

02. AWS Network

[VPN\(Virtual Private Network\)](#)

[VPC\(Virtual Private Cloud\)](#)

[VPC의 구성 요소](#)

[VPC의 생성 순서](#)

[서브넷과 가용영역](#)

[서브넷과 가용 영역이란?](#)

[IPv4 CIDR 설계 방법](#)

[생성내용](#)

[서브넷 생성 순서](#)

[인터넷 게이트웨이](#)

[인터넷 게이트웨이란?](#)

[생성 내용](#)

[인터넷 게이트웨이 생성 순서](#)

[NAT 게이트웨이](#)

[NAT 게이트웨이란?](#)

[생성 내용](#)

[라우팅 테이블](#)

[라우팅 테이블이란?](#)

[생성 내용](#)

[라우팅 테이블 사용 방법](#)

[라우팅 테이블 생성 순서](#)

[보안 그룹](#)

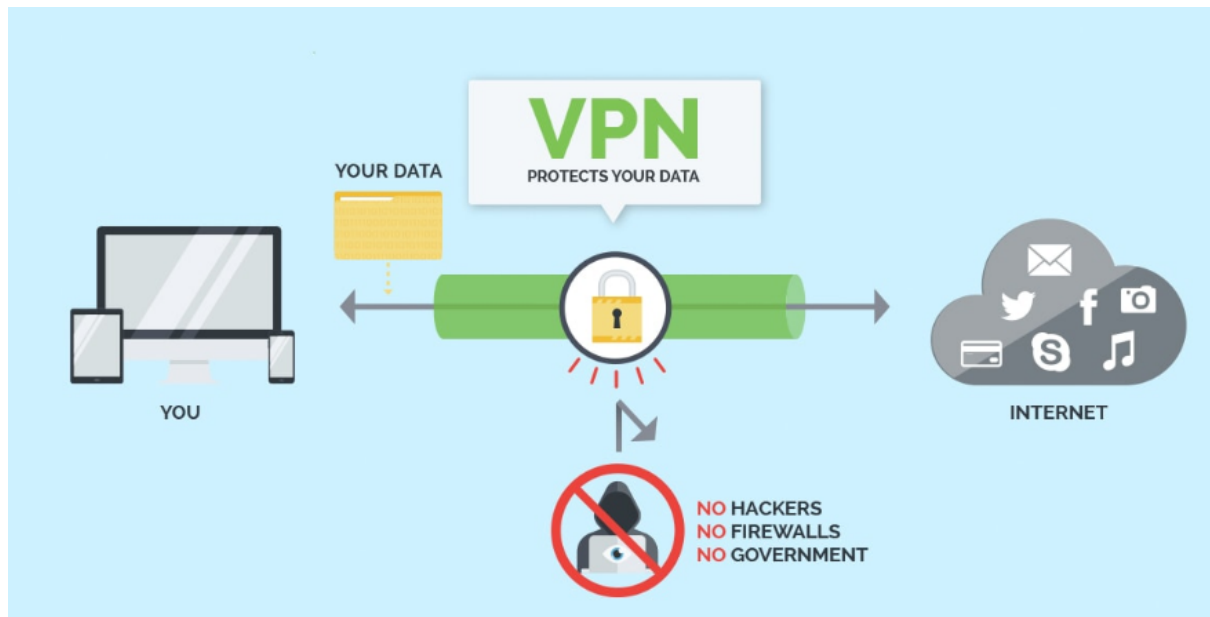
[생성 내용](#)

[생성 순서](#)

[생성 결과](#)

VPN(Virtual Private Network)

VPN은 큰 규모의 조직이 여러 곳에 분산되어 있는 컴퓨터들을 연결하는 보안성이 높은 사설 네트워크(Private Network)를 만들거나, 인터넷을 활용하여 원격지 간에 네트워크를 서로 연결하고 암호화 기술을 적용하여 보다 안정적이며, 보안성 높은 통신서비스를 제공하는 서비스이다.

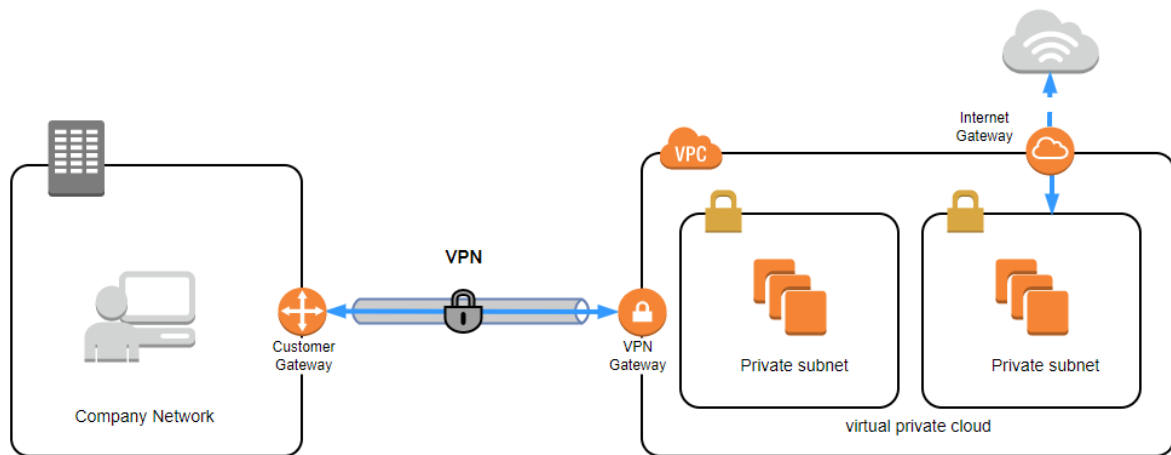


Amazon Web Service는 VPC(Virtual Private Cloud)와 VPC Gateway를 통해 On-Premise의 VPN장비와 Amazon Web Service 간의 VPN을 연결할 수 있으며, 이를 통해 보안성이 높은 하이브리드 클라우드 환경을 구현할 수 있다.

VPC(Virtual Private Cloud)

VPC는 AWS 클라우드에서 논리적으로 격리된 네트워크 공간을 할당하여 가상 네트워크에서 AWS 리소스를 이용할 수 있는 서비스를 제공한다.

Amazon VPC 자체 IP 주소 범위, 서브넷(Subnet) 생성, 라우팅 테이블(Routing Table) 및 네트워크 게이트웨이 구성 선택 등 가상 네트워킹 환경을 완벽하게 제어할 수 있으며, VPC에서 IPv4와 IPv6 모두 사용하여 리소스와 애플리케이션에 안전하고 쉽게 액세스할 수 있다.



구분	내용
서비스명	Amazon VPC(Virtual Private Cloud)
설명	직접 정의 가능한 가상 네트워크(Public Network)에서 AWS 리소스를 구동할 수 있는 논리적으로 격리된 네트워크 제공
주요 특징	- AWS에 사설 네트워크 구축 - 회사와 AWS간 VPN을 연결하거나 가상 네트워킹 구현 - 기존 데이터 센터와의 연결을 통해 하이브리드 환경 구성 - AWS를 회사 인프라의 일부처럼 사용할 수 있으며, 내부 시스템 소프트웨어의 연동이 매우 쉬움 - 세심한 네트워크 설정 가능 - 모든 리전에서 이용 가능
프리티어	VPC 자체는 비용이 발생하지 않지만, VPN 연결 시 네트워크 송/수신에 따른 종량제 비용 발생

VPC의 구성 요소

항목	값	설명
이름태그	sample-vpc	VPC를 식별하는 이름
IPv4 CIDR 블록	10.0.0.0/16	VPC에서 이용하는 프라이빗 네트워크의 IPv4 주소 범위
IPv6 CIDR 블록	IPv6 CIDR 블록 없음	VPC에서 이용하는 프라이빗 네트워크의 IPv6 주소 범위
테넌시(tenancy)	기본값	VPC 리소스의 전용 하드웨어에서의 실행 여부



IP 주소와 CIDR

IP주소는 네트워크상의 기기가 통신할 때 도착지가 되는 정보다. 비유하자면 유/무선 전화의 전화번호와 같은 것이다.

CIDR(classless-domain routing)은 IP주소를 관리하는 범위를 결정하는 방법의 하나다. 유/무선 전화의 전화번호를 시외 국번, 시내 국번, 가입자 번호로 구분해서 관리하는 것과 유사하다.

이름태그

VPC를 쉽게 식별하고자 알기 쉬운 이름을 붙인다. 이후에 자유롭게 변경할 수 있으므로 크게 고민하지 않고 이름을 붙이면 된다.

IPv4 CIDR 블록

VPC에서 사용하는 프라이빗 네트워크용 IP 주소의 범위를 지정한다. 프라이빗 네트워크에서 이용할 수 있는 IP 주소 범위는 다음 세 가지로 제공된다.

- 24비트 블록: 10.0.0.0 ~ 10.255.255.255
- 20비트 블록: 172.16.0.0 ~ 172.16.255.255
- 16비트 블록: 192.168.0.0 ~ 192.168.255.255



최대 16비트인 이유는?

24비트 블록에서 서브넷 마스크의 최대 범위를 8비트(10.0.0.0/8)로 설정한 경우, 10.0.0.0 ~ 10.255.255.255라는 최대 16,777,216개의 주소를 이용할 수 있다. 하지만 VPC에서 할당되는 서브넷 마스크는 16비트(10.0.0.0/16) 이하로만 해야 한다는 제한이 있다. 따라서 예를 들어 하나의 VPC 내부에서는 10.0.0.0 ~ 10.0.255.255와 같이 65,536개의 IP주소만 이용할 수 있다. 이것이 '최대 16비트'인 이유다.

