aws re/start

AWS Cloud의 네트워킹

네트워킹 기본 사항

학습 내용

강의 핵심 내용

학습 내용:

- 클라우드의 네트워킹을 설명합니다.
- Amazon Virtual Private Cloud(Amazon VPC)를 사용해 클라우드의 가상 네트워킹을 설명합니다.
- Virtual Private Cloud(VPC)의 주요 구성 요소를 설명합니다.
- 서브넷 및 Classless Inter-Domain Routing(CIDR) 블록 주소 지정을 Amazon VPC 기능과 연결합니다.

클라우드의 네트워킹

가상 네트워킹 돌이켜 보기

앞서 설명한 Amazon Web Services(AWS) 서비스와 기존 네트워크 토폴로지의 유사성을 비교하면 다음과 같습니다.

기존 토폴로지	AWS 서비스
데이터 센터	Amazon VPC
라우터	라우팅 테이블
스위치(서브넷)	서브넷
방화벽	보안 그룹 및 네트워크 액세스 제어 목록(네트워크 ACL)
서버 및 운영 체제	Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스
모뎀	인터넷 게이트웨이

Amazon VPC란?

Amazon VPC

Amazon VPC 돌이켜 보기

Amazon VPC는 AWS Cloud의 논리적으로 격리된 섹션을 프로비저닝하는 데 사용할 수 있는 서비스입니다. 이 서비스를 Virtual Private Cloud 또는 Amazon VPC라고 합니다. Amazon VPC를 사용하면 정의한 가상 네트워크에서 AWS 리소스를 시작할 수 있습니다.

Amazon VPC의 역할은?

- 다음을 포함한 가상 네트워킹 리소스를 제어할 수 있습니다.
  - IP 주소 범위 선택
  - 서브넷 생성
  - 라우팅 테이블 및 네트워크 게이트웨이 구성
- 네트워크 구성을 사용자 정의할 수 있는 기능을 제공합니다.
- 여러 계층의 보안 성능을 사용할 수 있는 기능을 제공합니다.

Amazon VPC를 사용해야 하는 이유

- 클라우드에서 몇 분 이내에 데이터 센터에 있던 논리적 환경을 가동할 수 있습니다.
- 회사 데이터 센터에서 장비를 유지 관리하는 것보다 비용 효율적이고 사용한 리소스에 대한 비용만 지불합니다.
- 기업이 AWS 클라우드 서비스를 간편하게 마이그레이션하여 사용할 수 있도록 설계되었습니다.
- 안전하고 확장 가능하며 신뢰할 수 있습니다.
- AWS와 제3자의 혁신적인 여러 서비스에서 작동합니다.
- 다양한 Amazon VPC를 생성하고 실제 가동되기 전에 테스트 환경을 생성할 수 있습니다.

Amazon VPC의 기능

Amazon VPC의 기능

Amazon VPC의 기능은 다음과 같습니다.

- AWS Cloud에 액세스할 수 있는 전용 AWS 계정이 있습니다.

