HANSUNG UNIVERSITY

Week 14

오픈소스 소프트웨어

한성대학교 컴퓨터공학부

한 기 준 교 수

가상 네트워크 서비스: VPC

Week 14

학습목표

- AWS VPC 이해하기
- 서브넷과 DHCP 이해하기
- 라우팅과 NAT 이해하기
- VPC 간 연결방법 이해하기

1 Amazon VPC

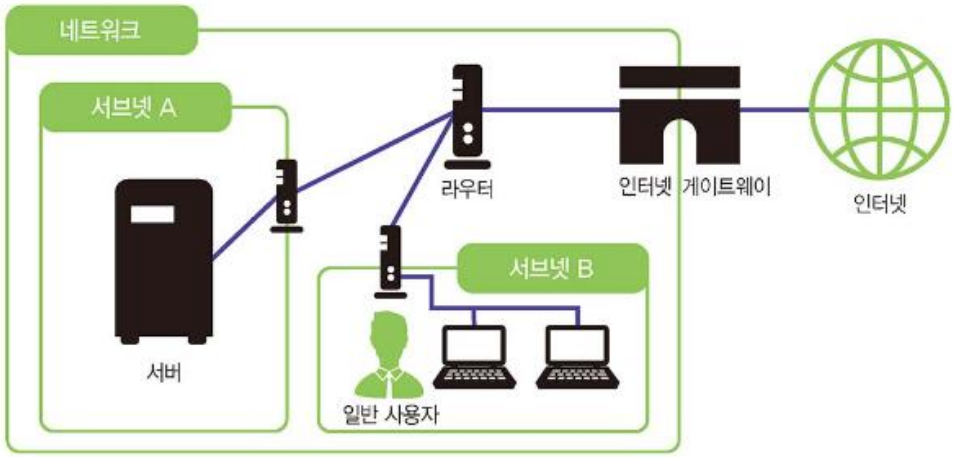
HANSUNG UNIVERSITY

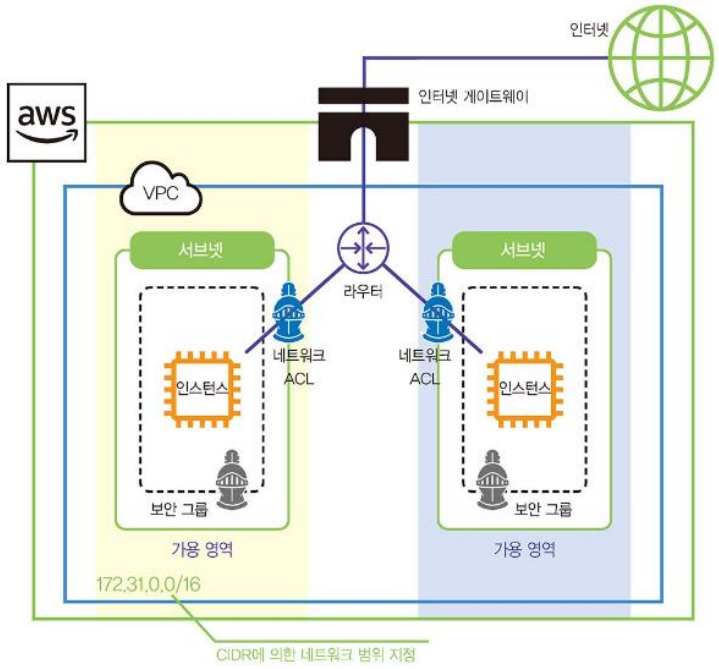
아마존 VPC

- 정의: AWS가 제공하는 AWS 계정 전용 가상 네트워크
- EC2 등의 AWS 서비스도 네트워크에 연결되어야 함
- 이러한 네트워크를 구축하기 위해 사용하는 Virtual Private Cloud (VPC)임
- Amazon VPC는 AWS 계정 전용 가상 네트워크 서비스로 AWS에서 제공하는 리소스만 설치할 수 있음
- 특히 EC2나 RDS의 경우 VPC를 선택하지 않으면 서버를 생성할 수 없음

VPC의 구성

- VPC 내에 서버를 설치하면 해당 네트워크에 소속되지만, 별도로 설정하지 않으면 VPC 자체는 격리된 네트워크가 됨
- 외부와 통신하려면 VPC를 인터넷 혹은 회사 내 LAN과 연결해야 함





VPC의 기능

- VPC는 네트워크, 서브넷 범위, 라우팅 테이블, 네트워크 게이트웨이 등과 같은 가상 네트워크 환경을 설정할 수 있음
- IPv4와 IPv6 둘 다 사용할 수 있음

