이상희 교사

AWS를 활용한 웹 서비스 구성하기

3단원 강의

- 1차수: AWS VPC 서비스
- 2차수: AWS IAM 서비스

1차수 학습목표

- AWS 의 핵심 서비스 중 하나인 VPC 서비스를 이해 할 수 있다

1차수 학습내용

- 기본 네트워크 개념 이해
  - OSI 7 layer 모델과 TCP/IP 모델
  - IP주소와 서브넷마스크
  - Port Address
  - DHCP
  - DNS
  - 라우팅
- VPC
  - 서브넷
  - 라우팅테이블
  - 네트워크 ACL
  - 보안그룹
  - 호스트 기반 방화벽

OSI 7 layer 모델과 TCP/IP 모델

1) OSI 7 Layer 모델

국제 표준화 기구(ISO)가 1984년에 발표한 OSI 7 Layer는 통신이 일어나는 과정을 7단계로 구분해서 한눈에 들어올 수 있도록 보여준다.

- 컴퓨터 통신 구조의 모델과 앞으로 개발될 프로토콜의 표준적인 뼈대를 제공하기 위해서 개발된 참조 모델

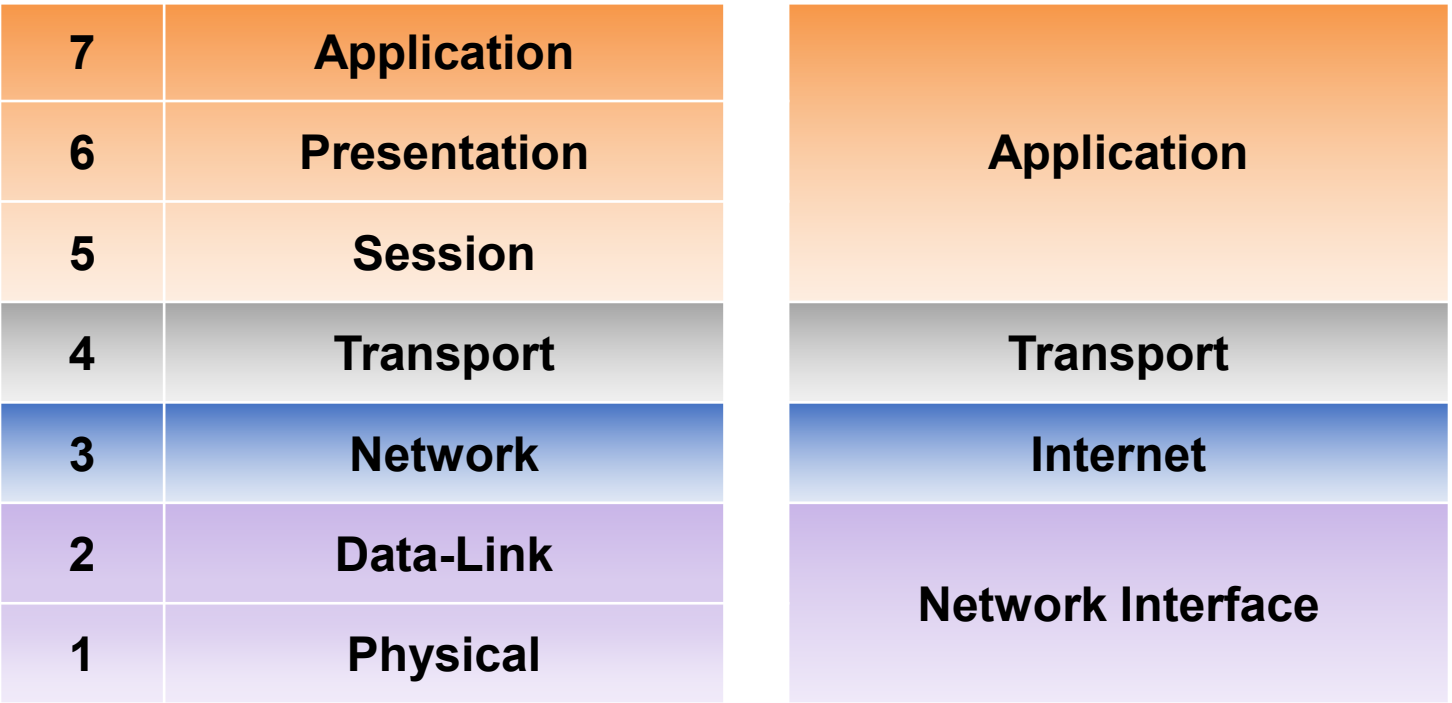
2) TCP/IP 모델

미국에서 개발한 인터넷의 기본 통신 프로토콜, DOD Model(미국방성 모델)을 기반으로 개발

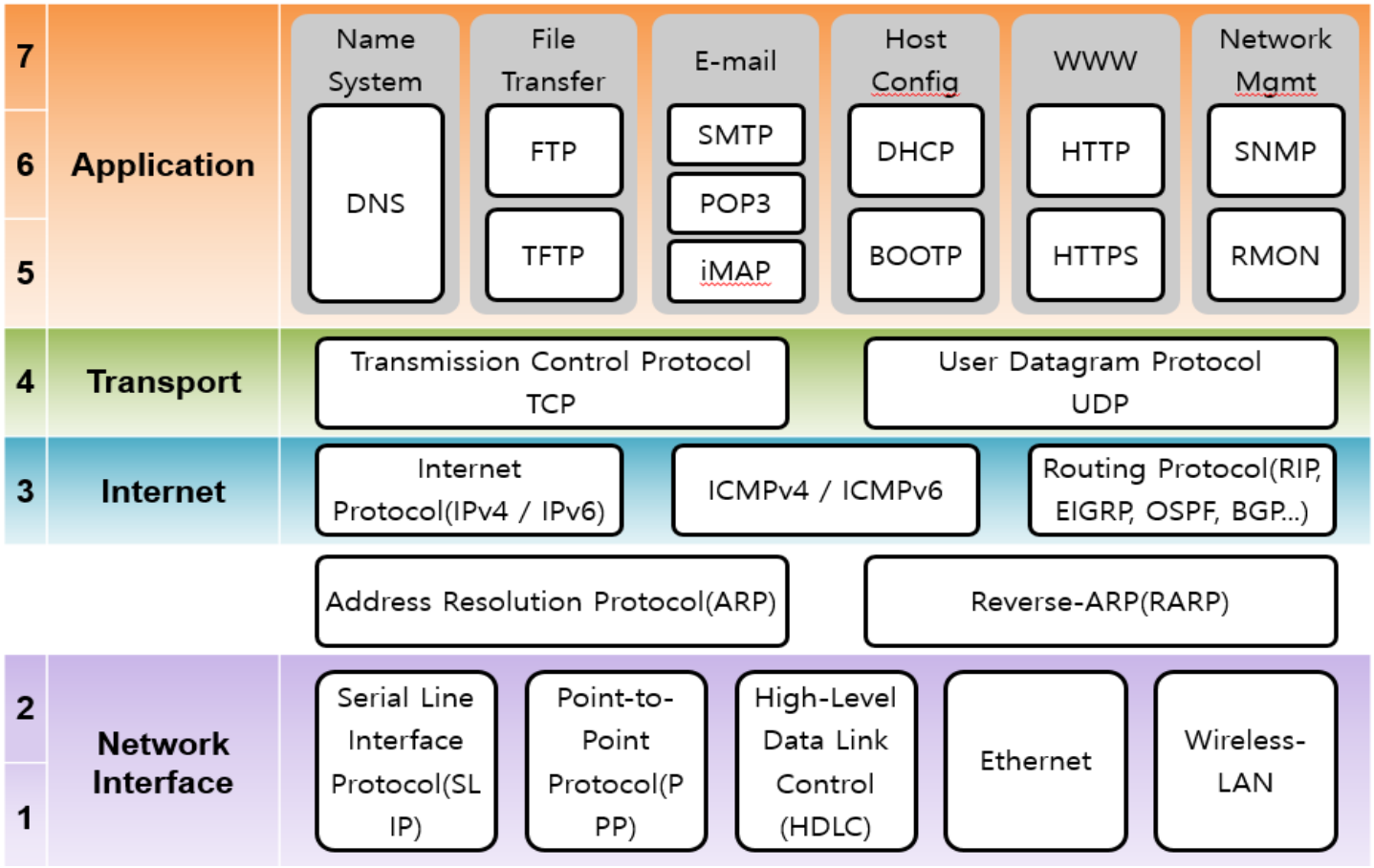
- TCP : 연결지향형 프로토콜, 세션의 연결과 종료, 흐름제어, 패킷의 분할 및 재조립
- IP : 비 연결지향형 프로토콜, 데이터 전송

→ OSI 7 Layer는 장비 개발자들이 어떻게 표준을 잡을지 결정할 때 사용하고 TCP/IP 는 실질적으로 사용되는 프로토콜이다.

OSI 7 layer Model VS TCP/IP Model



Protocol Mapping for Model



IP Address

→ **IP**는 논리적인 주소.

TCP/IP를 사용하는 네트워크 상에 연결된 장비들에게는 고유의 **IP**주소가 부여된다.
(주소가 같은 다른 장비가 존재한다면 **IP** 주소가 서로 충돌)

→ **IP address**는 네트워크 부분과 호스트 부분으로 구성.

(IP address = Network Part + Host Part)

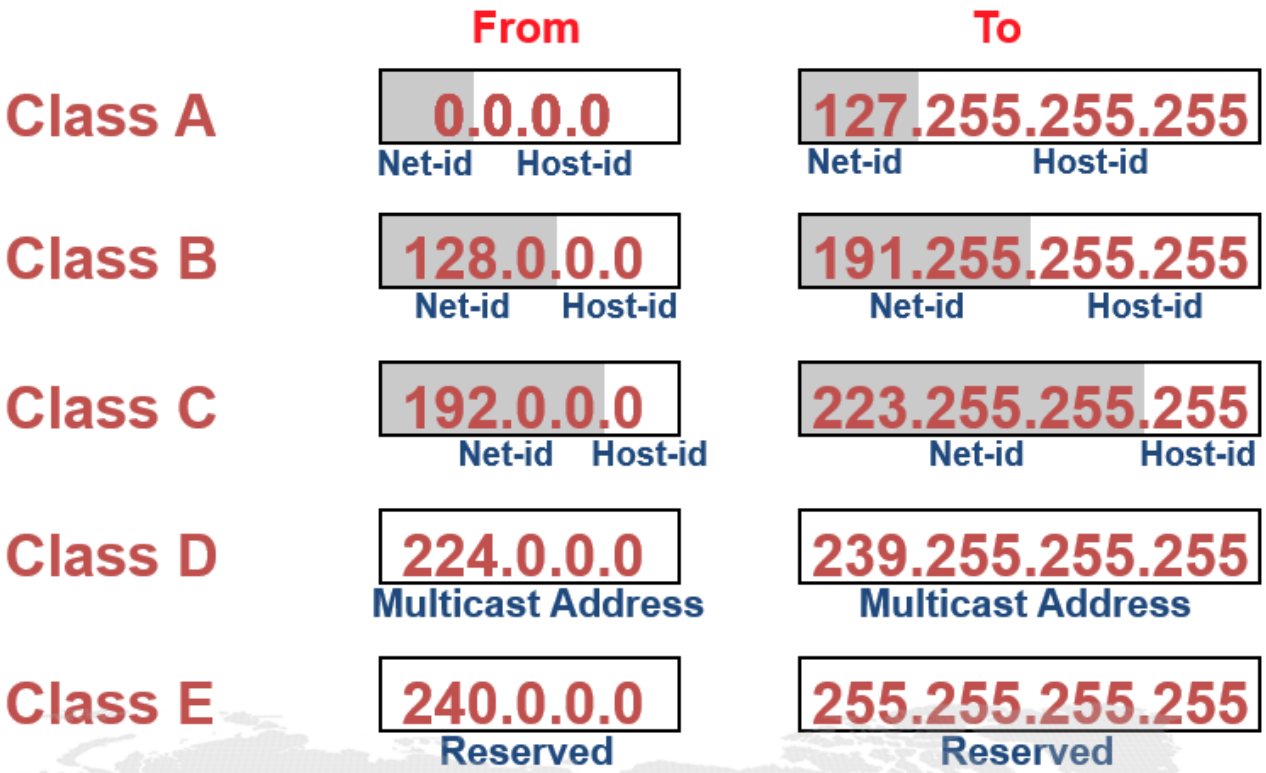
ex) 교실 이름과 학생 번호

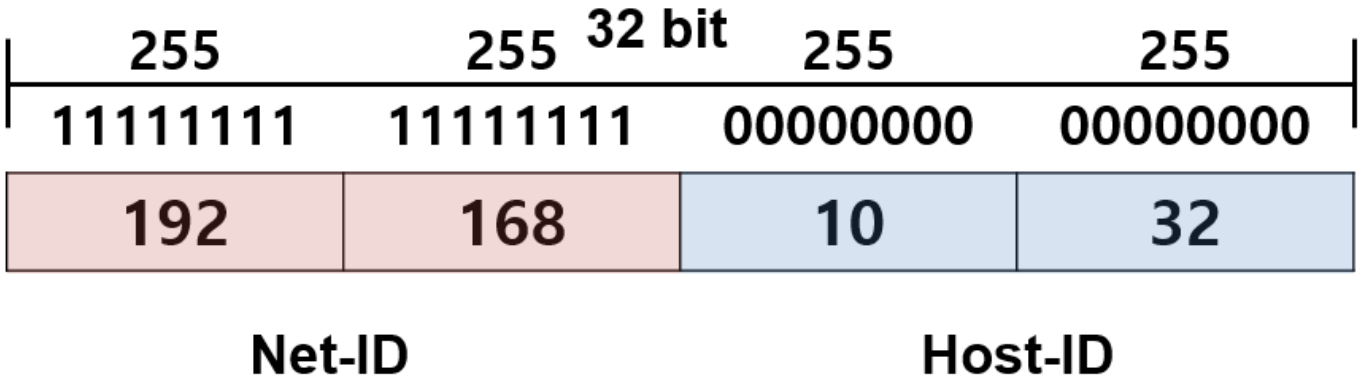
공인IP Vs 사설IP

- 공인 IP 주소는 더 광범위한 인터넷으로 식별됩니다.
- 사설 IP 주소는 네트워크 보안을 강화합니다.

- 공인 IP 주소
  - 인터넷을통해 연결 또는라우팅 할수 있는 IP 주소
  - 인스턴스와 인터넷간통신에 사용할 수있음
  - 또한, 공인 IP 주소할당 인스턴스에 DNS 호스트이름이 할당
- 사설 IP 주소
  - 인터넷을통해 연결 또는라우팅 할 수없는 IP 주소
  - 이 주소를 이용 동일 VPC에서 인스턴스간 통신을 위해 사용됨

IPv4 주소 클래스

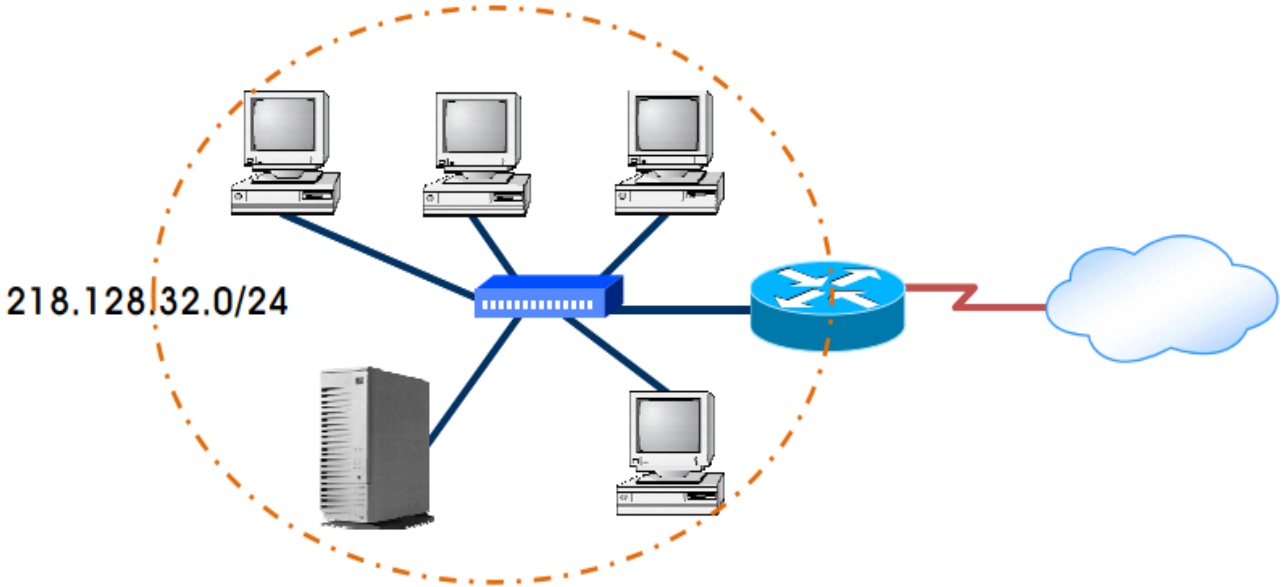

From
To
Class A
0.0.0.0
Net-id Host-id
127.255.255.255
Net-id Host-id
Class B
128.0.0.0
Net-id Host-id
191.255.255.255
Net-id Host-id
Class C
192.0.0.0
Net-id Host-id
223.255.255.255
Net-id Host-id
Class D
224.0.0.0
Multicast Address
239.255.255.255
Multicast Address
Class E
240.0.0.0
Reserved
255.255.255.255
Reserved



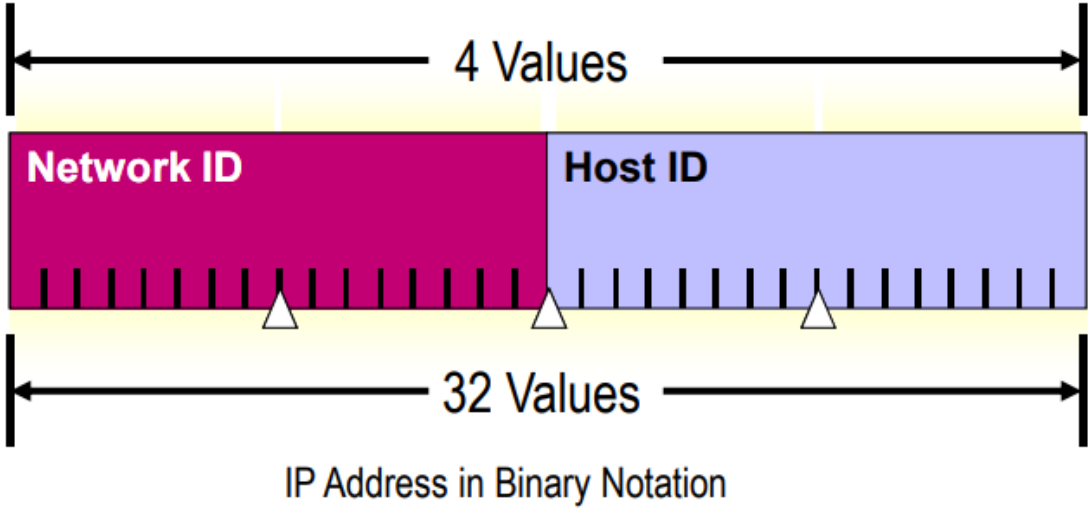
Subnet-mask : Net-ID와 Host-ID를 식별해주는 값

1은 Net-ID를 표시하고
0은 Host-ID를 표시한다

서브넷팅(Subneting)



- Broadcast Domain에 많은 호스트가 연결된 경우 호스트에 발생한 Broadcast traffic이 모든 호스트에 전달되어 많은 Broadcast Traffic이 발생하며 하나의 Broadcast Domain에서는 보안이 취약하기 때문에 Firewall이나 ACL과 같은 정책을 구현하기 위해서는 Network Segment를 나누는 것이 효율적이다.
- ISP업체에서는 회선을 임대한 기업들에 IP를 할당하기 위하여 Subnetting을 한 후에 IP를 할당하여 주소를 절약한다.



