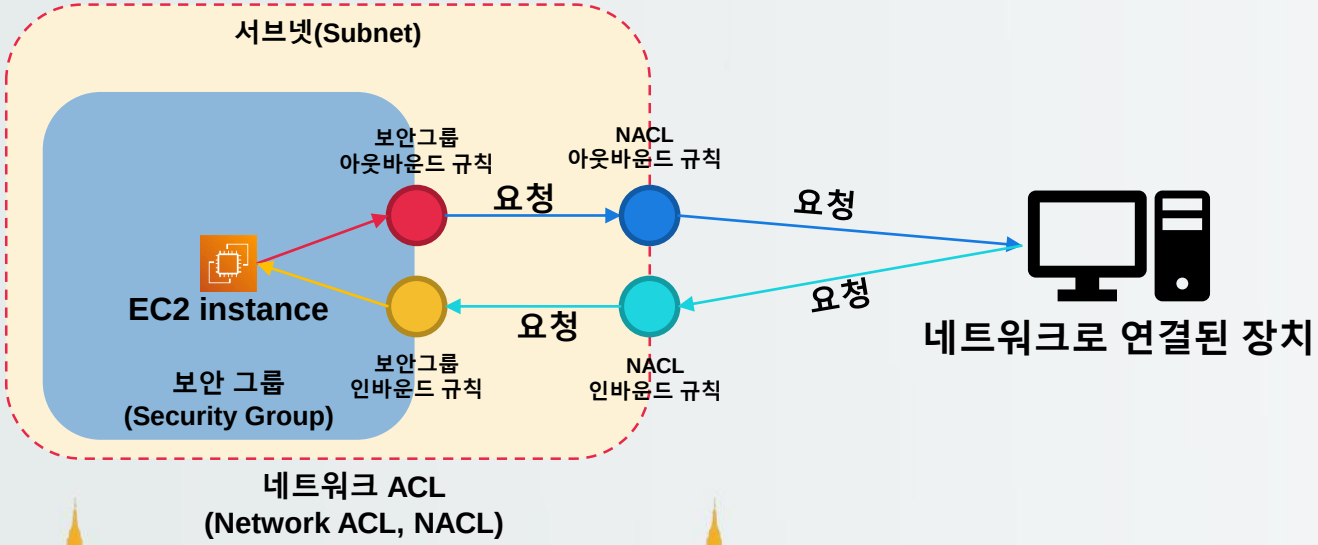
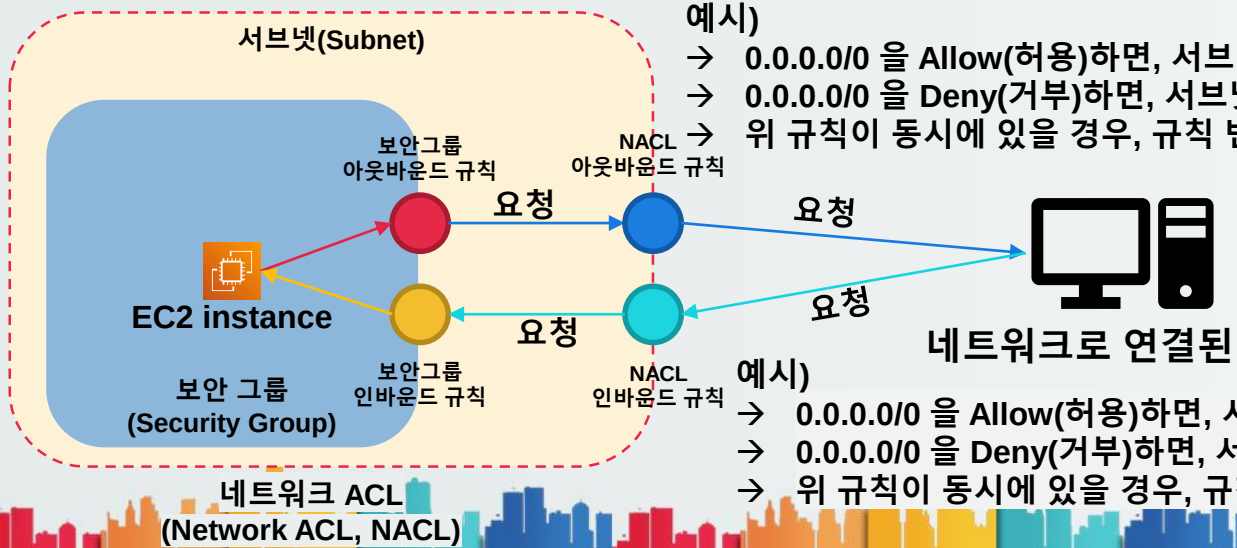
네트워크에 대한 접근 제어