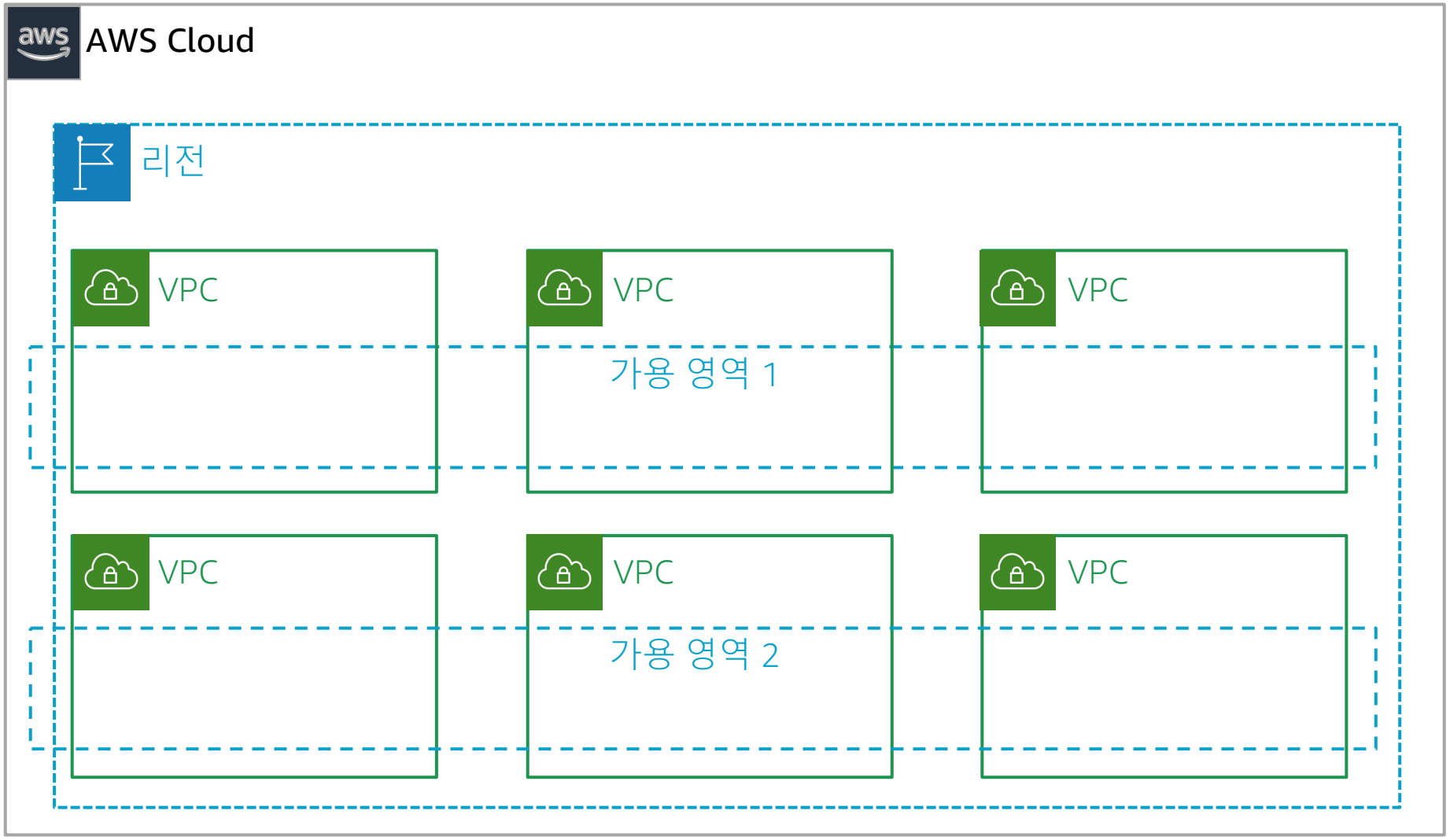
- 단일 AWS 리전에 속합니다.

- 여러 가용 영역에 걸쳐 있을 수 있습니다.

- 다른 Amazon VPC와 논리적으로 격리되어 있습니다.

Amazon VPC의 기능(계속)

여러 Amazon VPC는 AWS 리전의 서로 다른 가용 영역에 걸쳐 있을 수 있습니다.



