

샘플 페이지입니다.

# 01. [실습8-1] 멀티 리전 & 하이브리드 환경 종합 실습

난이도: ★★★(★) Extra Hard

## 실습 목표

멀티 리전 환경과 하이브리드 클라우드 환경에서 웹과 DB 서비스에 대한 동작을 통해 지금까지 지 설명 드린 다양한 AWS 네트워크 기술을 확인해 보는 종합 실습입니다.

## 실습 단계

### 1.1 실습 개요

- 1.1.1 실습 전 공지 사항
- 1.1.2 네트워크 대역 설계와 DNS 설계
- 1.1.3 웹 서비스와 DB 서비스
- 1.1.4 평상 시 서비스 상태 점검
- 1.1.5 장애 발생 시 동작

### 1.2 기본 환경 구성

- 1.2.1 [서울] CloudFormation 적용
- 1.2.2 [싱가포르] CloudFormation 적용

### 1.3 전송 게이트웨이와 온프레미스의 VPN 설정

- 1.3.1 [서울] VPN 설정
- 1.3.2 [서울] 전송 게이트웨이 라우팅 정보 추가
- 1.3.3 [서울] 통신 확인
- 1.3.4 [싱가포르] VPN 설정
- 1.3.5 [싱가포르] 전송 게이트웨이 라우팅 정보 추가
- 1.3.6 [싱가포르] 통신 확인

### 1.4 전송 게이트웨이 리전 간 피어링 설정

- 1.4.1 [싱가포르] 전송 게이트웨이 연결
- 1.4.2 [서울] 전송 게이트웨이 연결 수락
- 1.4.3 [서울] 전송 게이트웨이 라우팅 정보 추가
- 1.4.4 [싱가포르] 전송 게이트웨이 라우팅 정보 추가

### 1.4.5 [서울] 통신 확인

### 1.4.6 [싱가포르] 통신 확인

### 1.5 DB 복제 설정

- 1.5.1 [싱가포르] 서울 리전 DB 서버와 연결
- 1.5.2 [싱가포르] 마스터 DB 서버와 복제 관계 설정

### 1.6 평상시 확인

- 1.6.1 [서울 근접 사용자] 웹 서비스 접근
- 1.6.2 [싱가포르 근접 사용자] 웹 서비스 접근
- 1.6.3 [서울 근접 사용자] DB 데이터 추가
- 1.6.4 [싱가포르 근접 사용자] DB 데이터 확인
- 1.6.5 접속 동작 정리

### 1.7 장애 발생시 확인

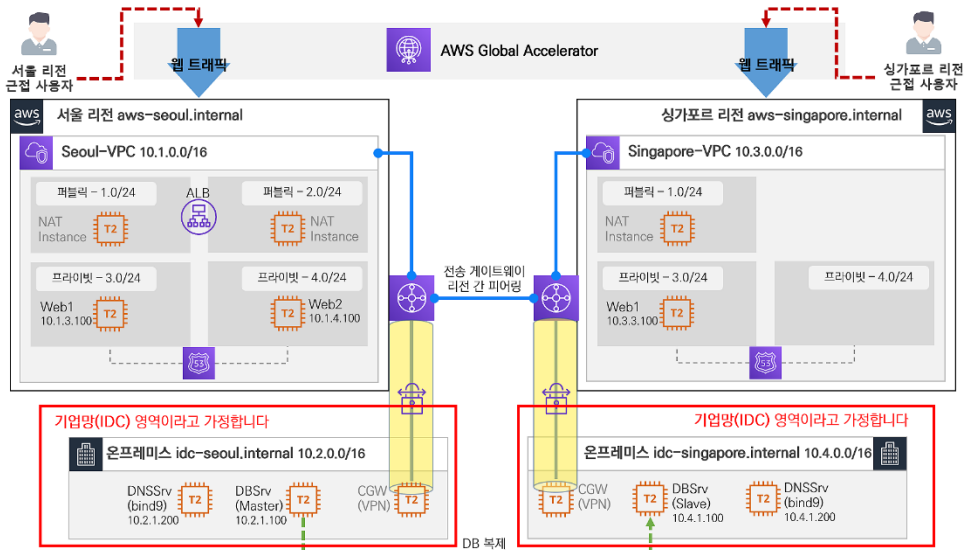
- 1.7.1 [서울] 온프레미스의 마스터 DB 중지
- 1.7.2 [서울] 웹 서버 상태 확인 및 데몬 상태 확인
- 1.7.3 ALB에서 상태 확인
- 1.7.4 [서울] Global Accelerator에서 상태 확인
- 1.7.5 [서울 사용자] 웹과 DB 서비스 접속

### 1.8 자원 삭제

## 8장

## 목표 구성도

▶ [그림 1] 멀티 리전 & 하이브리드 환경 종합 실습 목표 구성도



## 참고 사항

서울 온프레미스<sub>(IDC)</sub> 영역과 싱가포르 온프레미스<sub>(IDC)</sub> 영역은 별도의 AWS VPC 환경으로 구성하였습니다.

