



AWS Builders Korea Program 200

AWS Basic Networking Design

Boram Jeong
Amazon Web Services

[3/30] AWS Builders Korea Program [기본 과정]

시간	제목	발표내용
9:00 – 12:00	기본과정 : AWS Basic Networking Design 알아보기 (이론+실습)	<p>AWS Basic Networking Design 알아보기</p> <p>AWS의 기본 서비스 중 가상 네트워크에서 AWS 리소스를 구동할 수 있는 클라우드 상의 논리적으로 격리된 공간인 VPC에 대한 기본 개념에 대해 알아봅니다. 이와 더불어 Transit Gateway 구성과 VPN, DX 확장, Network Firewall 구성을 통해 기업에서 더욱 향상된 AWS Networking Design을 구현하는 방법을 이해할 수 있습니다.</p> <p>발표자: 정보람, AWS Solutions Architect</p>
12:00 – 13:30	점심시간	
13:30 – 17:00	기본과정 : AWS EC2 를 이용한 Immutable Infrastructure 구성 알아보기	<p>AWS EC2 를 이용한 Immutable Infrastructure 구성 알아보기</p> <p>AWS의 기본적인 Compute 서비스인 EC2를 이용하여 Immutable Infra 를 구성하는 방법을 소개 합니다. 개발계, 검증계, 운영계 상관없이 동일하게 EC2를 구성하고 싶으신가요? 운영환경의 EC2가 항상 운영가능한 상태(Golden-state)를 유지하길 바라시나요? SSH 접근없이 EC2를 관리하는 방법이 궁금하시다구요? 이 세션에서 EC2를 실전에서 잘 사용하는 방법에 대해 배워 볼 수 있습니다.</p> <p>발표자: 정영민, AWS Solutions Architect</p>



강연 중 질문하는 방법

- AWS Builders Go to Webinar “Questions” 창에 자신이 질문한 내역이 표시됩니다. 기본적으로 모든 질문은 공개로 답변됩니다만 본인만 답변을 받고 싶으면 (비공개)라고 하고 질문해 주시면 됩니다.

Questions

☒ Show Answered Questions

Question	Asker

Type answer here

고지 사항 (Disclaimer)

본 콘텐츠는 고객의 편의를 위해 AWS 서비스 설명을 위해 온라인 세미나용으로 별도로 제작, 제공된 것입니다. 만약 AWS 사이트와 콘텐츠 상에서 차이나 불일치가 있을 경우, AWS 사이트(aws.amazon.com)가 우선합니다. 또한 AWS 사이트 상에서 한글 번역문과 영어 원문에 차이나 불일치가 있을 경우(번역의 지체로 인한 경우 등 포함), 영어 원문이 우선합니다.

AWS는 본 콘텐츠에 포함되거나 콘텐츠를 통하여 고객에게 제공된 일체의 정보, 콘텐츠, 자료, 제품(소프트웨어 포함) 또는 서비스를 이용함으로써 인하여 발생하는 여하한 종류의 손해에 대하여 어떠한 책임도 지지 아니하며, 이는 직접 손해, 간접 손해, 부수적 손해, 징벌적 손해 및 결과적 손해를 포함하되 이에 한정되지 아니합니다.

실습 시작 전 준비 사항

AWS 계정으로 시작

1. 실습 전 계정을 꼭 신청해주세요 : <https://portal.aws.amazon.com/billing/signup#/start>
2. AWS 계정이 없으신 경우, 행사 참여 전에 미리 AWS 계정 생성 가이드를 확인하시고 AWS 계정을 생성해주시길 바랍니다.
 - *AWS 계정 생성 가이드:
<https://aws.amazon.com/ko/premiumsupport/knowledge-center/create-and-activate-aws-account/>
3. 웨비나 종료 후 설문조사에 참여해주신 분들께는 실습 비용 지원을 위한 AWS 크레딧(1인당 \$50 크레딧)을 추가로 지원합니다. 해당 AWS 크레딧은 등록하신 이메일 계정으로 4월 중 발송 드릴 예정입니다.
4. 검증된 호환성을 위하여 실습 시 사용할 웹 브라우저는 Mozilla Firefox 또는 Google Chrome Browser로 진행 부탁드립니다.

실습 마무리 및 설문 참여 방법

- 실습이 모두 끝난 후에는 자원 삭제를 잊지 마세요. 직접 준비하신 AWS 계정으로 실습을 진행하신 고객 분들의 경우, 가이드에 따라 자원 삭제를 진행하셔야 합니다. 또한, 기존에 사용하시던 자원이 있으신 고객 분들의 경우, **오늘 생성한 자원만 삭제**하는 것에 주의 부탁드립니다.
- 마지막으로 세션이 끝난 후, **GoToWebinar 창을 종료하면 설문 조사 창이** 나옵니다.
이때, 설문을 진행해 주시고 '크레딧 제공요청' 을 표기해주셔야 **AWS 크레딧**(1인당 \$50 크레딧) 을 제공받으실 수 있습니다.

AWS는 고객 피드백을 기반으로 의사 결정을 수행하며 이러한 피드백은 추후에 진행할 세션 방향을 결정합니다.
더 나은 세션을 위하여 여러분의 소중한 의견을 부탁드립니다.

감사합니다.



**더 나은 세미나를 위해
여러분의 의견을 남겨주세요!**

▶ 질문에 대한 답변 드립니다.

