 Tunneling 을 구성 합니다. Local IPv4 Network Cidr 은 OnPremise CIDR 를, Remote IPv4 Network Cidr 는 VPC CIDR 를 기입합니다.
4. VPC 는 OnPremise 를 대상으로 라우팅 테이블을 구성 합니다.
5. VPC 는 Security Group 를 구성 합니다. (SSH, ICMP 등)
6. OnPremise 는 VPN 서버(예:OpenSwan)설정에서 VPC 네트워크 연결을 허용 하도록 구성합니다.

VPC - Transit Gateway

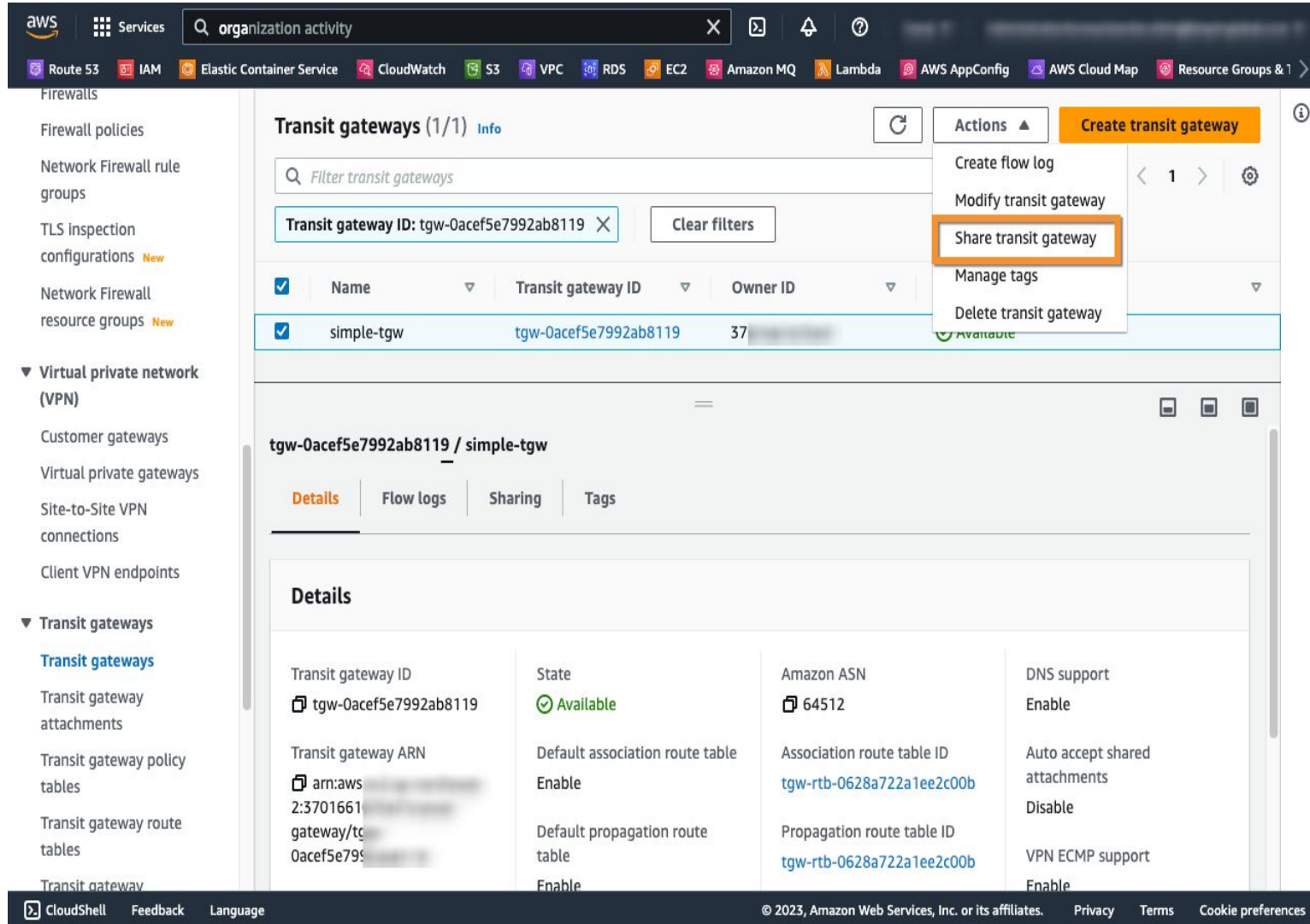
Transit Gateway(TGW)는 여러 VPC 및 온프레미스 네트워크 연결을 중앙 집중화하여 운영 관리를 편리하게 합니다. TGW 는 리전에 종속적이며, **Peering** 을 통해 다른 리전의 TGW 와 연결하고, TGW 리소스 공유 기능으로 다른 AWS 계정과 연결 할 수 있습니다. VPC CIDR 가 충돌되지 않도록 주의



Transit Gateway(TGW) 네트워크 구성 절차는 다음과 같습니다.