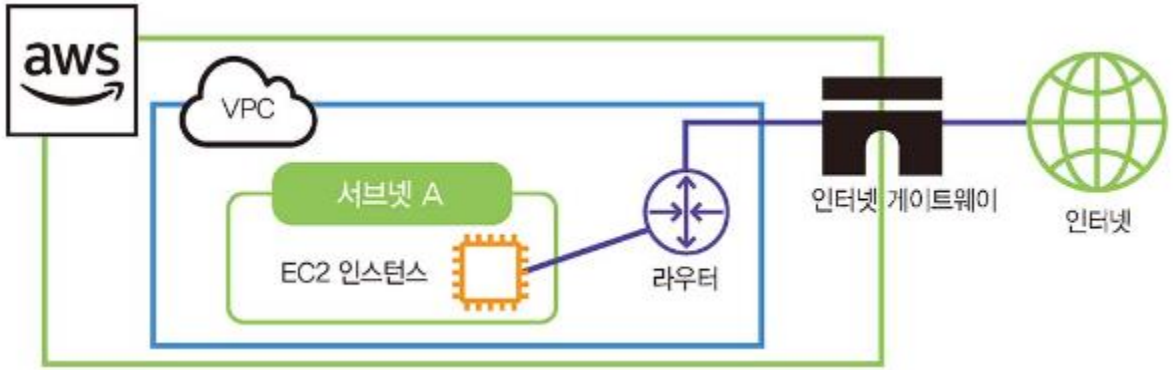
항목	내용
CIDR 블록	서브넷으로 네트워크를 나눈 범위
서브넷 마스크	네트워크의 크기를 계산하는 값
가용 영역	서브넷이 구축된 물리적 장소
인터넷 게이트웨이	인터넷에 접속하기 위한 출입구
라우팅	어떤 데이터를 어디에 보낼지 조정함
라우팅 테이블	라우팅에 대한 설정이 기록된 테이블
보안 그룹	AWS가 제공하는 가상 방화벽, 유입되는 데이터는 '거부 ' 가 기본 설정임
네트워크 ACL	AWS가 제공하는 가상 방화벽이며, 서브넷 단위로 설정됨

VPC 네트워크의 특징과 라우팅 테이블

- VPC는 물리적인 라우터가 아닌 소프트웨어가 라우팅을 수행함 (라우터는 IP주소를 갖지 않음)
- 라우팅은 설정된 라우팅 테이블에 따라 동작함
- 라우팅 테이블 하나에 서브넷 여러 개를 설정할 수 있음
- VPC 한 개에 인터넷 게이트웨이는 한 개만 설정할 수 있고, IP 주소를 갖지 않음
- 서브넷 사이의 통신은 라우터 없이 직접 통신할 수 있음

VPC 설정 유의 사항

- 서버(인스턴스)가 어떤 환경에 설치되어 있는지, 인터넷에 연결되야 하는지에 대한 설정이 필요함
- 인터넷 연결 여부 및 오토 스케일링에 대한 고려가 필수적임
  - 인터넷 연결이 필요하면 인터넷 게이트웨이를 설정해야 함
  - 오토 스케일링을 설정해야 한다면 IP주소를 많이 확보해야 함
- 보안 그룹과 네트워크 ACL을 설정하려면 인스턴스 용도에 맞는 포트를 설정해야 함
- 모든 포트가 닫힌 것이 기본 설정임



1 Amazon VPC

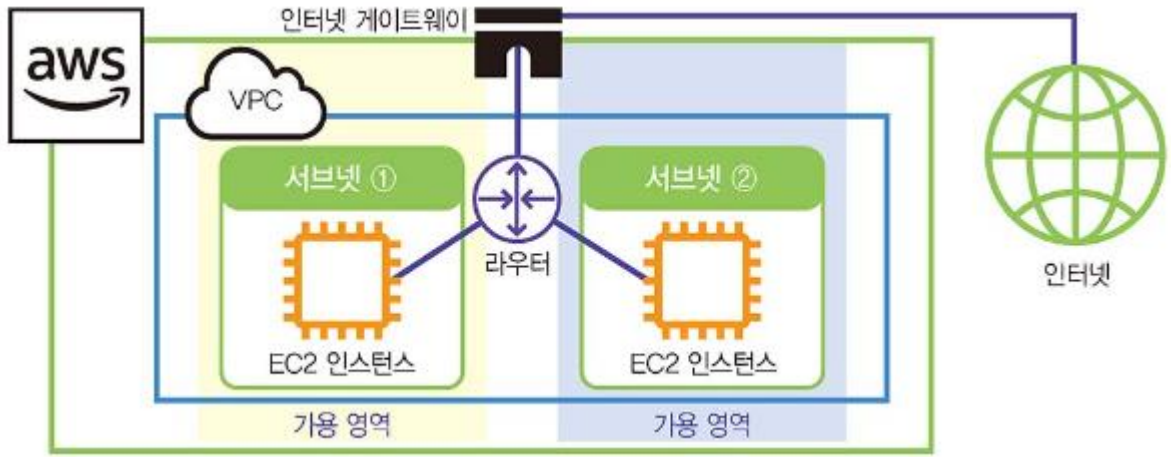
HANSUNG UNIVERSITY

VPC 사용 절차

- AWS에 로그인함
  - 리전을 선택하고 관리 콘솔에 접속함
  - VPC 대시보드에 접속함
- VPC를 생성함
  - VPC 이름을 정하고 CIDR 블록을 설정함
  - 테넌시 (하드웨어의 점유 여부)를 선택함
- 서브넷을 설정함
  - 서브넷 이름, 대상 VPC, 가용 영역, CIDR 블록을 설정함
- 인터넷에 연결함
  - 인터넷 게이트웨이를 생성함
  - IGW와 VPC를 연결함
  - 라우팅 테이블을 생성하고 라우팅을 설정함

기본 VPC

- 기본 VPC: 네트워크에 대한 지식이 없어도 이용할 수 있도록 리전별로 제공되는 기본 VPC 설정
- 기본 VPC에서 Elastic Load Balancing과 같은 서비스도 사용할 수 있음
- 기본 VPC는 서브넷과 인터넷 게이트웨이가 기본적으로 구성되어 있음
- 인터넷에 접속하고 싶지 않다면 별도의 VPC를 생성하거나 VPC 대시보드에 접속하여 기본 VPC를 변경해야 함



