

[스토리보드] 클라우드 보안 구축

07회차 : 계정보안 : VPC1

내용전문가	최민	교수설계(한기대)	한기대
협력업체	위지런	교수설계(협력업체)	김은혜

업무	작성자	버전	작성일	특이사항
SB 작성	위지런	V1.0	2023. 10.18	1차안 작성

과정명	클라우드 보안 구축	회차명	계정보안 : VPC1	화면번호	07_01
<div>▶ Intro</div> <div>• 학습열기</div> <div>• 학습목표</div> <div>▶ 본학습</div> <div>• VPC 개념 및 구성요소</div> <div>• VPC에서 다루는 기본 개념</div> <div>▶ 정리하기</div> <div>• 문제풀기</div> <div>• Outro</div>		Simple Storage Service(S3)보안2		학습목표	
		<div><div><div>STEP</div></div></div>			
		<div><div><div>#1</div><div>학습 목표</div></div><div><div>• VPC 개념과 주요 구성요소를 설명할 수 있다.</div><div>• VPC에서 다루는 CIDR, Subnet, Peering, Router, NAT, IG, Endpoint 등 개념을 설명할 수 있다.</div></div></div>			
		<div><div><div>#2</div><div>학습 내용</div></div><div><div>• VPC 개념 및 구성요소</div><div>• VPC에서 다루는 기본 개념</div></div></div>			
				화면설명	학습목표는 성우 음성 진행
				이미지 번호	
내레이션		성우: #1 #2이번 학습을 통해 여러분은 VPC 개념과 주요 구성요소, 그리고, VPC에서 다루는 CIDR, Subnet, Peering, Router, NAT, IG, Endpoint 등 개념을 설명할 수 있습니다.			

VPC란??

(Virtual Private Cloud)

VPC

논리적으로 격리된 가상의 네트워크 공간을 제공하는 서비스

VPC 내부 공간과 VPC 외부 공간이 논리적으로 완벽히 분리됨

VPC 내부 객체가 VPC 외부와 통신하려면 IGW(Internet Gateway) 또는 VPG(Virtual Private Gateway) 등이 필요

효과

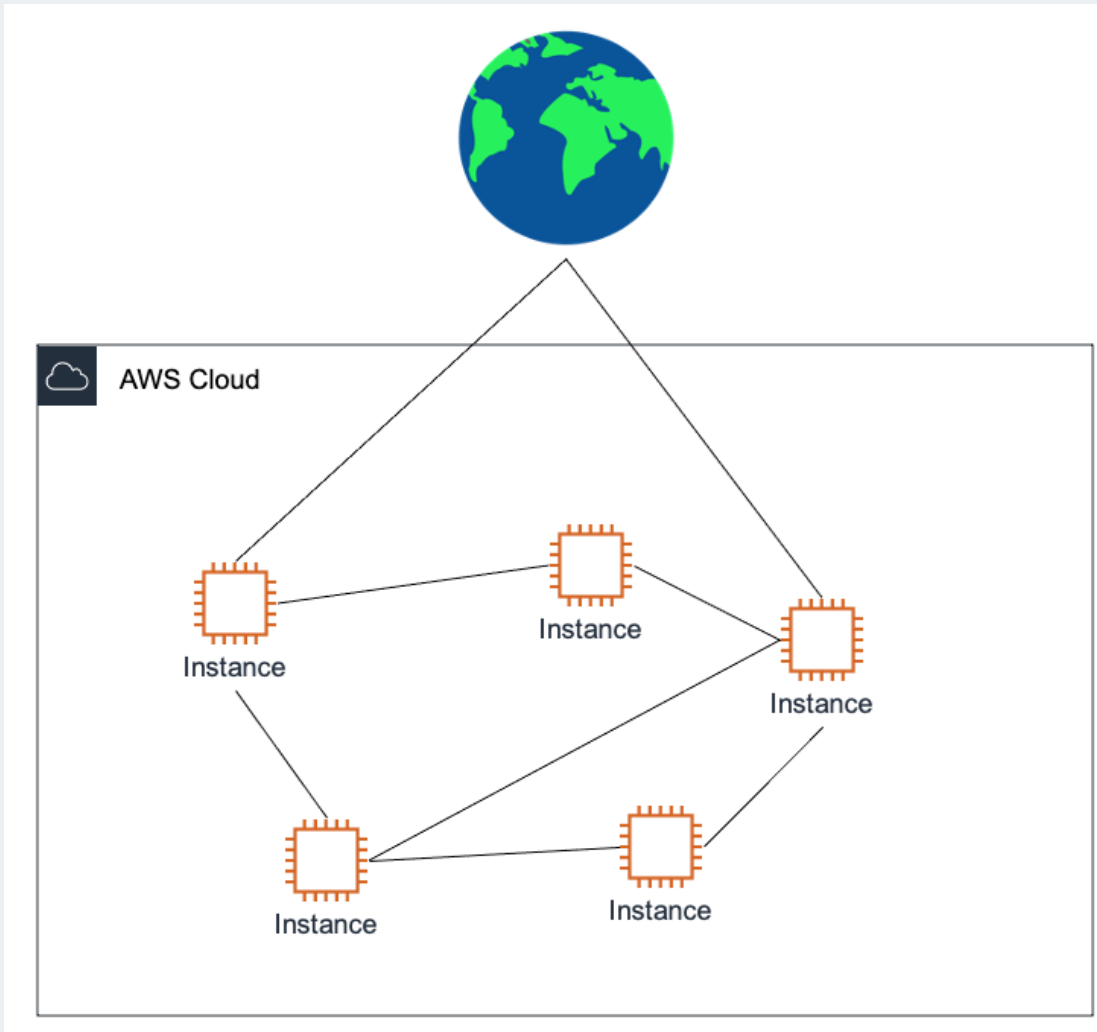
자신의 AWS 계정 내에 사설 IP주소를 기반으로 한
논리적인 네트워크 공간 구성 가능

