HANSUNG UNIVERSITY

클라우드컴퓨팅

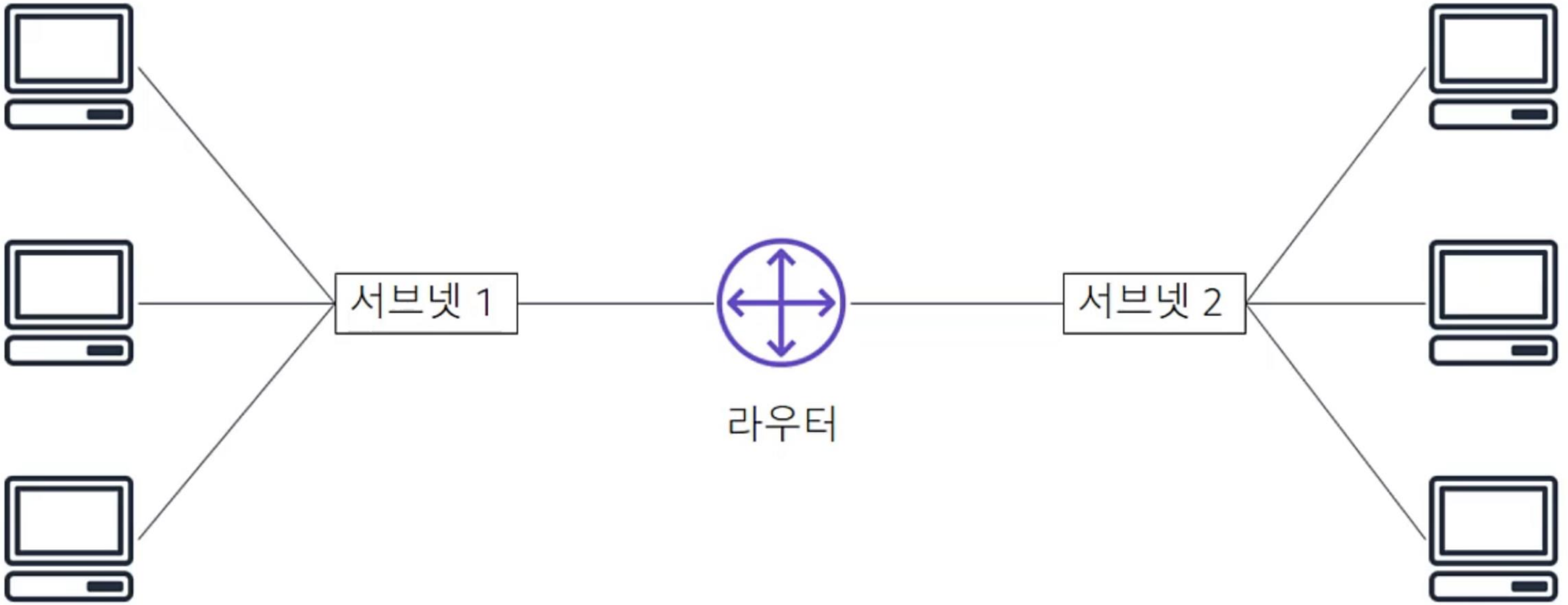
AWS Service - Network

Sung-Dong Kim,
School of Computer Engineering,
Hansung University

What to study

- 네트워크 기초
- AWS Virtual Private Cloud (VPC)
- VPC Networking
- VPC Security
- Amazon Route 53 DNS

