Lab5. Create an Additional Security Group and NACL

목적

이번 실습에서는 기본 보안 그룹과 NACL외에 추가적으로 사용자 정의형 보안 그룹과 NACL을 생성한다. 또한 추가적으로 생성한 보안 그룹을 Lab3에서 생성한 lab-eni에 연결한다. 새로 생성한 NACL의 인바운드 규칙과 아웃바운드 규칙을 편집하고 그리고 마지막으로 Lab2에서 생성한 lab-subnet과 연결한다.

사전 준비물

AWS Free-Tier 계정

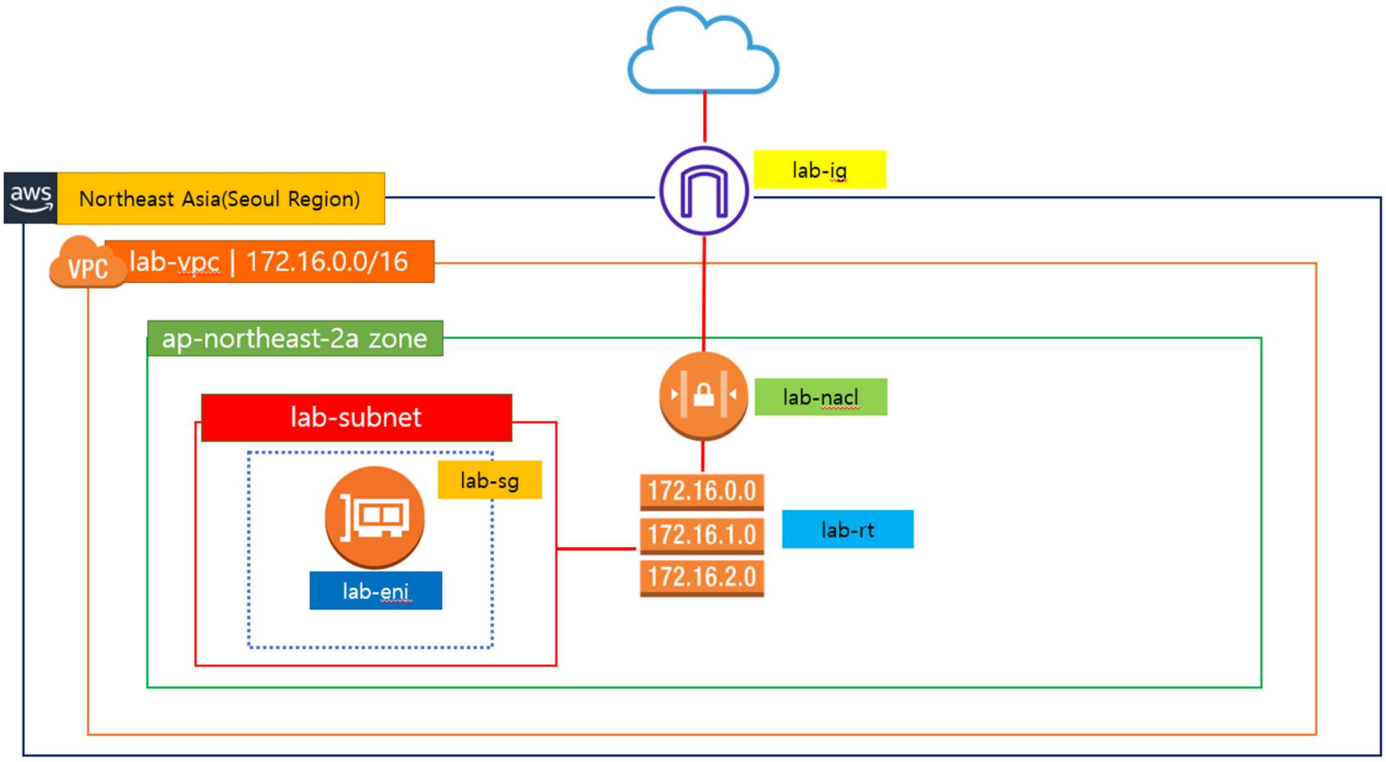
lab-vpc

lab-subnet

lab-eni

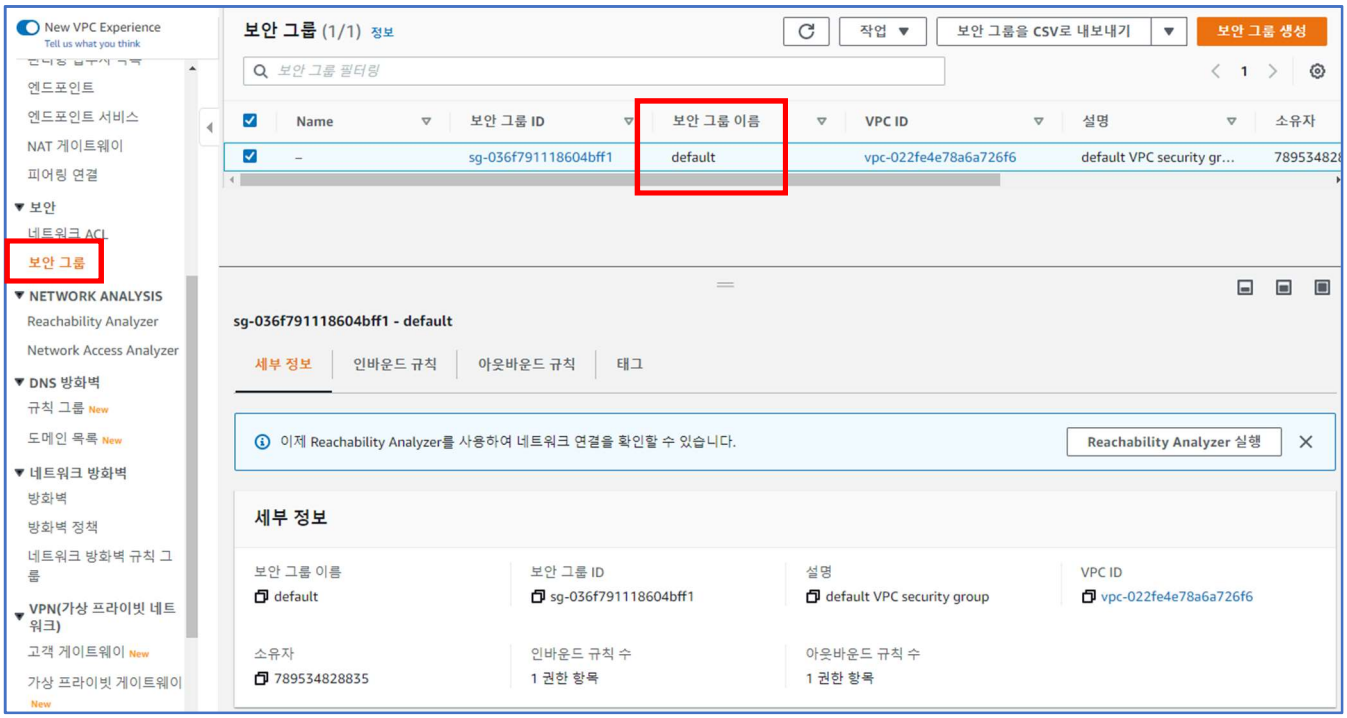
lab-ig

lab-rt

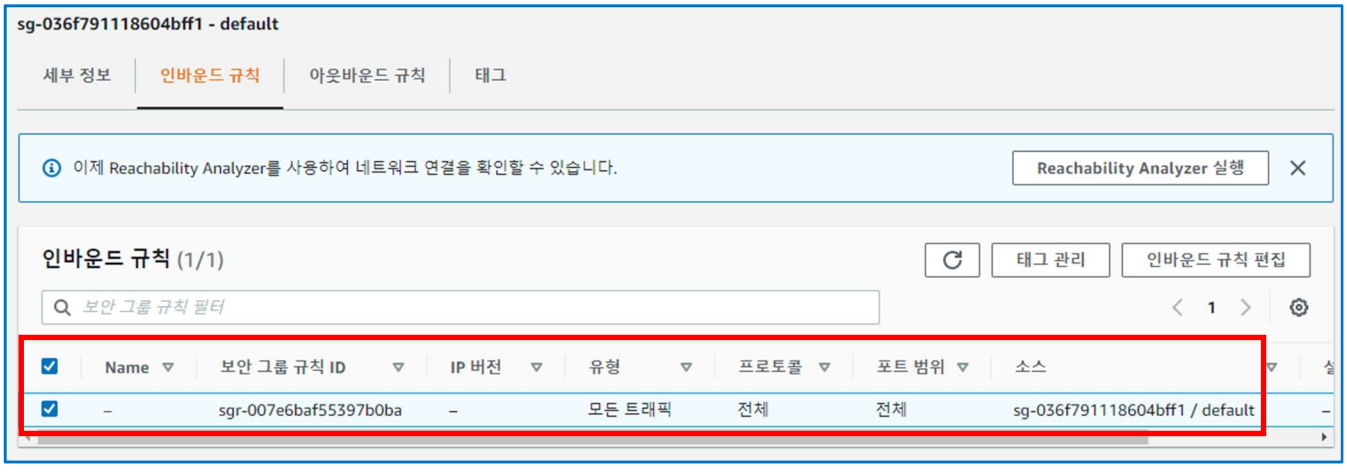


사용자 정의형 보안 그룹 생성하기

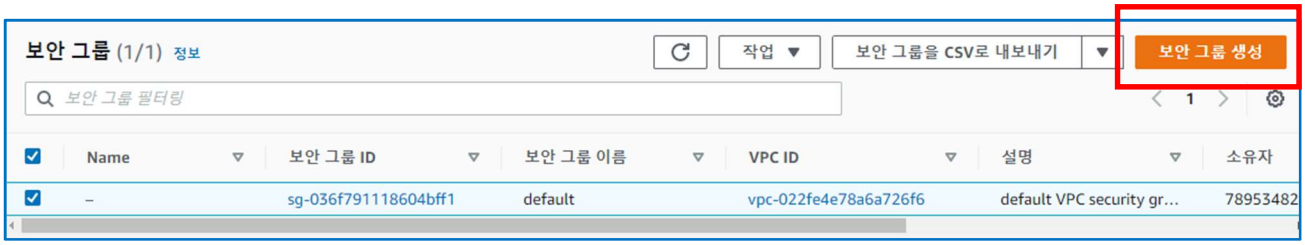
