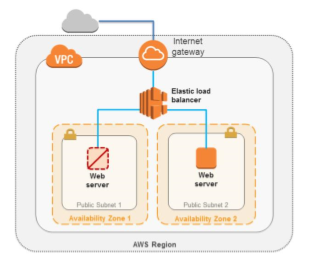
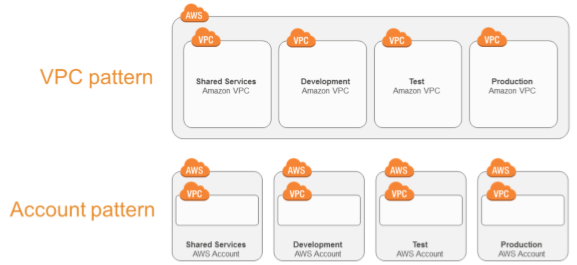
1. 파트1: 리전은 어떻게 선택합니까?
   1. 리전의 환경이 **데이터의 주권과 규정 준수** 요구 사항 충족?(**데이터 주권**)
   2. 리전이 사용자 또는 데이터 센터와 얼마나 가까운지?(**사용자와의 거리**)
   3. 고려 중인 리전이 환경에 필요한 **모든 서비스와 기능**을 제공하는지?(**서비스/기능**)
   4. 가장 **비용 효율적**인 리전을 선택하는지?(**비용 효율**)
2. 파트2: 가용 영역은 몇 개나 사용해야 합니까?
   1. 권장사항 및 모범 사례
      1. 권장 사항
         * 리전 당 **2개**의 가용 영역을 시작
      2. 모범 사례
         * 한 가용 영역 리소스에 접근할 수 없더라도 애플리케이션에 장애가 발생해서는 안됨
      3. 애플리케이션은 대부분 2개의 가용 영역 지원
      4. HA를 위해 3개 이상의 가용 영역 사용하면 비용 효율성이 떨어짐.
   2. 2개의 가용 영역 사용(사진 출처: 강의 자료)



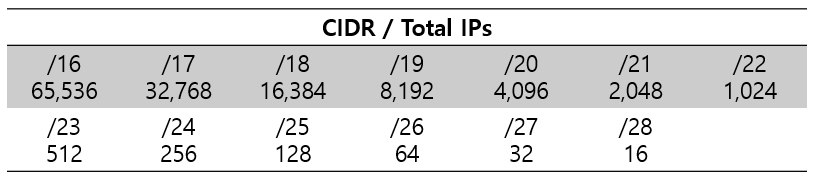
* 1. 2개의 가용 영역을 사용하는 다른 이유  
     시나리오별로 권장되는 가용 영역은 몇 개?
     1. Amazon EC2 스팟 인스턴스 사용률이 매우 높은 애플리케이션
        + 다양한 **요금 옵션**을 위해 **2개 이상**의 가용 영역
     2. MySQL, MS SQL Server 및 Oracle과 같은 데이터 소스를 사용하는 애플리케이션
        + **액티브 / 패시브 지원**을 위해 **2개**의 가용 영역
     3. Cassandra 또는 MongoDB와 같은 데이터 소스를 사용하는 애플리케이션
        + **매우 높은 가용성**을 위해 **2개 이상**의 가용 영역

1. 파트3: 모든 것을 하나의 VPC에 구성해야 합니까?
   1. 하나의 VPC 사용
      1. 하나의 VPC가 적절한 사용 사례는 **제한적**임.
      2. 사용 사례
         * 고성능 컴퓨팅
         * 자격증명관리
         * 한 명 또는 매우 작은 팀이 관리하는 소규모 단일 애플리케이션
         * 사용 사례 대부분 인프라를 조직하는데 2개의 기본 패턴 사용.  
           **다중 VPC** 및 **다중 계정**
   2. AWS 인프라 패턴(사진 출처: 강의 자료)