IPv6 CIDR 블록

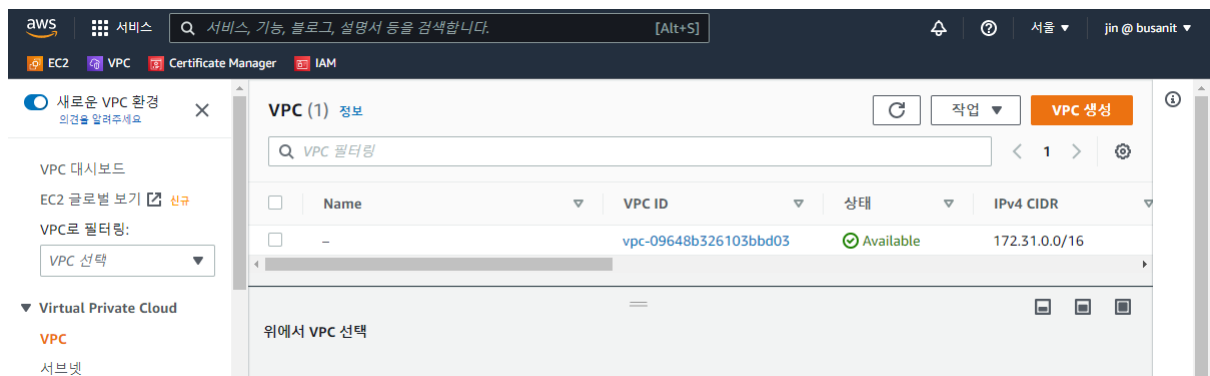
VPC에서 IPv6의 이용 여부를 지정한다. 특별한 의도가 없는 한 '없음'을 선택한다.


테넌시

VPC상의 리소스를 전용 하드웨어에서 실행할 때 지정한다. '기본'으로 설정하면 다른 AWS 계정과 하드웨어 리소스를 공유하도록 선택하는 것과 같다. 일반적인 이용일 때는 크게 문제가 없지만, 신뢰성이 매우 중요한 시스템의 경우에는 '전용'으로 설정하는 것을 검토해도 좋다. '전용'으로 설정하면 별도 비용이 추가된다.

VPC의 생성 순서

[서비스] - [VPC 대시보드] - [VPC] - [VPC 생성]



 Name이 '-' 인 VPC는 기본 VPC다. 기본 VPC는 2013년 12월 4일 이후에 AWS 계정을 계약한 경우, 모든 AWS 리전에서 제공된다. 기본 VPC는 블로그나 간단한 웹사이트를 즉시 만들고자 하는 이용자의 요구를 만족하려는 것으로 미리 간략한 설정을 마친 VPC이다. 특별히 비용이 들지 않으므로 그대로 남겨두어도 되지만, 불필요한 리소스에 신경이 쓰인다면 삭제해도 좋다.

aws
서비스
서비스, 기능, 블로그, 설명서 등을 검색합니다.
[Alt+S]

EC2
VPC
Certificate Manager
IAM

VPC > VPC > VPC 생성

VPC 생성

정보

VPC는 AWS 클라우드의 격리된 부분으로서, Amazon EC2 인스턴스와 같은 AWS 객체로 채워집니다.

VPC 설정

생성할 리소스 정보

VPC 리소스 또는 VPC 및 기타 네트워킹 리소스만 생성합니다.

☒ VPC만
☐ VPC 등

이름 태그 - 선택 사항

'Name' 키와 사용자가 지정하는 값을 포함하는 태그를 생성합니다.

sample-vpc

IPv4 CIDR 블록 정보

☒ IPv4 CIDR 수동 입력
☐ IPAM 할당 IPv4 CIDR 블록

IPv4 CIDR

10.0.0.0/16

IPv6 CIDR 블록 정보

☒ IPv6 CIDR 블록 없음
☐ IPAM 할당 IPv6 CIDR 블록
☐ Amazon 제공 IPv6 CIDR 블록
☐ 내가 소유한 IPv6 CIDR

테넌시 정보

기본값

태그

태그는 AWS 리소스에 할당하는 레이블입니다. 각 태그는 키와 선택적 값으로 구성됩니다. 태그를 사용하여 리소스를 검색 및 필터링하거나 AWS 비용을 추적할 수 있습니다.

키

Q Name

X

값 - 선택 사항

Q sample-vpc

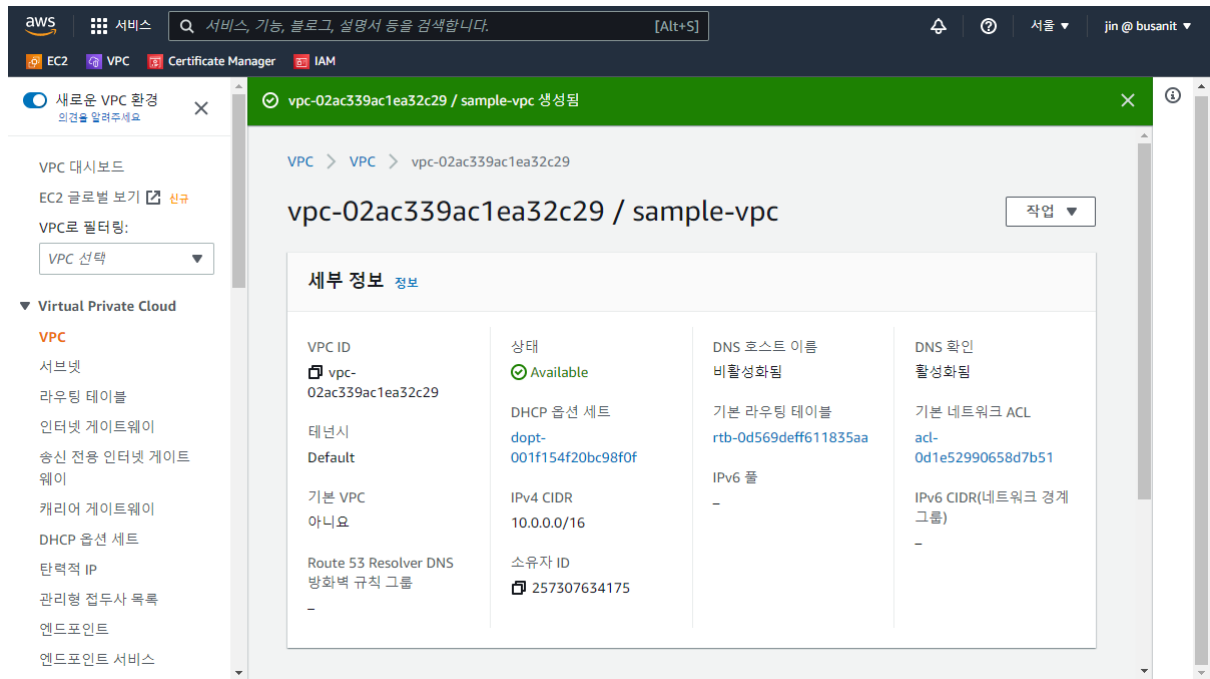
X

제거

새 태그 추가

49을(를) 태그.개 더 추가할 수 있습니다.

취소
VPC 생성



리소스 이름 규칙

다양한 리소스에 이름을 붙여야 하므로 이름 규칙을 만들어두면 고민을 줄일 수 있다.

시스템 이름-리소스 이름-(-리소스 식별자)

예: sample-vpc, sample-ec2-web01, sample-elb

서브넷과 가용영역

서브넷과 가용 영역이란?

VPC 안에는 하나 이상의 서브넷을 만들어야 한다. 서브넷은 VPC의 IP 주소 범위를 나누는 단위다. IP주소 범위를 나누는 대표적인 이유는 다음 두 가지다.

- 역할 분리: 외부에 공개하는 리소스 여부를 구별
- 기기 분리: AWS 안에서의 물리적인 이중화(다중화)를 수행

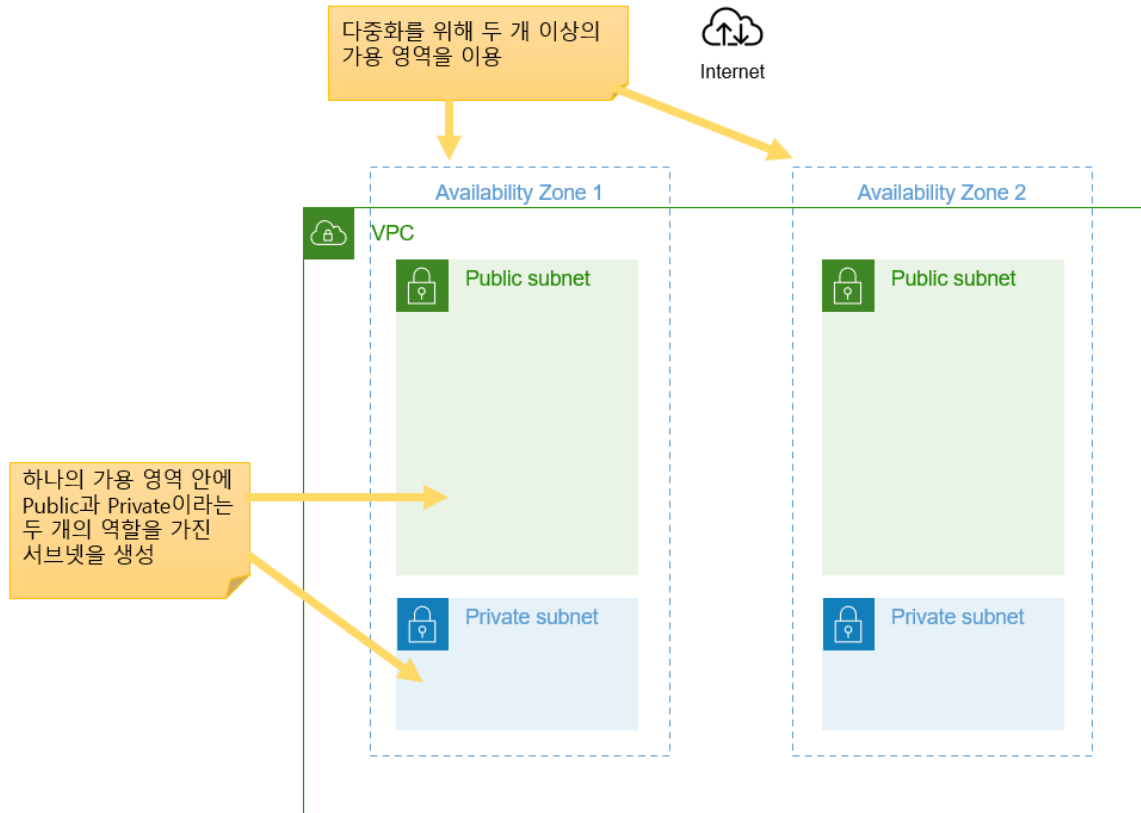
역할 분리

리소스가 담당하는 역할에 따라 분리한다. 시스템을 구축할 때는 다양한 리소스를 조합하게 된다. 예를 들어 리소스의 하나인 로드 밸런서는 외부 공개가 목적이므로 외부에서 접근할 수 있어야 한다. 반대로 DB 서버는 VPC 내부 서버에서의 사용을 전제로 하므로 외부에 공개되어서는 안된다. 이런 규칙을 리소스마다 개별적으로 할당하지 않고, 리소스가 포함된 그룹 전체에 대해 할당하면 설정 누락 등을 피할 수 있다.