1. **[서비스]** > **[VPC]**의 좌측 메뉴 중 **[보안]** > **[보안그룹]**을 클릭하여 **[보안 그룹]** 페이지로 이동한다. 현재 기본 보안 그룹만 생성되어 있음을 확인할 수 있다.



2. **[인바운드 규칙]** 탭을 클릭하여 **기본 보안 그룹**의 **인바운드 규칙**을 확인해 보면 모든 유형의 포트와 트래픽이 허용되어 있음을 확인할 수 있다.



3. 새 **보안 그룹** 생성을 위해 페이지 우측 상단의 **[보안 그룹 생성]**을 클릭한다.

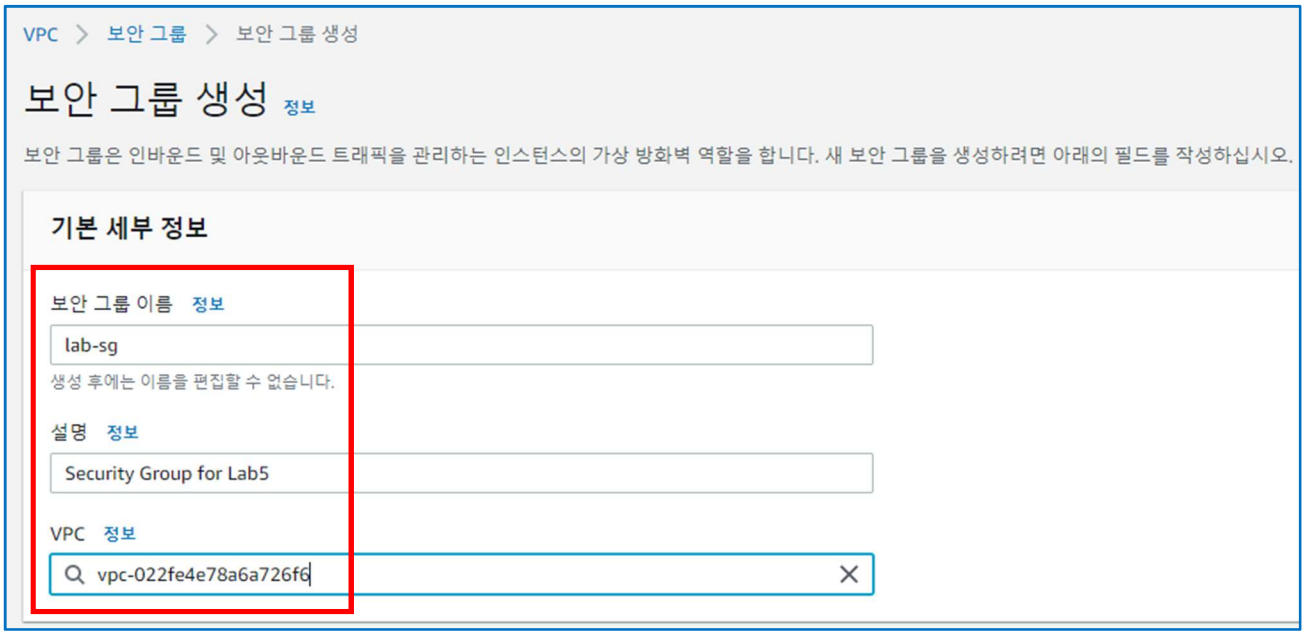


4. **[보안 그룹 생성]** 페이지에서 다음의 각 값을 설정한다.

   A. **[보안 그룹 이름]** : **lab-sg**

   B. **[설명]** : **Security Group for Lab5**

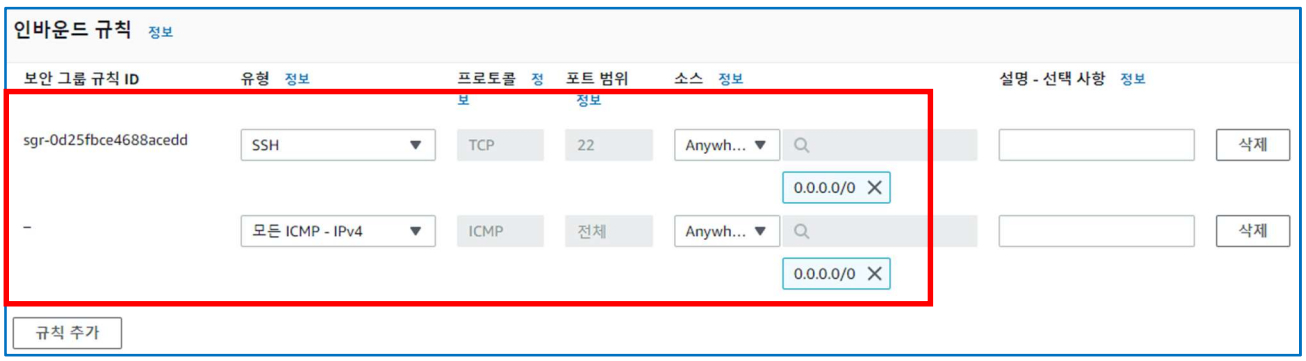
   C. **[VPC]** : **lab-vpc**



5. 페이지를 스크롤다운하여 **[인바운드 규칙]** 섹션으로 이동한다. **[규칙 추가]**를 클릭하여 다음과 같이 설정한다.

