aws re/start

Amazon VPC 연결 옵션

네트워킹

학습 내용

강의의 핵심

배울 내용은 다음과 같습니다.

- Virtual Private Cloud(VPC) 연결 옵션의 차이점 알아보기

주제:

- VPC 연결

주요 용어:

- Network address translation(NAT)
- NAT 게이트웨이
- NAT 인스턴스
- VPC 피어링

VPC 연결 시나리오 및 솔루션

전제 조건	추천 제품	솔루션 범주
인터넷에 프라이빗 서브넷 연결	• NAT 게이트웨이 • NAT 인스턴스	• Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 연결
다른 VPC에 VPC 연결	• VPC 피어링	• Amazon VPC 간 연결
외부 네트워크에 VPC 연결	• AWS 사이트 간 가상 프라이빗 네트워크(VPN) • AWS Direct Connect와 VPN • AWS VPN CloudHub	• Amazon VPC에 네트워크 연결 • VPN 연결
AWS 네트워크를 벗어나지 않고 VPC를 AWS 서비스에 연결	• AWS PrivateLink • VPC 게이트웨이 엔드포인트	• Amazon VPC 간 연결 • VPC 게이트웨이 엔드포인트
여러 VPC 및 외부 네트워크에 VPC 연결	• AWS Transit Gateway	• Amazon VPC에 네트워크 연결 • Amazon VPC 간 연결

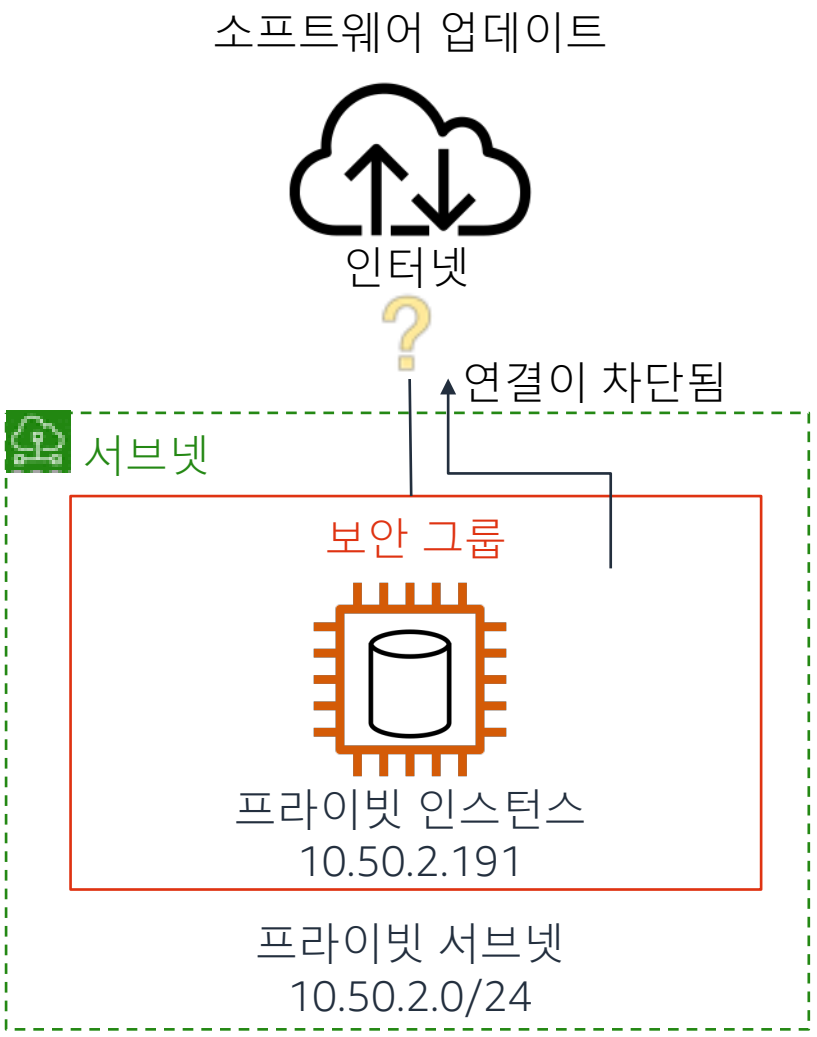
Network address translation(NAT)

당면 과제:

프라이빗 서브넷의 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 인터넷에 연결해야 합니다.

솔루션:

- ✓ NAT 게이트웨이
- ✓ NAT 인스턴스

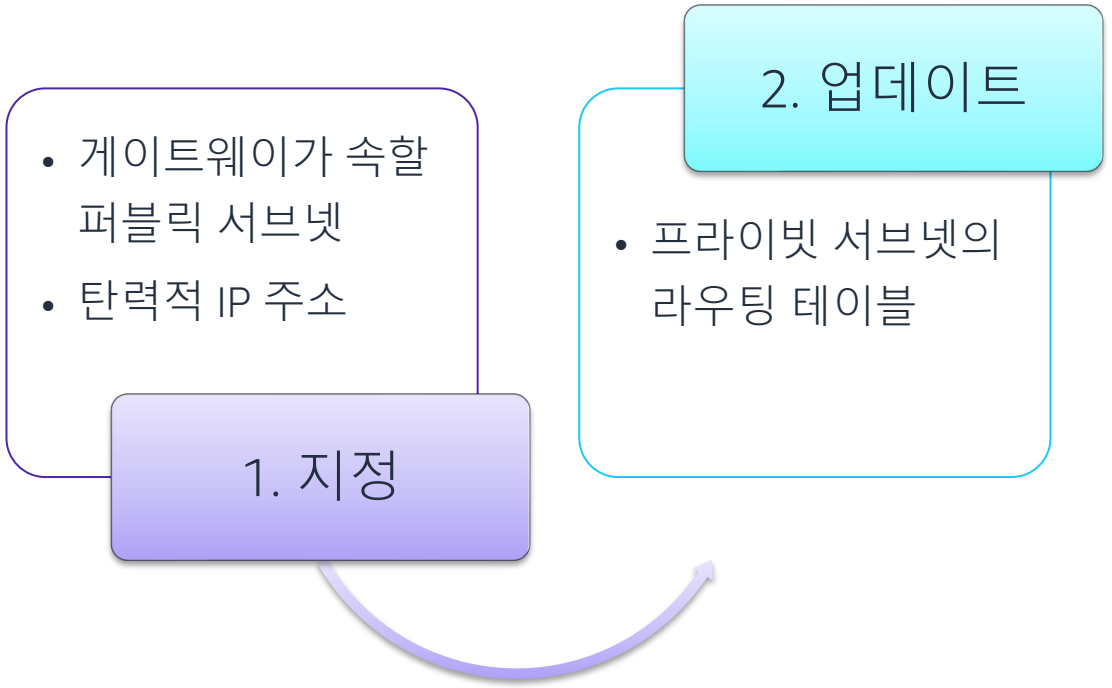


aws re/start

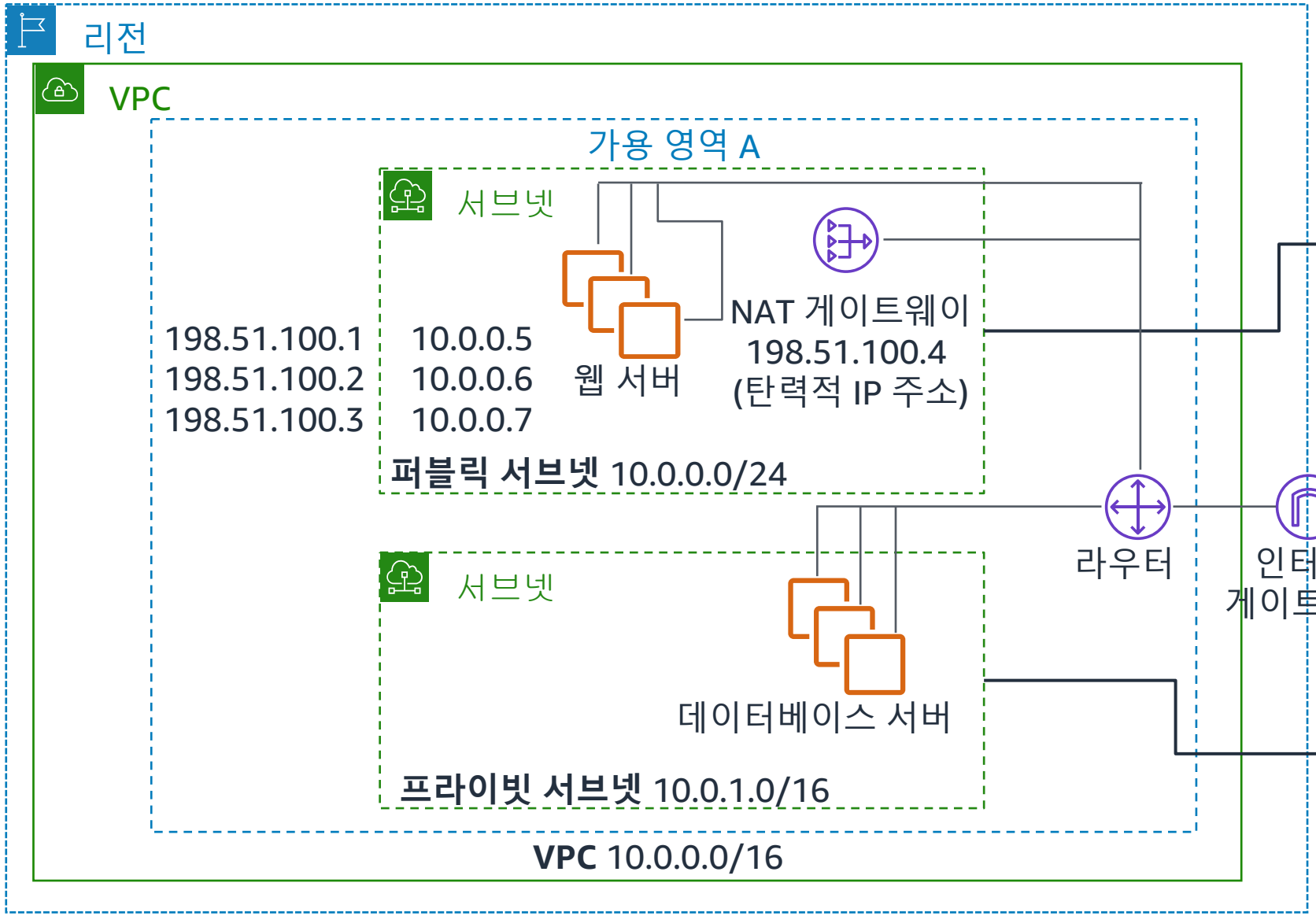
NAT 게이트웨이 특성 및 생성 단계

NAT 게이트웨이 특성

- AWS 관리형 서비스
- 가용 영역 내 기본 제공 이중화
- 탄력적 IP 주소 필요
- 프로토콜 지원:
  - Transmission Control Protocol(TCP)
  - User Datagram Protocol(UDP)
  - Internet Control Message Protocol(ICMP)