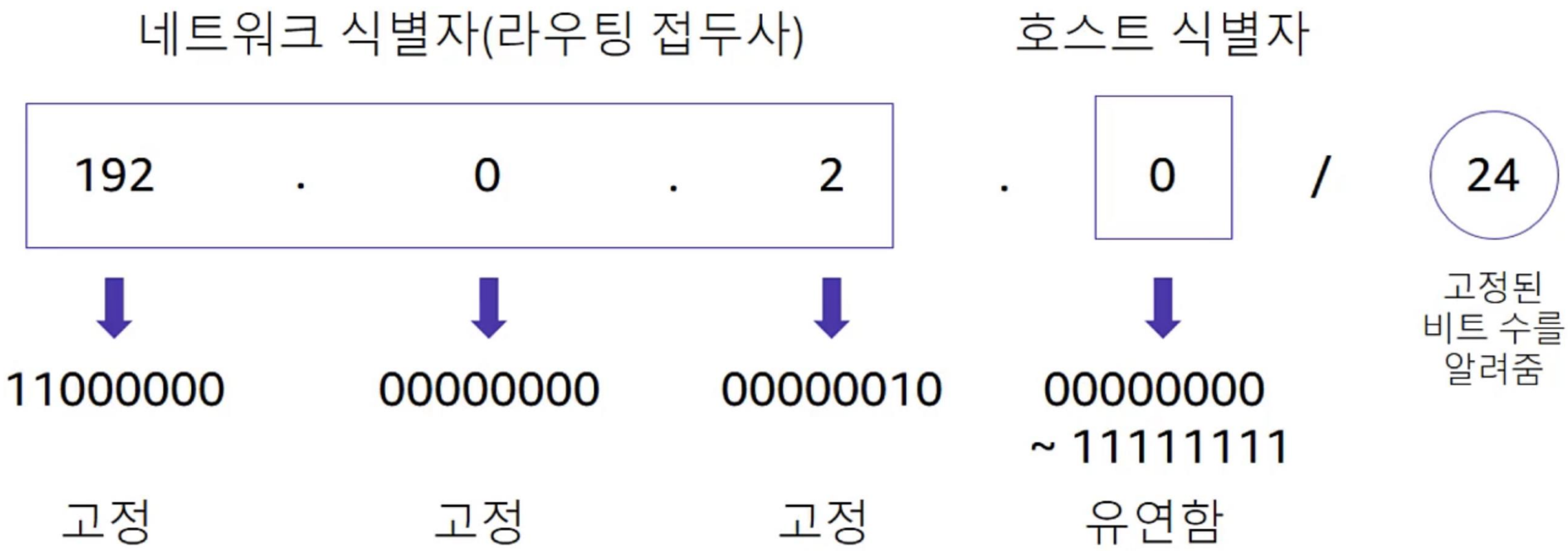
네트워크 기초


서브넷 1
서브넷 2
라우터

- IPv4(32 bit) 주소: 192.0.2.0
  - 탄력적 IP 주소를 통해 수동으로 할당
  - 서브넷 수준에서 public IP 주소 자동 할당 설정을 통해 자동으로 할당
- IPv6(128 bit) 주소: 2600:1f18:22ba:8c00:ba86:a05e:a5ba:00FF

CIDR (Classless Inter-Domain Routing)

- 클래스 없는 도메인 간 라우팅



OSI (Open Systems Interconnection) 모델

계층	번호	기능	프로토콜/주소
애플리케이션	7	애플리케이션이 컴퓨터 네트워크에 액세스하는 수단	HTTP(S), FTP, DHCP, LDAP
프레젠테이션	6	• 애플리케이션 계층이 데이터를 읽을 수 있도록 보장 • 암호화	ASCI, ICA
세션	5	순서에 따른 데이터 교환 지원	NetBIOS, RPC
전송	4	호스트 간 통신을 지원하는 프로토콜 제공	TCP, UDP
네트워크	3	라우팅 및 패킷 전달(라우터)	IP
데이터 링크	2	동일한 LAN 네트워크(허브 및 스위치)에서 데이터 전송	MAC
물리	1	물리적 매체를 통한 원시 비트스트림 전송 및 수신	신호(1 및 0)

Amazon Virtual Private Cloud (VPC)

Amazon VPC

AWS 클라우드의
프라이빗 네트워크
공간

워크로드의
논리적 격리 제공

리소스에 대한 사용자
지정 액세스 제어 및
보안 설정 허용

Amazon VPC

- AWS에서 논리적으로 격리된 네트워크 공간을 할당하여 가상 네트워크에서 AWS 리소스를 이용할 수 있는 서비스 제공
- AWS 계정을 위한 전용 가상 네트워크
- 리전, 가용 영역에 적용됨
- 구성 요소
  - 자체 IP 주소 범위
  - 서브넷 (subnet)
  - 라우팅 테이블 (routing table)
  - 네트워크 게이트웨이 (network gateway)

Amazon VPC

Private IP

- 인터넷을 통해 연결할 수 없음
- VPC 내부에서만 사용할 수 있는 IP
- VPC subnet 범위에서 자동 할당
- 동일 네트워크에서 instance 간의 통신에 사용

Public IP

- 인터넷을 통해 연결 가능
- 인스턴스와 인터넷 간의 통신을 위해 사용
- EC2 instance 생성 시 옵션으로 public IP 주소 사용 가능: instance 재부팅 시 다른 public IP가 할당됨

Amazon VPC

Elastic IP

- 동적 컴퓨팅을 위해 고안된 고정 public IP
- instance와 연결되지 않거나, 중지된 instance 또는 분리된 네트워크 인터페이스와 연결 시, 요금 발생

IP 주소 지정

- VPC 생성 시 IPv4 CIDR 블록에 VPC 할당
- IPv6도 지원
- 서브넷의 CIDR 블록은 중첩될 수 없음

x.x.x.x/16 또는 65,536개 주소(최대)

~

x.x.x.x/28 또는 16개 주소(최소)