## 1.1 실습 개요

### 1.1.1 실습 전 공지 사항

본 실습 구성은 실제 서비스 운영을 위한 아키텍처가 아닌 네트워크 실습을 중점에 둔 아키텍처입니다. 멀티 리전 서비스 동작을 위해 최소한의 기술을 적용하였으며, (예: DB 복제) 네트워크 이외에 다른 기술은 책의 주제에서 벗어나는 내용이므로 간략한 설명으로 대신하겠습니다. 난이도가 높은 만큼 앞서 1~7 장까지 내용을 충분히 숙지한 이후에 진행하기를 권장합니다.

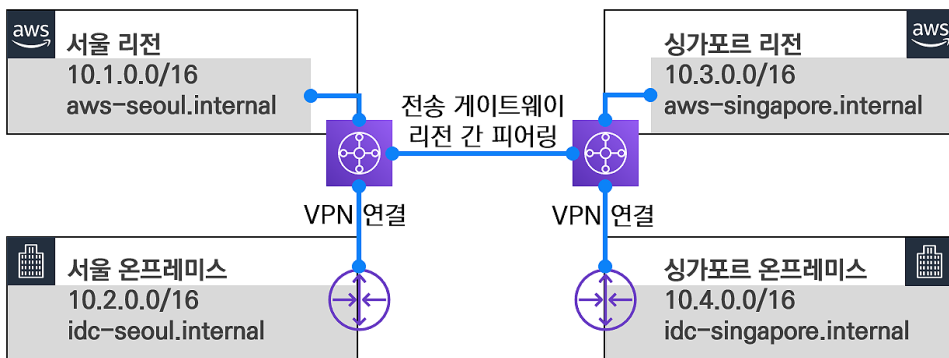
### 1.1.2 네트워크 대역 설계와 DNS 설계

서울과 싱가포르 리전에 각각 AWS 영역과 온프레미스 영역이 배치되어 있습니다. 네트워크 IP 대역은 다음과 같이 사용하고 있습니다.

- 서울 리전 AWS 영역: 10.1.0.0/16
- 서울 리전 온프레미스 영역: 10.2.0.0/16
- 싱가포르 리전 AWS 영역: 10.3.0.0/16
- 싱가포르 리전 온프레미스 영역: 10.4.0.0/16

각 영역마다 내부 도메인 <sup>Private DNS</sup>을 사용하고 있습니다. AWS 영역의 경우 Route 53 프라이빗 호스팅 영역을 사용하고, 온프레미스 영역의 경우 1 대의 인스턴스가 DNS 서버 역할을 합니다. 온프레미스 영역과 AWS 영역 간 DNS 질의 <sup>Query</sup>는 Route 53 Resolver를 통해서 처리합니다.

