



01

클라우드 네트워크 기본



1) 네트워크(Network)란?



세종사이버대학교

네트워크(Network)

Net(그물) + Work(일)

- 자원의 공유 / 교환을 위해
공통 약속들(통신 프로토콜)을
사용하는 상호연결된
디바이스들로 이루어진 시스템



AWS는 가상의 네트워크 공간인 VPC를 제공

2) 일반적인 네트워크 구성



라우터

- 서로 다른 지역의 컴퓨터를 연결하는 기기
- 2개 이상의 네트워크 간 최적 경로를 설정하여 데이터 패킷을 전송하는 인터넷 접속 장비 (Layer 3 Network Layer)

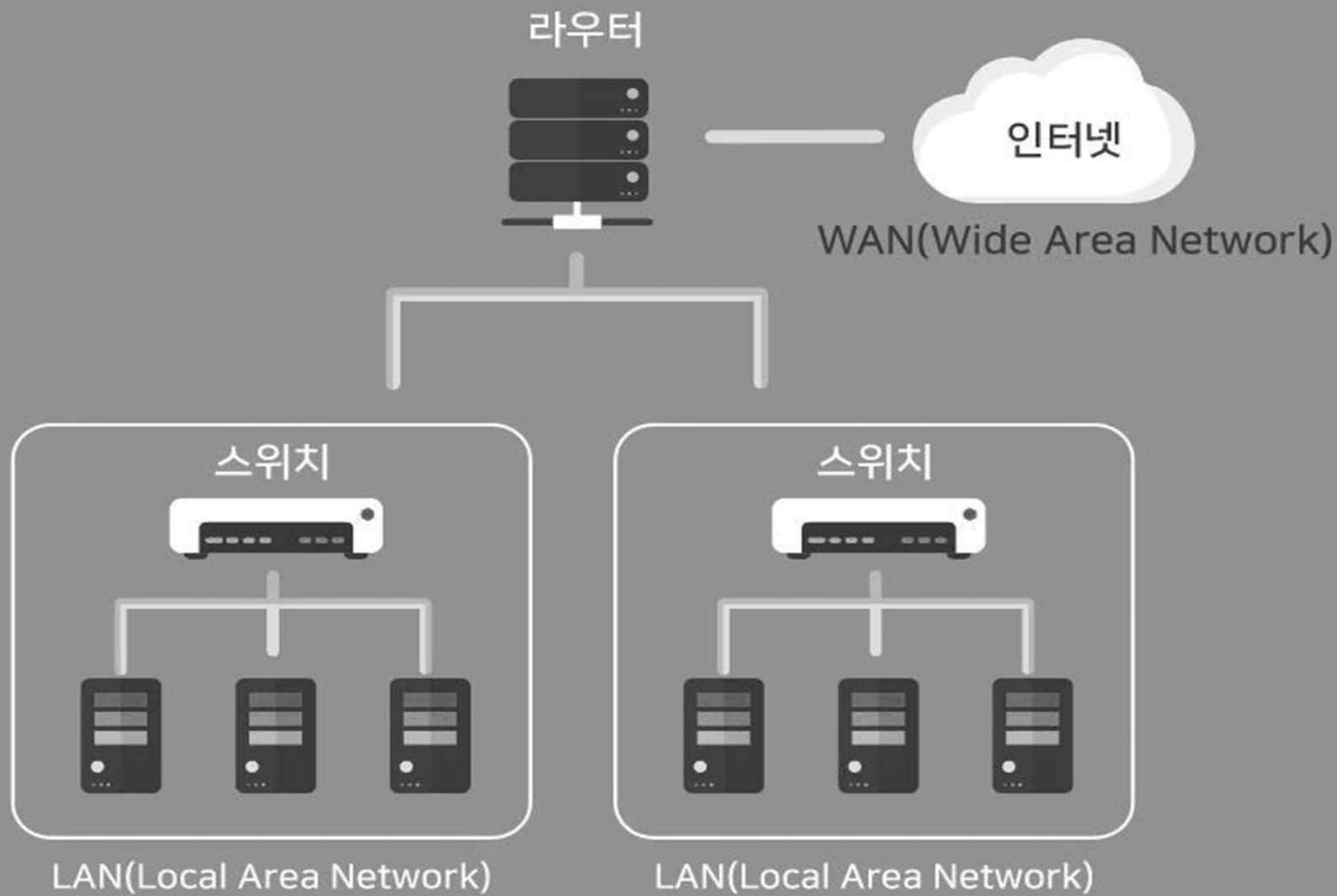
스위치

- MAC 주소 (Layer 2 Data Link Layer)를 이용하여 데이터를 전송하는 장비



AWS는 가상 프라이빗 네트워크 공간인 VPC내 암시적 라우터 (Implicit Router)가 존재하며, 라우팅 테이블로 네트워크 트래픽을 제어함

2) 일반적인 네트워크 구성

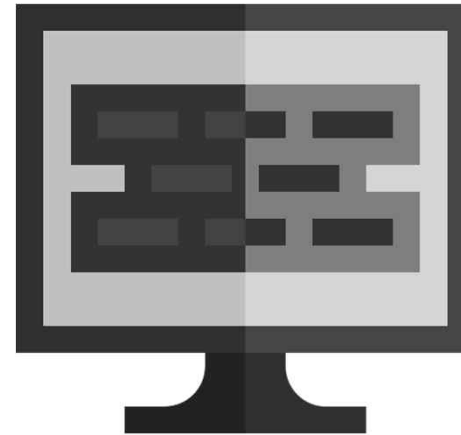


2) 일반적인 네트워크 구성



방화벽

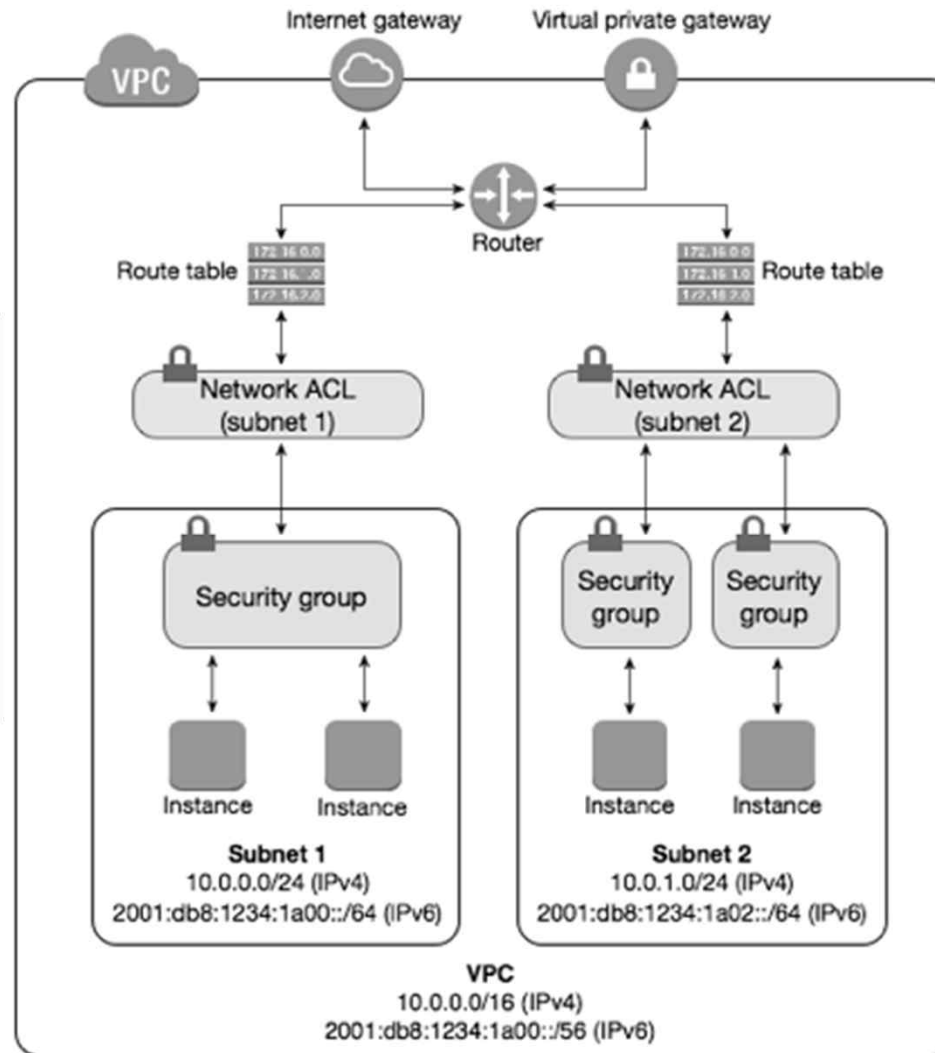
- 화재가 번지지 않도록 막는 소방 장비
- 인터넷 방화벽 : 외부로부터 내부망을 보호하기 위한 네트워크 구성요소
- 외부의 불법 침입으로부터 내부의 정보 자산을 보호 및 외부의 불법 정보 유입을 차단