- VPC 만들어 사설 IP주소 대역을 정의하면, 통신 가능

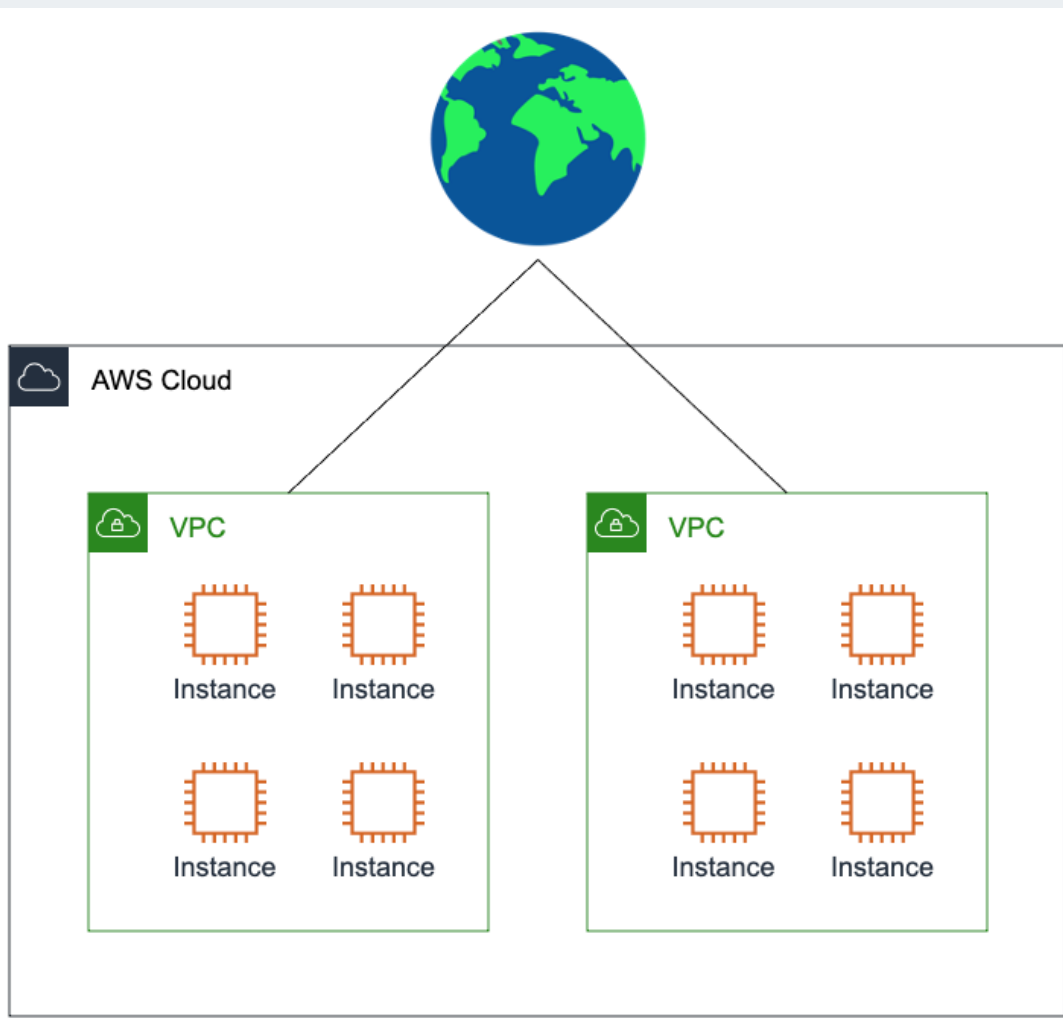
[예] || 10.0.0.0/16, VPC 내부적으로는 사설
IP주소만으로도 통신 가능