Amazon VPC

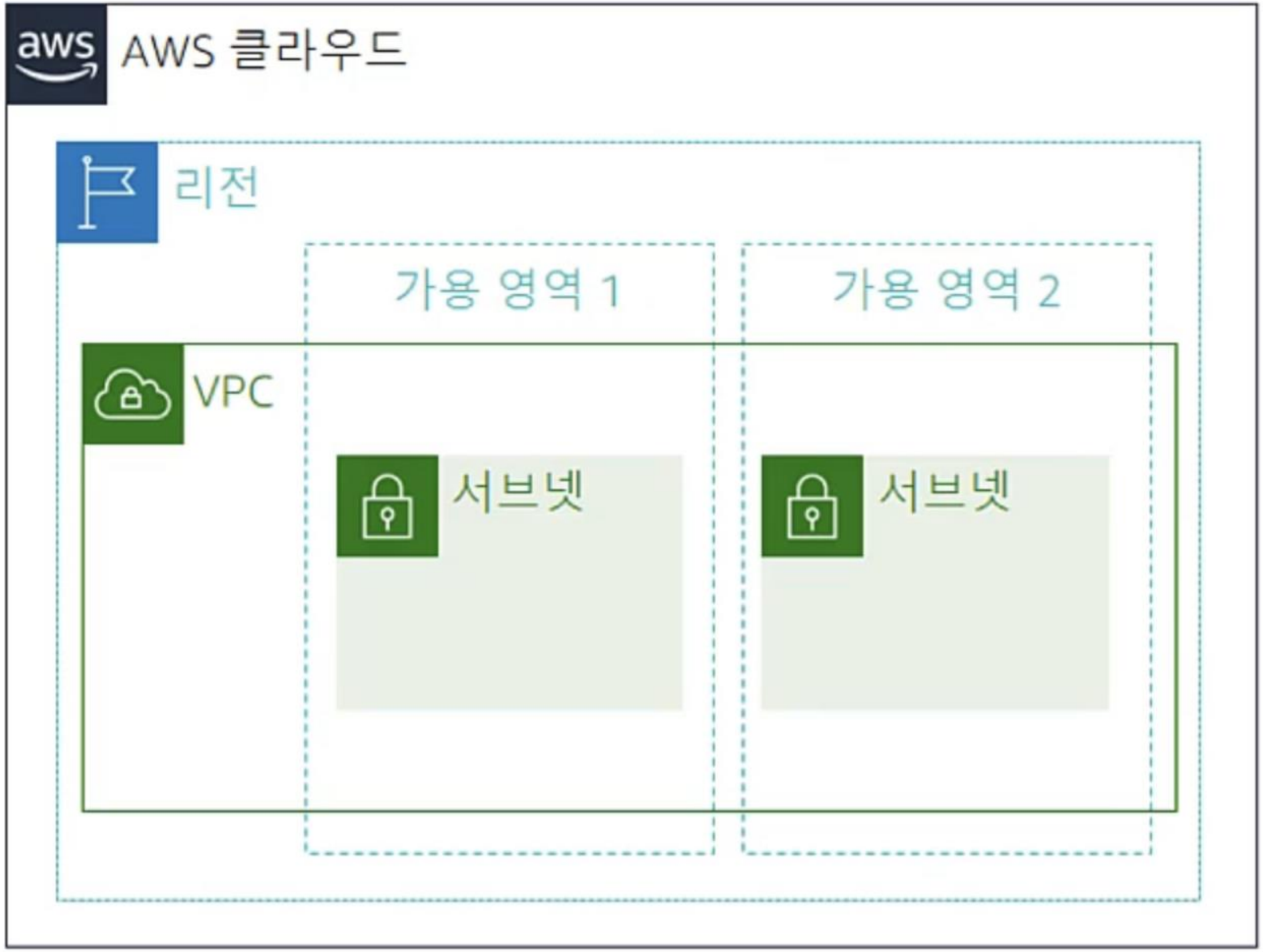
Subnet

- VPC 내부에서 분리된 IP block
- 각 AZ에 하나 이상의 subnet 추가 가능
- 단일 AZ에서만 생성 가능
- 여러 AZ로 확장 불가

Amazon VPC

- public subnet
  - subnet 네트워크 트래픽이 internet gateway (IG)로 라우팅 되는 subnet
  - 외부와 통신하는 web server
- private subnet
  - subnet 네트워크 트래픽이 internet gateway (IG)로 라우팅 되지 않는 subnet
  - 보안성이 필요한 DB server