AWS Builders Korea Program 3,4월 아젠다

Date	Time	Campaign Level	Subject	Session Title
3/29/2022	9:00 - 12:00	AWS Builders Korea - 100	AWS Cloud Overview	기초 과정: 클라우드 기초와 AWS 클라우드 컴퓨팅
	1:30 - 17:00	AWS Builders Korea - 100HOL	Web application	기초 과정 - 실습 : AWS 코어 서비스로 간단한 웹 애플리케이션 직접 만들기(feat. VPC, EC2, ELB)
3/30/2022	9:00 - 12:00	AWS Builders Korea - 200	Networking	기본과정 : AWS Basic Networking Design 알아보기 (이론+실습)
	1:30 - 17:00	AWS Builders Korea - 200	Compute	기본과정 : AWS EC2 를 이용한 Immutable Infrastructure 구성 알아보기
3/31/2022	9:00 - 12:00	AWS Builders Korea - 200	Storage	기본과정 : 워크로드에 적합한 스토리지 선택하기
	1:30 - 17:00	AWS Builders Korea - 200	Security	기본과정 : 보안의 기본! 최소권한원칙을 위한 IAM 이해하기
4/1/2022	9:00 - 12:00	AWS Builders Korea - 200	Database	기본과정 : 워크로드에 적합한 데이터베이스 선택하기
	1:30 - 17:00	AWS Builders Korea - 200	Analytics	기본과정 : DB보다 먼 빅데이터보다 가까운 Amazon Redshift 알아보기