해당 논리적 공간과 외부(인터넷/On Premise) 연동도 가능하며,
이 과정에서 방화벽같은 접근제어 정책을 설정할 수도 있음

VPC 사용하지 않는 경우



VPC 사용하는 경우



VPC를 적용하면 인스턴스가 VPC에 속함으로써 네트워크를 구분할 수 있고 VPC 별로 필요한 설정을 통해 인스턴스에 네트워크 설정을 적용

현재까지 명확히 VPC를 설정하지 않고 인스턴스 생성을 했다면 AWS에서 제공하는 default VPC에 인스턴스가 배치된 것

* AWS 클라우드의 경우 VPC의 중요성을 강조하여 2019년부터 모든 서비스에 VPC를 적용하고 있음

프로비저닝

정의한 가상 네트워크에서 AWS 리소스를 실행할 수 있는 AWS 클라우드의 논리적으로 격리된 영역

다음에 포함된 가상 네트워킹 리소스를 제어할 수 있음

IP 주소 범위
선택

서브넷 생성

라우팅
테이블 및
네트워크
게이트웨이
구성

VPC에 대한 네트워크 구성을 손쉽게 사용자 지정할 수 있음

다단계 보안을 사용할 수 있도록 지원

VPC

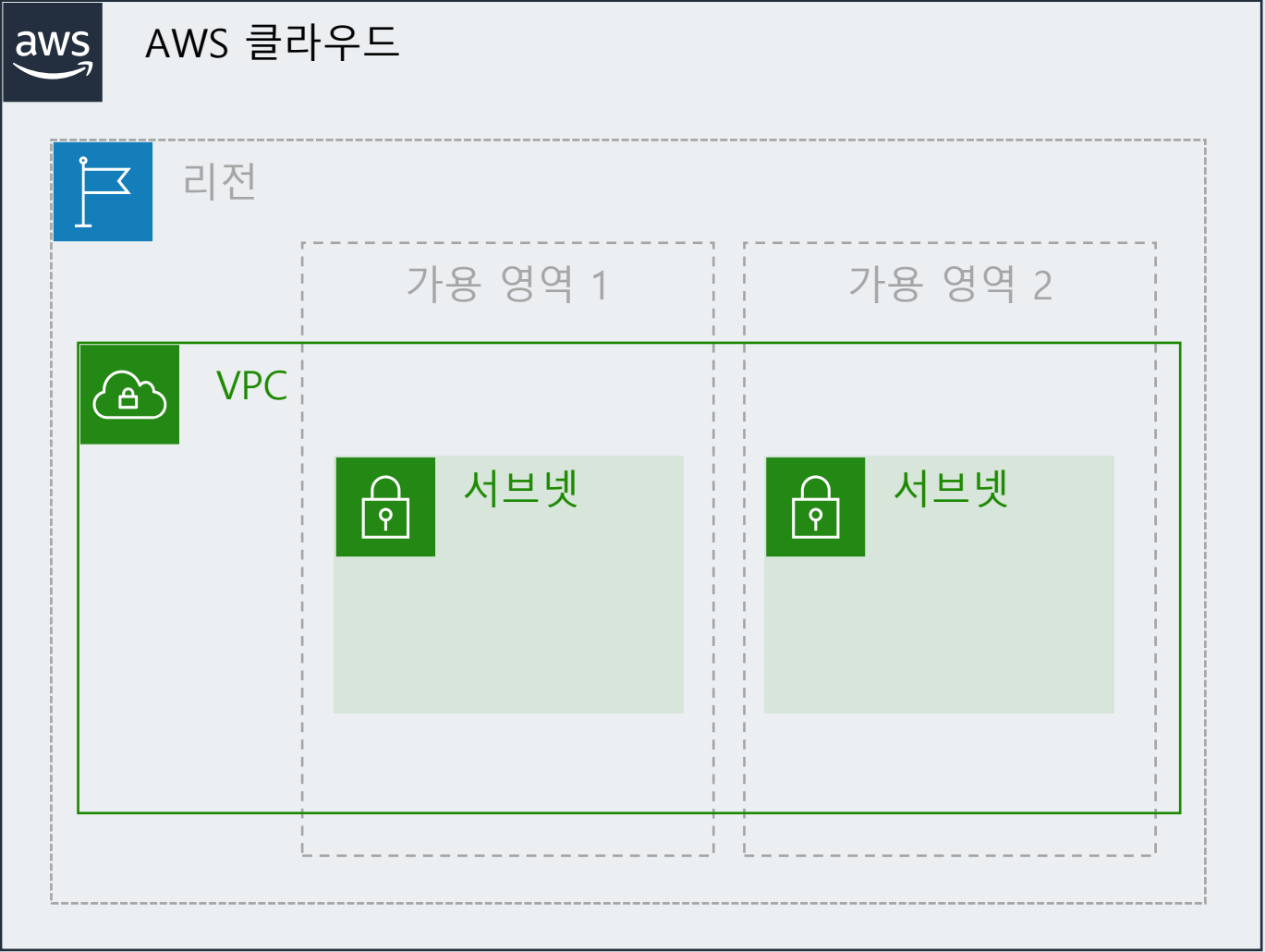
서브넷

- ✓ 다른 VPC와 논리적으로 격리됨
- ✓ 사용자의 AWS 계정 전용
- ✓ 단일 AWS 리전에 속하며 여러 가용 영역에 걸쳐 구현될 수 있음

VPC

서브넷

- ✓ VPC를 분할하는 IP 주소의 범위
- ✓ 단일 가용 영역에 속함
- ✓ 퍼블릭 또는 프라이빗으로 분류



► Intro

- 학습열기
- 학습목표

▶ **본학습**

- VPC 개념 및 구성요소
- VPC에서 다루는 기본 개념

▶ 정리하기

- 문제풀기
- Outro

VPC에서 다루는 기본 개념

- CIDR
- Subnet
- Peering
- Router
- IG
- NAT
- Endpoint

화면설명

이미지 번호

IPv4(32비트)
주소

192.0.2.0

IPv6(128비트)
주소

2600:1f18:22ba:8c00:ba86:a05e:a5ba:00FF

192

0

2

0



11000000

00000000

00000010

00000000

네트워크 식별자(라우팅 접두사)

192 . 0 . 2

11000000

고정

00000000

고정

00000010

고정

호스트 식별자

. 0 / 24

00000000
~ 11111111

유연함

고정된
비트 수를
알려줌

10진수

10.0.0.0/16

2진수

00001010.00000000.00000000.00000000

앞의 16비트는 Network ID, 뒤의 16비트는 Host ID

10.0.0.0/16으로 정의한 네트워크 주소 영역은
Network ID가 00001010.00000000으로 동일하고 Host별로
뒤의 16비트가 상이한 집합

VPC

독립된 하나의 네트워크를 구성하기 위한 가장 큰 단위

각 Region에 종속되며 사설 IP 대역(RFC1918)에 맞추어 설계



VPC에서 사용하는 사설 IP 대역

- 10.0.0.0 ~ 10.255.255.255(10/8 prefix)
- 172.16.0.0 ~ 172.31.255.255(182.16/12 prefix)
- 192.168.0.0 ~ 192.168.255.255(192.168/16 prefix)

VPC

VPC에서 IP 대역을 한번 설정하면 수정할 수 없음

각각의 VPC는 독립적이기 때문에 서로 통신할 수 없음

- 만일 통신을 원한다면 VPC 피어링 서비스 등으로 VPC 간에 트래픽을 라우팅할 수 있도록 설정 필요

각 대역폭마다 고정되어있는 Prefix가 다름

VPC

IPv4 주소 xxx.xxx.xxx.xxx

xxx

0~255 사이의 숫자이며
이는 8bits로 표현

10.0.0.0/16으로 설정된 IP 대역폭은
총 65,536개의 프라이빗 IPv4 주소

서브넷

VPC의 IP 주소를 나누어 리소스가 배치되는
물리적인 주소 범위

Public subnet

인터넷과 연결되어 있는
서브넷

Private subnet

인터넷과 연결되어 있지 않은
서브넷



인터넷 연결 여부로 Subnet을 구분하는 이유

- 보안을 강화하기 위한 목적

Public subnet

Public subnet에 존재하는
인스턴스는 인터넷에 연결되어
아웃바운드, 인바운드 트래픽을
주고받을 수 있음

Private subnet

외부에 노출이 되어 있지 않기
때문에 접근할 수 없음
(인터넷과 연결되어 외부에
노출되어 있는 면적을
최소화함으로써 네트워크 망에
함부로 접근 제한)