- Network ACL(NACL)을 통해 특정 서브넷에 위치한 모든 EC2 인스턴스에 대해 접근 가능한 네트워크 영역을 제한
  - 아웃바운드/인바운드 규칙을 통해 서브넷 내부로 들어오고 내부에서 나가는 트래픽을 제어
  - VPC를 생성하면 기본 NACL이 생성되어 있으며, 모든 서브넷이 해당 NACL을 사용하도록 설정



네트워크에 대한 접근 제어

- **NACL 설정**
  - NACL 규칙은 대상으로 나가고 원천에서 들어오는 트래픽에 대한 Allow(허용)과 Deny(거부)로 구성됨
  - NACL 생성 시 기본적으로 인/아웃 모두 0.0.0.0/0 에 대한 거부가 설정되어 있으며 제거 불가
  - 허용과 거부가 동시에 있을 경우 낮은 규칙번호가 우선순위가 높음
  - 아웃바운드 규칙에서 서브넷 내부에서 접근할 수 있는 외부의 네트워크 대역을 설정
  - 인바운드 규칙에서 서브넷 내부로 접근할 수 있는 외부의 네트워크 대역을 설정
  - 외부의 네트워크 대역은 인터넷이나 혹은 또 다른 네트워크일 수 있음



예시)
→ 0.0.0.0/0 을 Allow(허용)하면, 서브넷 외부로 나가는 모든 트래픽 허용
→ 0.0.0.0/0 을 Deny(거부)하면, 서브넷 외부로 나가는 모든 트래픽을 거부
→ 위 규칙이 동시에 있을 경우, 규칙 번호에 따라 허용 여부가 결정됨