AWS는 가상 방화벽 역할로써 인스턴스 수준 트래픽 통제를 수행하는 보안그룹(Security Group)과 서버넷 수준의 트래픽 통제를 하는 NACL(Network ACL)이 존재

2) 일반적인 네트워크 구성

보안그룹과
NACL 비교



3) 네트워크 주소 체계



세종사이버대학교

IP주소	‘192.168.0.1’과 같은 형태로 컴퓨터가 이해하기 쉬운 숫자 형태
도메인	‘aws.amazon.com’과 같은 형태로 사용자가 이해하기 쉬운 문자열 형태
IPV6	128 bit로 확장한 미래 인터넷 주소 체계로 현재는 IPV4의 32bit의 기존 주소 체계 사용
CIDR	IP 주소 할당 방법 (32bit 주소체계 = Network ID + Host ID)

Classless Inter-Domain Routing

4) 포트와 프로토콜



세종사이버대학교

포트

컴퓨터에서 통신에 사용하는 프로그램을
식별하는 번호

프로토콜

서로 간 통신을 위한 사전 약속

예 TCP/IP 혹은 HTTP

5) VPN (Virtual Private Network)



세종사이버대학교

VPN

퍼블릭 네트워크
(예 인터넷)을 통해
원격 사용자 /
컴퓨터를 사설
네트워크(온프레미스)에
연결 시 구현하는 보안
통신 채널



AWS의 VGW (Virtual Private Gateway)는
VPC와 온프레미스 간 VPN구성을 제공

6) DNS(Domain Name System)



DNS는 도메인 이름을 컴퓨터나 스마트폰 등 다양한 디바이스에서 읽을 수 있는 IP 주소로 변환하는 역할 수행

- 도메인 이름(예 www.naver.com)
- IP 주소(예 192.0.2.44)



모든 컴퓨터는 IP Address 사용해 통신을 수행

- DNS가 없었다면 웹 사이트에 접속하기 위해 해당 웹 서버의 IP Address를 기억하고 있어야 함



DNS는 도메인 이름을 IP 주소로 변환하여 사용자가 접속하고자 하는 웹 사이트로 라우팅될 수 있도록 지원함

6) DNS(Domain Name System)



세종사이버대학교



DNS 서비스가 있기 때문에 긴 숫자 형태인 IP 주소 대신 example.com과 같이 사람이 쉽게 기억할 수 있는 형태의 도메인 이름으로 입력해도 웹 사이트 접속이 가능



AWS는 Amazon Route 53라는 DNS 서비스를 이용하여 www.example.com와 같은 도메인 이름을 192.0.2.1과 같은 숫자 IP 주소로 변환하여 컴퓨터가 서로 통신을 수행할 수 있게 함



02

독립적인 나만의 가상 네트워크 공간 (VPC) 만들기



1) 기본 개념



세종사이버대학교

데이터센터

“ 컴퓨터 시스템, 스토리지 시스템,
통신 장비가 놓여지는 물리적인 전용 공간 ”

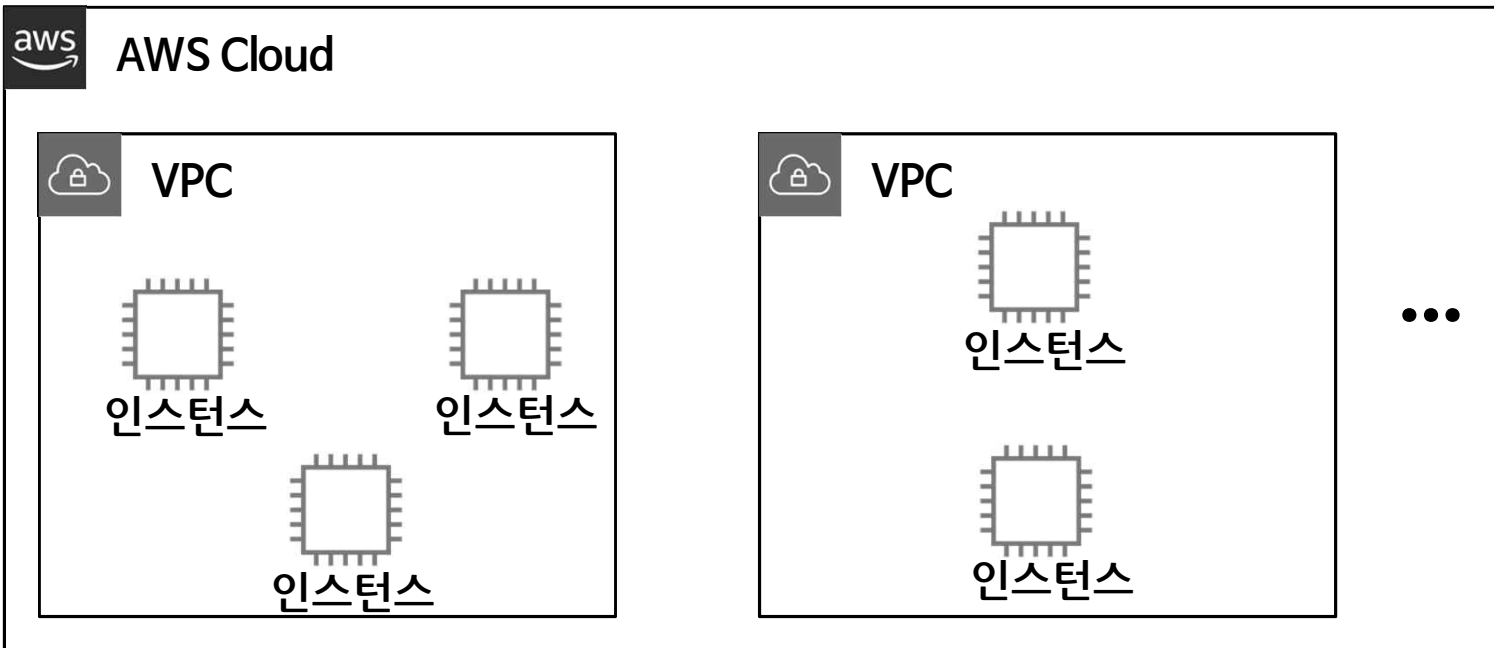


1) 기본 개념








Amazon VPC(Virtual Private Cloud)

EC2 인스턴스 및 기타 서비스들을
안전하게 격리하여 배치하기 위한 가상 데이터 센터









1) 기본 개념

AWS 네트워킹 서비스

명칭	아이콘	설명
VPC	 Amazon VPC	AWS 클라우드가 만드는 가상의 데이터 센터
VPN	 Customer gateway  VPN connection  VPN gateway	On-prem 데이터 센터와 VPC의 IPSEC VPN 연결
Direct Connect	 AWS Direct Connect	On-prem 데이터 센터와 VPC의 전용선 연결

1) 기본 개념

AWS 네트워킹 서비스

명칭	아이콘	설명
ELB	 Elastic Load Balancing  Application load balancer  Classic load balancer  Network load balancer	관리형 Load Balancer 서비스
Route53	 Amazon Route 53  Hosted zone	관리형 DNS 서비스

2) Amazon VPC(Virtual Private Cloud) 개요



사용자가 정의하는 AWS 클라우드 내 논리적으로 격리된 가상의 네트워크 공간



사용자별 네트워크 제어 가능

- IP 주소 범위 지정
- 용도에 맞는 서브넷(Subnet) 생성
- 트래픽 통제
 - 라우팅 테이블, Network ACL, 보안그룹(Security Group)
- VPC 확장을 위한 네트워크 게이트웨이 구성(Internet Gateway, NAT Gateway) 선택 등

2) Amazon VPC(Virtual Private Cloud) 개요



세종사이버대학교



온프레미스 데이터센터와 연결 옵션

- VPN, Direct Connect



IPv4, IPv6 지원

3) VPC 만들기 : 일반적인 절차



리전 (Region), IP 주소
범위 선택

가용영역 (AZ) 별
서브넷 (Subnet) 생성

라우팅 (Routing) 설정 — 라우팅 테이블 (서브넷 단위)

네트워크 트래픽
통제 (In/Out) — Network ACL (서브넷 수준), 보안그룹 (Security Group,
인스턴스 수준)

VPC 확장을 위한 네트워크
게이트웨이 구성 선택 — Internet Gateway, NAT Gateway

4) VPC 만들기 : 리전 (Region), IP 주소 범위 선택

 리전 선택 : 24개 리전 - 77개 ~ 216개 PoPs (2020년 8월 기준)