기기 분리

내결합성을 높이기 위해 기기를 분리한다. 내결합성이란 하드웨어 고장 등 예측할 수 없는 사태가 발생했을 때 시스템 자체를 사용하지 못하게 되는 것을 방지하는 능력이다. 클라우드라 하더라도 최종적으로는 어딘가 위치한 물리적인 기기상에서 작동한다. 예를 들어 서브넷이 여럿 존재하더라도, 그 서브넷이 같은 기기에 대한 것이라면 기기에 고장이 발생했을 때 동시에 서브넷 안의 리소스를 이용할 수 없게 된다.

VPC에는 가용 영역(각 리전 안의 여러 독립된 위치)이라는 개념이 존재한다. 가용 영역이 다르면 독립되었음을 보장할 수 있으므로, 가용 영역별로 서브넷을 제공하면 여러 서브넷을 동시에 이용하지 못하는 가능성을 낮출 수 있다.



IPv4 CIDR 설계 방법

서브넷을 한번 만들면 해당 서브넷이 이용하는 CIDR 블록은 변경할 수 없다. 따라서 처음부터 확실하게 CIDR을 설계해야 한다. 설계할 때는 다음 두 가지 항목을 고려한다.

- 생성할 서브넷의 수
- 서브넷 안에 생성할 리소스 수

서브넷의 CIDR 블록	서브넷 수	리소스 수
<p>VPC 16비트 서브넷 8비트 리소스 8비트</p>	256	251
<p>VPC 16비트 서브넷 4비트 리소스 12비트</p>	16	4091
<p>VPC 16비트 서브넷 2비트 리소스 14비트</p>	4	16379

리소스 수는 이론적인 최댓값에서 AWS가 예약한 5개를 뺀 값이다.

일반적으로는 서브넷 수와 리소스 수 각각에 여유를 두고 설정하는 것이 좋다.

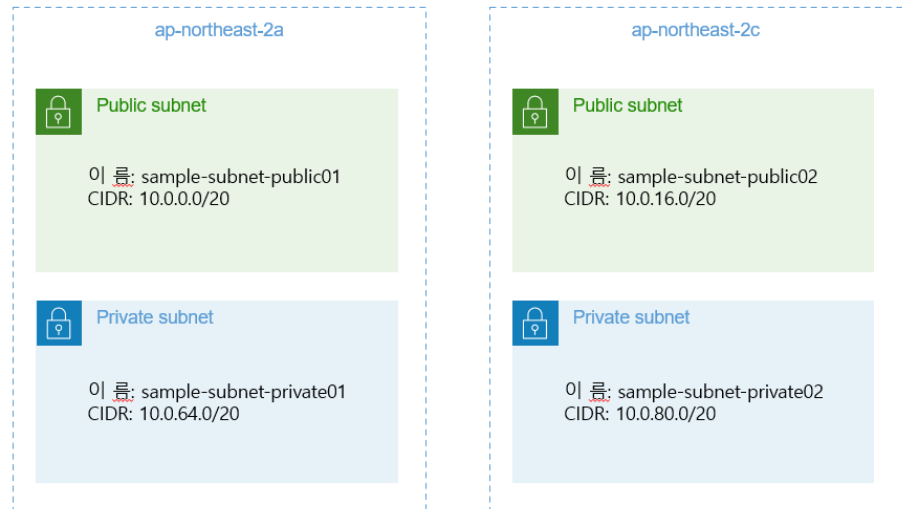
서브넷	CIDR 블록
public01	00001010.00000000.0000XXXX.XXXXXXXX (10.0.0.0/20)
public02	00001010.00000000.0001XXXX.XXXXXXXX (10.0.16.0/20)
private01	00001010.00000000.0100XXXX.XXXXXXXX (10.0.64.0/20)
private02	00001010.00000000.0101XXXX.XXXXXXXX (10.0.80.0/20)

서브넷은 최대 16개를 만들 수 있으며 여기에서는 그 중 4개를 이용한다. 서브넷 안에는 4,091개의 리소스를 생성할 수 있으므로 일반적인 상황에서 이용하기에는 충분한 범위다.

생성내용

공개용 외부 서브넷

비공개용 내부 서브넷



대상	항목	값	설명
외부 서브넷 1	VPC ID	VPC의 ID	서브넷을 생성할 VPC
	서브넷 이름	sample-subnet-public01	서브넷별 이름
	가용 영역	ap-northeast-2a	제공되는 가용 영역
	IPv4 CIDR 블록	10.0.0.0/20	VPC의 IP 범위에 포함되는 범위
외부 서브넷 2	VPC ID	VPC의 ID	-
	서브넷 이름	sample-subnet-public02	
	가용 영역	ap-northeast-2c	
	IPv4 CIDR 블록	10.0.16.0/20	
내부 서브넷 1	VPC ID	VPC의 ID	-
	서브넷 이름	sample-subnet-private01	
	가용 영역	ap-northeast-2a	
	IPv4 CIDR 블록	10.0.64.0/20	
내부 서브넷 2	VPC ID	VPC의 ID	-
	서브넷 이름	sample-subnet-private02	
	가용 영역	ap-northeast-2c	
	IPv4 CIDR 블록	10.0.80.0/20	

서브넷 생성 순서

aws
서비스
서비스, 기능, 블로그, 설명서 등을 검색합니다.
[Alt+S]
서울

EC2
VPC
Certificate Manager
IAM

VPC > 서브넷 > 서브넷 생성

서브넷 생성 정보

VPC

VPC ID
이 VPC에 서브넷을 생성합니다.

vpc-02ac339ac1ea32c29 (sample-vpc) ▼

연결된 VPC CIDR

IPv4 CIDR
10.0.0.0/16

서브넷 설정

서브넷의 CIDR 블록 및 가용 영역을 지정합니다.

1/1개 서브넷

서브넷 이름
'Name' 키와 사용자가 지정하는 값을 포함하는 태그를 생성합니다.

sample-subnet-public01

이름은 최대 256자까지 입력할 수 있습니다.

가용 영역 정보
서브넷이 상주할 영역을 선택합니다. 선택하지 않으면 Amazon이 자동으로 선택합니다.

아시아 태평양 (서울) / ap-northeast-2a ▼

IPv4 CIDR 블록 정보

▼ 태그 - 선택 사항

키

✕

값 - 선택 사항

✕

제거

새 태그 추가

49을(를) 태그.개 더 추가할 수 있습니다.

제거

새 서브넷 추가

취소

서브넷 생성

AWS

서비스

서비스, 기능, 블로그, 설명서 등을 검색합니다.

[Alt+S]

EC2

VPC

Certificate Manager

IAM

새로운 VPC 환경

외연을 알려주세요

VPC 대시보드

EC2 글로벌 보기

VPC로 필터링:

VPC 선택

Virtual Private Cloud

VPC

서브넷

서브넷 1개를 성공적으로 생성하였습니다. subnet-0010a1bb33dbcc2c7

서브넷 (8) 정보

작업

서브넷 생성

서브넷 필터링

1

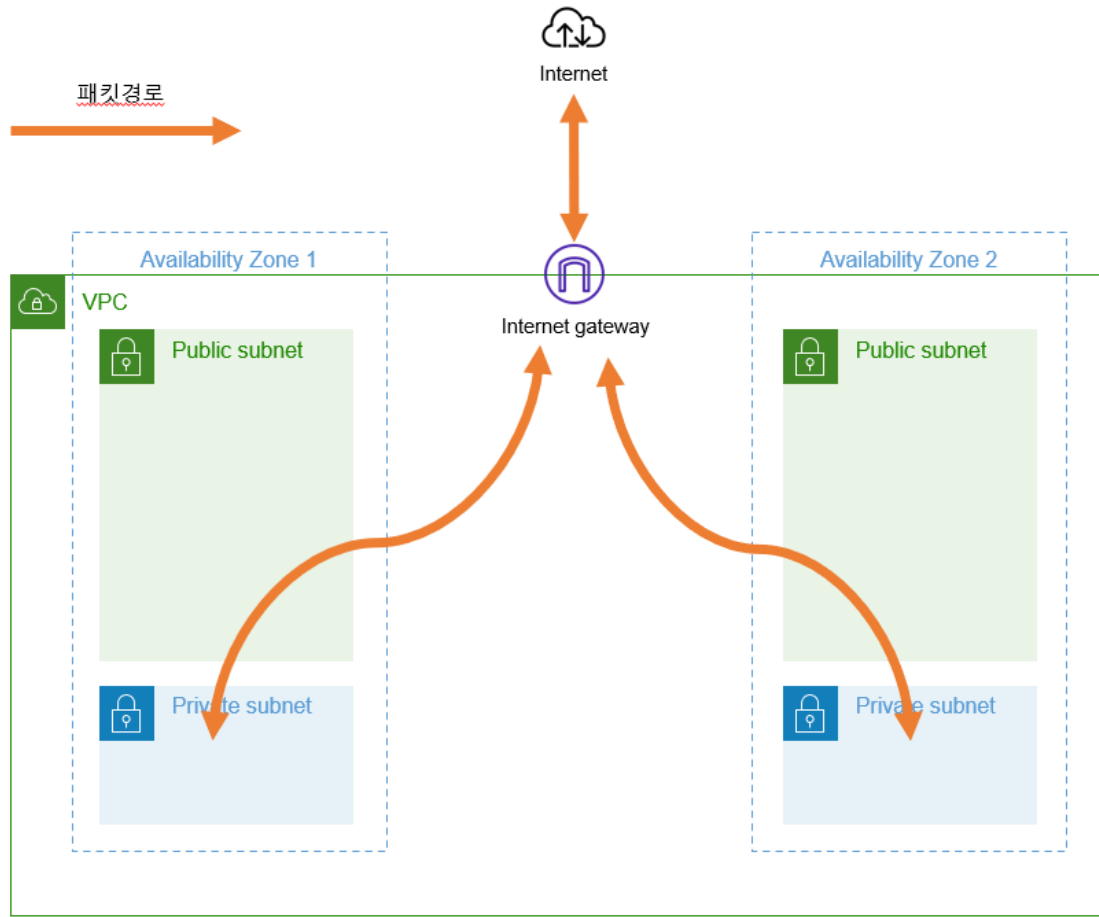
	Name	서브넷 ID	상태	VPC	IPv4 CIDR
<input type="checkbox"/>	sample-subnet-public02	subnet-0d510193a0aa74e46	Available	vpc-02ac339ac1ea32c29 sam...	10.0.16.0/20
<input type="checkbox"/>	sample-subnet-public01	subnet-0de6fa9a5fae4dfd1	Available	vpc-02ac339ac1ea32c29 sam...	10.0.0.0/20
<input type="checkbox"/>	sample-subnet-private02	subnet-0010a1bb33dbcc2c7	Available	vpc-02ac339ac1ea32c29 sam...	10.0.80.0/20
<input type="checkbox"/>	sample-subnet-private01	subnet-07ece67a7679c85bb	Available	vpc-02ac339ac1ea32c29 sam...	10.0.64.0/20