목차

- AWS VPC 개요
- AWS VPC 기본 구성
- 다양한 게이트웨이 서비스
- 네트워크 관련 추가 서비스



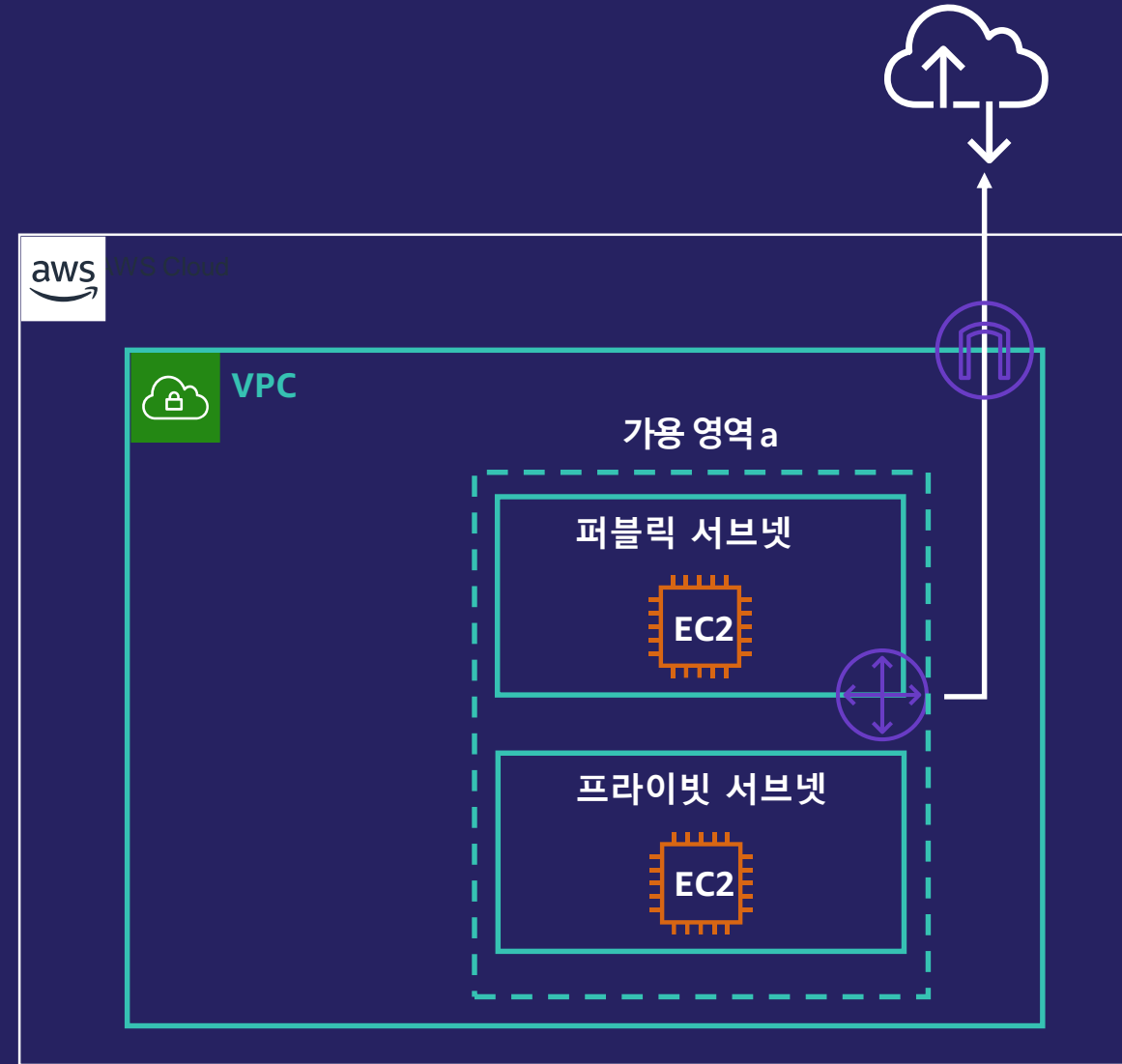
AWS VPC 개요



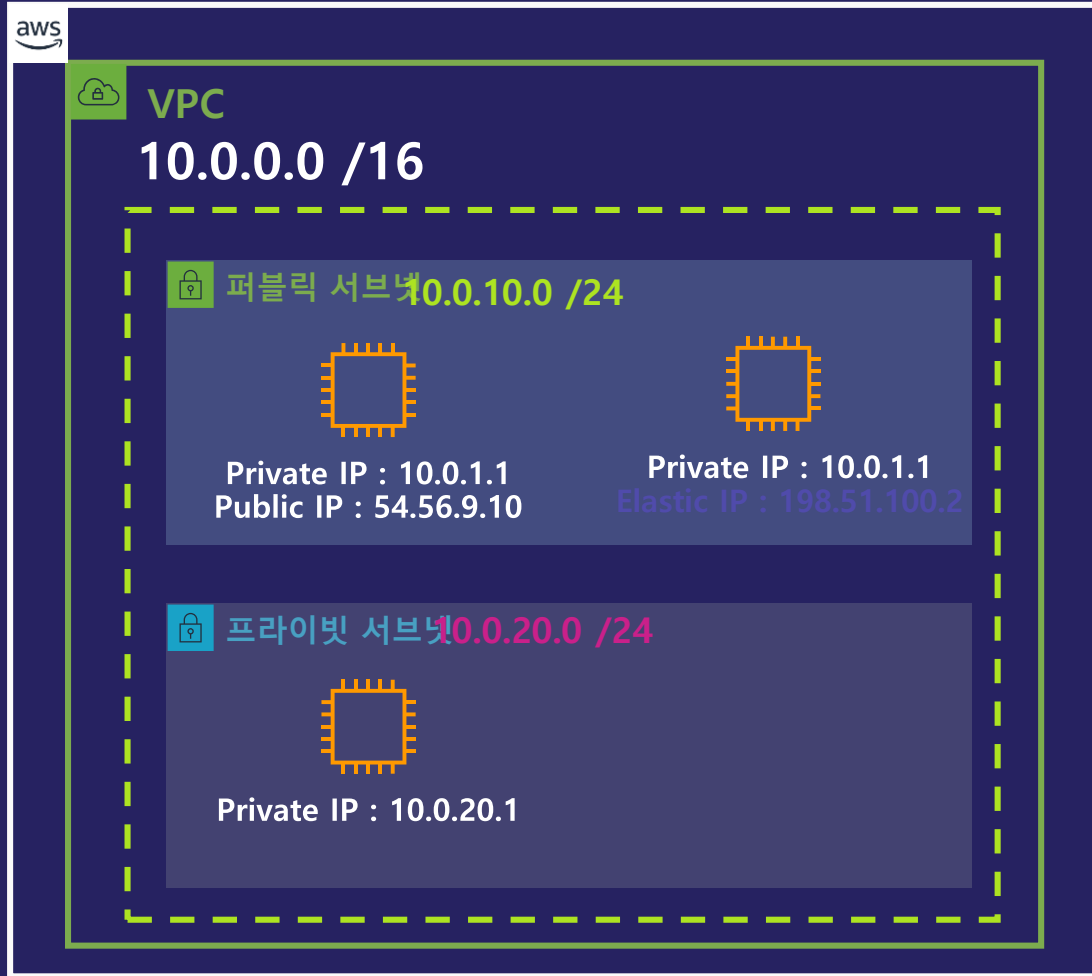
Amazon VPC 정의

Virtual Private Cloud

- 📦 사용자가 정의한 가상의 네트워크 공간
- 📦 완전한 네트워크 제어 가능
 - 📦 IP 범위
 - 📦 Subnet
 - 📦 Route Table
 - 📦 Network ACL, 보안 그룹
 - 📦 다양한 게이트웨이
- 📦 VPC 내의 모든 EC2 인스턴스들은 사설 IP가 부여됨
- 📦 개별 인스턴스에 공인 IP 할당 가능 (Public IP/Elastic IP)