○ 리전
● 제공 예정

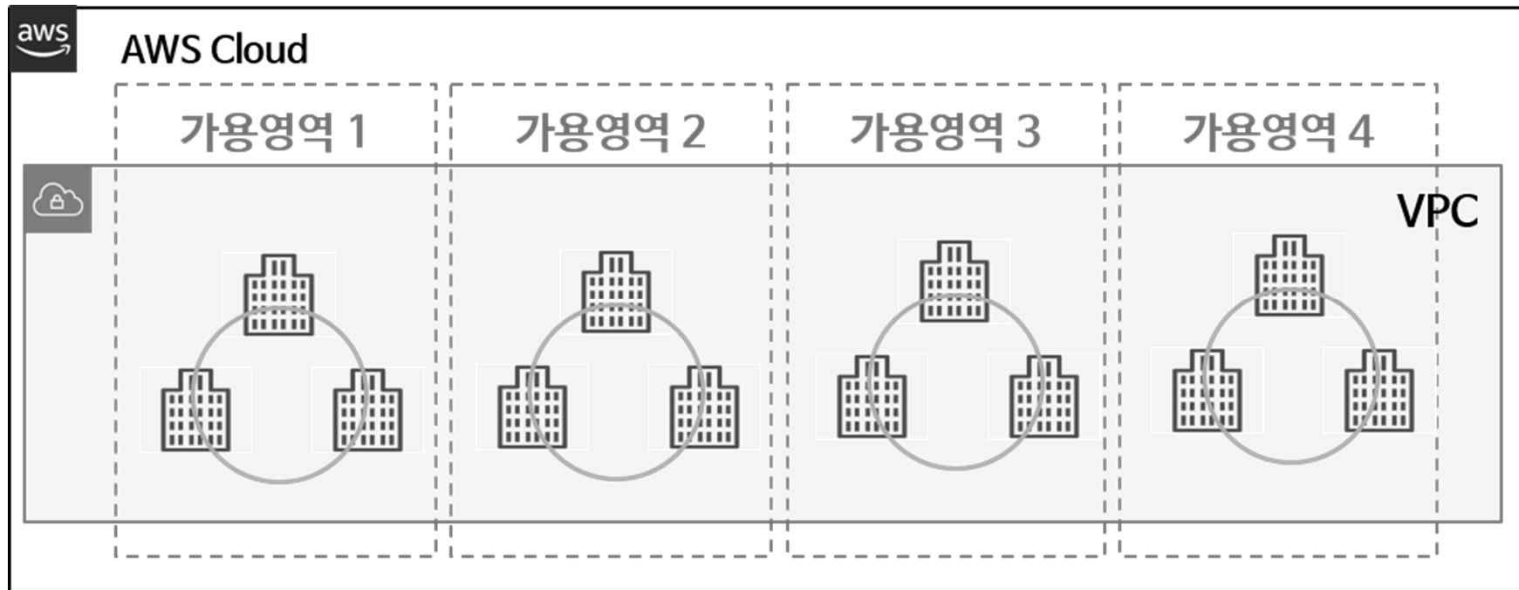
vocstartsoft/user914796=hyo... 서울	
미국 동부 (버지니아 북부)	us-east-1
미국 동부 (오하이오)	us-east-2
미국 서부 (캘리포니아)	us-west-1
미국 서부 (오레곤)	us-west-2
아프리카 (케이프타운)	af-south-1
아시아 태평양 (홍콩)	ap-east-1
아시아 태평양 (뽀모이)	ap-south-1
아시아 태평양 (서울)	ap-northeast-2
아시아 태평양 (싱가포르)	ap-southeast-1
아시아 태평양 (시드니)	ap-southeast-2
아시아 태평양 (도쿄)	ap-northeast-1
캐나다 (중부)	ca-central-1
유럽 (프랑크푸르트)	eu-central-1
유럽 (아일랜드)	eu-west-1
유럽 (런던)	eu-west-2
유럽 (밀라노)	eu-south-1
유럽 (파리)	eu-west-3
유럽 (스톡홀름)	eu-north-1
중동 (바레인)	me-south-1
남아메리카 (상파울루)	sa-east-1

4) VPC 만들기 : 리전(Region), IP 주소 범위 선택



리전, 가용 영역, VPC

▶ AWS 서울 리전(4개의 가용영역, 2020년 8월 기준)



4) VPC 만들기 : 리전 (Region), IP 주소 범위 선택



세종사이버대학교

 CIDR(Classless Inter-Domain Routing)

172.31.0.0/16 ← 접두사(Prefix) 길이

네트워크 ID

호스트 ID

IP

10101100.00011111.00000000.00000000

서브넷
마스크

11111111.11111111.00000000.00000000

IP 주소
범위

172.31.0.0 ~ 172.31.255.255 (65,536개, 2^{16})

4) VPC 만들기 : 리전 (Region), IP 주소 범위 선택



세종사이버대학교

IP 주소 범위 결정 시 고려사항



VPC CIDR 접두사 길이는 /16부터 /28까지임



VPC 확장 시나리오 고려

- 서비스 확장을 고려하여 충분히 큰 CIDR 지정
- 향후 AWS 내 동일 Region / 다른 Region으로의 VPC 확장
- 향후 고객사 On-Premise Network와의 연동



VPC의 Network 범위는 /16부터 /28까지 가능

4) VPC 만들기 : 리전 (Region), IP 주소 범위 선택



세종사이버대학교

IP 주소 범위 결정 시 고려사항



VPC Primary CIDR은 생성 후 변경 불가

- Secondary CIDR은 4개까지 추가 가능



RFC 1918 (Private IP 표준) 권장

- 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16



VPC를 온프레미스나 다른 VPC 등 다른 네트워크에 연결하려면
사용할 VPC CIDR은 다른 네트워크에서 이미 사용하는 주소와
중복되지 않아야 함

4) VPC 만들기 : 리전 (Region), IP 주소 범위 선택



세종사이버대학교

IP 주소 범위 결정 시 고려사항

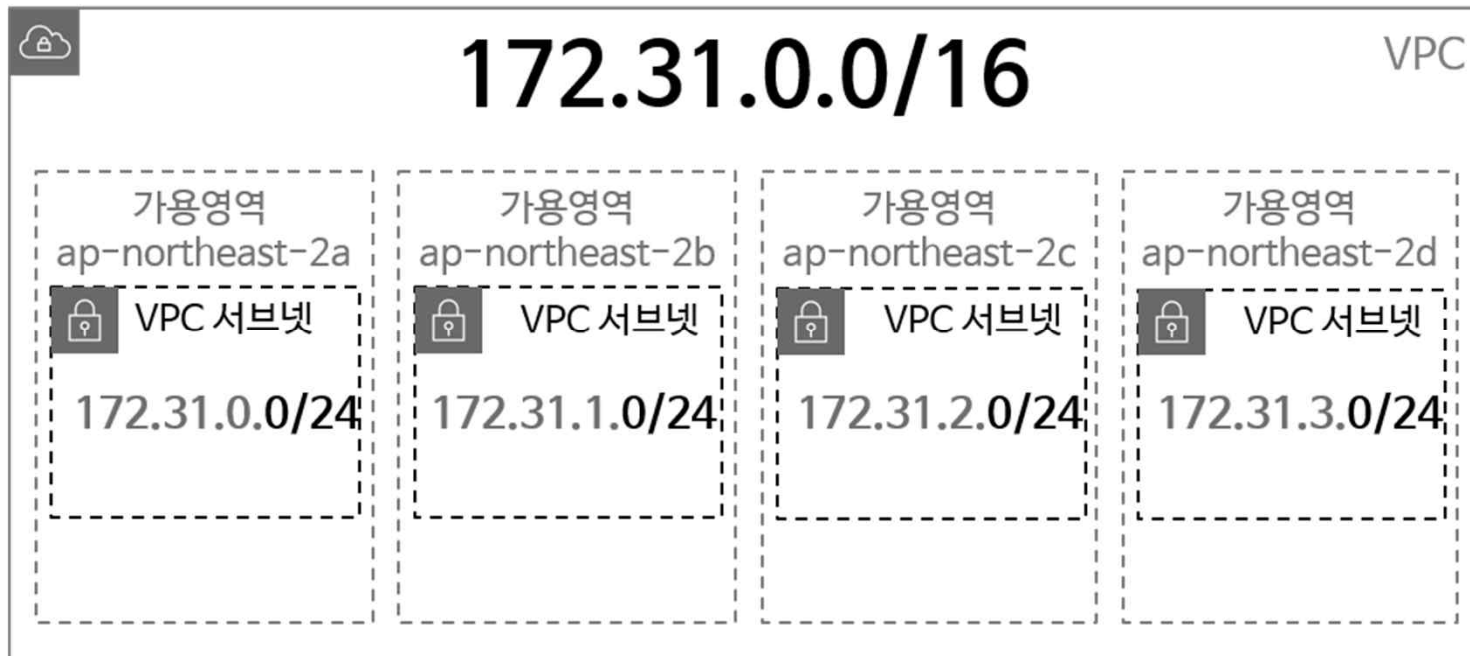
서브넷 Bits(CIDR)	# of hosts
/16	65,534
/17	32,766
/18	18,382
/19	8,190
/20	7,094
/21	2,046
/22	1,022
/23	510
/24	254
/25	128
/26	62
/27	30
/28	14