인터넷 게이트웨이

인터넷 게이트웨이란?

인터넷 게이트웨이란 VPC에서 생성된 네트워크와 인터넷 사이의 통신을 가능하게 하는 것이다.

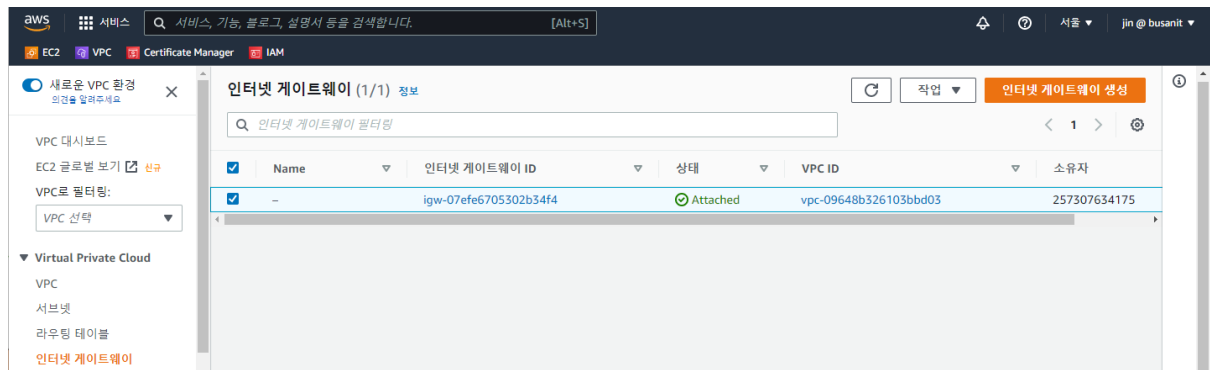
인터넷 게이트웨이가 없으면 VPC 안의 리소스는 서로 통신할 수 없다.



생성 내용

항목	값	설명
이름 태그	sample-igw	인터넷 게이트웨이에 붙이는 이름
VPC	sample-vpc	인터넷 게이트웨이와 연결할 VPC

인터넷 게이트웨이 생성 순서



VPC > 인터넷 게이트웨이 > 인터넷 게이트웨이 생성

인터넷 게이트웨이 생성 정보

인터넷 게이트웨이는 VPC를 인터넷과 연결하는 가상 라우터입니다. 새 인터넷 게이트웨이를 생성하려면 아래에서 게이트웨이 이름을 지정해야 합니다.

인터넷 게이트웨이 설정

이름 태그

'Name' 키와 사용자가 지정하는 값을 포함하는 태그를 생성합니다.

sample-igw

태그 - 선택 사항

태그는 AWS 리소스에 할당하는 레이블입니다. 각 태그는 키와 선택적 값으로 구성됩니다. 태그를 사용하여 리소스를 검색 및 필터링하거나 AWS 비용을 추적할 수 있습니다.

키

Q Name X

값 - 선택 사항

Q sample-igw X

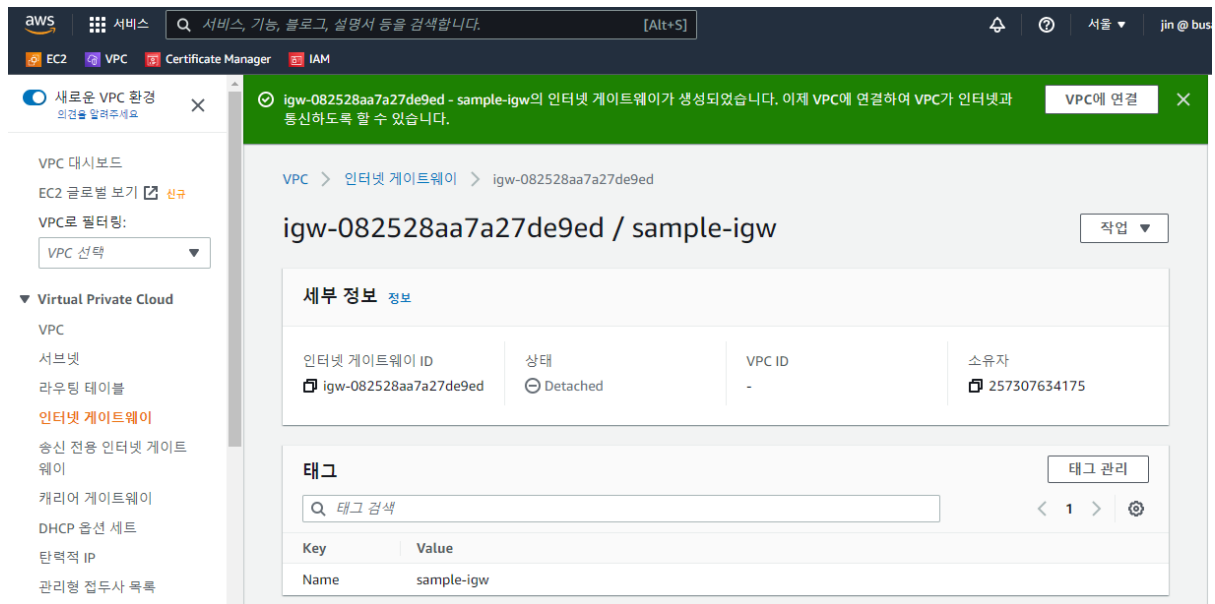
제거

새 태그 추가

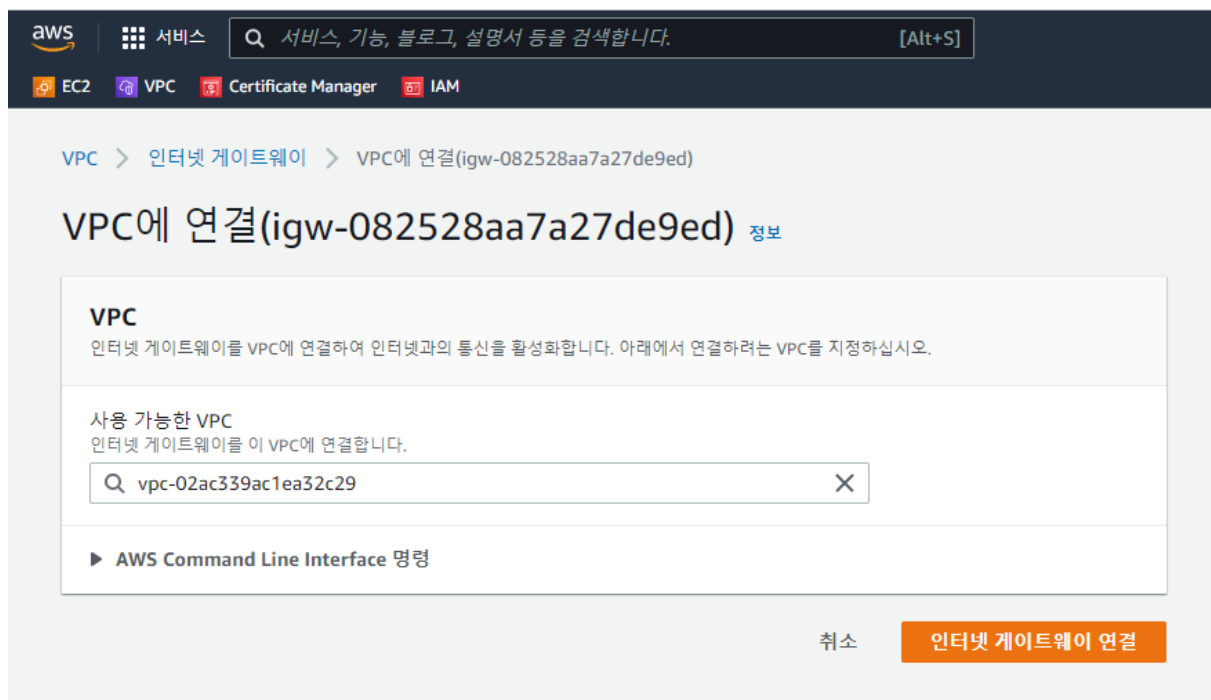
49글(을) 태그.개 더 추가할 수 있습니다.

