네트워크 및 콘텐츠 전송 서비스(1)

네트워크 중요 용어 익히기

1. IP 주소(Address)는 네트워크의 번지(주소)
    - IP 주소
        - 웹 서버의 위치를 특정할 수 있는 정보
        - 일반적으로 IPv4가 표준으로 사용됨
            - **IPv4:** 주소가 2^32개 (약 43억 개) 존재
            - **IPv6:** 주소가 2^128개 (약 340억 개) 존재
    - 최근 IPv4만으로는 주소를 할당할 수 없을 정도로 기기가 많아져 IPv6이 주목받고 있음

2. 퍼블릭 IP 주소와 프라이빗 IP 주소
    - **퍼블릭 IP 주소=글로벌 IP 주소=공인 IP:** 특정 가능한 주소(식별 가능)
    - **프라이빗 IP 주소=사설 IP:** 닫힌 네트워크(근거리 통신-LAN) 내에서만 식별 가능

3. CIDR 블록으로 IP 주소 범위 결정
    - **CIDR(Classless Inter-Domain Routing) 블록:** IP 주소를 이용해 네트워크 범위를 정하는 것
    - IP 주소를 나타내는 숫자열: 네트워크 부분 + 호스트 부분
        - 네트워크 부분: 네트워크 정의
        - 호스트 부분: 네트워크 안에서 접속 가능한 서버 등을 나타냄
    - 서브넷 마스크: ‘/’ 와 숫자로 네트워크 범위 표기

4. 방화벽에서 허용된 통신만 통과
    - 방화벽: 보안 위협으로부터 시스템을 지키기 위해 사용하는 것
        - 하드웨어 형태, 소프트웨어 형태
        - AWS: 보안 그룹, 네트워크 ACL 같은 방화벽 기능을 가진 서비스 존재

5. 부하 분산을 위해 여러 서버에 접속 분배
    - 부하 분산: 서버를 여러 대 구성해 각 서버가 처리를 나눠서 할 수 있게 구축하는 것
    - **로드 밸런서(Load Balancer):** 부하 분산을 위해 일반적으로 사용하는 장치

6. 라우팅 및 라우팅 테이블
    - 라우터(router): IP 주소를 찾기 위한 최적의 경로를 찾아 결정하고 연결해주는 것
    - 라우팅(routing): 라우터가 IP 주소까지의 경로를 결정하는 것
    - 라우팅 테이블: 라우터가 소유한 경로 정보

7. 도메인 이름과 IP 주소를 연결하는 DNS
    - 도메인(domain)
        - 점으로 연결된 문자열로 구성, 기업/단체 이름을 표현하는 경우 多
        - 해당 문자열에 표시되는 기업/단체 등이 제공하는 사이트의 주소 정의
        - IP 주소가 연결되어 있어 사용자는 도메인 이름 만으로 사이트에 접속 가능
    - **DNS(Domain Name System)**
        - 이름 해석: 도메인 이름에 연결된 IP 주소를 찾아주는 DNS의 기능

Amazon VPC로 가상 네트워크 만들기

1. 가상 네트워크 Amazon VPC

- **Amazon Virtual Private Cloud (이후 VPC):** AWS에서 생성할 수 있는 프라이빗 가상 네트워크 공간
- 퍼블릭 VPC, 프라이빗 VPC 구축 가능
- VPC 논리 분리, 여러 VPC 연결 가능
- VPC 제작 시 CIDR 블록을 지정하고 지정한 CIDE 블록 네트워크 확보
- VPC는 일반적으로 프라이빗 IP 주소 사용

  기본적으로 프라이빗 IP 주소 공간을 CIDR 블록에 지정하는 것이 좋음
- 외부 네트워크와의 접속을 검토하고 있을 경우 접속할 네트워크와 VPC의 CIDR 블록이 중복되지 않도록 주의해야 함 → 중복 시 직접 연결 불가
- 호스트 주소는 여유를 갖도록 가능한 한 많이 확보해두는 것이 좋음

2. VPC 및 서브넷 생성
   - AWS Management Console 또는 API를 사용해 생성 가능
     - VPC이름(Name 태그)
     - CIDR 블록
     - IPv6 설정
     - **테넌시 (전용 하드웨어 사용 여부):** 하드웨어 독점 경우에만 독점 옵션 지정
   - VPC 만으로는 EC2와 같은 자원을 네트워크에 만들 수 없음

     → VPC 안에 더 작은 네트워크 단위인 서브넷을 만들어야 함
   - 서브넷
     - 하나의 AZ에 속해야 하며, 여러 AZ에 걸쳐 있을 수 없음