NAT 게이트웨이가 있는 VPC의 아키텍처



사용자 지정 라우팅 테이블

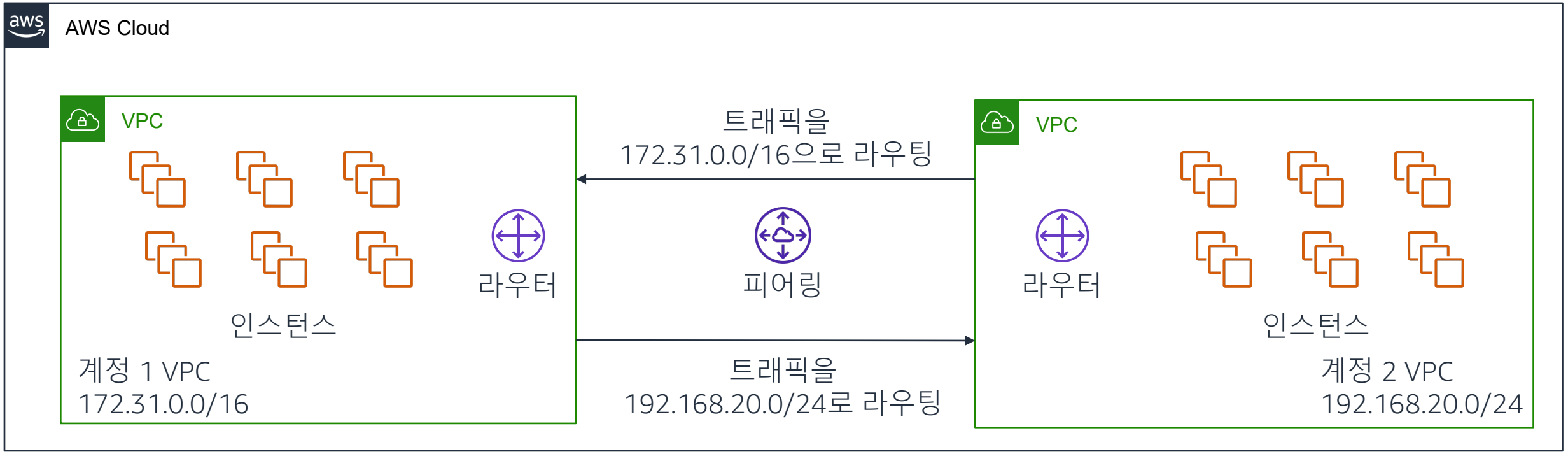
목적지	대상
10.0.0.0/16	로컬
0.0.0.0/0	internet-gateway-id

기본 라우팅 테이블

목적지	대상
10.0.0.0/16	로컬
0.0.0.0/0	NAT-gateway-id

aws re/start

Amazon VPC 피어링



프라이빗 라우팅 테이블

목적지	대상
171.31.0.0/16	로컬
192.168.20.0/24	NAT-gateway-id

프라이빗 라우팅 테이블

목적지	대상
192.168.20.0/24	로컬
172.31.0.0/16	PCX-XXXXXXX

aws re/start

VPC 피어링 연결 생성

VPC 피어링 연결을 생성하려면 다음을 수행합니다.

1. 요청자 VPC의 소유자가 VPC 연결 요청을 보냅니다.
2. 수락자 VPC의 소유자가 VPC 연결 요청을 수락합니다.
3. 두 소유자 모두가 두 참여 VPC에 라우팅 테이블 항목을 추가합니다.
4. 필요한 경우 소유자는 두 참여 VPC에서 보안 그룹 규칙을 조정합니다.
5. 필요한 경우 소유자는 VPC 연결에 대해 도메인 이름 시스템(DNS) 호스트 이름 확인을 활성화합니다.

VPC 피어링 연결을 위한 AWS CLI 명령

명령

```
aws ec2 create-vpc-peering-connection --vpc-id vpc-1a2b3c4d --peer-vpc-id vpc-11122233
```

예제: VPC 피어링을 위한 AWS CloudFormation

JavaScript Object Notation(JSON)의 AWS CloudFormation 스크립트 항목

```
{
"Type": "AWS::EC2::VPCPeeringConnection",
"Properties": {
  "PeerVpcId": "vpc-1a2b3c4d",
  "VpcId": "vpc-11122233",
  "PeerOwnerId": "444455556666",
  "PeerRegion": "us-east-1",
  "PeerRoleArn": "arn:aws:ec2:us-east-
1:444455556666"
   }
}
```

