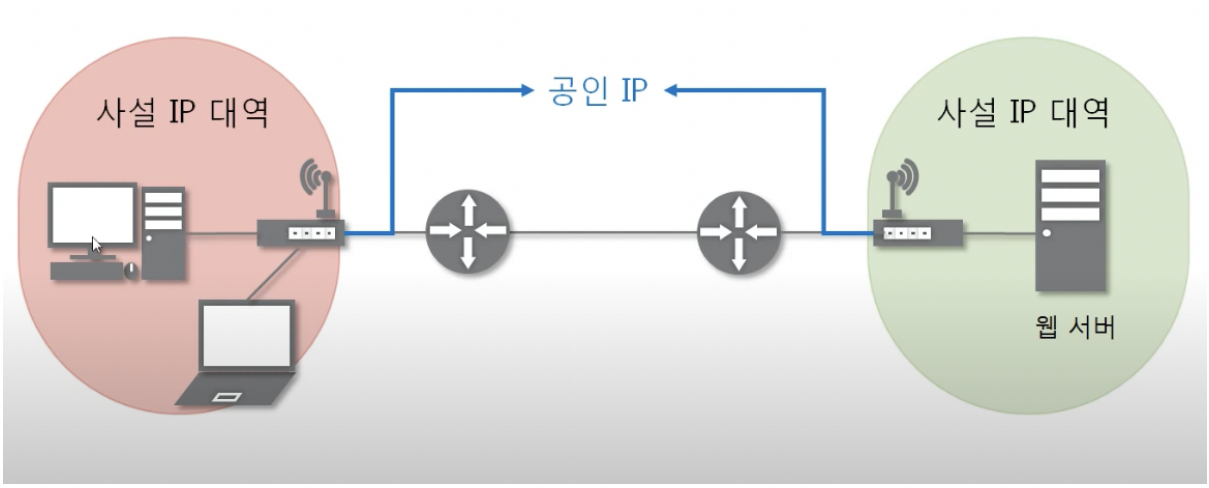
10장. NAT와 포트포워딩

담당	hong
날짜	@2022년 10월 9일
# 숫자	4

NAT (Network Address Translation; 네트워크 주소 변환)