Public IP / Elastic IP



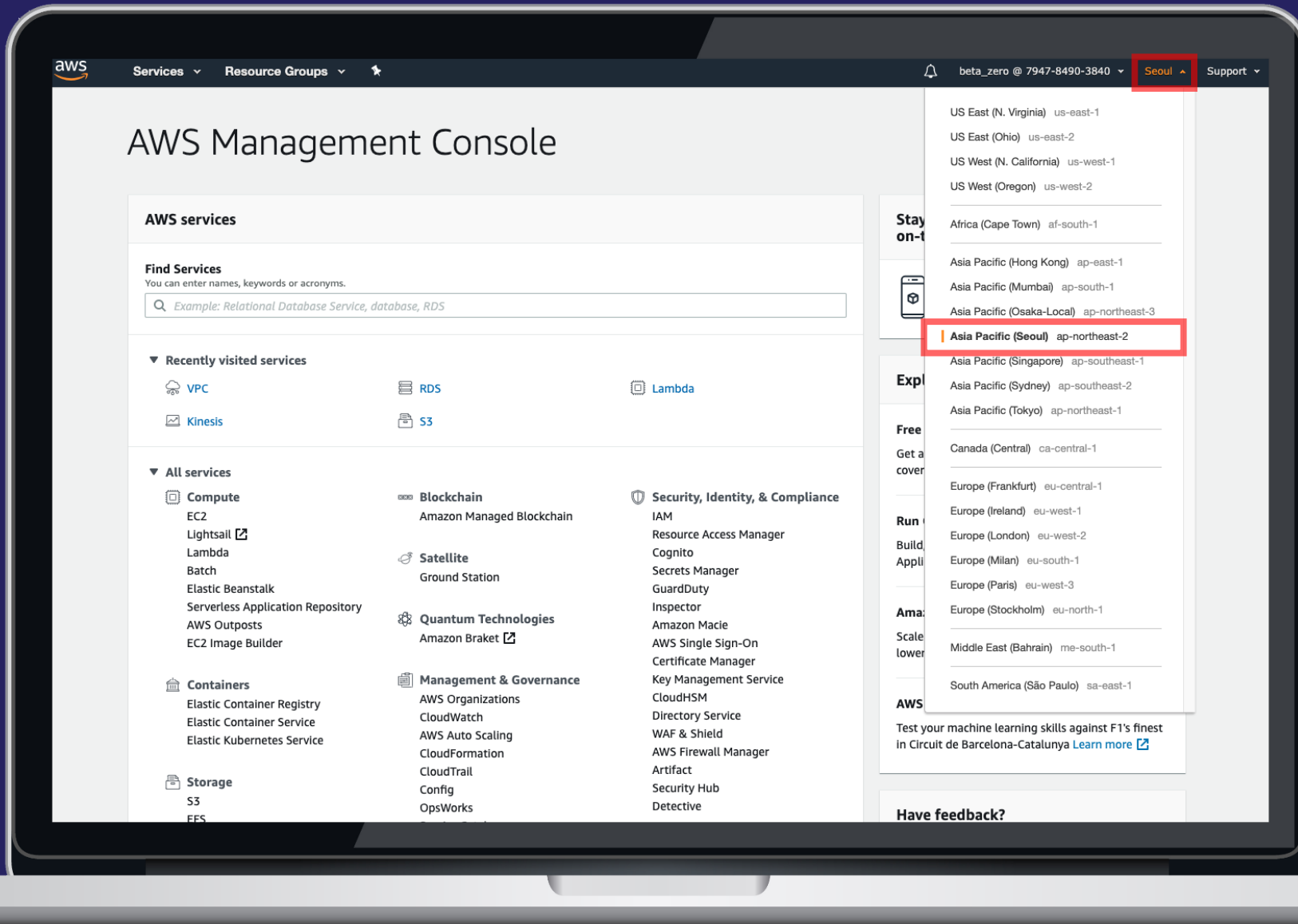
Public IP

- 유동 IP 주소

Elastic IP

- 고정 IP 주소
- Amazon EIP 주소 풀
또는
- Bring Your Own IP (BYOIP)

VPC 기본 구성 : 리전 선택



AWS 글로벌 인프라

서울 리전

ap-northeast-2



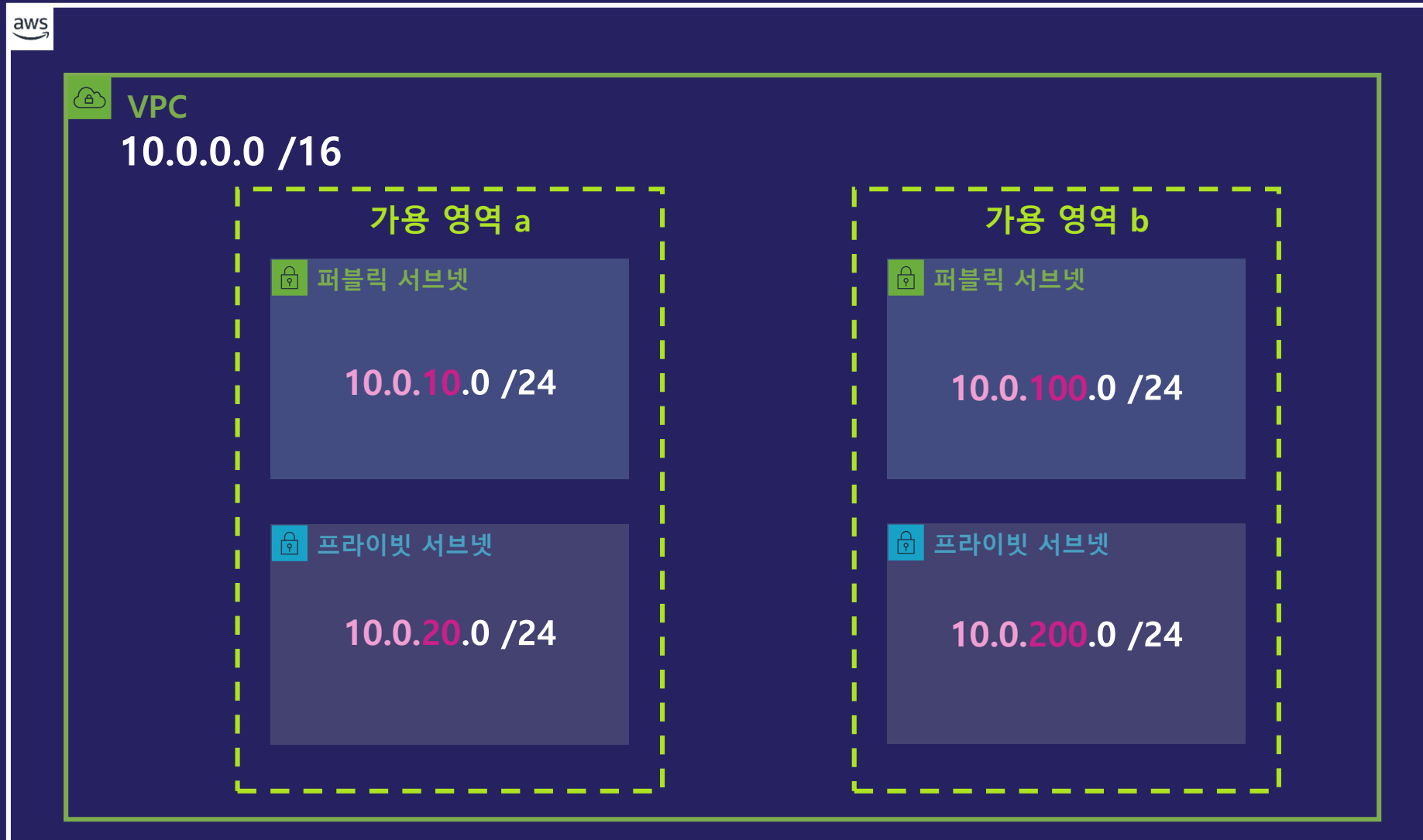
VPC 기본 구성 : 주소 범위



VPC 기본 구성 : 주소 범위

- ❏ 사설 IP 대역(RFC 1918 참고) 사용 권고
- ❏ 주 주소 범위 (CIDR 블록) 은 생성 후 변경 불가능
 - ❏ 보조 CIDR 블록 생성/제거 가능
- ❏ 생성 가능한 CIDR 블록 범위는 /28 (16) ~ /16 (65,536)
- ❏ 향후 직접 연결할 가능성이 있는 네트워크와 주소가 중복되지 않도록 할당

