Chapter 05

컴퓨팅 서비스의 네트워킹 요건

1. 트래픽의 시작 : IP 주소

- 트래픽을 전달하려면 통신 경로상의 모든 네트워크 디바이스가 목적지 IP를 명확히 인식할 수 있어야 한다.
- 이 디바이스들이 IP 주소만으로 트래픽을 전달할 수 있는 이유는 무엇일까?

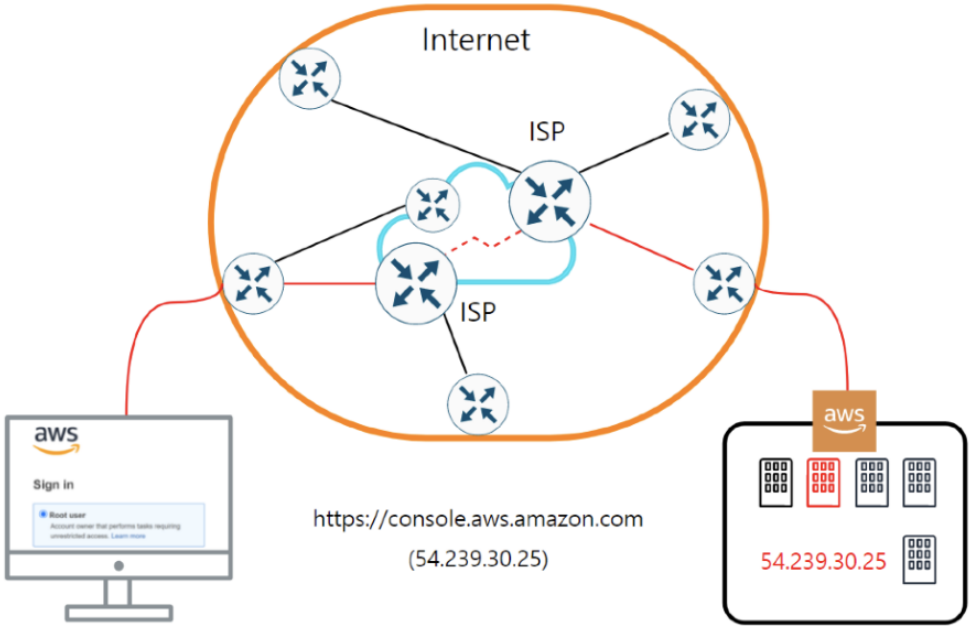
- IP 유형 = [정적/동적] + [퍼블릭/프라이빗]
  - IPv4는 물리적 32비트 숫자와 유형으로 구성된다.
  - IP는 반드시 이 2가지 성질이 있으므로 다음과 같이 4개 형태로 정리할 수 있다.
    - 동적 + 퍼블릭
    - 동적 + 프라이빗
    - 정적 + 퍼블릭
    - 정적 + 프라이빗

  - 정적 IP는 고정돼 바뀌지 않는 IP다.
  - 이와 달리 어느 시점부터 IP가 변경되면 동적 IP라고 한다.
  - IP가 주기적으로 변경되면 서비스를 제공할 도메인과 IP 매핑을 위한 DNS 설정이 어렵다.
  - 따라서 서비스용 IP는 정적 IP를 주로 사용한다.

1. 트래픽의 시작 : IP 주소

퍼블릭 IP와 인터넷 라우팅

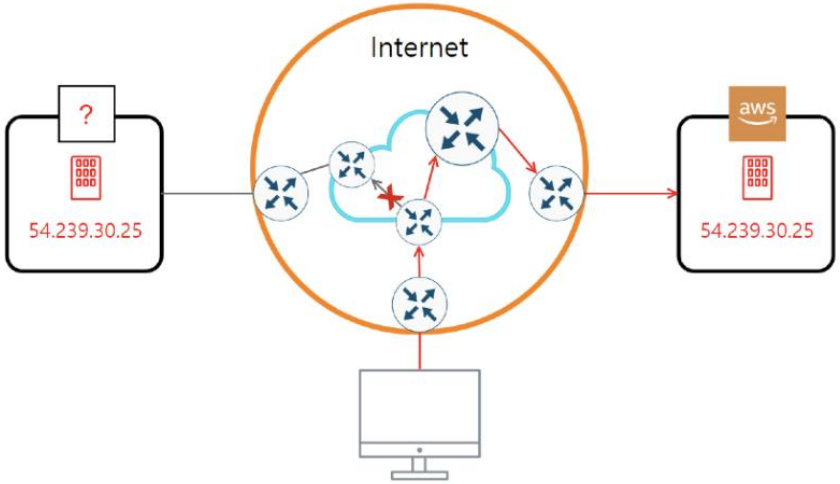
- 어느 한 IP가 퍼블릭과 프라이빗 중 어떤 성격을 띠는지는 누가 결정할까?
- 바로 ISP(Internet Service Provider)다.
- AWS 관리 콘솔에 접속하는 예를 들어보자.
- 그림은 사용자가 AWS 관리 콘솔에 접속하는 인터넷 경로를 나타낸 것이다.



1. 트래픽의 시작 : IP 주소

퍼블릭 IP와 인터넷 라우팅

- AWW ISP에게 일정 비용을 지불해 IP를 할당받는다.
- 그림은 아마존이 사용하는 IP를 다른 곳에서 임의로 사용한 모습이다.

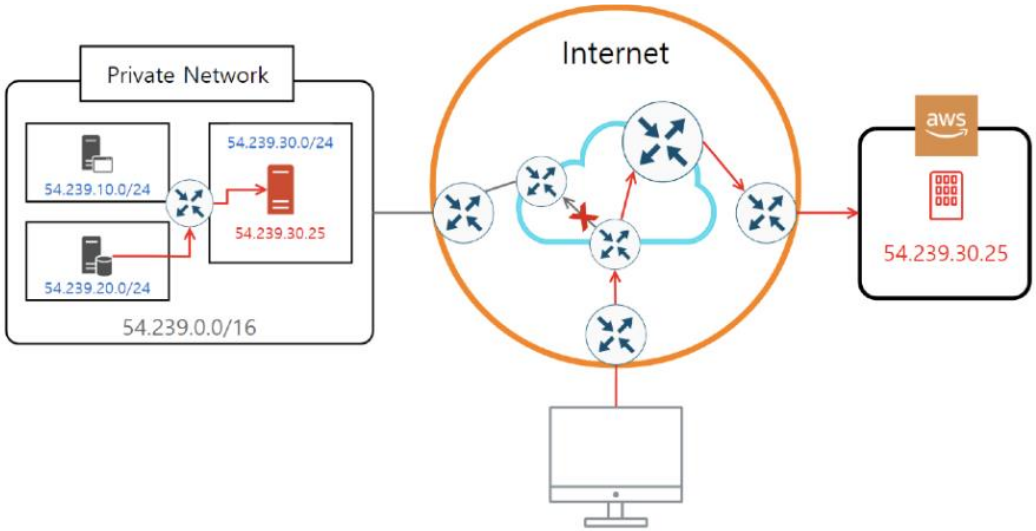


- 이처럼 다른 기업 또는 개인이 AWS의 IP를 디바이스에 임의로 할당해도, 그 디바이스로는 트래픽 전달이 안되기 때문에 인터넷 활동은 할 수 없다.
- 그러나 이 IP는 내부망에서는 중복이 없는 한 제약없이 사용할 수 있다.
- 이것을 프라이빗 IP라고 한다.
- 프라이빗 IP를 사용할 땐 NAT IP로써 인터넷에 접속할 수 있다.

1. 트래픽의 시작 : IP 주소

프라이빗 IP와 VPC CIDR 선정

- 그림은 AWS와 동일한 IP를 사설 네트워크 서버에 할당한 모습이다



- 그림의 54.239.0.0/16을 자세히 보면 VPC의 CIDR과 닮았음을 알 수 있다.
- VPC CIDR도 사설 네트워크처럼 사용자 마음대로 설정한다.

1. 트래픽의 시작 : IP 주소

프라이빗 IP와 VPC CIDR 선정

- [54.239.0.0/16] 네트워크 내부 사용자가 내부 서버[54.239.30.25]가 아닌 AWS 관리 콘솔 [54.239.30.25]에 접속하려면 어떻게 해야 할까?
- 사용자가 둘 중 어디로 접속하고 싶은지 네트워크는 알지 못한다.
- 사용자가 콘솔에 접속하도록 제어하는 방법은 있지만, 내부 서버 접속은 포기해야 한다.
- 이같은 네트워크 IP 충돌 이슈를 최소화하려면 사내 네트워크나 VPC CIDR은 고심해서 결정해야 한다
- CIDR의 인스턴스가 주로 통신할 인터넷 대상 IP가 인스턴트 IP와 중첩되면 잦은 통신 오류가 발생한다.
- 따라서 국가별 사용 IP 범위를 파악해 가급적 통신 빈도가 낮은 해외 IP를 CIDR로 채택하는 것이 좋다

1. 트래픽의 시작 : IP 주소

AWS의 IP 분류

- AWS IP를 다음 표처럼 분류할 수 있다.

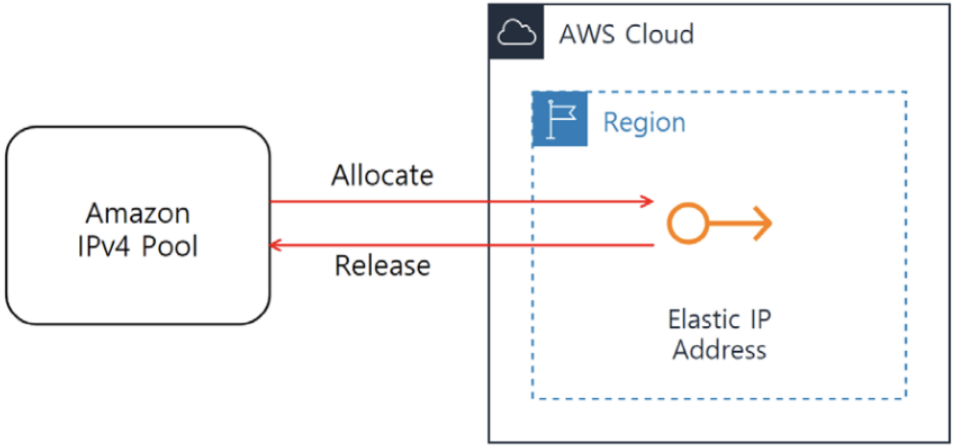
인터넷 접근성 / 고정 여부	퍼블릭	프라이빗
정적	탄력적 IP	·기본 프라이빗 IP ·보조 프라이빗 IP
동적	퍼블릭 IP	-

- 탄력적 IP(Elastic IP, EIP)는 정적 퍼블릭 IP로 리전에 종속된 네트워킹 리소스다.
- 인스턴스나 NAT 게이트웨이, 로드밸런서 등 인터넷 접속이 필요한 리소스에 연결해서 사용하며 리소스 자체만으로는 아무것도 할 수 없다.
- 탄력적 IP는 네트워크 인터페이스의 프라이빗 IP에 연결된다.
- Amazon의 IPv4 주소 풀은 Amazon의 퍼블릭 IP 모음이다.
- 사용자가 탄력적 IP 주소를 요청하면 AWS는 IPv4 주소 풀에 있는 IP 하나를 내 계정에 할당해 준다.