* 1. 패턴 선택
     1. 패턴을 결정하는 기본 요소: **조직의 복잡성**과 **워크로드 격리 요구사항**
     2. 단일 IT 팀? 🡪 **다중 VPC**
     3. IT 팀이 여러 개인 대규모 조직? 🡪 **다중 계정**
     4. 높은 수준의 워크로드 격리 요구됨? 🡪 **다중 계정**
  2. **다중 VPC** 패턴
     1. 기능
        + **하나의 AWS 계정** 사용
        + 애플리케이션 환경을 조직하는데 **2개 이상의 VPC** 사용
     2. 다음에 가장 적합
        + 관리형 서비스 공급자와 같은 **단일 팀 또는 단일 조직**
     3. 이유
        + 팀 수가 제한되면 **표준 유지 관리** 및 **액세스 관리**가 쉬움.
     4. 예외
        + **거버넌스** 및 **규정 준수 표준**은 조직의 복잡성과 관계없이 워크로드 격리를 요구할 수 있음.
  3. **다중 계정** 패턴
     1. 기능
        + 애플리케이션 환경을 조성하는데 **2개 이상의 AWS 계정** 사용
        + AWS 계정당 **하나의 VPC** 사용
     2. 다음에 가장 적합
        + **대규모 조직** 및 **IT 팀이 여러 개 있는 조직**
        + 빠른 성장이 예상되는 **중간 규모의 조직**
     3. 이유
        + **액세스** 및 **표준 관리**는 조직이 복잡할수록 더 어려울 수 있음.
  4. 그 외 중요한 고려 사항
     1. AWS 서비스 대부분이 **실제로 VPC 내에 위치하지는 않음**
     2. 이러한 서비스의 경우, 연결되지 않은 외부에서는 VPC가 **어떤 격리도 제공 X**
     3. AWS 리전간의 네트워크 트래픽은 기본적으로 AWS 글로벌 네트워크 백본 통과
     4. Amazon S3와 DynamoDB는 **VPC 엔드포인트가** 퍼블릭 인터넷을 통과하지 않고도 연결되도록 해 줌.

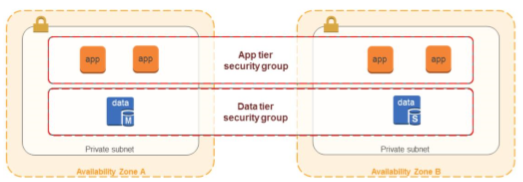
1. 파트4: VPC를 서브넷으로 어떻게 나눠야 합니까?
   1. VPC 및 IP 주소
      1. AWS VPC는 **/16** 과 **/28** 사이의 CIDR 범위를 사용할 수 있음.
      2. CIDR 범위의 숫자가 **하나씩 증가**할 때마다, 총 IP 수는 **절반으로 감소**



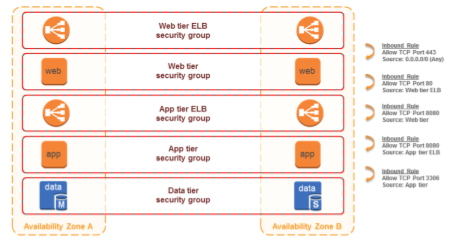
* 1. 서브넷이란 무엇입니까?
     1. 정의
        + CIDR 범위로 나누어진 네트워크의 세그먼트 또는 파티션
     2. 예
        + CIDR/22인 VPC는 총 1,024개의 IP를 포함
        + (유의)참고: 모든 서브넷에서 처음 4개와 마지막 1개의 IP주소는 AWS에서 사용하기 위해 예약되어 있음.
  2. 서브넷 사용 방법
  3. 서브넷의 권장 사항
     1. 가용 영역 당 **1개의 퍼블릭** 및 **1개의 프라이빗** 서브넷으로 시작
     2. 퍼블릭 서브넷보다 **프라이빗 서브넷에 더 많은 IP할당**  
        🡪 이유는 보안 때문임.
  4. 서브넷 크기
     1. 권장 사항
        + 작은 크기보다는 더 큰 크기의 서브넷 고려( /24)
     2. 워크로드 배치 간소화
        + 워크로드를 10개의 작은 서브넷 중 어디에 배치할지 선택하는 것이 1개의 큰 서브넷보다 더 복잡
     3. IP를 낭비하거나 IP가 부족할 확률이 낮음
        + 서브넷에서 사용 가능한 IP가 부족한 경우, 해당 서브넷에 IP를 추가할 수 없음
        + 예: 251개의 IP가 할당된 서브넷에서 IP를 25개만 사용하는 경우, IP가 부족한 다른 서브넷과 226개의 미사용 IP를 공유할 수 없음.
  5. 서브넷 유형(퍼블릭 / 프라이빗)  
     다음 리소스에 어떤 서브넷 유형을 사용해야 하는지?
     1. 데이터 스토어 인스턴스 🡪 프라이빗
     2. 배치 처리 인스턴스 🡪 프라이빗
     3. 백엔드 인스턴스 🡪 프라이빗
     4. 웹 애플리케이션 인스턴스 🡪 퍼블릭, 프라이빗

1. 파트5: VPC 트래픽은 어떻게 제어합니까?
   1. 보안 그룹  
      보안 그룹을 통해 VPC 트래픽 보안
      1. **하나 이상**의 인스턴스에 대한 인바운드 및 아웃바운드 트래픽을 제어하는 **가상 방화벽**
      2. **기본적으로 모든 수신 트래픽을 거부**하며, TCP, UDP 및 ICMP 프로토콜을 기반으로 필터링할 수 있는 허용 규칙 사용
      3. **상태 기반**이라 인바운드 요청이 허용되는 경우 아웃바운드 응답이 **자동으로 허용**됨.
      4. **소스/대상**을 **CIDR 블록** 또는 **다른 보안 그룹**으로 정의하여 보안 계층 생성 가능