1. TGW-A 에서 Transit Gateway(TGW-A) 를 생성 합니다.
2. VPC-2, VPC-3 에서 TGW를 연결(attach) 합니다.
3. VPC-1 에서 TGW 연결 요청(VPC-2,3)을 수락 합니다.
4. VPC-1, VPC-2, VPC-3 의 라우팅 테이블에서 **tgw-a** 를 **Destination** 으로 설정 합니다.
5. VPC-4 에서 Transit Gateway(TGW-B) 를 생성 합니다.
6. VPC-5 에서 TGW-B 를 연결(attach) 합니다.
7. VPC-4 에서 TGW 연결 요청(VPC-5)을 수락 합니다.
8. TGW-A 에서 Transit Gateway Peering을 생성하고 TGW-B 를 대상으로 설정 합니다.
9. TGW-B 에서 Transit Gateway Peering을 생성하고 TGW-A 를 대상으로 설정 합니다.
10. 각 Transit Gateway의 라우팅 테이블을 수정하여 대상 Transit Gateway의 CIDR 블록에 대한 라우팅 규칙을 추가합니다.

VPC - Transit Gateway Demo - create TGW



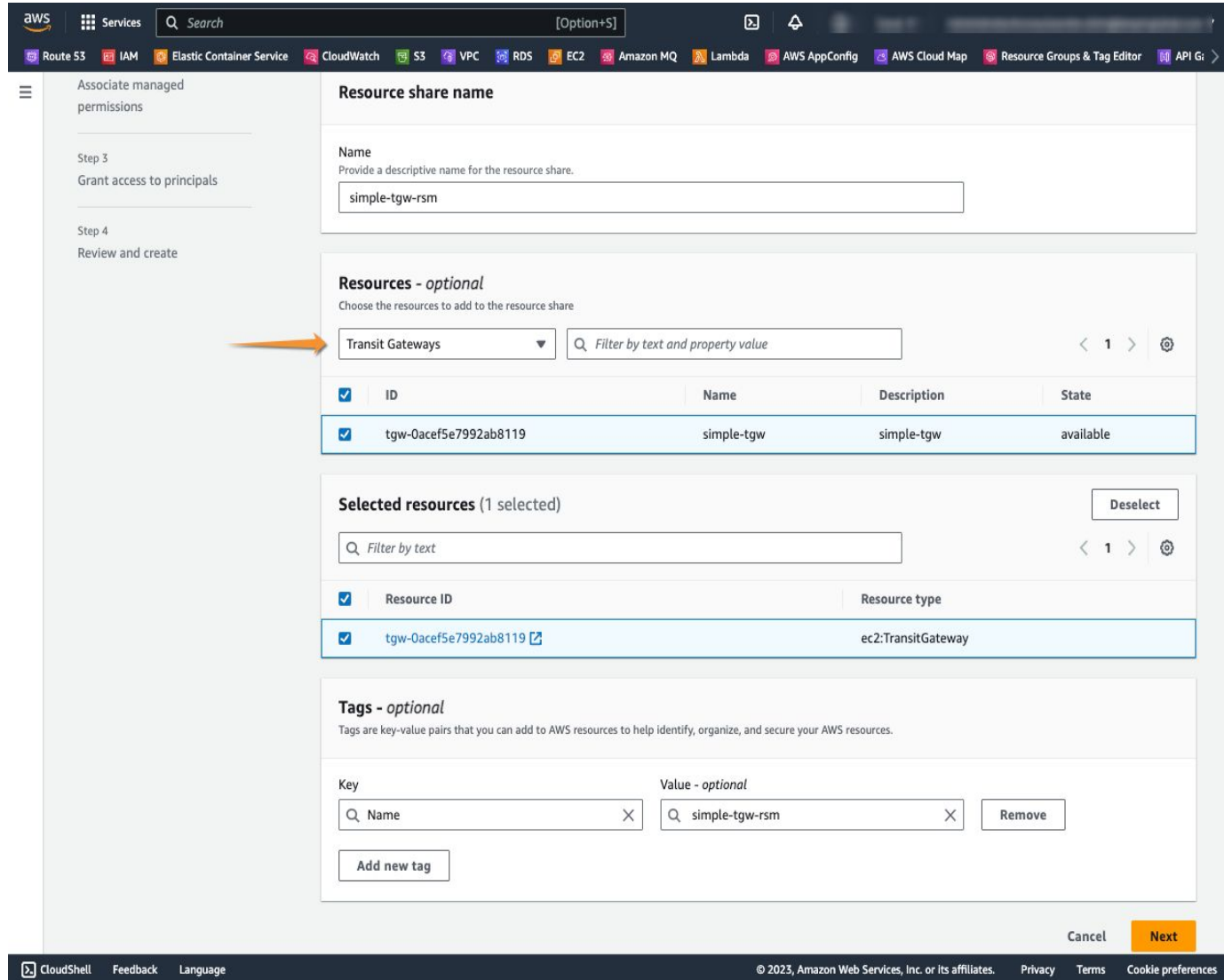
The screenshot shows the AWS Management Console for Transit Gateways. The left sidebar lists navigation options under 'Virtual private network (VPN)' and 'Transit gateways'. The main content area shows a list of transit gateways with one entry, 'simple-tgw', selected. The 'Actions' menu is open, and 'Share transit gateway' is highlighted. Below the list, the details for 'tgw-0acef5e7992ab8119 / simple-tgw' are displayed in a tabbed interface.

Details			
Transit gateway ID	State	Amazon ASN	DNS support
tgw-0acef5e7992ab8119	Available	64512	Enable
Transit gateway ARN	Default association route table	Association route table ID	Auto accept shared attachments
arn:aws:ec2:us-east-1:123456789012:transit-gateway/tgw-0acef5e7992ab8119	Enable	tgw-rtb-0628a722a1ee2c00b	Disable
	Default propagation route table	Propagation route table ID	VPN ECMP support
	Enable	tgw-rtb-0628a722a1ee2c00b	Enable

VPC 1 에서 Transit Gateway(TGW) - simple-tgw 를 생성 합니다.