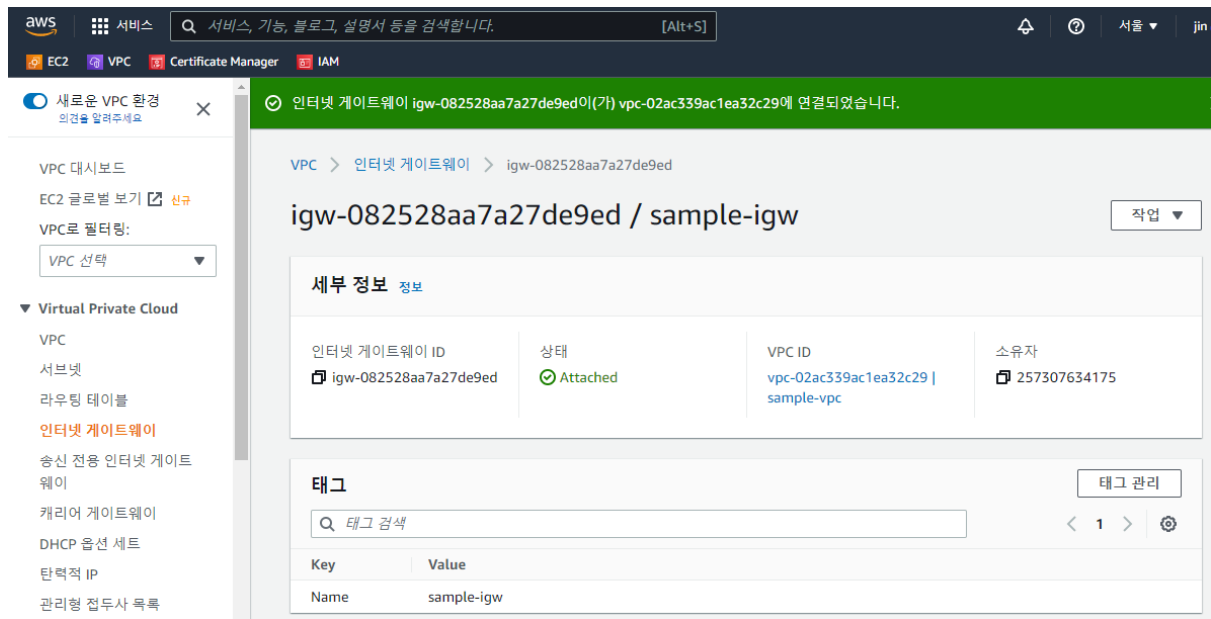
취소

인터넷 게이트웨이 생성



VPC에 연결



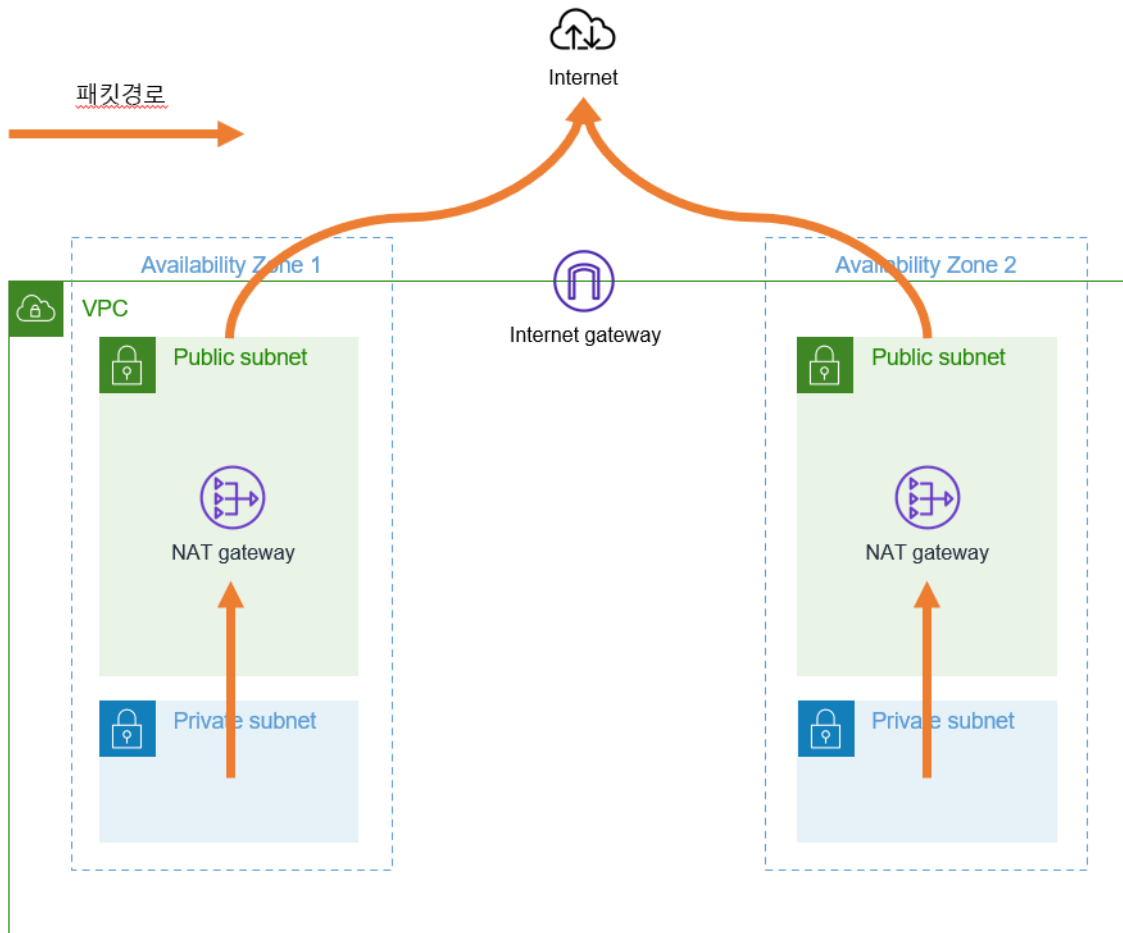


NAT 게이트웨이

NAT 게이트웨이란?

인터넷 게이트웨이의 역할은 'VPC에서 생성된 네트워크와 인터넷 사이의 통신을 수행하는 것'이다. 이때 VPC에서 생성된 네트워크 안에 만들어진 리소스는 외부 네트워크와 직접 통신하므로 공개 IP를 가져야 한다. 하지만 공개 IP를 가진다는 것은 인터넷에 직접 공개된다는 의미이므로, 애써 서버넷을 퍼블릭(공개)과 프라이빗(비공개)으로 구분한 의미가 사라진다.

NAT 게이트웨이는 퍼블릭 서버넷에 대해 생성한다. 이중성을 확보하려면 여러 NAT 게이트웨이를 생성하는 것이 좋다. 게이트웨이마다 각각 비용이 들기 때문에 하나의 NAT 게이트웨이만 제공해 운용하기도 한다.



탄력적 IP

AWS에서는 리소스에 공개 IP를 직접 할당할 수 없다. 대신 AWS에서는 공개 IP를 관리하는 탄력적 IP(Elastic IP) 기능을 제공한다. AWS에서 탄력적 IP를 생성하면 AWS로부터 공개 IP가 할당된다. 이 탄력적 IP를 리소스에 할당해서 리소스가 간접적으로 공개 IP를 갖도록 할 수 있다.

생성 내용

대상	항목	값	설명
NAT 게이트웨이 1	이름	sample-ngw-01	NAT 게이트웨이 이름
	<u>서브넷</u>	sample-subnet-public01	NAT 게이트웨이를 생성할 <u>서브넷</u>
	탄력적 IP할당 ID	(자동생성)	NAT 게이트웨이에 할당할 탄력적 IP
NAT 게이트웨이 2	이름	sample-ngw-02	-
	<u>서브넷</u>	sample-subnet-public02	
	탄력적 IP할당 ID	(자동생성)	

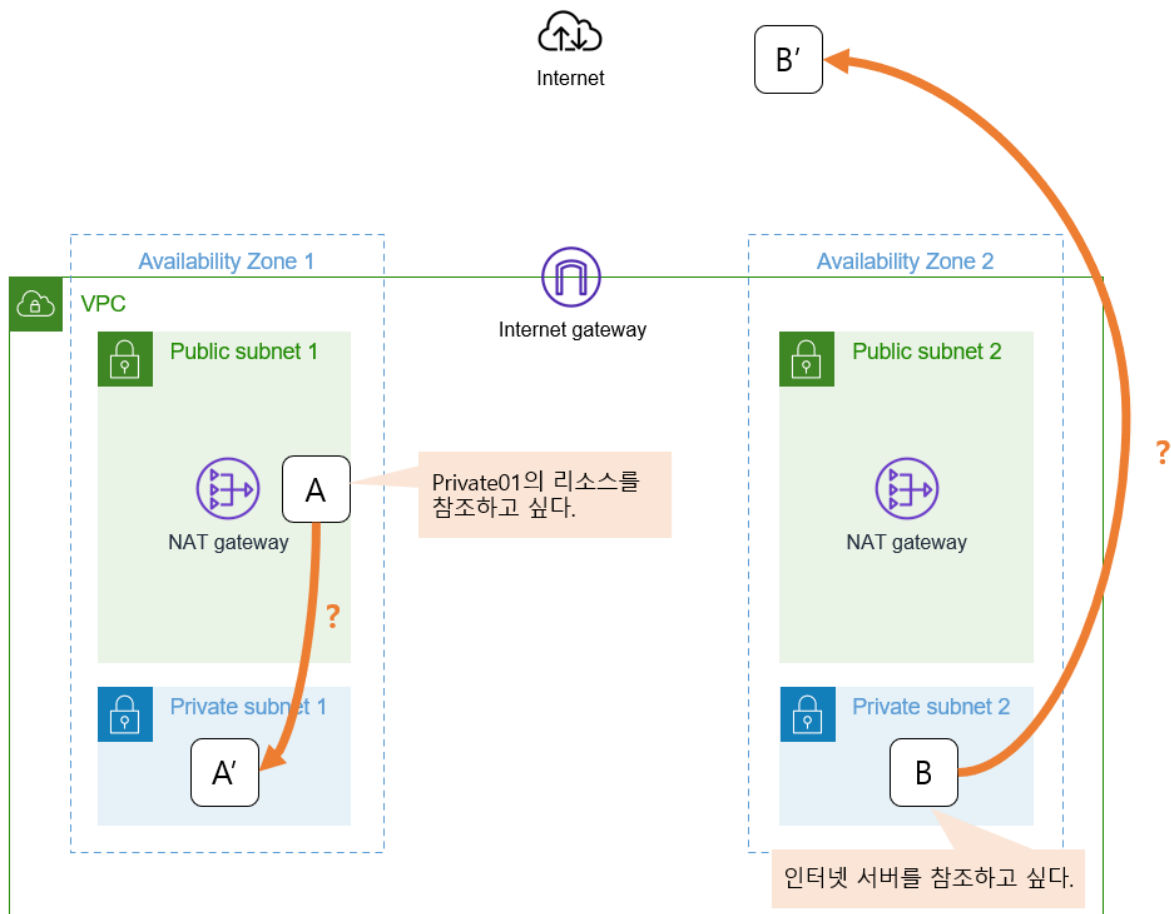


자동 생성한 탄력적 IP는 NAT 게이트웨이 생성을 중단하거나, 생성 후에 NAT 게이트웨이를 삭제해도 그대로 남아있다. 남은 탄력적 IP는 이용하지 않더라도 이 용료가 부과된다. NAT 게이트웨이를 삭제했을 때는 자동 생성된 탄력적 IP도 함께 삭제해야 한다.