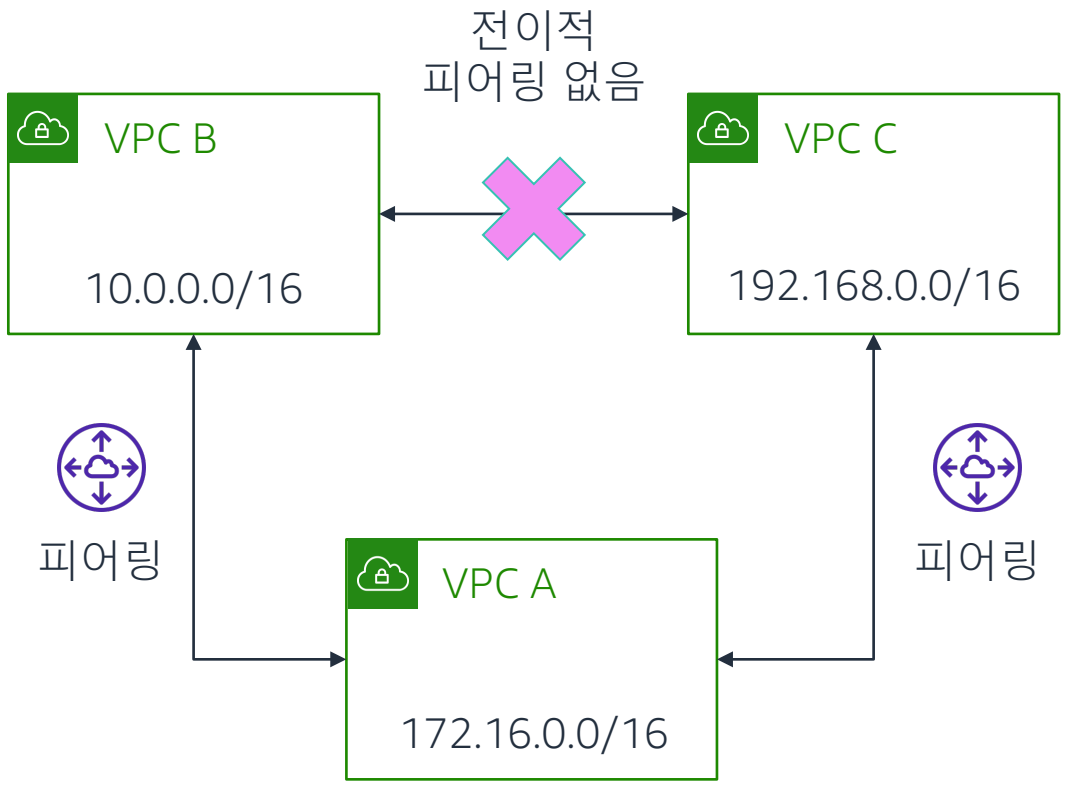
YAML Ain't Markup Language(YAML)의 AWS CloudFormation 스크립트 항목

```
Type: AWS::EC2::VPCPeeringConnection
Properties:
   PeerVpcId: vpc-1a2b3c4d
   VpcId: vpc-11122233
   PeerOwnerId: 444455556666
   PeerRegion: us-east-1
   PeerRoleArn: arn:aws:ec2:us-east-
1:444455556666
```

VPC 피어링 제한

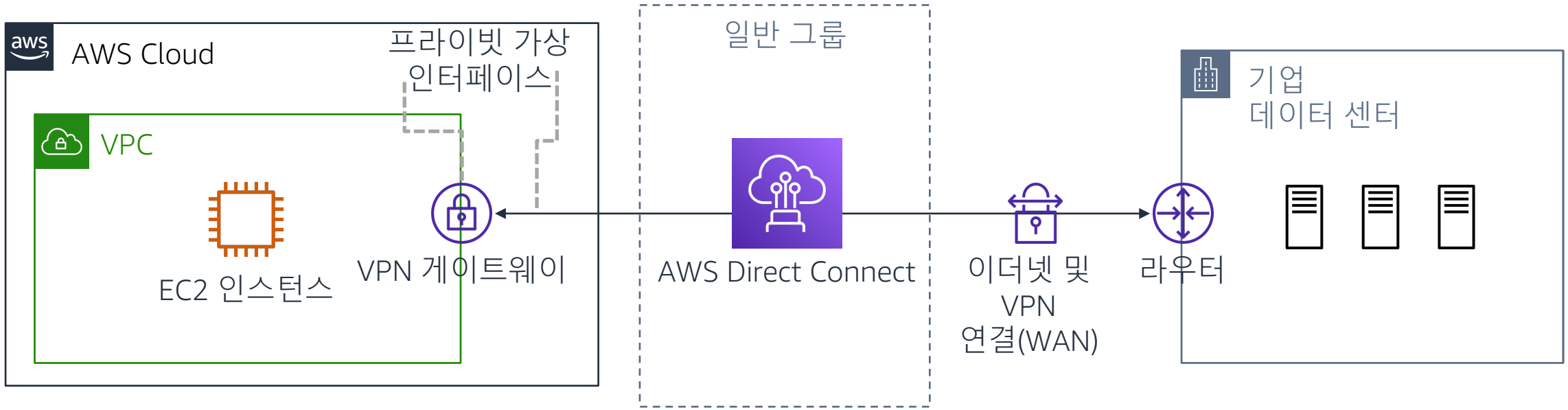
VPC 피어링 제한에는 다음이 포함됩니다.