VPC가 제공하는 망연계·서비스

**VPC
Peering**

**NAT
Gateway**

**VPC
Endpoint**

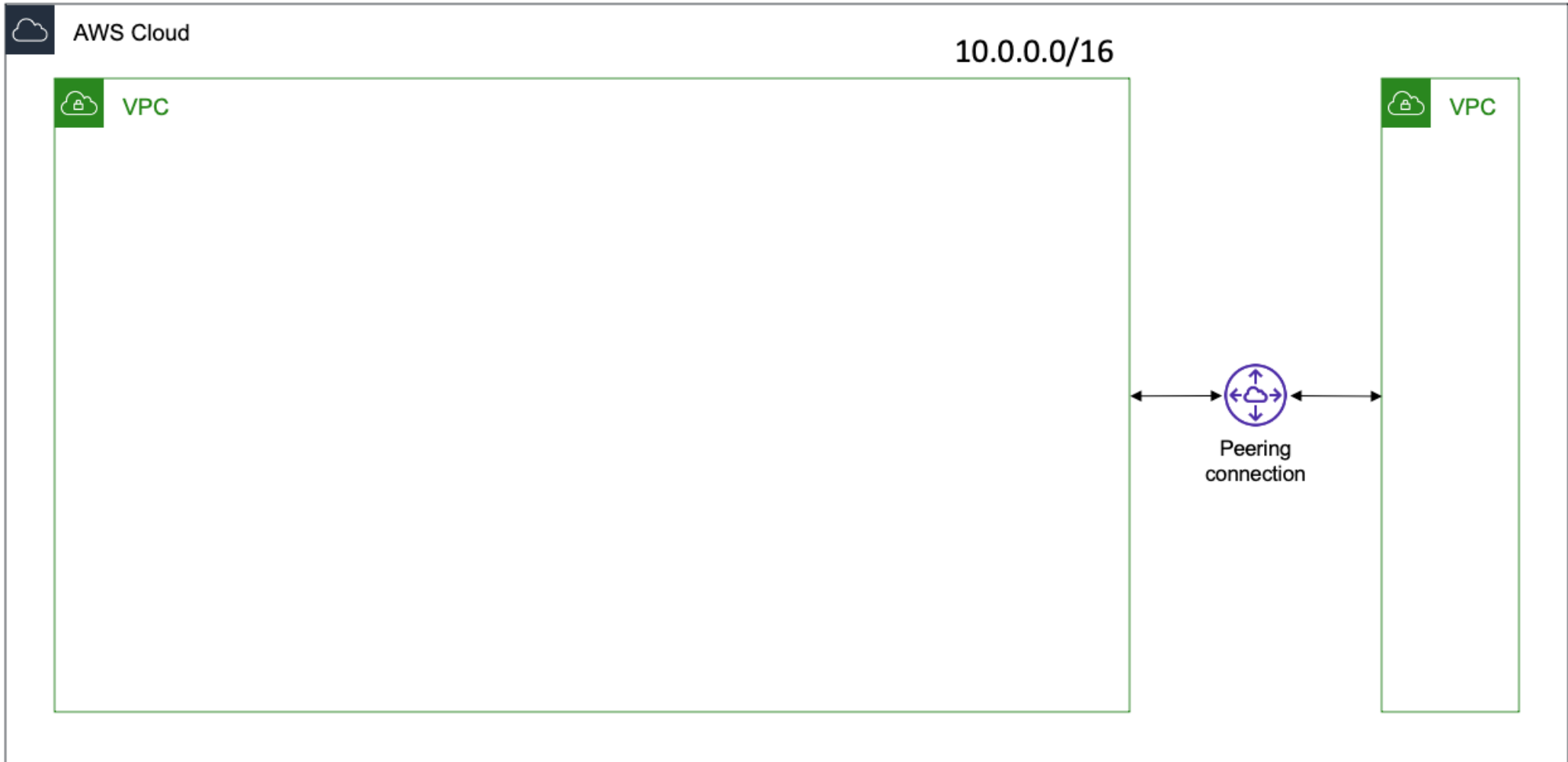
VPC Peering

손쉽게 한 VPC 객체가 다른 VPC 객체 간 사설 IP주소로 통신 가능



두개의 VPC 간에 VPC Peering 구성하기 위해서는?

- 두 VPC가 같은 Region에 위치해야 함
- 두 VPC의 사설 IP주소 대역이 겹치지 않아야 함



라우터

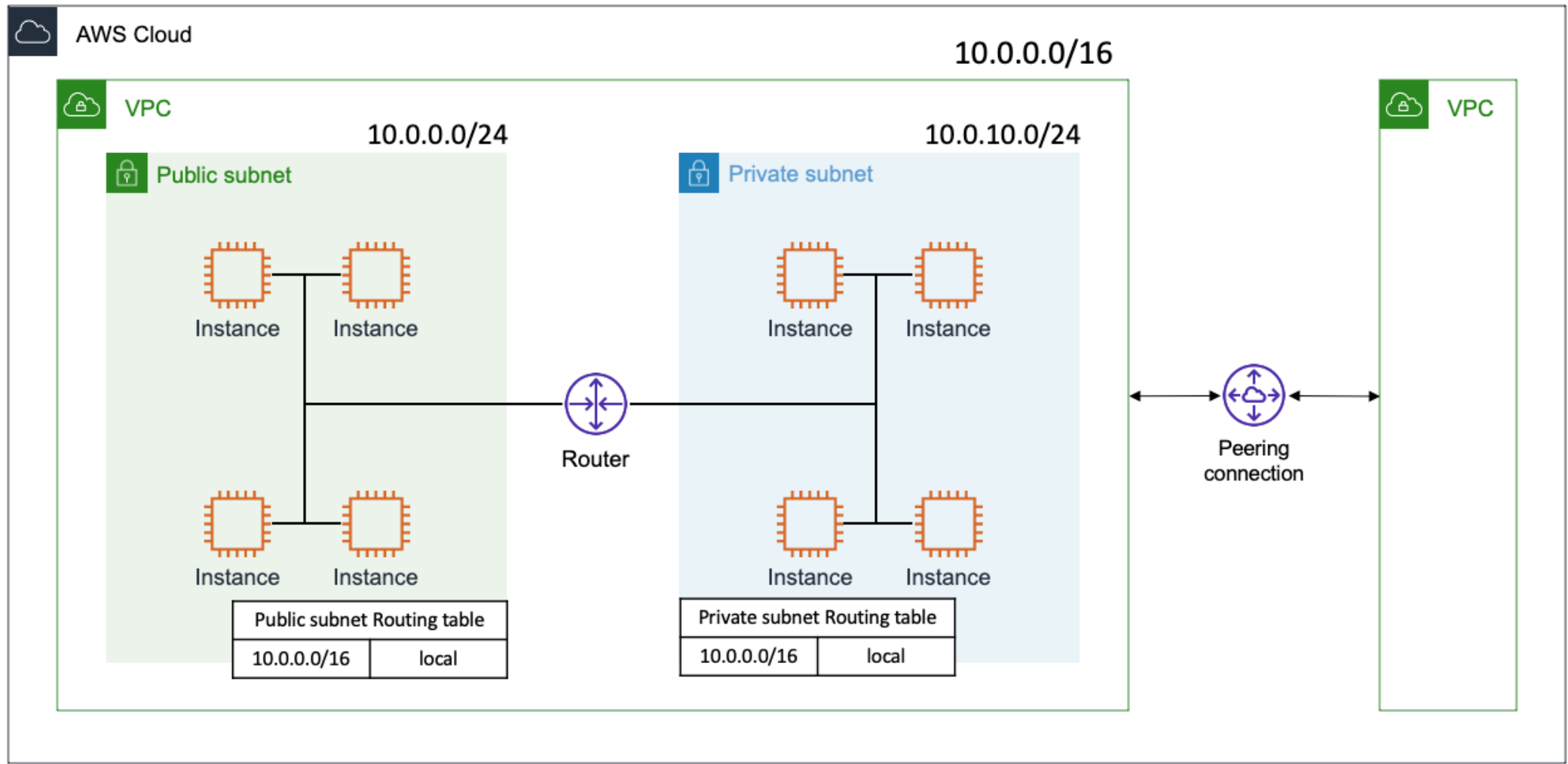
VPC 안에서 발생한 네트워크 요청을 처리하기 위해 어디로 트래픽을 전송해야 하는지 결정