라우팅 테이블

라우팅 테이블이란?

VPC상에 서브넷을 생성하고 리소스를 생성할 장소를 준비했다. 그리고 인터넷 게이트웨이와 NAT게이트웨이를 생성해 리소스가 인터넷과 통신할 수 있도록 출입구를 만들었다. 하지만 이 상태에서는 서브넷과 서브넷, 또는 서브넷과 각 게이트웨이가 통신할 수 있는 경로가 아직 존재하지 않는다. 따라서 어떤 서브넷 안의 리소스가 해당 서브넷 밖의 리소스에는 접근할 수 없다.



서브넷 사이의 통신 경로를 설정하고자 AWS에서는 라우팅 테이블 기능을 제공한다. 라우팅 테이블에는 '이 서버에 접속할 때는 이 곳을 경유한다'라는 규칙을 다음과 같은 테이블 형식으로 설정할 수 있다.

라우팅 테이블이 가진 정보(테이블 이미지)

속한 서브넷	Public Subnet 1, Public Subnet 2	
송신 대상지	타겟	용도
10.0.0.0/16	Local	VPC 안의 다른 리소스
0.0.0.0/0	Internet Gateway	기타 모든 통신 대상지

- 송신 대상지: 접속 대상 위치에 관한 정보다. 송신 대상지는 IP 주소를 지정한다. IP 주소는 특정 값을 지정하거나 CIDR 형식을 이용해 범위로 지정할 수 있다.
- 타깃: 경유지에 관한 정보다. 라우팅 테이블에 지정할 수 있는 타깃은 몇 가지가 있다.

라우팅 테이블의 대표적인 타깃

타깃	용도
로컬	동일 VPC 안의 리소스에 접근
인터넷 게이트웨이	퍼블릭 서브넷에 생성된 리소스가 인터넷 서버와 통신
NAT 게이트웨이	<u>프라이빗</u> 서브넷에 생성된 리소스가 인터넷 서버와 통신
VPN 게이트웨이	VPN을 통해 접속된 독자 네트워크상의 서버와 통신
VPC <u>피어링</u>	접속을 허가한 다른 VPC상의 리소스와 통신

실습에 필요한 라우팅 테이블 구조

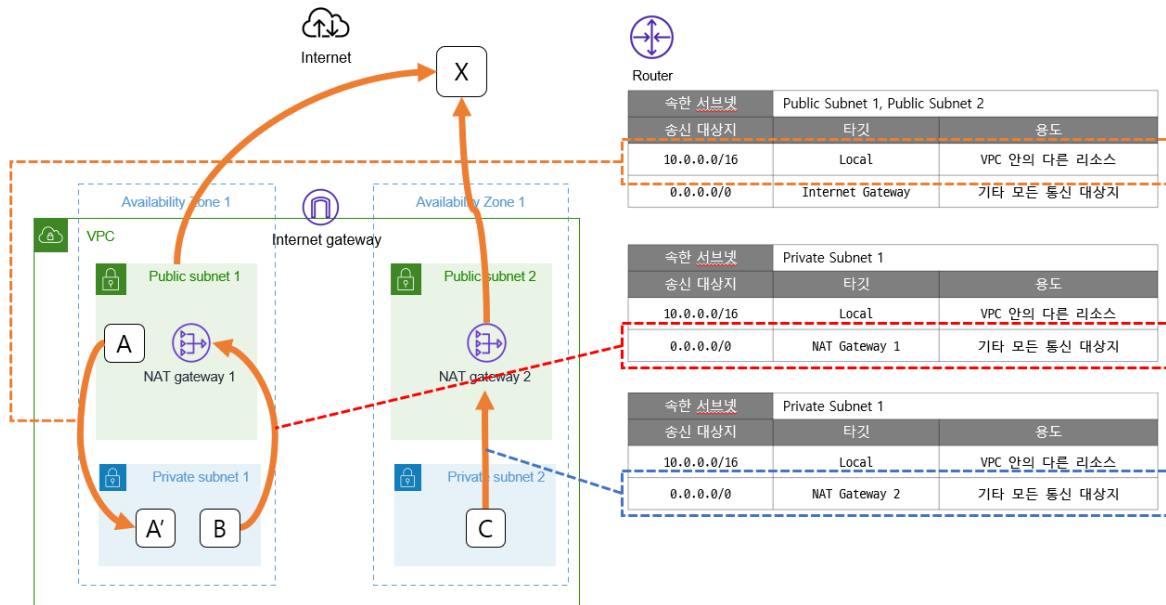
- 퍼블릭 라우팅 테이블: 퍼블릭 서브넷 1, 2 공용
- 프라이빗 라우팅 테이블 1: 프라이빗 서브넷 1용
- 프라이빗 라우팅 테이블 2: 프라이빗 서브넷 2용

생성 내용

대상	항목	값	
퍼블릭 서브넷용 (공용)	이름 태그	sample-rt-public	
		서브 카테고리	대상
		라우팅	로컬
			외부
		서브넷	퍼블릭 서브넷
			서브넷 ID
프라이빗 서브넷 1용	이름 태그	sample-rt-private01	
		서브 카테고리	대상
		라우팅	로컬
			외부
		서브넷	퍼블릭 서브넷
			서브넷 ID
프라이빗 서브넷 2용	이름 태그	sample-rt-private02	
		서브 카테고리	대상
		라우팅	로컬
			외부
		서브넷	퍼블릭 서브넷
			서브넷 ID

라우팅 테이블 사용 방법

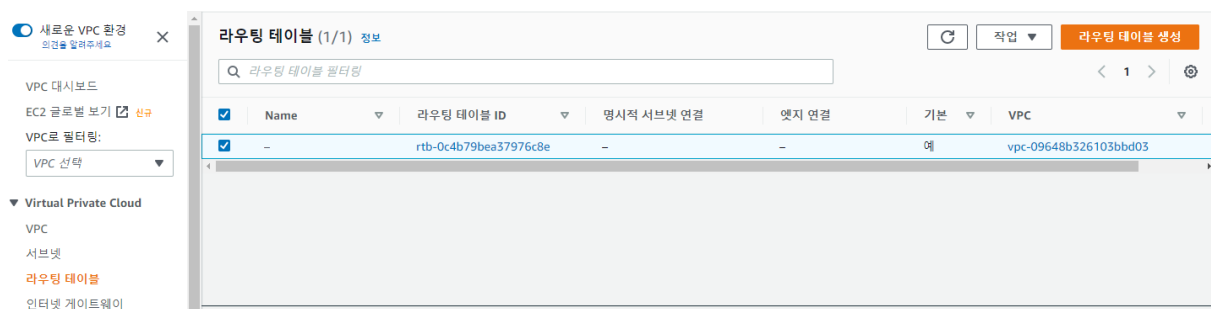
통신 내용	설명
A -> A'로 통신	리소스 A는 Public Subnet 1에 있으므로 퍼블릭 서브넷 공용 라우팅 테이블을 이용한다. 리소스 A'는 VPC 안에 있으므로 Local 타겟으로 접근한다.
B -> X로 통신	리소스 B는 Private Subnet 1에 있으므로 프라이빗 서브넷 1용 라우팅 테이블을 이용한다. 리소스 X는 VPC 밖(인터넷)에 있으므로 NAT 게이트웨이 1 경유로 접근한다.
C -> X로 통신	리소스 C는 Private Subnet 2에 있으므로 프라이빗 서브넷 2용 라우팅 테이블을 이용한다. 리소스 X는 VPC 밖(인터넷)에 있으므로 NAT 게이트웨이 2 경유로 접근한다.



라우터

일반적인 네트워크 설계에서는 라우팅 테이블에 수행하는 설정을 라우터에 대해 수행한다. 그러나 AWS 관리 콘솔에서는 라우터를 명시적으로 생성할 필요가 없다. 라우팅 테이블을 생성하면 라우터에 해당하는 것도 자동 생성된다.

라우팅 테이블 생성 순서



라우팅 테이블 생성 정보

라우팅 테이블은 VPC, 인터넷 및 VPN 연결 내 서브넷 간에 패킷이 전달되는 방법을 지정합니다.

라우팅 테이블 설정

이름 - 선택 사항

'Name' 키와 사용자가 지정하는 값을 포함하는 태그를 생성합니다.

VPC

이 라우팅 테이블에 대해 사용할 VPC입니다.

태그

태그는 AWS 리소스에 할당하는 레이블입니다. 각 태그는 키와 선택적 값으로 구성됩니다. 태그를 사용하여 리소스를 검색 및 필터링하거나 AWS 비용을 추적할 수 있습니다.

키

값 - 선택 사항

49을(를) 태그.개 더 추가할 수 있습니다.

새로운 VPC 환경
의견을 알려주세요

VPC 대시보드

EC2 글로벌 보기 신규

VPC로 필터링:

VPC 선택

Virtual Private Cloud

VPC

서브넷

라우팅 테이블

인터넷 게이트웨이

송신 전용 인터넷 게이트웨이

캐리어 게이트웨이

DHCP 옵션 세트

탄력적 IP

관리형 접두사 목록

엔드포인트

rtb-09f0258d4a1d021bf | sample-rt-public 라우팅 테이블이 성공적으로 생성되었습니다.