1. 트래픽의 시작 : IP 주소

AWS의 IP 분류

- 그림은 Amazon IPv4 주소 풀에서 리전으로 탄력적 IP를 할당 또는 릴리스하는 모습을 보여준다.



- 퍼블릭 IP도 Amazon IPv4 주소 풀에서 할당받지만 탄력적 IP처럼 계정이 소유하진 못한다.
- 따라서 계정과 리소스 사이 IP 연결 및 해제 작업은 생략된다.

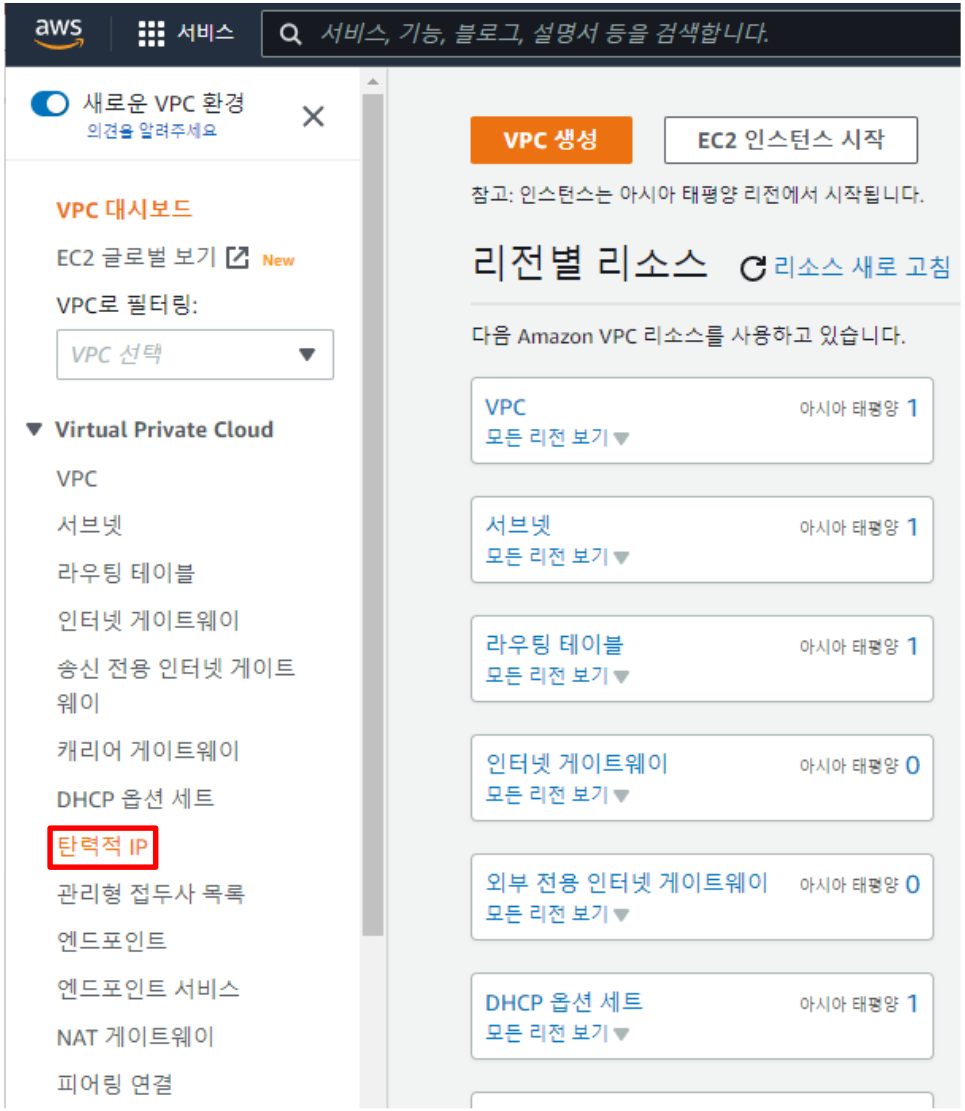
1. 트래픽의 시작 : IP 주소

실습. 탄력적 IP 할당 예제

- 탄력적 IP 메뉴에서 우측 상단 탄력적 IP주소할당 버튼을 클릭한다.
- 메뉴

1. 트래픽의 시작 : IP 주소

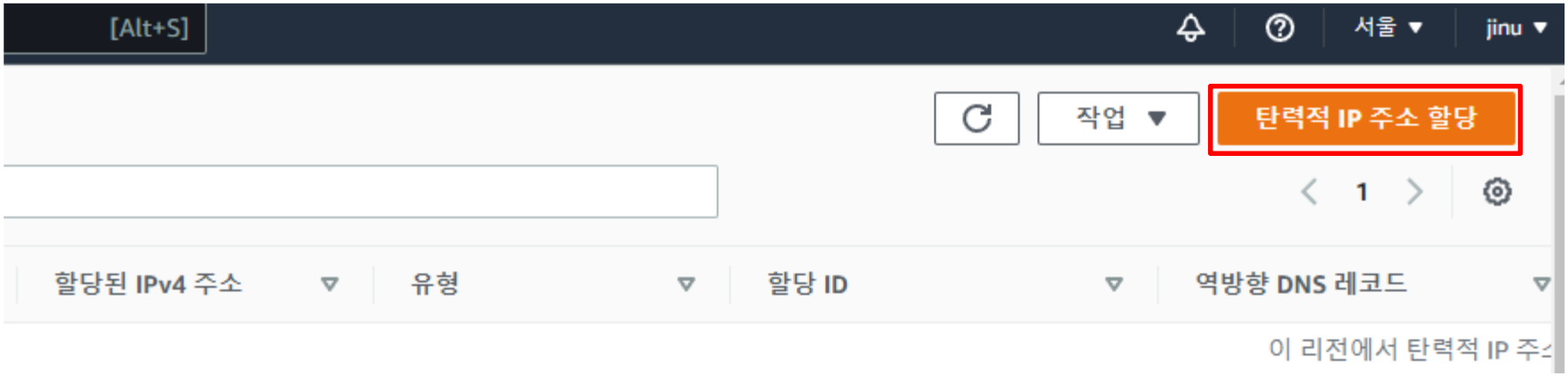
- **실습. 탄력적 IP 할당 예제**
  - 서비스>VPC>탄력적 IP를 선택한다.



1. 트래픽의 시작 : IP 주소

실습. 탄력적 IP 할당 예제

- 서비스>VPC>탄력적 IP를 선택한다.



1. 트래픽의 시작 : IP 주소

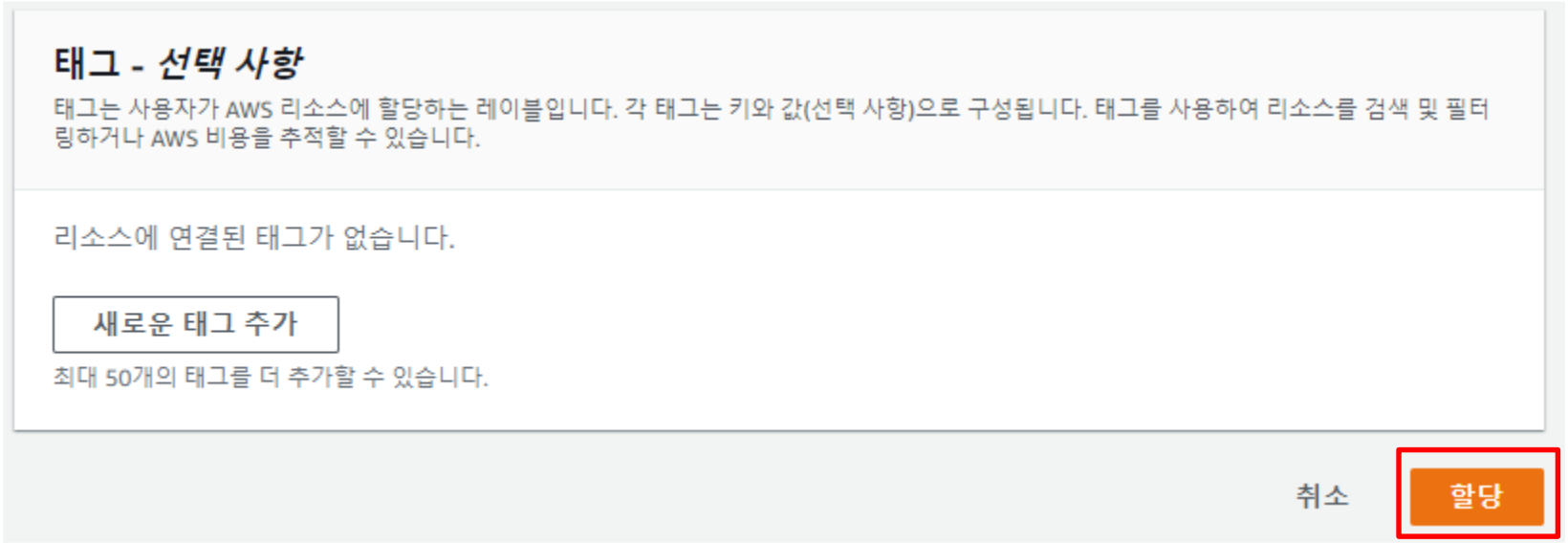
실습. 탄력적 IP 할당 예제

- 이미 선택된 네트워크 경계 그룹과 Amazon의 IPv4주소 풀옵션을 확인한다.

1. 트래픽의 시작 : IP 주소

실습. 탄력적 IP 할당 예제

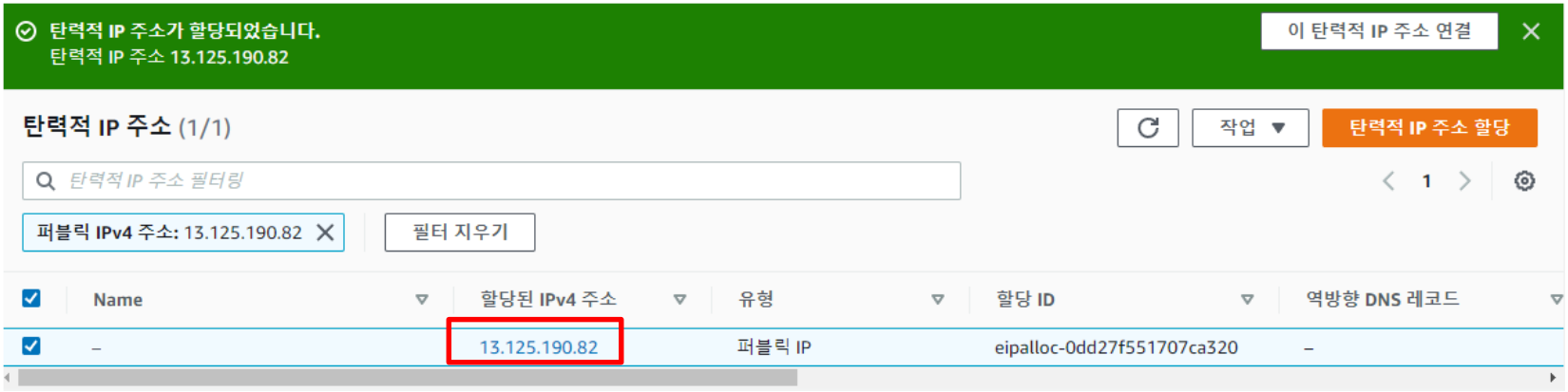
- 할당 (Allocate) 버튼을 클릭하면 탄력적 IP가 생성된다.