- CIDR (Classless Inter-network Domain Routing)이란 주소 재할당 개념이다. 기존 Class기반 주소에서 Class를 제외하고 32bit 전체 bit에 대해 Network과 Host를 재 설정한 주소 구조이다. 기존 Class 기반 주소에 비해 주소 손실을 줄여 주고, Router에는 구조화된 주소 할당으로 인해 Routing Table을 줄여 packet Delay를 줄인다.

- 더 이상 클래스 A, B, C가 없습니다.
- VPC당 5개 CIDR 블록이 있습니다.
- 중첩이 허용되지 않습니다.

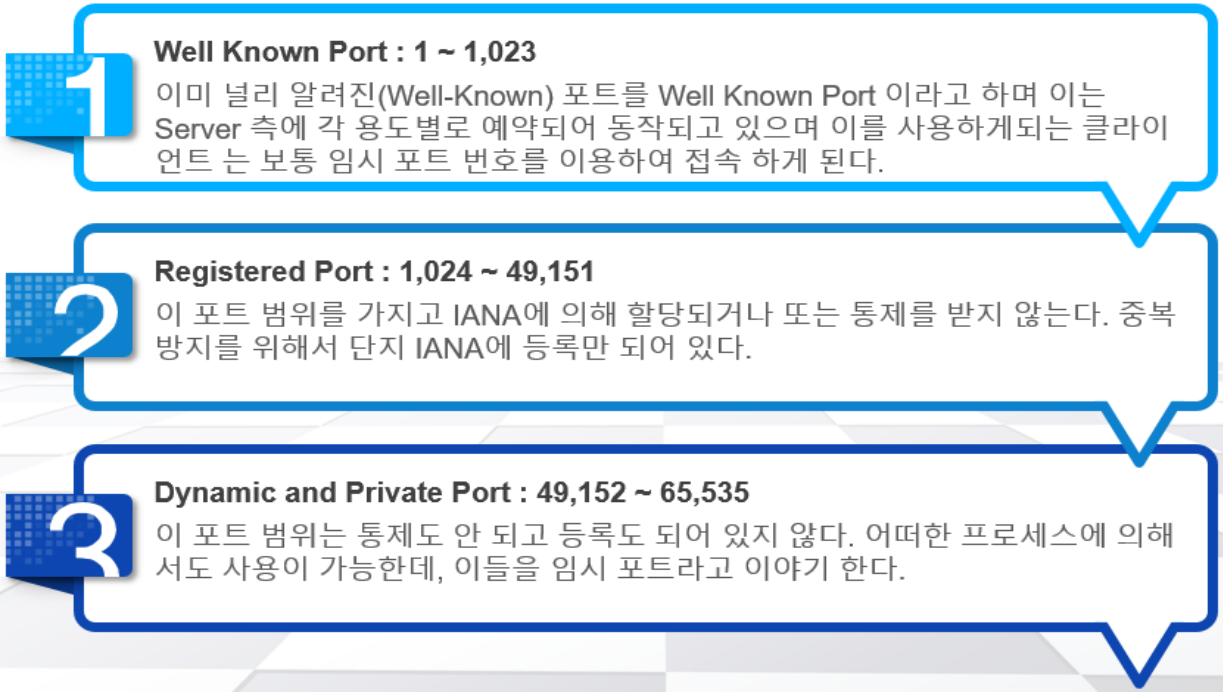
0.0.0.0/0	= 모든 IP
10.22.33.44/32	= 10.22.33.44
10.22.33.0/24	= 10.22.33.*
10.22.0.0/16	= 10.22.*.*

CIDR	총 IP
/28	16
...	...
/20	4,096
/19	8,192
/18	16,384
/17	32,768
/16	65,536

- IPv4 서브넷에는 /28(16개 IP 주소)과 /16(65,536개 IP 주소) 사이에서 블록크기를 지정가능
- IPv6-전용서브넷의 IPv6 CIDR 블록의크기는 /64의 고정접두부(prefix) 길이가 존재

Port Address

인터넷 할당 번호 관리 기관(Internet Assigned Number Authority, IANA)은 포트 번호를 세 개의 번위로 나누어서 관리 하고 있다.
참조 사이트 : http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml



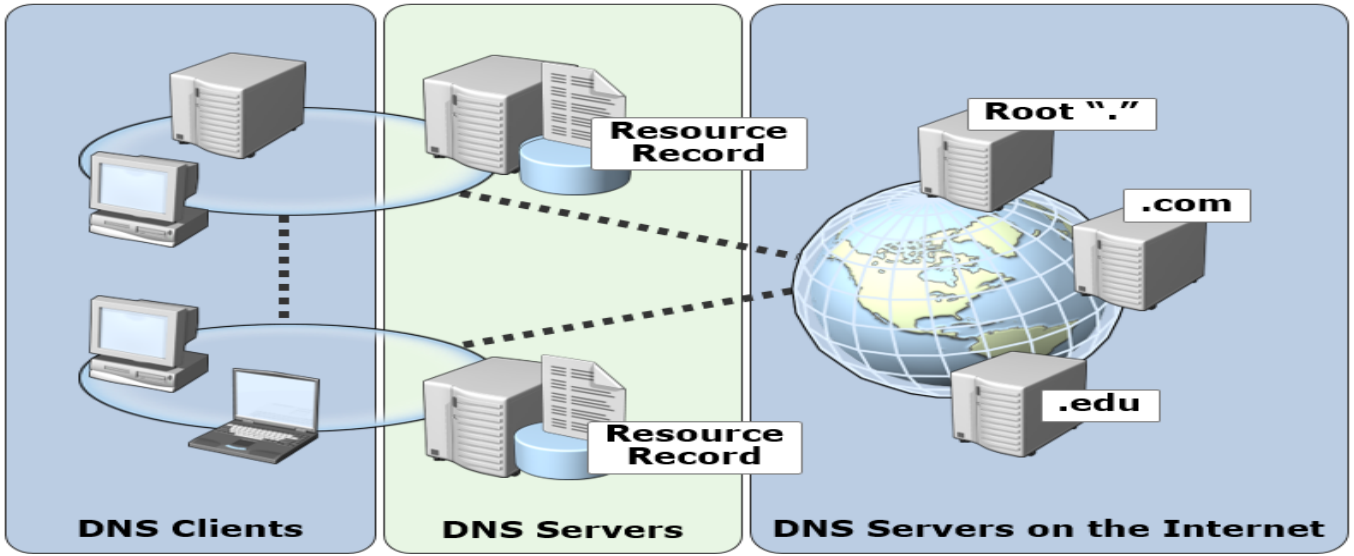
DHCP (Dynamic Host Configuration Protocol)

- 동적으로 IP 주소를 일정 기간 임대를 하는 프로토콜
- DHCP 서버나 장비는 UDP 프로토콜 포트 번호 67과 68을 사용하여 동작함
- IP주소를 임대하는 개념하에 임대 시간이 존재하며 임대 시간이 만료되면 반환하거나 갱신을 수행

DNS (Domain Name System)

InterNet이나 Intranet 또는 클라우드내에서 통신하고자 하는 IP가 배정된 호스트의 주소를 도메인 네임이라는 문자 형태로 구성된 이름을 알려주는 서비스입니다 (Host Name Resolution서비스) AWS에서는 Route53 서비스로 제공

예:ns.google.com -> 8.8.8.8
Ns.google.com 이라는 것이 도메인 네임이며 ns. google.com에 해당하는호스트의 IP 주소가 무엇인지를 알려준다
UDP 프로토콜을 사용하며, 포트 번호 53 사용하여 동작

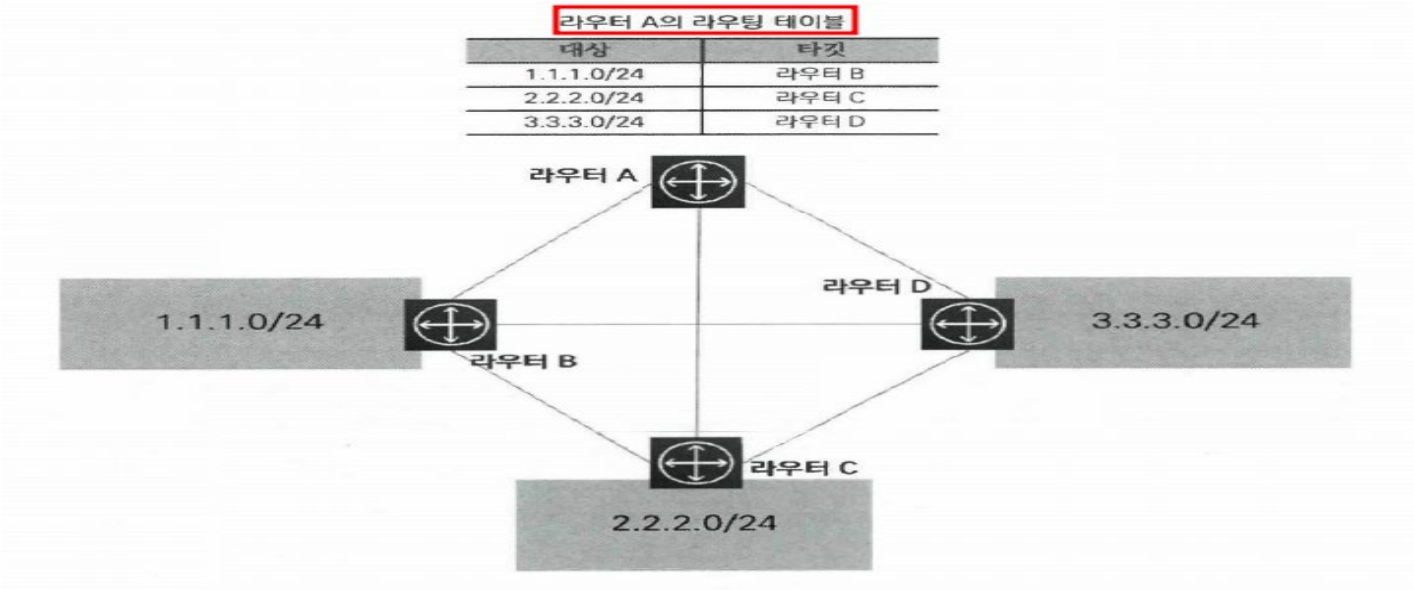


✓ **라우팅(Routing)**

네트워크는 여러 개의 서브넷으로 이루어져 있으며, 목적지 IP 로 향할 때 여러 노드를 거쳐서 통신이 발생

복잡하게 연결된 네트워크망에서 최적의 경로를 잡아 통신하는 것

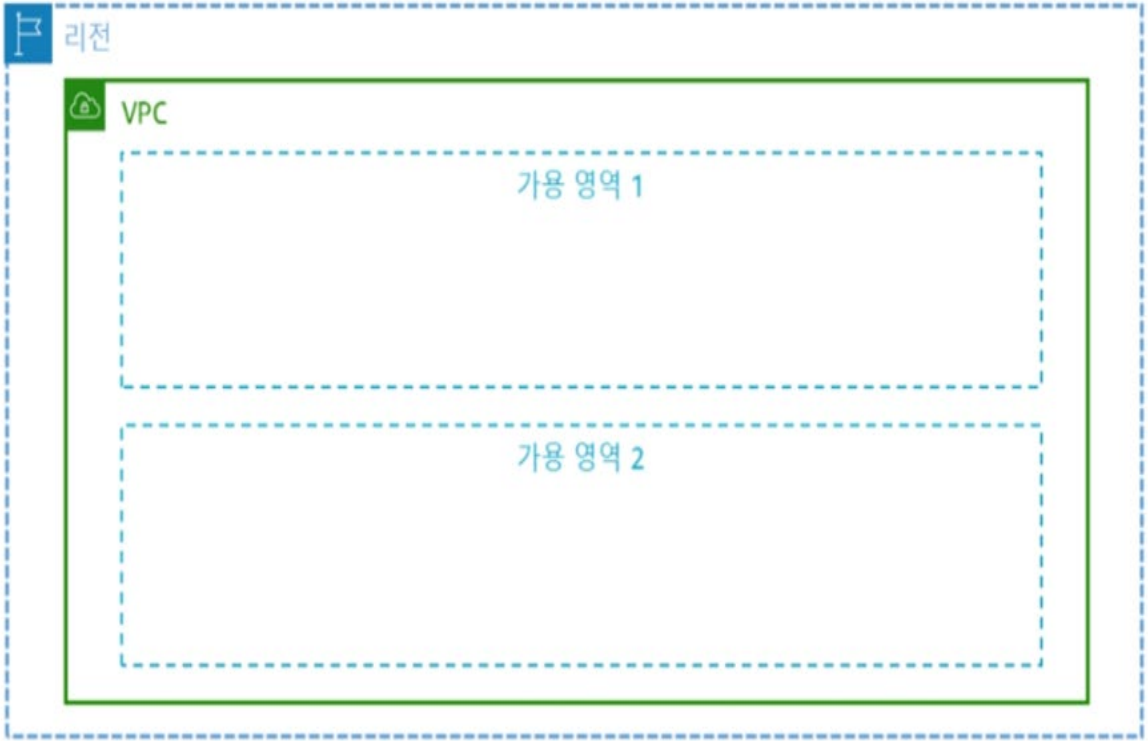
라우터는 라우팅을 수행하는 장비이며 라우팅 테이블을 통해 목적지IP 가 어느경로로 향하는지 기록하고 해당경로로 데이터를 전달함



- VPC
  - 서브넷
  - 라우팅테이블
  - 네트워크 ACL
  - 보안그룹
  - 호스트 기반 방화벽

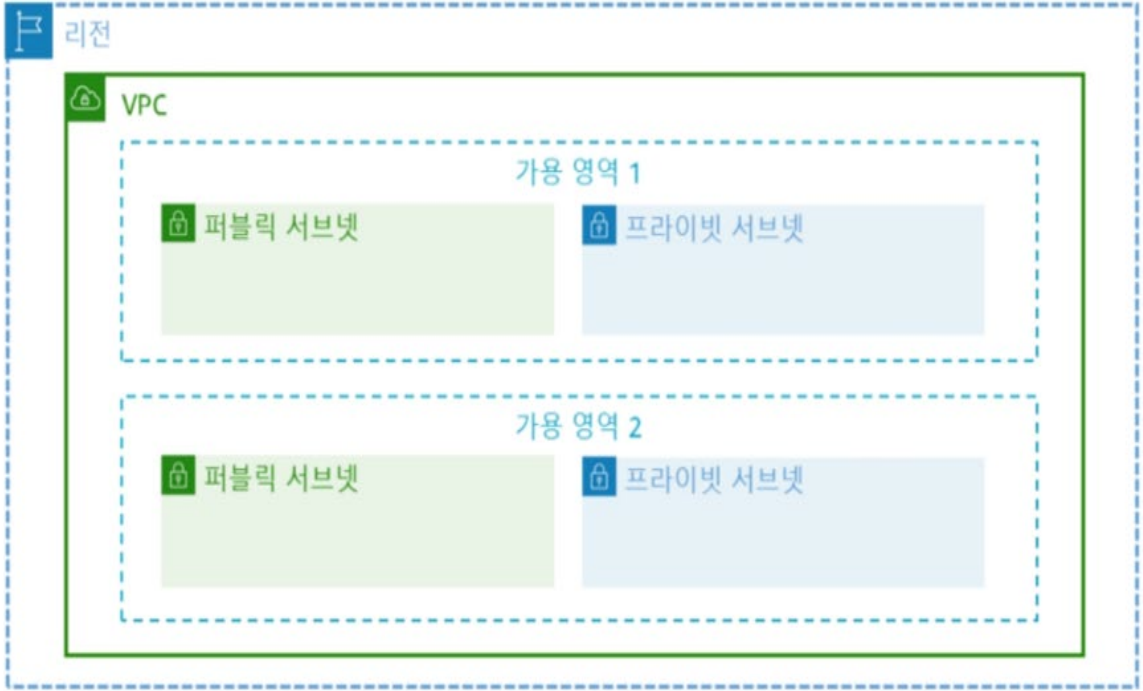
Amazon Virtual Private Cloud(Amazon VPC)

- 워크로드의 논리적 격리를 제공합니다.
- 리소스에 대한 사용자 지정 액세스 제어 및 보안 설정을 허용합니다.
- 단일 AWS 리전에 바인딩됩니다.



서브넷

- 서브넷은 VPC CIDR 블록의 하위 집합입니다.
- 서브넷 CIDR 블록은 중첩될 수 없습니다.
- 각 서브넷은 하나의 가용 영역 내에 상주합니다.
- 하나의 가용 영역에 서브넷이 여러 개 포함될 수 있습니다.



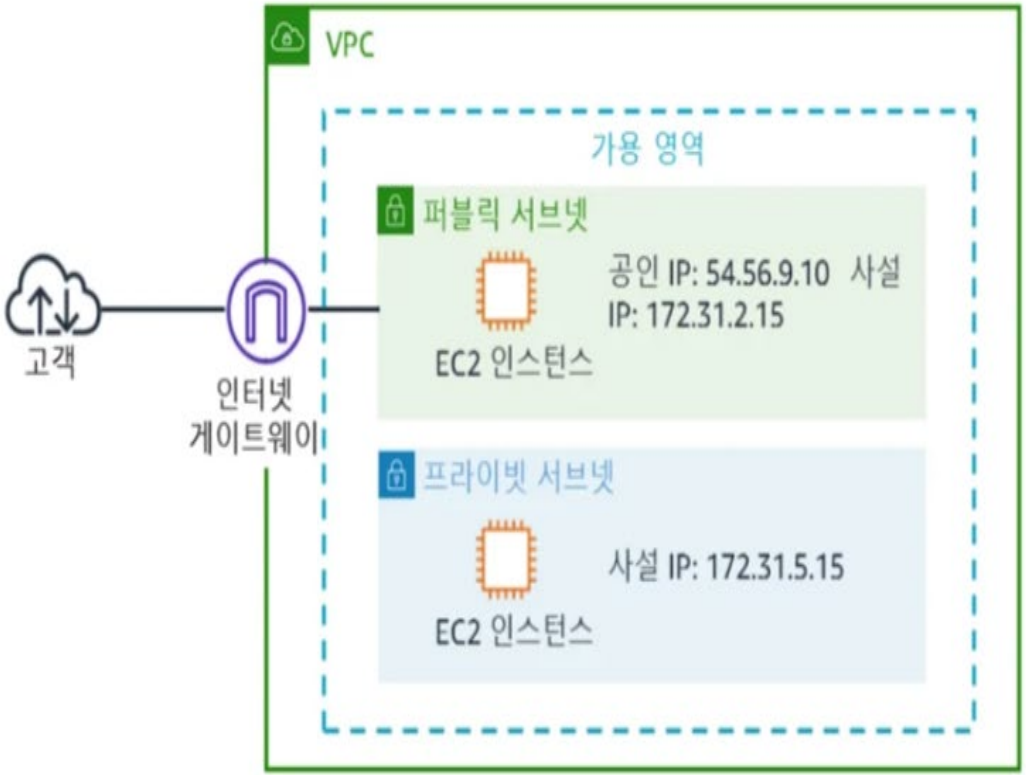
서브넷을 사용하여 VPC분리

- 서브넷을 사용하여 라우팅 및 보안을 위해 리소스를 격리합니다.
- AWS는 각 서브넷에서 5개의 IP 주소를 예약합니다.