       → 여러 AZ에 자원을 배치해 가용성을 높이려면 서브넷도 여러 개 생성해야 함
     - 생성할 VPC의 CIDR 블록 범위 내에서 CIDR 블록을 지정해야 함

Amazon VPC의 주요 기능 사용법

1. 라우팅 정보를 설정해 인터넷과 통신

- 라우팅 테이블: 네트워크의 경로 정보
  - 온프레미스: 라우터와 같은 네트워크 기기에 라우팅 테이블 설정
  - AWS
    - VPC에 라우팅 테이블 생성, 각 서브넷에 사용할 라우팅 테이블 지정
    - VPC를 통해 흐르는 패킷은 이 라우팅 테이블의 정보를 기반으로 경로 결정
    - VPC를 만들 때 기본적으로 하나의 라우팅 테이블 생성 → VPC 외부로는 통신X
    - 외부와 통신하려면 외부 라우팅 정보를 추가

      → 인터넷 게이트웨이를 통해 인터넷과 통신
- 인터넷 게이트웨이
  - 서브넷 안에 있는 EC2와 같은 자원이 인터넷과 통신할 수 있게 하기 위한 기능
  - 인터넷 게이트웨이 생성 → 서브넷 라우팅 테이블에 설정 → 인터넷 VPC 통신 가능
  - 퍼블릭 서브넷: 인터넷 게이트웨이로 가는 경로가 설정된 서브넷

    프라이빗 서브넷: 인터넷 게이트웨이를 통해 인터넷과 통신할 수 없는 서브넷
  - EC2
    - 퍼블릭 IP, Elastic IP: EC2에 설정 가능한 퍼블릭 IP 주소
    - 퍼블릭 IP: 자동으로 부여되는 IP 주소, 재부팅 시마다 변경

      Elastic IP: 정적 IP, 영구적으로 사용 가능한 IP 주소
- NAT(Network Address Translation) 게이트웨이
  - 인터넷에서 VPC로 통신 불가능한 단방향 통신 → 외부와 더 안전히 통신
  - 프라이빗 IP 주소를 퍼블릭 IP 주소로 변환
  - 외부 통신을 수행하는 서브넷의 라우팅 테이블에 경로 정보를 등록해야 이용 가능
- VPC 접근 제어 및 통신 로그 확인

    - 네트워크 접근 제어 목록(이후 네트워크 ACL): 서브넷 단위로 접근 제어 설정 가능
    - 보안 그룹과 조합해 접근 제어 설정 가능
    - VPC 흐름 로그: VPC 내의 IP 트래픽 상황을 로그로 저장할 수 있는 기능
    - 네트워크 인터페이스(ENI, Elastic Network Interface)

VPC에서 VPC, 외부 서비스, 온프레미스와의 연결

1. VPC와 외부 네트워크 연결
    - VPC 피어링: 서로 다른 두개의 VPC를 연결해 통신, 연결된 VPC의 CIDR 블록은 겹치면 안됨
    - AWS Transit Gateway(이후 Transit Gateway): AWS 네트워크 연결을 중앙에서 관리

2. VPC와 VPC 외 AWS 서비스 연결
    - VPC 엔드포인트: AWS 서비스가 프라이빗 네트워크로 통신하게 할 수 있음
    - 게이트웨이 엔드포인트
        - S3, DynamoDB에서 사용하는 VPC 엔드포인트
        - AWS 서비스와의 통신은 퍼블릭 IP 이용
    - 인터페이스 엔드포인트
        - AWS PrivateLink라는 기능을 사용해 서브넷에 서비스 접속용 ENI(네트워크 인터페이스)를 생성해 프라이빗 IP로 통신
        - 많은 AWS 서비스 지원

3. VPC와 온프레미스 네트워크 연결
    - AWS Site-to-Site
        - 온프레미스 환경의 네트워크와 VPC를 VPN으로 연결하는 기능

    - **VPN(Virtual Private Network)**
        - 가상으로 프라이빗 네트워크를 구성해 통신하는 기술
        - VPN 접속 시 외부 네트워크와 프라이빗 IP 주소로 통신 가능
- AWS Client VPN: 특정 단말과 비공개로 연결하고 싶은 경우
- AWS Direct Connect
    - AWS와 온프레미스 환경을 전용선으로 연결하는 기능
    - AWS의 데이터 센터와 직접 연결하는 것이 아닌, Direct Connect 로케이션이라는 기존 연결 지점을 통해 연결
    - VPN 연결과 비교해 빠르고 고품질의 네트워크 사용 가능