1. 트래픽의 시작 : IP 주소

실습. 탄력적 IP 할당 예제

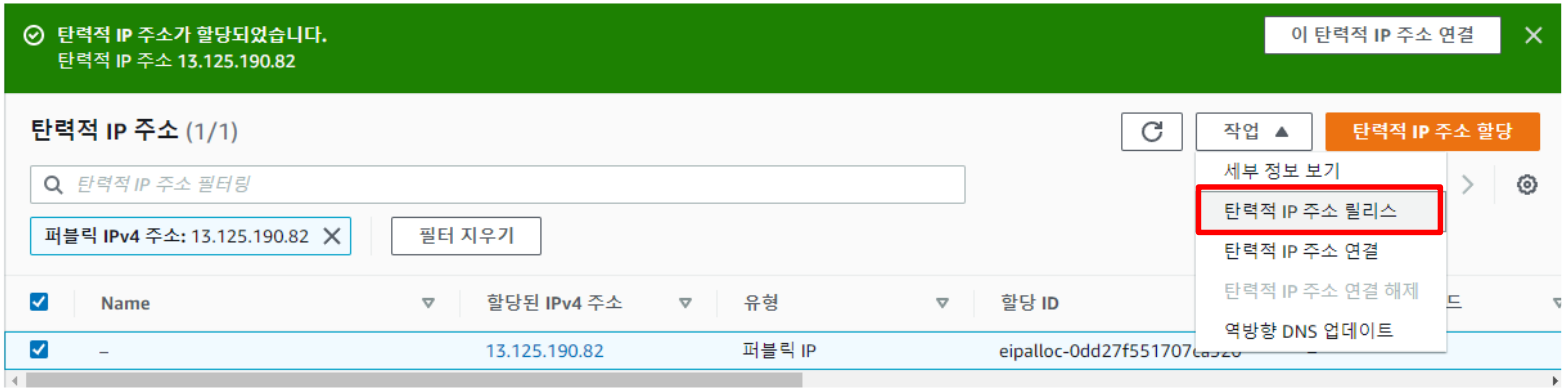
- 생성된 탄력적 IP 주소를 확인한다.



1. 트래픽의 시작 : IP 주소

실습. 탄력적 IP 할당 예제

- 탄력적 IP 미사용 시 작업 > 탄력적 IP 주소 릴리스 메뉴로 Amazon 풀에 반환한다.



1. 트래픽의 시작 : IP 주소

AWS에서의 네트워크 경계 그룹(Network Border Group)

- 네트워크 경계 그룹(Network Border Group)이란 AWS가 퍼블릭 IP를 광고하는 영역.
- 그림은 웹 브라우저로 https://ip-ranges.amazonaws.com/ip-ranges.json에 접속한 결과의 일부이다


```
{
  "syncToken": "1657291988",
  "createDate": "2022-07-08-14-53-08",
  "prefixes": [
    {
      "ip_prefix": "3.5.140.0/22",
      "region": "ap-northeast-2",
      "service": "AMAZON",
      "network_border_group": "ap-northeast-2"
    },
    {
      "ip_prefix": "13.34.37.64/27",
      "region": "ap-southeast-4",
      "service": "AMAZON",
      "network_border_group": "ap-southeast-4"
    },
```

1. 트래픽의 시작 : IP 주소

퍼블릭 IPv4주소 풀

- Amazon의 IPv4 주소 풀은 AWS의 모든 퍼블릭 IP를 뜻한다.
- AWS 계정으로 가져오는 퍼블릭 IPv4 주소(Bring Your Own IP, BYOIP)는 온프레미스 네트워크에서 사용하는 퍼블릭 IP를 AWS로 옮겨 사용하는 것을 뜻한다.
- IPv4 주소의 고객 소유 풀(Customer-owned IP address, CoIP)은 고객이 소유한 네트워크 주소 풀이다.
- AWS Outposts는 AWS 리전을 온프레미스까지 확장해서 사용하는 서비스로, VPC의 일부 서브넷을 온프레미스 인프라상에 생성할 수 있다.
- AWS Outposts를 이용하려면 AWS에서 제공하는 별도 장치를 온프레미스에 설치하고 AWS 리전과 연동해야 한다.

2. 트래픽 전달의 주체 : 탄력적 네트워크 인터페이스(ENI)

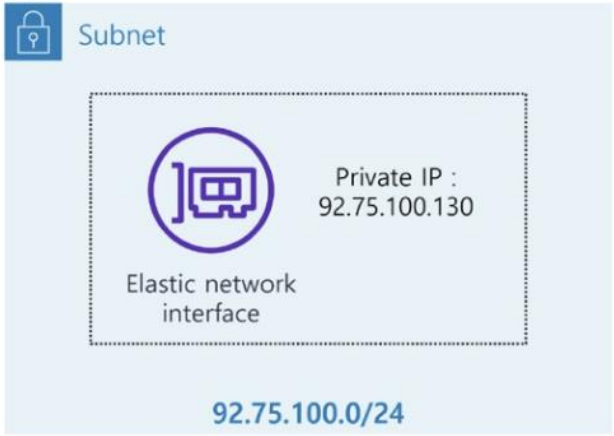
VPC 서비스의 전용배송원 : ENI

- ENI는 온프레미스 서버의 NIC(Network Interface Card)에 상응하는 가상장치다.
- ENI는 인스턴스가 만들어 낸 트래픽을 네트워크로 전송하거나 네트워크에서 들어온 트래픽을 수신한다.
- VPC 네트워킹은 반드시 ENI를 기반으로 한다.
- 그러나 모든 AWS 서비스가 VPC 네트워킹 환경을 이용하는 것은 아니다.
- 예컨대 S3도 IP 접근이 가능하지만 ENI가 연결돼 있진 않다.
- 물론 우리에게 보이지 않는 S3 전용 인터페이스가 있기에 IP 통신이 가능할 것이다.
- 이처럼 ENI가 없는 서비스는 자체 보안 기능과 정책 권한으로 통제한다.

2. 트래픽 전달의 주체 : 탄력적 네트워크 인터페이스(ENI)

VPC 서비스의 전용배송원 : ENI

- ENI는 서브넷에 생성하므로, 그림처럼 최소 1개의 프라이빗 IP를 소유한다.
- 이를 기본 프라이빗 IPv4주소라 한다.
- 서브넷 CIDR 범위 내에서 ENI의 프라이빗 IP를 직접 지정하거나 자동 할당 기능을 이용할 수도 있다.
- ENI는 개별 생성이 가능하지만 그 자체만으로는 아무 기능도 못한다.
- 반드시 VPC 서비스에 연결된 상태로 존재해야 한다.



2. 트래픽 전달의 주체 : 탄력적 네트워크 인터페이스(ENI)

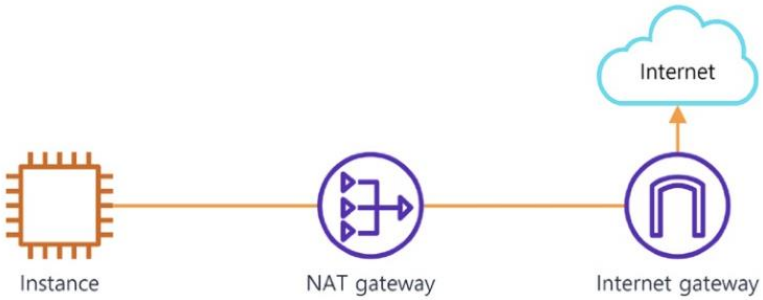
ENI의 2가지 유형

- **ENI는 다양한 형태로 서비스에 연결돼 트래픽을 송수신한다.**
- **ENI 사용은 곧 VPC 네트워킹을 의미하므로, ENI에 연결된 모든 서비스는 반드시 VPC 네트워킹의 보안 통제를 받는다.**
- **ENI가 연결된 서비스는 크게 2가지 서비스로 분류한다.**
  - A 유형: 데이터 처리가 주 역할인 서비스
  - B 유형: 트래픽 전송이 주 역할인 서비스
- **A 유형 서비스는 인스턴스나 RDS, Lambda, EFS 등이 있다.**
  - 이들은 애플리케이션 실행, 컴퓨팅, 스토리지 등 데이터 가공이나 저장이 주된 역할이며 ENI는 단지 트래픽을 전송하는 수단에 불과하다.
- **B 유형 서비스는 NAT 게이트웨이나 전송 게이트웨이 같은 네트워크 디바이스로 트래픽 전송이 주 목적이다.**
  - 물론 트래픽 전달 과정에서 경로를 제어하지만, 트래픽에 포함된 데이터 내용을 변경 또는 가공하진 않는다.

2. 트래픽 전달의 주체 : 탄력적 네트워크 인터페이스(ENI)

ENI의 2가지 유형

- 그림은 프라이빗 인스턴스 트래픽이 NAT 게이트웨이를 경유해 인터넷으로 전달되는 경로를 나타낸다.
- 인스턴스(A 유형)에서 전송할 데이터는 가공된 것일 수 있지만, NAT 게이트웨이(B 유형) 통과 전후 패킷은 별도 가공없이 출발지 IP만 퍼블릭으로 변환해 인터넷으로 전달한다.

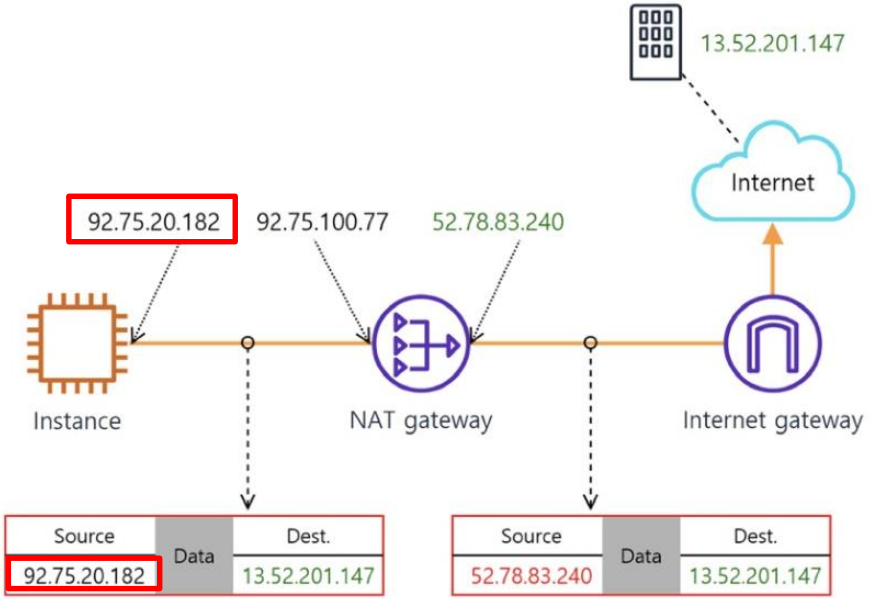


- 이처럼 ENI가 기생하는 서비스의 형태는 다르지만 트래픽을 전달한다는 측면에서는 일치한다.
- 이들은 모두 서비스 > EC2 > 네트워크 인터페이스 메뉴에서 확인할 수 있다.
- 지금부터 A 유형 서비스에 연결된 ENI를 컴퓨팅 ENI, B 유형 서비스에 연결된 ENI를 라우팅 ENI 정의하자.
- AWS 공식 용어는 아니다.
- 컴퓨팅 ENI와 라우팅 ENI는 2가지 큰 차이점이 있다.