2 서브넷과 DHCP

HANSUNG UNIVERSITY

서브넷: 커다란 네트워크를 작게 나눈 네트워크

- 네트워크를 분할해 직접 통신할 수 있는 범위를 좁히고, 방화벽을 설정해 보안을 강화하는 것을 목적으로 함
- AWS의 경우 어떤 가용 영역의 서브넷을 들지 설정함 (즉, 서브넷은 물리적인 장소를 특정함)
- VPC는 사용자가 사용할 수 있는 네트워크 범위를 생성하고, 그 용도에 따라 작은 네트워크 (서브넷)을 설정함
  - 서브넷을 나누어 서브넷 A는 공개하고 서브넷 B는 비공개하는 등 서브넷별로 다른 역할을 부여할 수 있음
- 일반적인 네트워크의 경우 서브넷끼리 통신하려면 라우팅이 필요하지만, VPC의 경우에는 라우팅 없이 통신할 수 있음

2 서브넷과 DHCP

HANSUNG UNIVERSITY

CIDR (Classless Inter-Domain Routing)

- 네트워크와 서브넷의 범위를 나누는 데 사용되는 표기법
- /(슬래시) 뒤에 네트워크 길이를 숫자로 적어서 표기함
- CIDR은 IP 주소의 수를 나타냄 (/24 = 256개, /20 = 4,096개)
- 네트워크 범위는 범위 안에서 가장 첫번째 IP주소와 CIDR 순으로 표기함

2 서브넷과 DHCP

HANSUNG UNIVERSITY

네트워크 클래스

- 규모에 따라 A, B, C 세 클래스가 있음
- 기본 VPC는 /16 (B 클래스)로 설정되어 있으며 이를 /20으로 분할한 서브넷이 각 가용 영역에 구성되어 있음
- /20 서브넷은 IP주소 4,096개를 가지기 대문에 오토 스케일링을 설정해도 될 만큼 충분한 수의 IP 주소를 가지고 있음
- AWS의 경우 서브넷으로 사용할 수 있는 범위는 /16 (B 클래스 최대치) 이하이기 때문에 A 클래스를 서브넷으로 설정할 수 없음

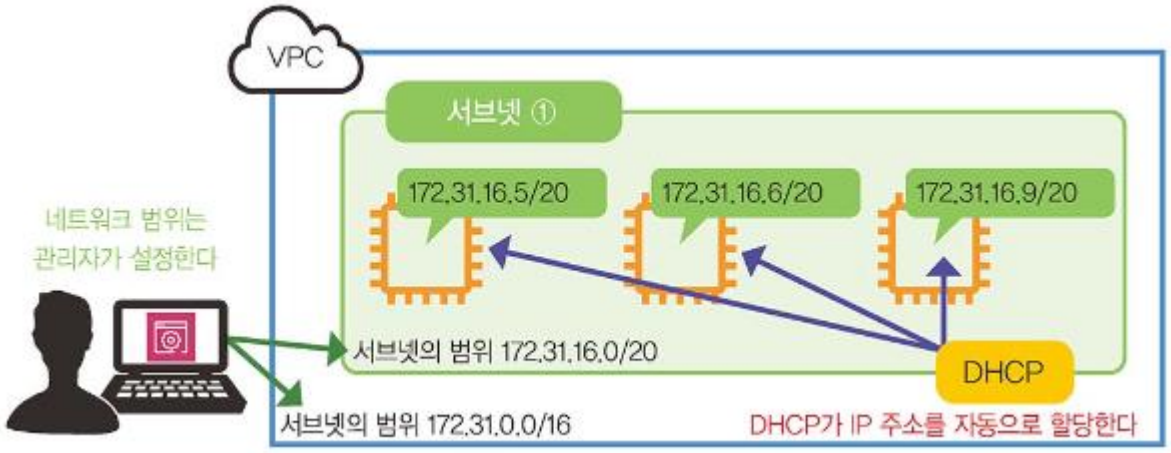
클래스	CIDR	IP 주소 수	사설 IP 범위
A 클래스	/8 ~ /15	131.072 ~ 16.777.216	10.0.0.0 ~ 10.255.255.255
B 클래스	/16 ~ /23	512 ~ 65,536	172.16.0.0 ~ 173.31.255.255
C 클래스	/24 ~ /32	1 ~ 256	192.168.0.0 ~ 192.168.255.255

2 서브넷과 DHCP

HANSUNG UNIVERSITY

IP 주소 할당과 DHCP

- AWS의 VPC는 EC2, RDS 인스턴스 외에도 라우터나 인터넷 게이트웨이의 IP 주소로도 앞서 설명한 예약 주소를 사용할 수 있음
- 네트워크 및 서브넷에 사용되는 IP 주소의 범위는 관리자가 설정할 수 있고 DHCP에서 각 인스턴스에 IP 주소를 자동으로 할당함
- VPC에는 DHCP 서버가 동작하고 있어 인스턴스가 추가되면 해당 서브넷 범위의 IP 주소 중에 하나가 할당됨
- VPC가 일반적으로 사용하는 IP 주소는 사설 IP 주소임