각각의 서브넷은 네트워크 트래픽 전달 규칙에 해당하는 라우팅 테이블을 가지고 있으며 요청이 발생하면 가장 먼저 라우터로 트래픽을 전송

라우팅 테이블

- 트래픽이 어느곳으로 이동할 것인지 알려주는 이정표
- 서브넷이 안팎으로 나가는 트래픽에 대하여 라우팅 경로를 지정하는 역할

일반적으로 VPC 내부 네트워크에 해당하는 주소는 local로 향하도록 함



IG

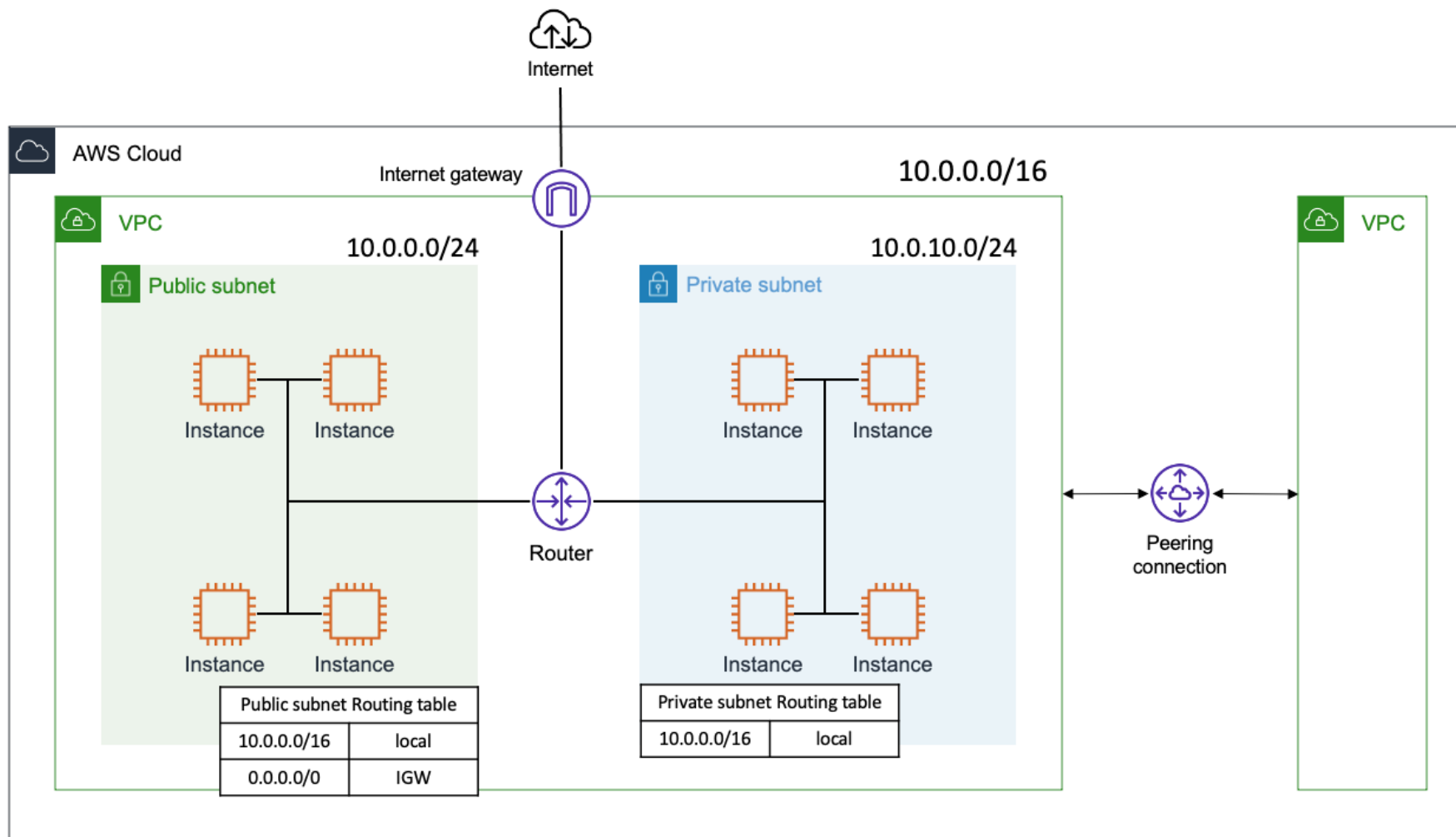
(Internet Gateway)