2. 트래픽 전달의 주체 : 탄력적 네트워크 인터페이스(ENI)

ENI 유형 비교(1): 소스/대상 확인

- ENI는 소스/대상 확인(Source/dest. check) 속성이 있다.
- 이는 ENI가 패킷을 전송하고 수신할 때 출발지 IP와 목적지 IP를 검사할 것인지를 선택하는 옵션이다.
- 다음 그림은 ENI의 트래픽 전송을 상세히 표현한 토폴로지다.
- 인스턴스는 현재 소스/대상 확인 옵션이 켜져 있고('예') NAT 게이트웨이는 꺼둔('아니오')상태다.



- 소스/대상 확인 옵션이 켜져 있으면, 두 IP가 같을 때만 패킷을 전송하게 된다.
- 이때 인스턴스의 ENI는 패킷 전송 전, 패킷의 출발지 IP와 ENI의 IP가 꼭 같아야만 패킷을 전송할 수 있다.

2. 트래픽 전달의 주체 : 탄력적 네트워크 인터페이스(ENI)

ENI 유형 비교(1): 소스/대상 확인

- NAT 게이트웨이는 프라이빗 영역의 패킷을 퍼블릭(인터넷)으로 전달해야 하므로, 프라이빗 IP와 퍼블릭 IP를 모두 소유한다.
- NAT가 인스턴스에게 전달받은 패킷의 목적지는 [13.52.201.147]이고, NAT의 프라이빗 IP는 [92.75.100.77]이므로 IP가 서로 다르다(대상 확인).
- 그러나 NAT 게이트웨이의 소스/대상확인 옵션이 꺼져 있으므로 두 IP가 달라도 패킷을 전달할 수 있다.
- 소스/대상확인 옵션이 켜진 상태라면 해당 패킷은 더 이상 전달되지 못하고 소멸한다.
- 인스턴스도 이 옵션을 끈다면 어떻게 될까?
- 이상없이 패킷을 전달한다.
- 왜냐하면 설정이 켜져 있을 때만 통제하기 때문이다.
- 따라서 옵션이 꺼지면 모든 패킷을 전송/수용하고, 옵션이 켜지면 패킷을 선별해 전송/수용한다.

2. 트래픽 전달의 주체 : 탄력적 네트워크 인터페이스(ENI)

ENI 유형 비교(1): 소스/대상 확인

- 이처럼 인스턴스가 사용하는 컴퓨팅 ENI는 소스/대상확인 옵션이 켜져 있고 NAT 게이트웨이가 사용하는 라우팅 ENI는 꺼진 상태로 생성된다.
- 2가지 ENI를 표로 비교해보자.

ENI 유형 / 소스/대상 확인	컴퓨팅 ENI	라우팅 ENI
예	O (기본값)	설정 불가
아니오	O	O (기본값)

- 컴퓨팅 ENI는 설정을 켜거나 끌 수 있으나 라우팅 ENI는 설정을 켤 수 없음을 알 수 있다.
- 그러므로 인스턴스와 같은 컴퓨팅 ENI 서비스에 소스/대상확인 설정이 꺼져 있다면 그 인스턴스를 트래픽 전송의 경유지로 활용할 수 있어 보안에 취약하다.
- 따라서 인스턴스를 게이트웨이로 사용하지 않는다면 소스/대상 확인 옵션은 반드시 켜야 한다.

2. 트래픽 전달의 주체 : 탄력적 네트워크 인터페이스(ENI)

요청자 관리형 ENI

- NAT 게이트웨이도 라우팅 ENI 중 하나로서 소스/대상확인 옵션을 변경하는 기능이 없다.
- 그럼 NAT 게이트웨이가 사용하는 ENI의 설정을 강제로 바꾸면 어떻게 될까?
- 오류가 나타난다.
- AWS는 NAT 게이트웨이의 ENI 설정을 ENI 메뉴에서 함부로 바꾸지 못하도록 안전 장치를 걸어놨기 때문이다.
- 그림은 NAT 게이트웨이가 사용하는 ENI를 찾아 소스/대상 확인 속성을 변경한 결과다.
- NAT 게이트웨이 메뉴에서 제공하지 않는 기능은 ENI 메뉴에서도 마음대로 변경할 수 없으므로 오류가 발생했다.

2. 트래픽 전달의 주체 : 탄력적 네트워크 인터페이스(ENI)

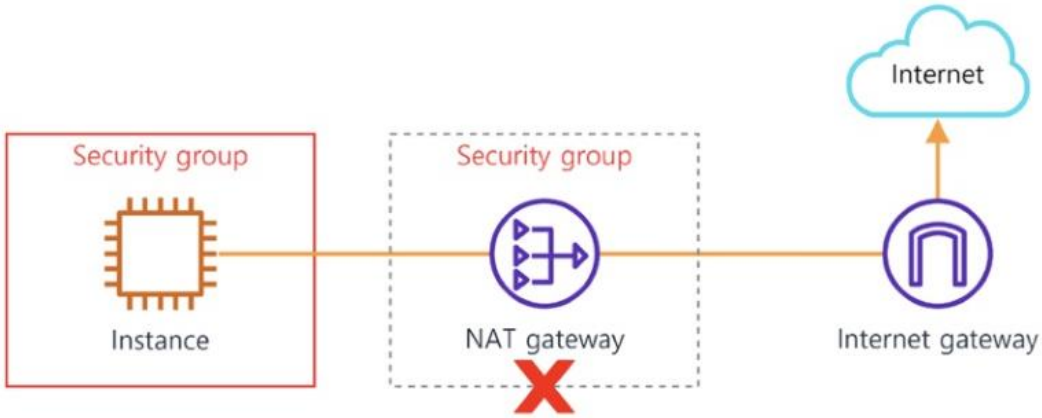
요청자 관리형 ENI

- AWS는 서비스의 본 기능을 무시한 사용자가 ENI 메뉴에서 설정 임의 변경을 못하도록 요청자 관리형(Request-managed)속성을 뒀다.
- 이 속성값은 AWS에서 지정하며 사용자가 바꿀 수 없다.
- 요청자 관리형 속성값이 '예'로 설정된 서비스는 ENI가 장착된 서비스 메뉴에서만 ENI 속성을 조작할 수 있다.
- 예컨대 NAT 게이트웨이 메뉴로써 ENI 속성을 건드려야 한다.
- 따라서 앞 그림의 좌측 작업 리스트에 보이는 모든 작업이 가능하다.
- 그렇다고 이 기능 모두가 NAT 게이트웨이 서비스 메뉴에서 조작할 수 있는 것도 아니다.
- AWS가 허용하는 NAT 게이트웨이 관련 기능 내에서만 가능하다.
- 요청자 관리형 속성값이 '아니요'라면 상기 작업을 마음대로 실행할 수 있다.
- 컴퓨팅 ENI 및 라우팅 ENI 구분과 관계없이, 인스턴스를 제외한 대부분의 서비스는 요청자 관리형 ENI를 사용한다.

2. 트래픽 전달의 주체 : 탄력적 네트워크 인터페이스(ENI)

ENI 유형 비교(2): 보안 그룹(SG)강제 적용

- 그림은 컴퓨팅 ENI와 라우팅 ENI를 비교하고 있다.
- 컴퓨팅 ENI를 사용하는 컴퓨팅 서비스(인스턴스)는 데이터 처리와 보관을 담당하므로 데이터 보호에 각별히 유의해야 한다.
- 이런 특성 때문에 VPC는 컴퓨팅 ENI를 보안 그룹으로 보호한다.
- 접속 대상 IP와 포트만 보안 그룹에 등록해서 외부로부터 컴퓨팅 서비스와 데이터를 보호하고 있다.

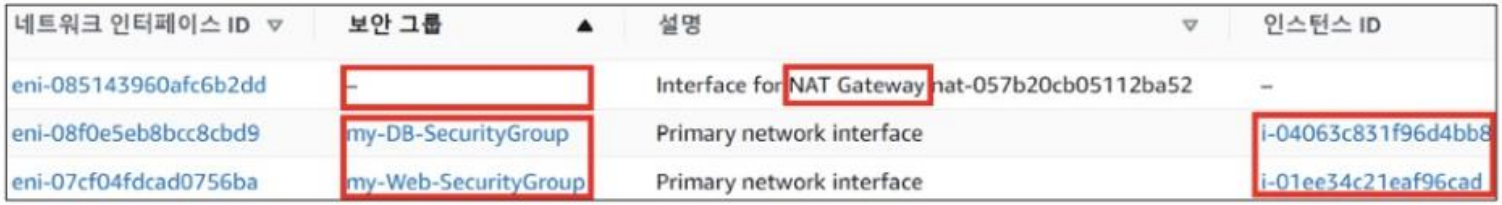


- ENI 목록에서 보안 그룹이 연결된 ENI는 컴퓨팅 ENI다.
- 반대로 연결된 보안 그룹이 보이지 않는다면 라우팅 ENI일 것이다.

2. 트래픽 전달의 주체 : 탄력적 네트워크 인터페이스(ENI)

IT COOKBOOK

- ENI 유형 비교(2): 보안 그룹(SG)강제 적용
  - 그림은 NAT 게이트웨이와 인스턴스의 ENI 목록이다.
  - 첫 번째 ENI는 NAT 게이트웨이가 사용하는 것으로, 연결된 보안 그룹이 없다.
  - 반면 두 번째와 세 번째 ENI는 인스턴스에 연결된 ENI로, 보안 그룹이 연결된 것을 확인할 수 있다.