CIDR /22 인 VPC는 총 1,024개 IP 주소를 포함합니다.

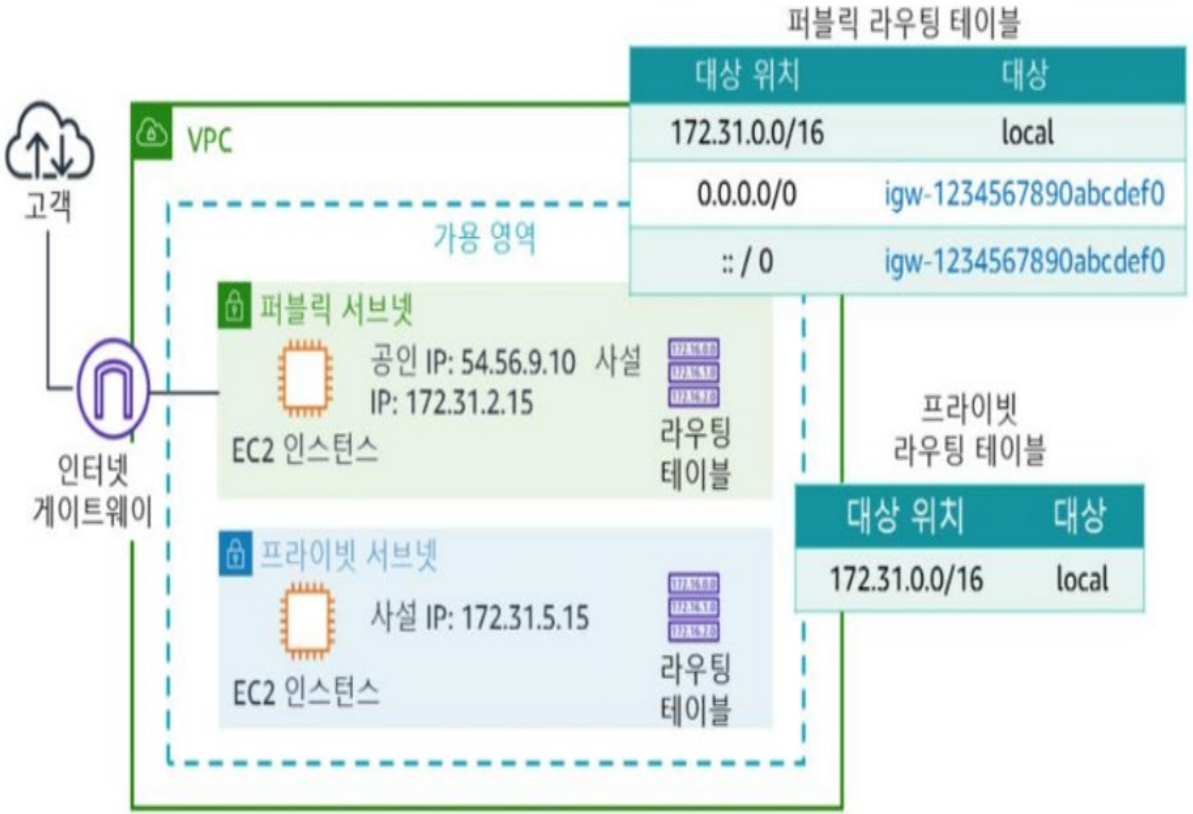
인터넷게이트웨이

- 인터넷 게이트웨이는 VPC의 인스턴스와 인터넷 간 통신을 허용합니다.
- 기본적으로 수평 확장되고 중복되며 고가용성입니다.
- 인터넷으로 라우팅 가능한 트래픽에 대한 서브넷 라우팅 테이블에 대상을 제공합니다.



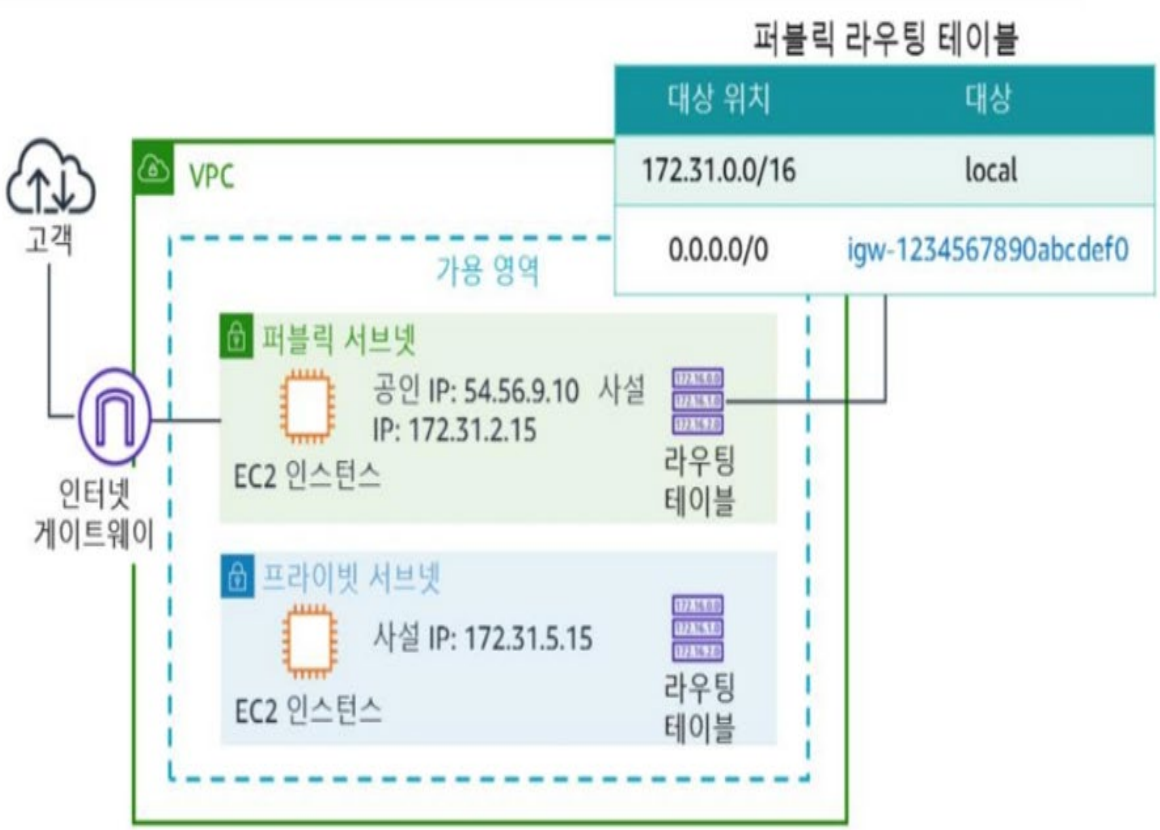
라우팅테이블

- VPC에는 **암시적 라우터**가 있습니다.
- 라우팅 테이블을 사용하여 네트워크 트래픽을 디렉션합니다.



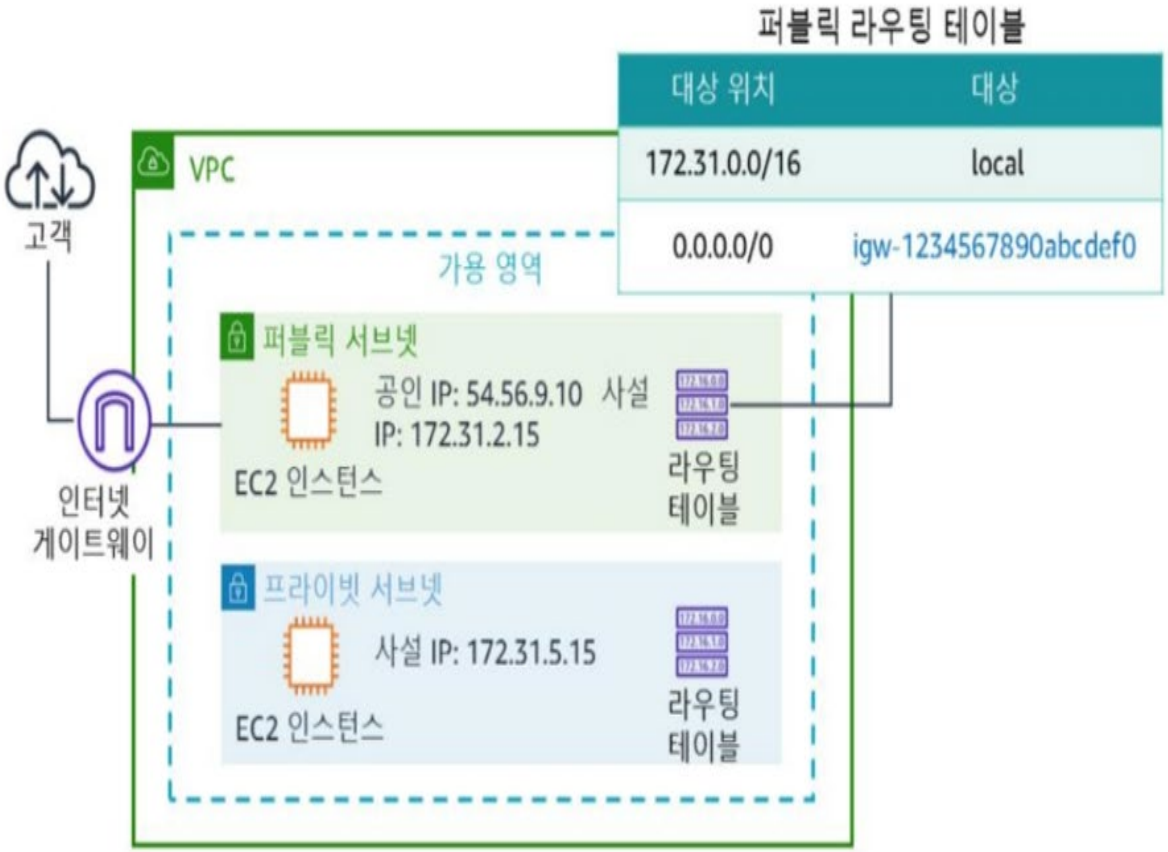
공용서브넷

- 퍼블릭 서브넷은 공인 IP 주소를 통한 외부 통신을 허용합니다.
- 자동 아웃바운드 라우팅은 없습니다.
- 인터넷 게이트웨이를 통해 인터넷에 액세스합니다.



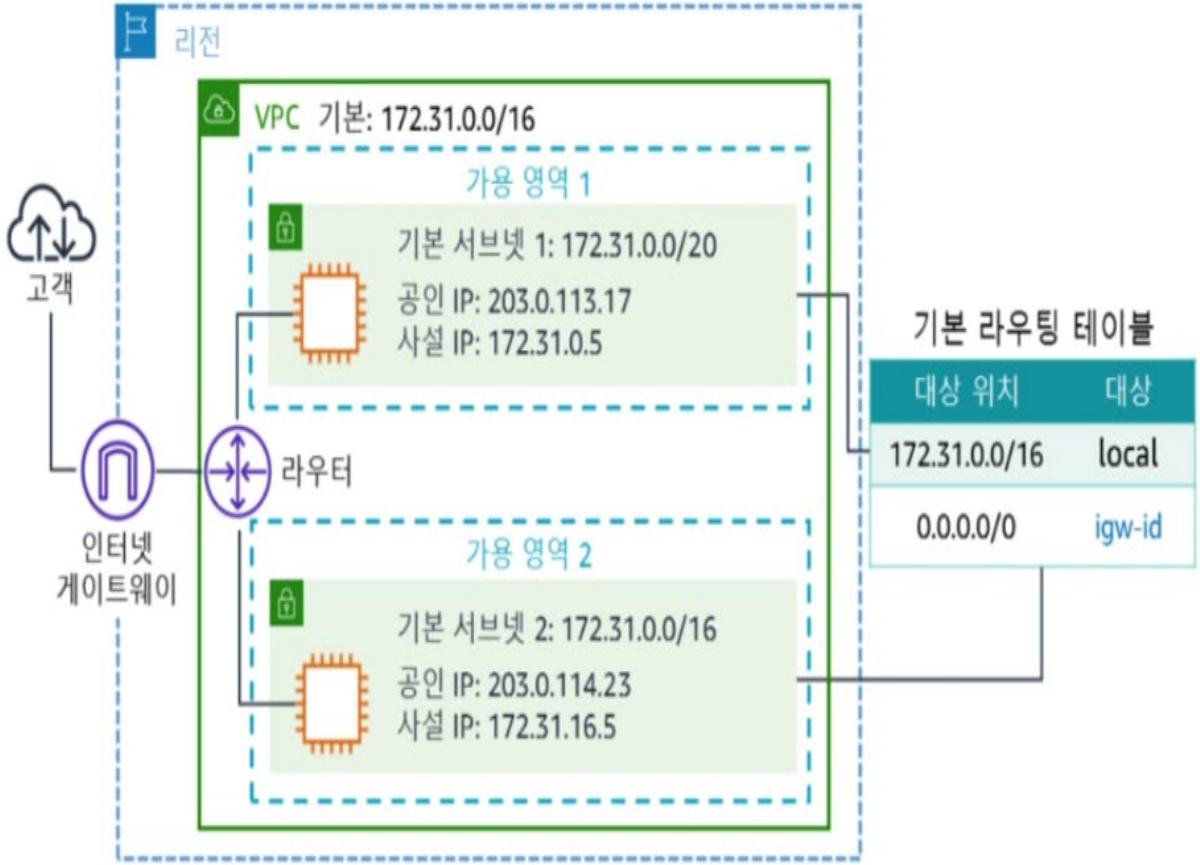
사설서브넷

- 퍼블릭 서브넷은 공인 IP 주소를 통한 외부 통신을 허용합니다.
- 자동 아웃바운드 라우팅은 없습니다.
- 인터넷 게이트웨이를 통해 인터넷에 액세스합니다.



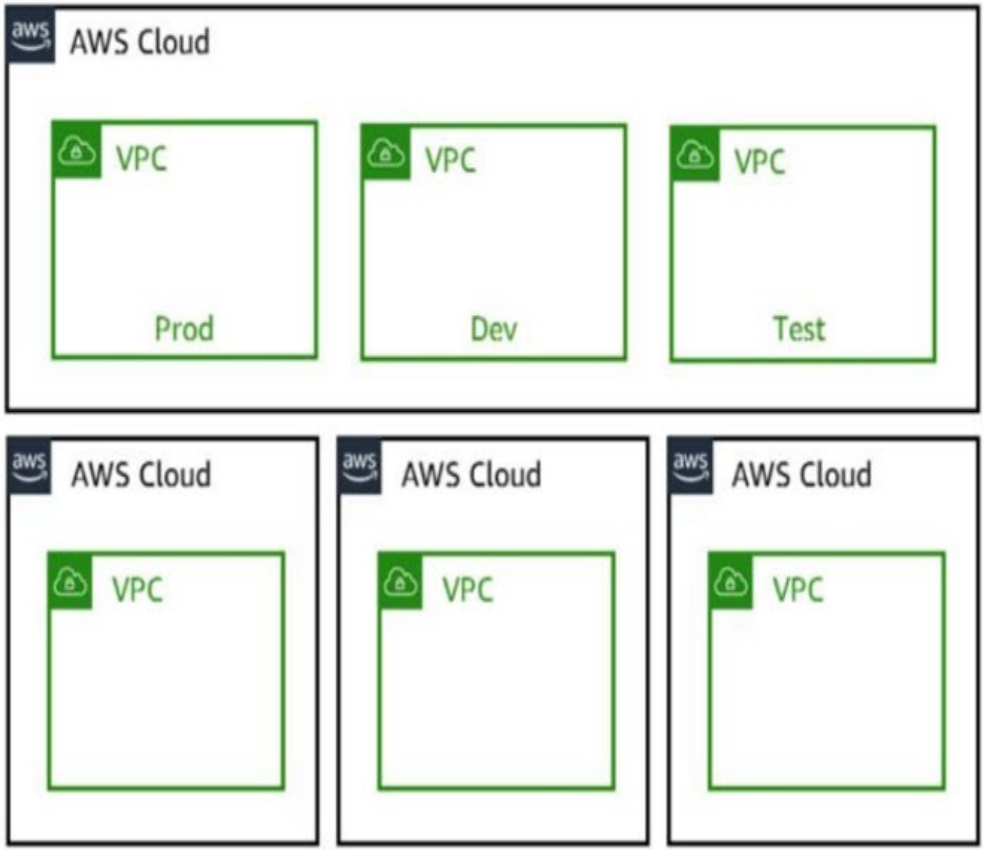
기본 Amazon VPC

- 기본 Amazon VPC는 계정 생성 시 프로비저닝됩니다.
- 이러한 VPC에서는 AWS 리소스가 즉시 시작됩니다.
- 리전당 여러 가용 영역에 걸쳐 있습니다.
- 고객이 소유하고 제어합니다.



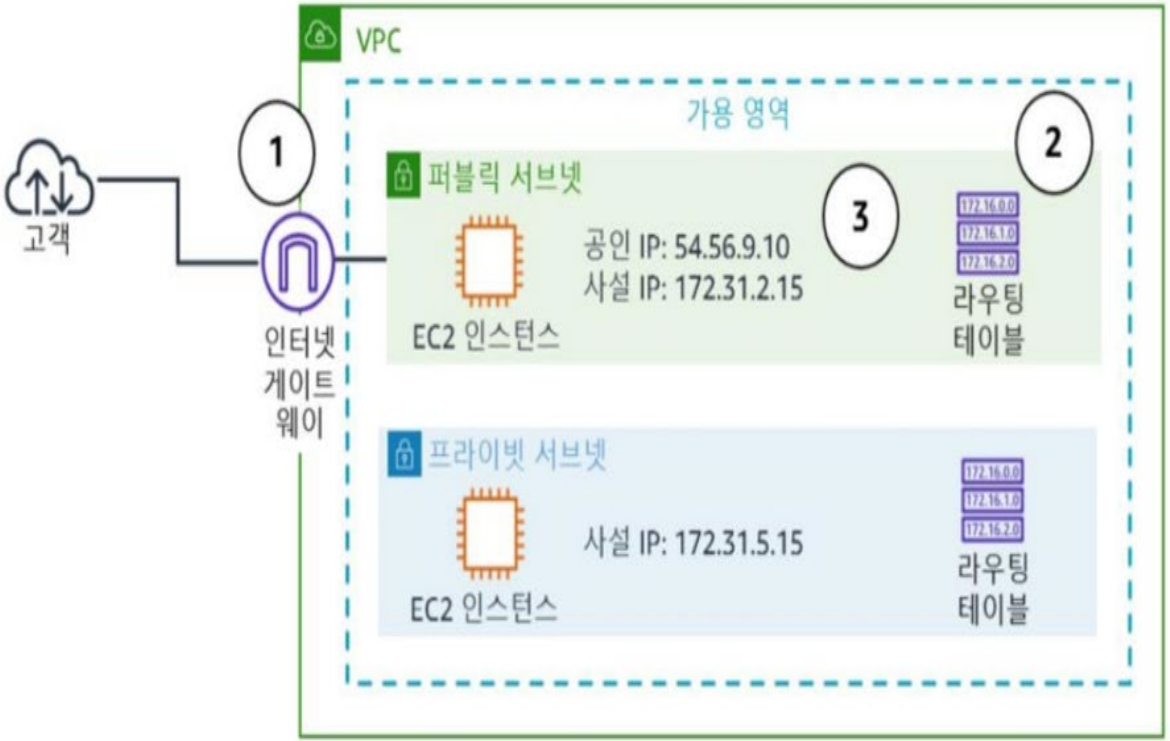
다중 VPC 구현의 장점

- 다중 VPC는 워크로드의 논리적 격리를 생성합니다.
- 보안 강화를 위해 VPC를 다중 계정으로 배포할 수 있습니다.