VPC > 라우팅 테이블 > rtb-09f0258d4a1d021bf

rtb-09f0258d4a1d021bf / sample-rt-public

작업 ▼

이제 Reachability Analyzer를 사용하여 네트워크 연결을 확인할 수 있습니다.

×

세부 정보 정보

라우팅 테이블 ID

rtb-09f0258d4a1d021bf

VPC

vpc-071ef3b8b93974b28 | sample-vpc

기본

아니요

소유자 ID

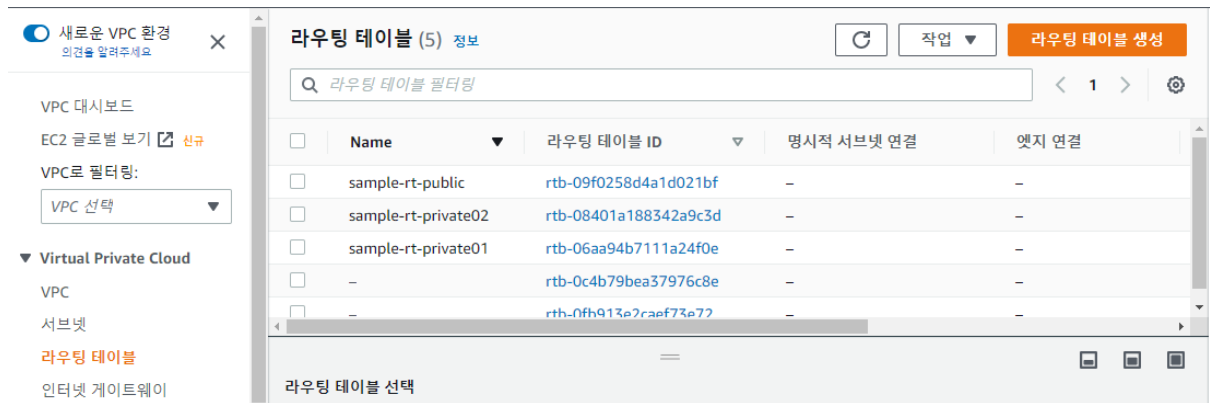
257307634175

명시적 서브넷 연결

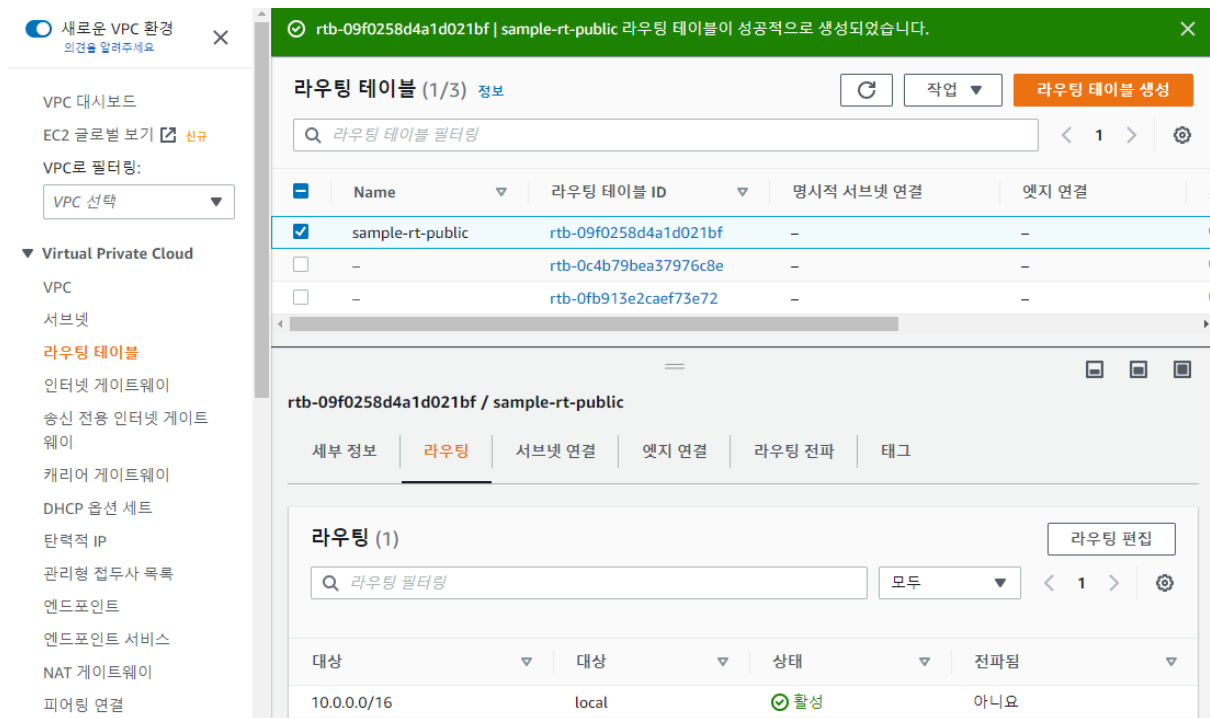
-

엣지 연결

-



라우팅 테이블을 클릭해 [라우팅] - [라우팅 편집]을 선택한다.



[라우팅 추가] 버튼을 클릭하면 새로운 행이 추가된다.

송신 대상지에는 0.0.0.0/0을 입력하고 대상은 '인터넷 게이트웨이'를 선택했을 때 표시되는 'sample-igw'를 선택한다.

[변경 사항 저장]을 클릭한다.

라우팅 편집

라우팅 편집

대상

10.0.0.0/16

대상

상태

🟢 활성

전파됨

아니요

라우팅 편집

대상

대상

상태

-

전파됨

아니요

제거

라우팅 추가

취소

미리 보기

변경 사항 저장

‘서브넷 연결 편집’ 화면에서 편집중인 라우팅 테이블이 속하는 서브넷을 지정한다.

서브넷은 여러 개를 지정할 수 있다.

sample-subnet-public01(10.0.0.0/20)와 sample-subnet-public02(10.0.16.0/20)에 연결되므로 이 2개의 서브넷에 체크한 후 [연결 저장]을 클릭한다.

새로운 VPC 환경

의견을 알려주세요

VPC 대시보드

EC2 글로벌 보기

VPC로 필터링:

VPC 선택

Virtual Private Cloud

VPC

서브넷

라우팅 테이블

인터넷 게이트웨이

송신 전용 인터넷 게이트웨이

캐리어 게이트웨이

DHCP 옵션 세트

탄력적 IP

관리형 접두사 목록

엔드포인트

엔드포인트 서비스

NAT 게이트웨이

피어링 연결

라우팅 테이블 (1/5) 정보

	Name	라우팅 테이블 ID	명시적 서브넷 연결	옛지 연결
<input checked="" type="checkbox"/>	sample-rt-public	rtb-09f0258d4a1d021bf	-	-
<input type="checkbox"/>	sample-rt-private02	rtb-08401a188342a9c3d	-	-
<input type="checkbox"/>	sample-rt-private01	rtb-06aa94b7111a24f0e	-	-
<input type="checkbox"/>	-	rtb-0c4b79bea37976c8e	-	-
<input type="checkbox"/>	-	rtb-0fb913e2cae773e77	-	-

rtb-09f0258d4a1d021bf / sample-rt-public

세부 정보

라우팅

서브넷 연결

옛지 연결

라우팅 전파

태그

명시적 서브넷 연결 (0)

서브넷 연결 편집

서브넷 ID	IPv4 CIDR	IPv6 CIDR
서브넷 연결 없음		
서브넷 연결이 없습니다.		

서브넷 연결 편집

이 라우팅 테이블과 연결된 서브넷을 변경합니다.

이용 가능한 서브넷 (2/4)

< 1 > ⚙

<input type="checkbox"/>	이름	서브넷 ID	IPv4 CIDR	IPv6 CIDR	라우팅 테이블 ID
<input type="checkbox"/>	sample-subnet-private02	subnet-09279cb8401954e47	10.0.80.0/20	-	기본 (rtb-0fb913e)
<input checked="" type="checkbox"/>	sample-subnet-public01	subnet-00d7357e27e3f4d7d	10.0.0.0/20	-	기본 (rtb-0fb913e)
<input checked="" type="checkbox"/>	sample-subnet-public02	subnet-027b54fba9f7608b8	10.0.16.0/24	-	기본 (rtb-0fb913e)
<input type="checkbox"/>	sample-subnet-private01	subnet-04dca061db8202f7c	10.0.64.0/20	-	기본 (rtb-0fb913e)

선택한 서브넷

subnet-027b54fba9f7608b8 / sample-subnet-public02 X

subnet-00d7357e27e3f4d7d / sample-subnet-public01 X

취소

연결 저장

sample-rt-private01과 sample-rt-private02도 각 항목에 맞게 설정한다.

새로운 VPC 환경

VPC 대시보드

EC2 글로벌 보기

VPC로 필터링

Virtual Private Cloud

VPC

서브넷

라우팅 테이블

인터넷 게이트웨이

라우팅 테이블 (5) 정보

< 1 > ⚙

<input type="checkbox"/>	Name	라우팅 테이블 ID	명시적 서브넷 연결	옛지 연결	기본	VPC
<input type="checkbox"/>	sample-rt-public	rtb-09f0258d4a1d021bf	2 서브넷	-	아니요	vpc-071ef
<input type="checkbox"/>	sample-rt-private02	rtb-08401a188342a9c3d	subnet-09279cb840195...	-	아니요	vpc-071ef
<input type="checkbox"/>	sample-rt-private01	rtb-06aa94b7111a24f0e	subnet-04dca061db820...	-	아니요	vpc-071ef
<input type="checkbox"/>	-	rtb-0c4b79bea37976c8e	-	-	예	vpc-0964e
<input type="checkbox"/>	-	rtb-0fb913e2cae773e72	-	-	예	vpc-071ef

라우팅 테이블 선택

보안 그룹

보안그룹이란?