다중 AWS 어카운트에 TGW 를 공유하기 위해 “Share transit gateway” 구성을 설정 합니다.

VPC - Transit Gateway Demo - share TGW



The screenshot shows the AWS IAM console interface for creating a resource share. The left sidebar indicates the current step is 'Grant access to principals'. The main content area is divided into sections: 'Resource share name', 'Resources - optional', 'Selected resources', and 'Tags - optional'.

Resource share name

Name
Provide a descriptive name for the resource share.
simple-tgw-rsm

Resources - optional
Choose the resources to add to the resource share

Transit Gateways

<input checked="" type="checkbox"/>	ID	Name	Description	State
<input checked="" type="checkbox"/>	tgw-0acef5e7992ab8119	simple-tgw	simple-tgw	available

Selected resources (1 selected) Deselect

<input checked="" type="checkbox"/>	Resource ID	Resource type
<input checked="" type="checkbox"/>	tgw-0acef5e7992ab8119 link	ec2:TransitGateway

Tags - optional
Tags are key-value pairs that you can add to AWS resources to help identify, organize, and secure your AWS resources.

Key: Value - optional: Remove

Add new tag

Cancel Next

리소스 공유 유형을 Transit Gateway 를 선택하고, 앞서 생성한 tgw 인스턴스 아이디와, 리소스 아이디를 선택 합니다.

VPC - Transit Gateway Demo - share TGW

The screenshot shows the AWS IAM console interface. The top navigation bar includes the AWS logo, a search bar, and a list of services: Route 53, IAM, Elastic Container Service, CloudWatch, S3, VPC, RDS, EC2, Amazon MQ, Lambda, AWS AppConfig, AWS Cloud Map, Resource Groups & Tag Editor, and API Gateway. The breadcrumb trail indicates the current path: Resource Access Manager > Shared by me: Resource shares > Create resource share. The left sidebar shows a step-by-step progress: Step 1 (Specify resource share details), Step 2 (Associate managed permissions - currently active), Step 3 (Grant access to principals), and Step 4 (Review and create). The main content area is titled 'Associate managed permissions' with a subtitle: 'To specify which actions principals are allowed to perform on shared resources, choose the managed permission to associate with each shared resource type.' Below this, a section titled 'Managed permission for ec2:TransitGateway' contains a 'Managed permissions' subsection. It states 'For this resource type, only one managed permission is available.' and shows a text box with 'AWSRAMDefaultPermissionTransitGateway' and a refresh icon. There is a button 'Create customer managed permission' with an external link icon. Below that is a 'Version' subsection stating 'You can use only the default version of a managed permission when creating a resource share.' and shows a dropdown menu with '1 (default)' selected. At the bottom of the main content area is a link 'View the policy template for this managed permission'. At the bottom right of the console are three buttons: 'Cancel', 'Previous', and 'Next'.

Transit Gateway 의
IAM 액세스 정책을
선택 합니다.

고객 전용 TGW
연결 구성을 위한
Custom 액세스
정책을 생성하고
적용할 수 있습니다.

VPC - Transit Gateway Demo - share TGW

The screenshot shows the AWS IAM console interface for granting access to principals. The left sidebar indicates the current step is 'Step 3 - optional: Grant access to principals'. The main content area is titled 'Principals - optional' and contains two radio button options for sharing resources. The second option, 'Allow sharing only within your organization', is selected. Below these options, there is a section for adding principals, including a dropdown for 'Select principal type' (set to 'AWS account') and a text input for 'Enter an AWS account ID'. A table at the bottom lists 'Selected principals (2)', showing two AWS accounts with their IDs and principal types. Navigation buttons 'Cancel', 'Previous', and 'Next' are at the bottom right.

Principals - optional

☐ Allow sharing with anyone
You can share resources with any AWS accounts, roles, and users. If you are in an organization, you can also share with the entire organization or organizational units in that organization.

☒ Allow sharing only within your organization
You can share resources with the entire organization, organizational units, or AWS accounts, roles, and users in that organization.

Principals
You can add multiple principals of different types.

Select principal type
AWS account ▼

Enter an AWS account ID
[Input field]

An AWS account ID is a 12-digit number.

Add

Selected principals (2)
The following principals will be allowed access to the shared resources.

Filter by text

<input type="checkbox"/>	Principal ID	Principal type
<input type="checkbox"/>	97 [redacted] 34	AWS account
<input type="checkbox"/>	33 [redacted] 67	AWS account

Cancel Previous Next

공유 범위와 공유 대상 주체를 지정하여 TGW 를 공유 할 수 있습니다.

공유 대상 주체 유형은 아래와 같습니다.

- AWS account
- Organization
- Organization unit(OU)
- IAM role
- IAM user
- Service principal

VPC - Transit Gateway Demo - attachment TGW

aws 서비스 검색 [옵션+S]

Route 53 EC2 IAM Elastic Container Service VPC Amazon MQ AWS AppConfig AWS Cloud Map Resource Groups & Tag Editor RDS API Gateway CloudWatch Key Managem

Transit Gateway Attachment 생성 정보

Transit Gateway(TGW)는 동일한 AWS 계정 내 또는 AWS 계정 간에 연결(VPC 및 VPN)을 상호 연결하는 네트워크 전송 허브입니다.

세부 정보

이름 태그 - 선택 사항
키가 Name으로 설정되고 값이 지정된 문자열로 설정된 태그를 생성합니다.

common-vpc-to-simple-tgw

Transit gateway ID 정보
tgw-0acef5e7992ab8119

연결 유형 정보
VPC

VPC 연결

VPC 연결을 선택하고 구성합니다.