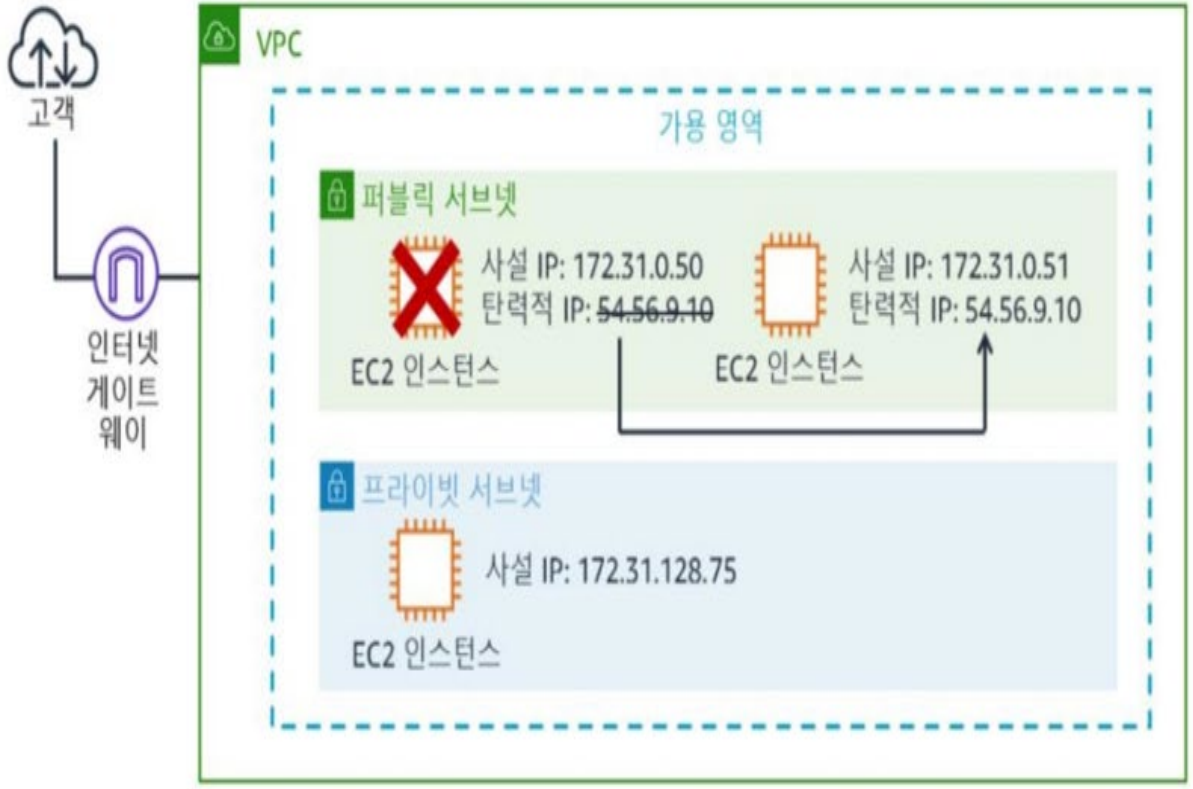
단일 VPC내에서 인스턴스를 공개접근 가능하게 설정

1. 인터넷 게이트웨이를 생성하려 VPC에 연결합니다.
2. 퍼블릭 라우팅 테이블을 업데이트합니다.
3. EC2 인스턴스에 공인 IP 주소를 할당합니다.



Elastic IP

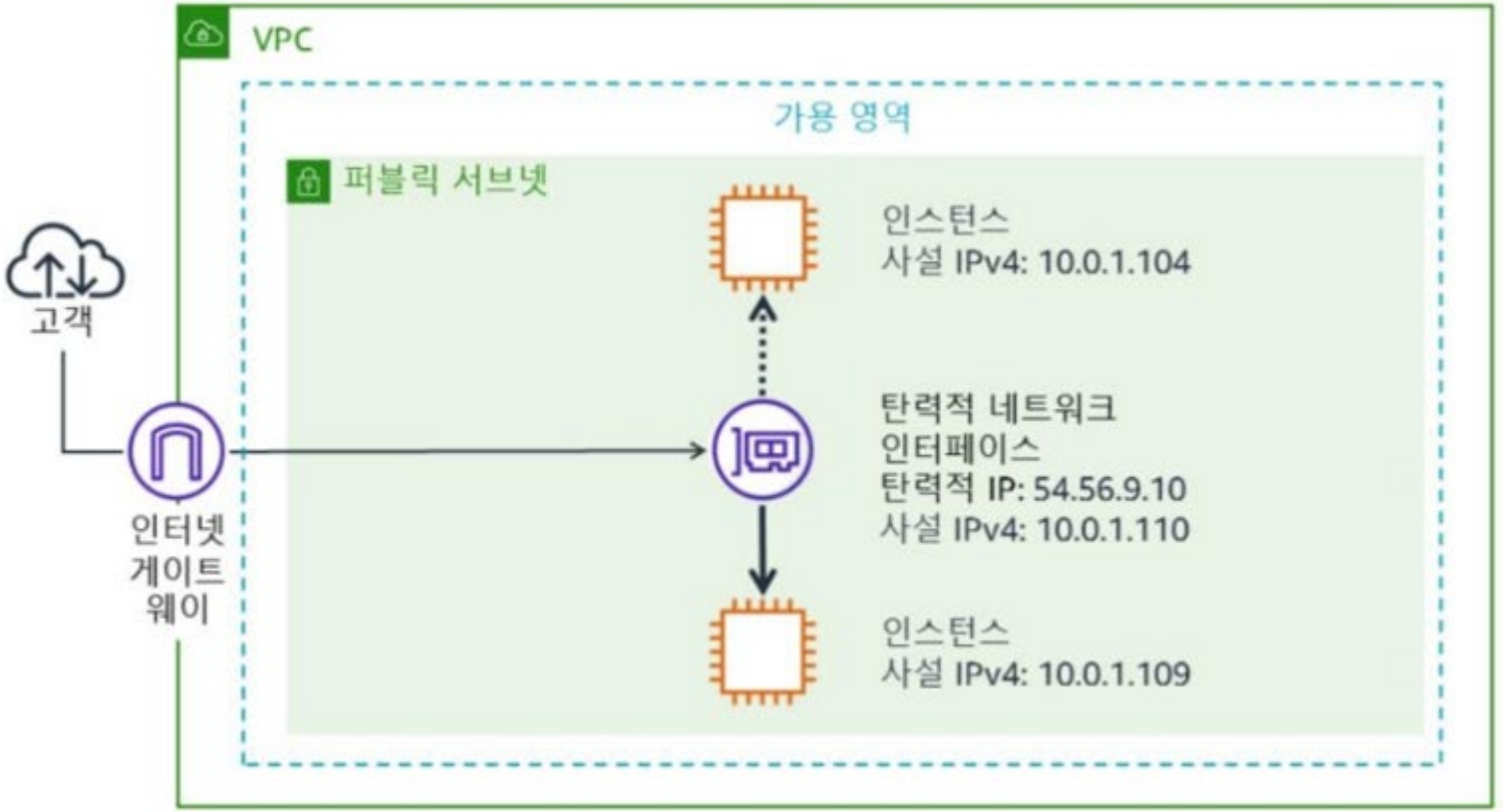
- 탄력적 IP 주소는 인스턴스 또는 네트워크 인터페이스와의 연결을 허용합니다.
- 재연결 즉시 새 트래픽을 디렉션할 수 있습니다.
- 리전당 5개로 제한됩니다.
- BYOIP(Bring Your Own IP)를 지원합니다.



Elastic Network Interface

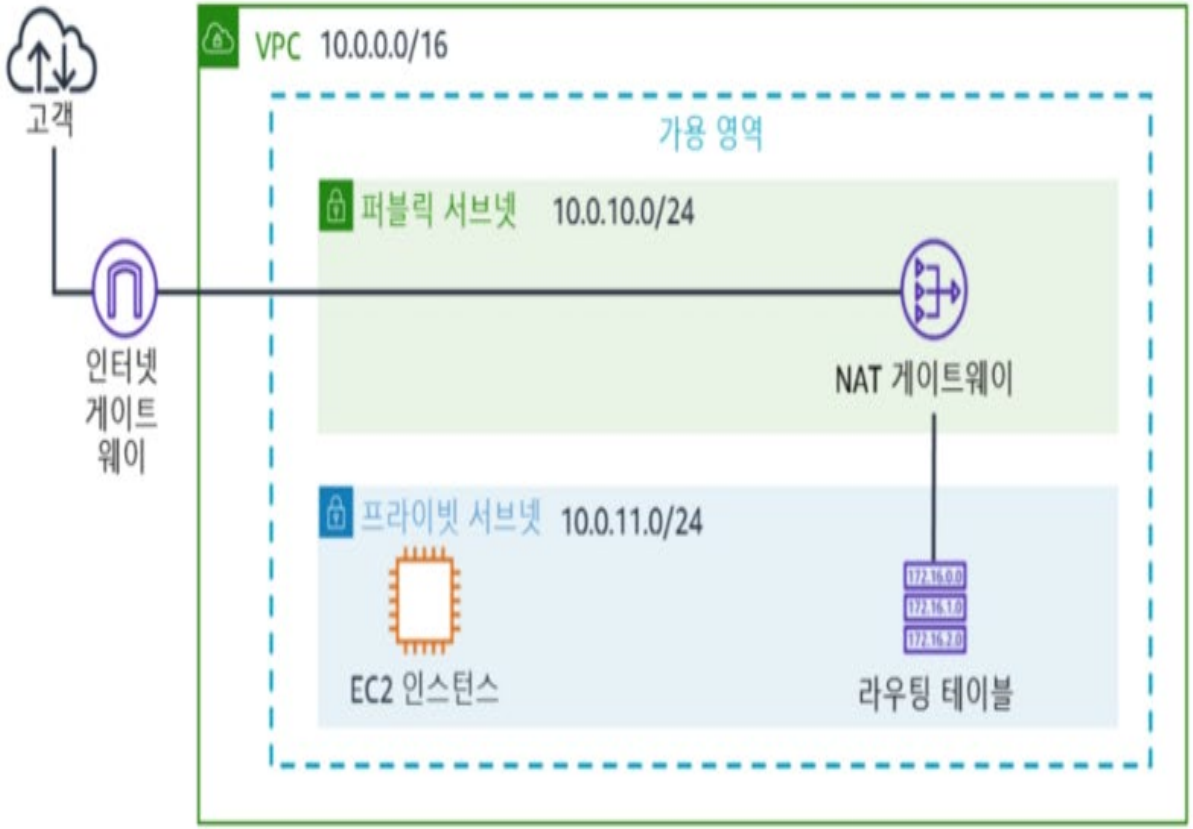
탄력적 네트워크 인터페이스는 다음을 지원하는 가상 네트워크 인터페이스입니다.

- 동일한 가용 영역의 리소스 간에 이동이 가능
- 사설 IP 주소, 탄력적 IP 주소 및 Mac 주소를 유지 관리



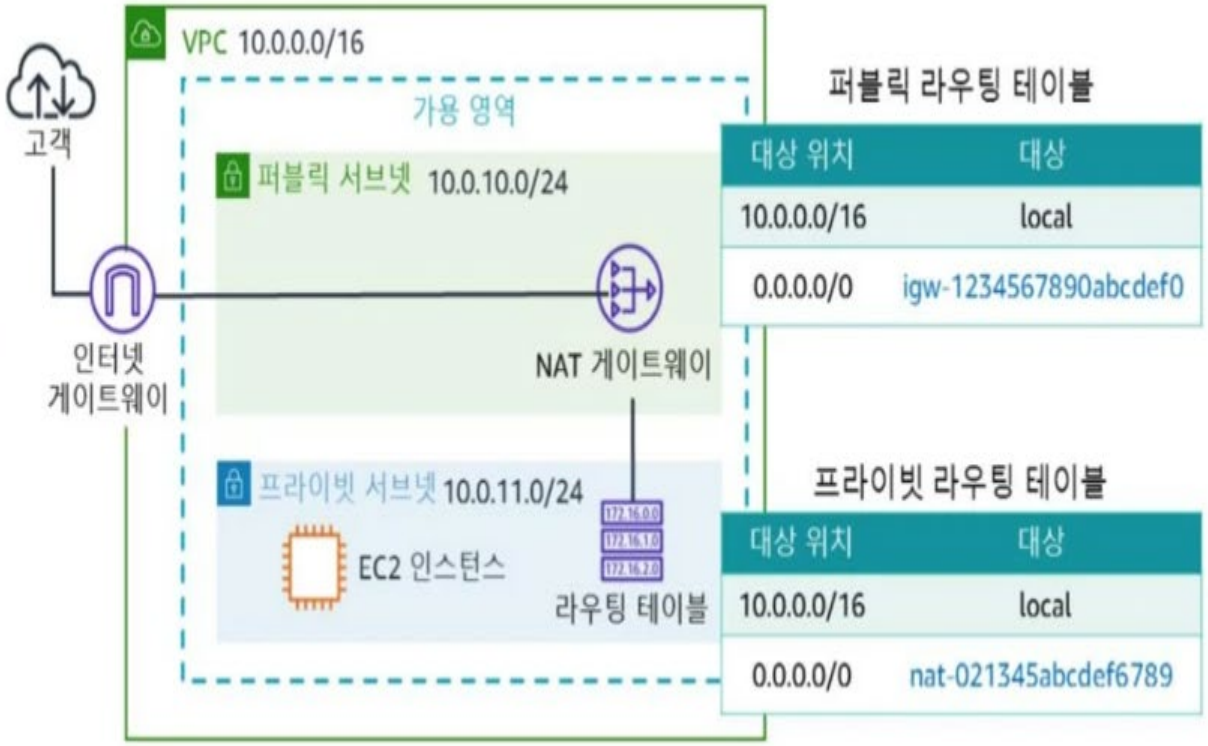
NAT (Network Address Translation)

- NAT는 프라이빗 서브넷의 인스턴스가 인터넷 또는 다른 AWS 서비스로의 아웃바운드 트래픽을 전송할 수 있도록 합니다.
- NAT 프로세스에 대한 제어를 강화하려면 Amazon EC2를 사용하여 자체 NAT 인스턴스를 생성합니다.



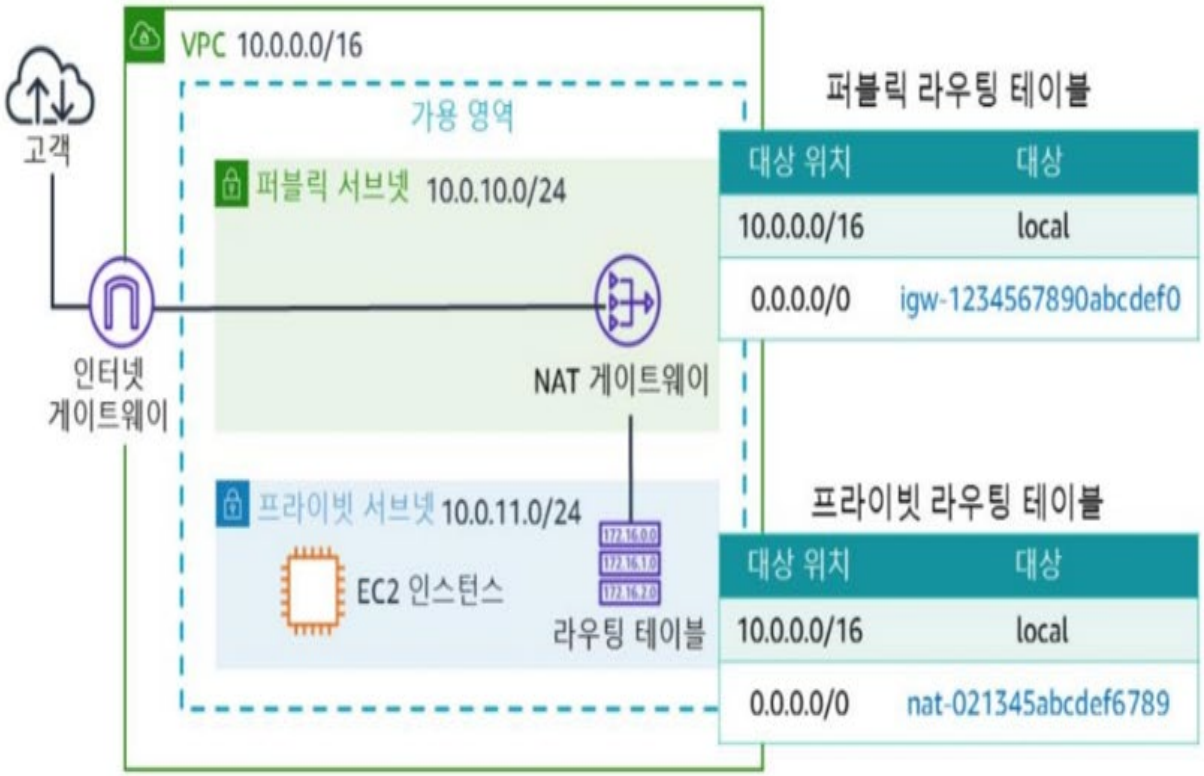
NAT Gateway

- 퍼블릭 서브넷용 라우팅 테이블은 모든 인터넷 트래픽을 인터넷 게이트웨이로 보냅니다.
- 프라이빗 서브넷용 라우팅 테이블은 모든 IPv4 인터넷 트래픽을 NAT 게이트웨이로 보냅니다.
- NAT 게이트웨이는 탄력적 IP 주소를 프라이빗 서브넷으로부터의 트래픽에 대한 소스 IP로 사용합니다.