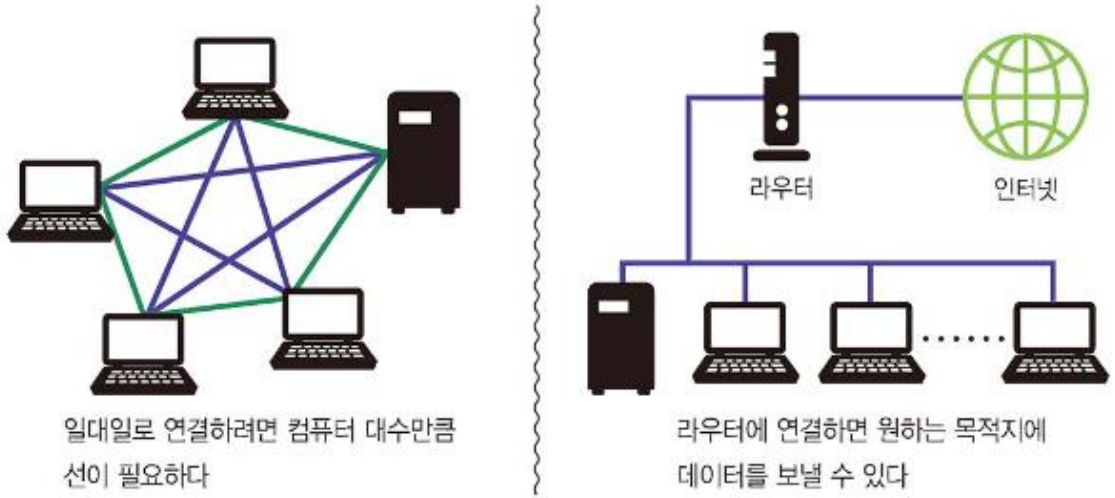


3 라우팅과 NAT

HANSUNG UNIVERSITY

네트워크와 라우팅

- 네트워크: PC 여러 대가 서로 통신할 수 있도록 연결되어 있는 상태
  - PC를 서로 일대일로 연결
  - LAN, WAN, 인터넷으로 연결해 라우터를 통해 데이터를 주고받음
- 라우팅: 데이터를 라우터로 보내고, 라우터가 목적지로 보내는 방식



일대일로 연결하려면 컴퓨터 대수만큼 선이 필요하다

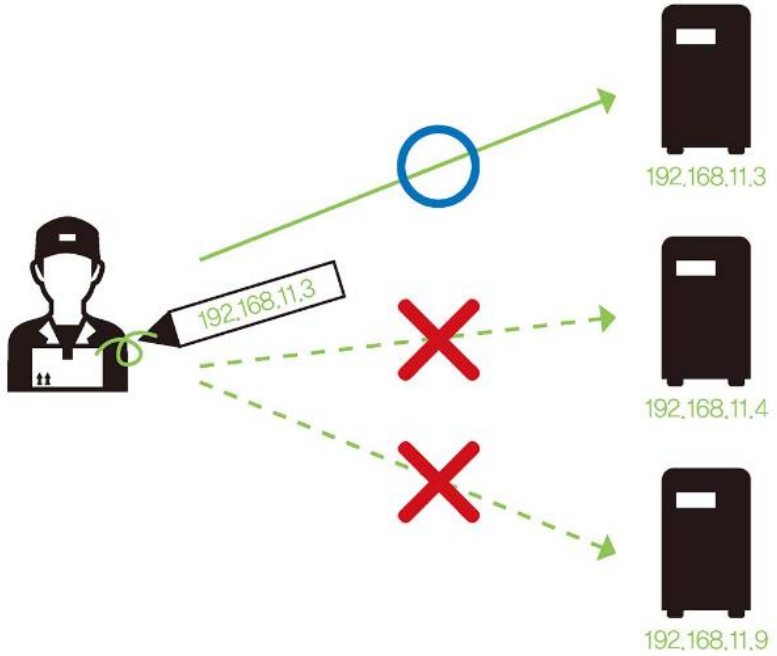
라우터에 연결하면 원하는 목적지에 데이터를 보낼 수 있다

3 라우팅과 NAT

HANSUNG UNIVERSITY

IP 주소와 게이트웨이

- IP주소: 라우터가 각 PC에 데이터를 전달하기 위해 대상을 식별할 수 있는 주소
- 라우터에는 목적지로 가장 빠르게 전송할 수 있는 경로 정보가 설정되어 있음
- 라우터는 네트워크의 관문에 위치해 있기 때문에 관문이라는 의미의 게이트웨이라고 불림
- 기본 게이트웨이: 자신 이외의 접속되어 있는 모든 것 (대부분의 경우 인터넷과의 연결점)

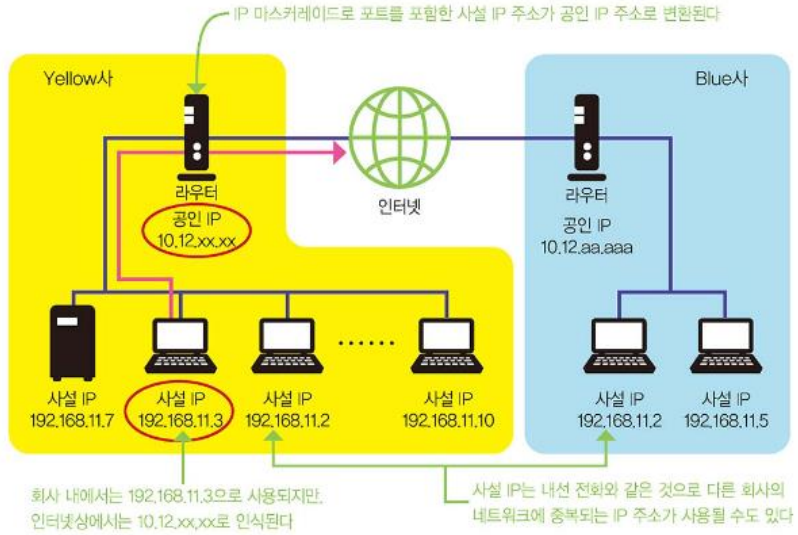


3 라우팅과 NAT

HANSUNG UNIVERSITY

IP 마스커레이드

- 게이트웨이의 역할을 하는 라우터가 LAN에서 전송되는 데이터를 인터넷으로 보내고, 인터넷에서 들어오는 데이터를 목적지 PC로 전송함
- LAN 내부의 PC에는 사설 IP 주소를 할당하는 게 일반적임
- 인터넷상에서 공인 UP주소가 없다면 식별할 수 없기 때문에 게이트웨이가 사설IP주소를 공인 IP주소로 변환하고 가정/회사 내에서는 공인 IP주소 하나를 공동으로 사용함
- 주소 변환을 담당하는 것이 IP 마스커레이드 (masquerade) 혹은 NAPT (Network Address Port Translation)임