☒ DNS 지원 정보

☐ IPv6 지원 정보

☐ 어플라이언스 모드 지원 정보

VPC ID
Transit Gateway에 연결할 VPC를 선택합니다.

vpc-0a2ee...

서브넷 ID 정보
Transit Gateway VPC 연결을 생성할 서브넷을 선택합니다.

☒ ap-northeast-2a subnet-0d4bfdfc

☐ ap-northeast-2b 사용 가능한 서브넷 없음

☒ ap-northeast-2c subnet-05505e7cf

CloudShell 의견 언어

© 2023, Amazon Web Services, Inc. 또는 계열사. 개인 정보 보호 약관 쿠키 기본 설정

VPC 2 에서 공유된 TGW 를 선택하여 VPC 연결을 요청합니다.

VPC - Transit Gateway Demo - accept TGW

aws

Services

Search

[Option+S]

Route 53

IAM

Elastic Container Service

CloudWatch

S3

VPC

RDS

EC2

Amazon MQ

Lambda

AWS AppConfig

AWS Cloud Map

Resource Groups & Tag Editor

API Gate

resource groups

Virtual private network (VPN)

Customer gateways

Virtual private gateways

Site-to-Site VPN connections

Client VPN endpoints

Transit gateways

Transit gateways

Transit gateway attachments

Transit gateway policy tables

Transit gateway route tables

Transit gateway multicast

Traffic Mirroring

Mirror sessions

Mirror targets

Mirror filters

VPC > Transit gateway attachments > tgw-attach-0dc842b0f05f19167

tgw-attach-0dc842b0f05f19167

Details

Transit gateway attachment ID

tgw-attach-0dc842b0f05f19167

Transit gateway ID

tgw-0acef5e7992ab8119

Transit gateway owner ID

47

Subnet IDs

2 Subnets

State

Pending Acceptance

Resource owner ID

34 (Shared)

DNS support

Enable

Resource type

VPC

Resource ID

vpc-0a2ee61aa985c3fbb

IPv6 support

Disable

Actions

Create flow log

Modify transit gateway attachment

Manage tags

Accept transit gateway attachment

Reject transit gateway attachment

Delete transit gateway attachment

-

Appliance Mode support

Disable

Flow logs

Tags

Flow logs

CloudShell

Feedback

Language

© 2023, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

VPC 1 의 TGW
연결에서 VPC 2 연결
요청을 수락 합니다.

VPC - Transit Gateway Demo - Review

Associations

tgw-rtb-0628a722a1ee2c00b / simple-tgw-rt

Details

Associations

Propagations

Prefix list references

Routes

Tags

Associations (1/1) Info

Filter associations

1

Refresh

Delete association

Create association

Attachment ID	Resource type	Resource ID	State
tgw-attach-0dc842b0f05f19167	VPC	vpc-0a2c...	Associated

Propagations

tgw-rtb-0628a722a1ee2c00b / simple-tgw-rt

Details

Associations

Propagations

Prefix list references

Routes

Tags

Propagations (1/1) Info

Filter propagations

1

Refresh

Delete propagation

Create propagation

Attachment ID	Resource type	Resource ID	State
tgw-attach-0dc842b0f05f19167	VPC	vpc-0a2c...	Enabled

Routes

Details

Associations

Propagations

Prefix list references

Routes

Tags

Filter routes by CIDR (2)

Exact CIDR

Longest prefix match

Supernet of match

Subnet of match

Routes (1/1)