Amazon VPC



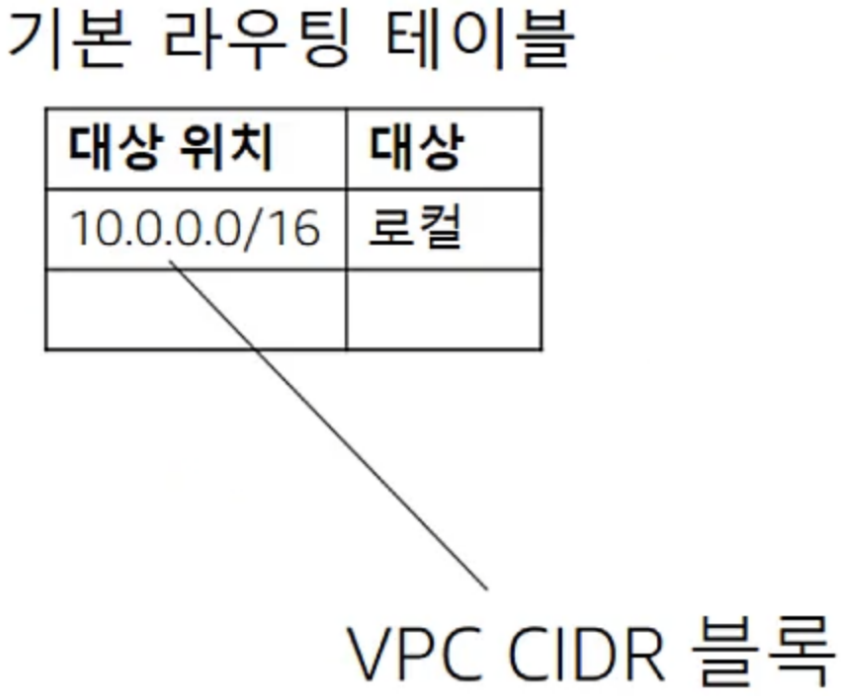
예약된 IP 주소

CIDR 블록 10.0.0.0/24의 IP 주소	다음 용도로 예약됨
10.0.0.0	네트워크 주소
10.0.0.1	내부 통신
10.0.0.2	DNS(Domain Name System) 확인
10.0.0.3	향후 사용
10.0.0.255	네트워크 브로드캐스트 주소