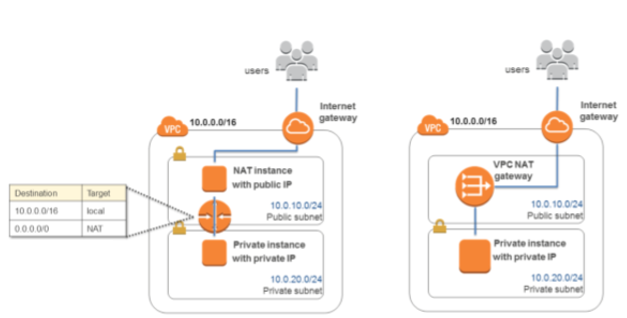
보안그룹을 사용하여 **리소스에서 송수신되는 트래픽과 리소스 사이의 트래픽 제어**(사진 출처: 강의 자료)



* 1. 보안그룹이 구성되는 방법
     1. 기본적으로 모든 새롭게 생성되는 보안 그룹은 모든 목적지에 대한 모든 아웃바운드 트래픽 허용
        + 보안 그룹의 기본 아웃바운드 규칙 수정 시 **복잡성이 증가**하므로 수정하지 않은 것이 좋음.
     2. 대부분 조직은 애플리케이션 내 각 기능 티어(웹/앱/데이터 등)에 대한 인바운드 규칙으로 보안 그룹 생성
  2. **보안 그룹 체인 다이어그램**(사진 출처: 강의 자료) 중요!!!!



* 1. 네트워크 ACL
     1. 서브넷에서 송수신 되는 트래픽을 제어하는 **선택적 가상 방화벽**
     2. 기본적으로 **모든** 송수신 트래픽 허용, **상태 비저장** 규칙 사용하여 트래픽의 허용 여부 결정
     3. 상태 비저장 규칙은 모든 인바운드와 아웃바운드 트래픽을 검사하여 연결은 추적하지 않음
     4. 규칙은 보안 그룹처럼 인스턴스 수준이 아니하 **서브넷 경계**에만 적용
  2. 인터넷 게이트웨이
     1. VPC의 인스턴스와 인터넷 간에 통신 허용
     2. 기본적으로 가용성이 뛰어나며, 중복적이고, 수평적으로 확장
     3. 인터넷으로 라우팅 가능한 트래픽을 위해 서브넷 라우팅 테이블의 대상 제공
  3. VPC로 트래픽 보내기  
     VPC 서브넷의 인스턴스에 대한 인터넷 액세스 활성화 시
     1. 인터넷 게이트웨이를 VPC에 연결
     2. 서브넷의 라우팅 테이블이 인터넷 게이트웨이를 가리키도록 함(PS)
     3. 서브넷의 인스턴스가 퍼블릭 IP 주소 또는 탄력적 IP 주소를 갖도록 함
     4. NACL 및 보안 그룹에 관련 트래픽이 인스턴스에서 송수신 되도록 허용해야 함.
  4. 프라이빗 인스턴스의 아웃바운드 트래픽은 어떻게 되나요?
     1. Network Address Translation 서비스
        + 프라이빗 서브넷의 인스턴스가 인터넷 또는 다른 AWS 서비스로의 아웃바운드 트래픽을 시작하도록 활성화
        + 프라이빗 인스턴스가 인터넷에서 들어오는 트래픽을 수신하지 못하도록 차단
        + 두 가지 옵션
          1. 퍼블릭 서브넷의 NAT로 설정된 Amazon EC2 인스턴스
          2. NAT 게이트웨이
  5. VPC NAT 게이트웨이와 Amazon EC2의 NAT 인스턴스 비교(사진 출처: 강의 자료)



왼쪽: 퍼블릭 서브넷의 NAT로 사용되는 Amazon EC2 인스턴스

오른쪽: NAT 게이트웨이

* 1. VPC 트래픽의 로깅(Amazon VPC 흐름 로그)
     1. VPC의 트래팩 흐름 세부정보 캡처
     2. VPC 서브넷 및 ENI에 대해 활성화될 수 있음
     3. 로그는 CloudWatch Logs로 게시됨.
     4. 사용 사례
        + 연결 문제 해결
        + 네트워크 액세스 규칙 테스트
        + 트래픽 모니터링
        + 보안 인스턴트 탐지 및 조사

1. 파트6: 여러 개의 VPC를 서로 연결할 수 있습니까?
   1. 고객 게이트웨이(CGW)
      1. VPN 터미널 당 1개
   2. 해결 방안
      1. VPC 피어링
      2. VPC 피어링의 동작 방식
      3. VPC 피어링 규칙
      4. VPC 피어링 보안
2. 파트7: 온프레미스 구성요소를 환경에 통합하려면 어떻게 합니까?
3. 파트8: 기본 VPC와 기본 서브넷이란 무엇이고, 왜 사용해야 합니까?