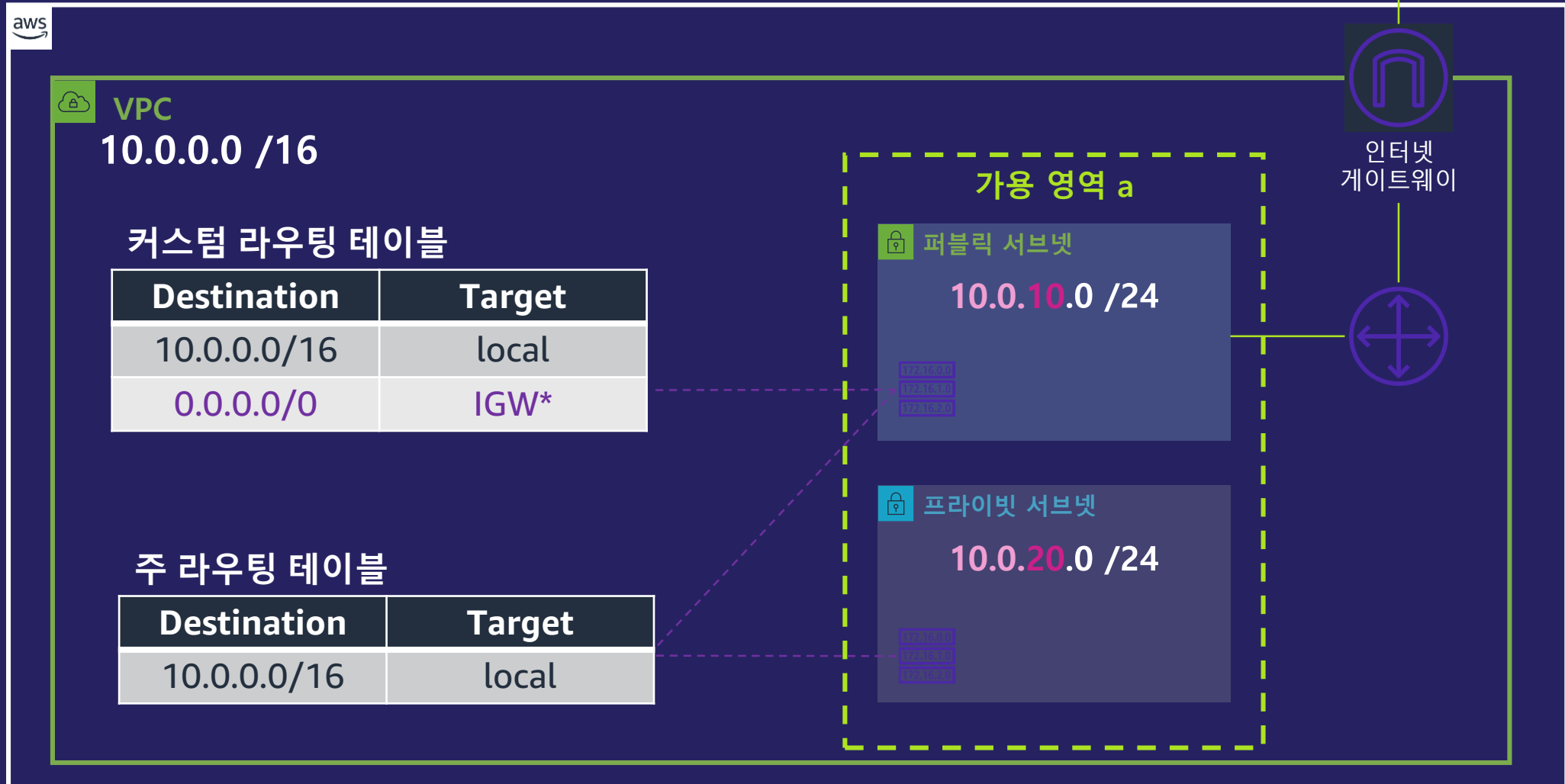
VPC 기본 구성 : 서브넷



VPC 기본 구성 : 서브넷

- ❏ VPC CIDR 블록 범위에서 리전 별 세부 서브넷 정의
 - ❏ 서브넷 범위는 보통 /24 (256) 이상을 권고
 - ❏ 5개의 주소는 (처음 4개, 마지막 1개)는 예약된 주소로 사용 불가
- ❏ 서브넷 종류
 - ❏ 퍼블릭 서브넷
 - ❏ 프라이빗 서브넷
- ❏ 서브넷 생성 후, 주소 범위 변경 불가능