   A. **[유형]** : **모든 ICMP-IPv4**, **[소스] : Anywhere-IPv4**

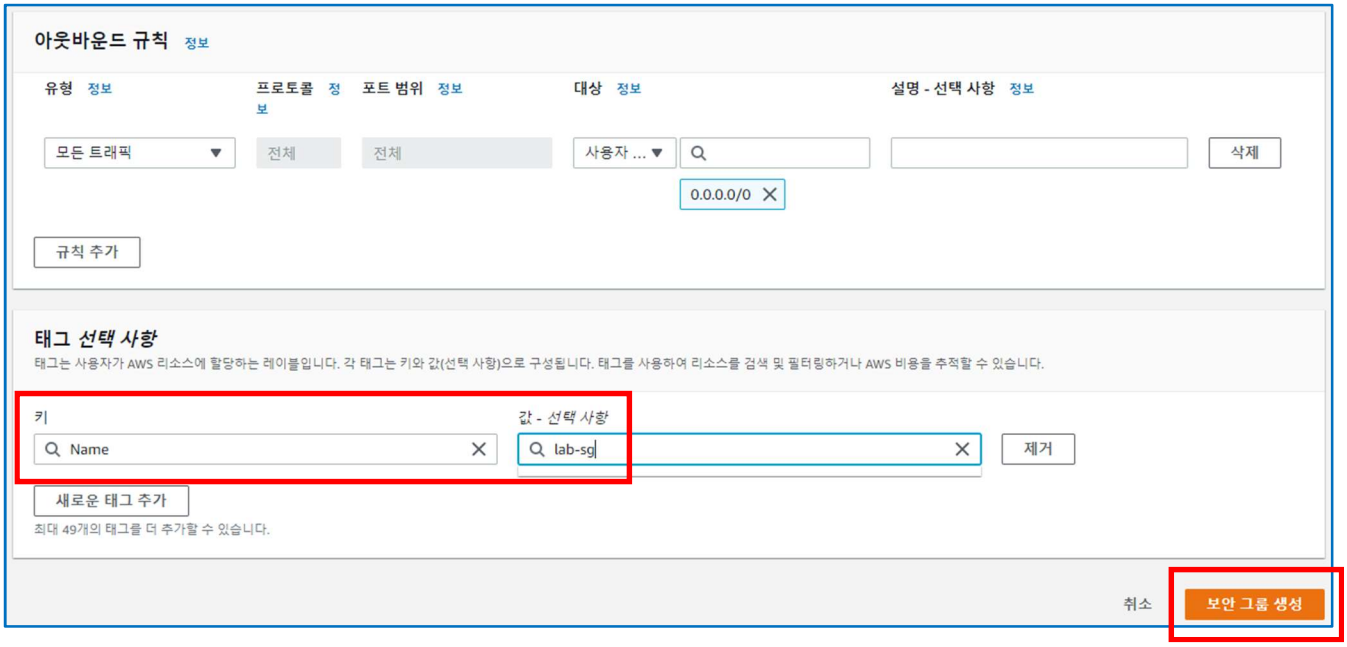
   B. **[유형]** : **SSH**, **[소스]** : **Anywhere-IPv4**



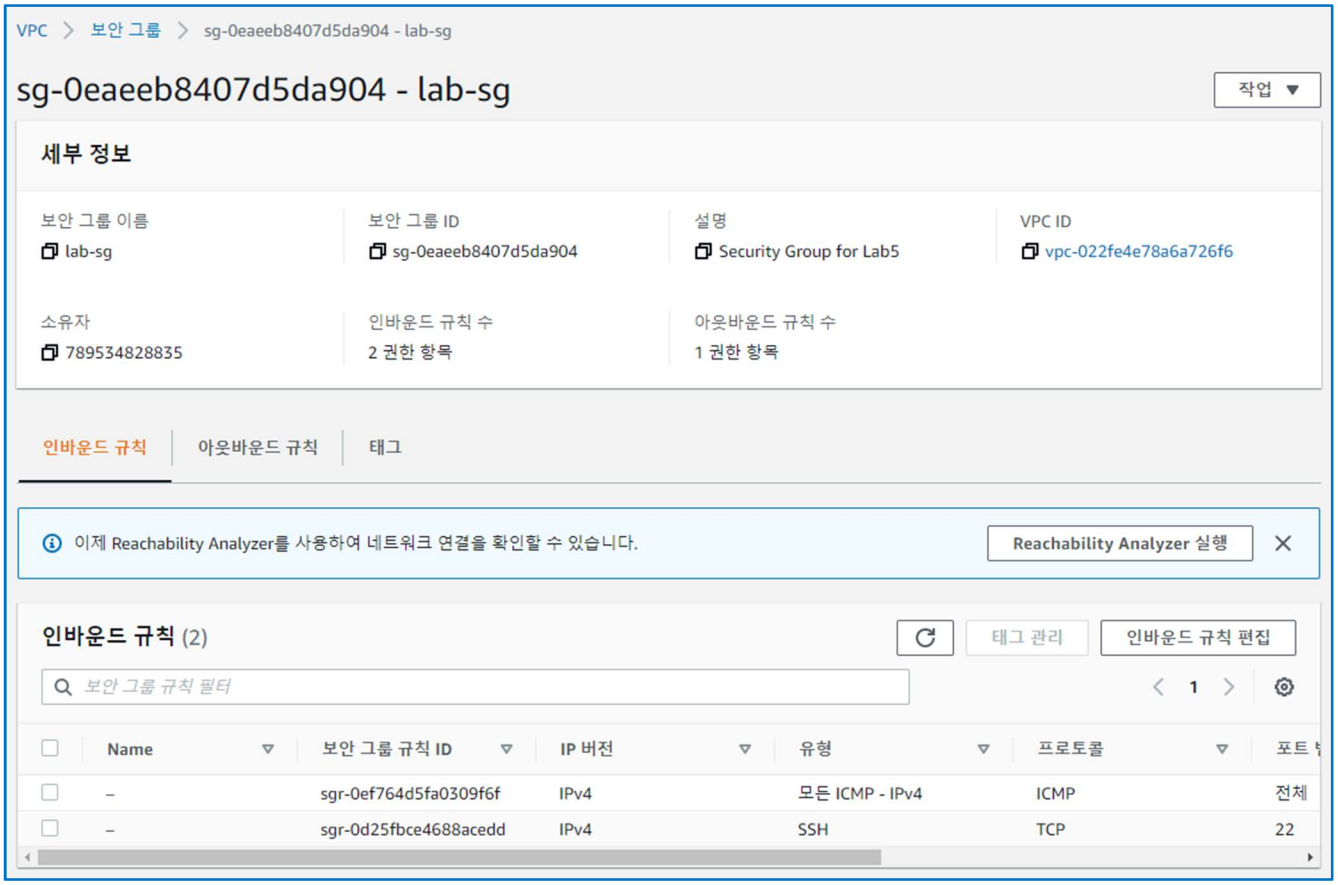
6. **[아웃바운드 규칙]**은 기본값 그대로 사용하기로 한다. **[태그]** 섹션에서 **키**와 **값**을 설정한 후 **[보안 그룹 생성]** 버튼을 클릭한다.