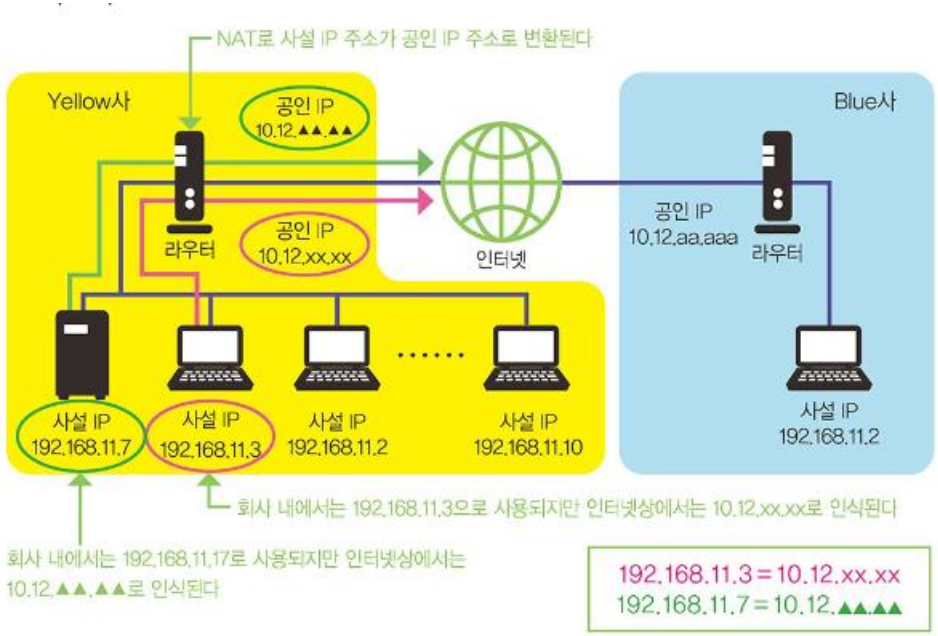


3 라우팅과 NAT

HANSUNG UNIVERSITY

NAT (Network Address Translation)

- IP 마스커레이드를 사용하면 내부에서 외부로 나가는 것은 가능하지만, 외부에서 내부로 들어오는 것은 불가능함
- 서버가 양방향으로 통신할 수 있도록 IP 마스커레이드를 설정해야 함
- IP 마스커레이드는 공인 IP 하나만 설정할 수 있기 때문에 서버가 여러 대라면 공인 IP 주소를 여러 개 설정할 수 있는 NAT를 사용해야 함
- IP 마스커레이드와 NAT의 차이점
  - IP 마스커레이드는 일대다인 것에 비해 NAT는 다대다의 특성을 지님
  - IP 마스커레이드는 포트를 변환할 수 있으나, NAT는 포트를 변환할 수 없음
- NAT와 UP 마스커레이드는 AWS의 인터넷 게이트웨이와 NAT 게이트웨이에 해당함