5) VPC 만들기 : 가용 영역별 서브넷 생성



세종사이버대학교

가용영역과 서브넷 배치



5) VPC 만들기 : 가용 영역별 서브넷 생성



세종사이버대학교

서브넷 IP 주소 범위

172.31.0.0/24

	네트워크 ID	서브넷 ID	호스트 ID
IP	10101100.00011111.00000000.00000000		
서브넷 마스크	11111111.11111111.11111111.00000000		
IP 주소 범위	172.31.0.0 ~ 172.31.0.255 (256개, 2 ⁸)		



5) VPC 만들기 : 가용 영역별 서브넷 생성

서브넷 생성시 고려사항



Subnet Network 범위는 /16(65,536 IPv4 주소)부터 /28(16 IPv4 주소)까지 가능



예약된 IP 주소(Subnet CIDR이 10.0.0.0/24인 경우)

10.0.0.0	네트워크 주소
10.0.0.1	VPC 라우터용으로 예약된 주소
10.0.0.2	AWS에서 예약한 DNS 주소, AmazonProvidedDNS
10.0.0.3	AWS에서 향후 사용을 위하여 예약
10.0.0.255	브로드캐스트 주소, VPC에서는 브로드캐스트를 지원하지 않으며, AWS에서 예약

5) VPC 만들기 : 가용 영역별 서브넷 생성



세종사이버대학교

서브넷 생성시 고려사항



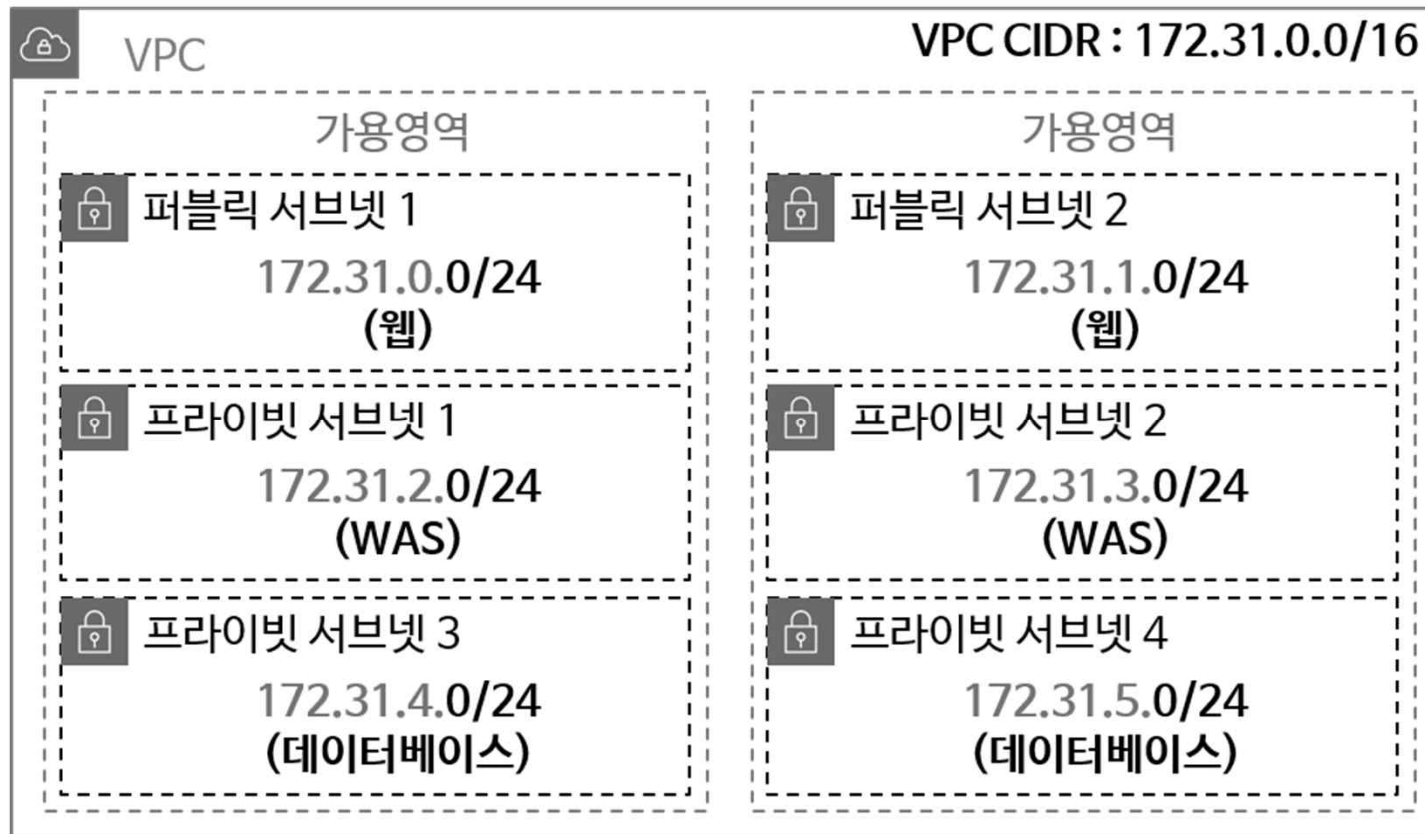
Subnet의 CIDR은 생성 후 변경 불가능



Application의 고가용성을 위해 복수개의 가용영역에 Subnet 생성 (Multi-AZ 아키텍처)