   A. **[키]** : **Name**

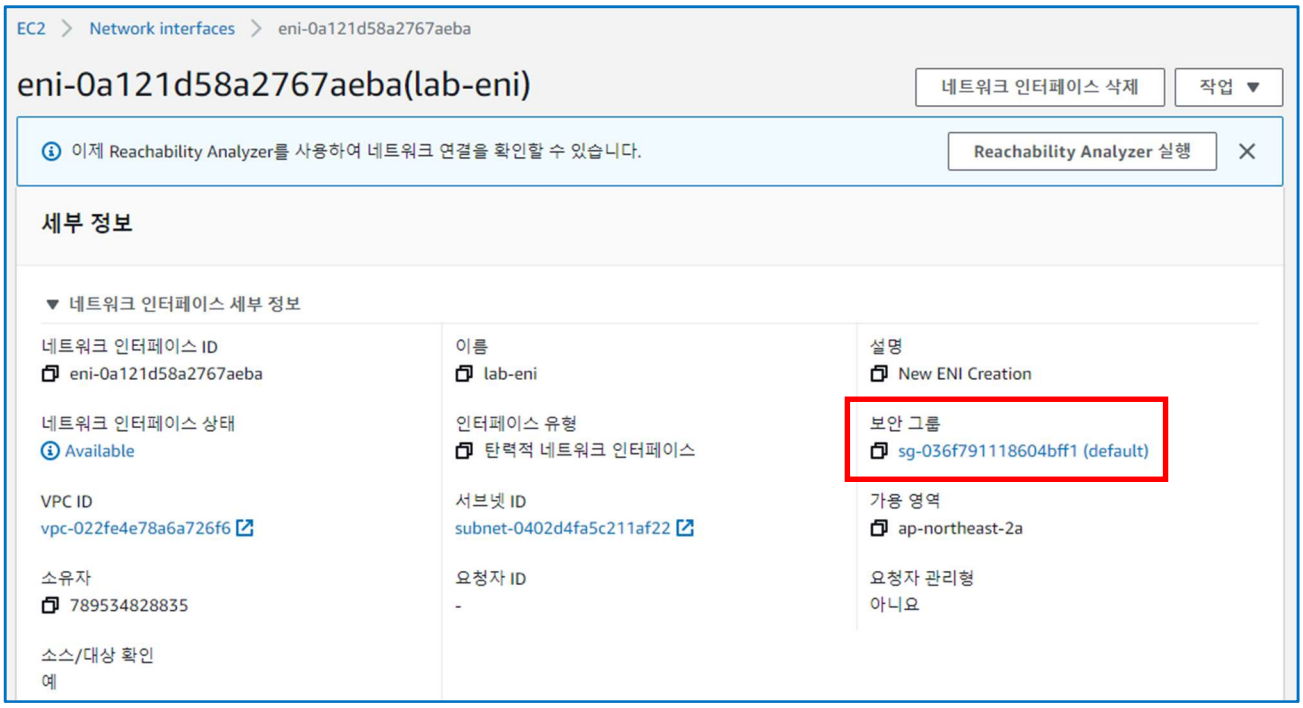
   B. **[값]** : **lab-sg**



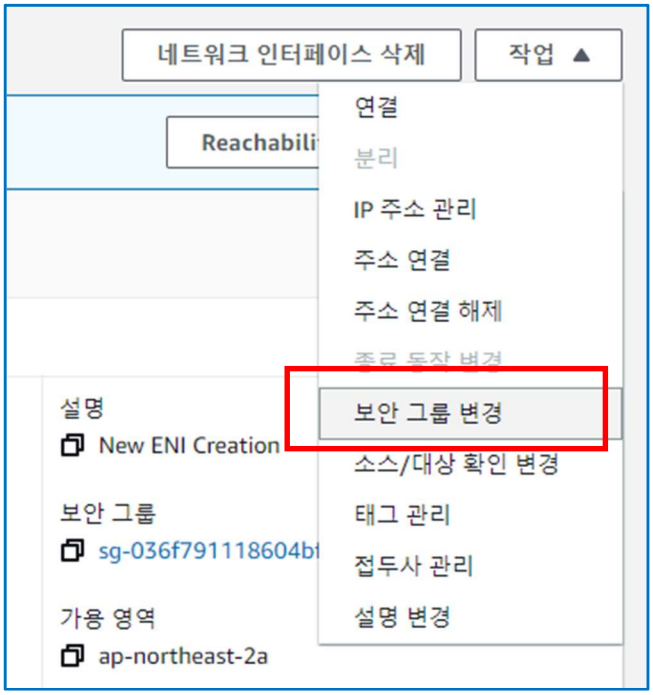
7. 보안 그룹이 잘 생성되었다.



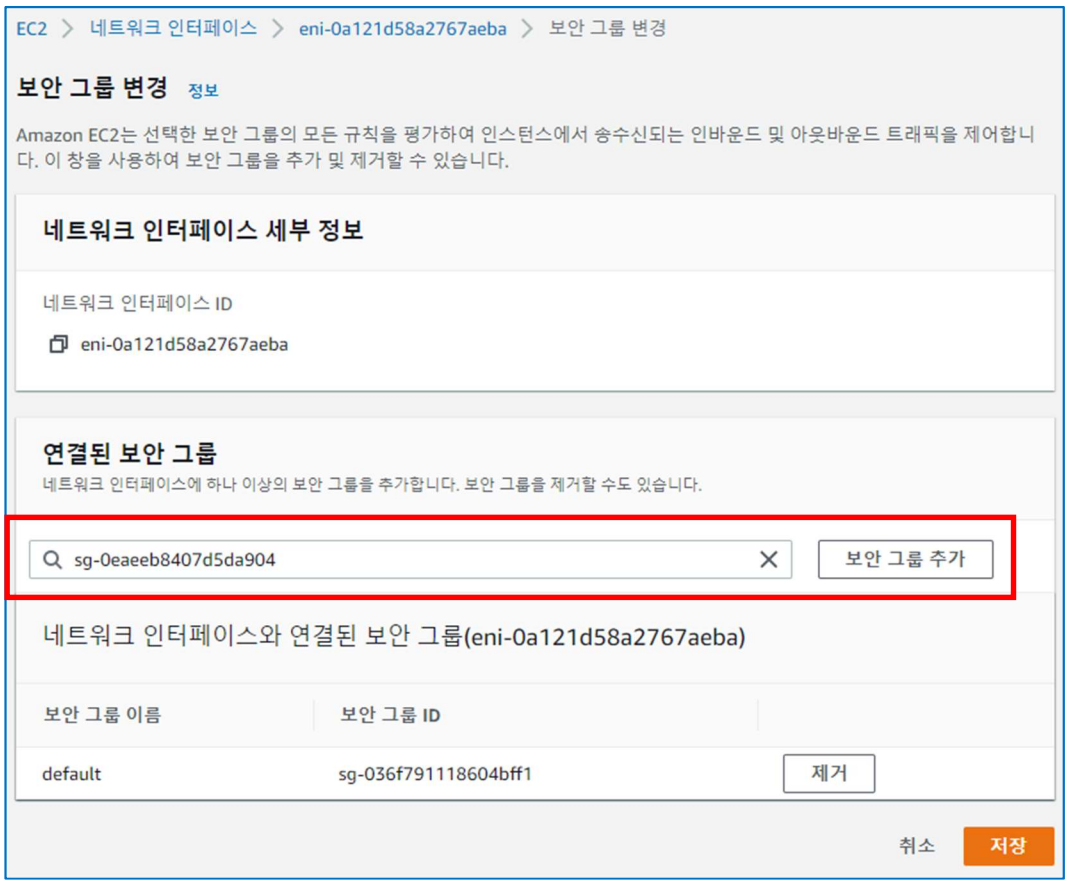
8. **[서비스]** > **[EC2]** > **[네트워크 및 보안]** > **[네트워크 인터페이스]**를 클릭하여 **Lab3**에서 생성한 **lab-eni** 상세 페이지로 이동한다. 현재 **[보안 그룹]**은 **기본 보안 그룹**으로 설정되어 있음을 확인할 수 있다.