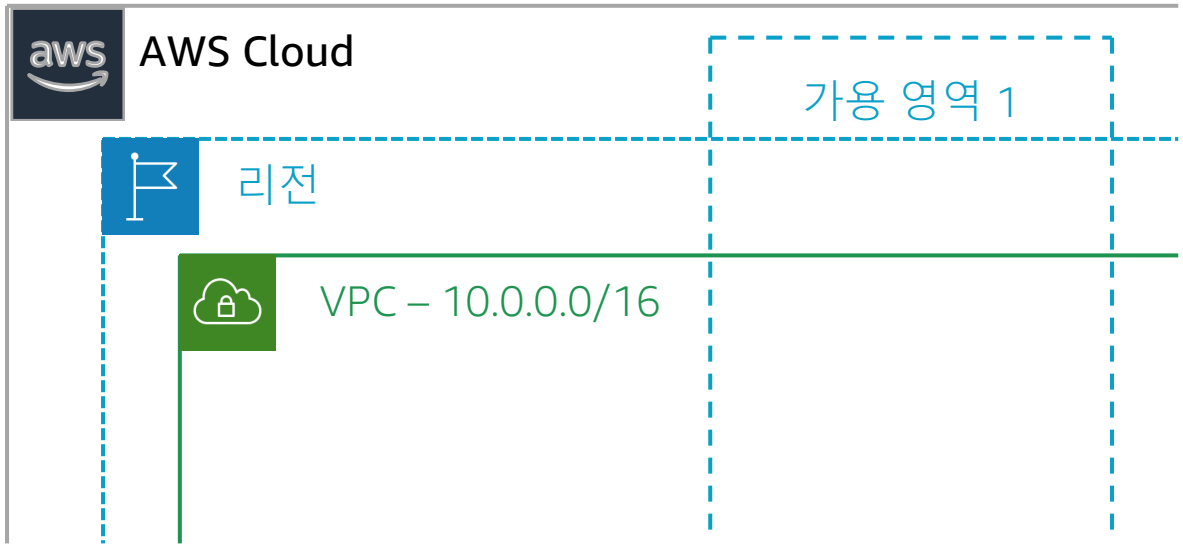
Amazon VPC의 IP 주소 지정

Amazon VPC의 IP 주소 지정

IP 주소 지정은 Amazon VPC에서 어떻게 작동할까요?

VPC를 생성할 때 CIDR 블록(예: 10.0.0.0/16)을 선택해 IPv4 주소 범위를 지정해야 합니다.

- Amazon VPC 주소 범위는 최대 /16(주소 65,536개), 최소 /28(주소 16개)일 수 있습니다.
- 사설 IP 범위는 RFC 1918에 따라 사용해야 합니다.



Amazon VPC의 IP 주소 범위는 CIDR 블록으로 지정됩니다.

사설 IP 주소 범위

Amazon VPC가 생성되면 다음의 사설 IPv4 주소 범위(RFC 1918에도 지정됨)에서 CIDR 블록을 선택합니다.

RFC 1918 범위	Amazon VPC CIDR 블록의 예제
10.0.0.0~10.255.255.255	10.0.0.0/16
172.16.0.0~172.31.255.255	172.31.0.0/16
192.168.0.0~192.255.255	192.168.0.0/16

- 허용되는 블록 크기는 /28 이상, /16 이하입니다.
- 비공개 범위를 벗어나는, 공개적으로 라우팅 가능한 CIDR 블록을 사용할 수는 있지만 권장되지 않습니다. 이 경우 인터넷에 공개적으로 라우팅 가능한 리소스를 사용하면 문제가 될 수 있습니다.

Amazon VPC 구성 요소

Amazon VPC

Amazon VPC란?

- Amazon VPC는 데이터 센터의 기존 네트워크와 유사하게 정의한 가상 네트워크입니다.

VPC에서 중요한 개념

- **CIDR 블록:** 개인 범위는 /16 ~ /28에서 제공되어야 합니다.
- **서브넷:** VPC 내 IP 주소 범위를 할당합니다.
- **라우팅 테이블:** VPC가 트래픽을 라우팅하는 데 사용되는 규칙(경로라고도 함)입니다.
- **인터넷 게이트웨이:** VPC에 연결하고 VPC에서 인터넷으로 전달되는 통신을 허용합니다.
- **VPC 엔드포인트:** 인터넷이 필요 없는 AWS 서비스 간의 비공개 연결입니다.

Amazon VPC에 액세스하는 일반적인 방법

- AWS Management Console
- AWS Command Line Interface(AWS CLI)

Amazon VPC 구성 요소

다음 구성 요소를 사용하여 Amazon VPC의 네트워킹을 구성할 수 있습니다.

- Amazon VPC
- 인터넷 게이트웨이
- Network Address Translation(NAT) 게이트웨이
- 라우팅 테이블
- 퍼블릭 및 프라이빗 서브넷
- 보안 그룹
- 네트워크 ACL

인터넷 게이트웨이

인터넷 게이트웨이란?