Amazon VPC

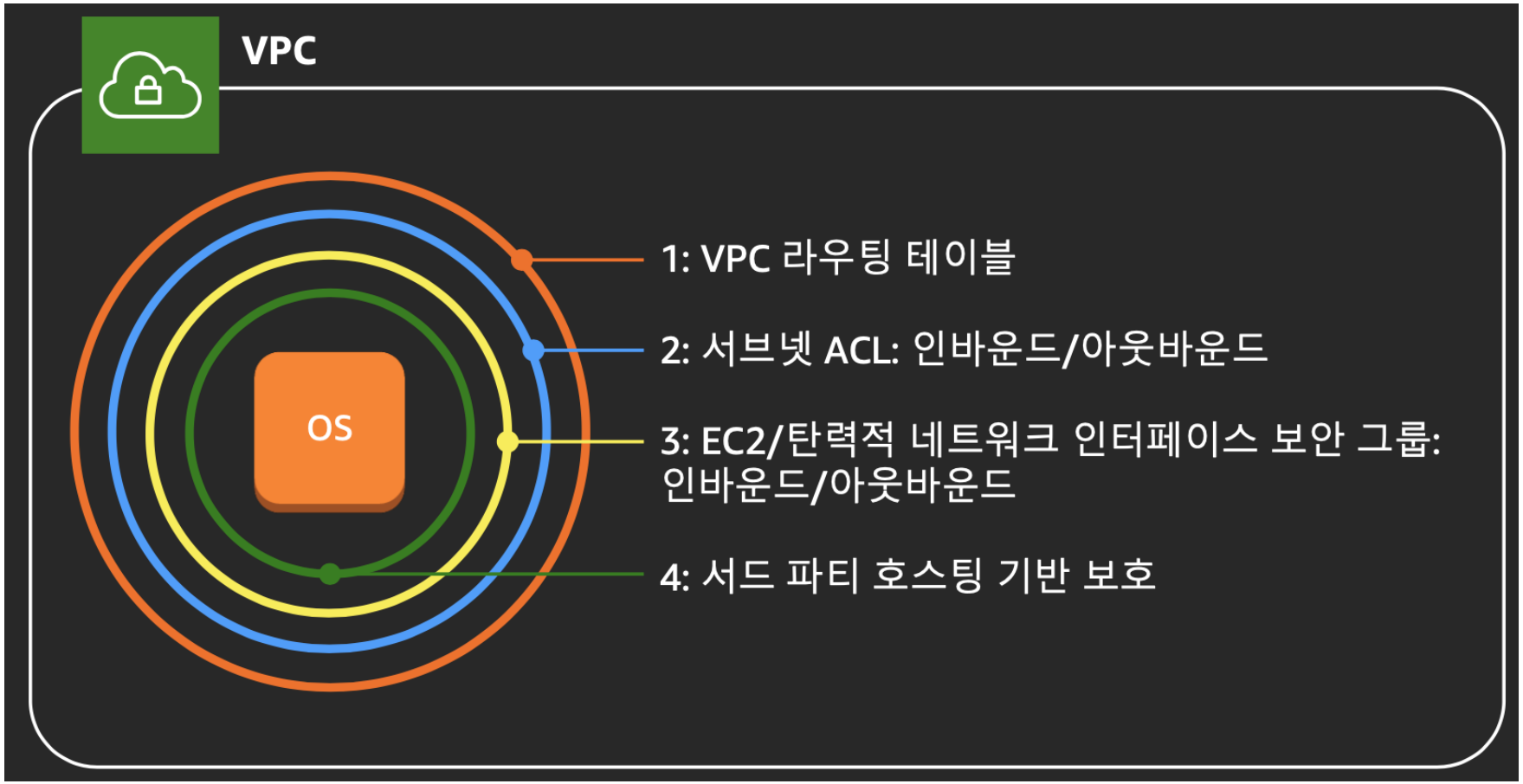
routing table

- 외부로 나가는 outbound traffic에 대해 허용된 경로를 지정하는 것
- VPC subnet 내에 생성된 packet이 목적지로 이동하기 위해 어떤 경로로 이동되어야 하는지를 알려줌
- 서브넷은 라우팅 테이블 (최대 1개)과 연결되어야 함



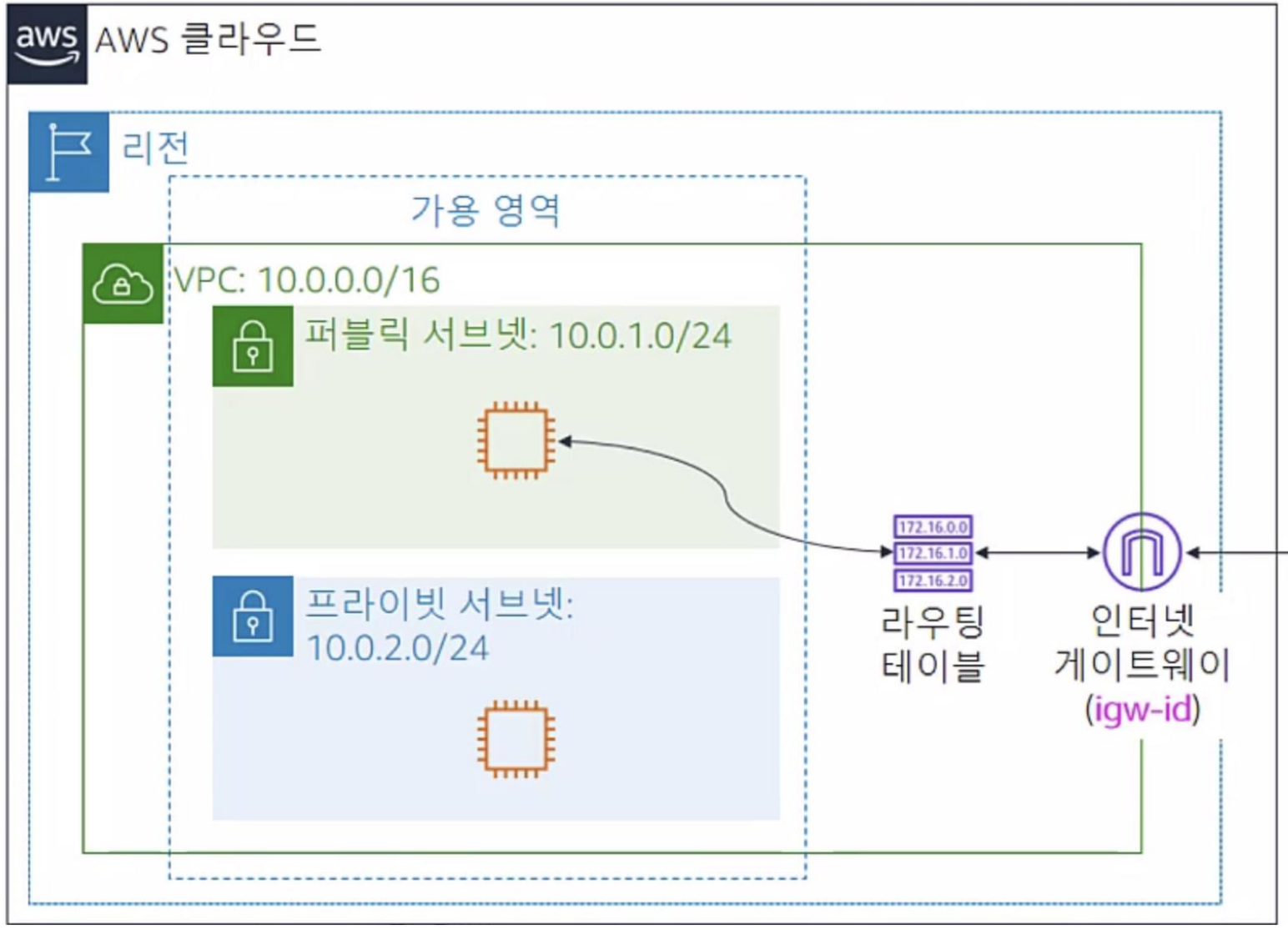
계층화된 네트워크 방어

- 심층 보안: 모든 계층에서의 보안



VPC Networking

VPC Networking



퍼블릭 서브넷 라우팅 테이블

대상 위치	대상
10.0.0.0/16	로컬
0.0.0.0/0	igw-id

인터넷 게이트웨이 (Internet Gateway)

