



# AWS Cloud 네트워킹 및 Amazon Virtual Private Cloud

네트워킹

# 학습 내용

## 강의의 핵심

배울 내용은 다음과 같습니다.

- AWS Cloud 네트워킹에서의 Amazon Virtual Private Cloud(Amazon VPC)의 기초적인 역할 설명하기
- VPC 내부의 네트워킹 구성 요소와 그 용도 식별하기

주제:

네트워킹 및 Amazon Virtual Private Cloud(Amazon VPC)

주요 용어:

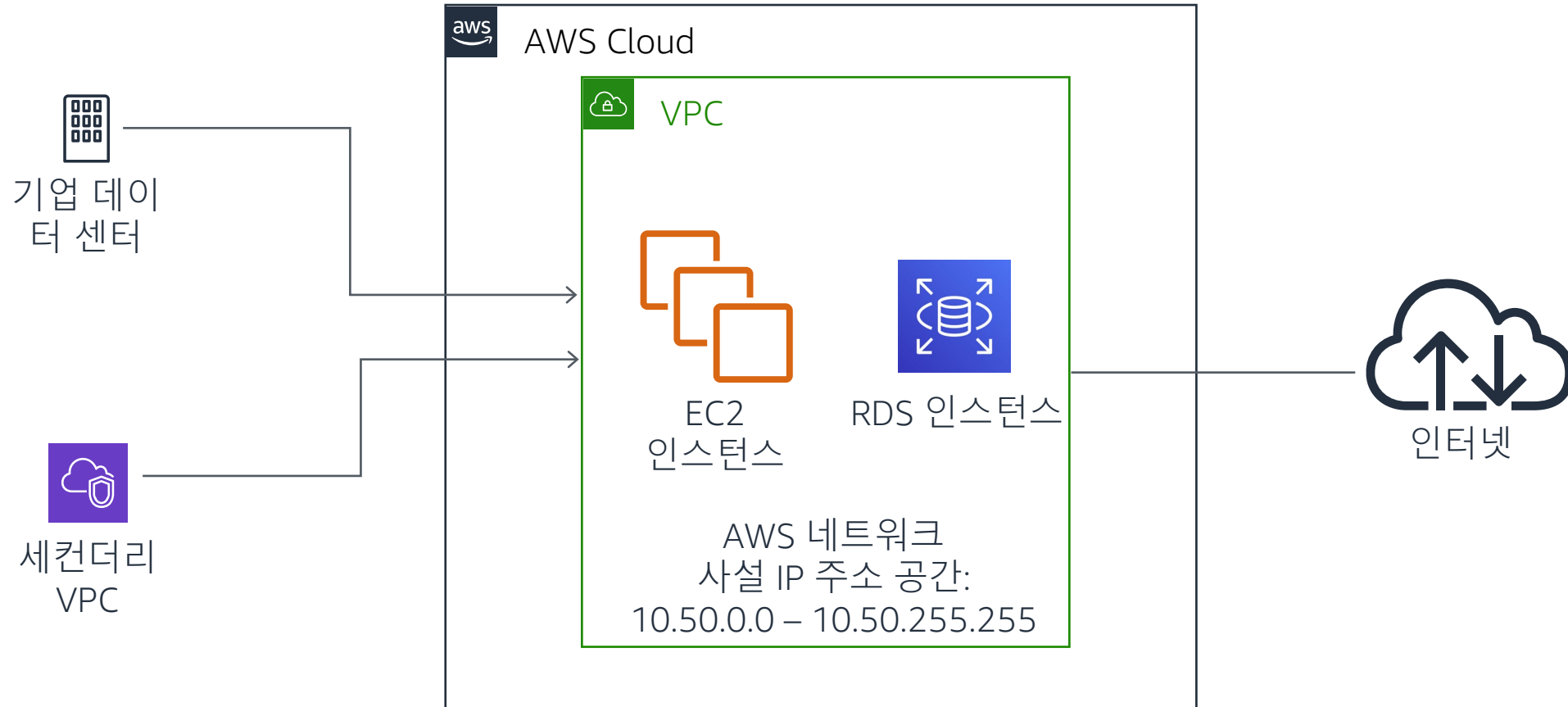
- AWS Cloud 네트워킹
- VPC
- 서브넷
- 보안 그룹
- 기본 네트워크 인터페이스
- 인터넷 게이트웨이
- 가상 프라이빗 게이트웨이(VGW)
- 고객 게이트웨이
- Classless Inter-Domain Routing(CIDR)