- IP 주소 범위가 겹치지 않아야 합니다.
- 전이적 피어링, 엣지 라우팅 또는 인터넷 게이트웨이 액세스가 없습니다.
- VPC 간 NAT 라우팅이 없습니다.
- 사설 IP 주소의 DNS 조회 확인이 없습니다.
- 리전 전반에 걸쳐 상호 참조 보안 그룹을 지원합니다
.



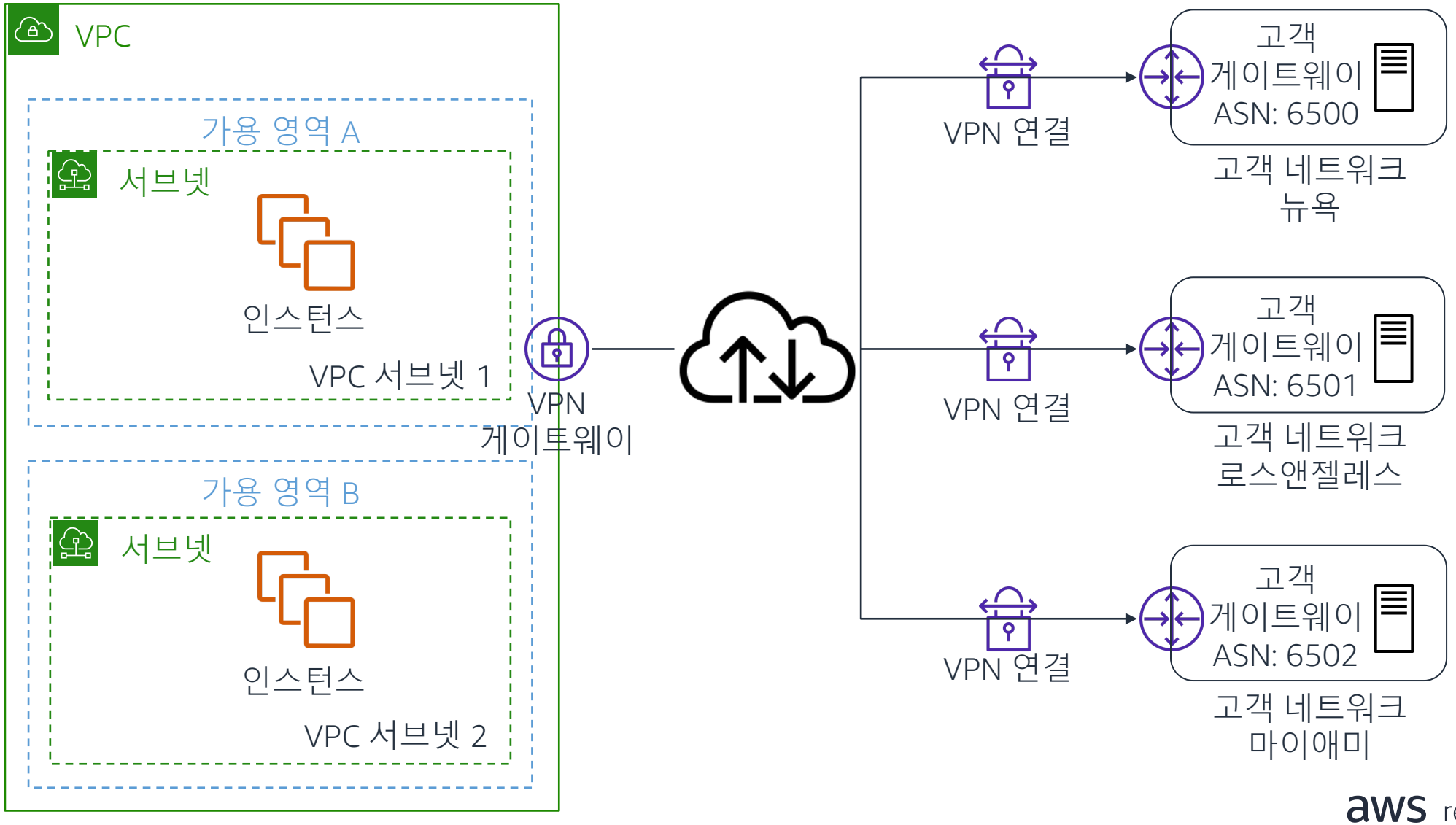
aws re/start

AWS Direct Connect와 VPN