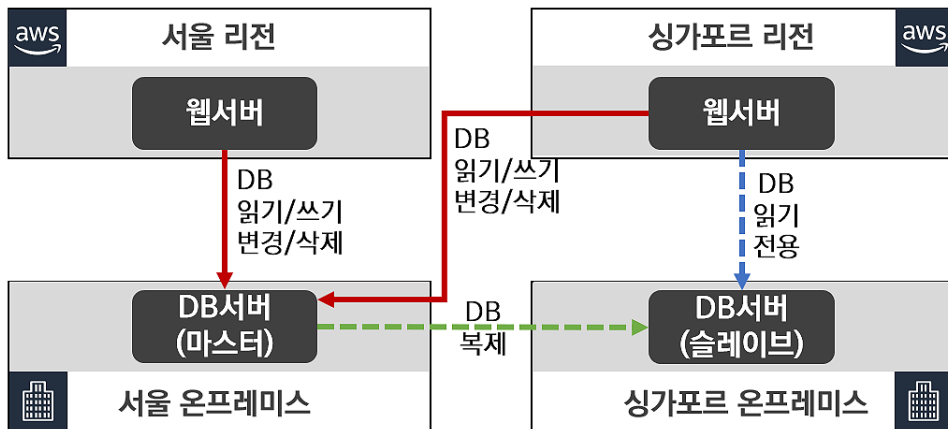
▶ [그림 1-1-1] 네트워크 대역 설계와 DNS 설계



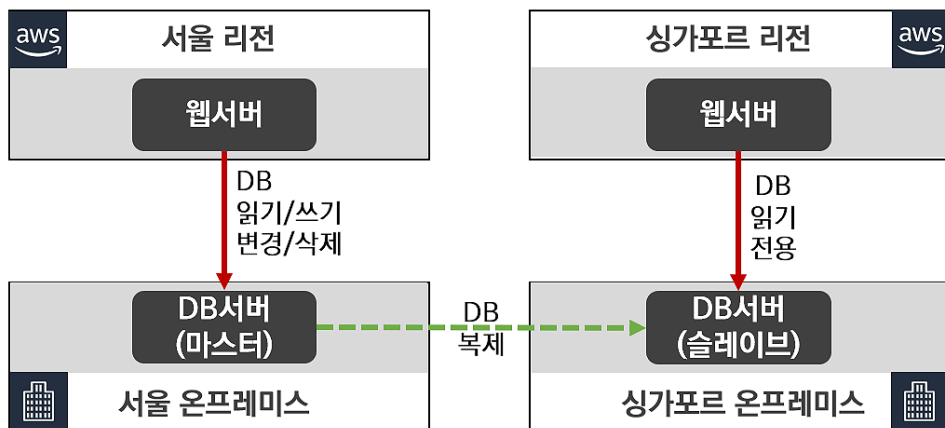
### 1.1.3 웹 서비스와 DB 서비스

일반적으로 데이터베이스의 부하를 줄이기 위해서 읽기 전용 <sup>(슬레이브 DB)</sup> 데이터베이스를 별도로 구성합니다. 평상시 DB 읽기 요청 시 슬레이브 DB로 연결하며, DB 변경 <sup>(쓰기/삭제)</sup> 요청 시에는 마스터 DB로 연결합니다.

➤ [그림 1-1-2] 일반적인 웹 서버와 DB 서버의 동작



➤ [그림 1-1-3] 실습 전용의 웹 서버와 DB 서버의 동작

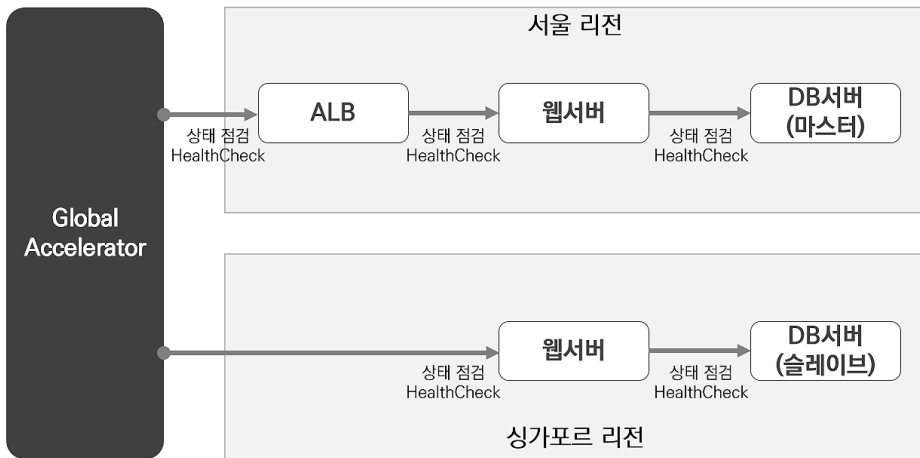


일반적인 웹 서버와 DB 서버의 동작은 [그림 1-1-2]와 같지만 이번 실습에서는 단순한 구성과 확인을 위해서 [그림 1-1-3]과 같이 평상시에 싱가포르 웹서버에 DB 변경 요청 시는 거절하도록 설정하였습니다.