프로젝트:

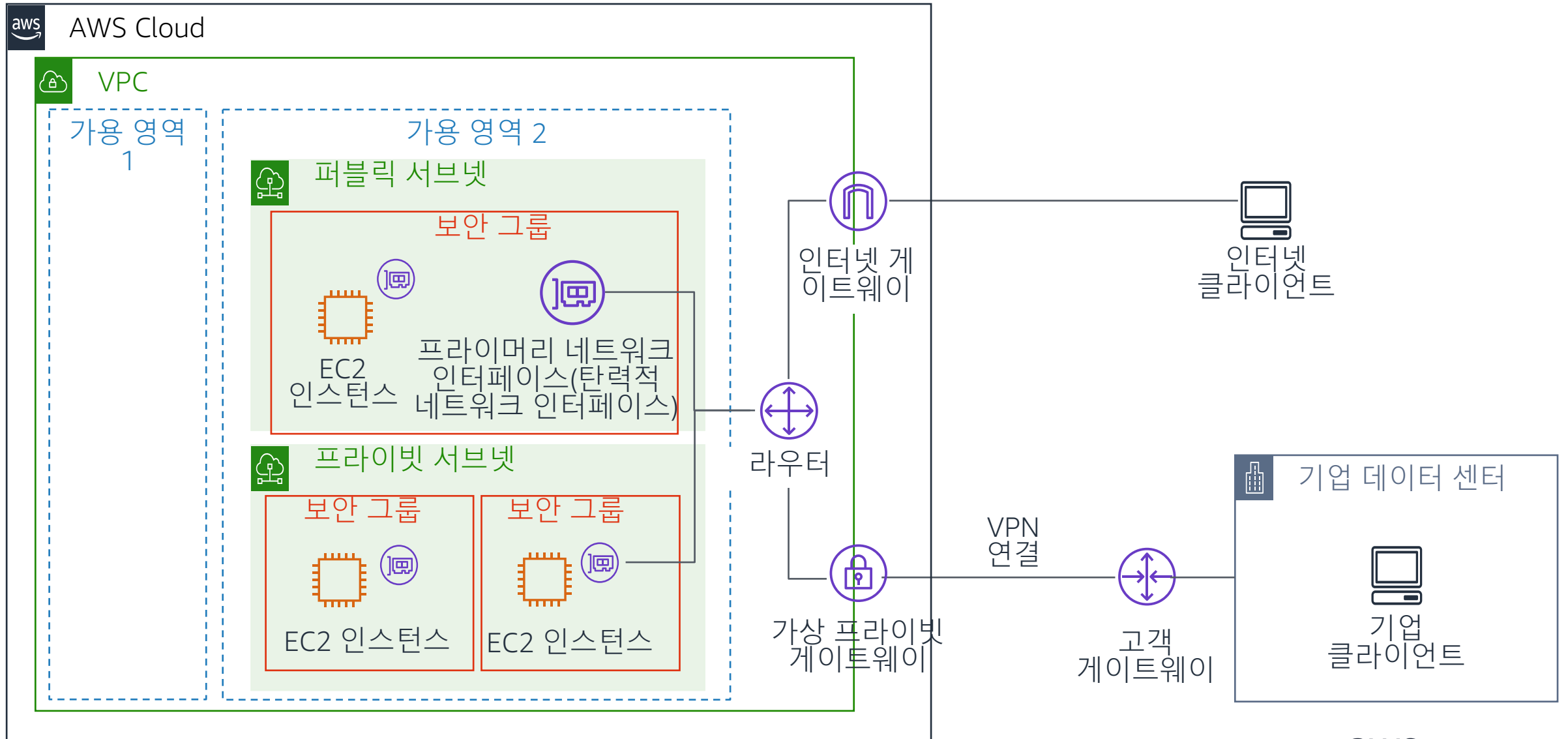
문제 해결 기술 자료



# AWS Cloud 네트워킹



# AWS 네트워킹 구성 요소



# Amazon VPC 및 VPC

VPC는 AWS Cloud의 논리적으로 격리된 섹션에서 프로비저닝되는 가상 네트워크입니다.