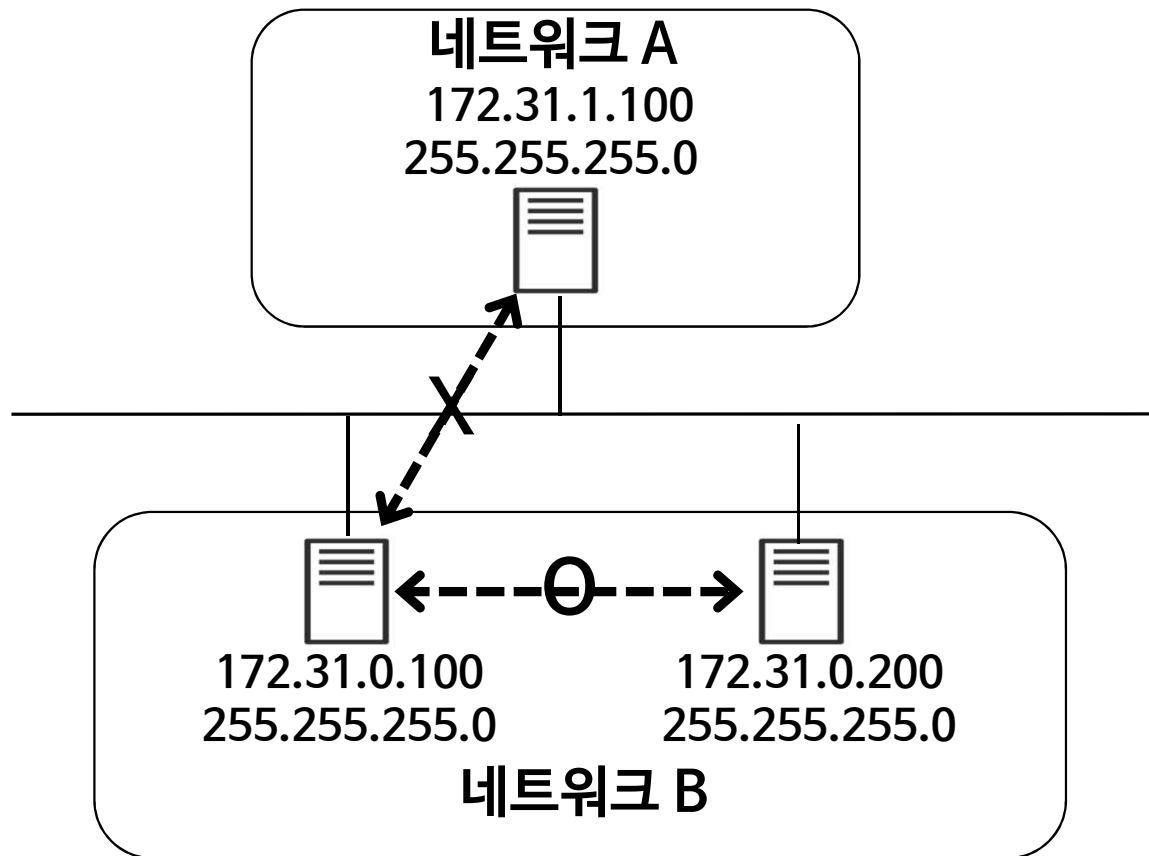
5) VPC 만들기 : 가용 영역별 서브넷 생성

서브넷 구성 예시



6) VPC 만들기 : 라우팅 설정

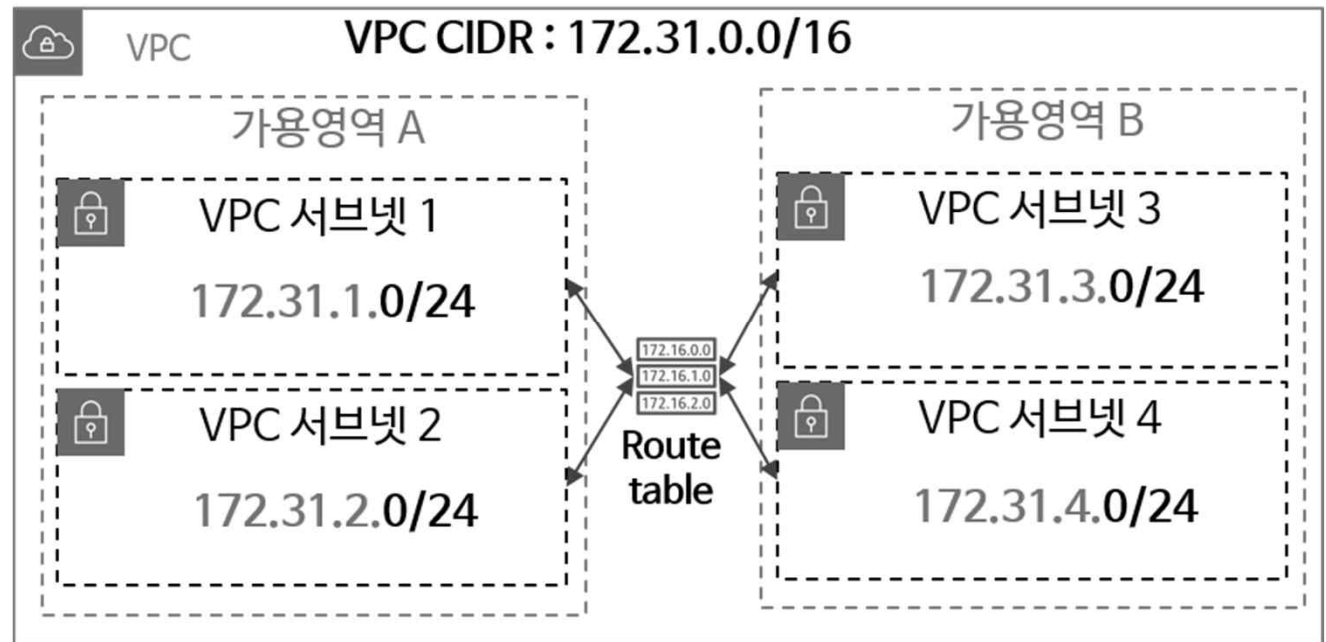
 다른 네트워크와의 통신은 라우팅을 설정하지 않는 한 불가능



6) VPC 만들기 : 라우팅 설정

Main Route Table

- Main Route Table은 VPC 생성시 자동으로 생성
- VPC내 모든 서브넷은 암시적으로 (Implicitly) 적용
- 서브넷 : Route Table = 1:1
- 삭제 불가





6) VPC 만들기 : 라우팅 설정

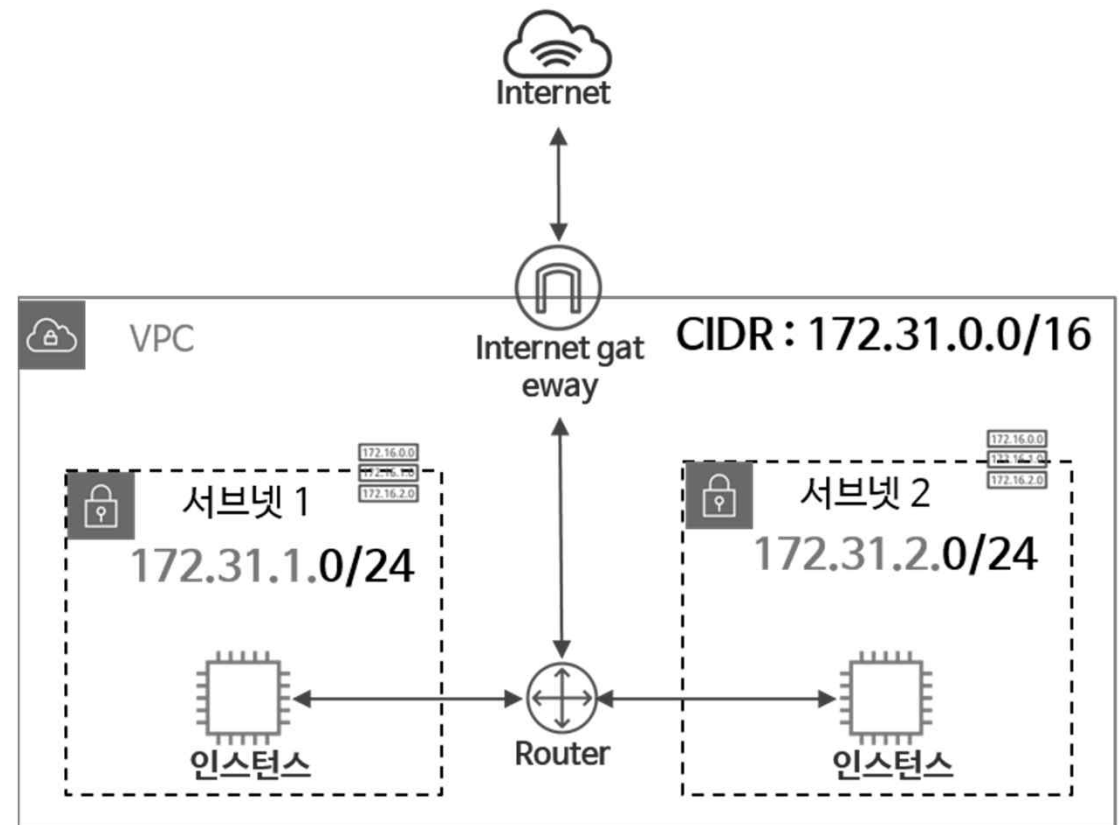
Custom Route Tables

- VPC 외부 리소스 (예 인터넷, 온프레미스 데이터센터)와 통신을 위한 Route Rule 추가
- 명시적으로 (Explicitly) 서브넷에 Association