### 1.1.4 평상시 서비스 상태 점검

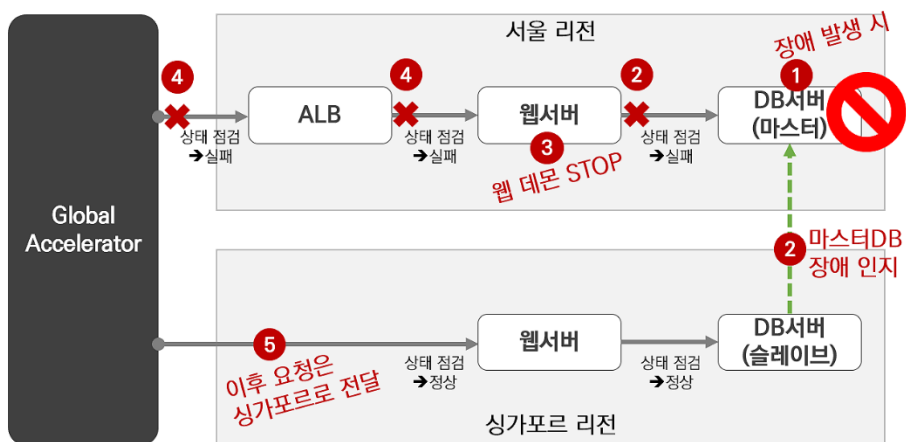
평상시에 각각의 연결 대상에 대해서 상태 점검(Health Check)을 하며, 문제가 발생 시 다른 대상을 연결하거나 혹은 에러를 반환합니다.

▶ [그림 1-1-4] 상태 점검(Health Check) 구간



### 1.1.5 장애 발생 시 동작

▶ [그림 1-1-5] 서울 리전 문제나 마스터 DB 장애 발생 시 동작



[그림 1-1-5]는 마스터 DB 문제가 발생하거나 서울 리전 자체의 문제가 발생 시 동작 절차입니다. 해당 웹 서비스의 경우 DB 서버에서 읽어오는 데이터가 중요하기 때문에 DB 서버와 연결에 문제가 발생하면 웹 서버의 웹 서비스 데몬을 중지하도록 설정하였습니다.

이후 웹 서버의 상태 점검을 하는 ALB와 Global Accelerator도 상태 점검에서 실패를 확인하면 싱가포르 리전으로 서비스를 넘기게 됩니다. 동작 과정의 상세 정보는 뒤에 실습에서 확인할 수 있습니다.

## 1.2 기본 환경 구성

이번 실습에서 대부분의 자원은 제공되는 CloudFormation 템플릿에 의해서 자동으로 구성됩니다.

### ☞ [참고 사항]

비용이 발생하는 서비스들이 있으니 실습을 진행하고 완료 시 바로 삭제하기를 바랍니다.

### IP 주소와 도메인 정보

AWS 서울 리전

IP	도메인	역할
10.1.3.100	websrv1.awsseoul.internal	웹서버
10.1.4.100	websrv2.awsseoul.internal	웹서버

서울 온프레미스

IP	도메인	역할
10.2.1.100	dbsrv.idcseoul.internal	DB서버(마스터)
10.2.1.200	dnssrv.idcseoul.internal	DNS서버

AWS 싱가포르 리전

IP	도메인	역할
10.3.3.100	websrv1.awssingapore.internal	웹서버

싱가포르 온프레미스

IP	도메인	역할
10.4.1.100	dbsrv.idcsingapore.internal	DB서버(슬레이브)
10.4.1.200	dnssrv.idcsingapore.internal	DNS서버

### 1.2.1 [서울] CloudFormation 적용

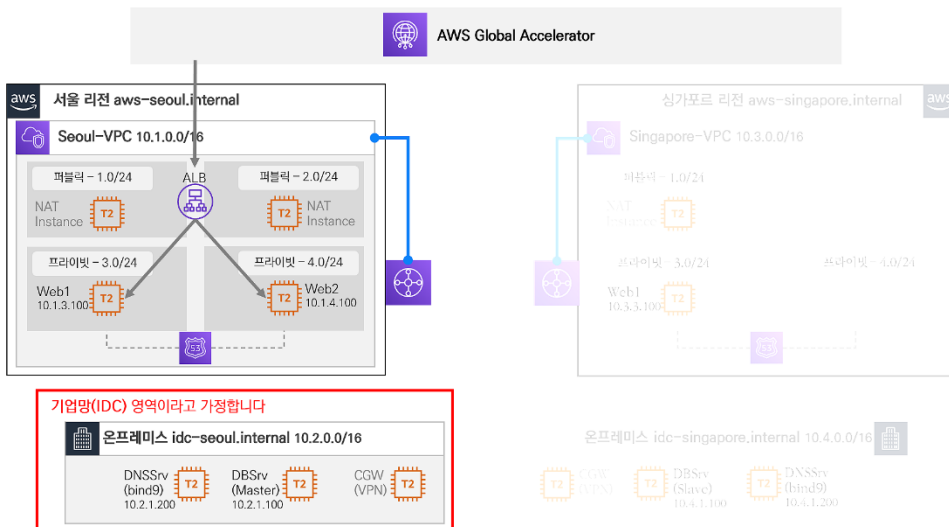
먼저 서울 리전에 CloudFormation 을 배포하고 이후에 싱가포르 리전에 배포합니다.