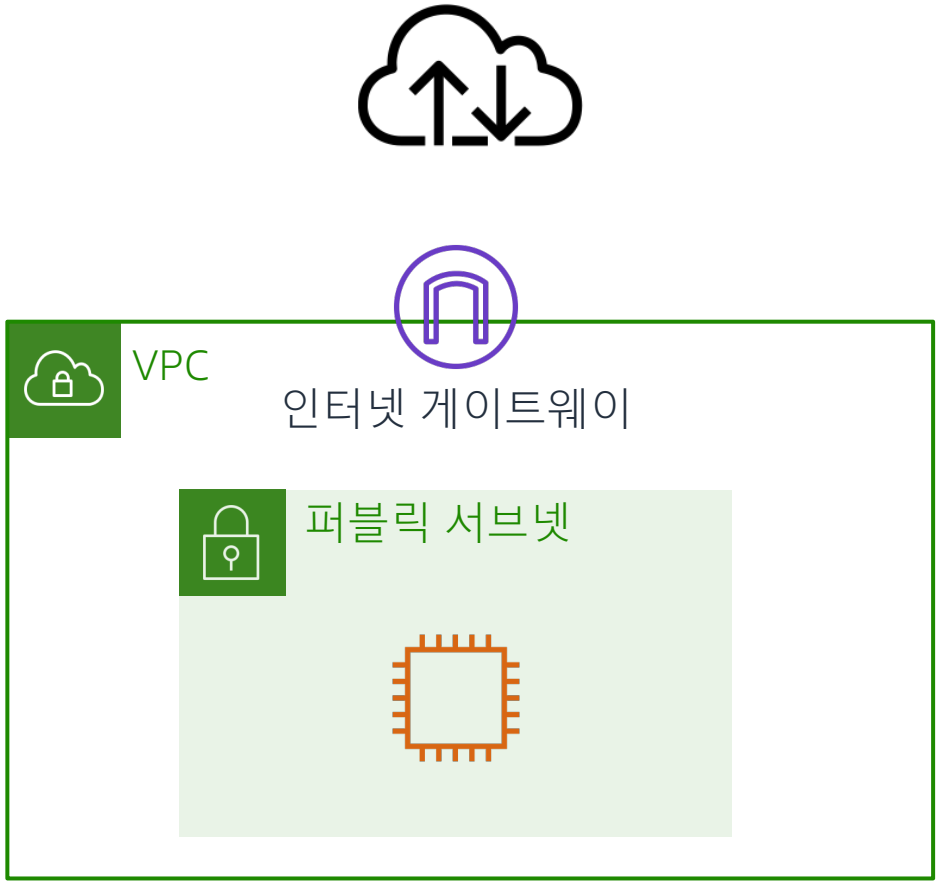
- 인터넷 게이트웨이는 VPC에서 인터넷으로 전달되는 통신을 허용합니다. 트래픽 요구 사항을 충족하며, 이중화되고, 고가용성을 유지하도록 수평 확장됩니다.

퍼블릭 서브넷:

- 인터넷 게이트웨이 측 경로가 있는 라우팅 테이블에 연결됩니다.
- 경로는 0.0.0.0/0, 대상은 IGW-xxxxx입니다.

공인 IP 주소:

- 인스턴스가 인터넷으로 통신하려면 공인 IPv4 또는 탄력적 IP 주소가 있어야 합니다.



aws re/start

NAT 게이트웨이

NAT 게이트웨이란?

- NAT 게이트웨이는 프라이빗 서브넷의 인스턴스를 VPC 외부에 연결할 수 있게 해 주지만, VPC 외부의 모든 항목에서 연결을 시작할 수는 없습니다. RESET 플래그가 전송됩니다.

퍼블릭 서브넷:

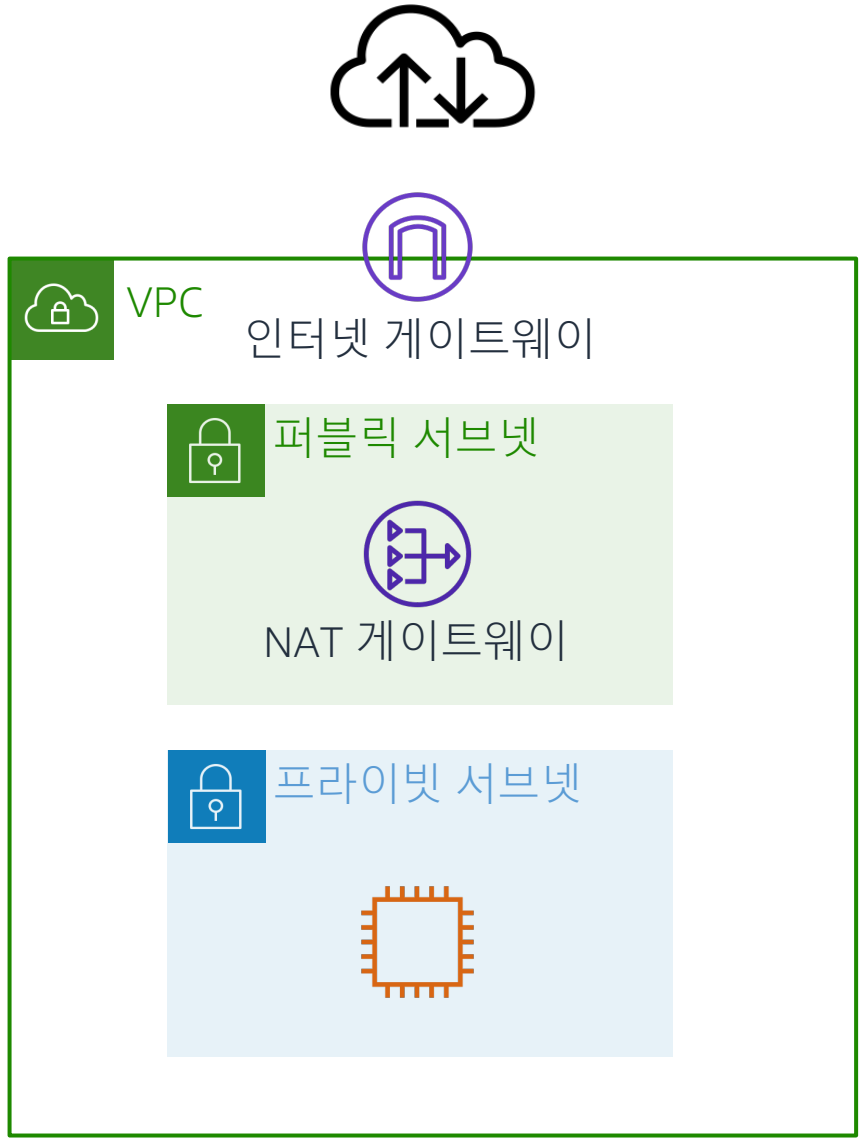
- NAT 게이트웨이에는 공인 IP 주소인 탄력적 IP 주소가 할당되며, 퍼블릭 서브넷에 있습니다.

프라이빗 서브넷:

- 경로는 0.0.0.0/0이고, 대상은 프라이빗 서브넷에 연결된 라우팅 테이블의 nat-xxxxx입니다.

사설 IP 주소:

- NAT 게이트웨이로 인해 프라이빗 서브넷의 인스턴스에는 공인 IP 주소가 필요하지 않습니다.



라우팅 테이블

라우팅 테이블이란?

- 라우팅 테이블에는 VPC 내에서 네트워크 트래픽을 지시하는 경로와 대상이 있습니다.

대상 위치:

- 대상 위치는 IP 주소와 CIDR 범위입니다(예: 0.0.0.0/0은 인터넷임).

대상:

- 대상은 게이트웨이 또는 네트워크 인터페이스입니다. 목적지 트래픽에서 사용됩니다.

라우팅 테이블 연결:

- 각 라우팅 테이블은 서브넷에 연결되어야 합니다. 라우팅 테이블은 서브넷과 게이트웨이를 함께 연결합니다.

대상 위치	대상
10.0.0.0/16	로컬
0.0.0.0/0	igw-id

퍼블릭 서브넷과 프라이빗 서브넷

서브넷이란?

- VPC 내 IP 주소의 범위입니다.

가용 영역:

- 서브넷은 영역에 걸쳐 있을 수 없기 때문에 가용 영역별로 하나의 서브넷이 있습니다.