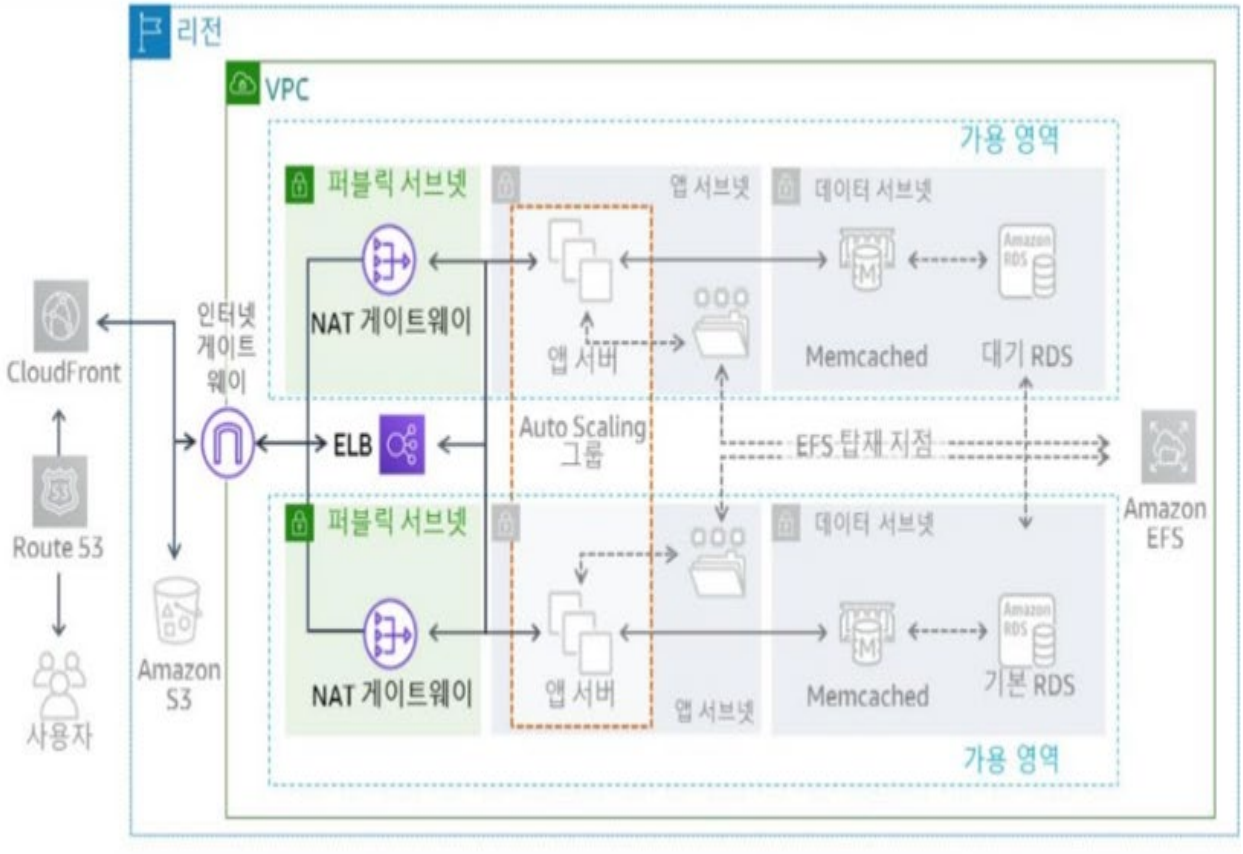
사설 서브넷을 인터넷에 연결

- 프라이빗 서브넷의 인스턴스가 인터넷 또는 다른 AWS 서비스로의 아웃바운드 트래픽을 시작할 수 있습니다.
- AWS에 의해 관리되는 NAT 게이트웨이는 프라이빗 인스턴스가 인터넷에서 인바운드 트래픽을 수신하는 것을 차단합니다.



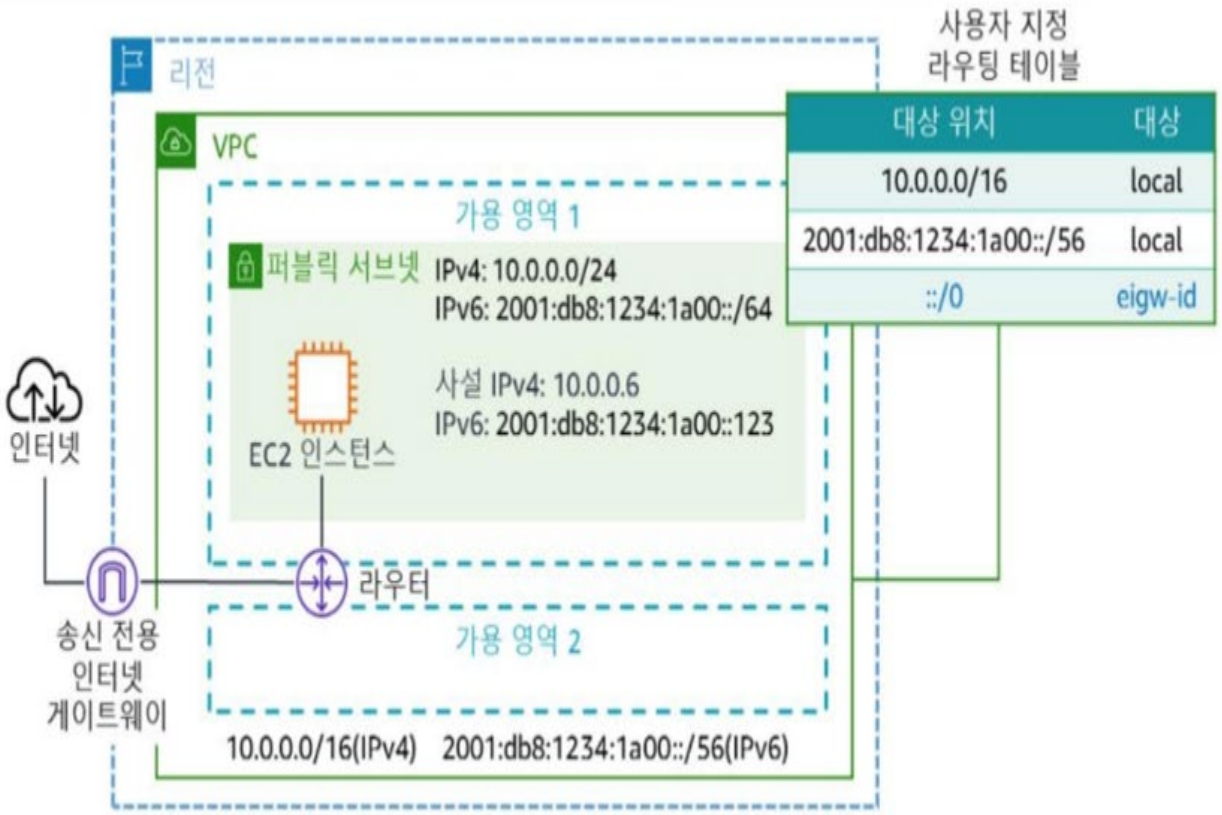
여러 가용 영역에 VPC배포

- 여러 가용 영역에 VPC를 배포하여 고가용성을 달성합니다.
- 각 가용 영역에서 서브넷을 생성합니다.
- 각 가용 영역에 리소스를 배포합니다.
- 로드 밸런서를 사용하여 가용 영역 간에 트래픽을 분산합니다.

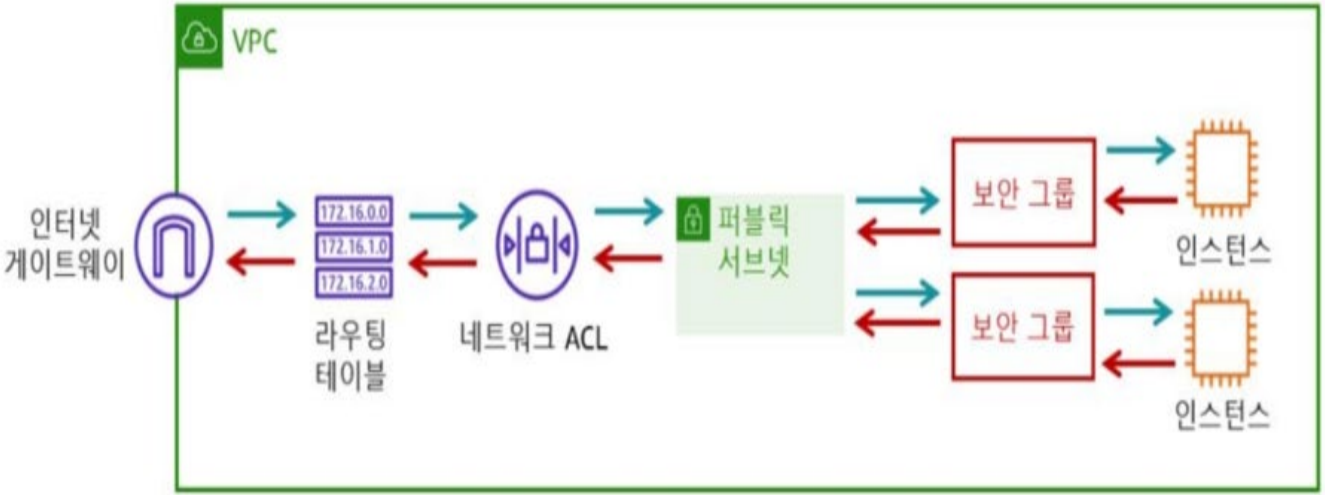


송신 전용 인터넷 게이트웨이

- 송신 전용 인터넷 게이트웨이는 IPv6 인스턴스를 통해 통신하는 VPC 구성 요소입니다.
- 인터넷에서 시작하는 통신을 차단합니다.

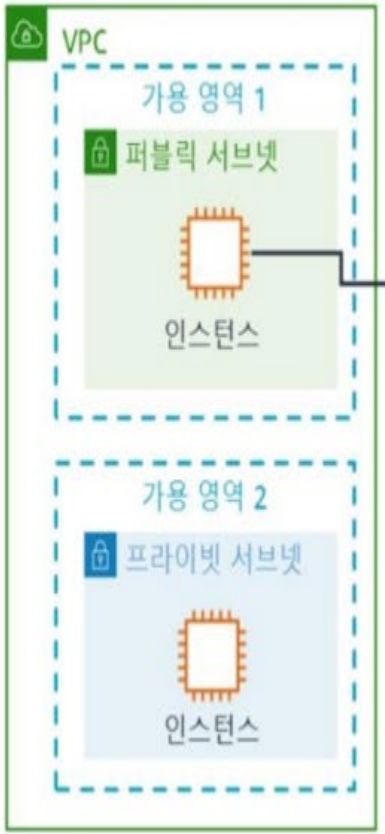


VPC 심층 방어


VPC
인터넷
게이트웨이
172.16.0.0
172.16.1.0
172.16.2.0
라우팅
테이블
네트워크 ACL
퍼블릭
서브넷
보안 그룹
보안 그룹
인스턴스
인스턴스

네트워크 ACL

- 네트워크 ACL은 서브넷 경계에서 방화벽 역할을 합니다.
- 기본적으로 모든 인바운드 및 아웃바운드 트래픽을 허용합니다.
- 상태 비저장이므로 모든 트래픽에 대한 명시적인 규칙이 필요합니다.



nacl-MyNACL1

인바운드

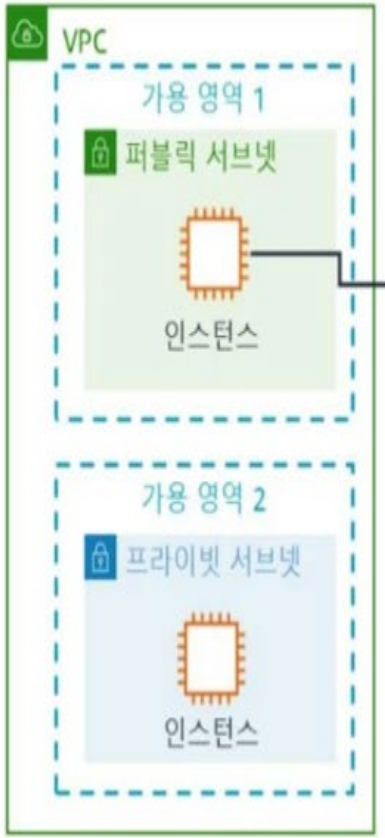
규칙 #	유형	프로토콜	포트 범위	소스	허용 또는 거부
100	HTTP	TCP	80	0.0.0.0/0	허용
101	HTTPS	TCP	443	0.0.0.0/0	허용
*	모든 트래픽	모두	모두	0.0.0.0/0	거부

아웃바운드

규칙 #	유형	프로토콜	포트 범위	대상 위치	허용 또는 거부
100	사용자 지정 TCP 규칙	TCP	1024-65535	0.0.0.0/0	허용
*	모든 트래픽	모두	모두	0.0.0.0/0	거부

네트워크 ACL 규칙

- 특정 보안 요구 사항에서만 권장됩니다.
- 허용 및 거부 규칙이 있습니다.
- 규칙은 번호가 가장 낮은 규칙부터 평가됩니다.



nacl-MyNACL1

인바운드

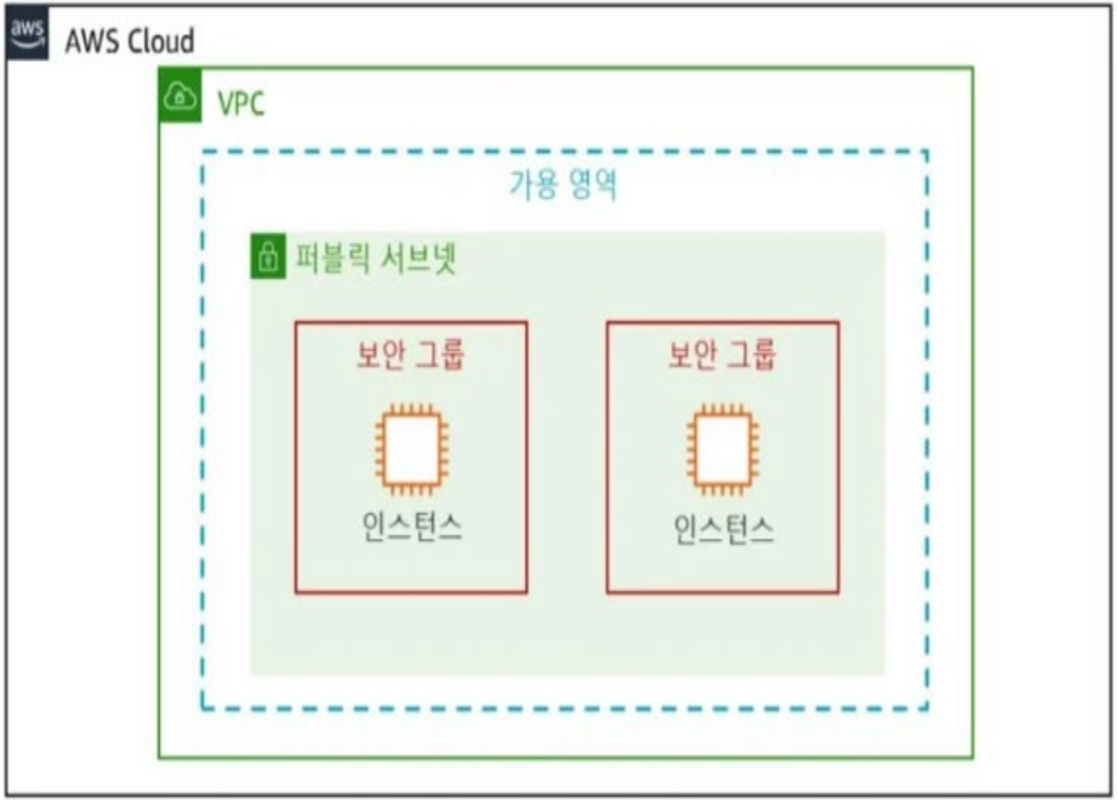
규칙 #	유형	프로토콜	포트 범위	소스	허용 또는 거부
100	HTTP	TCP	80	0.0.0.0/0	허용
101	HTTPS	TCP	443	0.0.0.0/0	허용
*	모든 트래픽	모두	모두	0.0.0.0/0	거부

아웃바운드

규칙 #	유형	프로토콜	포트 범위	대상 위치	허용 또는 거부
100	사용자 지정 TCP 규칙	TCP	1024-65535	0.0.0.0/0	허용
*	모든 트래픽	모두	모두	0.0.0.0/0	거부

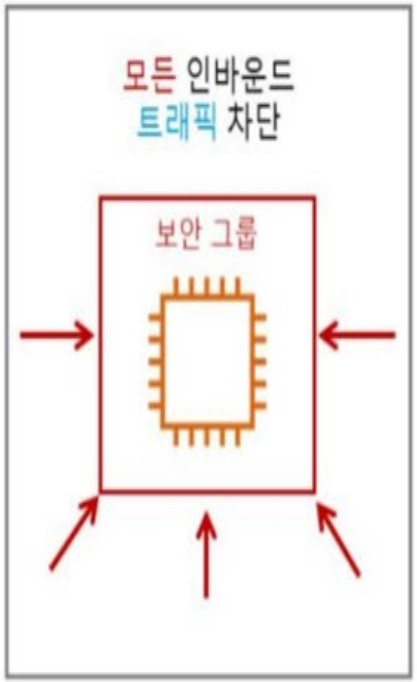
보안그룹

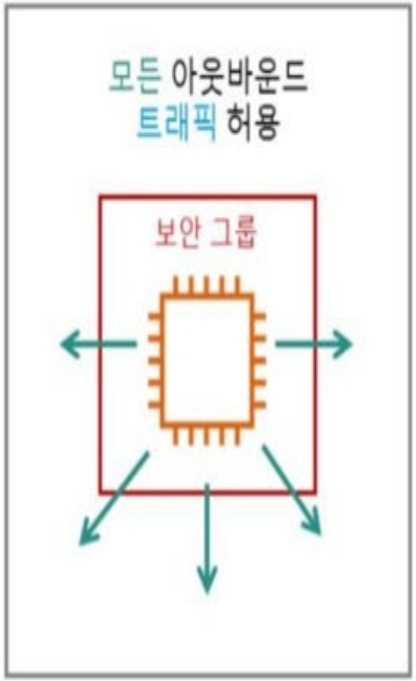
- 보안 그룹은 AWS 리소스에 대한 인바운드 및 아웃바운드 트래픽을 제어하는 가상 방화벽입니다.
- IP 프로토콜, 포트 또는 IP 주소를 기반으로 트래픽을 허용합니다.
- 상태 기반 규칙을 사용합니다.



기본보안그룹과 사용자 정의 보안 그룹

- 기본 VPC 내의 보안 그룹은 모든 트래픽을 허용합니다.
- 새 보안 그룹은 인바운드 규칙이 없고 아웃바운드 트래픽을 허용합니다.