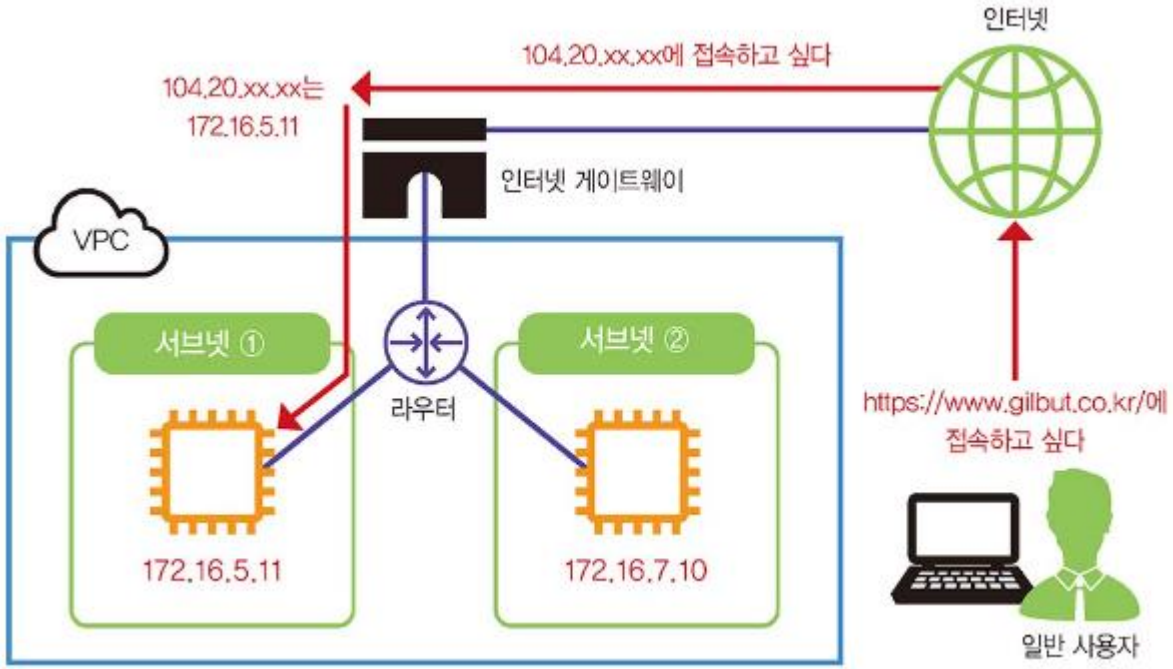


3 인터넷/NAT 게이트웨이

HANSUNG UNIVERSITY

인터넷 게이트웨이

- EC2 인스턴스와 인터넷 연결을 담당하는 역할을 수행함
- 요청된 EC2 인스턴스의 연결 정보를 가지고 있는 인터넷 게이트웨이가 공인 IP 주소를 사설 IP 주소로 변환하여 해당 EC2 인스턴스에 요청을 보냄

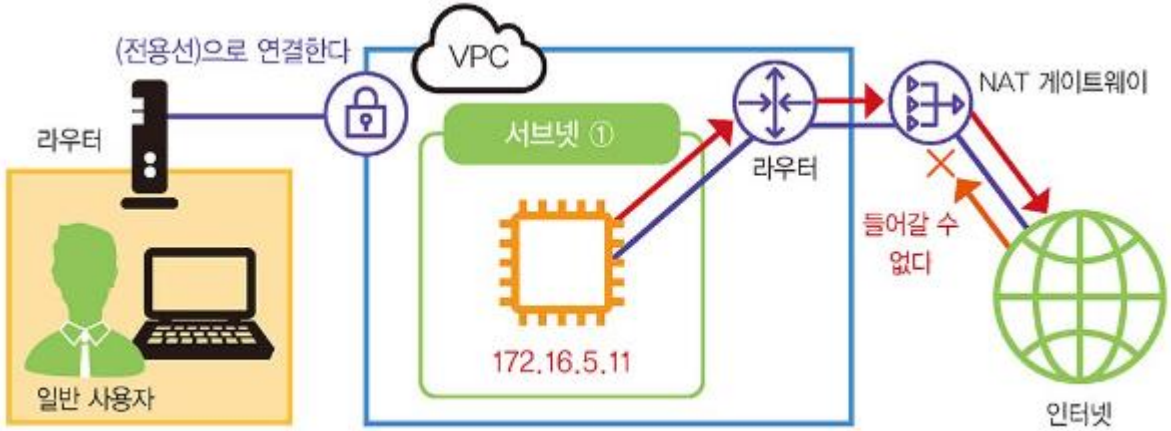


3 인터넷/NAT 게이트웨이

HANSUNG UNIVERSITY

NAT 게이트웨이

- 회사 내부에서만 사용하는 서버가 인터넷에 연결해야 할 때 사용할 수 있는 게이트웨이
- 서브넷에서 인터넷으로 접속할 수 있으나, 인터넷에서 서브넷으로 접속하지 못함



4 보안 그룹과 네트워크 ACL

HANSUNG UNIVERSITY

보안 그룹과 네트워크 ACL

- 방화벽: 네트워크 통신을 제어하는 방식
- 보안 그룹과 네트워크 ACL은 인바운드 트래픽 (데이터가 유입되는 것)과 아웃바운드 트래픽 (데이터가 유출되는 것)을 제어함
- 반드시 양쪽 모두 설정해야 하며 명시적으로 설정하지 않으면 기본 설정이 적용됨
- 네트워크 ACL은 서브넷 단위로 설정하기 때문에 개별 인스턴스에 설정할 필요가 없음

항목	보안 그룹	네트워크 ACL
설정 범위	인스턴스에 대해 설정함 (보안 그룹을 최대 5개 설정할 수 있음)	서브넷에 설정함
규칙	규칙 허용만 가능함	규칙 허용과 거부가 가능함
설정	스테이트풀 (Stateful)	스테이트레스 (Stateless)
규칙의 적용 순서	모든 규칙을 확인하여 트래픽의 허가 여부를 정함	순서대로 규칙을 처리하고 트레픽의 허가 여부를 정함

4 보안 그룹과 네트워크 ACL

HANSUNG UNIVERSITY

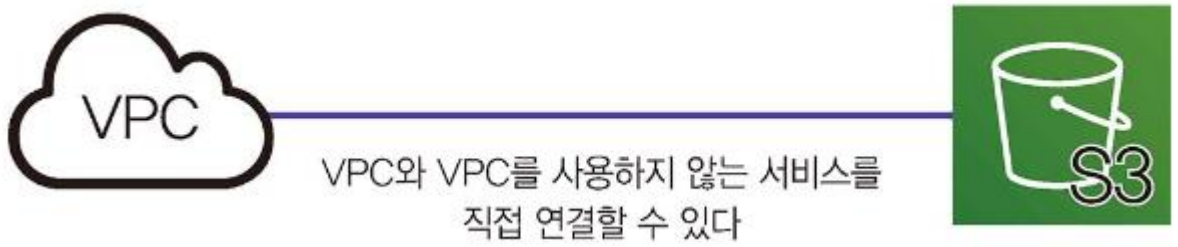
인바운드, 아웃바운드 설정 및 주요 포트 번호

- 트래픽은 인바운드, 아웃바운드 각각 포트 단위로 허가 여부를 설정함
- 포트: 통신의 입구
- 보안 그룹은 인바운드를 허가하지 않으며 아웃바운드를 허가하고, 네트워크 ACL은 양쪽 모두를 허가하는것이 기본 설정임
- 보안 그룹은 필요한 포트만 허가하는 것이 일반적임
- 주요 포트 번호
  - 25: 메일 송신을 위한 SMTP 서비스
  - 80: 웹 송수신을 위한 HTTP 서비스
  - 443: 웹 송수신을 위한 HTTPS 서비스
  - 3306: 데이터베이스 통신을 위한 SQL Server 서비스
  - 3389: 원격 데스크탑 연결을 위한 RDP 서비스