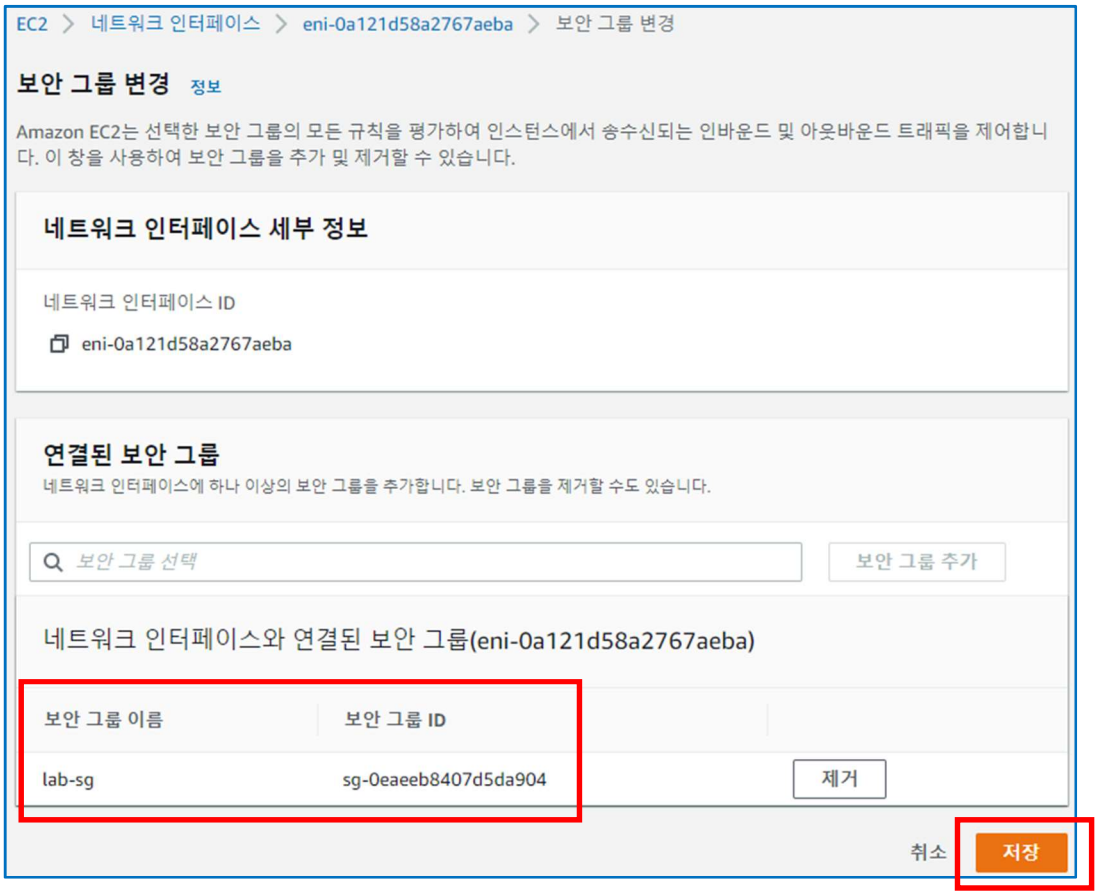
9. 방금 생성한 **lab-sg 보안 그룹**과 연결하기 위해 **[작업]** > **[보안 그룹 변경]**을 클릭한다.



10. **[보안 그룹 변경]** 페이지에서 **[연결된 보안 그룹]**의 값을 **lab-sg**로 선택한다. 그리고 **[보안 그룹 추가]** 버튼을 클릭한다.



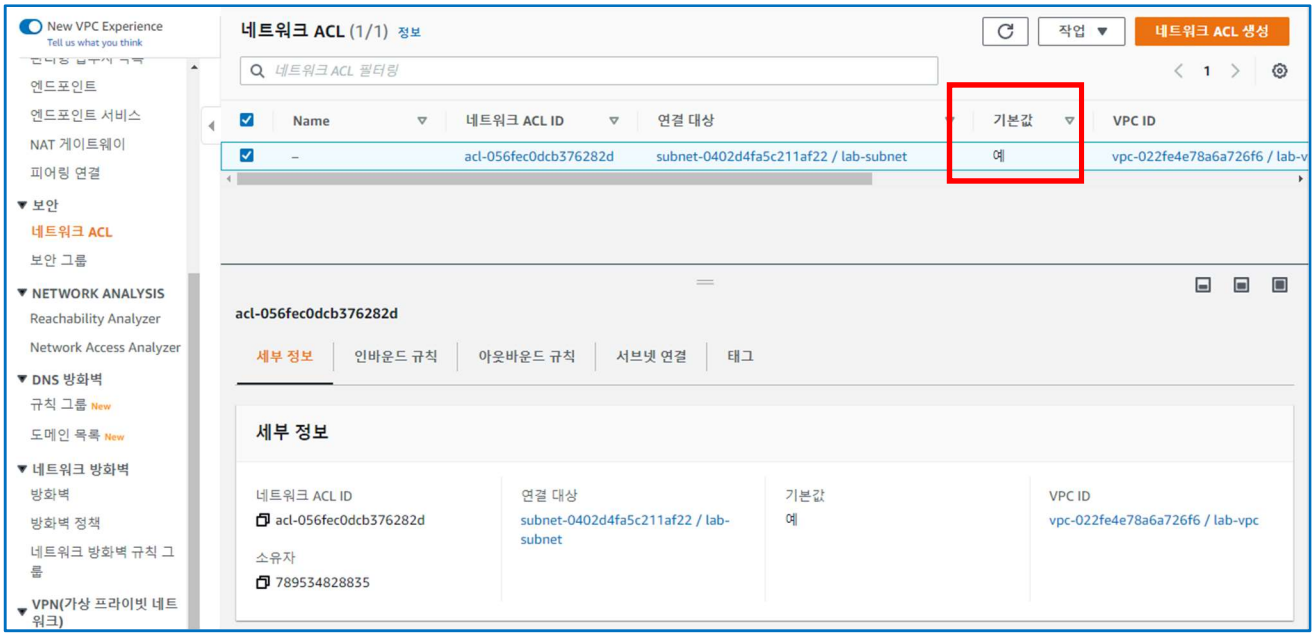
11. 그리고 **default 보안 그룹**은 **[제거]** 버튼을 클릭하여 제거한다. 그리고 **[저장]**을 클릭한다.



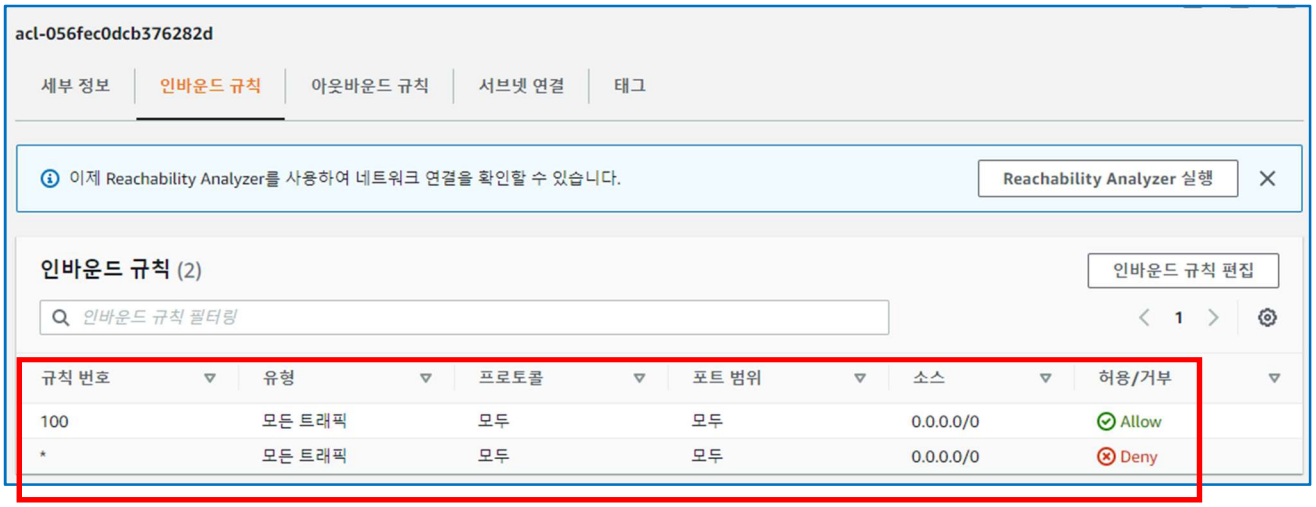
12. **lab-eni**의 **보안 그룹**이 변경됐음을 확인한다.