**[경로]** 서울 리전 선택 → 서비스 → CloudFormation → 스택 → 스택 생성

**[1]** 다운로드 링크: <http://bit.ly/cnbl08011>

CloudFormation 적용을 위해 상단의 링크를 통해 템플릿을 다운로드하고 스택을 생성하여 AWS 자원을 자동으로 생성합니다. CloudFormation 스택 생성 시 **'AWS CloudFormation 에서 사용자 지정 이름으로 IAM 리소스를 생성할 수 있음을 승인합니다.'** 체크를 하고 스택을 생성해야 합니다.

➤ **[그림 1-2-1]** 서울 리전 CloudFormation에 의해 배포되는 자원



대략 9 분 정도 후에 배포가 완료되며, 배포 후 출력 정보를 확인합니다. CloudFormation 스택의 출력 정보 중 Global Accelerator ARN <sup>Amazon Resource Names</sup> 정보는 싱가포르 리전 배포에 사용하게 됩니다.



➤ [그림 1-2-2] 서울 리전 CloudFormation 스택 생성 후 출력 정보 확인

Multi-Seoul

스택 정보 | 이벤트 | 리소스 | **출력** | 파라미터 | 템플릿 | 변경 세트

출력 (4)

출력 검색

키	값	설명
CGWVPC2Instance1	13.209.122.238	Public IP assigned to VPC2 Instance1 eth0 interface
GAListenerARN	arn:aws:globalaccelerator:--:accelerator/439fdc33-539c-403b-acb6-f7bac60ab309/listener/047f15cf	Global Accelerator Arn
MasterDBVPC2Instance2	3.34.191.233	Public IP assigned to VPC2 Instance2 eth0 interface
SeoulTransitGatewayID	tgw-04550aee67639c79d	Seoul TransitGateway ID

## 1.2.2 [싱가포르] CloudFormation 적용

싱가포르 리전에 CloudFormation 을 배포합니다.

[경로] 싱가포르 리전 선택 ➔ 서비스 ➔ CloudFormation ➔ 스택 ➔ 스택 생성

1 다운로드 링크: <http://bit.ly/cnbl08012>

스택 생성 시 파라미터에서 'GAListenARN'의 값은 [그림 1-2-2]에서 확인한 값을 입력합니다.

➤ [그림 1-2-3] 싱가포르 리전에서 스택 생성 시 파라미터 값 설정

1단계  
템플릿 지정

2단계  
스택 세부 정보 지정

3단계  
스택 옵션 구성

4단계  
검토

### 스택 세부 정보 지정

**스택 이름**

스택 이름  
Multi-Singa  
스택 이름은 문자(a-z 및 a-과 숫자(0-9) 및 대시(-))를 포함할 수 있습니다.

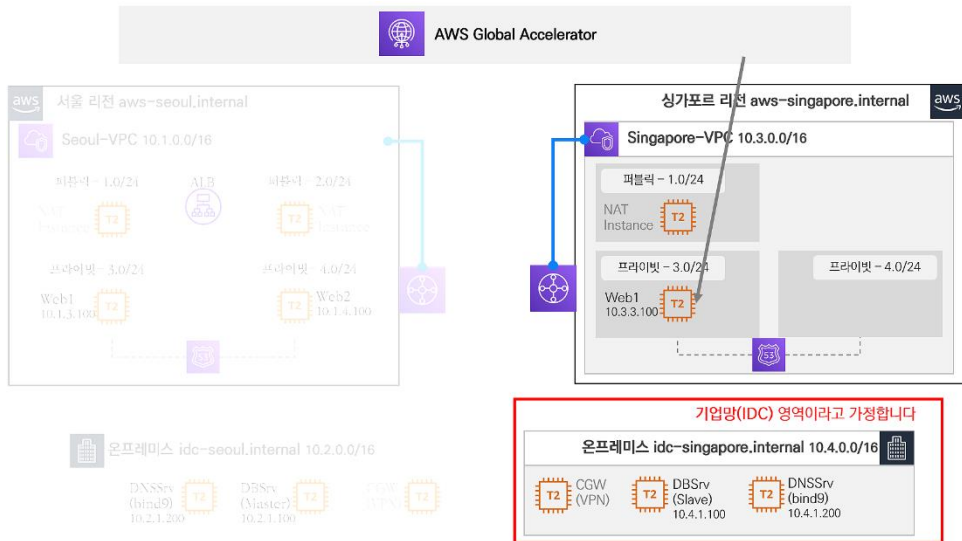
**파라미터**

파라미터는 템플릿에서 정의되며, 이를 통해 스택을 생성하거나 업데이트할 때 사용자 지정 값을 입력할 수 있습니다.