- 서브넷으로 논리적 분리 지원
- 세부적으로 강화된 보안 제공
- 선택적 하드웨어 가상 프라이빗 네트워크 (VPN) 지원



Amazon VPC

# Amazon VPC 구성: IP 주소 지정

## IP 주소 지정:

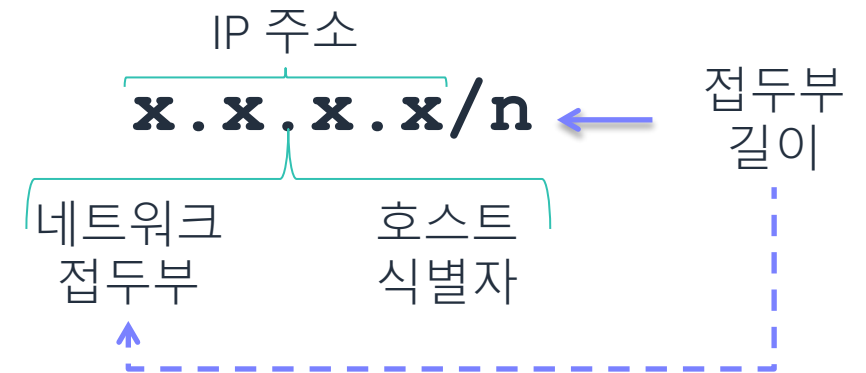
- 유효한 사설 IP 주소 범위는 RFC(Request for Comment) 1918에 따라 정의됩니다.
- VPC에서는 /16과 /28 사이의 네트워크만 정의할 수 있습니다.

### 모범 사례

겹치지 않는 IP 주소 범위를 사용합니다.  
VPC를 RFC1918에 정의된 범위로 제한하여 라우팅 문제를 방지합니다.

# Classless Inter-Domain Routing(CIDR) 표기법

CIDR 블록:	비트 표현:	해당 주소 범위:
10.50.1.0/24	00001010.00110010.00 000001.xxxxxxxxx	10.50.1.0 – 10.50.1.255
10.50.1.0/27	00001010.00110010.00 000001.000xxxxx	10.50.1.0 – 10.50.1.31
10.50.1.132/32	00001010.00110010.00 000001.10000100	10.50.1.132 (단일 주소)
0.0.0.0/0	xxxxxxxx.xxxxxxxxx.xxxxxx xx.xxxxxxxxx	0.0.0.0 – 255.255.255.255 (모든 주소)



# VPC를 생성하는 AWS CLI 명령 예제

## 명령

```
$ aws ec2 create-vpc --cidr-block 10.0.0.0/16
```

Create VPC | VPC Management

https://console.aws.amazon.com/vpc/home

aws Services Resource Groups N. Virginia Support

VPCs > Create VPC

### Create VPC

A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances. You must specify an IPv4 address range for your VPC. Specify the IPv4 address range as a Classless Inter-Domain Routing (CIDR) block; for example, 10.0.0.0/16. You cannot specify an IPv4 CIDR block larger than /16. You can optionally associate an Amazon-provided IPv6 CIDR block with the VPC.

Name tag MomPopCafeVPC ⓘ

IPv4 CIDR block\* 10.0.0.0/24 ⓘ

IPv6 CIDR block ☒ No IPv6 CIDR Block ⓘ  
☐ Amazon provided IPv6 CIDR block

Tenancy Default ⓘ

\* Required

Cancel Create

Feedback English (US) © 2008 - 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use