사용자 정의형 NACL 생성하기

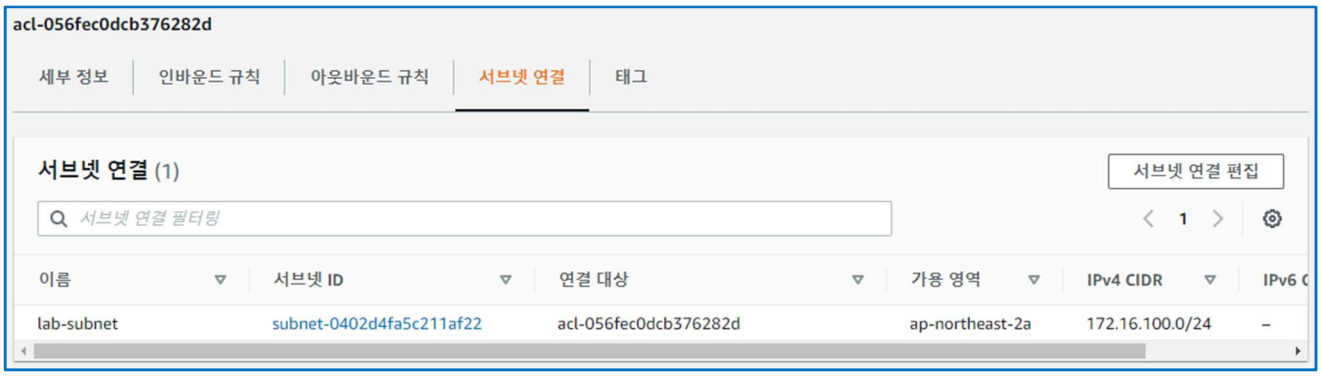
1. **[보안]** > **[네트워크 ACL]**을 클릭하여 **네트워크 ACL** 페이지로 이동한다. 현재 **기본 NACL**만 있다.



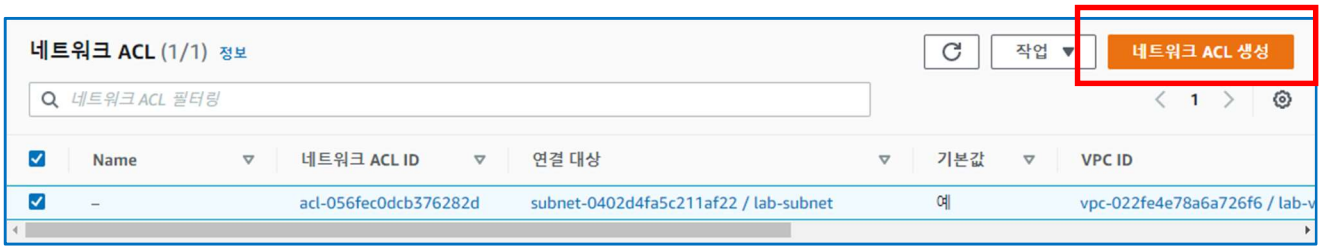
2. **[인바운드 규칙]** 탭을 클릭한다. 모두 허용 규칙이 저장돼 있으므로 블랙 기반 경합 방식임을 알 수 있다. **아웃바운드 규칙**도 이와 같다.



3. **[서브넷]** 탭을 클릭해보면, **기본 NACL**은 **lab-subnet**과 연결되어 있음을 확인할 수 있다.



4. 새 네트워크 ACL을 생성하기 위해 페이지 우측 상단의 **[네트워크 ACL 생성]**을 클릭한다.



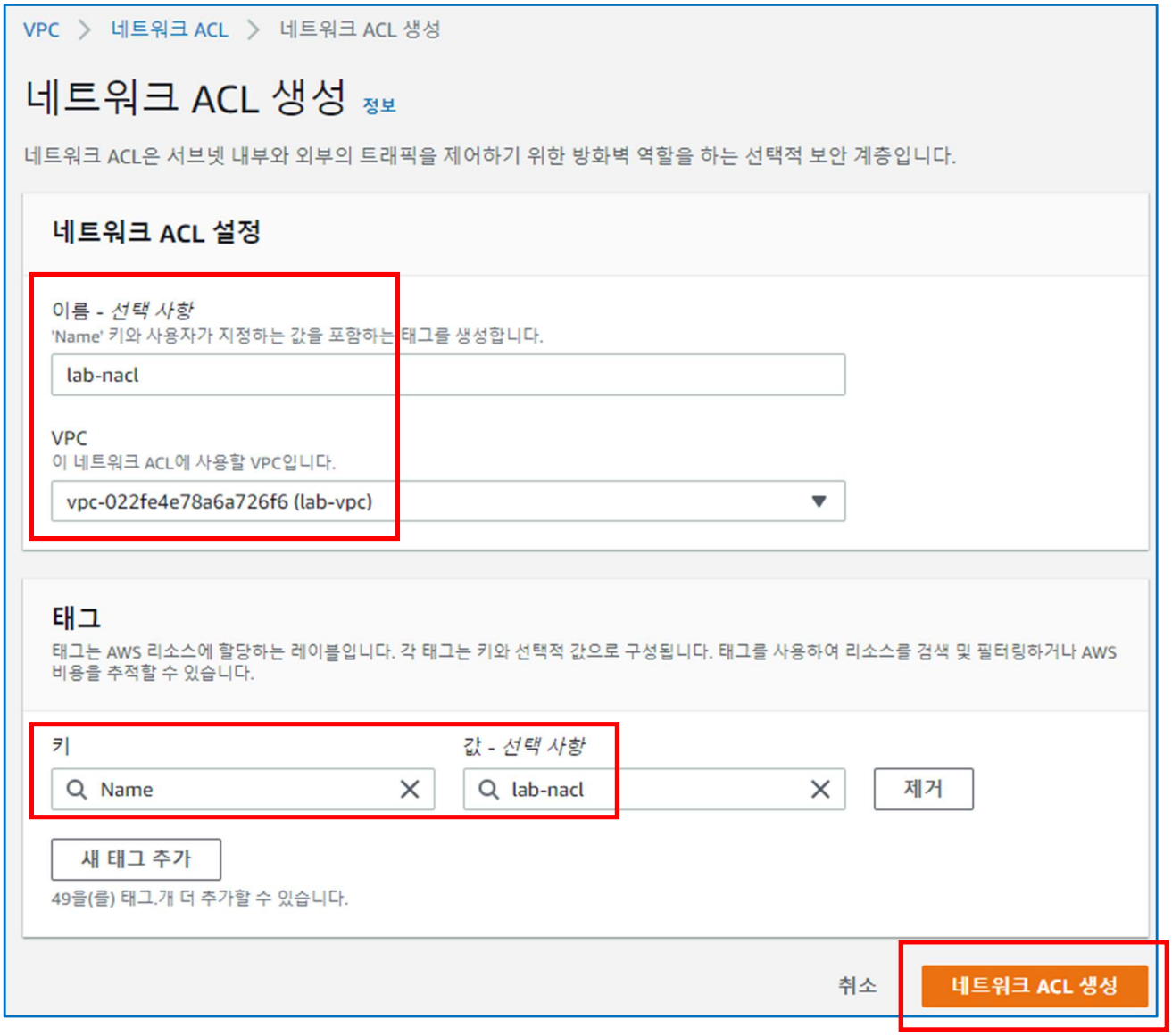
5. **[네트워크 ACL 생성]** 페이지에서 다음의 값을 설정한 후, **[네트워크 ACL 생성]** 버튼을 클릭한다.