네트워크 인터페이스 ID	보안 그룹	설명	인스턴스 ID
eni-085143960afc6b2dd	–	Interface for NAT Gateway nat-057b20cb05112ba52	–
eni-08f0e5eb8bcc8cbd9	my-DB-SecurityGroup	Primary network interface	i-04063c831f96d4bb8
eni-07cf04fdcad0756ba	my-Web-SecurityGroup	Primary network interface	i-01ee34c21eaf96cad

2. 트래픽 전달의 주체 : 탄력적 네트워크 인터페이스(ENI)

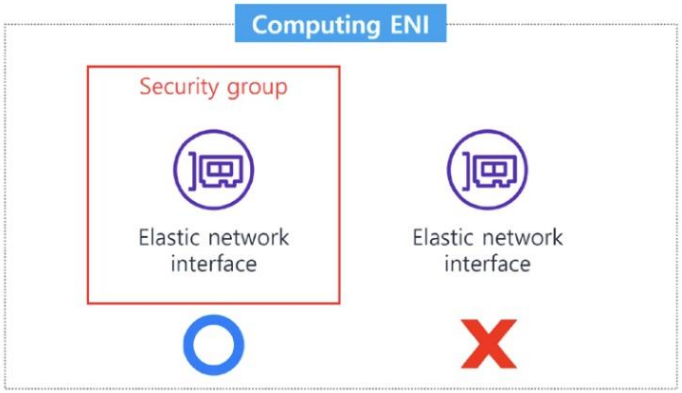
SG와 서브넷에 의존하는 ENI

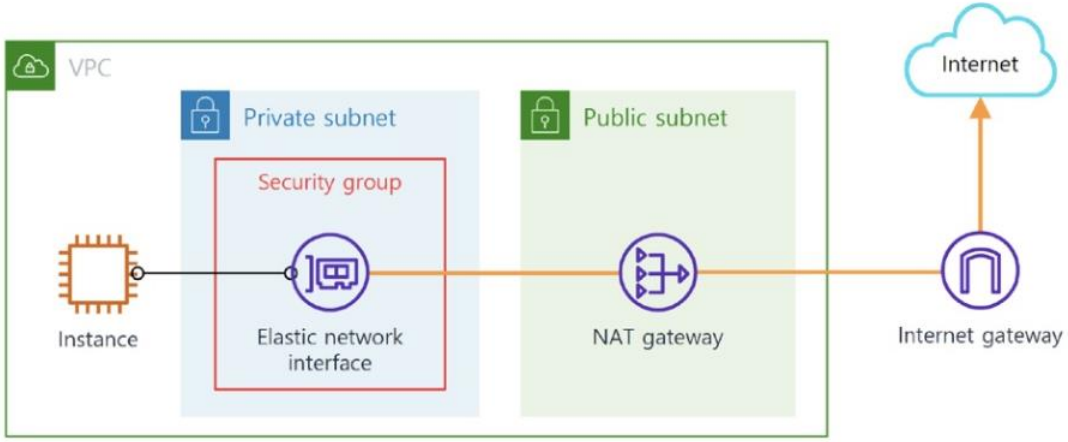
- **6장에서 VPC 네트워킹을 다음과 같이 정의했다.**
  - AWS 서비스가 네트워크 인터페이스를 사용하면 자동으로 보안 그룹, 네트워크 ACL 그리고 라우팅 테이블의 통제를 받게 된다.
  - 이를 두고 서비스가 VPC 네트워킹을 사용한다고 말한다.
- **여기서 말하는 네트워크 인터페이스는 컴퓨팅 ENI를 뜻한다.**
- **라우팅 ENI는 상기 정의에서 보안 그룹 부분만 제외하고 네트워크 ACL과 라우팅 테이블의 통제를 받는다.**
- **컴퓨팅 ENI의 수명 주기는 보안 그룹과 함께 한다.**
- **ENI를 사용하는 모든 컴퓨팅 서비스는 생성 단계에서 보안 그룹을 반드시 지정하도록 설계돼 있다.**

2. 트래픽 전달의 주체 : 탄력적 네트워크 인터페이스(ENI)

SG와 서브넷에 의존하는 ENI

- 왼쪽 그림은 컴퓨팅 ENI와 보안 그룹의 상호 의존성을 보여준다.
- 보안 그룹은 홀로 존재할 수 있지만, 컴퓨팅 ENI는 보안 그룹이 반드시 연결돼 있어야 한다.





- ENI의 부모는 서브넷이다.
- 따라서 서브넷이 반드시 생성돼 있어야 한다.
- 서브넷의 패런트는 VPC이므로 오른쪽 그림과 같은 토폴로지를 완성할 수 있다.
- 보안 그룹을 사용하는 컴퓨팅 ENI(인스턴스와 사용하지 않는 라우팅 ENI(NAT 게이트웨이)를 함께 보여준다.

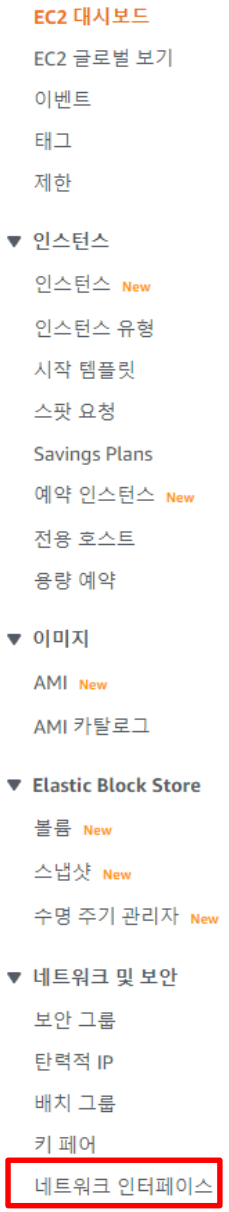
2. 트래픽 전달의 주체 : 탄력적 네트워크 인터페이스(ENI)

- **ENI 보호 = VPC 보호**
  - VPC 트래픽의 시작과 끝은 ENI이다.
  - 따라서, VPC 보안을 강화하려면 ENI에 연결된 보안 그룹과 서브넷에 연결된 네트워크 ACL, 그리고 라우팅 테이블을 안전하게 통제하면 된다.
  - 퍼블릭 인스턴스를 보안 그룹, 네트워크 ACL, 그리고 라우팅 테이블로 안전하게 통제하는 방식은 VPC 네트워킹 환경에서 할 수 있는 최대의 노력이다.
  - 이보다 더 높은 보안은 없다.
  - 즉, 반드시 필요한 규칙만 등록해서 사용해야 한다.
  - 따라서 자주 사용하는 서비스의 개별 특징을 이해하고 그 성격에 따라 보안통제 계획을 세워 관리해야할 것이다.

2. 트래픽 전달의 주체 : 탄력적 네트워크 인터페이스(ENI)

IT COOKBOOK

- **실습. ENI 생성 예제**
  - 서비스 > EC2 > 네트워크 및 보안 > 네트워크 인터페이스 메뉴를 선택한다.

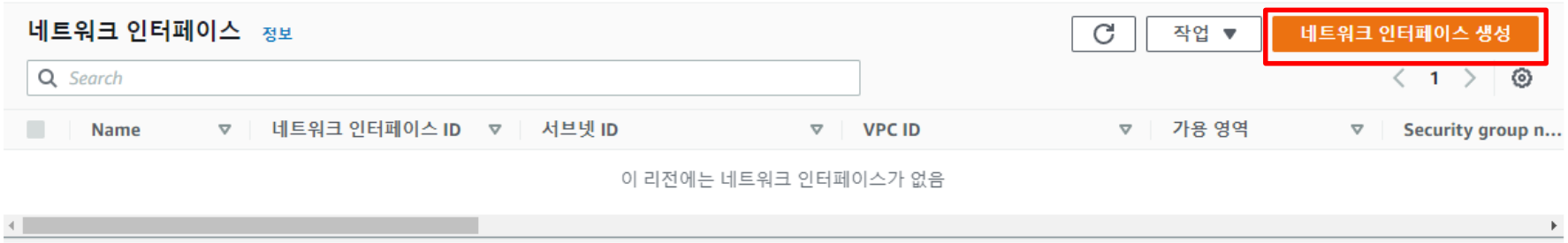


2. 트래픽 전달의 주체 : 탄력적 네트워크 인터페이스(ENI)

IT COOKBOOK

실습. ENI 생성 예제

- 네트워크 인터페이스 메뉴에서 네트워크 인터페이스 생성 버튼을 클릭한다.



2. 트래픽 전달의 주체 : 탄력적 네트워크 인터페이스(ENI)

실습. ENI 생성 예제

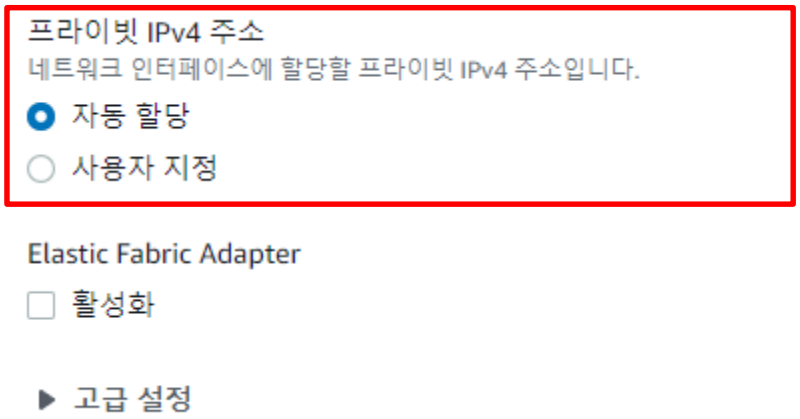
- Description(ENI 설명)을 입력하고, ENI가 위치할 서브넷을 선택한다.
- 실습에서 만든 서브넷 중 하나를 선택할 수도 있다.

2. 트래픽 전달의 주체 : 탄력적 네트워크 인터페이스(ENI)

IT COOKBOOK

실습. ENI 생성 예제

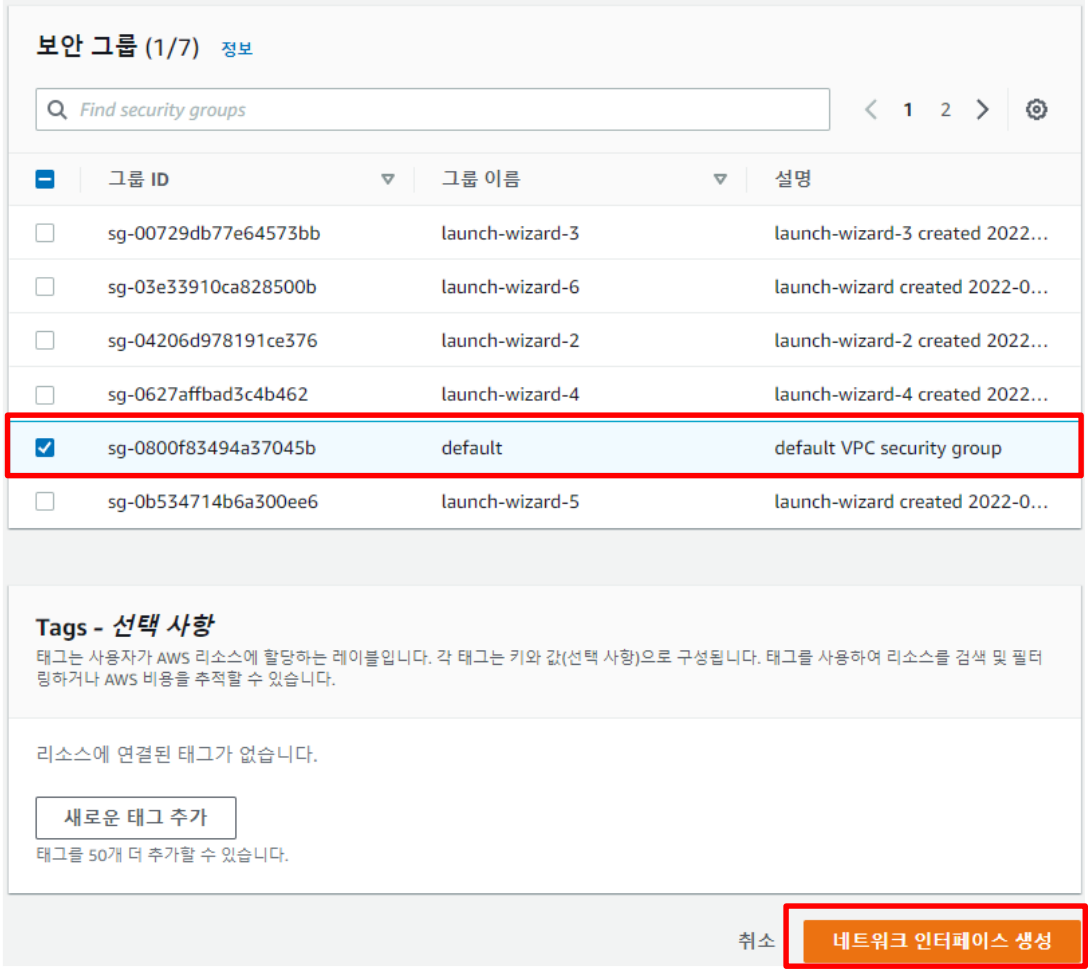
- 프라이빗 IP는 자동 할당과 사용자 지정 중에서 선택할 수 있다.
- 자동 할당 선택 시 서브넷 CIDR 범위의 IP 하나를 랜덤으로 할당받는다.
- 사용자지정을 선택하면 그림처럼 원하는 IP를 IPv4 형식에 맞게 입력해야 한다.