VPC 기본 구성 : 라우팅 테이블



VPC 기본 구성 : 라우팅 테이블

📦 라우팅 테이블

- 📦 서브넷 단위로 설정
- 📦 네트워크 트래픽이 향하는 방향을 결정해주는 규칙 세트
- 📦 Destination과 Target 명시

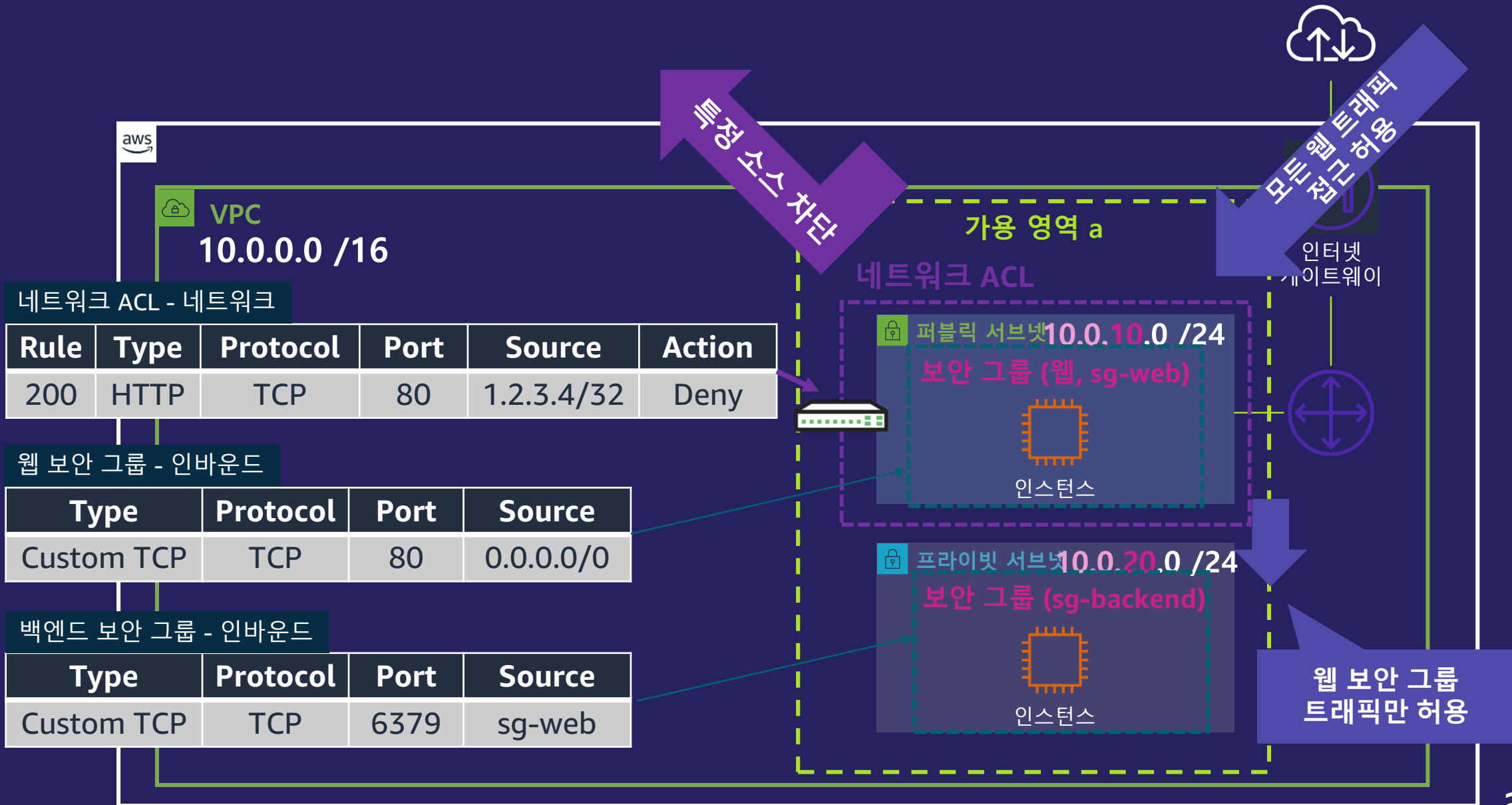
📦 VPC 내에 생성된 모든 서브넷은 기본적으로 로컬 라우터를 통해 상호 통신