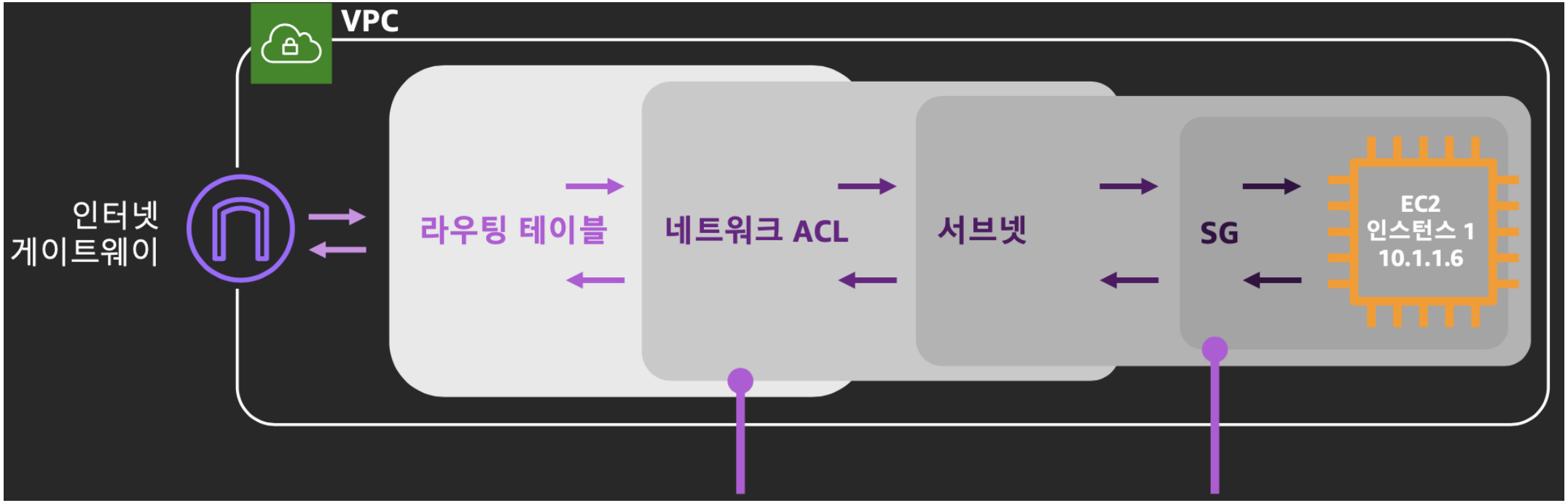
- Gateway: 한 네트워크(segment)에서 다른 네트워크로 이동하기 위하여 거쳐야 하는 지점
- VPC와 인터넷 간에 통신을 할 수 있게 해 줌
- VPC에서 호스팅 하는 리소스와 인터넷 간의 통신을 가능하게 해주는 AWS 컴포넌트
- public IP/elastic IP를 가진 인스턴스들에 대해 NAT 역할 담당
- public subnet: 서브넷 라우터에 attach 되어 있는 IG가 있을 때
- private subnet: ~ IG가 없을 때

NAT 게이트웨이

- Network Address Translation
- 외부 네트워크에 알려진 것과 다른 IP 주소를 사용하는 내부 네트워크에서 내부 IP를 외부 IP로 변환하는 서비스

VPC Security

Amazon Security



네트워크 ACL (액세스 제어 목록)