2. 트래픽 전달의 주체 : 탄력적 네트워크 인터페이스(ENI)

실습. ENI 생성 예제

- 컴퓨팅 ENI는 보안 그룹을 반드시 지정해야 한다.
- 보안 그룹을 선택하고 네트워크 인터페이스생성 버튼을 클릭하면 ENI 생성이 완료된다.



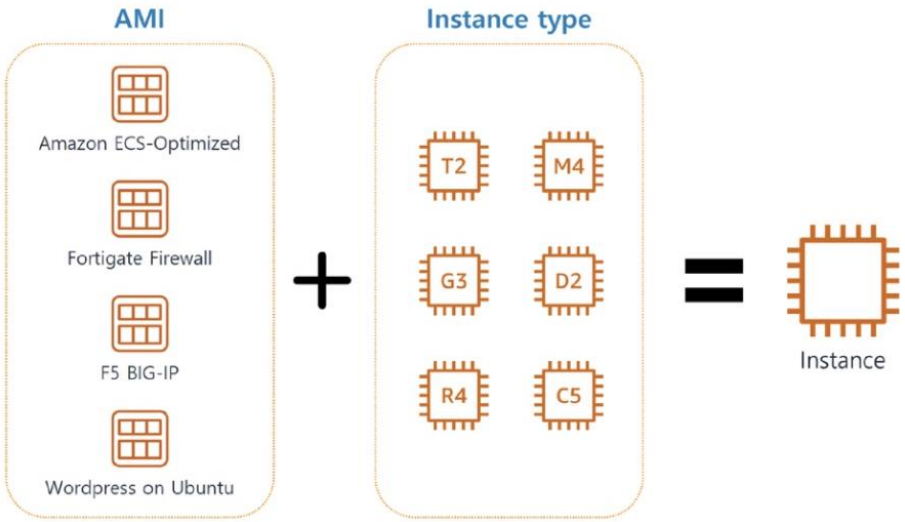
3. 트래픽 생성의 주체 : EC2 인스턴스

트래픽 공장의 대표 이사: 인스턴스

- 인스턴스는 가상 서버다.
- Linux나 Windows 같은 OS가 설치된 일반적인 서버만 떠올릴 수 있지만 AWS가 제공하는 인스턴스의 활용 범위는 무궁무진하다.
- 모든 종류의 운영체제는 물론이고 AWS Marketplace를 이용해 데이터 분석이나 블록체인용 머신도 구축할 수 있다.
- 또 방화벽이나 라우터, VPN 등 네트워크 어플라이언스 장비뿐만 아니라 스토리지 서비스도 인스턴스로 구현할 수 있다.
- 그럼 이것을 가능케 하는 요소는 무엇일까?
- 바로 AMI(Amazon Machine Image)이다.
- 인스턴스를 생성하려면 반드시 하나의 AMI를 선택해야 한다.
- 선택한 AMI에 따라서 OS만 설치된 깡통 서버가 되기도 하고, 네트워크 디바이스로 변신하기도 한다.
- 또 사용자가 원하는 소프트웨어가 OS에 설치된 형태로 제공하기도 한다.
- 이처럼 클라우드 사용자의 요구사항을 담아 패키징하거나 서드파티가 판매하는 제품을 소프트웨어 형태의 이미지로 만든 것이 AMI다.

3. 트래픽 생성의 주체 : EC2 인스턴스

- 트래픽 공장의 대표 이사: 인스턴스
  - 그림은 인스턴스 생성 방식을 보여준다.



  - AMI의 특성과 활용 방식에 따라 인스턴스에 필요한 설정이 조금씩 달라진다.

3. 트래픽 생성의 주체 : EC2 인스턴스

인스턴스로 위장한 AWS 서비스들

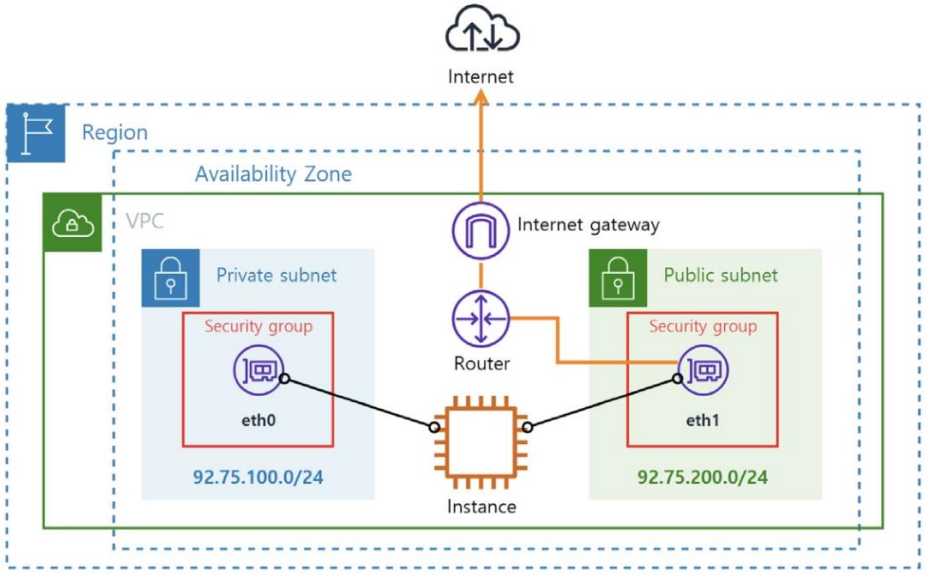
- 이와 같이 AMI를 선택해서 인스턴스를 사용하는 방식이 있는 반면 AWS 자체 서비스가 인스턴스 형태로 생성되는 방식도 있다.
- 이같은 서비스를 생성하면 인스턴스가 만들어지고 그 위에서 서비스가 작동한다.
- 정리하면 EC2 인스턴스 목록에서 확인할 수 있는 서비스는 크게 2개로 분류할 수 있다.
  - A 유형 : EC2 메뉴 인스턴스 시작 버튼으로 생성한 서비스
  - B 유형 : AWS 자체 서비스 메뉴에서 생성한 컴퓨팅 서비스
- 2가지 유형 모두 인스턴스로 동작하지만 관리 측면에서 일부 차이가 있다.

구분 \ 서비스 유형	A 유형	B 유형
AMI 직접 선택	O (필수)	X (불가)
생성 화면	인스턴스 메뉴	개별 서비스 메뉴
기능/옵션 설정	인스턴스 or 관리자 화면 직접 접속	개별 서비스 메뉴
트래픽 전송 매체	ENI	

3. 트래픽 생성의 주체 : EC2 인스턴스

인스턴스의 위상

- VPC 네트워킹 보안 통제 측면에서 A와 B 유형은 크게 차이가 없다.
- 생성된 방식이나 유형과 무관하게, 모든 인스턴스는 최소 1개 이상의 ENI를 연결해야 하기 때문이다.
- 따라서 모든 인스턴스는 VPC 보안 통제를 받는다.



3. 트래픽 생성의 주체 : EC2 인스턴스

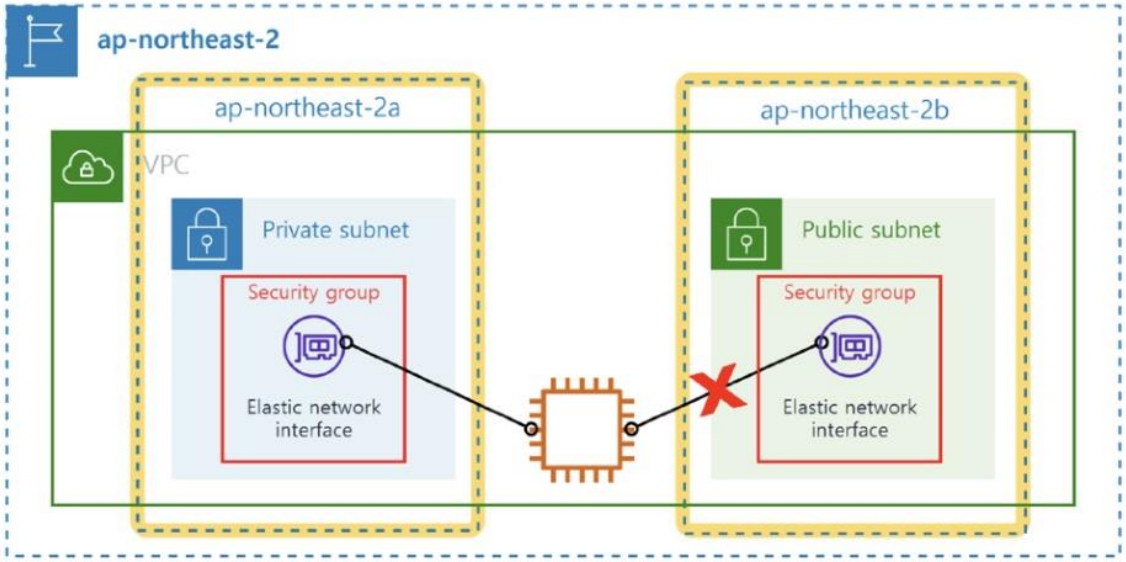
인스턴스의 위상

인스턴스의 조건

- 인스턴스 생성 시점에 기본 네트워크 인터페이스(Primary Network Interface)도 자동으로 생성되면서 서로 연결된다.
- eth0으로 표현하는 이 기본 네트워크 인터페이스는 인스턴스와 분리할 수 없다.
- 인스턴스는 최소 1개 이상의 ENI가 연결돼 있어야 한다.
  - 인스턴스에 ENI가 1개 존재한다면 eth0이다.
  - ENI는 서브넷(패런트)에 생성된다.
- 인스턴스의 부모는 가용 영역과 VPC다.
- 그러므로 그 둘의 교집합 영역에 놓여야 한다.
- 정리하면 인스턴스는 수명 주기 동안 기본 네트워크 인터페이스(eth0)의 가용 영역을 벗어날 수 없다.