📦 그 외의 경우, 추가적인 라우팅 규칙 설정 필요

- 📦 예: 인터넷, 사내 VPN 통신 및 전용선 등




📦 서브넷에 별도 라우팅 테이블을 지정하지 않으면, 주 라우팅 테이블 할당

VPC 기본 구성 : 트래픽 제어






VPC 기본 구성 : 트래픽 제어

Network ACL

-  서브넷 단위
-  Allow / Deny 규칙
-  응답 트래픽에 대한 명시적 허용 필요

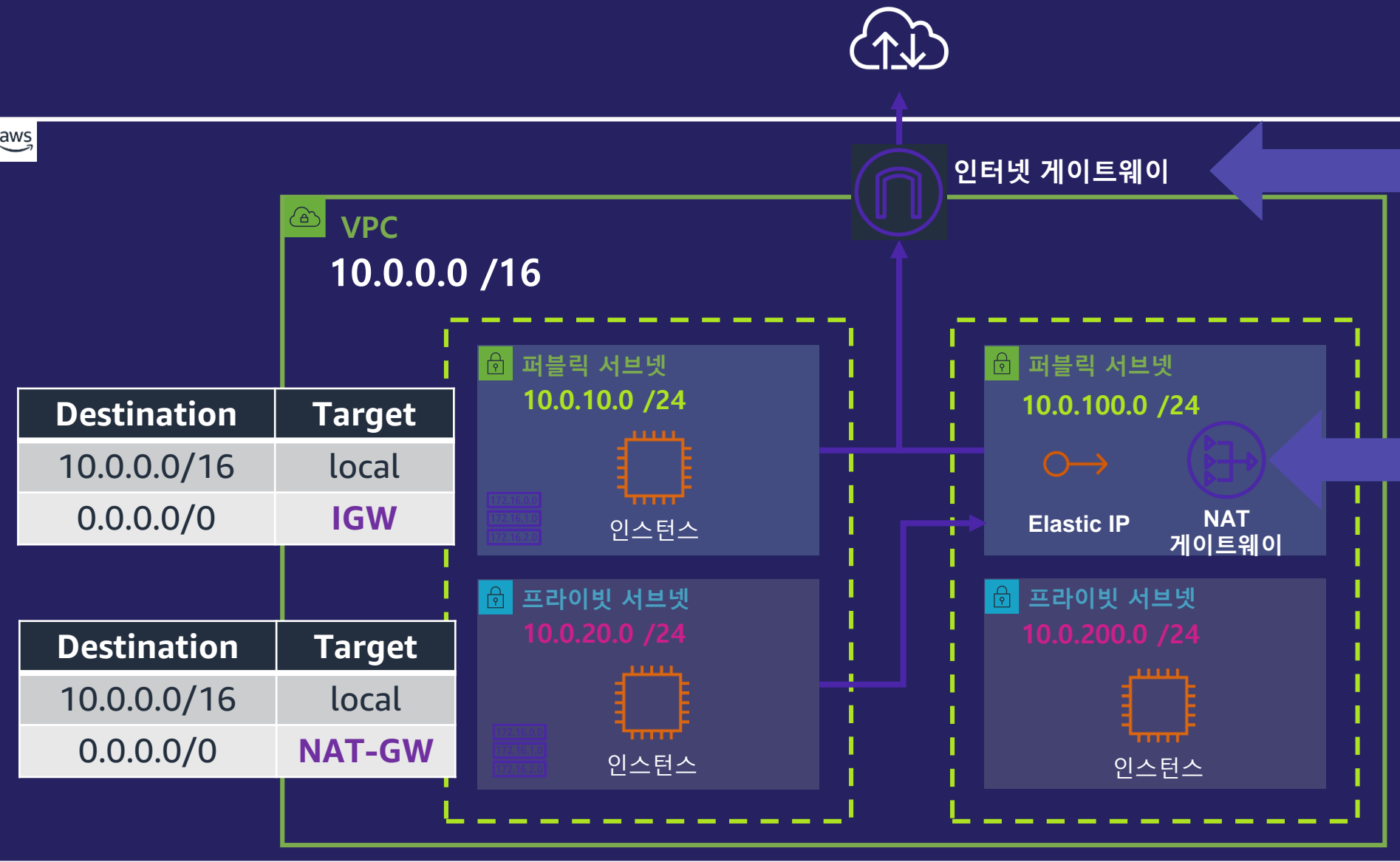
보안 그룹

-  인스턴스 단위
-  Allow 규칙
-  응답 트래픽 자동 허용

다양한 게이트웨이 서비스



Internet Gateway



Destination	Target
10.0.0.0/16	local
0.0.0.0/0	IGW

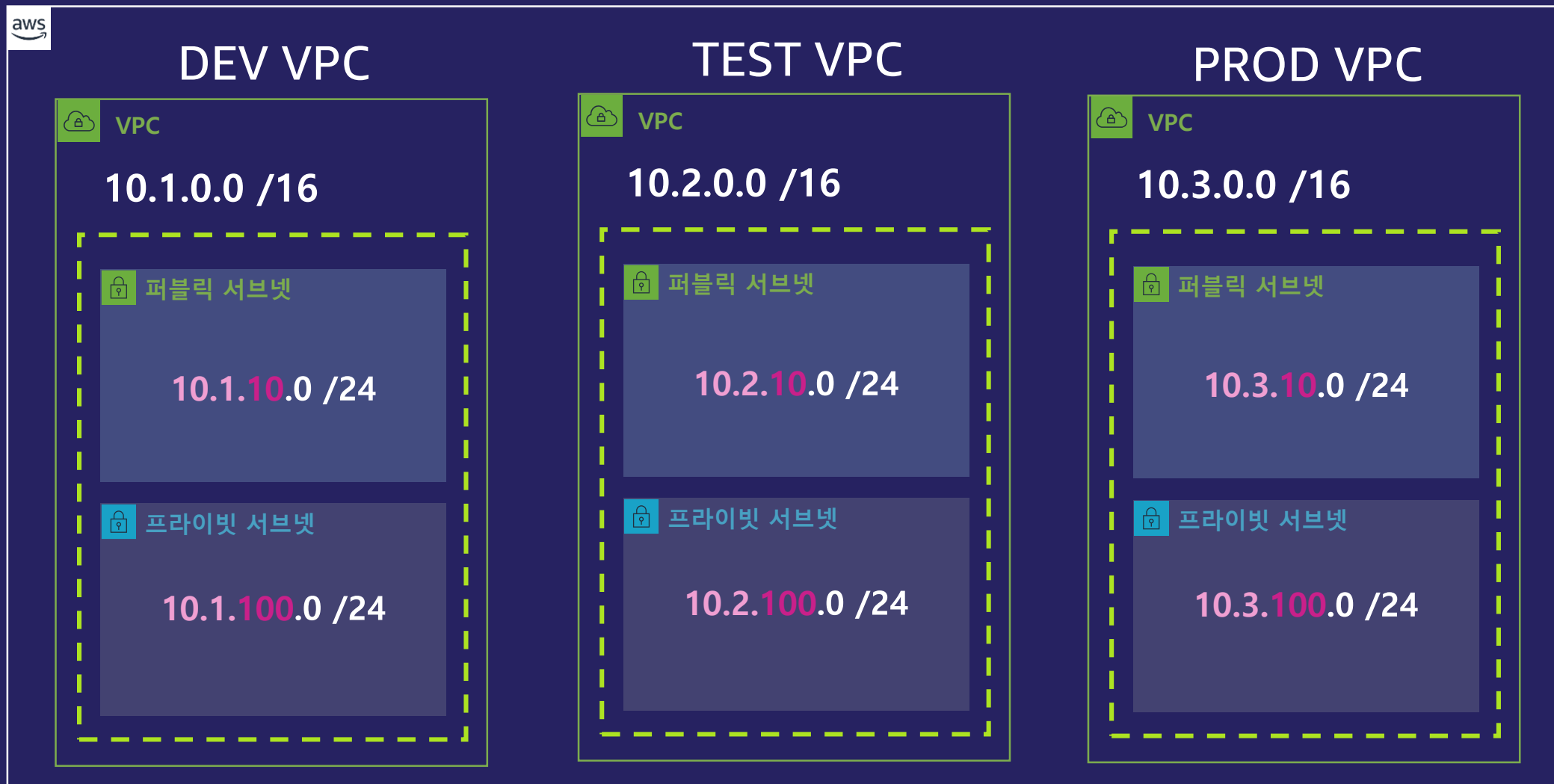
Destination	Target
10.0.0.0/16	local
0.0.0.0/0	NAT-GW