VPC상에 다양한 리소스를 생성할 준비를 마쳤다. 하지만 이 상태에서는 인터넷을 통해 모든 리소스에 접근할 수 있다. VPC 안의 리소스를 보호하려면 외부로부터의 접근에 제한을 걸어야 한다.

이런 접근 제한을 수행하기 위해 보안 그룹이라는 기능을 제공한다.

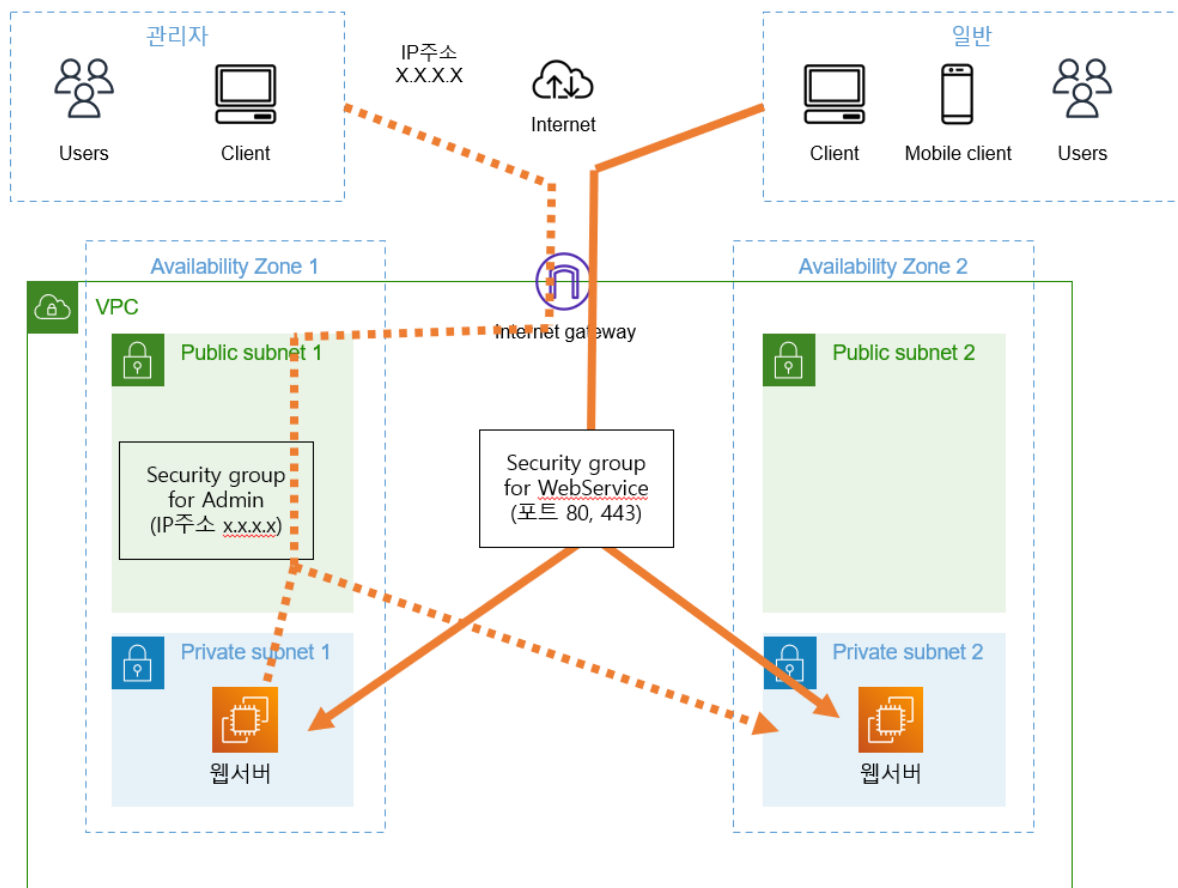


네트워크 액세스 컨트롤 리스트

같은 용도로 네트워크 액세스 컨트롤 리스트(Network Access Control List, 네트워크 ACL)라는 기능도 있다. 이 기능을 구분해 사용함으로써 보안 설정을 간소화할 수 있는 경우도 있다.

보안 그룹에서는 외부로부터의 접근을 다음과 같은 두 가지 개념을 이용해 제어할 수 있다.

- 포트 번호
- IP 주소



포트 번호를 이용한 제어에서는 제공하는 서비스의 종류를 지정할 수 있다. 예를 들어 웹 서비스에 접근할 때 쓰이는 80번(HTTP)과 443(HTTPS) 또는 서버에 접속해서 유지 보수할 때 쓰이는 22번(SSh) 등을 많이 지정한다.

IP 주소를 이용한 제어에서는 접속원을 지정할 수 있다. 소속된 회사나 학교 등 조직 내 네트워크에서 작업할 경우 인터넷에 접속하는 IP 주소는 보통 한정된다. 이러한 IP 주소들을 지정함으로써 조직 외부로부터의 접근을 막을 수 있다.

생성 내용

다음과 같은 2개의 보안 그룹이 필요하다.

- 모든 리소스에 접속하는 입구인 '점프 서버'
- 요청이나 처리를 분산하는 '로드 밸런서'

점프 서버용 보안 그룹 설정 항목

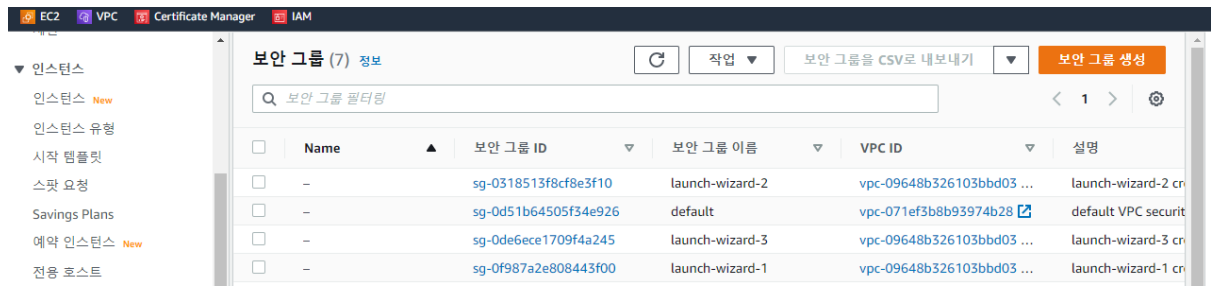
항목	값	설명
보안 그룹 이름	sample-sg-bastion	보안 그룹에 붙이는 이름
설명	for bastion server	보안 그룹의 대상이나 용도 설명
VPC	sample-vpc	보안 그룹을 생성한 VPC
<u>인바운드</u> 규칙	<ul style="list-style-type: none"> • 유형: SSH • 소스: 0.0.0.0/0 	<ul style="list-style-type: none"> • 유형에는 외부로부터의 접속을 허가하는 포트번호 또는 프로토콜을 지정 • 소스에는 외부로부터의 접속을 허가하는 IP 주소를 지정 • 0.0.0.0/0은 임의의 위치 (즉, 모든 위치)로부터의 접속을 허가

로드밸런서용 보안 그룹 설정 항목

항목	값	설명
보안 그룹 이름	sample-sg-elb	보안 그룹에 붙이는 이름
설명	for load balancer	보안 그룹의 대상이나 용도 설명
VPC	Sample-vpc	보안 그룹을 생성한 VPC
<u>인바운드</u> 규칙	<ul style="list-style-type: none"> • 유형: HTTP, HTTPS • 소스: 0.0.0.0/0 	<ul style="list-style-type: none"> • 유형에는 외부로부터의 접속을 허가하는 포트번호 또는 프로토콜을 지정 • 소스에는 외부로부터의 접속을 허가하는 IP 주소를 지정 • 0.0.0.0/0은 임의의 위치 (즉, 모든 위치)로부터의 접속을 허가

생성 순서

[인스턴스] - [보안 그룹]에서 [보안 그룹 생성] 클릭



보안 그룹 생성 정보

보안 그룹은 인바운드 및 아웃바운드 트래픽을 관리하는 인스턴스의 가상 방화벽 역할을 합니다. 새 보안 그룹을 생성하려면 아래의 필드를 작성하십시오.

기본 세부 정보

보안 그룹 이름 정보

sample-sg-bastion

생성 후에는 이름을 편집할 수 없습니다.

설명 정보

for bastion server

VPC 정보

vpc-071ef3b8b93974b28

인바운드 규칙 추가

인바운드 규칙 정보

유형 정보	프로토콜 정보	포트 범위 정보	소스 정보	설명 - 선택 사항 정보
SSH	TCP	22	Anywh... 0.0.0.0/0	

규칙 추가

로드밸런서용 보안 그룹 추가

보안 그룹 생성 정보

보안 그룹은 인바운드 및 아웃바운드 트래픽을 관리하는 인스턴스의 가상 방화벽 역할을 합니다. 새 보안 그룹을 생성하려면 아래의 필드를 작성하십시오.

기본 세부 정보

보안 그룹 이름 정보

sample-sg-elb

생성 후에는 이름을 편집할 수 없습니다.

설명 정보

for load balancer

VPC 정보

Q vpc-071ef3b8b93974b28 X

인바운드 규칙 정보

유형 정보

HTTP

프로토콜
정보

TCP

포트 범위 정보

80

소스 정보

Anywh... Q

0.0.0.0/0 X

설명 - 선택 사항 정보

삭제

HTTPS

TCP

443

Anywh... Q

0.0.0.0/0 X

삭제

규칙 추가

생성 결과

보안 그룹 (2) 정보



작업 ▼

보안 그룹을 CSV로 내보내기 ▼

보안 그룹 생성

Q 보안 그룹 필터링

< 1 > ⚙

search: samp X

필터 지우기

<input type="checkbox"/>	Name ▼	보안 그룹 ID ▼	보안 그룹 이름 ▼	VPC ID ▼	설명
<input type="checkbox"/>	sample-sg-elb	sg-0e7e40f36a3ee6c7f	sample-sg-elb	vpc-071ef3b8b93974b28 🔗	for load balancer
<input type="checkbox"/>	sample-sg-bastion	sg-0934de51e5384440b	sample-sg-bastion	vpc-071ef3b8b93974b28 🔗	for bastion server