IG

VPC 리소스와 인터넷 간 통신을 활성화하기 위해 VPC에 연결하는 게이트웨이

Public subnet만 외부와 통신하므로,
Public subnet의 라우팅 테이블에만 IGW로 향하는 규칙을 포함

목적지의 IP 주소가 10.0.0.0/16(VPC 내부)에 해당하는지 확인하고,
그 외 모든 트래픽은 IG를 통해 외부로 전송





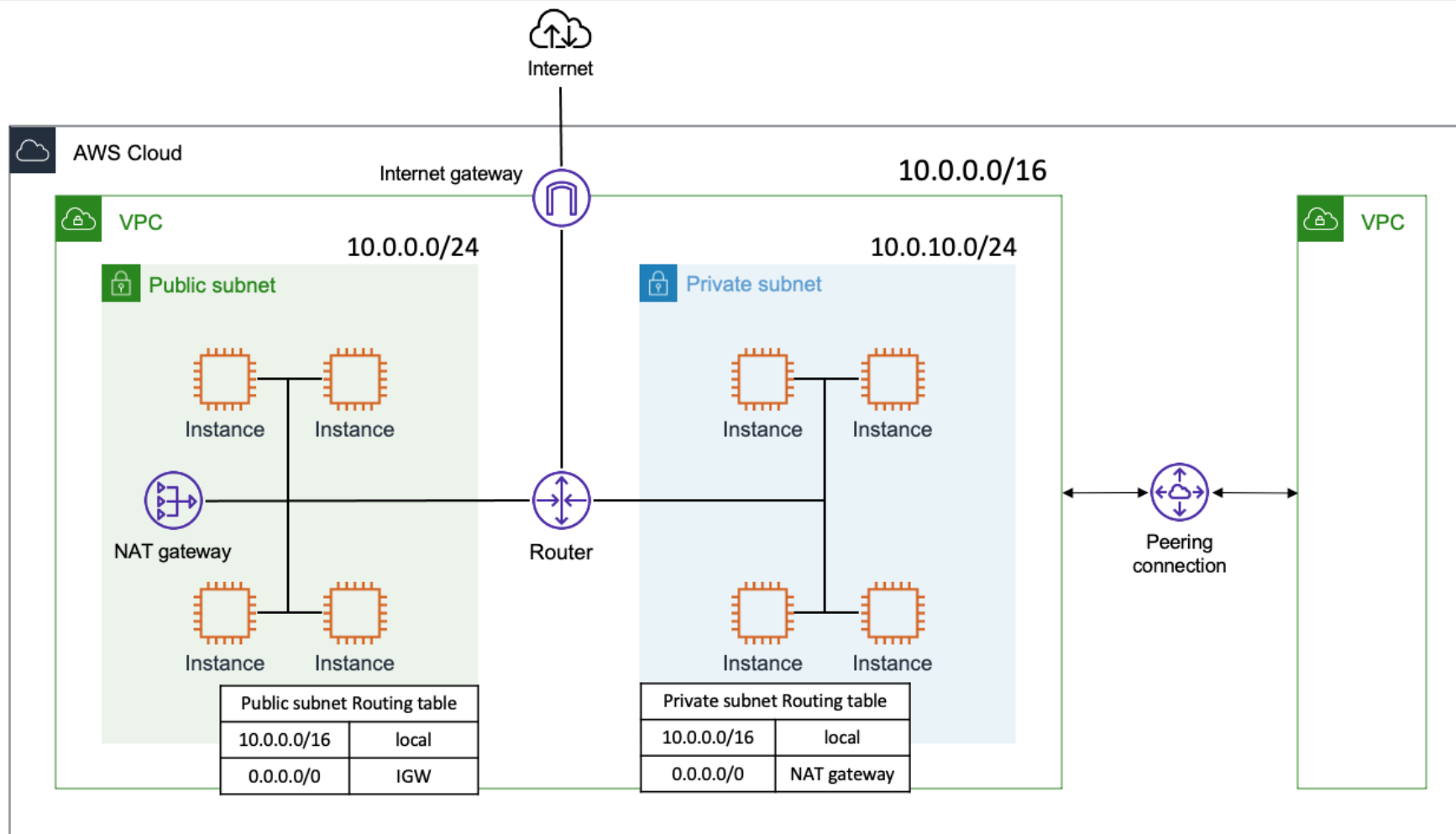
Private subnet의 트래픽은 무조건 VPC 내에서만 처리되는가?

- Private subnet 역시 마찬가지로 인터넷과 통신 가능
- Private subnet에서 직접하는 것은 불가능
(트래픽을 Public subnet에 속한 인스턴스에 전송해서
인터넷과 통신)

NAT 게이트웨이 사용

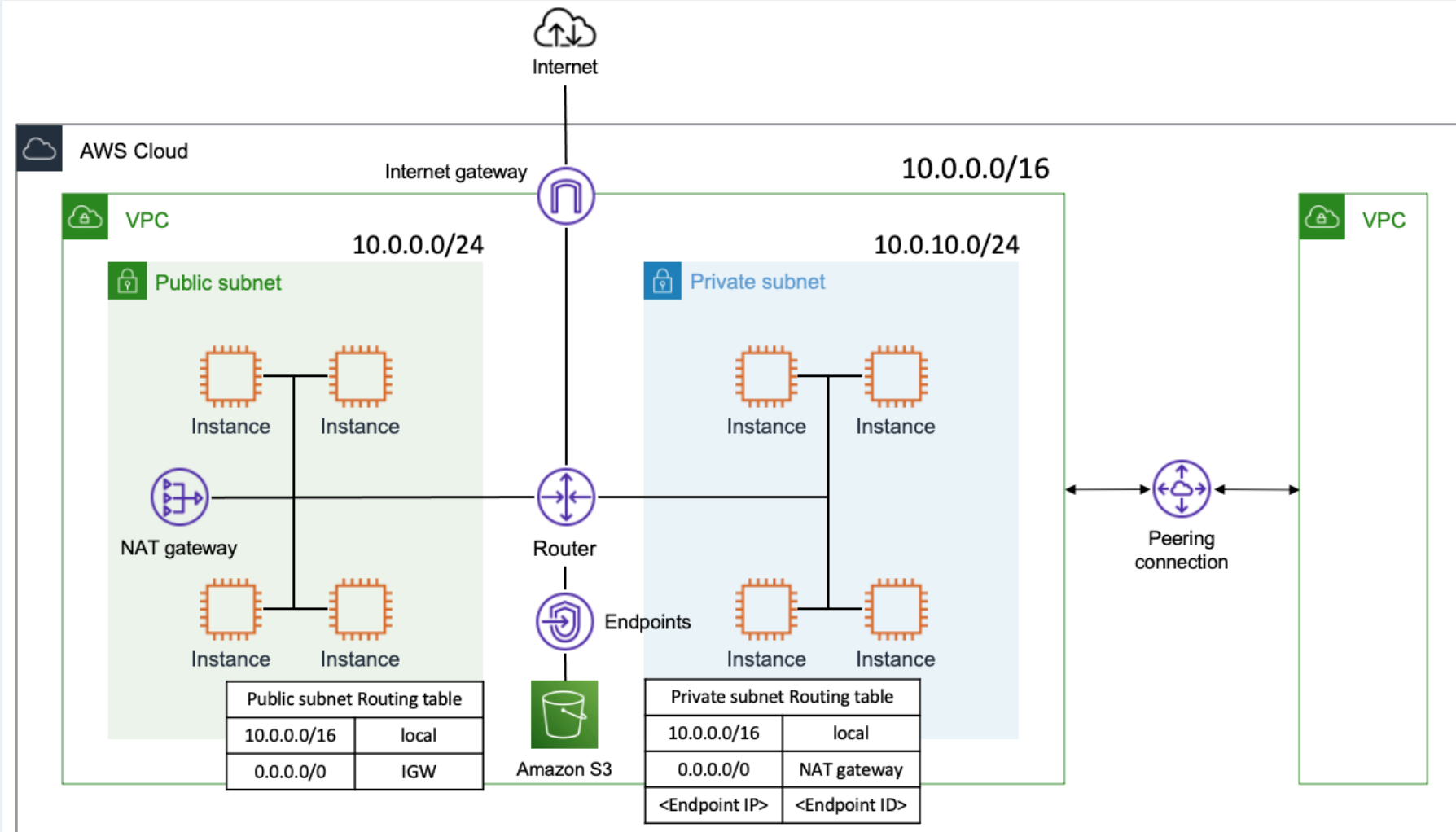
Private subnet에서 발생한 요청이 VPC 내부의 주소를 목적지로 하는 것이 아니면, Public subnet에 존재하는 NAT로 트래픽을 전송

NAT는 Public subnet의 라우팅 규칙에 따라 처리하므로, Private subnet에서 인터넷과 통신하도록 포워딩



엔드포인트

인터넷 게이트웨이나 NAT 게이트웨이와 같은 다른 게이트웨이 없이 AWS 서비스와 연결하여 통신할 수 있는 Private connection을 제공하는 서비스



웹서버 인스턴스 실행 실습

- 웹서버 인스턴스 실행

ES2 인스턴스 시작



- </> AWS 서비스 중 EC2를 검색하고 선택하여 “인스턴스 시작” 선택
- </> 인스턴스 이름: “ws1”

이름 및 태그 [정보](#)

이름

[추가 태그 추가](#)

AMI 선택 : 사용 가능한 Quick Start AMI 목록



Amazon Linux, Amazon Linux 2023 AMI 선택

- Amazon Machine Image(AMI) 유형에 따라 시작할 EC2 인스턴스에서 실행할 운영 체제를 결정함

▼ 애플리케이션 및 OS 이미지(Amazon Machine Image) 정보

AMI는 인스턴스를 시작하는 데 필요한 소프트웨어 구성(운영 체제, 애플리케이션 서버 및 애플리케이션)이 포함된 템플릿입니다. 아래에서 찾고 있는 항목이 보이지 않으면 AMI를 검색하거나 찾아보십시오.