- 서브넷과 주고받는 트래픽 허용/거부
- 서브넷 수준에서 2차 방어 계층으로 보안 강화

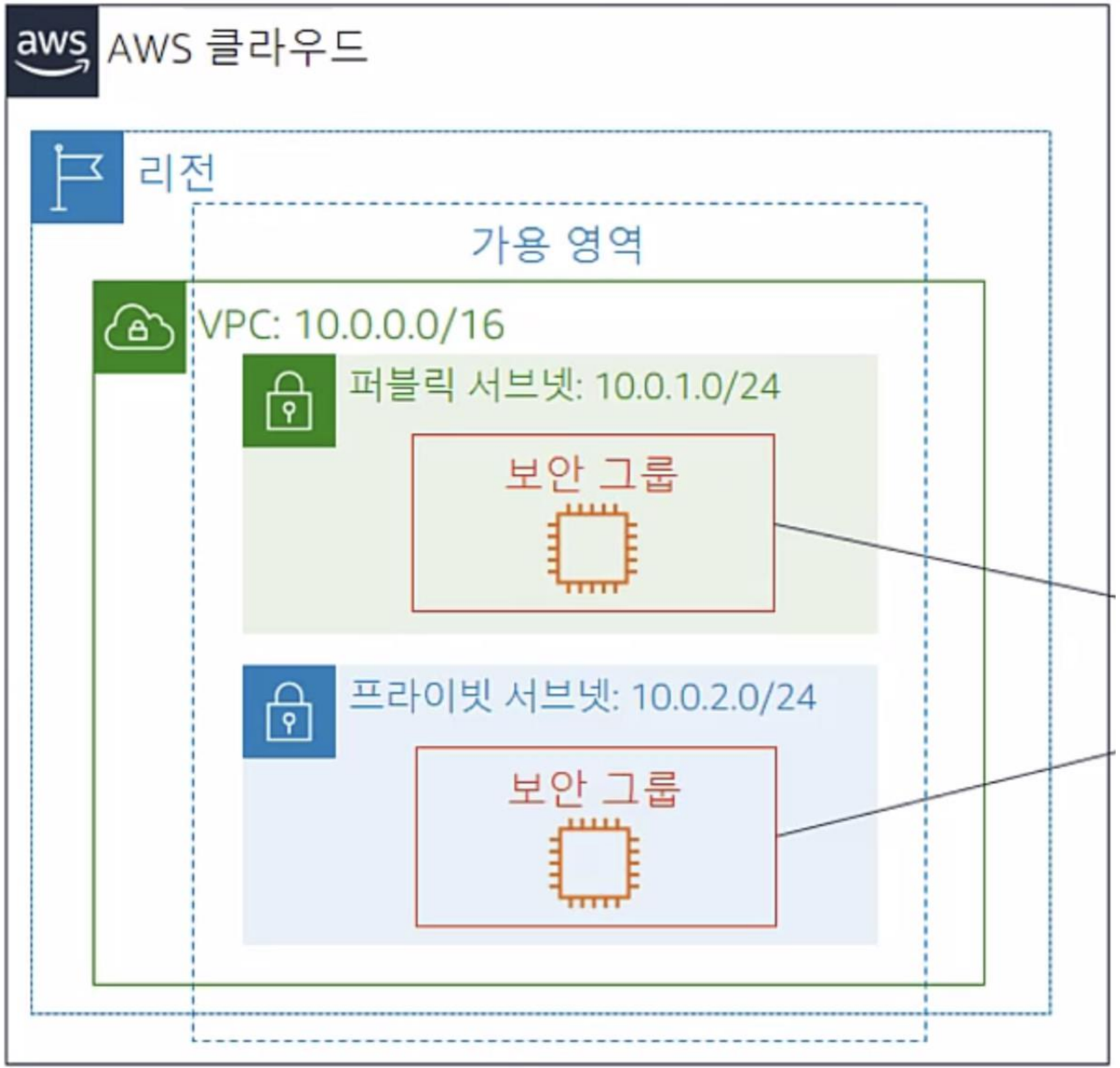
보안 그룹

- 네트워크 인터페이스(인스턴스) 수준에서 인바운드/아웃바운드 트래픽을 허용하는 데 사용
- 일반적으로 애플리케이션 개발자가 관리

VPC Security

보안 그룹

- 인스턴스 수준에서 작동



VPC Security

보안 그룹

- 인바운드 및 아웃바운드 인스턴스 트래픽을 제어하는 규칙이 있음
- 기본 보안 그룹
  - 모든 인바운드 트래픽 거부
  - 모든 아웃바운드 트래픽 허용

VPC Security

Inbound				
Type	Protocol	Port Range	Source	Description
HTTP	TCP	80	0.0.0.0/0	All web traffic
HTTPS	TCP	443	0.0.0.0/0	All web traffic
SSH	TCP	22	54.24.12.19/32	Office address
Outbound				
Type	Protocol	Port Range	Source	Description
All traffic	All	All	0.0.0.0/0	
All traffic	All	All	::/0	

VPC Security

네트워크 ACL (Access Control List)

- 별개의 인바운드 및 아웃바운드 규칙
- 기본 네트워크 ACL: 인바운드/아웃바운드 IPv4 트래픽을 모두 허용

VPC Security

Inbound					
Rule #	Type	Protocol	Port Range	Source	Allow/Deny
100	All IPv4 traffic	All	All	0.0.0.0/0	ALLOW
*	All IPv4 traffic	All	All	0.0.0.0/0	DENY
Outbound					
Rule #	Type	Protocol	Port Range	Source	Allow/Deny
100	All IPv4 traffic	All	All	0.0.0.0/0	ALLOW
*	All IPv4 traffic	All	All	0.0.0.0/0	DENY