Filter routes

1

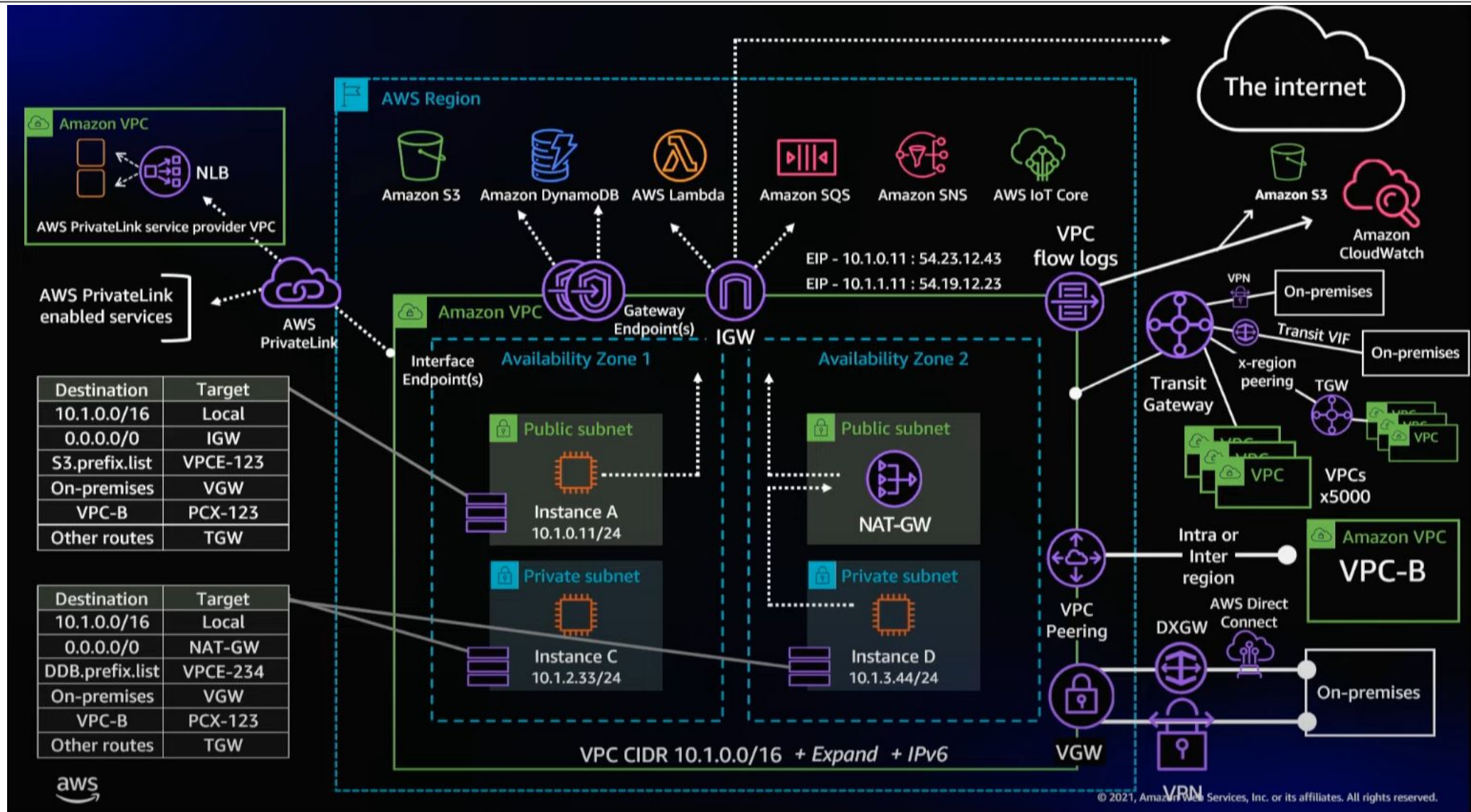
Refresh

Actions

Create static route

CIDR	Attachment ID	Resource ID	Resource type	Route type
10.200.0.0/16	tgw-attach-0dc842b0f05f19167	vpc-0a2c...	VPC	Propagated

VPC Architecture



Think Together

- VPC 네트워크에서 가장 안전한 설계는 무엇 일까요?
- 고 가용성을 위해 어떤것을 제공 하면 되나요?
- 보안 안정성과 성능은 높이면서도 비용을 줄이는 VPC 네트워크 설계 기법은 무엇일까요?
- 운영의 편의 / 자동화는 어떻게 도달 할 수 있나요?
- VPC 네트워크 영역에서 발생하는 트러블은 어떤 것들이 있나요?
- 자동화로 인해 발생하는 문제가 있을 까요?
- NoCode 는 무엇 인가요?
- 하루 매출 80 억을 매출을 발생하는 AWS 서비스를 운영하고 있습니다.
 - AWS 감사에서 외부망으로부터 EC2 WEB 서버가 권고하지 않는 포트인 22, 1521, 8080,3306,6379 포트를 허용하도록 되어 있어 조치 권고를 받았습니다. 보안 그룹이 문제로 식별이 되었는데요 여러분은 보안그룹을 수정할 수 있을까요?

VPC 네트워크 보안

Security Group

VPC - Security Group

Inbound rules (38)								Manage tags	Edit inbound rule
<input type="text" value="Filter security group rules"/>							< 1 >		
<input type="checkbox"/>	Name ▾	Security group rule... ▾	IP versi... ▾	Type ▾	Protocol ▾	Port range ▾	Source ▾		
<input type="checkbox"/>	-	sgr-059f0e89d7e029396	-	Custom TCP	TCP	8090	sg-08ae03a797671e141 / mea-mc1p-costetl-gbs-sg		
<input type="checkbox"/>	-	sgr-0083d1a6e2b996...	-	Custom TCP	TCP	8080 - 9140	sg-0082195a3348a76b2 / mea-mc1p-padm-web-sg		
<input type="checkbox"/>	-	sgr-0de033955244c19...	-	Custom TCP	TCP	8080 - 9140	sg-05e24f6cca54d0da4 / mea-mc1p-awsbatch-sg		
<input type="checkbox"/>	-	sgr-0722c20f3b286641f	-	Custom TCP	TCP	8080 - 9140	sg-02dec432baa99a4da / mea-mc1p-openapi-cost-sg		
<input type="checkbox"/>	-	sgr-0f662d71b6d8cda6c	-	Custom TCP	TCP	8080 - 9140	sg-0133e3d77fe169a72 / mea-mc1p-orgtree-web-sg		
<input type="checkbox"/>	-	sgr-0252a7051c1624f69	-	Custom TCP	TCP	8080 - 9140	sg-08f2ff09ea8750742 / mea-mc1p-cost-admin-sg		
<input type="checkbox"/>	-	sgr-0c4cec8f38973ffc6	-	Custom TCP	TCP	8080 - 9140	sg-0ecd7327ebc46dfa1 / mea-mc1p-cre-api-sg		
<input type="checkbox"/>	-	sgr-09868cf5d6c43709b	-	Custom TCP	TCP	8080 - 9000	sg-0b0a0a36b4e778803 / mea-mc1p-gbs-batch-sg		
<input type="checkbox"/>	-	sgr-0da29e69b3036c5...	-	Custom TCP	TCP	8080 - 9140	sg-0f3b606a4caa3b6ef / mea-mc1p-gov-web-sg		
<input type="checkbox"/>	-	sgr-0778e735b9168e...	-	Custom TCP	TCP	8080 - 9140	sg-0ae1393ed026c2006 / mea-mc1p-cre-web-sg		
<input type="checkbox"/>	-	sgr-034116d2510642...	-	Custom TCP	TCP	8080 - 9140	sg-0eb9dff81d5c9e1a6 / mea-mc1p-svcgrp-batch-sg		
<input type="checkbox"/>	-	sgr-0d35de0fb4c856171	-	Custom TCP	TCP	8080 - 9140	sg-0596485f903dacbcc / mea-mc1p-cost-web-sg		
<input type="checkbox"/>	-	sgr-0c773b1be596bd7...	-	Custom TCP	TCP	8080 - 9140	sg-0ff610a58c0913829 / mea-mc1p-assetaws-proc...		
<input type="checkbox"/>	-	sgr-0baac1234a602c315	-	Custom TCP	TCP	8080 - 9140	sg-0fb17e30397164ce5 / mea-mc1p-kpi-web-sg		
<input type="checkbox"/>	-	sgr-0421f94fd12c3bc90	-	Custom TCP	TCP	8080 - 9140	sg-0c7a328aafce2b331 / mea-mc1p-kpi-api-sg		
<input type="checkbox"/>	-	sgr-0213c72d71049344f	-	Custom TCP	TCP	8080 - 9140	sg-0d7e5952f23530923 / mea-mc1p-sso-web-sg		
<input type="checkbox"/>	-	sgr-0536cb44d7cd96ef3	-	Custom TCP	TCP	8080 - 9140	sg-028455757ec331912 / mea-mc1p-padm-api-sg		