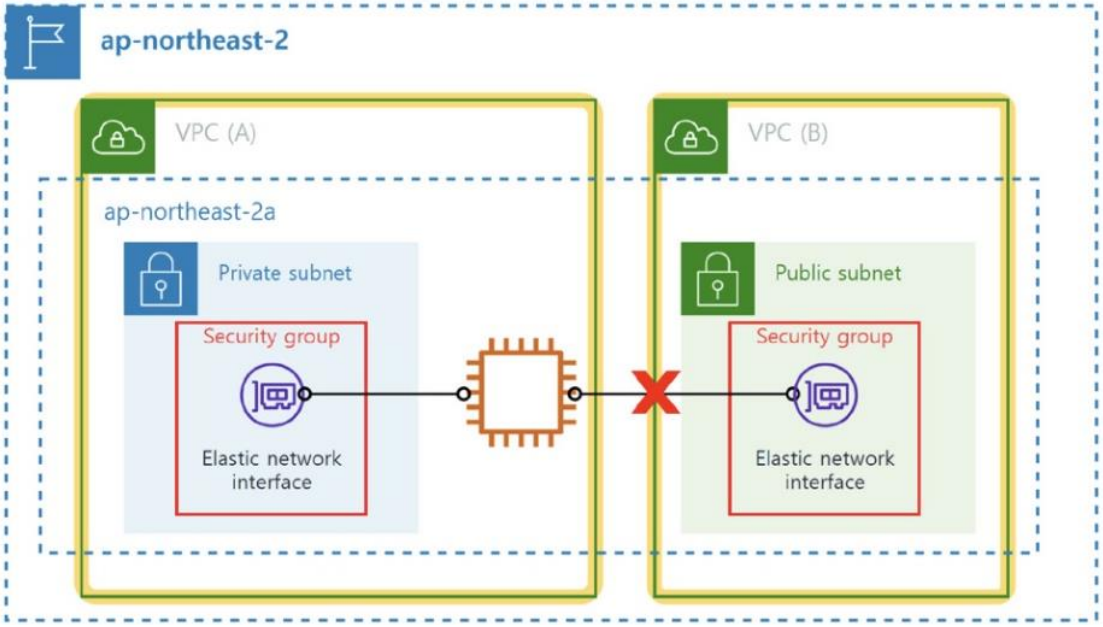
3. 트래픽 생성의 주체 : EC2 인스턴스

- **인스턴스는 바람둥이? 2개 서브넷에 양다리 걸치기**
  - 그림은 프라이빗 인스턴스에 퍼블릭 ENI 연결을 시도한 모습이다.
  - 같은 VPC에 생성된 서브넷이라 무난히 연결될거라 생각했지만 불가능하다.
  - 인스턴스는 같은 가용 영역에만 놓일 수 있기 때문이다.



3. 트래픽 생성의 주체 : EC2 인스턴스

- 인스턴스는 바람둥이? 2개 서브넷에 양다리 걸치기
  - 이번에는 그림처럼 같은 가용 영역이지만 다른 VPC(A와 B)에 놓인 2개 ENI를 연결해보자.
  - 인스턴스는 여러 VPC에 공존할 수 없으므로 연출이 불가능하다.

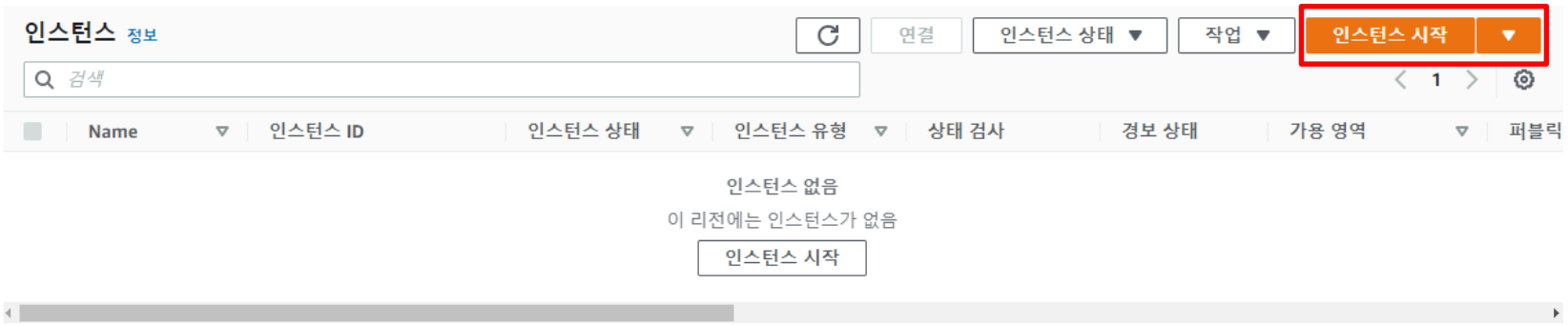


  - 정리하면 같은 VPC와 가용 영역에만 인스턴스가 놓일 수 있다.

3. 트래픽 생성의 주체 : EC2 인스턴스

실습. 인스턴스 생성 예제

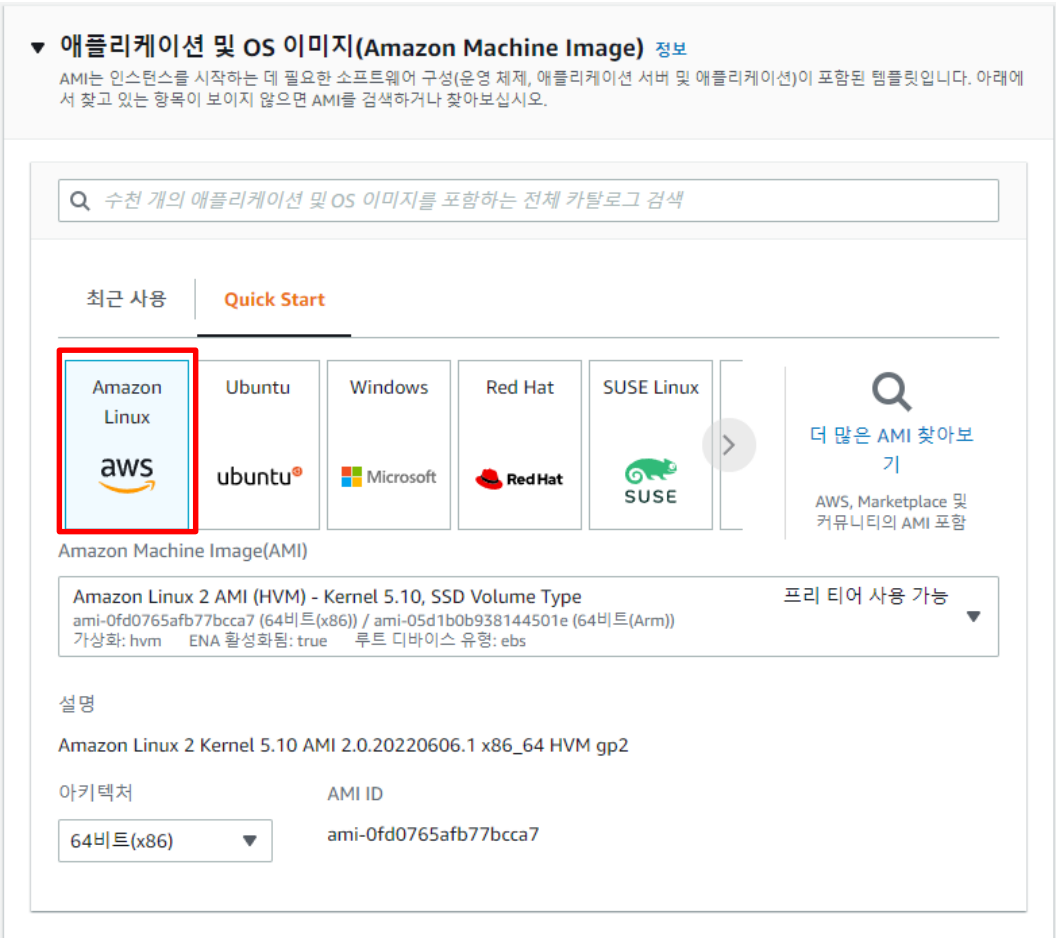
- 서비스 > EC2 > 인스턴스 메뉴로 들어가서 인스턴스 시작 버튼을 클릭한다.



3. 트래픽 생성의 주체 : EC2 인스턴스

실습. 인스턴스 생성 예제

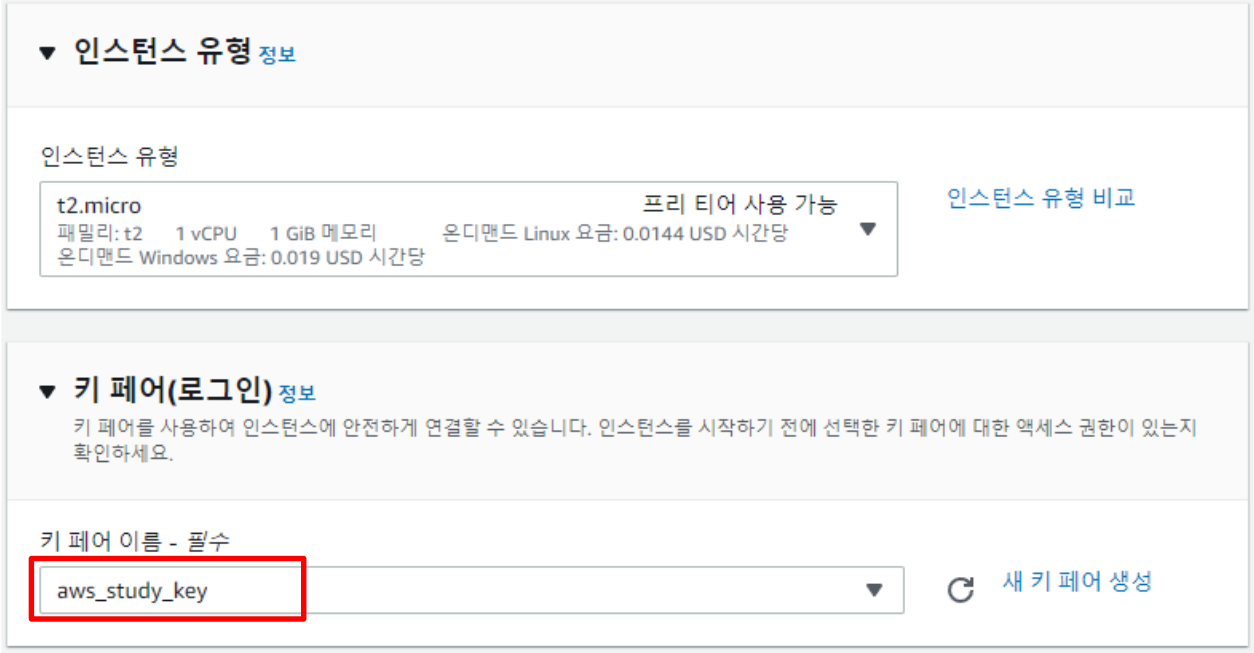
- Amazon Machine Image(AMI) 선택 메뉴에서 Amazon Linux를 선택한다.