사용자 지정 보안 그룹 규칙

인바운드

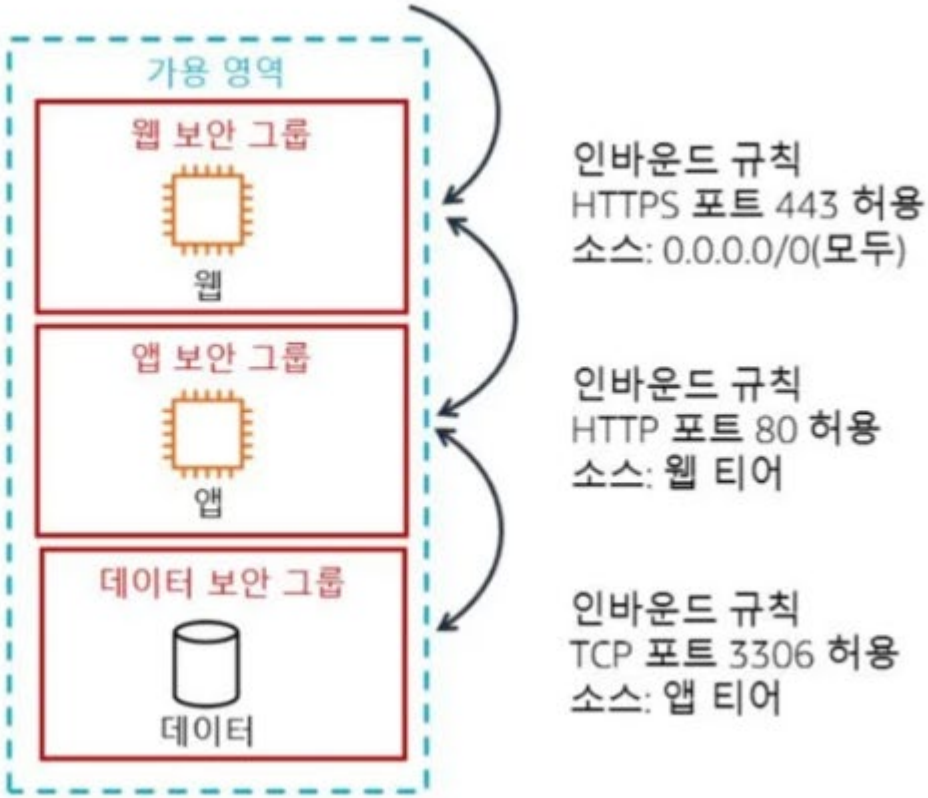
소스	프로토콜	포트	설명
0.0.0.0/0	TCP	80	모든 IPv4 주소로부터의 인바운드 HTTP 액세스를 허용
0.0.0.0/0	TCP	443	모든 인바운드 HTTPS 트래픽을 허용

아웃바운드

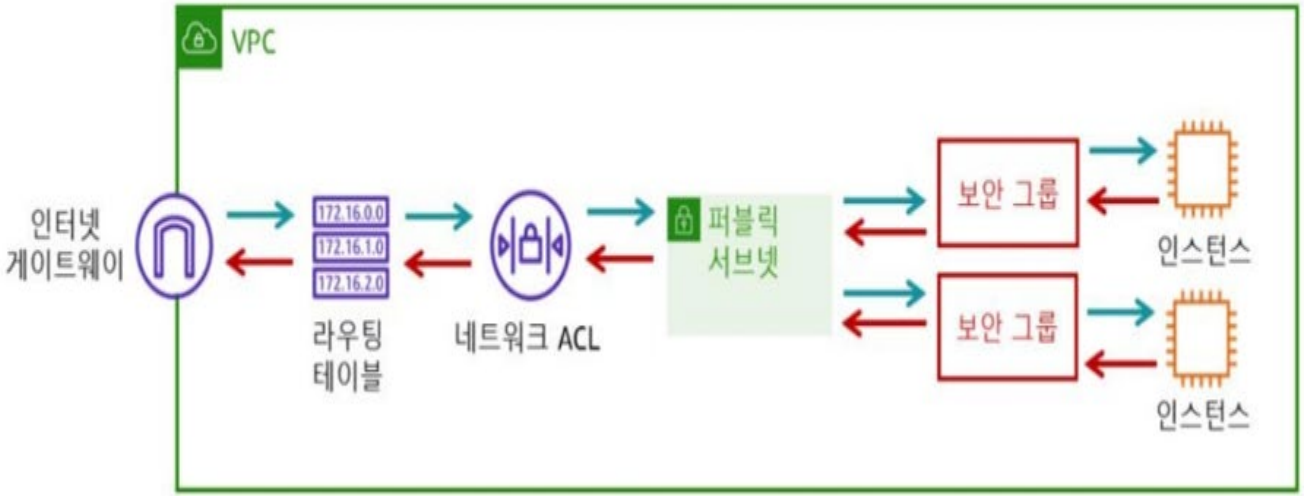
대상 위치	프로토콜	포트	설명
DB 서버의 SG ID	TCP	1433	지정된 보안 그룹의 인스턴스에 대한 아웃바운드 Microsoft SQL Server 액세스를 허용
MySQL 서버의 SG ID	TCP	3306	지정된 보안 그룹에 있는 인스턴스에 대한 아웃바운드 MySQL 액세스를 허용

보안 그룹 연결

- 인바운드와 아웃바운드 규칙은 트래픽이 상위 티어에서 하위 티어로 흐르도록 허용합니다.
- 보안 그룹은 서브넷 전체에서 보안 위반을 방지하는 방화벽 역할을 합니다.



다중 방어 계층이 있는 인프라 구조

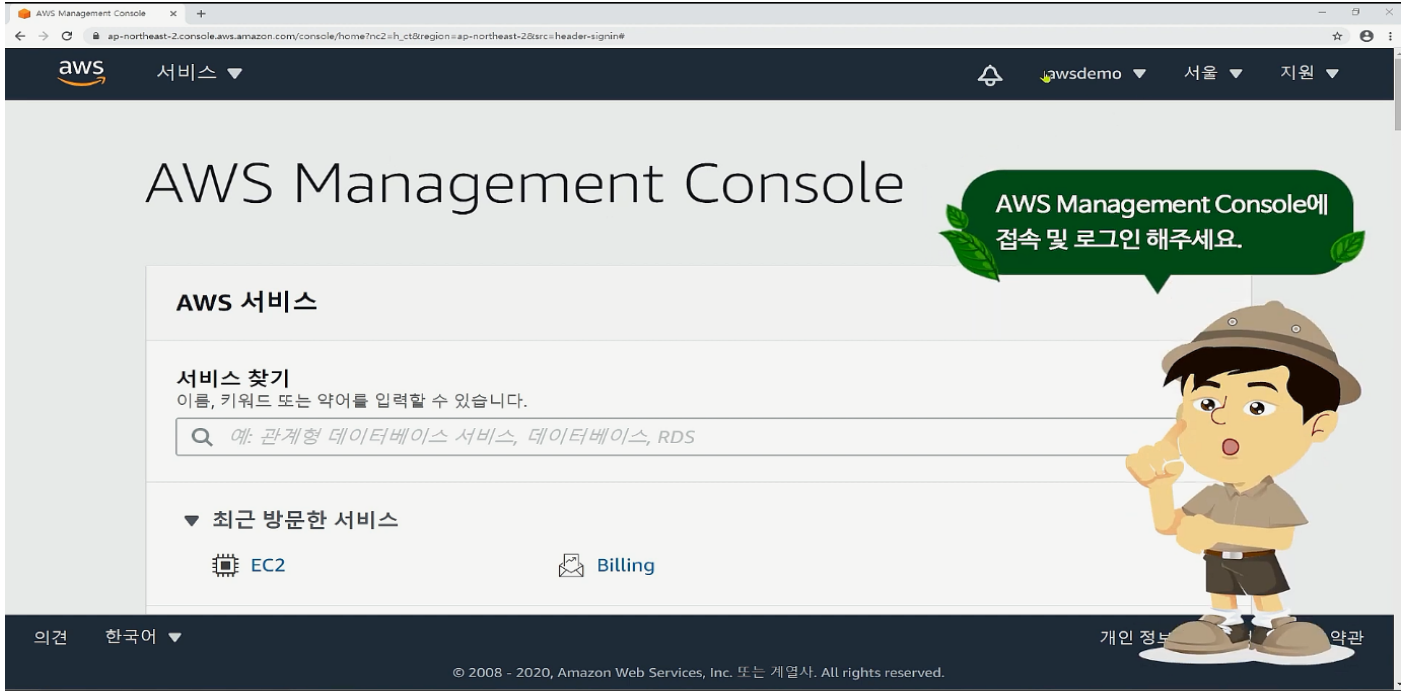


보안 그룹과 네트워크 ACL 비교

보안 그룹	네트워크 ACL
탄력적 네트워크 인터페이스에 연결되고 하이퍼바이저에서 구현됨	서브넷에 연결되고 네트워크에 구현됨
허용 규칙만 지원	허용 및 거부 규칙 지원
상태 기반 방화벽	상태 비저장 방화벽
모든 규칙은 트래픽 허용 여부를 결정하기 전에 평가됨	모든 규칙은 트래픽 허용 여부를 결정할 때 순서대로 처리됨
인스턴스에 수동으로 지정해야 함	인스턴스가 서브넷에 추가될 때 자동으로 적용됨
통신을 허용하려면 구성이 필요	기본적으로 통신 허용

VPC 서비스 실습 시연

https://rumble.com/v33ukie-aws-vpc-2023.html



Q1

VPC의 핵심개념을 설명한 것 중 틀린 것 하나를 고르시오

가.서브넷 -VPC의 IP 주소 범위

나.라우팅 테이블 -네트워크 트래픽을 전달할 위치를 결정하는 데 사용되는 라우팅이라는 규칙 집합

다.인터넷 게이트웨이-VPC의 리소스와 인터넷 간의 통신을 활성화하기 위해 VPC에 연결하는 게이트웨이

라.VPC 로드밸런서-인터넷 게이트웨이, NAT 디바이스, VPN 연결 또는 AWS Direct Connect 연결을 필요로 하지 않고 PrivateLink 구동 지원 AWS 서비스 및 VPC 엔드포인트 서비스에 VPC를 비공개로 연결할 수 있음 VPC의 인스턴스는 서비스의 리소스와 통신하는 데 퍼블릭 IP 주소를 필요로 하지 않음VPC와 기타 서비스 간의 트래픽은 Amazon 네트워크를 벗어나지 않음

A

라 (VPC 엔드포인트를 설명한 것이며 VPC 로드밸런서는 없음)

Q2

아래 괄호에 들어갈 숫자는 몇개인가?

VPC생성시 16비트의 CIDR별로 구성을 하게 되면 호스트 ID가 16 비트를 사용할 수 있기 때문에 최대 ( )개의 호스트를 연결할 수 있는 사설네트워크를 작성할 수 있다.

A

약 6만 5천 개(2^16 ;65536개)

이상희 교사

AWS를 활용한 웹 서비스 구성하기

3주차 강의

1차수: AWS VPC 서비스

2차수: AWS IAM 서비스

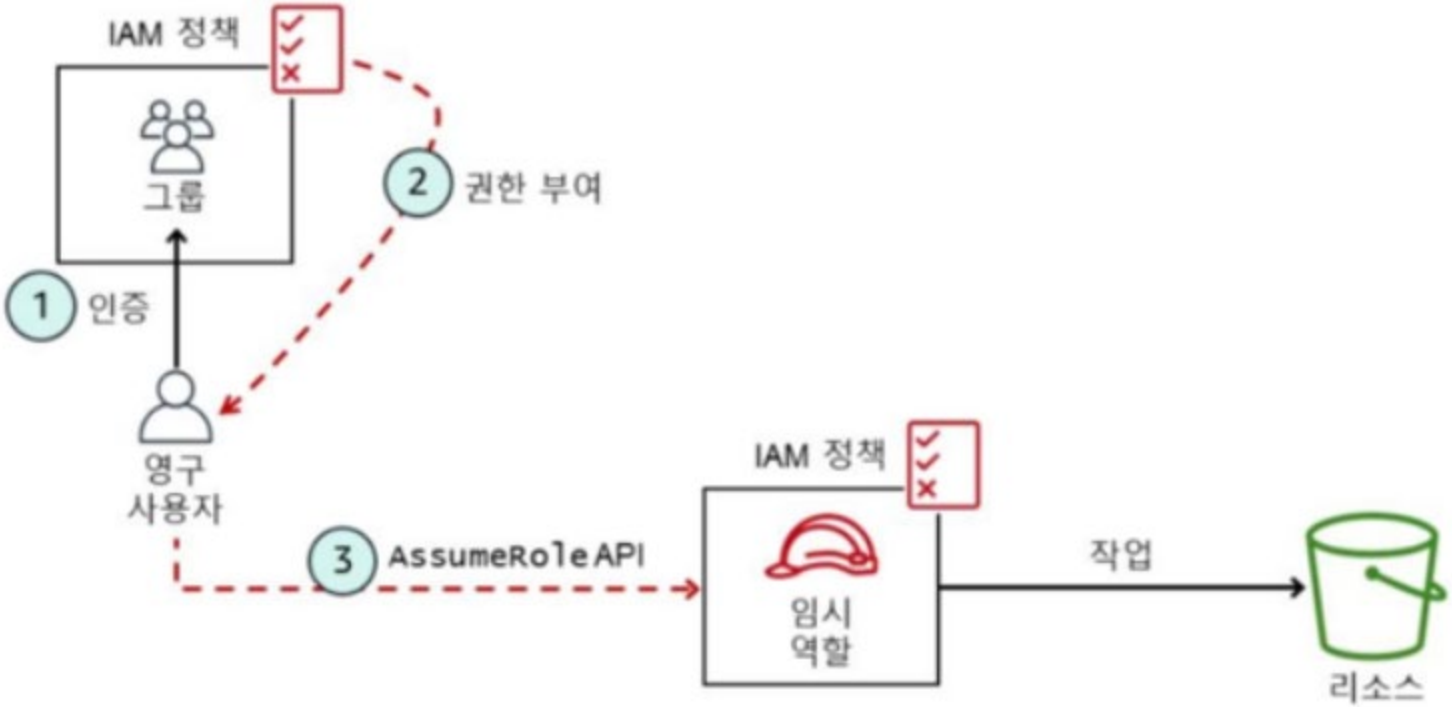
2차수 학습목표

- AWS 의 계정보안 서비스인 IAM을 이해 할 수 있다

2차수 학습내용

- IAM과IAM 사용자, 그룹 및 정책을 사용하여 계정보안을 적용하는 방법
- IAM을 검토
- IAM 보안주체가 될수있는것이 무엇인지 식별
- AWS 리소스의 계층적방어를 제공을 위한 자격증명기반정책 및 리소스기반 정책을 적용할 시기
- 정책의 구성요소

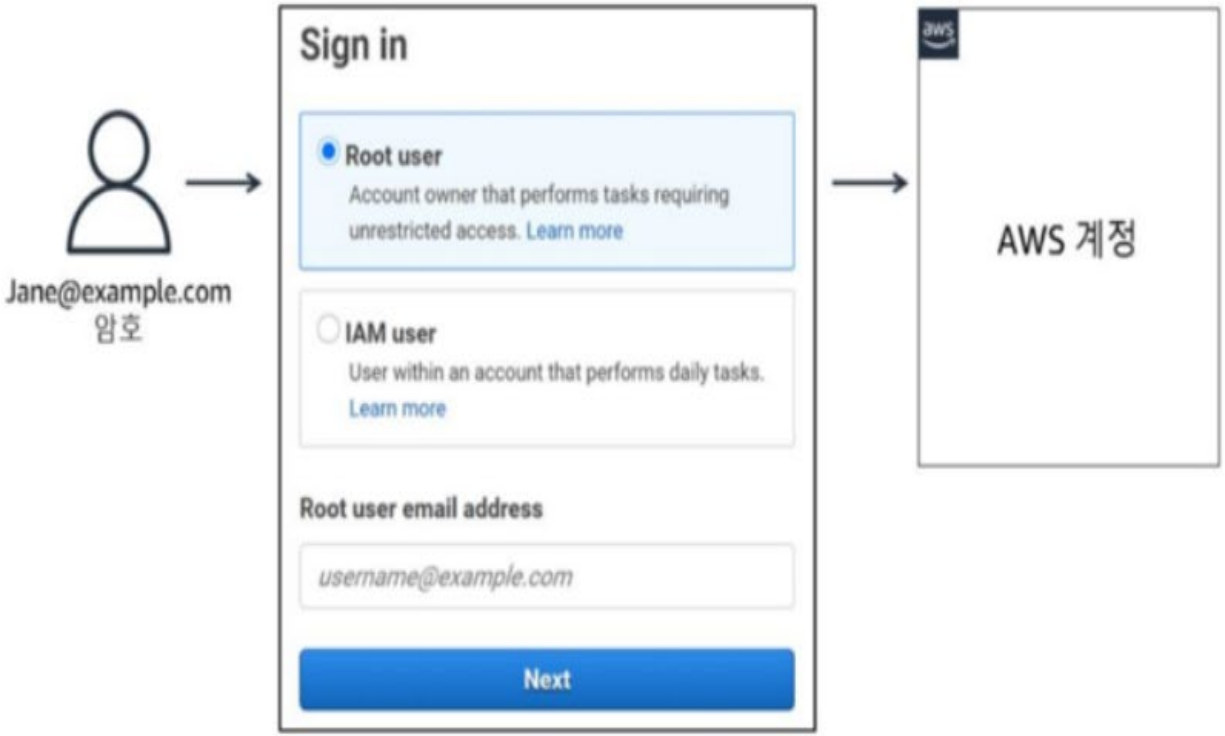
계정보안 솔루션



AWS계정 루트사용자

루트 사용자:

- AWS 서비스에 대한 전체 액세스 권한을 보유
- 단일 계정 모델에서 제한이 없음
- AWS와의 일상적인 상호 작용에 사용하면 안 됨



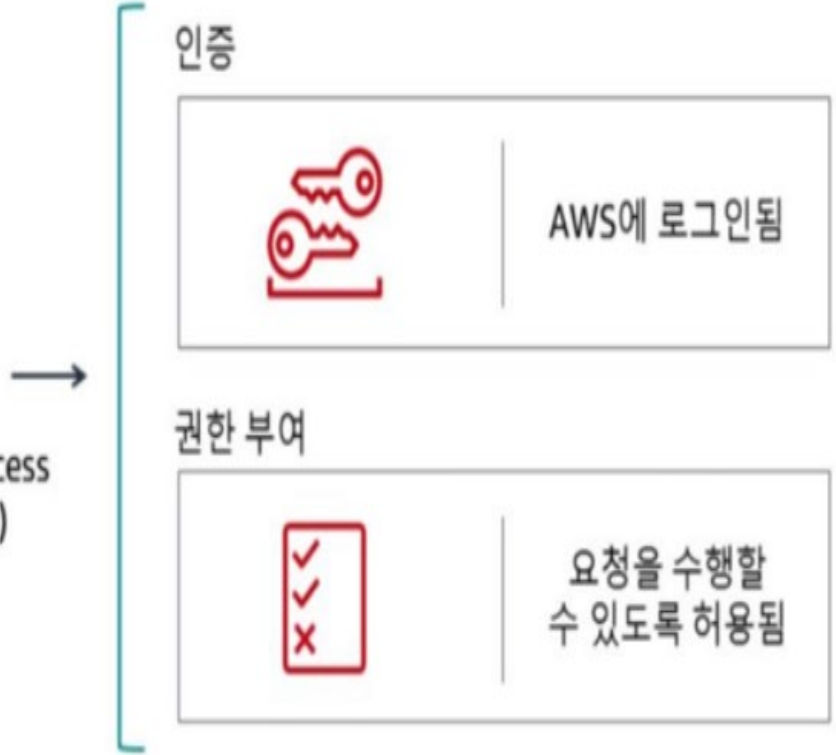
AWS 계정루트 사용자'(https://docs.aws.amazon.com/IAM/latest/UserGuide/id_root-user.html

IAM (Identity and Access Management)

IAM을 사용하여 다음을 수행합니다.