VPC - Security Group

Inbound rules

Outbound rules

Tags

Outbound rules (13)

🔄

Manage tags

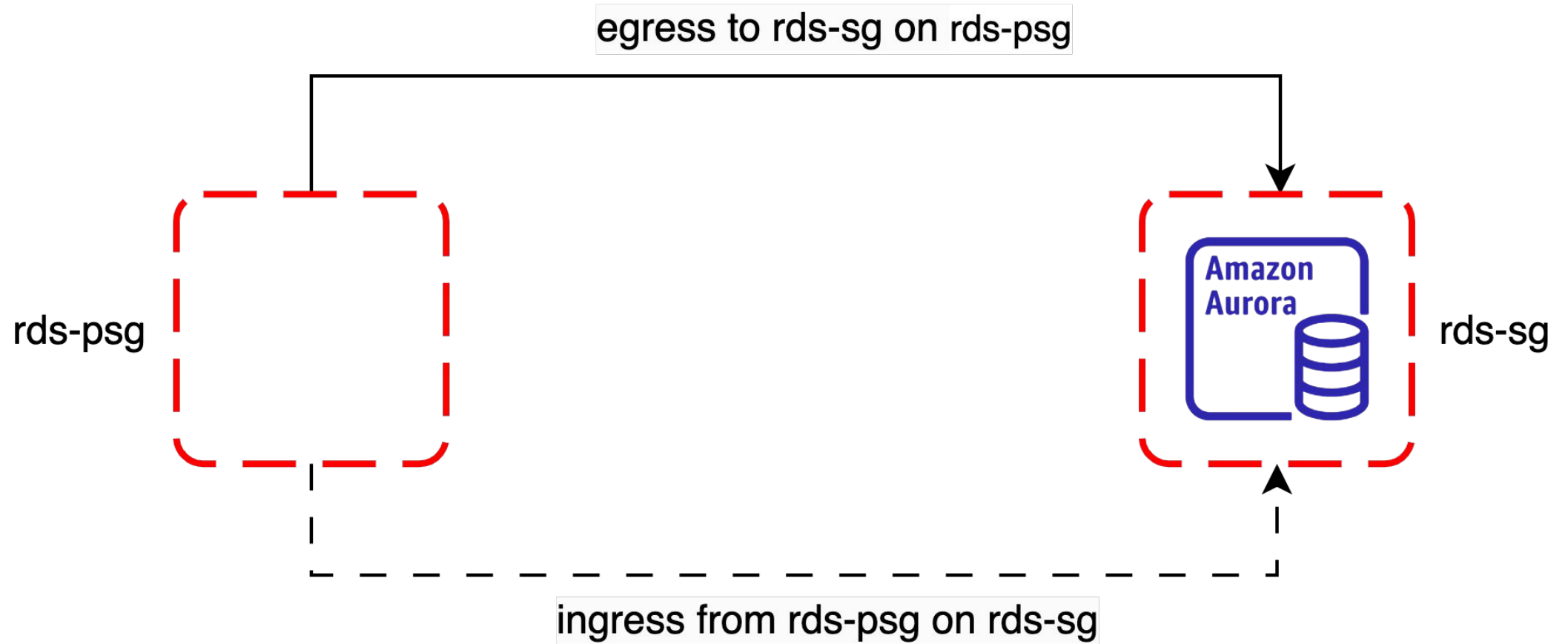
Edit outbound rules

🔍 Filter security group rules

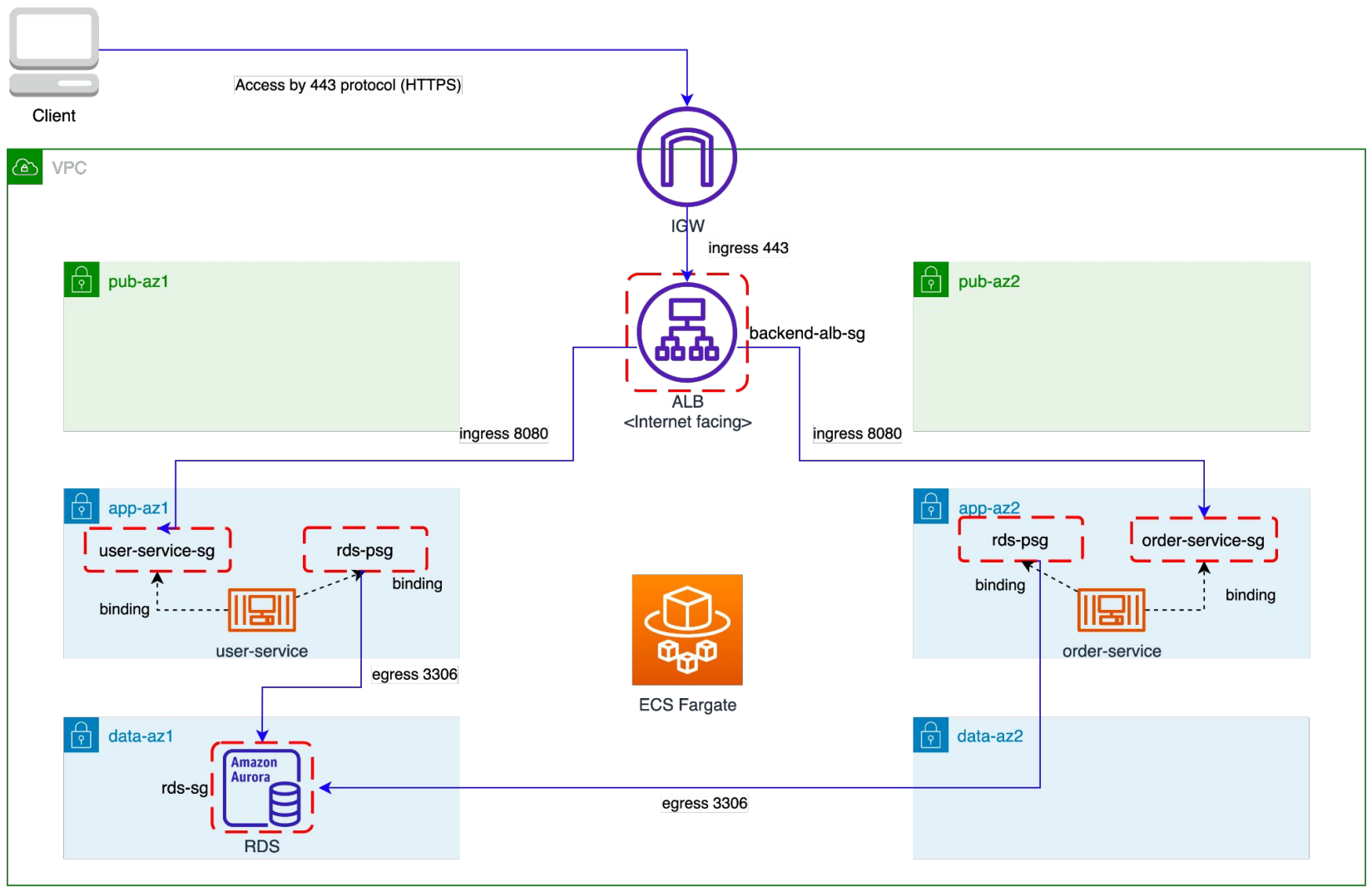
< 1 > ⚙️

<input type="checkbox"/>	Name ▾	Security group rule... ▾	IP versi... ▾	Type ▾	Protocol ▾	Port ra... ▾	Destination ▾	Description ▾
<input type="checkbox"/>	–	sgr-0d10cfe0159e9c392	–	Custom TCP	TCP	8080	sg-0ae12eae9d9cd0cb0 / mea-mc1p-earth-api-sg	mea-mc1p-earth-api
<input type="checkbox"/>	–	sgr-0460a1c2693b8a5...	–	Custom TCP	TCP	8080	sg-0c7a328aafce2b331 / mea-mc1p-kpi-api-sg	mea-mc1p-kpi-api
<input type="checkbox"/>	–	sgr-0e82631321a032f05	–	Custom TCP	TCP	9081	sg-014ba9581c8d73918 / mea-mc1p-costopt-api-sg	mea-mc1p-costopt-api
<input type="checkbox"/>	–	sgr-029f04d4ad1da1078	–	Custom TCP	TCP	9031	sg-0ecd7327ebc46dfa1 / mea-mc1p-cre-api-sg	mea-mc1p-cre-api
<input type="checkbox"/>	–	sgr-0f09dd54c76957e93	–	Custom TCP	TCP	8080	sg-0b0a0a36b4e778803 / mea-mc1p-gbs-batch-sg	mea-mc1p-gbs-batch