GAListenerARN  
GA Listener ARN Name  
arn:aws:globalaccelerator:--:accelerator/439fdc33-539c-403b-acb6-f7bac60ab309/listener/047f15cf

GAListenerARN 값  
입력

➤ [그림 1-2-4] 싱가포르 리전 CloudFormation에 의해 배포되는 자원



Global Accelerator 는 서울 리전 CloudFormation 배포 때 성성이 되었고, 싱가포르 리전에서는 타깃 대상으로 Web1 인스턴스가 자동으로 등록됩니다. 대략 9 분 정도 후에 배포가 완료됩니다.

🔍 [참고 사항]

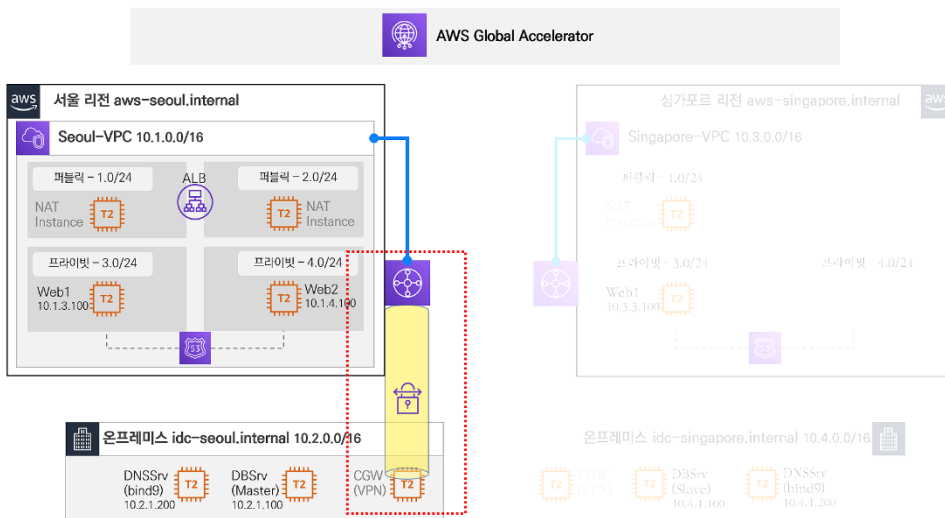
이번 실습에서 NAT 게이트웨이 대신 NAT 인스턴스를 배치한 이유는 비용 때문입니다. NAT 게이트웨이(서울 리전)는 시간당 \$0.059 비용과 NAT 게이트웨이를 통한 데이터 처리 요금이 1GB 당 \$0.059 비용이 필요합니다. 특히 인터넷에서 AWS로 향하는 트래픽은 무료인데 반해, NAT 게이트웨이를 사용 시 해당 비용도 유료의 데이터 처리 요금이 발생합니다. 예를 들면 EC2가 YUM으로 필요한 프로그램을 설치 시 인터넷에서 AWS쪽으로 설치 파일을 다운로드 시 데이터 처리 요금이 발생합니다. 하지만 NAT 인스턴스를 사용 시 프리 티어의 남은 용량으로 사용할 수 있기 때문에 추가 비용이 발생하지 않습니다.

## 1.3 전송 게이트웨이와 온프레미스의 VPN 설정

먼저 온프레미스에 IDC-CGW 인스턴스에 VPN 설정이 필요합니다. 참고로 AWS VPN 은 CloudFormation에 의해 미리 설정되어 있습니다.

### 1.3.1 [서울] VPN 설정

➤ [그림 1-3-1] 서울 리전 VPN 설정 도식화



[그림 1-3-1]과 같이 서울 리전의 전송 게이트웨이와 온프레미스 IDC-CGW 간에 VPN을 설정합니다. 먼저 사이트 간 VPN 연결의 Tunnel 1 외부 IP 주소 정보를 확인합니다.

**[경로]** 서울 리전 선택 ➔ 서비스 ➔ VPC ➔ VPN ➔ 사이트 간 VPN 연결 ➔ 생성된 VPN 연결 선택