- 사용자, 그룹 및 역할을 생성하고 관리
- AWS 서비스 및 리소스에 대한 액세스를 관리
- 액세스 제어를 분석
- 회사 디렉터리와 통합

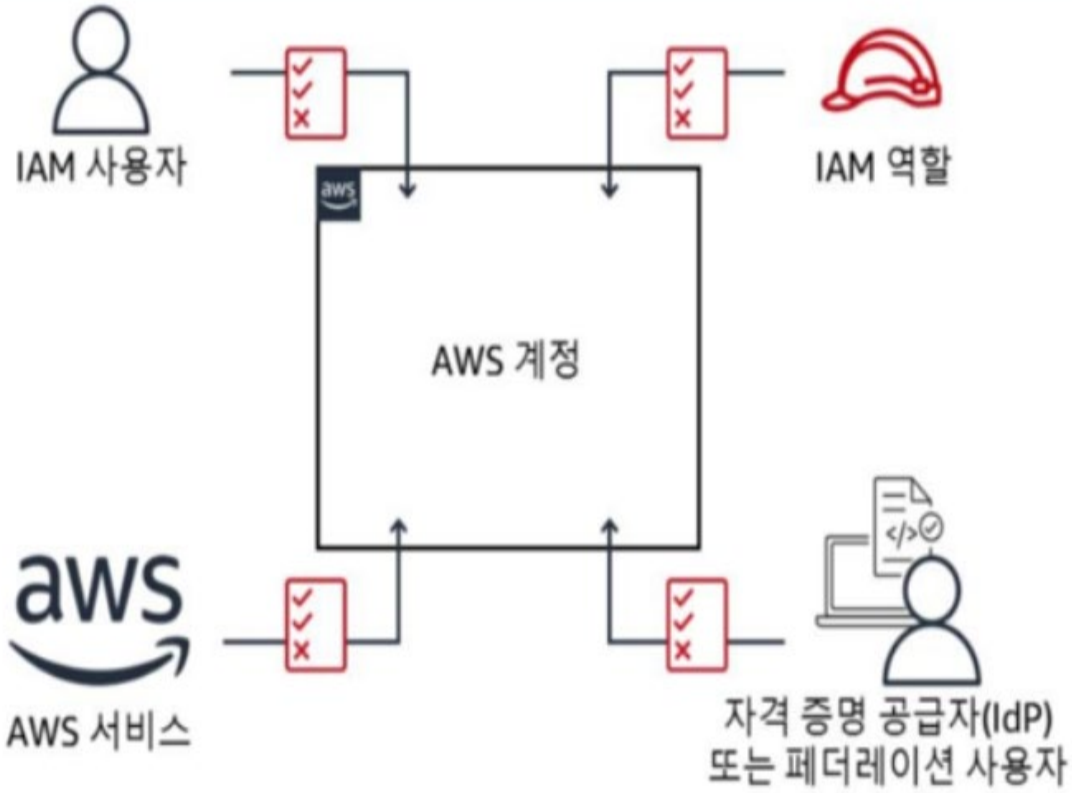
AWS Identity and Access Management(IAM)



보안주체

보안 주체:

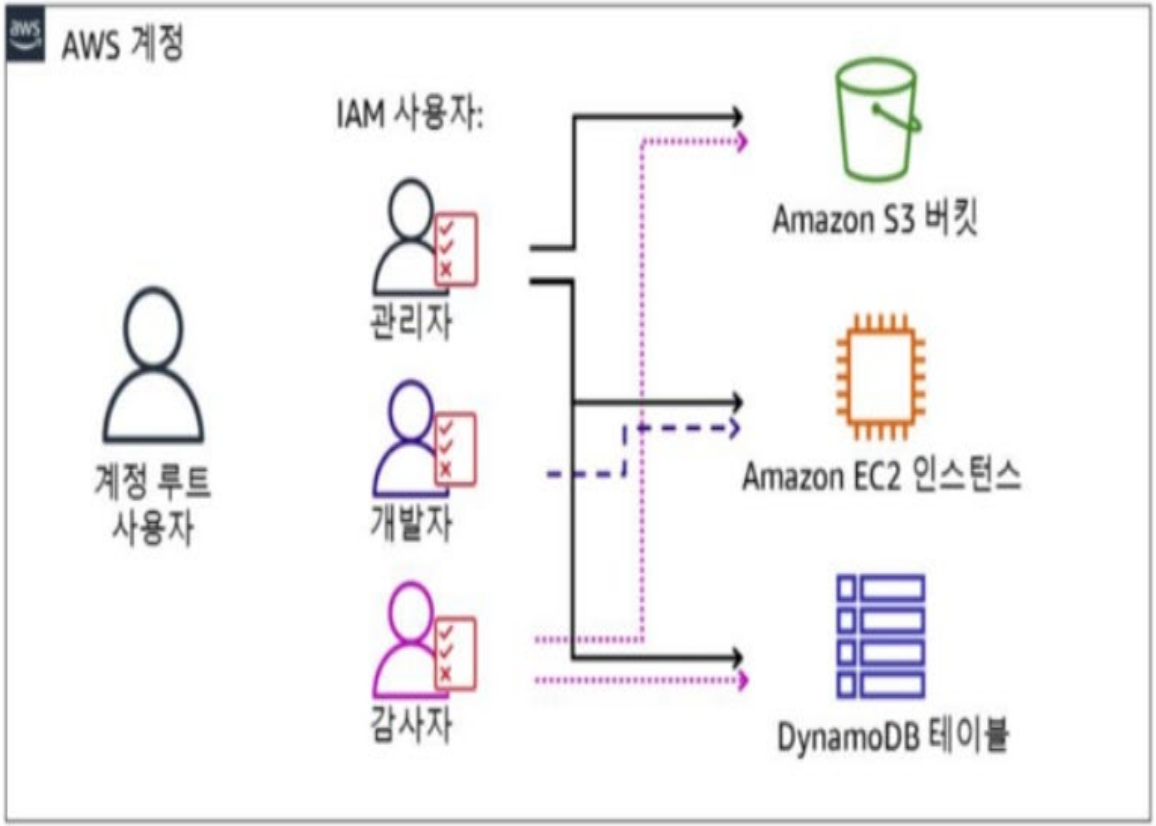
- AWS 리소스에 대한 작업을 요청할 수 있는 권한을 가진 엔터티
- 사용자 또는 서비스일 수 있음



IAM사용자

IAM 사용자는 AWS 계정 내의 사용자입니다.

- 각 사용자에게는 자체 보안 인증 정보가 있습니다.
- 사용자는 권한에 따라 특정 AWS 작업을 수행할 권한을 보유합니다.

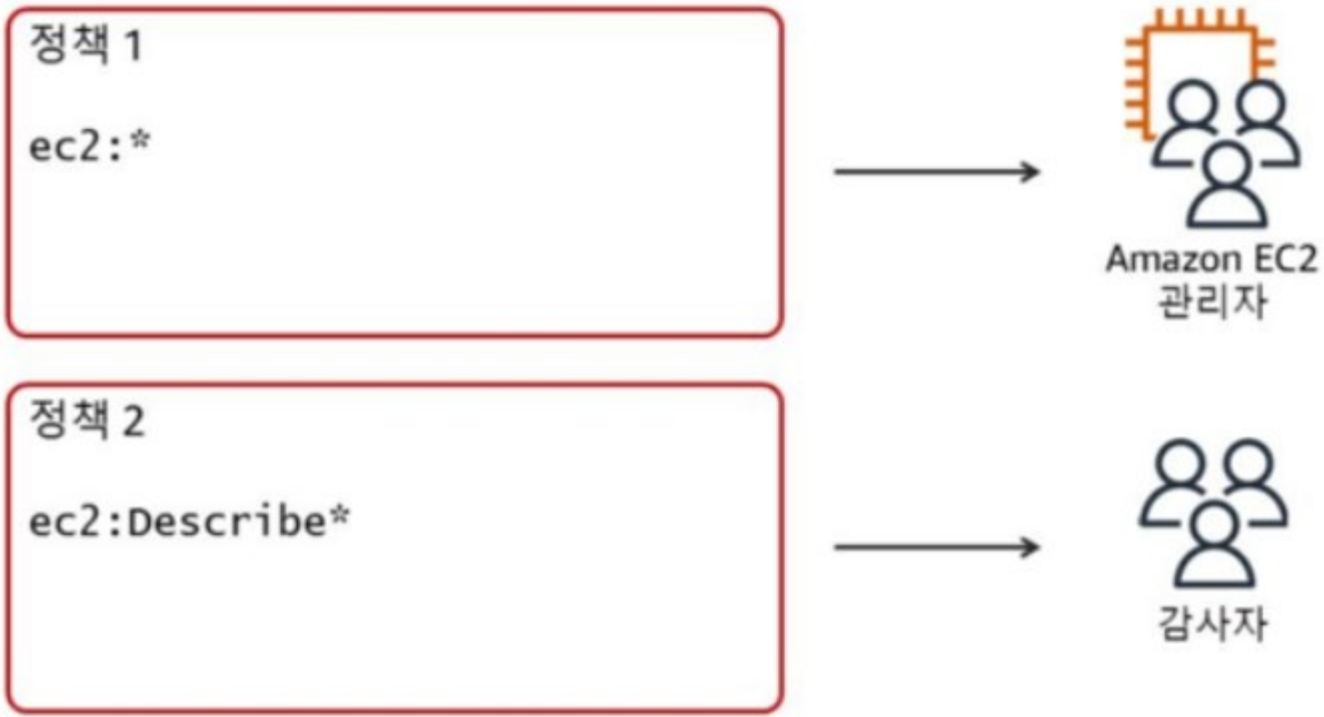


IAM 사용자'https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users.html

AWS API와 상호작용

IAM 사용자암호 관리
(https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_password s_admin-change-user.html)

다양한 권한세트 위임



Amazon EC2의IAM정책(https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-policies-for-amazon-ec2.html)

사용자인증정보 및 작동 방식

보안 인증 정보 유형	용도
루트(계정 소유자) 이메일 및 암호	계정 생성 및 해지(일상 작업용이 아님)
IAM 사용자 이름 및 암호	콘솔 액세스
액세스 키 ID 및 비밀 액세스 키	API 및 SDK를 통한 AWS CLI 및 프로그래밍 방식 요청
MFA	루트 및 IAM 사용자에 대해 활성화할 수 있는 추가 보안 계층

AWS 보안 인증정보 이해 및 얻기
(https://docs.aws.amazon.com/general/latest/gr/aws-sec-cred-types.html)

AWS CLI 또는 SDK를 사용한 인증

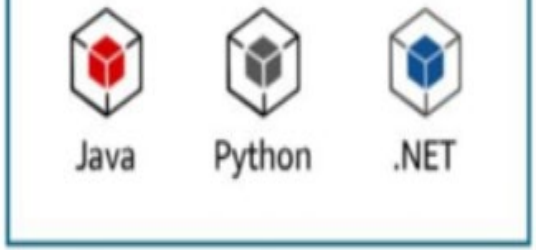
IAM
사용자

액세스 키 ID: AKIAIOSFODNN7EXAMPLE
비밀 액세스 키: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY

AWS CLI

```
$ aws configure
AWS Access Key ID [**********MPLE:
Default region name [ap-southeast-1]:
Default output format [json]:
```

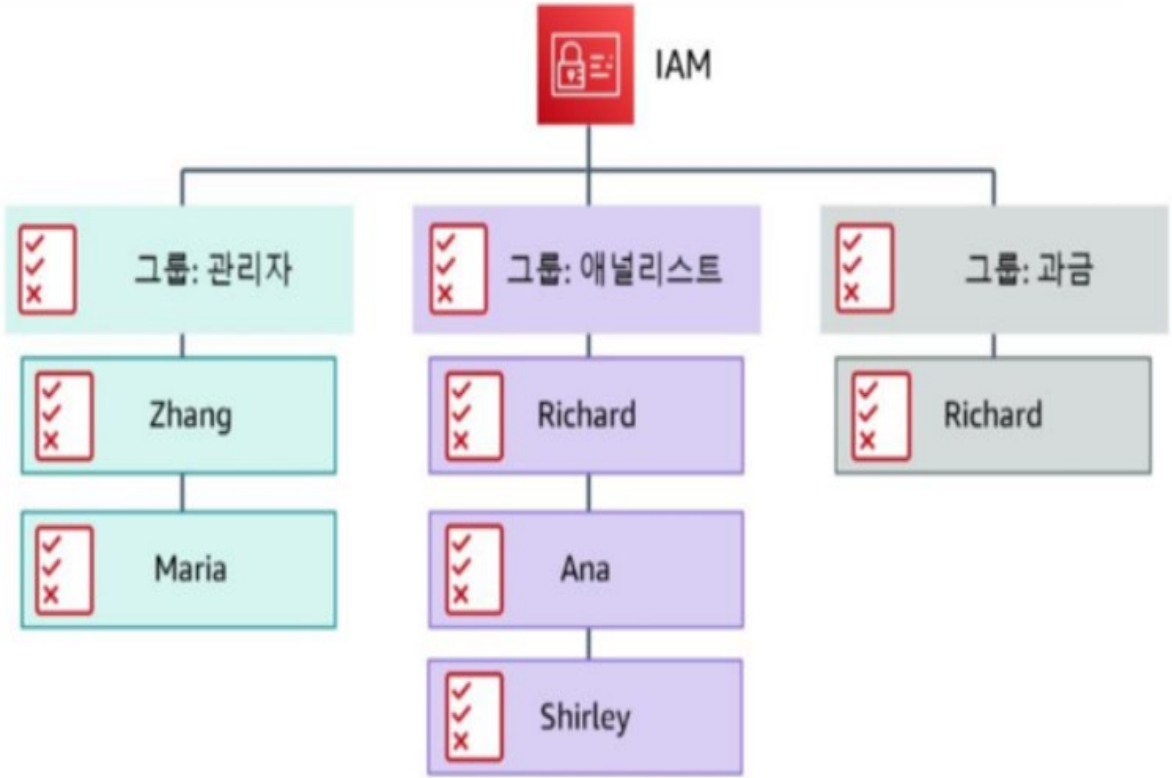
AWS SDK 및 API



AWS Command Line Interface(http://docs.aws.amazon.com/cli/latest/userguide/cli-chap-welcome.html)

IAM 사용자그룹

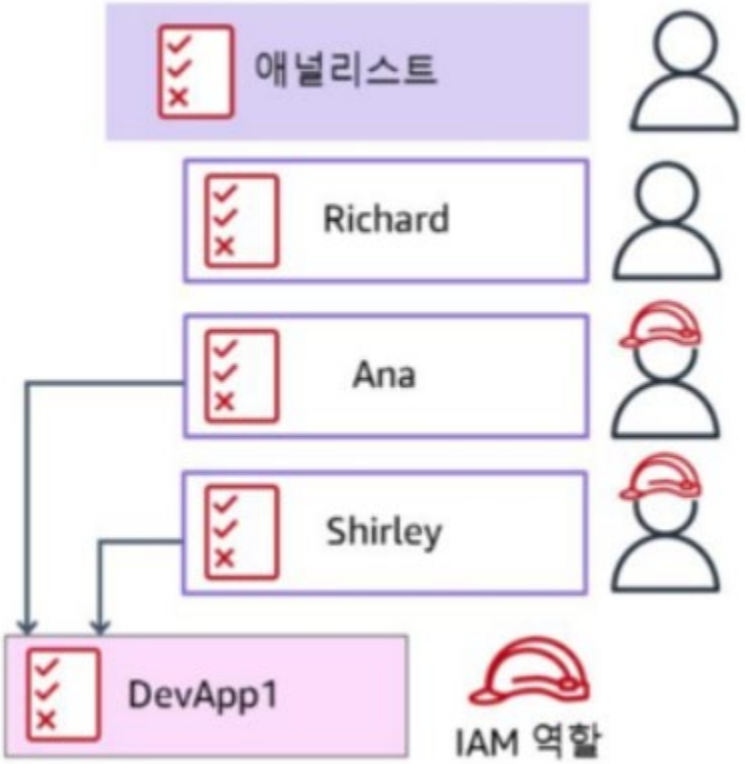
- IAM 사용자를 하나 이상의 IAM 사용자 그룹에 할당합니다.
- 해당 그룹의 모든 사용자에게 적용할 정책을 IAM 사용자 그룹에 연결합니다.



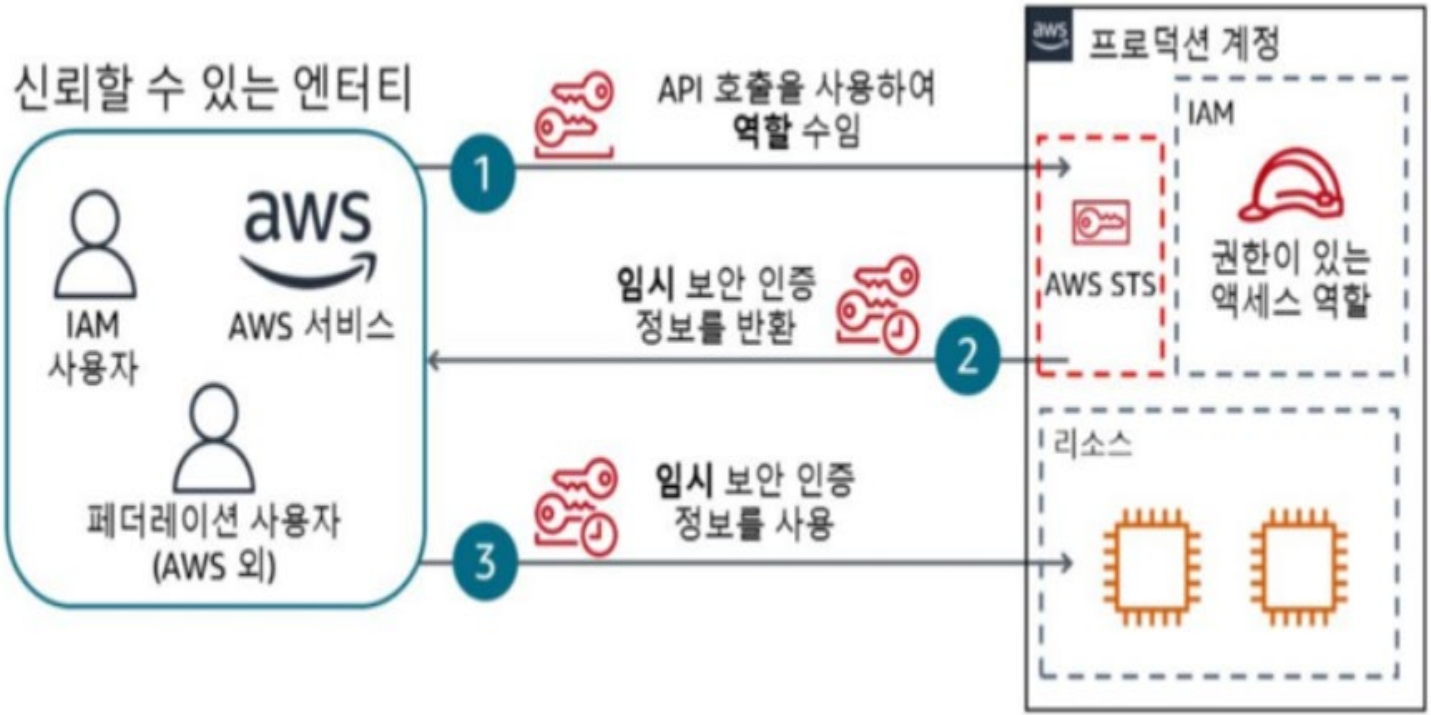
IAM 사용자 그룹 https://docs.aws.amazon.com/IAM/latest/UserGuide/id_groups.html

IAM 역할

- 권한을 특정 사용자 또는 서비스에 위임합니다.
- 사용자는 다른 사용자와 보안 인증 정보를 공유하지 않고 역할을 수임합니다.
- 권한은 수임한 역할에 따른 작업을 수행하는 동안만 유효합니다.