3. 트래픽 생성의 주체 : EC2 인스턴스

실습. 인스턴스 생성 예제

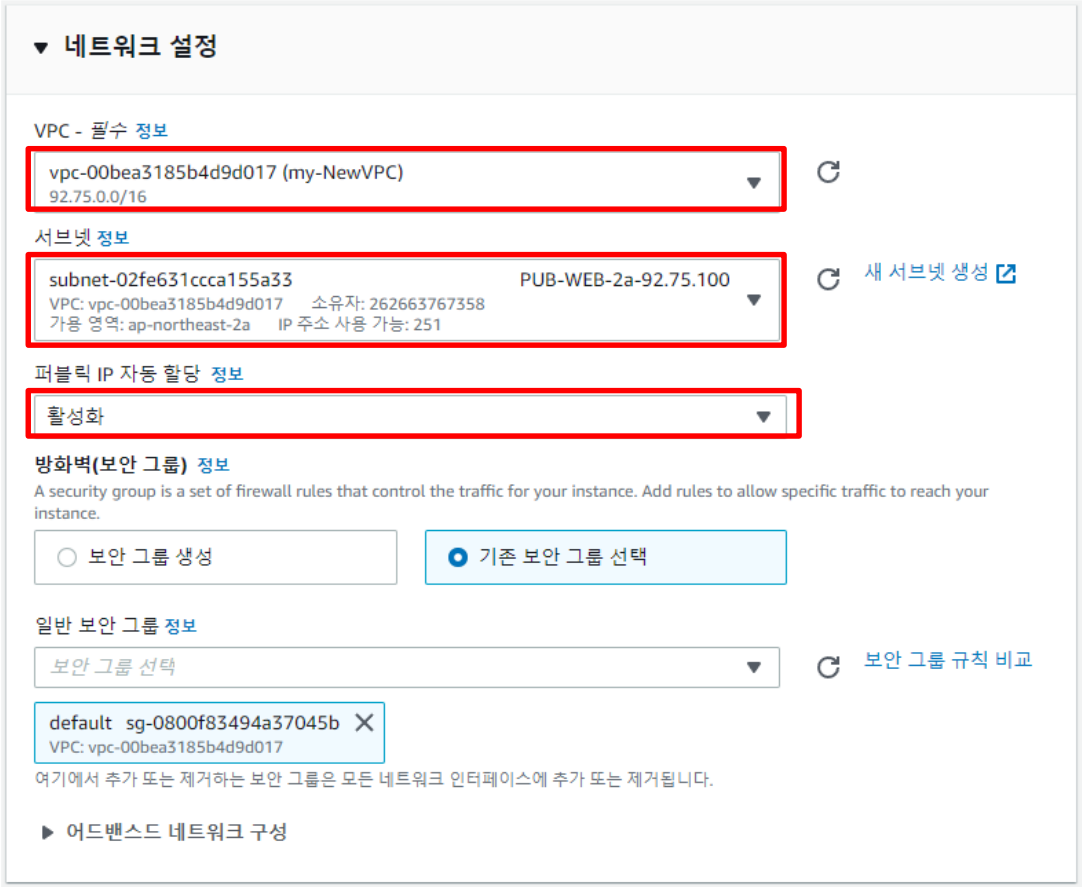
- 인스턴스 유형은 기본설정 그대로 유지한다.
- 키페어 메뉴에서는 생성된 키페어를 선택한다.



3. 트래픽 생성의 주체 : EC2 인스턴스

실습. 인스턴스 생성 예제

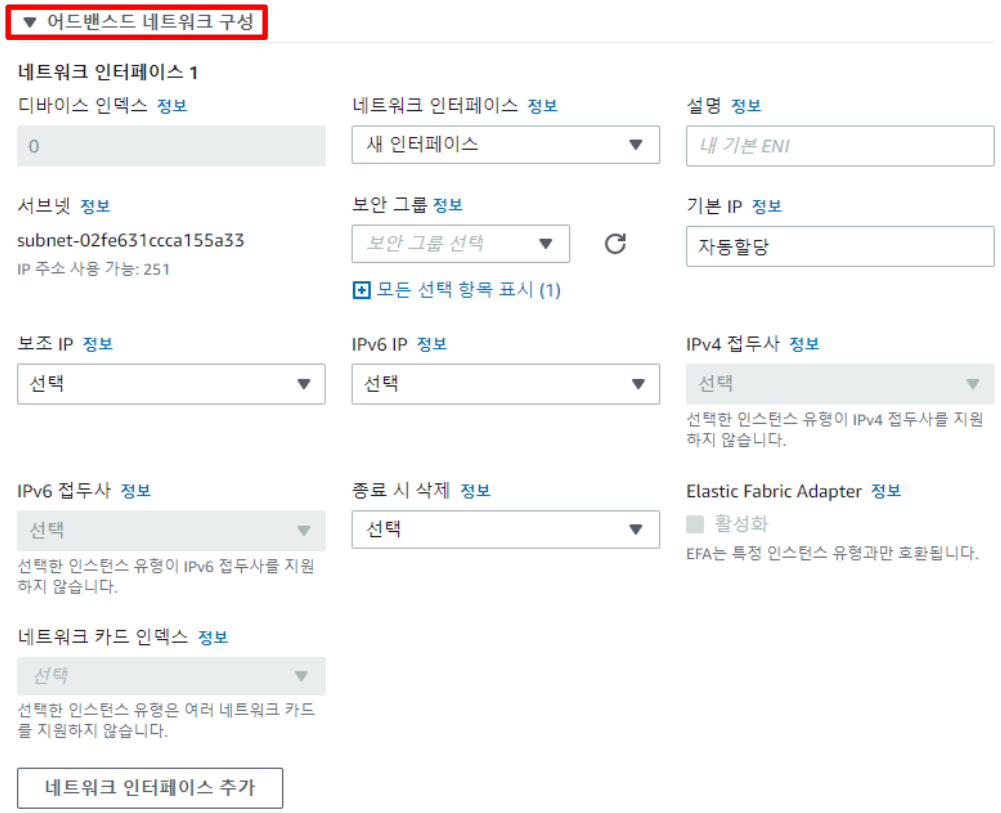
- [네트워크 설정 메뉴]에서 VPC 실습 단계에서 만든 VPC를 선택한다.
- 서브넷은 서브넷 실습 단계에서 만든 서브넷 중 하나를 선택한다.
- 그 아래 퍼블릭 IP 자동 할당은 활성화를 선택한다.



3. 트래픽 생성의 주체 : EC2 인스턴스

실습. 인스턴스 생성 예제

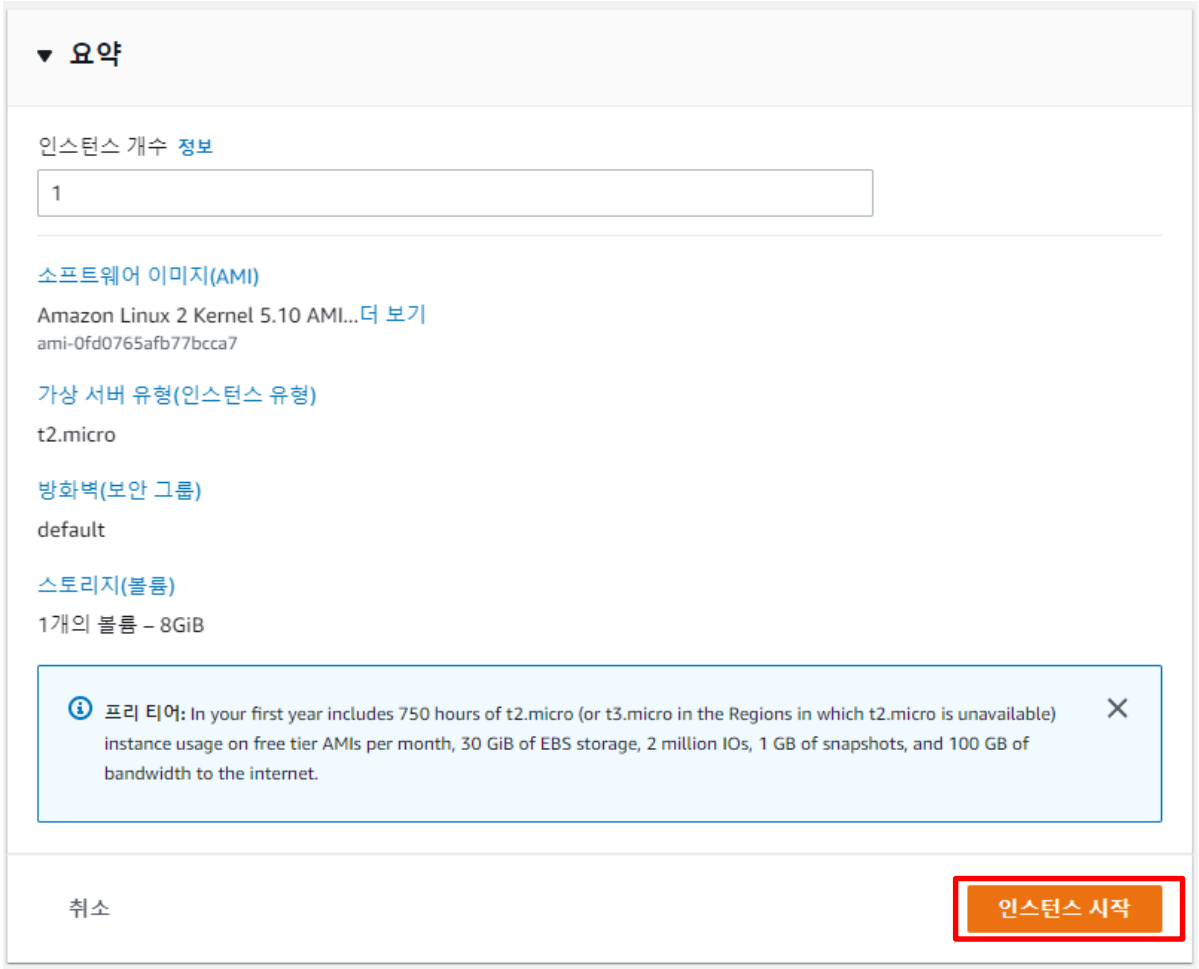
- 어드벤스드 네트워크 구성을 클릭한다.
- 인스턴스는 최소 1 개의 ENI(eth0)가 연결돼 있어야 한다.
- 기본값은 자동 할당이다.
- 이 옵션을 그대로 두면, 위에서 선택한 서브넷 범위 IP 하나를 자동으로 할당받는다.



3. 트래픽 생성의 주체 : EC2 인스턴스

실습. 인스턴스 생성 예제

- 요약 메뉴에서 인스턴스 시작 버튼을 클릭한다.



Thank You