퍼블릭 서브넷:

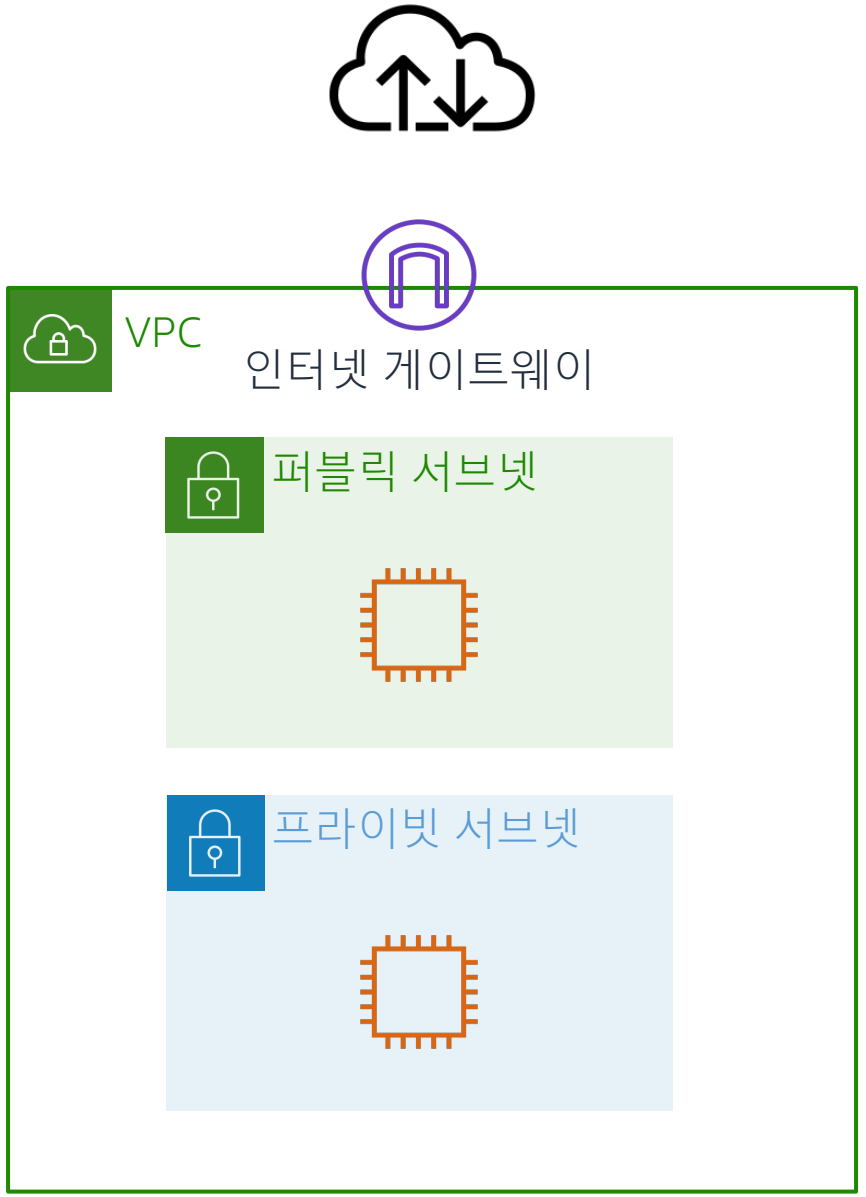
- 트래픽은 인터넷 게이트웨이와 연결된 라우팅 테이블을 통해 인터넷 게이트웨이로 라우팅됩니다.

프라이빗 서브넷:

- 트래픽은 인터넷으로 라우팅되지 않습니다.

서브넷 크기 조정:

- VPC에 두 개 이상의 서브넷이 생성된 경우, 서브넷의 CIDR 블록이 서로 중첩되지 않아야 합니다.



보안 그룹

보안 그룹이란?