Custom Route Table

Destination	Target
172.31.0.0/16	local
0.0.0.0/0	lgw-bc3e5cd5

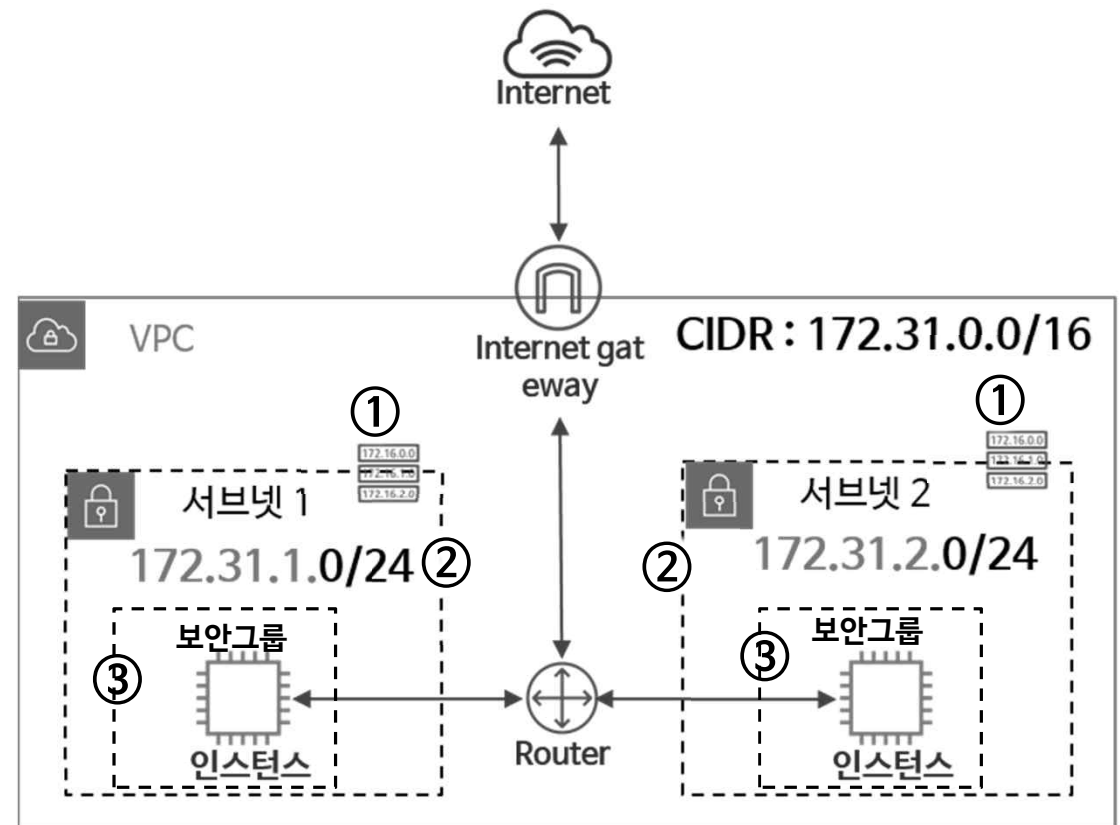


7) VPC 만들기 : 네트워크 트래픽 통제

① Route Table

② Network ACL

③ 보안그룹



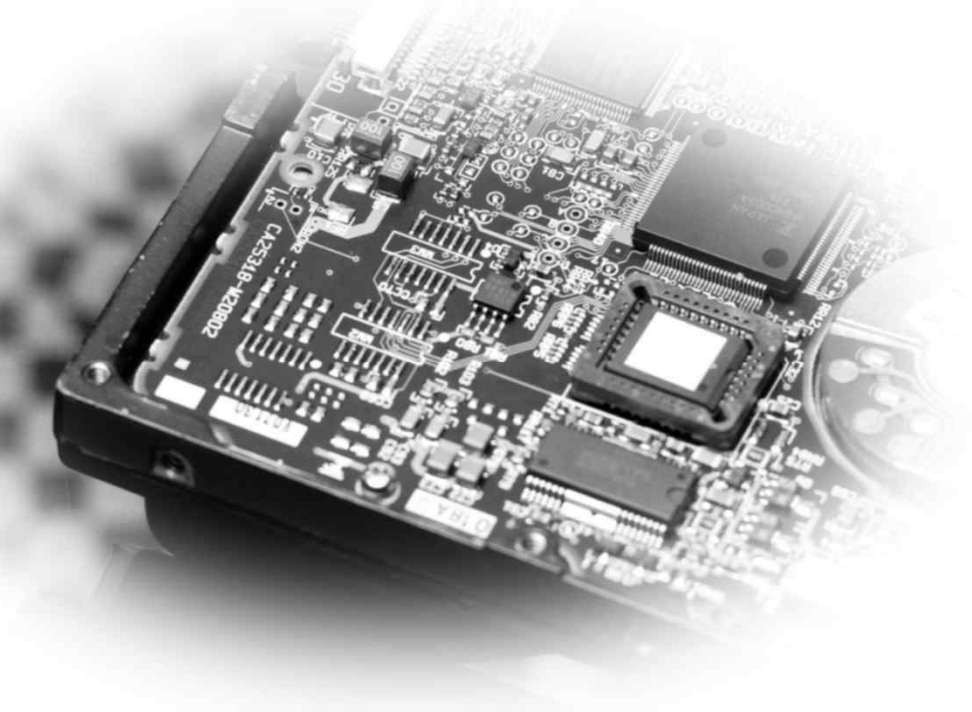
7) VPC 만들기 : 네트워크 트래픽 통제



세종사이버대학교

Route Table

“서브넷 단위 라우팅 통제”



7) VPC 만들기 : 네트워크 트래픽 통제



세종사이버대학교

Network ACL

✓	서브넷 단위
✓	Stateless 방화벽
✓	인바운드 & 아웃바운드 Rule 각각 적용
✓	허용(Allow), 거부(Deny) Rule
✓	매칭되는 낮은 번호 Rule 우선 처리(위에서 아래로)
✓	서브넷은 한 번에 오직 1개의 NACL을 가짐

- 그러나, 1개 NACL은 다수 서브넷 Association 가능

7) VPC 만들기 : 네트워크 트래픽 통제



세종사이버대학교



Network ACL

NACL의 Inbound Rule 예

Inbound						
Rule #	Type	Protocol	Port range	Source	Allow/Deny	Comments
100	HTTP	TCP	80	0.0.0.0/0	ALLOW	Allows inbound HTTP traffic from any IPv4 address.
110	HTTPS	TCP	443	0.0.0.0/0	ALLOW	Allows inbound HTTPS traffic from any IPv4 address.
120	SSH	TCP	22	192.0.2.0/24	ALLOW	Allows inbound SSH traffic from your home network's public IPv4 address range (over the internet gateway).
130	RDP	TCP	3389	192.0.2.0/24	ALLOW	Allows inbound RDP traffic to the web servers

7) VPC 만들기 : 네트워크 트래픽 통제



세종사이버대학교

보안그룹



인스턴스 단위



Stateful 방화벽

- Incoming Rule에 적용된 것은 자동으로 Outgoing Rule에 적용



허용(Allow) Rule Only(디폴트로 모든 Rule Deny)