# Amazon VPC 예약된 IP 주소

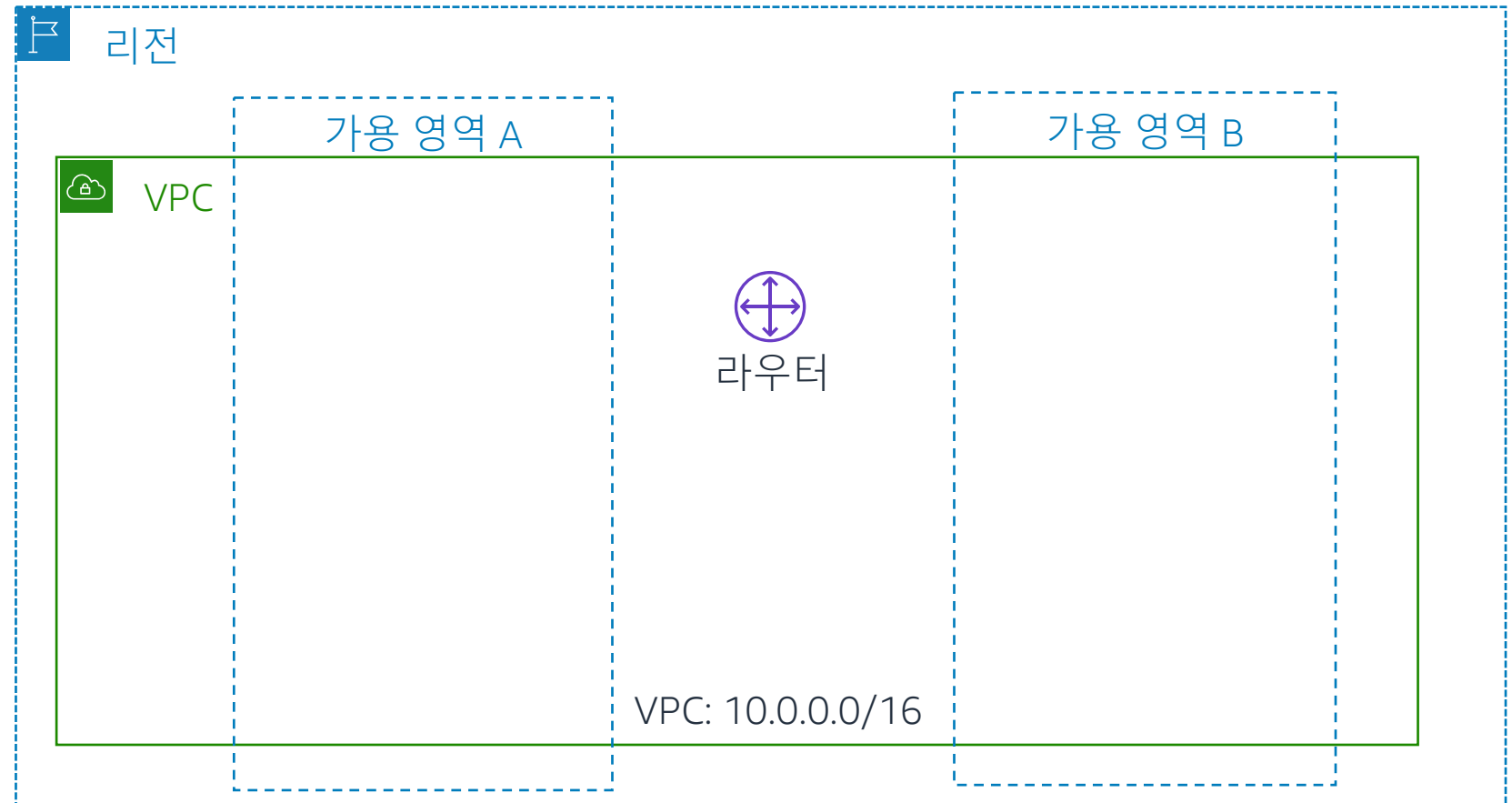
CIDR 블록	근거
10.0.0.0	네트워크 주소입니다.
10.0.0.1	AWS에서 VPC 라우터 주소용으로 예약해 둔 주소입니다.
10.0.0.2	Domain Name Server(DNS) 서버의 IP 주소는 항상 VPC 네트워크 범위의 기본 IP 주소에 2를 더한 값입니다. 그러나 VPC는 각 서브넷 범위에 2를 더한 기본값도 예약합니다.
10.0.0.3	AWS에서 차후 사용을 위해 예약해 둔 주소입니다.
10.0.0.255	네트워크 브로드캐스트 주소입니다. AWS는 VPC에서 브로드캐스트를 지원하지 않으므로 이 주소는 예약되어 있습니다.