   A. **[이름]** : **lab-nacl**

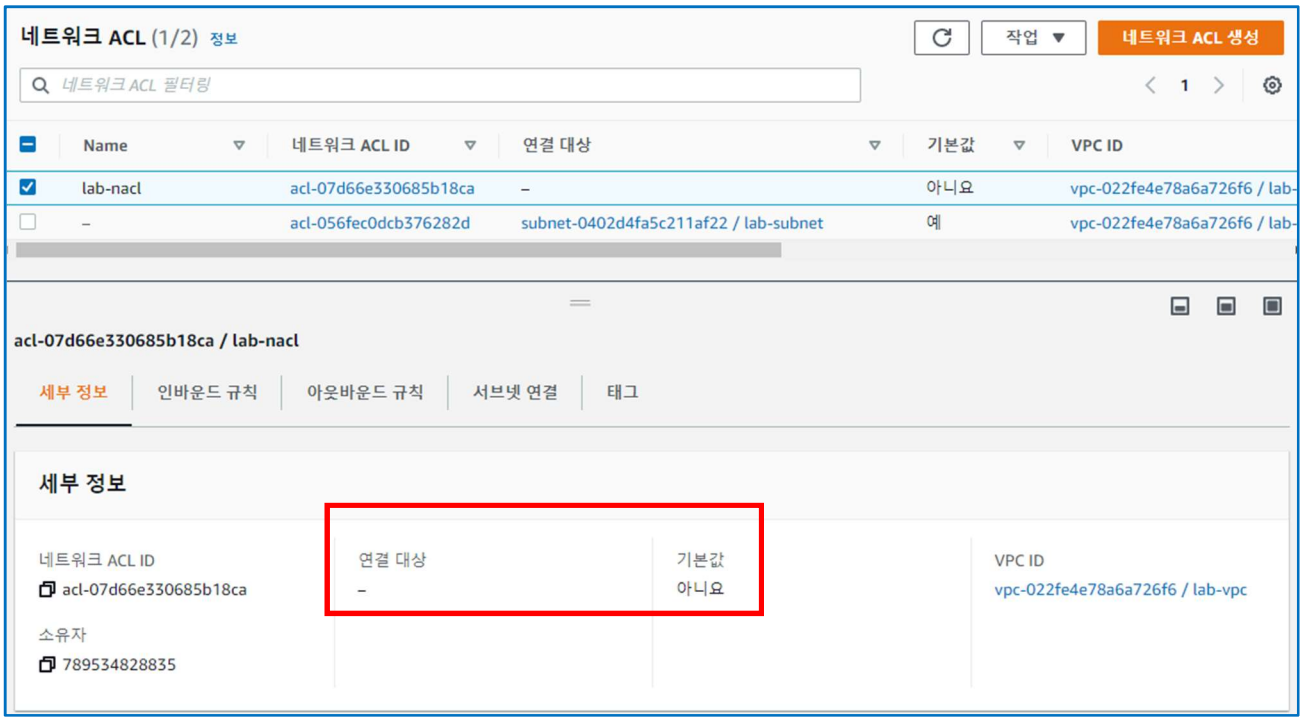
   B. **[VPC]** : **lab-vpc**

   C. **[키] : Name**

   D. **[값]** : **lab-nacl**



6. **네트워크 ACL**이 잘 생성되었다. 방금 생성한 **lab-nacl**은 연결된 **서브넷**이 없고 **기본 NACL**이 아님을 알 수 있다.



7. 먼저 **[인바운드 규칙]** 탭과 **[아웃바운드 규칙]** 탭을 클릭하면 **모두 거부** 규칙만 저장돼 있어 화이트기반 결합 방식임을 알 수 있다.

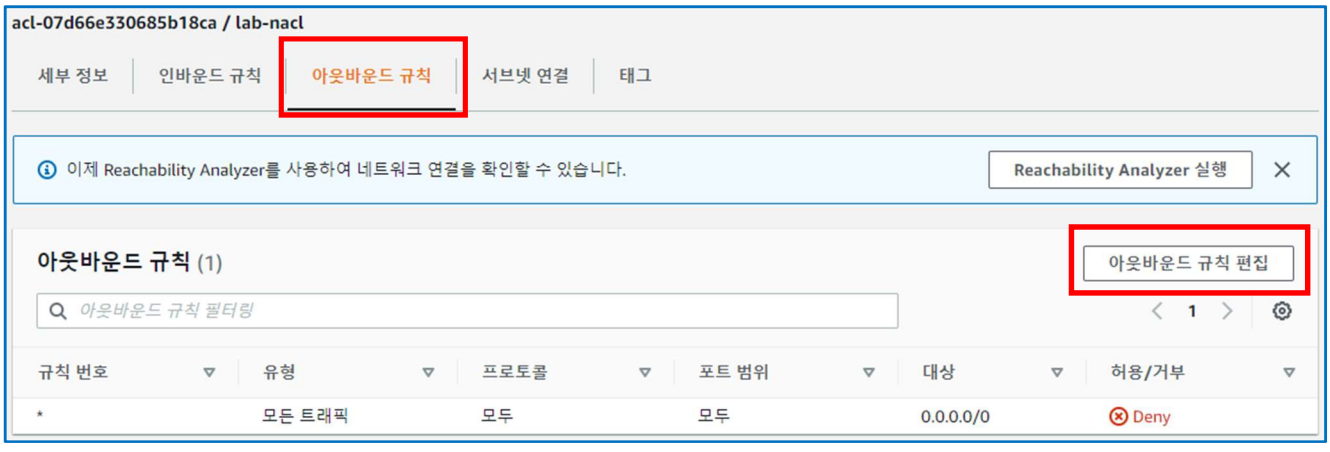
8. **인바운드 규칙**과 **아웃바운드 규칙**을 편집해서 클라이언트 접속을 허용하기로 한다. **[인바운드 규칙]** 탭에서 **[인바운드 규칙 편집]**을 클릭한다.

9. **[인바운드 규칙 편집]** 페이지에서 **[새 규칙 추가]** 버튼을 클릭하여 다음과 같이 설정하고 **[변경 사항 저장]** 버튼을 클릭한다.

   A. [규칙 번호] : 100, [유형] : 모든 ICMP – IPv4, [소스] : 0.0.0.0/0, [허용/거부] : 허용

   B. [규칙 번호] : 200, [유형] : SSH(22), [소스] : 0.0.0.0/0, [허용/거부] : 허용

10. **[아웃바운드 규칙]** 탭의 **[아웃바운드 규칙 편집]**을 클릭한다.