5 VPC 엔드포인트

HANSUNG UNIVERSITY

- **VPC 엔드포인트: VPC 내부에서 VPC 외부로 접속하기 위한 연결점을 제공하는 서비스**
  - VPC 외부의 다른 서비스와 VPC를 연결하려면 인터넷 게이트웨으를 사용해 인터넷으로 접속해야 함
  - AWS의 모든 서비스가 VPC내에 설치되어 있는 것은 아님 (예: S3, DynamoDB)
  - 인터넷 게이트웨이를 통하지 않고, S3와 같은 VPC 외부에 있는 서비스와 VPC를 연결해주는 것이 VPC 엔드포인트 서비스임
  - VPC의 출입구로 엔드포인트를 설정하면 S3와 직접 연결할 수 있음

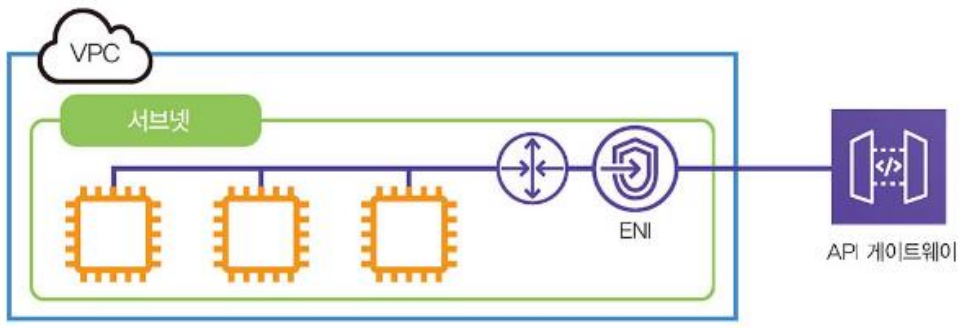


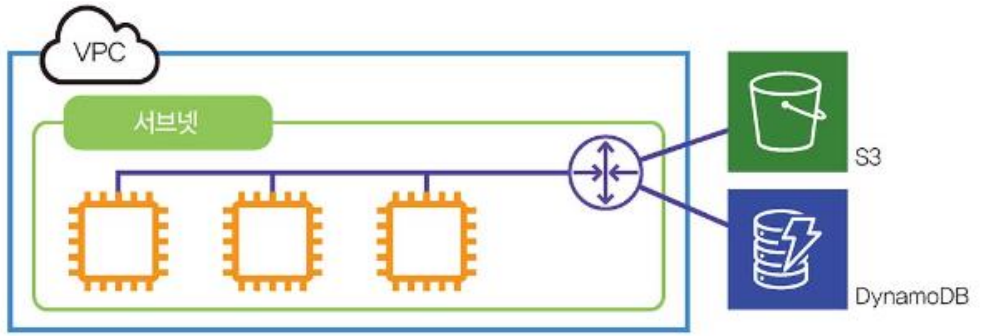
5 VPC 엔드포인트

HANSUNG UNIVERSITY

인터페이스/게이트웨이 엔드포인트

- 인터페이스 엔드포인트: 네트워크 인터페이스로 구축하는 유형
  - 사설 IP주소를 가진 ENI가 존재하며, 각 서비스와 연결하는 출입구 역할을 함
  - AWS PrivateLink라는 방식을 사용하기 때문에 AWS 외의 타사 서비스가 PrivateLink를 지원한다면 사용할 수 있음
- 게이트웨이 엔드포인트: 라우팅 테이블에 설정된 내용을 라우팅하는 유형
  - 서비스 리전 단위로 라우팅 테이블을 설정함
  - 한번 설정하면 해당 리전의 모든 서비스에 사용할 수 있음
  - S3와 DynamoDB가 게이트웨이 엔드포인트 방식을 채택하고 있음