VPC Security

속성	보안 그룹	네트워크 ACL
범위	인스턴스 수준	서브넷 수준
지원되는 규칙	허용 규칙만	허용 및 거부 규칙
상태	상태 저장(규칙에 관계없이 반환 트래픽이 자동으로 허용됨)	상태 비저장(반환 트래픽이 규칙에 의해 명시적으로 허용되어야 함)
규칙 순서	모든 규칙은 트래픽 허용을 결정하기 전에 평가됨	규칙은 트래픽 허용을 결정하기 전에 번호순으로 평가됨

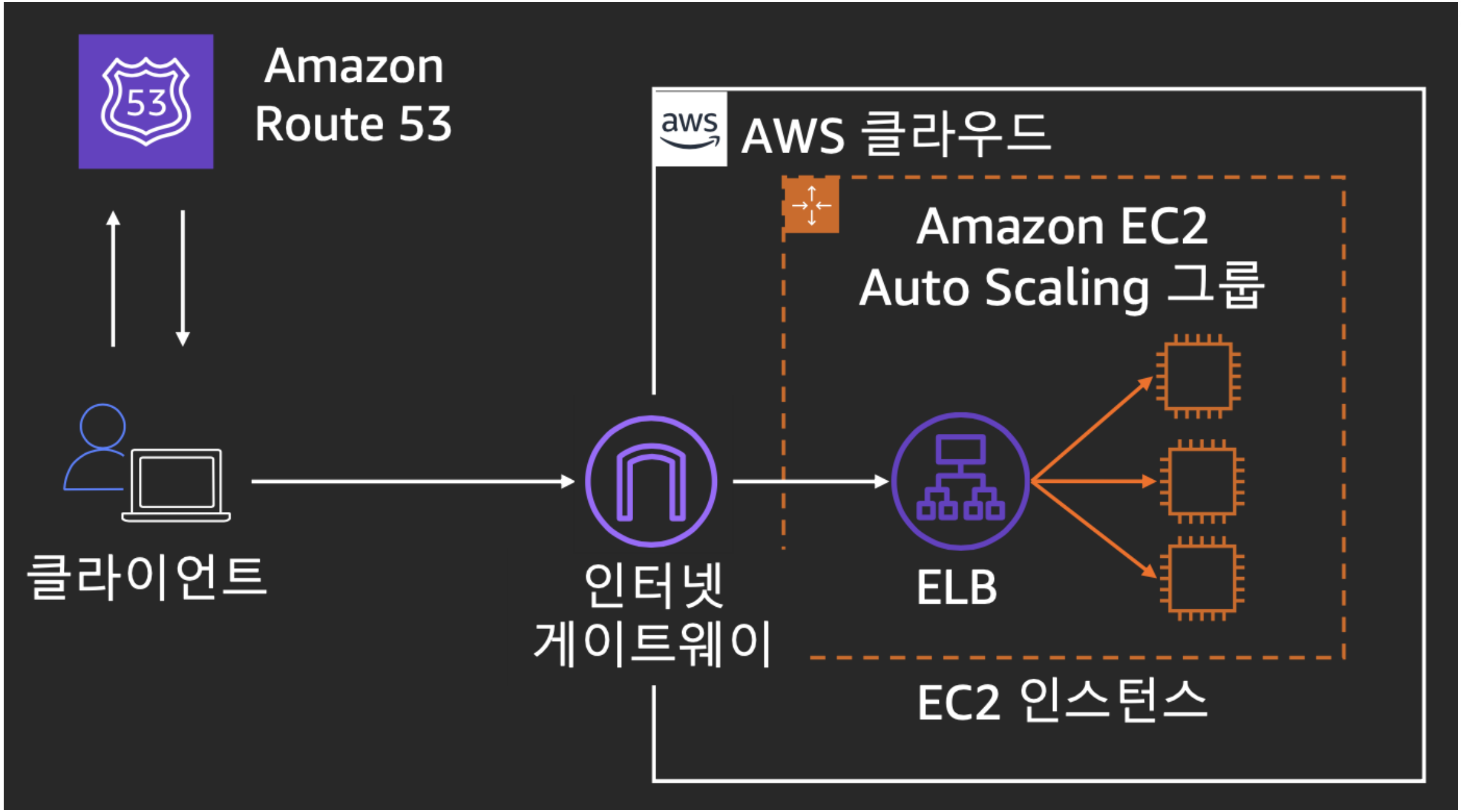
Amazon Route 53 DNS

Route 53 DNS


www.example.com
요청
Route 53에서 IP
주소 확인
사용자
DNS 해석기
Amazon
Route 53
IP 주소
192.0.2.0 반환
IP 주소 192.0.2.0
반환

Route 53 DNS

- 가용성과 확장성이 우수한 DNS (Domain Name System) 웹 서비스
- 리소스 상태를 확인하는데 사용
- 트랙픽 흐름을 나타냄
- 도메인 이름을 등록할 수 있도록 지원


Amazon
Route 53
AWS 클라우드
Amazon EC2
Auto Scaling 그룹
클라이언트
인터넷
게이트웨이
ELB
EC2 인스턴스