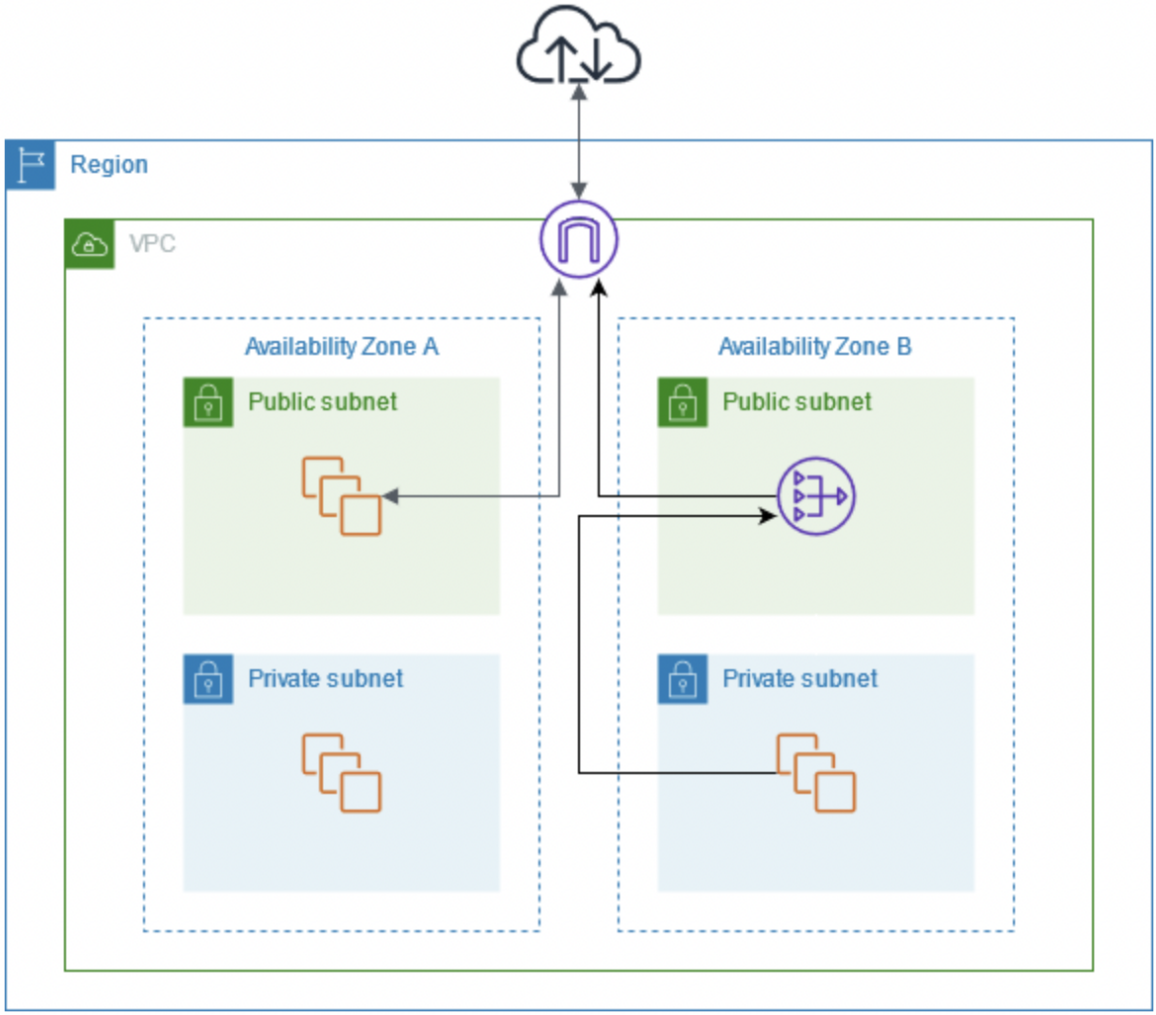
개념

- IP 패킷의 TCP/UDP 포트 숫자와 소스 및 목적지의 IP 주소를 재기록하면서 라우터를 통해 네트워크 트래픽을 주고 받는 기술.
- == 특정 IP 주소에 특정 포트 번호로 가는 패킷을, 다른 IP 주소에 다른 포트 번호로 바꾸어 주는 것.
- **사설 IP를 공인 IP 를 변환하는 것에 사용되며, 다른 곳에도 응용된다.**