Q 수천 개의 애플리케이션 및 OS 이미지를 포함하는 전체 카탈로그 검색

최근 사용

내 AMI

Quick Start

Amazon Linux
aws


macOS
Mac

Ubuntu
ubuntu

Windows
Microsoft

Red Hat
Red Hat

SUSE Linux
SUSE



더 많은 AMI 찾아보기

AWS, Marketplace 및 커뮤니티의 AMI 포함

Amazon Machine Image(AMI)

Amazon Linux 2023 AMI

ami-0f2ce0bfb34039f29 (64비트(x86)) / ami-034bd1a31f7fbf204 (64비트(Arm))
가상화: hvm ENA 활성화됨: true 루트 디바이스 유형: ebs

프리 티어 사용 가능

설명

Amazon Linux 2023 AMI 2023.1.20230809.0 x86_64 HVM kernel-6.1

아키텍처

64비트(x86)

AMI ID

ami-0f2ce0bfb34039f29

확인된 공급 업체

인스턴스 유형 선택

인스턴스에 할당된 하드웨어 리소스를 정의

인스턴스 유형

t2.micro

Configure the Network settings

Next to [Network settings], choose [Edit], then configure

- Network: lab-vpc
- Subnet: lab-subnet-public2 (not Private!)
- Auto-assign public IP: Enable

인스턴스 구성

이전에 생성한 Web Security Group을 사용하도록 인스턴스 구성

- 방화벽(보안 그룹)에서 기존 보안 그룹 선택(existing security group)을 선택
- 공통 보안 그룹에서 웹 보안 그룹(Web Security Group)을 선택

Security Group은
인스턴스에 대한 HTTP 액세스를 허용함

네트워크 설정 구성



</> VPC 선택 콤보박스 선택

- 네트워크: testvpc-vpc
- 서브넷: testvpc-subnet-public2(프라이빗 아님)
- 공용 IP 자동 할당: 사용

▼ 네트워크 설정 정보

VPC - 필수 정보

vpc-4c180324
172.31.0.0/16 (기본값) ▲

Q

vpc-025acb5aa8e91d300 (DemoVPC1)
10.0.0.0/16

vpc-4c180324
172.31.0.0/16 (기본값) ✓

vpc-0634b49a03fa9367f (TesVPC)
10.0.0.0/16

vpc-0c56d1c1d4e68adb (testvpc-vpc)
10.0.0.0/16

VPC - 필수 정보

vpc-0c56d1c1d4e68adb (testvpc-vpc)
10.0.0.0/16

서브넷 정보

subnet-01c37f7165308ac7e testvpc-subnet-public1-ap-northeast-2a

VPC: vpc-0c56d1c1d4e68adb 소유자: 174391244474 가용 영역: ap-northeast-2a


사용 가능한 IP 주소: 250 CIDR: 10.0.0.0/24

퍼블릭 IP 자동 할당 정보

활성화

네트워크 설정 구성



-  웹 보안 그룹을 사용하도록 인스턴스를 구성
- 방화벽(보안 그룹)에서 기존 보안 그룹 선택을 선택
 - 일반 보안 그룹에서 웹 보안 그룹을 선택
- ➡ 결과 : 인스턴스에 대한 HTTP 액세스를 허용

방화벽(보안 그룹) 정보

보안 그룹은 인스턴스에 대한 트래픽을 제어하는 방화벽 규칙 세트입니다. 특정 트래픽이 인스턴스에 도달하도록 허용하는 규칙을 추가합니다.

☒ 보안 그룹 생성

☐ 기존 보안 그룹 선택

스토리지 구성



Amazon Linux 게스트 운영 체제


- 호스팅할 인스턴스 루트 볼륨이 크기가 8GiB인 범용 SSD(gp3) 하드 드라이브에서 실행(default)


▼ 스토리지 구성 정보

[어드밴스드](#)

1x GiB

루트 볼륨 (암호화되지 않음)

 프리 티어를 사용할 수 있는 고객은 최대 30GB의 EBS 범용(SSD)또는 마그네틱 스토리지를 사용할 수 있습니다.



새 볼륨 추가

0x 파일 시스템

[편집](#)



스토리지 구성



- ☐ 시작할 때 인스턴스에서 실행할 스크립트를 구성
- “고급 세부 정보” 패널을 확장
 - 페이지 하단으로 스크롤한 다음 페이지의 코드를 복사하여 사용자 데이터 상자에 붙여넣음

▶ 고급 세부 정보 [정보](#)

스크립트



스크립트

- 인스턴스의 게스트 OS에서 루트 사용자 권한으로 실행
- 인스턴스가 처음 시작될 때 자동으로 실행됨

```
#!/bin/bash
# Install Apache Web Server and PHP
dnf install -y httpd wget php mariadb105-server
# Download Lab files
wget https://aws-tc-largeobjects.s3.us-west-2.amazonaws.com/CUR-TF-100-ACCLFO-2/2-lab2-vpc/s3/lab-app.zip
unzip lab-app.zip -d /var/www/html/
# Turn on web server
chkconfig httpd on
service httpd start
```

➡ 웹 서버, 데이터베이스 및 PHP 라이브러리를 설치

➡ 웹 서버에 PHP 웹 응용 프로그램을 다운로드하여 설치

➡ 웹 서버 구동

화면 오른쪽, 요약 패널 하단에서 **인스턴스 시작** 선택 → “성공”

EC2에 대한 모든 **인스턴스 보기** 선택

“ws1” 상태 확인 옆에 통과된 2/2 확인을 표시할 때까지 대기

- 시간이 소요될 수 있음

EC2 인스턴스에서 실행되는 웹 서버에 연결

- 웹 서버 선택하면 “퍼블릭 IPv4 DNS” (또는 IP 주소)값을 복사하여 웹브라우저에서 접속

- 문세물기
- Outro

QUIZ



Start

학습한 내용을 바탕으로 문제를 풀어봅시다.