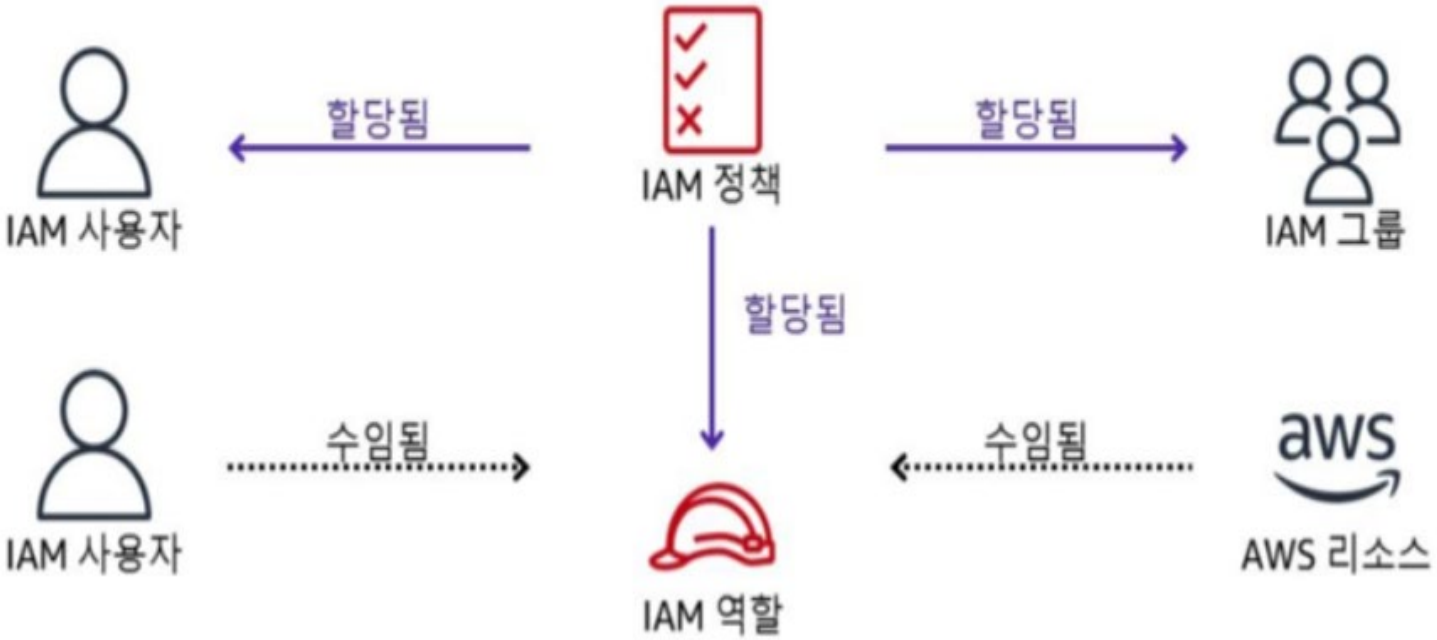


역할 수임



IAM 역할 사용(https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use.html)
AWS Security Token Service API 참조
(https://docs.aws.amazon.com/STS/latest/APIReference/Welcome.html)

IAM 정책 할당


IAM 사용자
할당됨
IAM 정책
할당됨
IAM 그룹
할당됨
IAM 사용자
수임됨
수임됨
aws
IAM 역할
AWS 리소스

역할 사용의 장점

IAM 역할은 AWS에 대한 제한된 sudo 액세스 권한이라고 생각하면 됩니다.

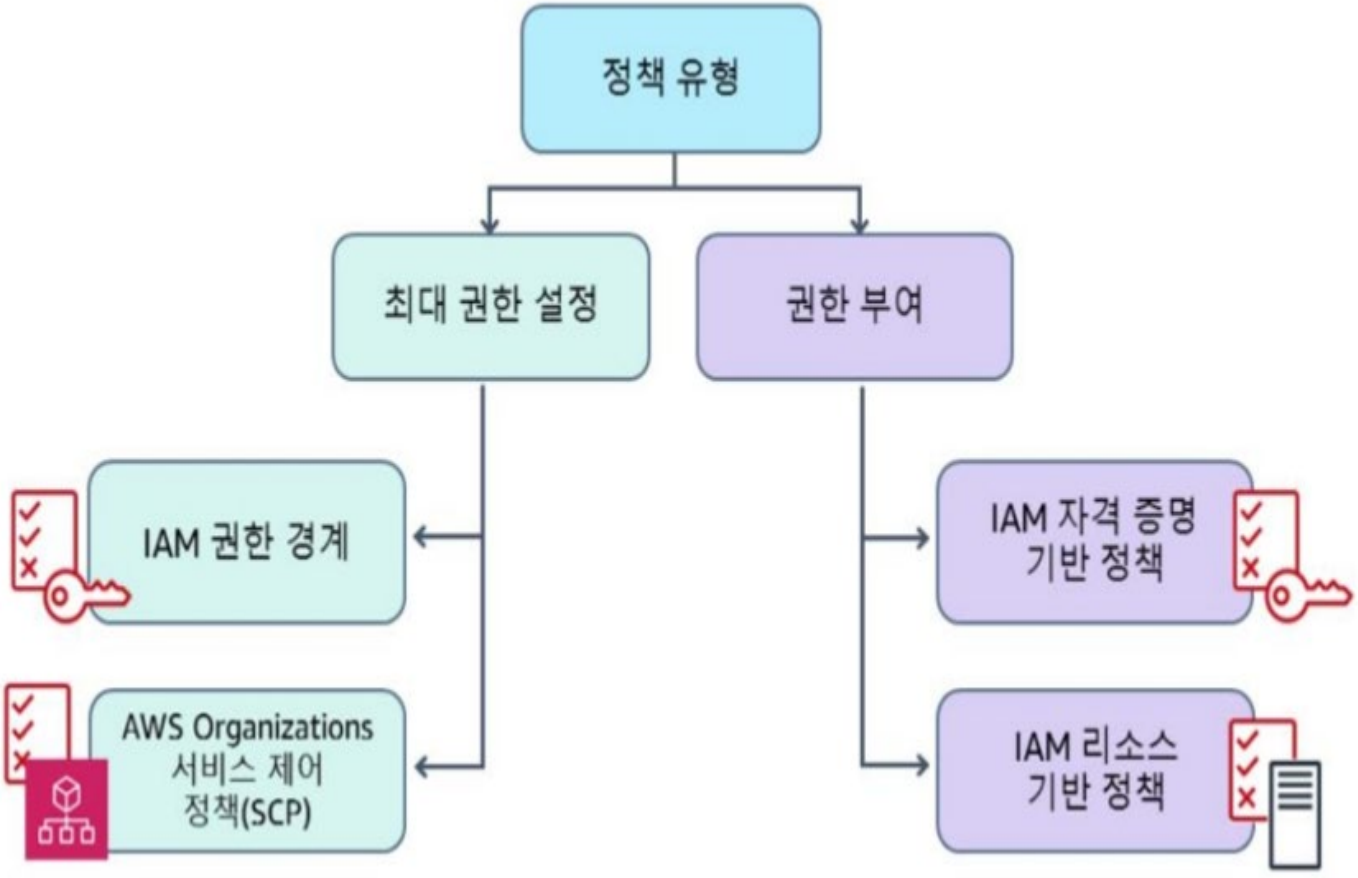
 사람	• 직원에게 교차 계정 액세스 권한을 부여합니다. • 현재 IdP의 자격 증명를 사용하여 리소스에 액세스합니다.
 애플리케이션	• AWS 또는 온프레미스에서 실행되는 애플리케이션이 AWS API 호출을 수행하도록 허용합니다.
 AWS 서비스	• AWS 서비스가 사용자 대신 AWS API 호출을 수행하도록 허용합니다.

보안 정책 사용자 사례

"제가 개발자 계정에서 앱을 테스트하는 동안 다른 팀의 개발자가 저의 EC2 인스턴스를 중지했습니다. 그들은 이 인스턴스에 접근하면 안 되는 것이었습니다."

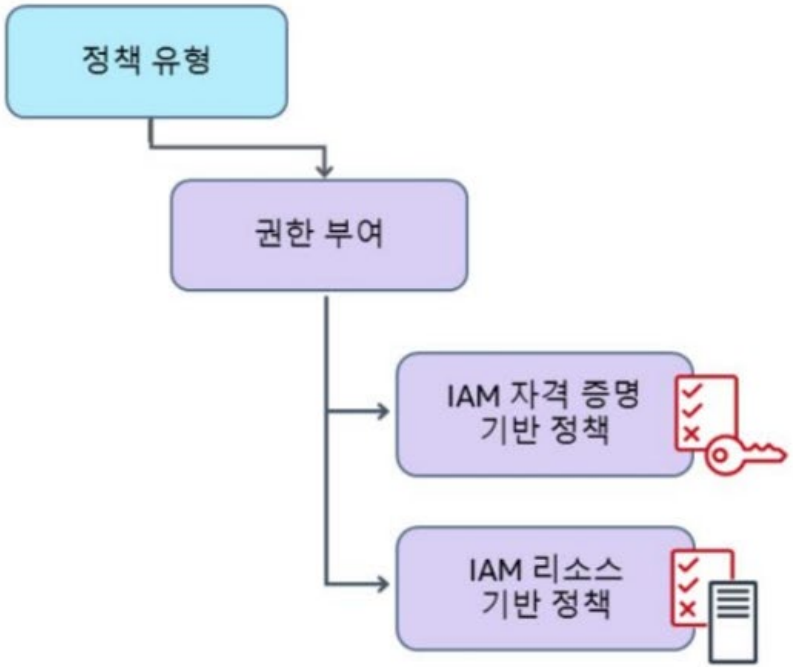
- 애플리케이션 개발자

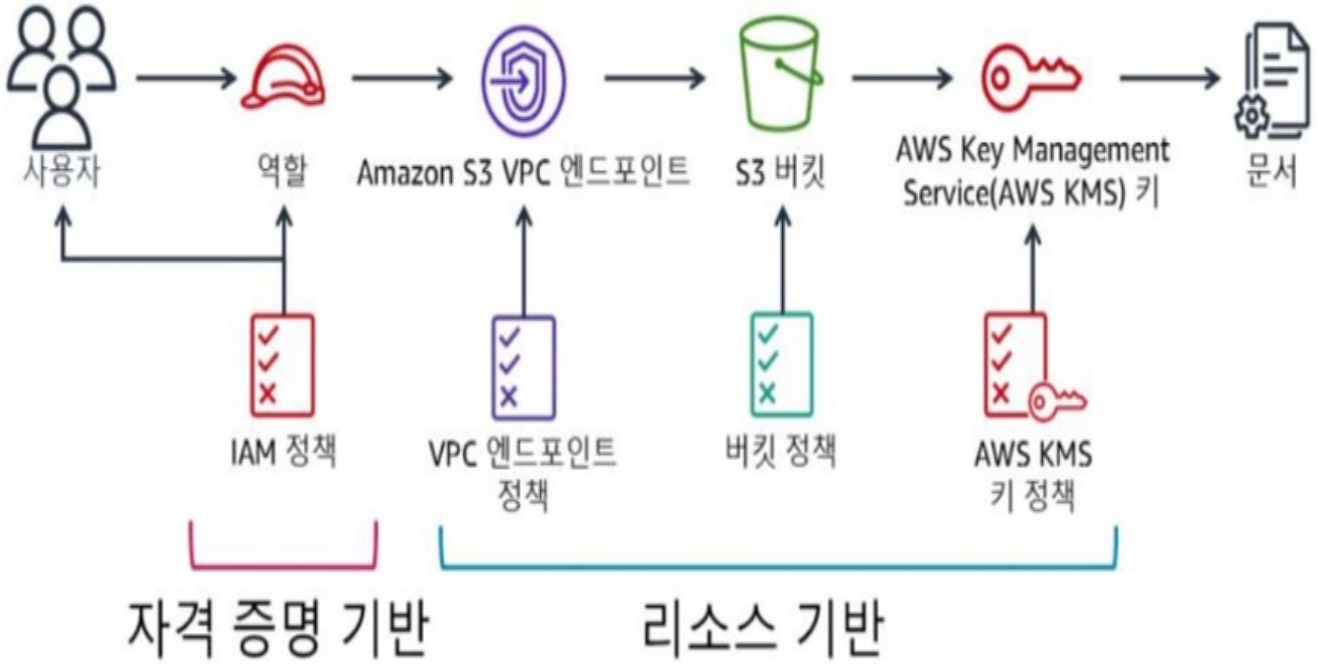
보안정책 범주


정책 유형
최대 권한 설정
권한 부여
IAM 권한 경계
AWS Organizations
서비스 제어
정책(SCP)
IAM 자격 증명
기반 정책
IAM 리소스
기반 정책

권한부여

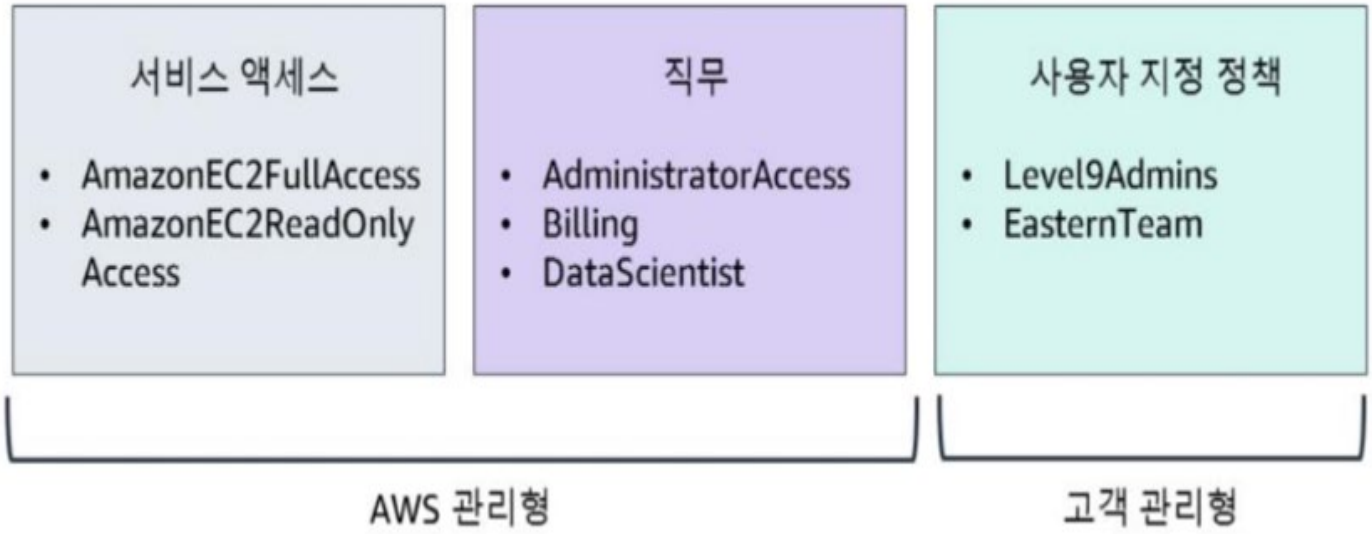
- 자격 증명 기반 정책은 사용자, 그룹 및 역할에 할당됩니다.
- 리소스 기반 정책은 리소스에 할당됩니다.
- 누군가가 리소스에 액세스를 시도하면 리소스 기반 정책이 확인됩니다.





정책평가 로직
(https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_evalu ation-logic.html)

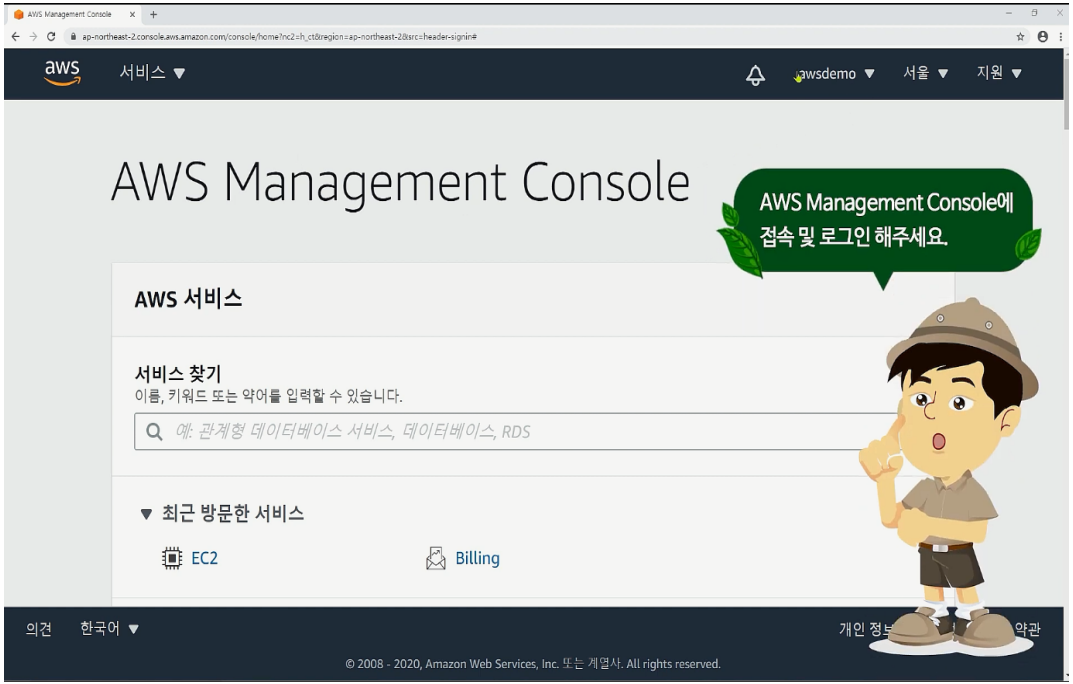
자격증명 기반 정책의 유형



인라인 정책 대신 고객관리형정책 사용(https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#best-practice-managed-vs-inline

IAM 서비스 실습 시연

- https://rumble.com/v33ukq6-aws-iam-2023.html



학습점검

Q 1

다음 중 IAM 기능에 대해 잘못 설명한 것은?

가.AWS 계정에 대한 공유 액세스

암호나 액세스 키를 공유하지 않고도 AWS 계정의 리소스를 관리하고 사용할 수 있는 권한을 다른 사람에게 부여가능

나.세분화된 권한부여 기능

리소스에 따라 여러 사람에게 다양한 권한을 부여가능.

다.멀티 팩터 인증(MFA)

보안 강화를 위해 계정과 개별 사용자에게 2팩터 인증을 추가가능. MFA를 사용할 경우 계정 소유자나 사용자가 계정 작업을 위해 암호나 액세스 키뿐 아니라 특별히 구성된 디바이스의 코드도 제공해야 함

라.자격 증명 연동

IAM 기능은 AWS 고유한 보안 매카니즘이므로 기업 네트워크나 인터넷 자격 증명 공급자와 같은 다른 곳에 이미 암호가 있는 사용자에게 AWS 계정에 대한 임시 액세스 권한을 부여할 수 없음

A

라 (IAM 기능은 기업 네트워크나 인터넷 자격 증명 공급자와도 연동이 가능하다)

Q2

참 ,거짓을 판별하시오

루트 사용자는 일상적인 AWS 계정관리 업무에 사용하면 안됩니다

A

참 (권한 위임이 가능한 IAM 을 이용하여 루트사용자 이용에 따르는 보안 위협을 감소하는 것이 좋다)