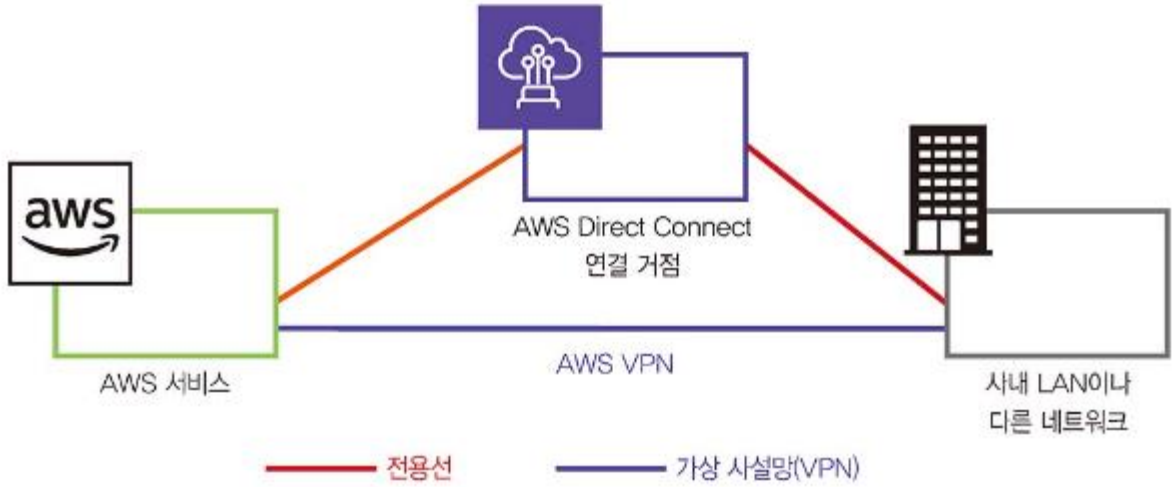


6 VPC 연결

HANSUNG UNIVERSITY

VPC 연결

- VPC는 다른 VPC를 VPC 피어링이라는 기능을 통해 연결할 수 있음
- VPC는 물리적인 네트워크 혹은 다른 클라우드에도 접속할 수 있음
- VPN을 사용하면 AWS와 사내 LAN, 온프레미스를 안전하게 연결될 수 있어 해킹 위험을 줄일 수 있음
- AWS는 전용선 서비스로 AWS Direct Connect를 제공하며 가상 사설망 서비스로 AWS VPN을 제공함



6 VPC 연결

HANSUNG UNIVERSITY

전용선과 가상 사설망

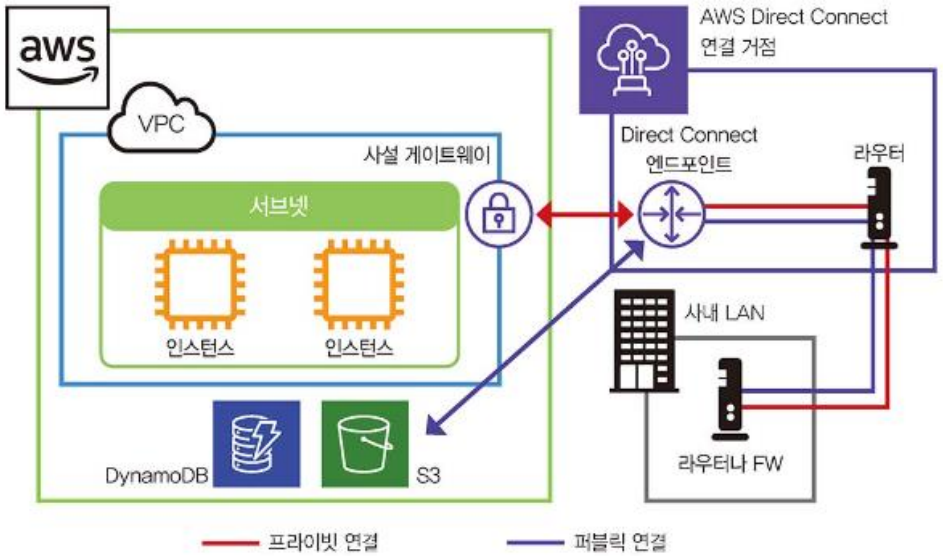
- WAN (Wide Area Network): 네트워크와 네트워크를 연결해 커다란 네트워크를 구축하는 것
  - 전용선: 통신 사업자가 직접 연결할 수 있는 전용선을 임대하여 구축함. 비싸지만 안전하고 신뢰성이 높음
  - 가상 사설망: 보유하고 있는 회선 및 공용 회선을 사용하여 거점끼리 통신을 암호화하여 연결함. 비용은 싸지만 신뢰성이 낮음.
- 인터넷 VPN은 인터넷 회선만 사용하므로 VPN을 지원하는 라우터만 설치하면 사용가능함

6 VPC 연결

HANSUNG UNIVERSITY

AWS Direct Connect: VPC나 AWS 서비스와 다른 네트워크를 전용선으로 연결하는 서비스

- 전용선에 접속하기 때문에 회선 공사가 필요함
- AWS에 해당 접속을 처리할 라우터를 설치해야 하므로 도입 규모가 크며 월 비용도 많이 발생함
- 비용을 줄이기 위해 AWS 파트너가 제공하는 연결 서비스를 사용할 수 있음
- 프라이빗 연결: VPC에 사설 게이트웨이를 구축하고 이를 경유하여 통신하는 방법
- 퍼블릭 연결: VPC를 지원하지 않은 서비스를 사용할 수 없을때 각 서비스에 직접 연결하는 방법



6 VPC 연결

HANSUNG UNIVERSITY

AWS VPN

- 인터넷 VPN을 사용하여 다른 네트워크와 연결함
- VPC에 VPG (Virtual Private Gateway)를 구축하면 주요 라우터 기종의 설정 파일을 사용할 수 있어 이를 수정하여 라우터를 설정함
- 간단한 반면 인터넷을 사용하므로 네트워크 품질과 속도를 보장하지 않음
- 퍼블릭, 프라이빗 연결과 같은 구분이 없고 VPC만 접속할 수 있음
- VPC를 지원하지 않는 서비스에 접속해야 할 경우 VPC에 연결한 다음 이를 해당 서비스로 연결함

6 VPC 연결

HANSUNG UNIVERSITY

- **전송 게이트웨이 :VPC나 온프레미스를 하나로 묶어 서로 연결하는 접속점을 제공하는 서비스**
  - 서로 다른 AWS 계정을 연결할 수 있음
  - 네트워크 여러 개를 중앙 거점으로 집약하여 통신 경로를 통합적으로 처리함
  - 중앙 거점을 활용함으로 연결된 네트워크 수가 많아져도 VPC 피어링, AWS Direct Connect 게이트웨이 등을 통합 관리하기 때문에 효율적으로 네트워크를 관리할 수 있음