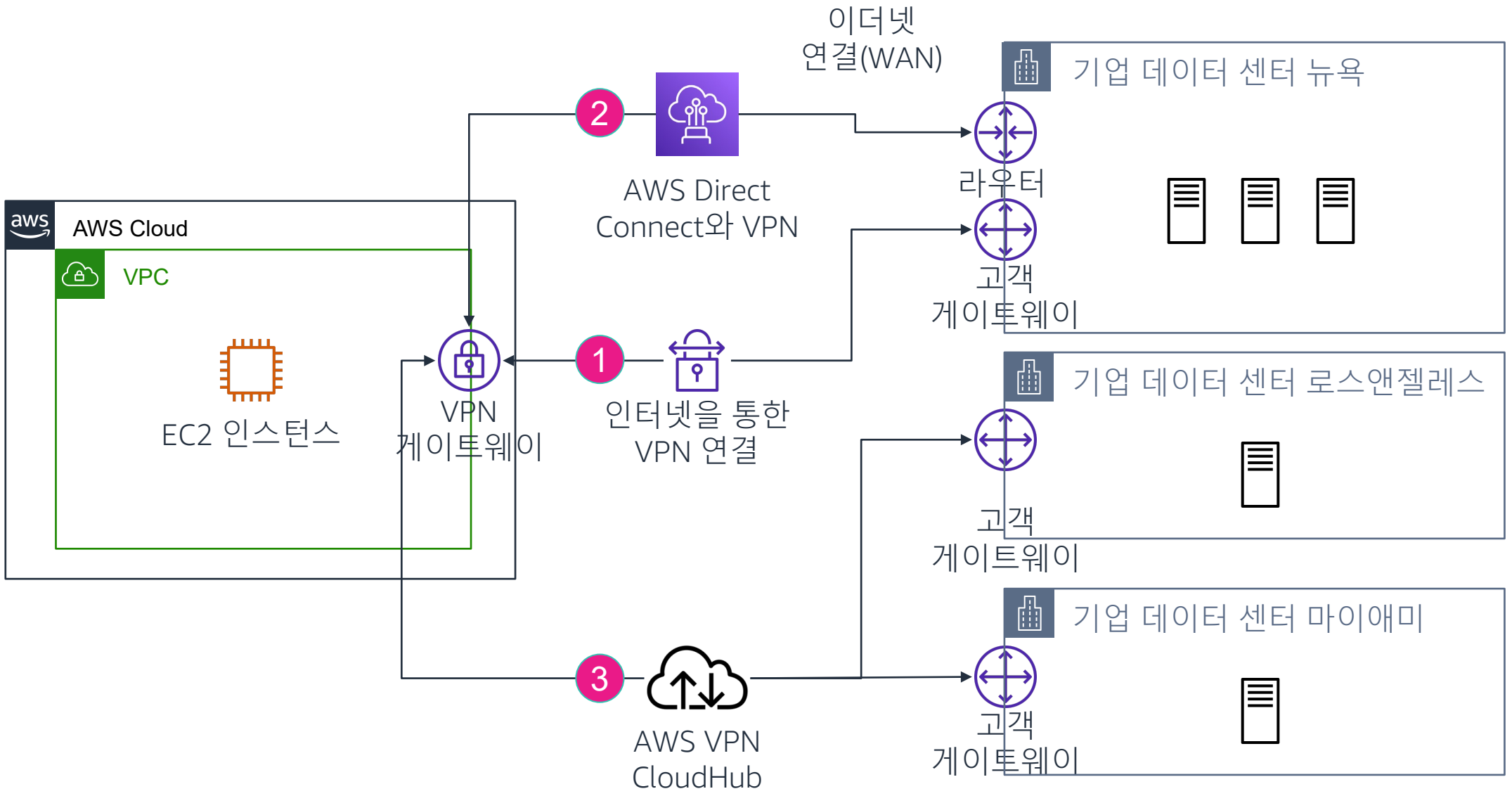
aws re/start

AWS VPN CloudHub



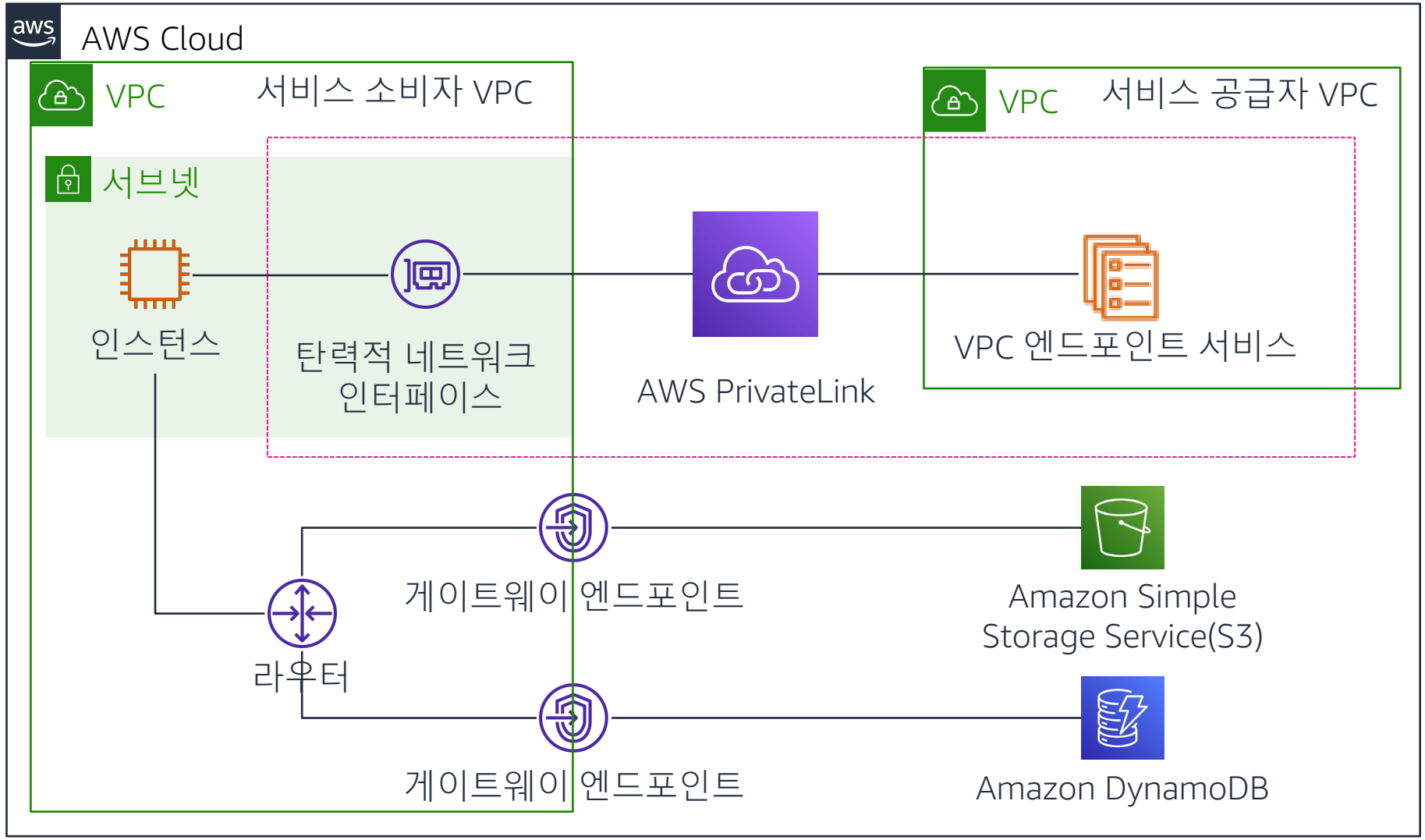
aws re/start

VPN 연결 옵션

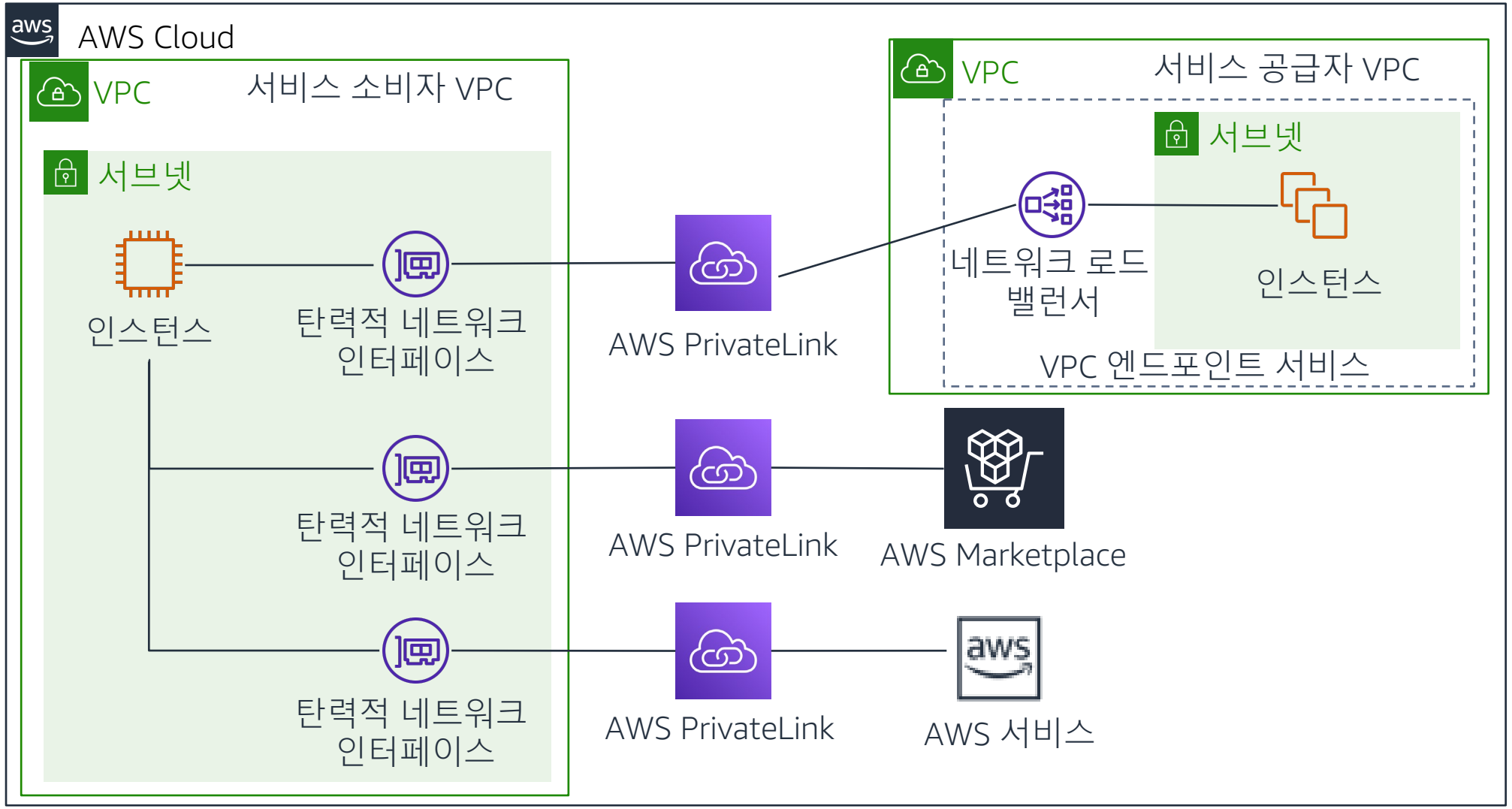


aws re/start

VPC 엔드포인트