총 3문제가 제시되며,
문제를 풀 수 있는 기회는 1번입니다.

과정명	클라우드 보안 구축	회차명	계정보안 : VPC1	화면번호	07_05
<div>▶ Intro</div> <div>• 학습열기</div> <div>• 학습목표</div> <div>▶ 본학습</div> <div>• VPC 개념 및 구성요소</div> <div>• VPC에서 다루는 기본 개념</div> <div>▶ 정리하기</div> <div>• 문제풀기</div> <div>• Outro</div>	<div>문제풀기</div> <div>오늘 학습한 내용을 퀴즈를 통해 확인해 보세요.</div> <div><div>Q1</div><div>1. 보안그룹(security group)에 대한 설명으로 적절하지 않은 것은?</div><div><div>① 범위는 인스턴스나 인터페이스 수준에서 설정한다.</div><div>② 사용가능한 규칙은 ALLOW와 DENY 규칙이다.</div><div>③ 상태유지(stateful) 특성을 가진다.</div><div>④ 규칙순서는 어떤 트래픽을 허용하는 결정을 내리기 전에 모든 규칙을 평가한다.</div></div></div> <div><div>정답) 2</div><div>해설) 보안그룹(security group)의 범위는 인스턴스나 인터페이스 수준에서 설정한다. 보안그룹은 상태유지(stateful) 특성을 가집니다. 또한 보안그룹의 규칙순서는 어떤 트래픽을 허용하는 결정을 내리기 전에 모든 규칙을 평가합니다.</div></div>			<div>화면설명</div> <div>[문제풀기]</div> <div>- 4지선다 3문제</div> <div>- ‘못한, 않는, 아닌’과 같은 부정표현에는 밑줄 긋기</div> <div>- 확인버튼: 답을 선택하지 않고 클릭 시, ‘답을 선택해주세요.’ 팝업 나오기</div> <div>- 답을 선택 후 처음 클릭 시, 답이 틀렸을 경우 ‘다시 생각해 보세요.’ 팝업 나오기</div> <div>- 답을 선택한 후 두 번째 클릭이거나, 맞은 답을 선택하고 클릭했을 때는 바로 정답 해설 페이지로 이동하기</div>	
				<div>이미지 번호</div>	
	내레이션				

퀴즈 3문항

번호	문제	보기	정답	해설
2	다음 보기의 내용이 맞으면 O, 틀리면 X를 선택하시오.	“AWS 외부에서 일반적인 사용자가 AWS 내 서버에 접근할 때, 외부 요청은 Network ACL을 정책을 먼저 적용된 후, Security Group 정책이 적용된다.”	O	AWS 외부에서 일반적인 사용자가 AWS내 서버에 접근할 때, 외부 요청은 Network ACL을 정책을 먼저 적용된 후, Security Group 정책이 적용됩니다.
3	다음 보기의 내용이 맞으면 O, 틀리면 X를 선택하시오.	“AWS 내부에 위치한 사용자(프로그램)이 동일 서브넷에 위치한 AWS 서버에 접속하는 경우, 요청은 Security Group 정책만 적용된다.”	O	AWS 내부에 위치한 사용자(프로그램)이 동일 서브넷에 위치한 AWS 서버에 접속하는 경우, 요청은 Security Group 정책만 적용됩니다.

과정명	클라우드 보안 구축	회차명	계정보안 : VPC1	화면번호	07_05
<div><div>▶ Intro</div><div>• 학습열기</div><div>• 학습목표</div><div>▶ 본학습</div><div>• VPC 개념 및 구성요소</div><div>• VPC에서 다루는 기본 개념</div><div>▶ 정리하기</div><div>• 문제풀기</div><div>• Outro</div></div>				화면설명	
<div><div><div><div>결과 보기</div><div>총 3문항 중 1 문항을 맞히셨습니다.</div><div><div>Q1</div><div>Q2</div><div>Q3</div></div><div><div>틀린 문제 다시 풀기→</div><div>정답 및 해설→</div><div>학습 완료(참고문헌)</div></div></div></div></div>					
내레이션					

과정명	클라우드 보안 구축	회차명	계정보안 : VPC1	화면번호	07_05
<div>▶ Intro</div> <div>• 학습열기</div> <div>• 학습목표</div> <div>▶ 본학습</div> <div>• VPC 개념 및 구성요소</div> <div>• VPC에서 다루는 기본 개념</div> <div>▶ 정리하기</div> <div>• 문제풀기</div> <div>• Outro</div>	<div><div>X</div><div>클라우드 보안 구축</div><div>계정보안 : VPC1</div><div>수고하셨습니다.</div><div>참고자료</div><div><div><div>• Neha Kewate, “A Review on AWS - Cloud Computing Technology”, International Journal for Research in Applied Science and Engineering Technology, 10.22214/ijraset.2022.39802, 2022, Vol 10(1)</div><div>• D. Stalin David, Mamoonaa Anam, Chandraprabha Kaliappan, S. Arun Mozhi Selvi, Dilip Kumar Sharm, “Cloud Security Service for Identifying Unauthorized User Behaviour”, Computers Materials & Continua, 10.32604/cmc.2022.020213, 2022, Vol 70(2)</div><div>• 임재덕, “클라우드 컴퓨팅 발전법 주요내용 및 정책방향”, 미래창조과학부</div><div>• 임철수, “클라우드 컴퓨팅 보안기술”, 정보보호학회지 정보보호 특집</div><div>• 앤서니 T, “미래코드 클라우드 컴퓨팅”, 전자신문사</div><div>• 편집부, “클라우드 컴퓨팅 차세대 컴퓨팅 기술”, 데이코 산업 연구소</div><div>• 엄철수, “클라우드 컴퓨팅의 기초” 서경대학교</div><div>• 정인호, “클라우드 컴퓨팅”, 명지대학교</div></div></div></div>			화면설명	
				이미지 번호	
내레이션					

7회차 메타데이터

- 주요학습내용 : 해당 회차 또는 레슨의 주요학습내용을 자세히 기입해 주세요.
- 검색 키워드 : 학습자가 검색창에 어떤 검색어를 입력하면 본 회차 또는 본 레슨이 검색될 수 있을지 검색 키워드를 5개 기입해 주세요.

제목	주요학습내용	검색 키워드1	검색 키워드2	검색 키워드3	검색 키워드4	검색 키워드5
계정보안: VPC1	<ul style="list-style-type: none">• VPC 개념 및 구성요소• VPC에서 다루는 기본 개념	클라우드 보안	VPC	CIDR	Subnet	Peering