목적

1. 공인 IP 주소 절약: 제한된 수의 인터넷 IPv4 주소 문제를 해결하기 위함
2. 보안 목적

NAT Gateway in AWS



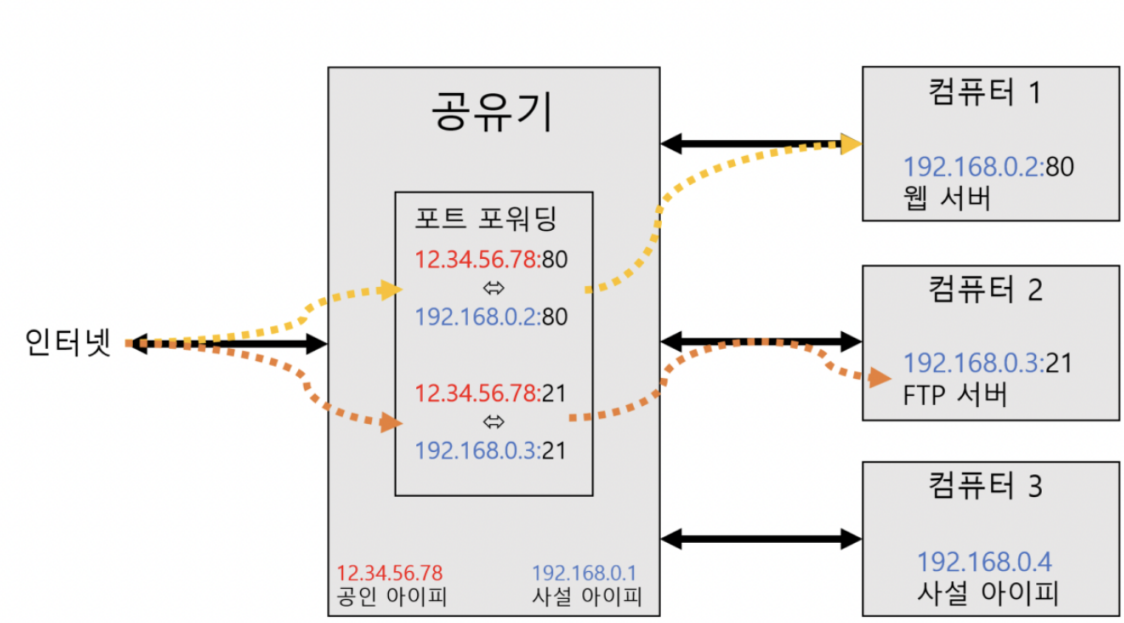
- NAT 를 처리해주는 장치
- private 서브넷의 인스턴스는, VPC 외부의 서비스에 연결할 수 있으나, 외부에서는 private 서브넷의 인스턴스와 연결할 수 없다 => NAT Gateway 를 통해 통신이 가능
- public NAT Gateway
    - 퍼블릭 서브넷에 NAT 게이트웨이를 생성하고 생성 시 탄력적 IP 주소를 NAT 게이트웨이와 연결
    - NAT 게이트웨이는 인스턴스의 소스 IP 주소를 NAT 게이트웨이의 IP 주소로 변환
- private NAT Gateway
    - 프라이빗 서브넷에 NAT 게이트웨이를 생성하고, NAT 게이트웨이에서 Transit Gateway 또는 가상 프라이빗 게이트웨이를 통해 트래픽을 라우팅
    - 탄력적 IP 주소를 프라이빗 NAT 게이트웨이에 연결할 수 없다

- https://docs.aws.amazon.com/ko_kr/vpc/latest/userguide/nat-gateway-scenarios.html

참고 2. NAT 와 Proxy Server 의 차이

구분	Proxy Server	NAT
공통점	IP 변환이 이루어짐 (목적지에서 실제 출발지 IP 를 알 수 없음)	
	내부 서버/IP 와 직접 통신하지 않음 -> 보안 강화	
OSI 계층	애플리케이션 계층에서 동작 (HTTP)	네트워크 계층에서 동작 (IP 패킷 수정)
역할	출발지 / 목적지 사이의 중개지(대리인) 역할(한 네트워크 단말기와 다른 네트워크 단말기가 직접 연결되지 않고 프록시 네트워크가 정보를 얻는 것)	사설IP -> 공인IP 로 변환해주는 역할
동작 위치	대체적으로 사내망의 DMZ 존에 존재 (DMZ: 내부/외부 네트워크 사이에 존재하는 영역)	라우터나 방화벽에서 동작
캐싱 기능	O	X
인증 기능	O	X

포트 포워딩



개념

- 특정 IP 주소와 포트 번호의 통신 요청을, 특정 다른 IP 와 포트 번호로 전달해주는(포워딩), NAT 를 응용한 기술이다.
- 게이트웨이(외부망)의 반대쪽에 위치한 사설 네트워크에 상주하는 호스트에 대한 서비스를 생성하기 위해 사용된다.
- **== 특정한 포트로 들어오는 데이터 패킷을 다른 포트로 바꿔서 다시 전송해주는 작업**
- [외부포트(호스트):내부포트] 로 표현한다.
  - ex) docker run --name my-test -p 8080:9090 ubuntu:14.04
  - == 호스트 시스템의 8080 포트로 유입되는 트래픽은 모두 도커 컨테이너의 9090 번 포트로 포워딩한다.

목적

- 가정용 네트워크와 원격 기기 사이를 직접 연결하는 경우 유용 ex) 원격 데스크톱 연결, 원격 서버 연결 등

포트 포워딩 설정 실습

-