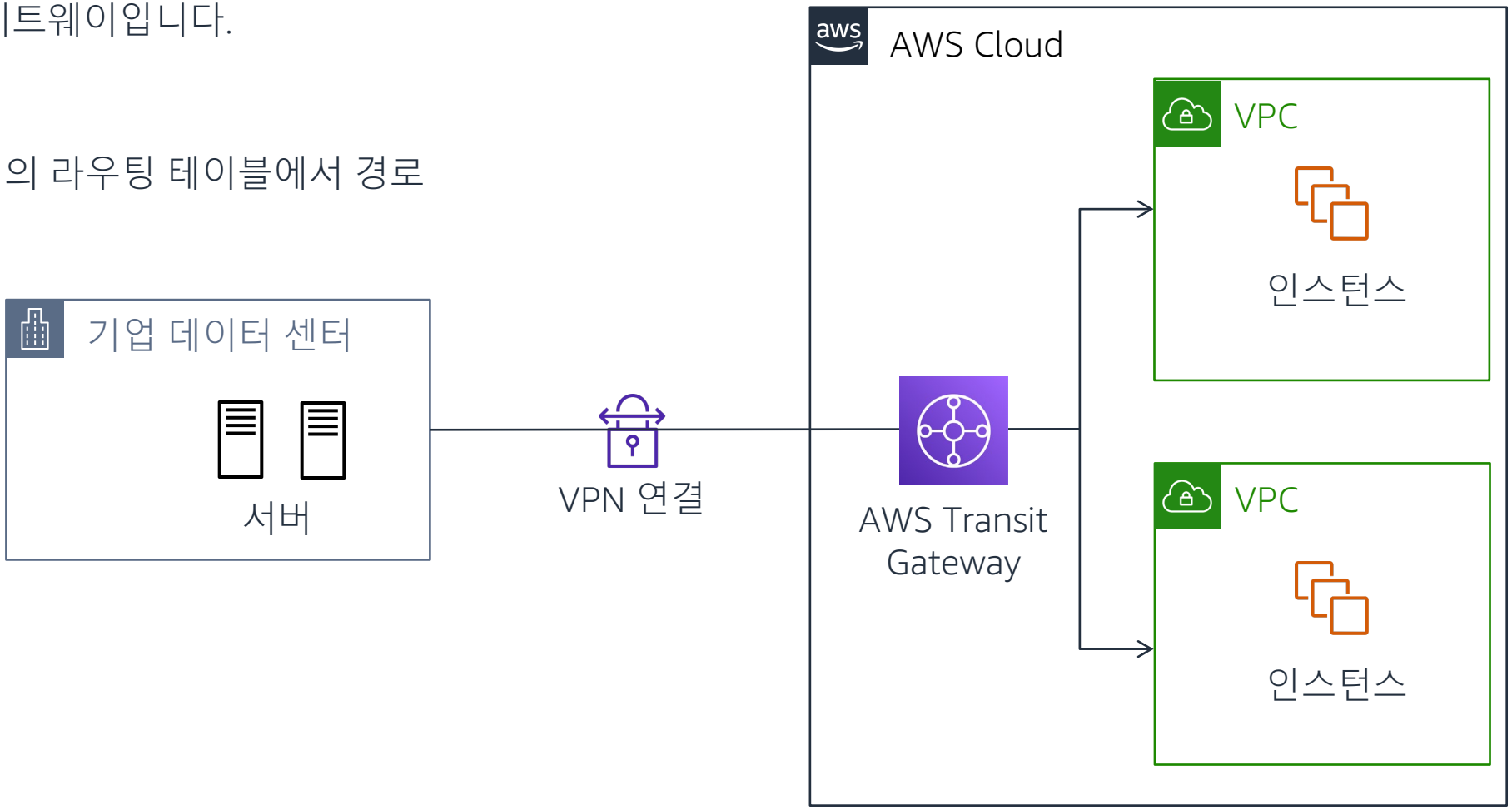
AWS PrivateLink 인터페이스 엔드포인트



AWS Transit Gateway

AWS Transit Gateway는 수천 개의 VPC와 온프레미스 네트워크를 연결하는 단일 게이트웨이입니다.

- VPC 및 VPN에 연결
- 연결된 VPC 및 VPN 연결의 라우팅 테이블에서 경로 전파 지원



aws re/start

핵심 사항

- AWS는 VPC를 다른 VPC, 외부 엔드포인트 및 AWS 서비스에 연결하기 위한 다양한 옵션을 제공합니다.
- NAT 디바이스는 프라이빗 서브넷의 인스턴스에서 인터넷 또는 기타 AWS 서비스로 트래픽을 전달한 다음 인스턴스에 응답을 다시 보냅니다.
- 다음과 같은 다양한 연결 옵션이 있습니다.
  - 클라우드 피어링
  - AWS Direct Connect와 VPN
  - AWS VPN CloudHub

aws re/start