인바운드 혹은 아웃바운드 Rule

7) VPC 만들기 : 네트워크 트래픽 통제



세종사이버대학교

보안그룹



순서에 관계없이 모든 Rule 적용



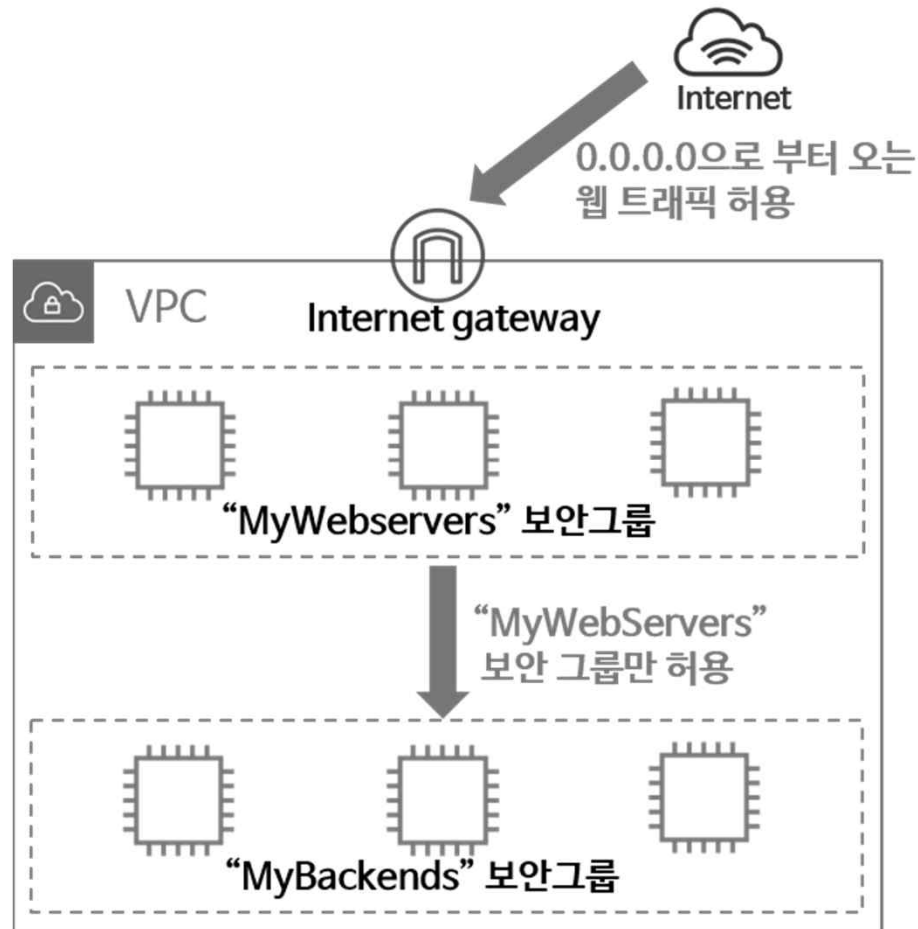
인스턴스는 보안그룹 여러 개를 가질 수 있음

7) VPC 만들기 : 네트워크 트래픽 통제

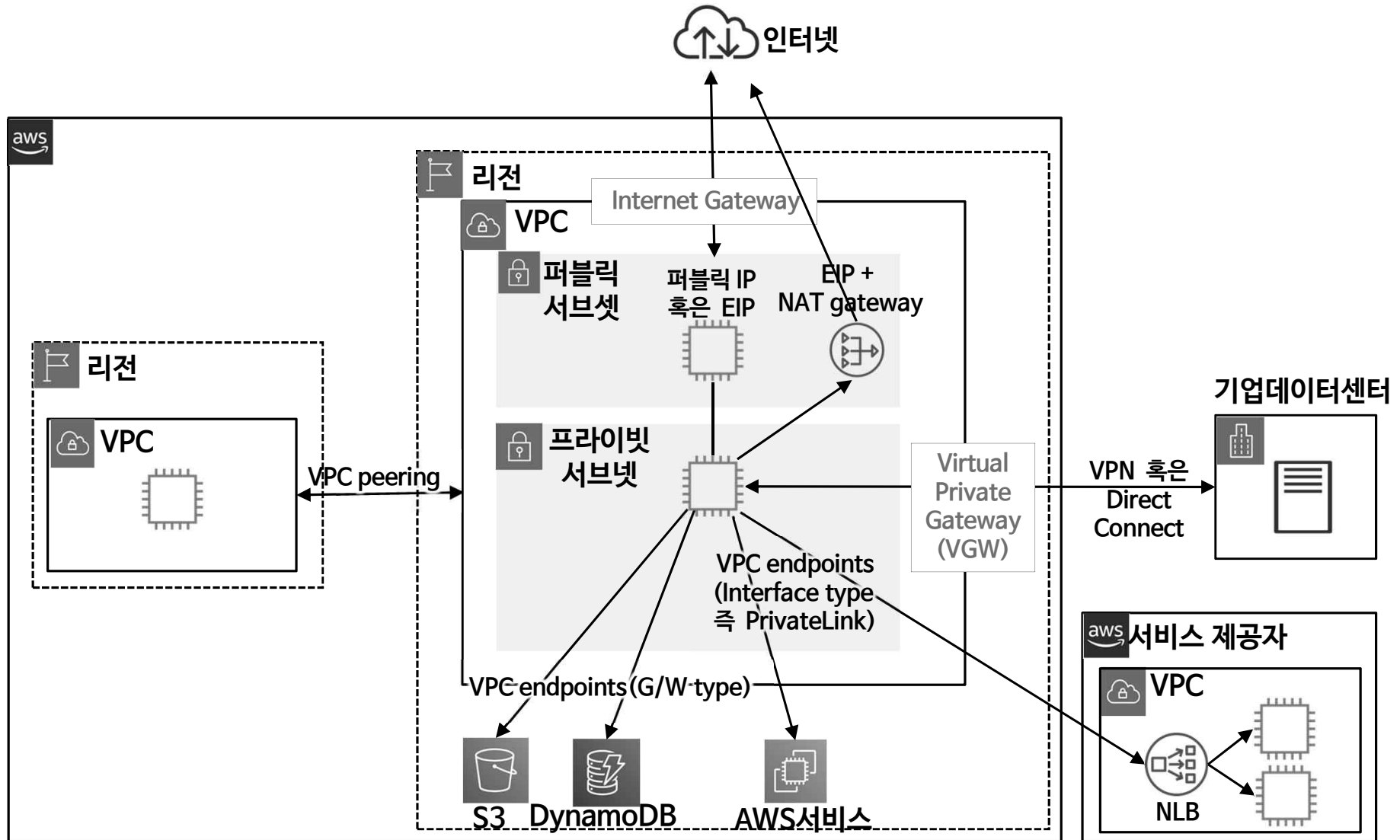


세종사이버대학교

보안그룹



8) VPC 확장 시나리오



8) VPC 확장 시나리오



인터넷 연결 : VPC Internet Gateway(IGW)



관리형 서비스(Managed Service)

- 확장성, 가용성, 중복성 보장 설계



VPC당 부착 가능한 Internet Gateway는 1개



VPC당 인스턴스와 인터넷 간의 통신



1:1 NAT(Network Address Translation) 수행

- 인터넷과 연결하려는 EC2 인스턴스는 퍼블릭 IP 혹은 EIP(Elastic IP)를 가져야 함

8) VPC 확장 시나리오



세종사이버대학교

인터넷 연결 : VPC Internet Gateway(IGW)



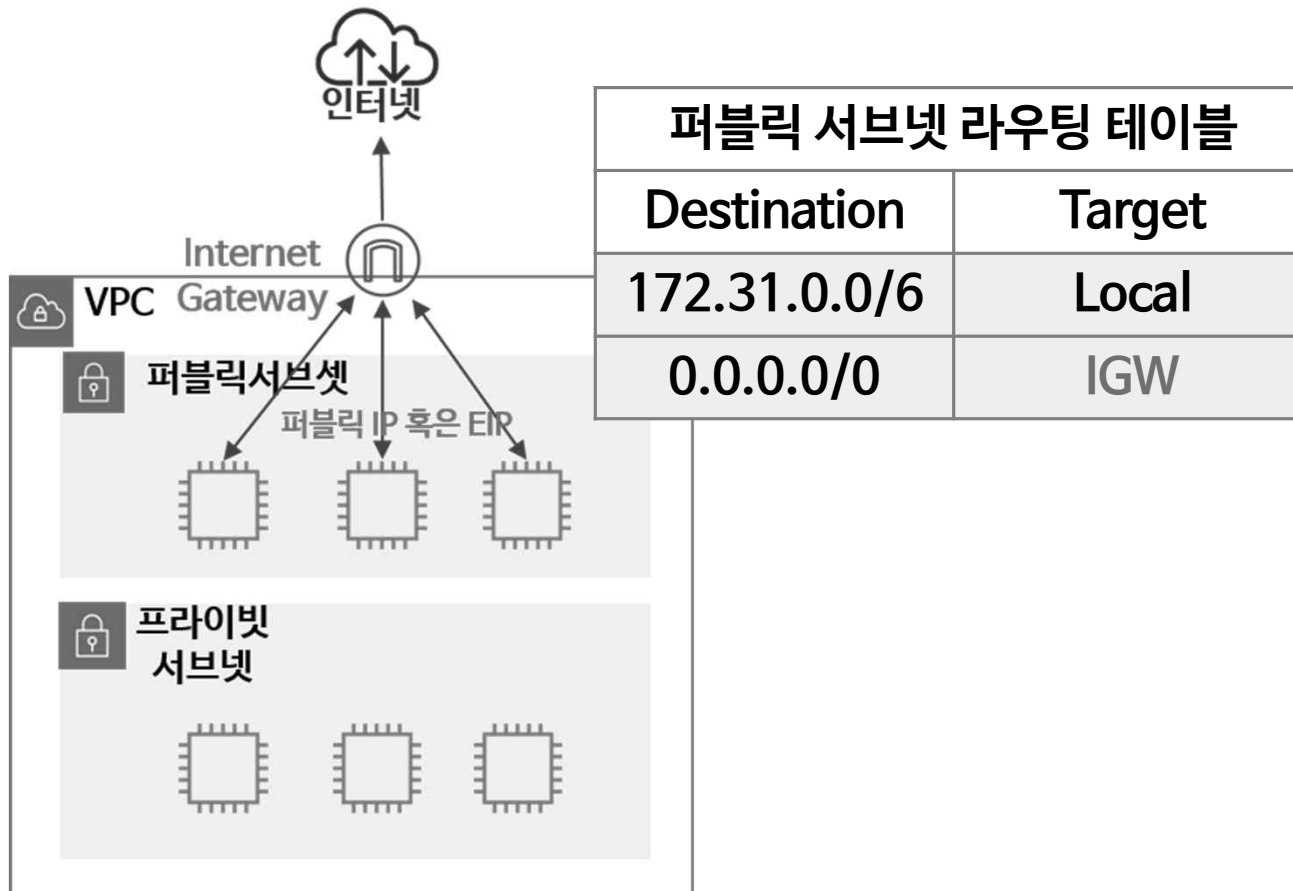
퍼블릭 서브넷의 라우팅 테이블 수정 필요



IPv4, IPv6 지원

8) VPC 확장 시나리오

인터넷 연결 : VPC Internet Gateway(IGW)



8) VPC 확장 시나리오



인터넷 연결 : VPC NAT Gateway(NAT-GW)



관리형 서비스(Managed Service)



