Module 4

VPC (Virtual Private Cloud)

- AWS에서 사용 가능한 가상의 프라이빗 네트워크
- EC2 인스턴스와 ELB 요소 배치 가능
- 프라이빗 게이트웨이로 VPC 간의 VPN 연결 생성
- 리전 내 모든 영역에 걸칠 수 있음

인터넷 게이트웨이

- VPC와 인터넷 간 연결 → 게이트웨이가 없으면 접근 불가능

비공개 리소스만 존재하는 VPC 접근?

가상 프라이빗 게이트웨이

- 보호된 인터넷 트래픽이 VPC로 들어오도록 허용 하는 구성 요소
- 승인된 네트워크에서 나오는 트래픽만 VPC로 들어가도록 허용

AWS Direct Connect

- 데이터센터 – VPC 비공개 전용 연결 설정 서비스
- 네트워크 비용 절감, 대역폭 증가

서브넷 및 네트워크 액세스 제어

- 기본 네트워크 액세스 제어 목록은 상태 비저장, 모든 인바운드 / 아웃운드 트래픽을 허용

패킷

- 인터넷에 보내는 메시지, 서브넷 경계를 지나면 네트워크 ACL에서 검사
- 인터넷 / 네트워크를 통해 전송되는 데이터 단위

서브넷

- 보안 또는 운영 요구사항에 따라 리소스를 그룹화 할 수 있는 VPC 내의 섹션
- 퍼블릭 또는 프라이빗으로 구성
- 퍼블릭 서브넷 : 누구나 액세스할 수 있는 리소스 포함
- 프라이빗 서브넷 : 프라이빗 네트워크를 통해서만 접근 가능한 리소스

VPC의 네트워크 트래픽

- 패킷은 인터넷 게이트웨이 를 통해 VPC 로 이동
- 서브넷을 거칠 때 권한 확인 (네트워크 ACL)

네트워크 ACL(액세스 제어 목록)

- 서브넷 수준에서 인바운드 / 아웃바운드 트래픽을 제어하는 `가상 방화벽`
- 트래픽 허용 여부를 결정할 때 `낮은 번호의 규칙부터 순서대로 처리` 함

상태 비저장 패킷 필터링

- 네트워크 ACL이 수행, 서브넷 경계를 거치는 패킷만 확인
- 이전 요청을 기억하지 않고 `규칙 목록에 따라서만` 패킷 응답 확인
- 인스턴스 권한 필요 (보안 그룹)

보안 그룹

- 기본적으로 모든 인바운드 트래픽 거부, 모든 아웃바운드 트래픽 허용

상태 저장 패킷 필터링

- 들어오는 패킷에 대한 이전 결정 기억
- 패킷 응답이 인스턴스로 반환될 때 보안 그룹의 기억

글로벌 네트워킹

- AWS 인프라와 고객 간의 상호작용

1. Route 53

- `DNS` 로서의 가용성, 확장성 뛰어남
- 지연 시간, 지리적 위치, 지역 근접성, 가중치 라운드 로빈 등 사용
- 외부 인프라로 전달 및 확장 가능

2. Amacon CloudFront

- 동일한 정적 자산을 복사 후 고객 중심의 리전에서 배포

DNS(Domain Name System)