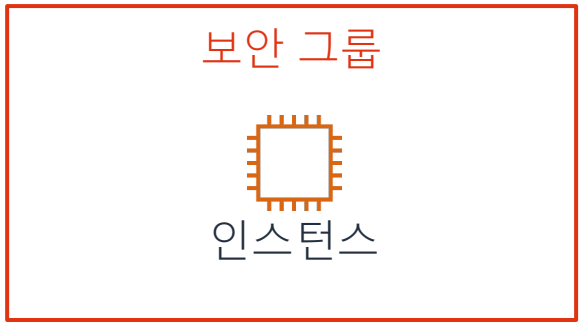
- 들어오는 트래픽을 제어하는 것은 EC2 인스턴스 수준의 방화벽입니다.

상태 기반:

- 보안 그룹은 상태 기반입니다. 상태 기반은 인스턴스의 요청이 전송되면 인바운드 규칙에 관계없이 응답 트래픽이 다시 흐르도록 허용됨을 의미합니다.

기본값으로 모든 트래픽을 차단합니다.

- 보안 그룹은 기본값으로 모든 트래픽을 차단합니다. 프로토콜, 포트 범위, 인터넷 제어 메시지 프로토콜(ICMP) 유형, 소스 또는 대상 위치를 허용해야 합니다.



네트워크 ACL

네트워크 ACL이란?

- 서브넷 수준에서 방화벽 역할을 합니다.

무상태 방식:

- 나가는 트래픽은 다시 들어오게 해야 합니다.

기본 ACL은 기본값으로 모든 트래픽을 허용합니다.

- 기본값으로 모든 트래픽을 허용하지만, 트래픽을 허용하거나 거부하는 규칙을 만들 수 있습니다.

사용자 지정 ACL은 기본값으로 모든 트래픽을 거부합니다.

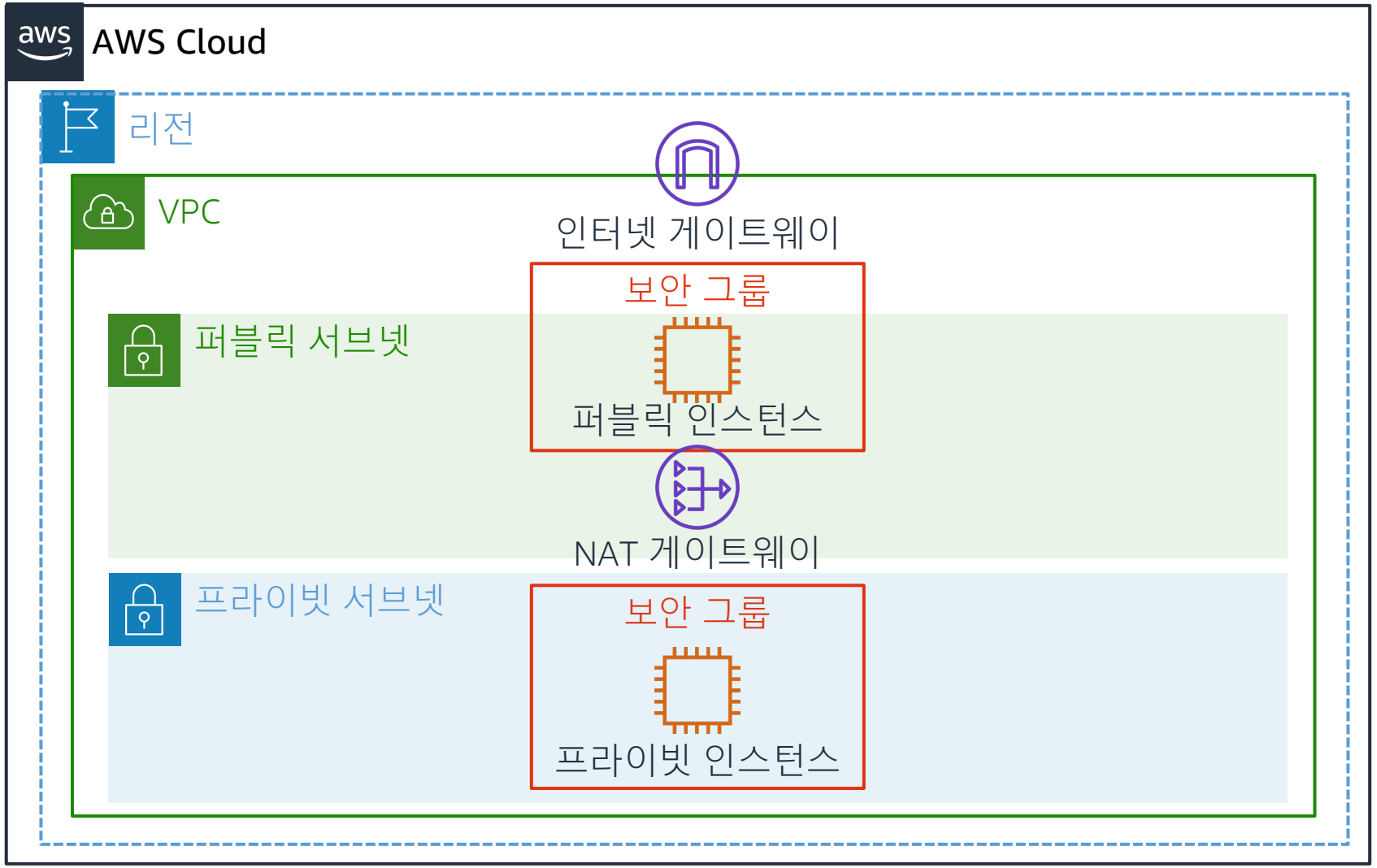
- 규칙이 추가될 때까지 모든 트래픽(인바운드/아웃바운드)을 차단하거나 거부합니다.