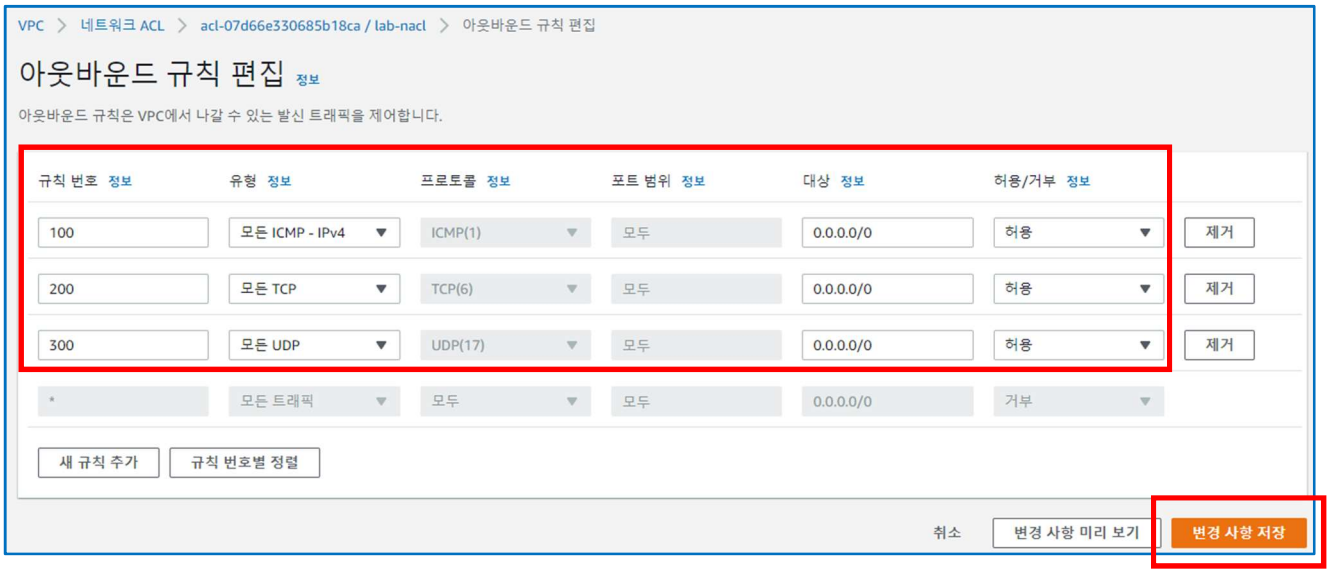


11. **[아웃바운드 규칙 편집]** 페이지에서 다음과 같이 각각의 값을 설정한 후, **[변경 사항 저장]**을 클릭한다.

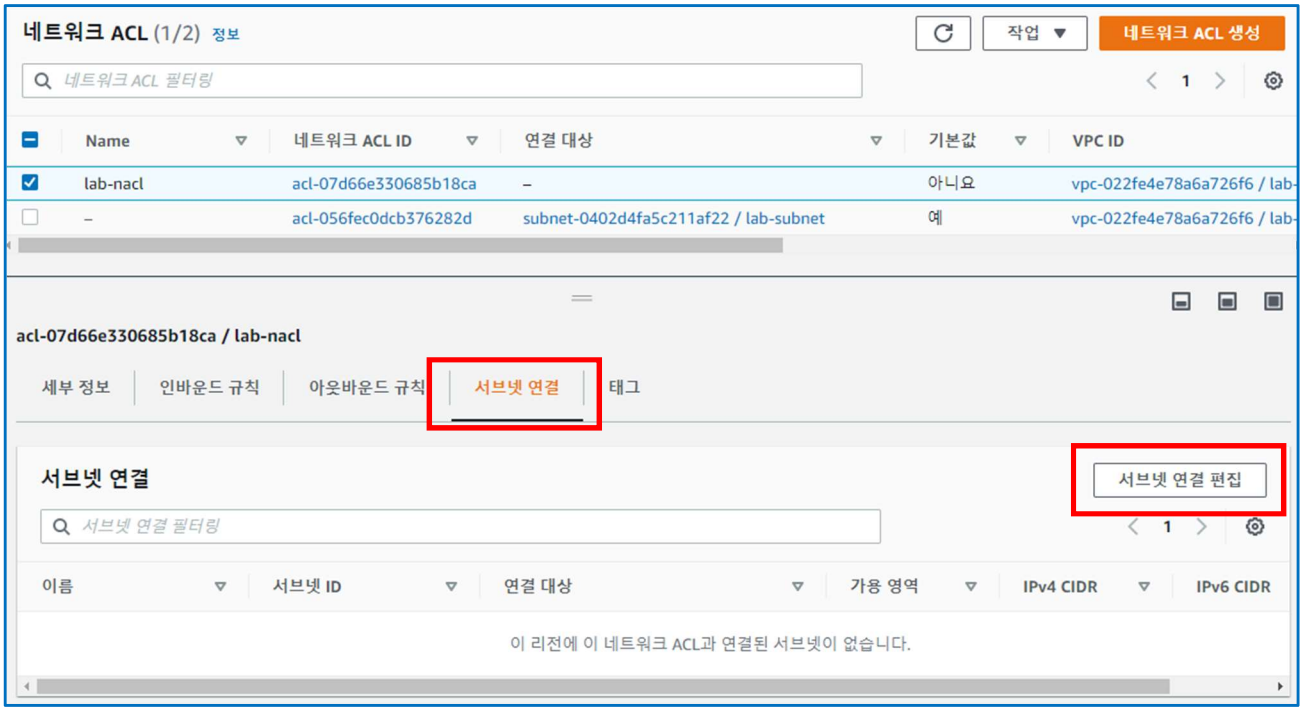
   A. [규칙 번호] : 100, [유형] : 모든 ICMP – IPv4, [대상] : 0.0.0.0/0, [허용/거부] : 허용

   B. [규칙 번호] : 200, [유형] : 모든 TCP, [대상] : 0.0.0.0/0, [허용/거부] : 허용

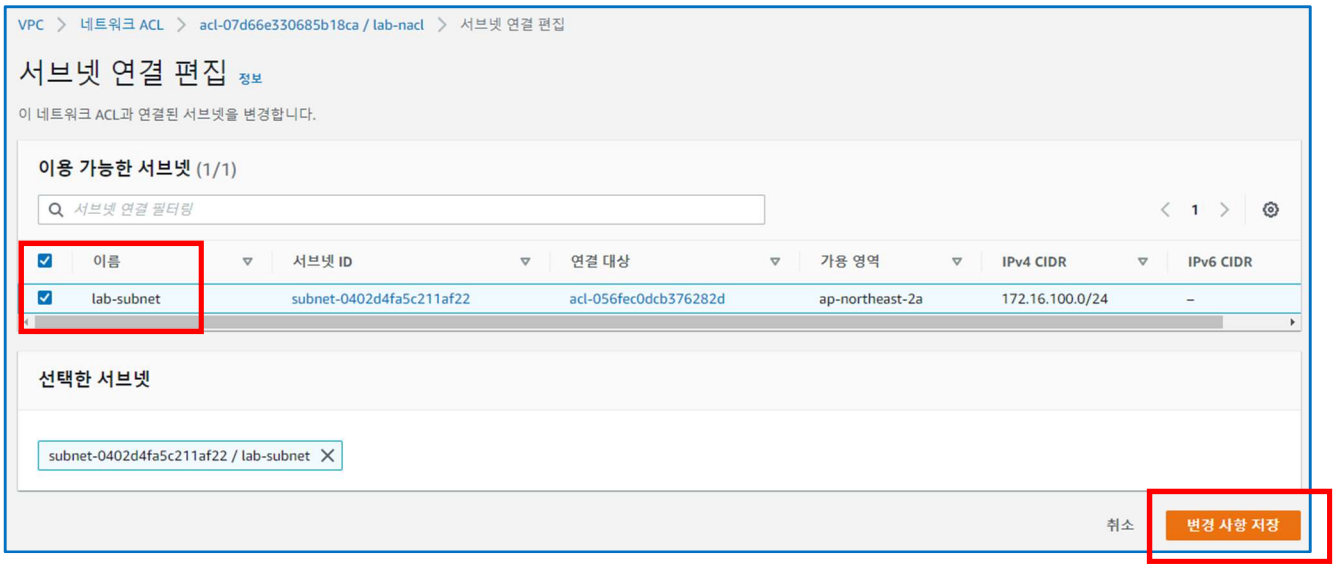
   C. [규칙 번호] : 300, [유형] : 모든 UDP, [대상] : 0.0.0.0/0, [허용/거부] : 허용



12. 방금 생성한 **lab-nacl**은 아직 **서브넷**에 연결되어 있지 않다. **서브넷**에 연결하기 위해 **[서브넷 연결 편집]**을 클릭한다.



13. **[서브넷 연결 편집]** 페이지에서 **[이용 가능한 서브넷]** 목록에서 **Lab2**에서 생성한 **lab-subnet**을 체크하고, **[변경 사항 저장]**을 클릭한다.



14. 이번 실습에서 생성한 **lab-nacl**의 **인바운드 규칙**과 **아웃바운드 규칙** 그리고 **서브넷 연결**까지 모두 마쳤다.