# Amazon VPC

## 특성

기본 라우팅 테이블

목적지	대상
10.0.0.0/16	로컬

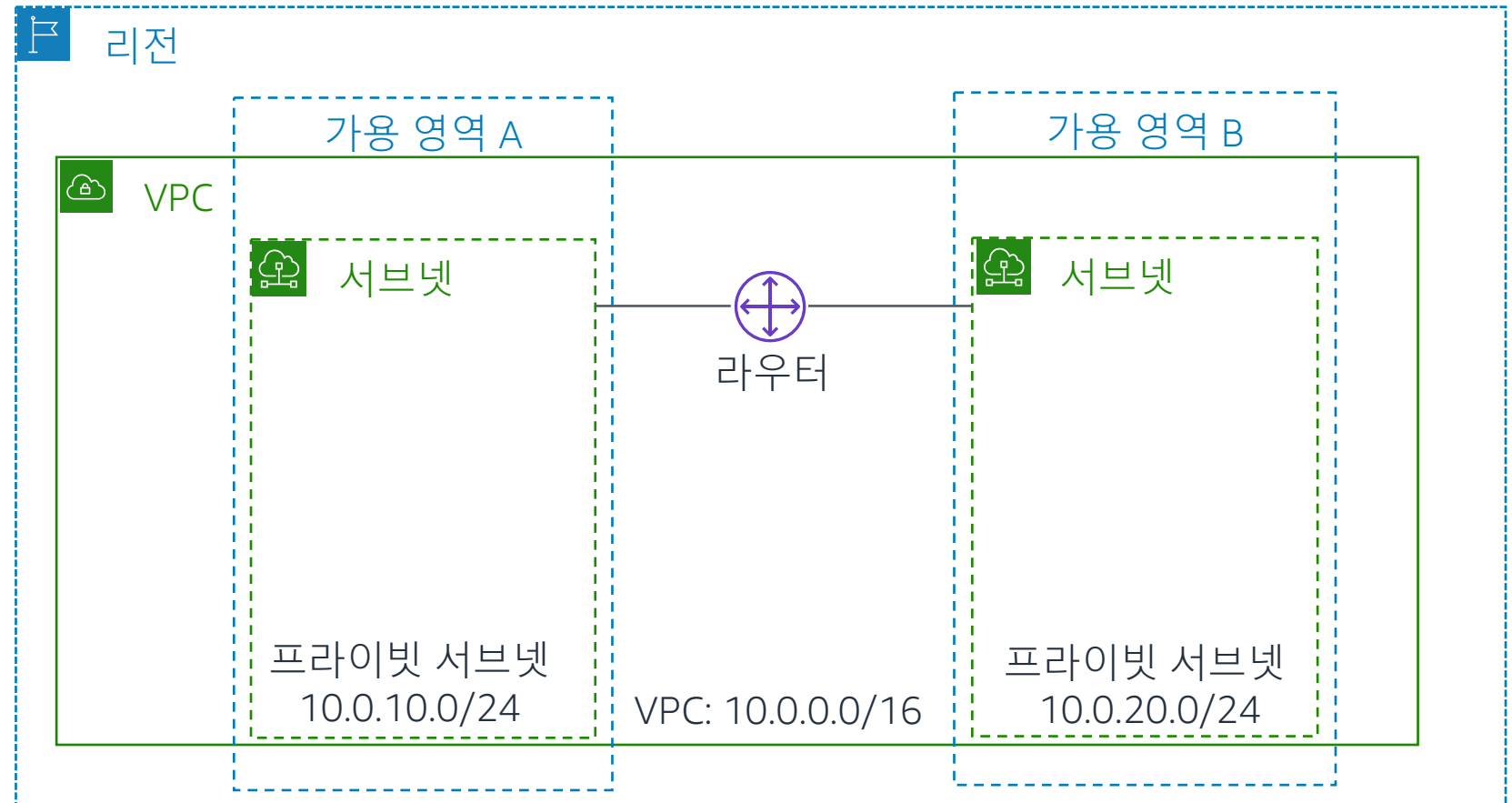


# Amazon VPC 구성 요소

## 서브넷

기본 라우팅 테이블

