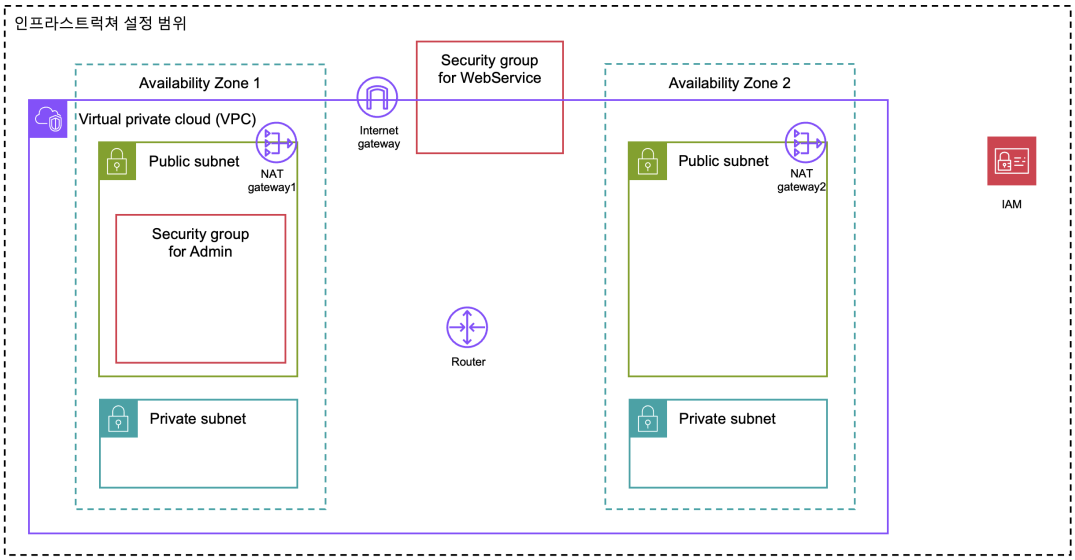
# 4장 AWS 아키텍처

Infrastructure 즉 인프라 설정 범위에 대한 AWS Architecture

2023.8.31




AWS에서 네트워크를 구축할 때 **VPC(Virtual Private Cloud)**라는 시스템을 이용할 수 있습니다. VPC는 가상의 사설망으로, 물리적인 기기를 사용하지 않고도 가상의 네트워크를 구축할 수 있습니다.

그림에서는 두 곳의 가용영역이 존재하며, 가용 영역별로 public 서브넷과 private 서브넷, NAT Gateway를 제공하고 있습니다. VPC를 설정을 할 때는 최소 2개의 가용영역을 사용해야하며, multi AZ를 사용하면 만약 어떤 가용영역에 문제가 생기더라도 다른 가용영역에서 대체할 수 있습니다. (재해복구시스템으로 사용)

public subnet은 간단하게 설명하면 외부에서 접근이 가능한 네트워크영역이고, private subnet은 외부에서 다이렉트로 접근이 불가능한 네트워크영역입니다.

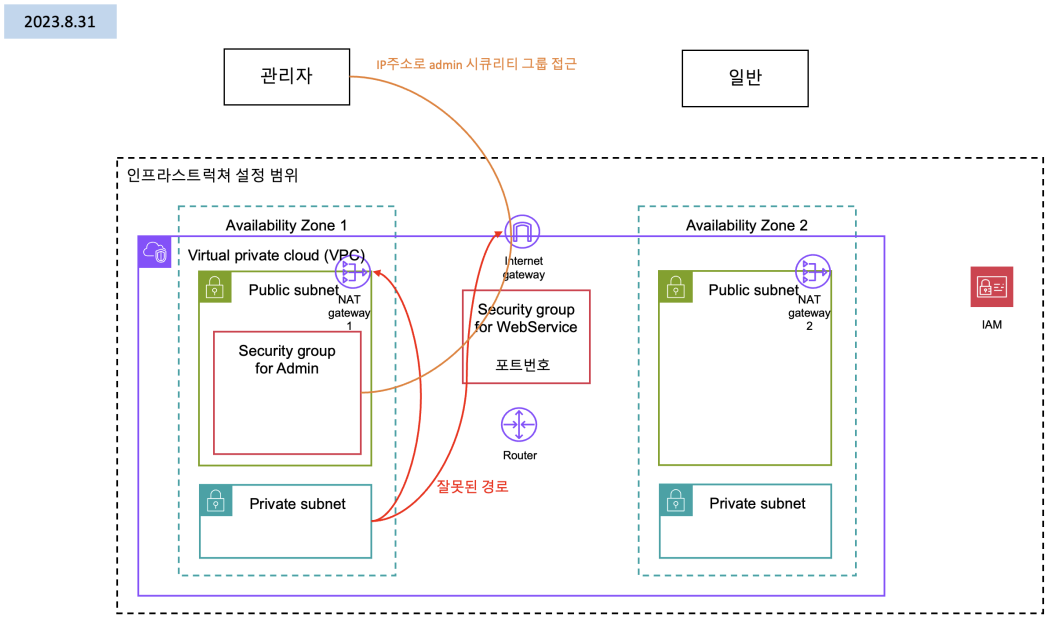
인프라 AWS 아키텍처에서는 인터넷 게이트웨이와 NAT게이트웨이가 있습니다.

**인터넷 게이트웨이**는 VPC로 생성된 네트워크와 인터넷 사이의 통신을 가능하게 하며, 인터넷 게이트웨이가 없다면 인터넷과 VPC 안의 리소스는 서로 통신할 수 없습니다.

**NAT게이트웨이**는 네트워크 주소변환 시스템인 NAT(Network Address Translation)을 구현하는 게이트웨이입니다. 프라이빗 서브넷에 생성된 리소스에 접하지 못하도록 하기 위해, NAT 게이트웨이는 퍼블릿 서브넷에 대해서 생성합니다.

서브넷과 서브넷 또는 서브넷과 각 게이트웨이가 통신할 수 있는 경로를 설정하고자 할 때 **라우팅 테이블**을 사용합니다.

해당 아키텍처에서는 2개의 보안그룹이 있는데, ‘security group for webservice’는 특정 포트 번호를 통해 외부 접근을 제어하며, ‘security group for Admin’은 IP 주소를 이용해 외부 접근을 제어합니다.




**IAM(Identity and Access Manager)는** AWS의 리소스에 대한 개별적으로 접근제어와 권한을 가지도록 계정 또는 그룹을 생성, 관리하는 서비스입니다. MFA 등과 같은 인증 시스템을 통해 보안 안정성을 높일 수 있습니다.