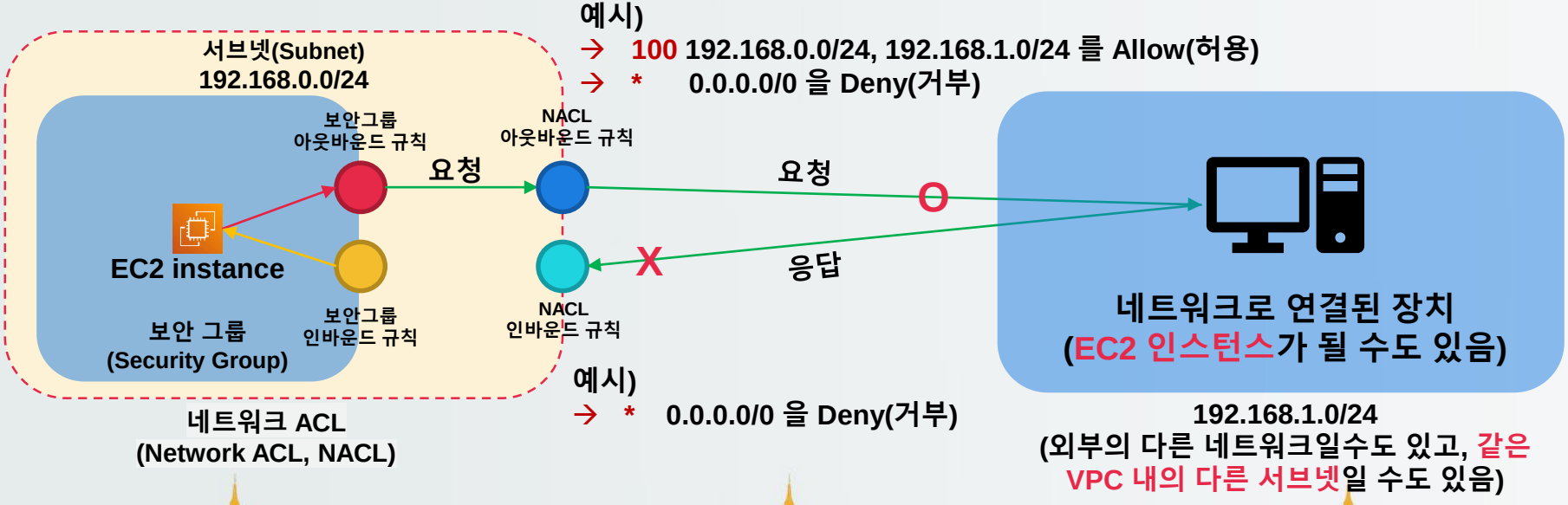
예시)
→ 0.0.0.0/0 을 Allow(허용)하면, 서브넷 외부에서 들어오는 모든 트래픽 허용
→ 0.0.0.0/0 을 Deny(거부)하면, 서브넷 외부에서 들어오는 모든 트래픽을 거부
→ 위 규칙이 동시에 있을 경우, 규칙 번호에 따라 허용 여부가 결정됨