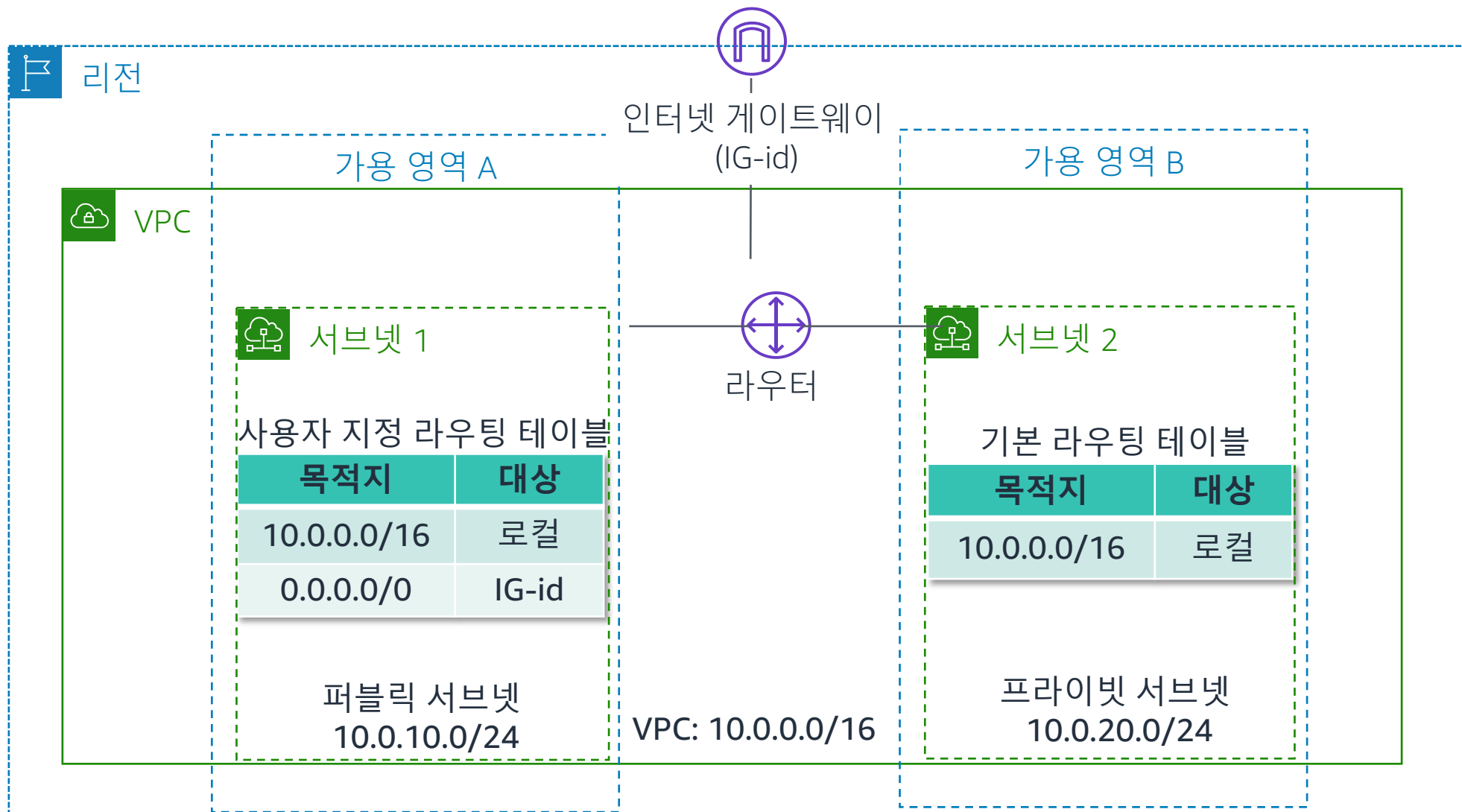
목적지	대상
10.0.0.0/16	로컬



# 공인 IP 서브넷 자동 할당 기능

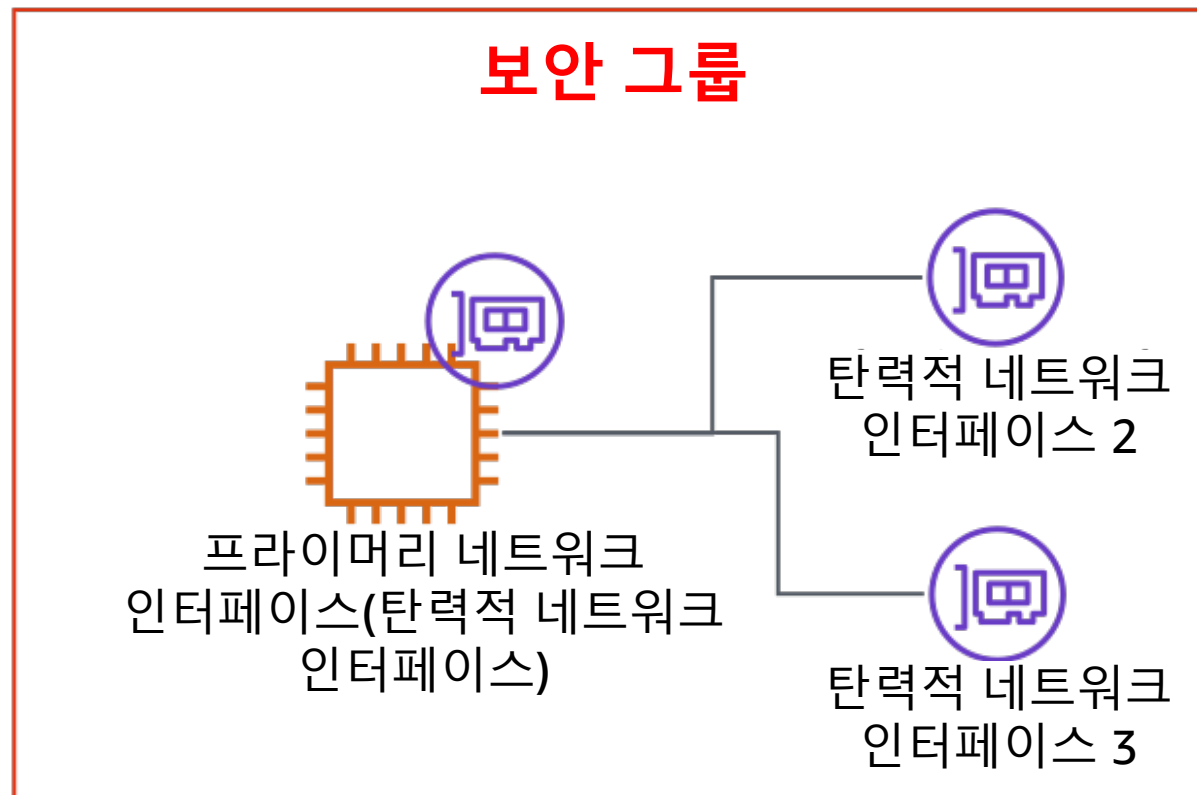
- 기본 Amazon VPC에서 시작된 인스턴스만 생성 중 공인 IP 주소를 받습니다.
- 사용자 지정 VPC에서 생성된 인스턴스가 공인 IP 주소를 받으려면 기본 설정을 재정의해야 합니다.
- 또는 서브넷에서 **자동 할당 IP 수정** 설정을 구성하여 공인 IP 주소를 인스턴스에 자동으로 할당합니다.
- 탄력적 IP 주소와 달리 공인 IP 주소는 고정되지 않습니다.