규칙:

- 네트워크 ACL에는 별도의 인바운드/아웃바운드 규칙이 있습니다. 각 규칙은 10 또는 100 단위로 트래픽을 허용하거나 거부할 수 있습니다.

Amazon VPC의 예제

이 이미지는 완전히 작동하는 Amazon VPC의 예입니다.



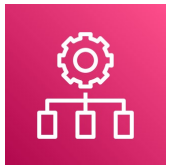
Amazon VPC에서 다른 AWS 서비스 사용

Amazon VPC에서 사용할 수 있는 제품과 서비스

Amazon VPC는 AWS 기본 서비스로, 많은 AWS 서비스에서 작동합니다.

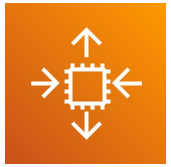
- 일례로, 운영 체제 또는 서버인 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스가 Amazon VPC에 배포되는 경우를 들 수 있습니다.
- Amazon VPC를 이해하고 구현하면 다른 AWS 서비스를 충분히 사용할 수 있습니다.


Amazon VPC


AWS OpsWorks


Amazon DynamoDB


AWS Elastic Beanstalk


Amazon EC2 Auto Scaling


Amazon Relational Database Service(Amazon RDS)


AWS Data Pipeline


Elastic Load Balancing


Amazon Elastic File System(Amazon EFS)


Amazon ElastiCache


Amazon Simple Storage Service(Amazon S3)


Amazon WorkSpaces


Amazon EMR

aws re/start

데모

이 데모에는 다음 구성 요소로 기본 Amazon VPC를 생성하는 방법이 나와 있습니다.

- Amazon VPC
- 인터넷 게이트웨이
- NAT 게이트웨이
- 라우팅 테이블
- 퍼블릭 및 프라이빗 서브넷
- 보안 그룹
- 네트워크 ACL
- EC2 인스턴스(인터넷 게이트웨이 연결을 보여 주는 퍼블릭 서브넷과 NAT 게이트웨이 작동 방식을 보여 주는 프라이빗 서브넷당 하나)

ping 명령을 사용해 연결을 확인합니다.

aws re/start

확인 질문

보안 그룹은 어떤 수준에서 보호합니까?

선택할 수 있는 가장 큰 CIDR 블록은 무엇입니까?

요점

- Amazon VPC는 AWS Cloud에서 사용자 정의 네트워크를 구축하는 데 사용할 수 있는 서비스입니다.
- VPC의 IP 주소 범위는 CIDR 블록을 사용해 정의됩니다.
- Amazon VPC 내에서 다음 구성 요소를 생성할 수 있습니다.
  - 인터넷 게이트웨이
  - NAT 게이트웨이
  - 라우팅 테이블
  - 퍼블릭 및 프라이빗 서브넷
  - 보안 그룹
  - 네트워크 ACL

aws re/start

감사합니다.

aws re/start