<input type="checkbox"/>	–	sgr-03694440fa72a0ba1	–	Custom TCP	TCP	8080	sg-06f97d9cd13cf6df9 / mea-mc1p-costdis-api-sg	mea-mc1p-costdis-api
<input type="checkbox"/>	–	sgr-0e5d9fd6b80cdd564	–	Custom TCP	TCP	8080	sg-0550c1f5f962c9369 / mea-mc1p-portal-app-clssg	mea-mc1p-portal-api
<input type="checkbox"/>	–	sgr-047a85ccdb3f90b43	–	Custom TCP	TCP	9135	sg-028455757ec331912 / mea-mc1p-padm-api-sg	mea-mc1p-padm-api
<input type="checkbox"/>	–	sgr-0f5a2c5cd8f2cfbd2	–	Custom TCP	TCP	8080	sg-0e85235a0a0f48b5c / mea-mc1p-adm-api-sg	mea-mc1p-adm-api
<input type="checkbox"/>	–	sgr-04a8ad0b745c93c10	–	Custom TCP	TCP	8080	sg-0089ed68091ffddad / mea-mc1p-cost-api-sg	mea-mc1p-cost-api
<input type="checkbox"/>	–	sgr-0906ab7e430700...	–	Custom TCP	TCP	9111	sg-0a18bbca1a7bf0416 / mea-mc1p-orgtree-api-sg	mea-mc1p-orgtree-api
<input type="checkbox"/>	–	sgr-022754229e6d1f3a5	–	Custom TCP	TCP	9091	sg-0837c5cf6e8178321 / mea-mc1p-gov-api-sg	mea-mc1p-gov-api
<input type="checkbox"/>	–	sgr-0619be6796245c1...	–	Custom TCP	TCP	8080	sg-0f5f5e895c3e5ba74 / mea-mc1p-asset-apiv2-sg	mea-mc1p-asset-apiv2