# Amazon VPC 구성 요소: 라우팅 테이블



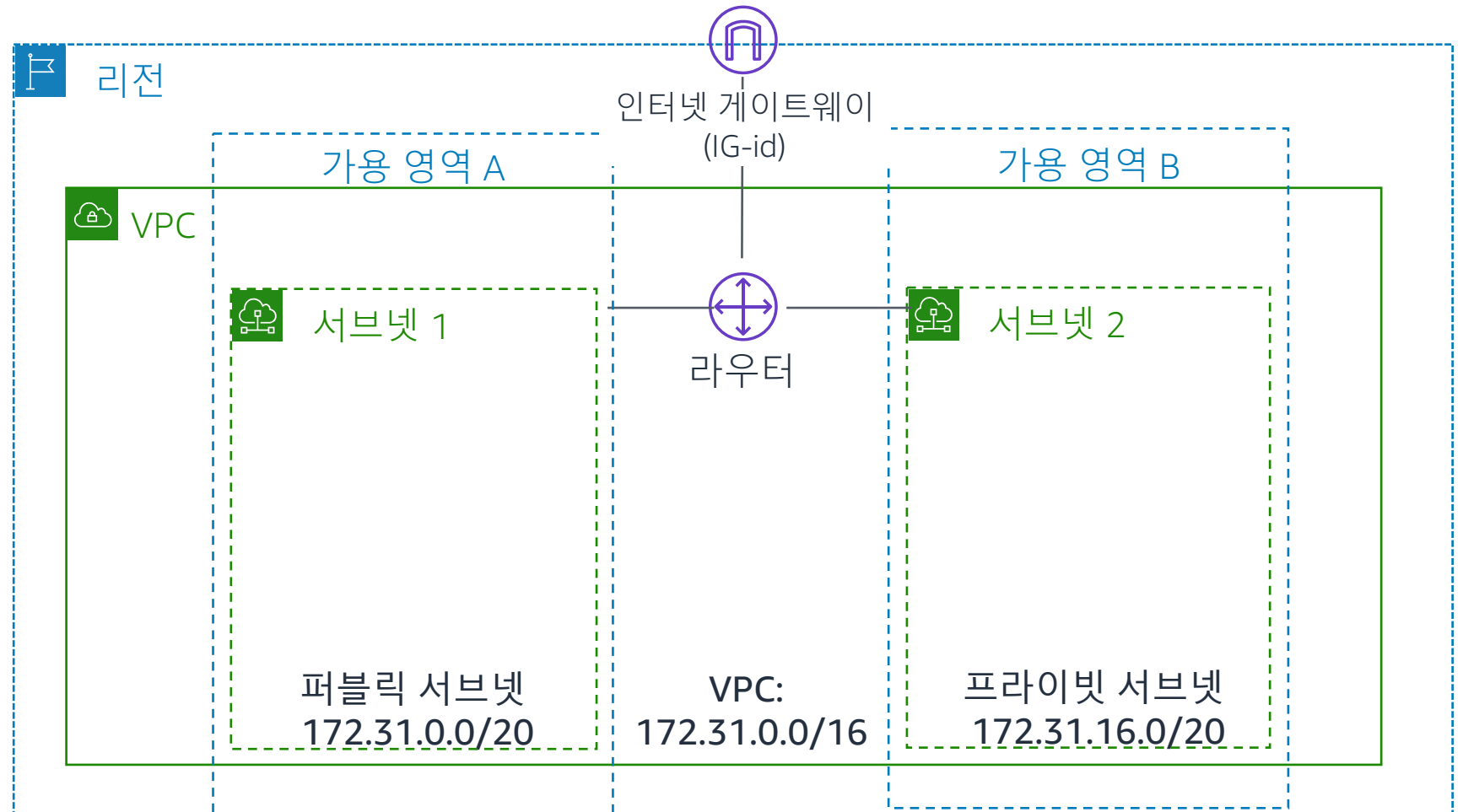
# Amazon VPC 구성 요소: 탄력적 네트워크 인터페이스

탄력적 네트워크 인터페이스는 EC2 인스턴스에 연결된 가상 네트워크 인터페이스(NIC)입니다.



# 기본 VPC

목적지	대상
172.31.0.0/16	로컬
0.0.0.0/0	IG-id



# VPC용 DNS 옵션

VPC용 도메인 이름 시스템(DNS) 옵션에는 다음이 포함됩니다.

Amazon에서 제공하는 DNS 서버(Amazon Route 53 Resolver)

자체 DNS 서버

Amazon Route 53 프라이빗 호스팅 영역



# 핵심 사항



- **Amazon VPC를 사용하여 Virtual Private Cloud(VPC)를** 프로비저닝합니다.
  - AWS 리소스 실행을 위해 논리적으로 격리된 AWS Cloud 섹션
  - 사용자가 정의하고 제어하는 가상 네트워크
  - 고유한 IP 주소 범위 선택, 서브넷 생성, 라우팅 테이블 및 네트워크 게이트웨이 구성
- VPC는 한 리전에서 사용 가능한 모든 가용 영역(AZ)에 걸쳐 있으며 AZ에서 여러 서브넷을 생성할 수 있습니다.
- 라우팅 테이블은 네트워크 트래픽이 VPC 안팎으로 전달되는 방식을 제어합니다.
- 탄력적 네트워크 인터페이스는 가상화된 네트워크 어댑터입니다.
  - EC2 인스턴스를 포함한 다양한 유형의 인스턴스에 할당 가능
  - 해당 IP 주소를 유지하고 재부팅 후에도 지속됨