Internet Access가 불가능한 프라이빗 서브넷에 있는 인스턴스들이 패치, 업데이트 다운로드 등을 위해 구성



인터넷 인터페이스를 위해 NAT Gateway 당 하나의 EIP 필요



TCP, UDP, ICMP Protocol 지원



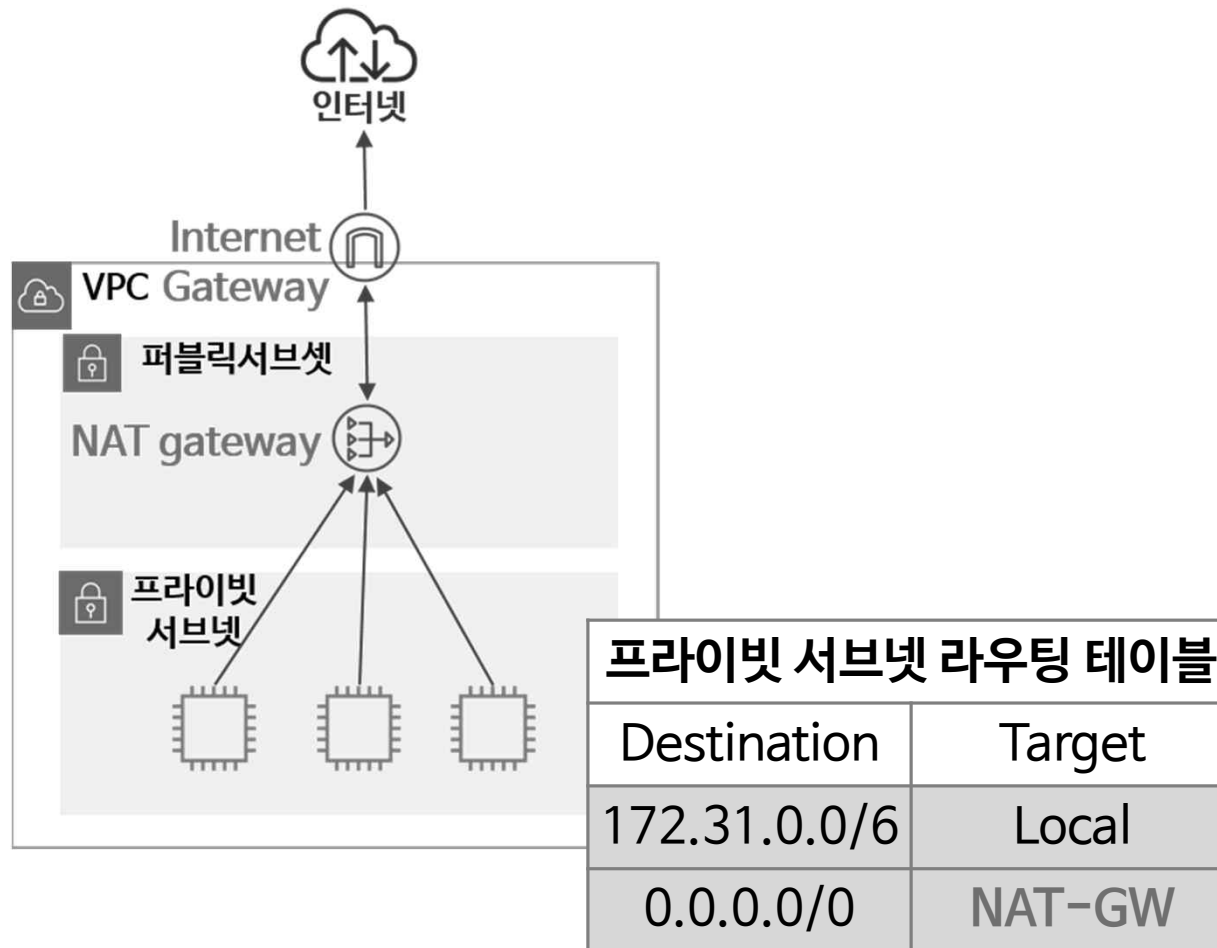
Network ACL을 통해 트래픽 통제

예

외부의 특정 서버에서만 Download 가능하도록 NACL로 통제 가능

8) VPC 확장 시나리오

인터넷 연결 : VPC NAT Gateway(NAT-GW)



8) VPC 확장 시나리오



인터넷 연결 : EIP(Elastic IP) 주소



Account에 할당되어 변경되지 않는 IP(고정 IP)



리전당 기본 5개의 Elastic IP 주소 할당 가능
(Soft-Limit)

- 할당(Allocation) / 반납(Release)
 - Account에 EIP 할당 혹은 반납
- 연결(Associate) / 분리(Disassociate)
 - EC2 혹은 NAT GW에 EIP 연결 혹은 분리

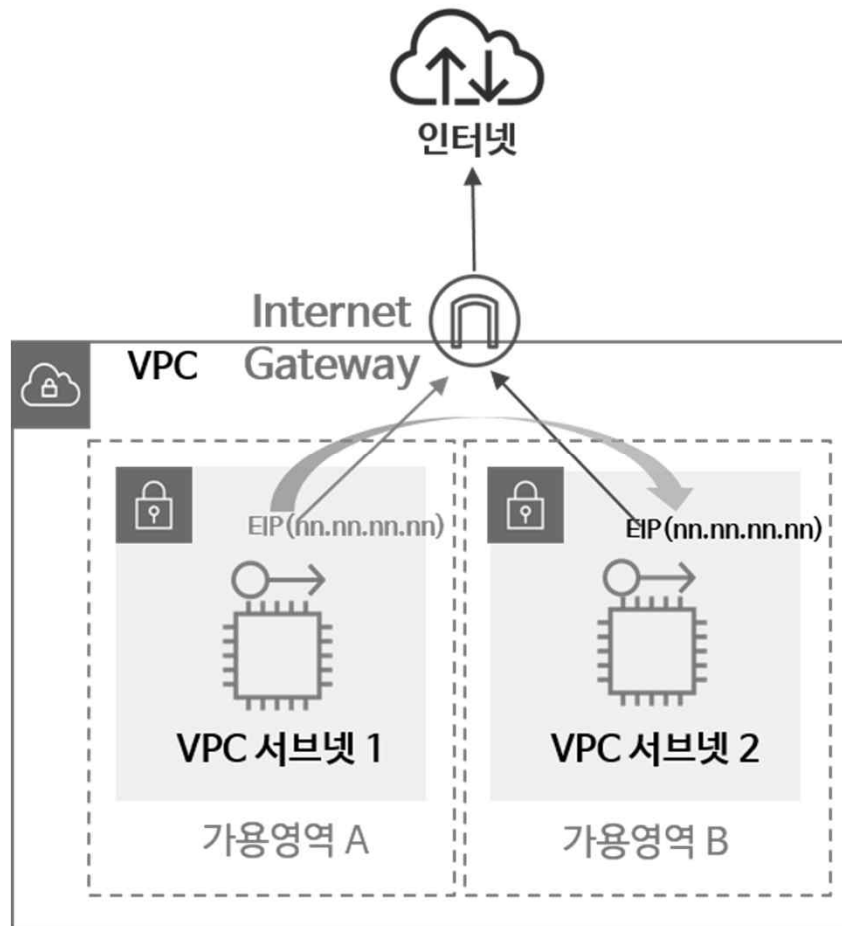


EC2 인스턴스 장애 시, 다른 EC2 인스턴스로 EIP를
Re-Associate하여 사용 가능

8) VPC 확장 시나리오



인터넷 연결 : EIP(Elastic IP) 주소



8) VPC 확장 시나리오



세종사이버대학교

VPC간 연결 : VPC peering

✓	IPv4 또는 IPv6 주소를 사용하여 2개 VPC간을 연결
✓	사용자의 자체 VPC 또는 다른 AWS 계정의 VPC와 피어링 연결 가능, 리전 간 연결 가능
✓	고가용성 및 Traffic에 대한 수평적 확장 제공
✓	라우팅 테이블을 이용하여 통제 가능하고, Transit Routing은 제공 안 됨
구성 사례	인증, 디렉터리 서비스, 모니터링, 로깅, 공통 서비스

8) VPC 확장 시나리오



세종사이버대학교

기업데이터센터 연결



VPN(가상사설망) 연결

- IPSEC 기반 Site to Site VPN



Direct Connect

- 전용선을 통한 기업데이터센터와 직접 연결

8) VPC 확장 시나리오



세종사이버대학교

네트워크 아키텍처의 단순화 : AWS Transit Gateway 활용




Regional 서비스인 AWS Transit Gateway를
활용하여 다수 VPC, VPN, Direct Connect를 연결



리전 간 Transit Gateway Peering 활용

8) VPC 확장 시나리오



 AWS 서비스 혹은 파트너 서비스와 인터넷을
경유하지 않은 프라이빗 연결
(IGW, NAT G/W 또는 VPN 불필요) : VPC Endpoint 활용

VPC Endpoint

Gateway Type

- 인터넷을 경유하지 않고
S3, DynamoDB
서비스로 프라이빗 연결

VPC Endpoint

Private Link Interface Type

- Private Link를 지원하는
AWS Services 혹은
파트너 서비스에 대하여
VPC Endpoint Network
Interface에 기반한
프라이빗 연결

9) VPC 실습 데모



세종사이버대학교



VPC 마법사를 통해
퍼블릭 서브넷(Public Subnet)과
프라이빗 서브넷(Private Subnet)
만들기

9) VPC 실습 데모



세종사이버대학교



리전(Region) 간 VPC Peering으로
글로벌 통합 네트워크 환경 구축하기