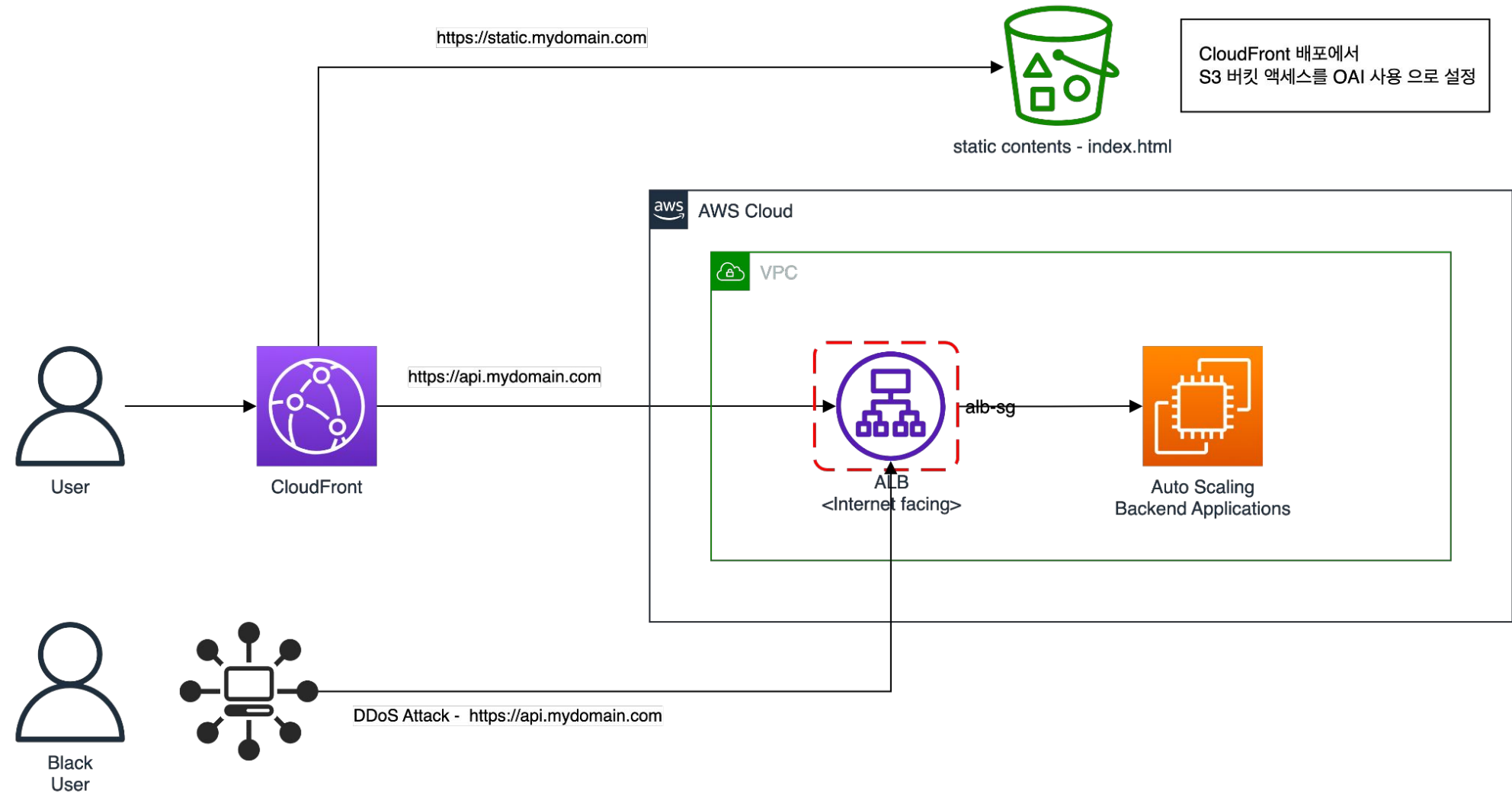
VPC - Security Group



Advanced Security Group Practice



Advanced Security Policy for Service



Advanced Security Policy for Service

<http://draw.io/>

<https://symplesims.github.io/>

<https://github.com/orgs/chiwooiac/repositories>

<https://github.com/orgs/chiwoo-cloud-native/repositories>



감사합니다

BESPIN GLOBAL