네트워크에 대한 접근 제어

- **NACL 설정**
  - AWS 관리 콘솔에서 NACL 설정 화면

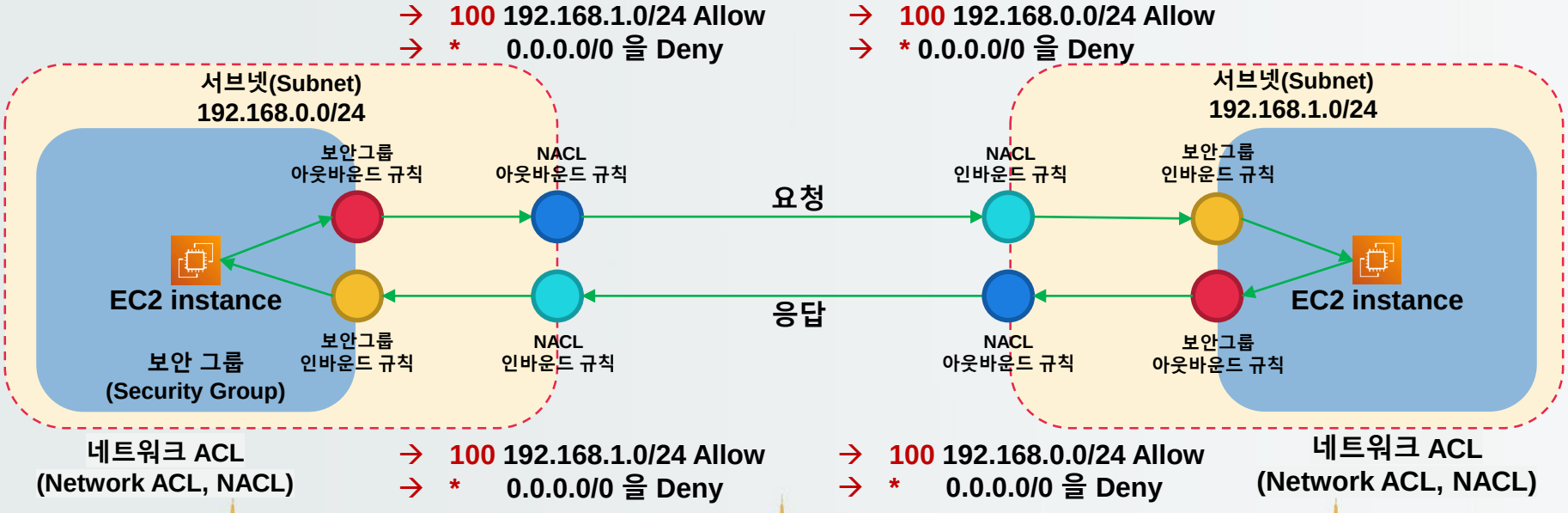
네트워크에 대한 접근 제어

- **NACL 설정**
  - 보안그룹과 달리 서브넷 내부에서 시작된 요청에 대한 응답도 명시적으로 인바운드에서 허용해야 함
  - 외부에서 시작된 요청과 내부에서 시작된 요청에 대한 응답 두 가지 모두 NACL 인바운드 허용 규칙에 있어야 함
  - 서브넷 내부에서의 통신은 NACL에 영향을 받지 않음



네트워크에 대한 접근 제어

- 두 Subnet 간의 NACL 설정
  - 각 서브넷에 서로 다른 NACL이 설정되어 있을 경우, 아래와 같이 각각 인바운드/아웃바운드 설정이 되어야 함
  - 보안그룹 규칙은 서로 간에 통신을 허용하는 상태임을 가정함



서브넷 내부에서의 통신과 NACL

유형	프로토콜	포트 범위	대상
All traffic	ALL	ALL	0.0.0.0/0

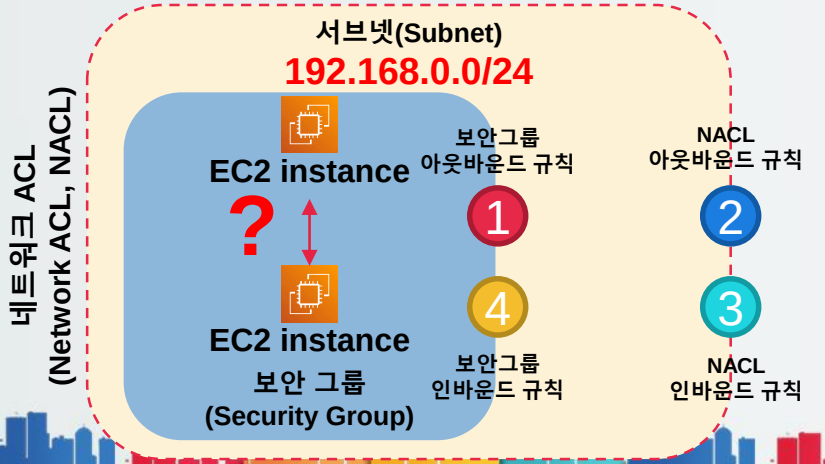
유형	프로토콜	포트 범위	대상
All traffic	ALL	ALL	0.0.0.0/0

규칙번호	유형	프로토콜	포트 범위	대상	허용/거부
*	All traffic	ALL	ALL	0.0.0.0/0	거부
100	All traffic	ALL	ALL	0.0.0.0/0	허용

규칙번호	유형	프로토콜	포트 범위	대상	허용/거부
*	All traffic	ALL	ALL	0.0.0.0/0	거부
100	All traffic	ALL	ALL	0.0.0.0/0	허용

두 EC2 인스턴스는 동일한 보안그룹을 사용할 때,

두 EC2 인스턴스 간 접속이 가능한가?



NACL 동작 방식 퀴즈

유형	프로토콜	포트 범위	대상

유형	프로토콜	포트 범위	소스

규칙번호	유형	프로토콜	포트 범위	대상	허용/거부
*	All traffic	ALL	ALL	0.0.0.0/0	거부

규칙번호	유형	프로토콜	포트 범위	대상	허용/거부
*	All traffic	ALL	ALL	0.0.0.0/0	거부