VPC와 인터넷 간에 통신을 도와줌

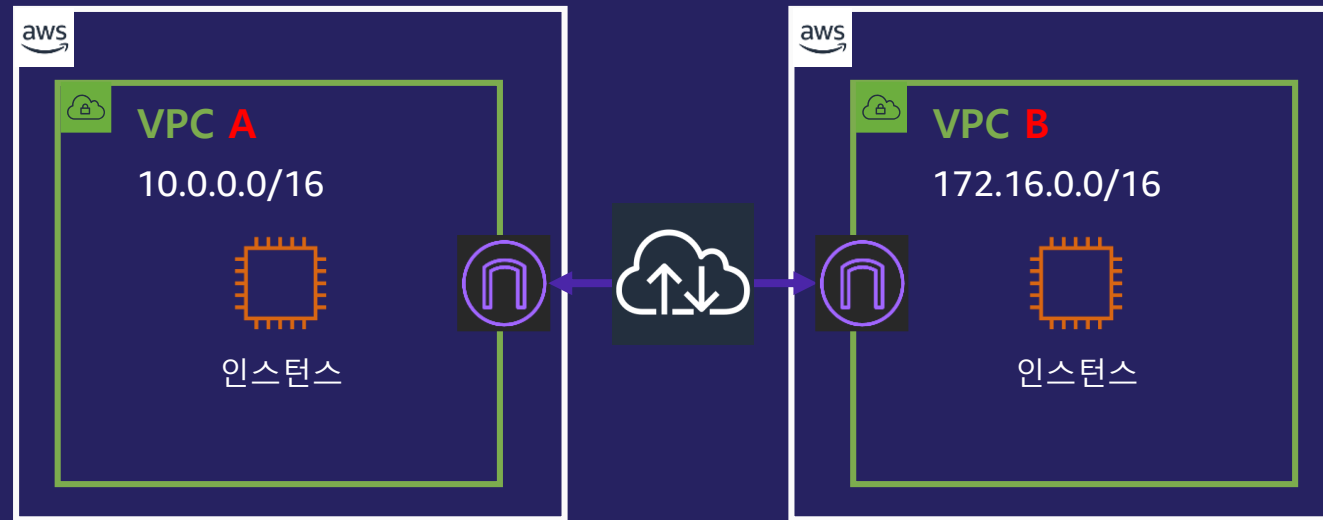
- 인터넷 라우팅이 가능한 트래픽에 대한 VPC 라우팅 테이블에 대상을 제공
- 네트워크 주소 변환

- 프라이빗 서브넷에 위치한 인스턴스의 라이브러리 설치, 패치 및 업데이트 등 수행
- 인터넷 통신을 위해 NAT 게이트웨이 당 하나의 Elastic IP 필요

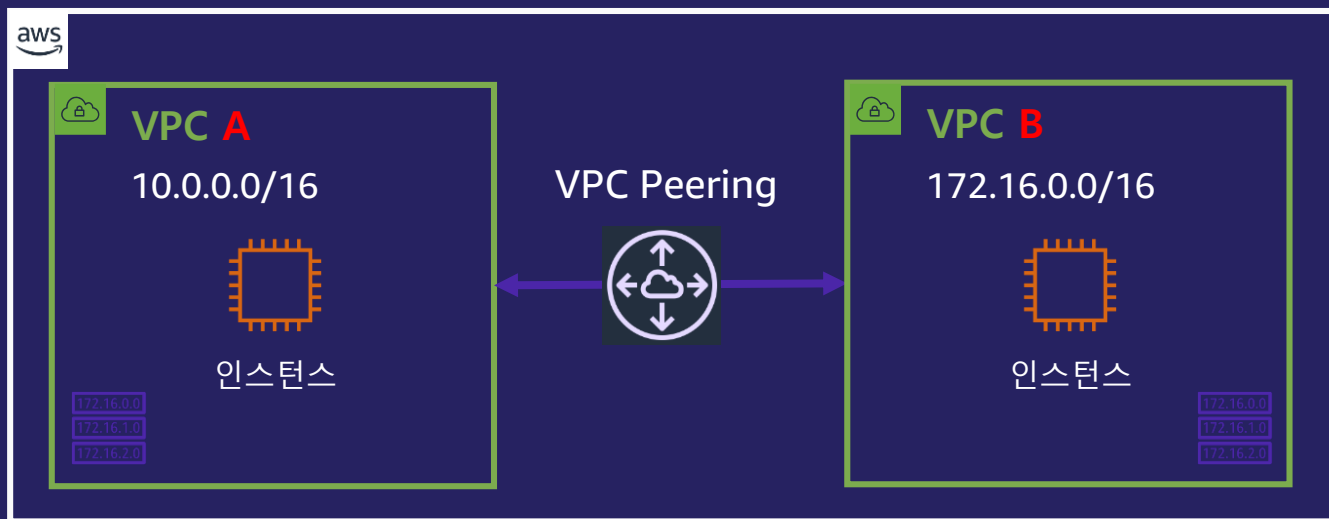
환경별 VPC 구성



VPC간 연결 방법 1 : Internet Gateway



VPC간 연결 방법 2 : VPC Peering

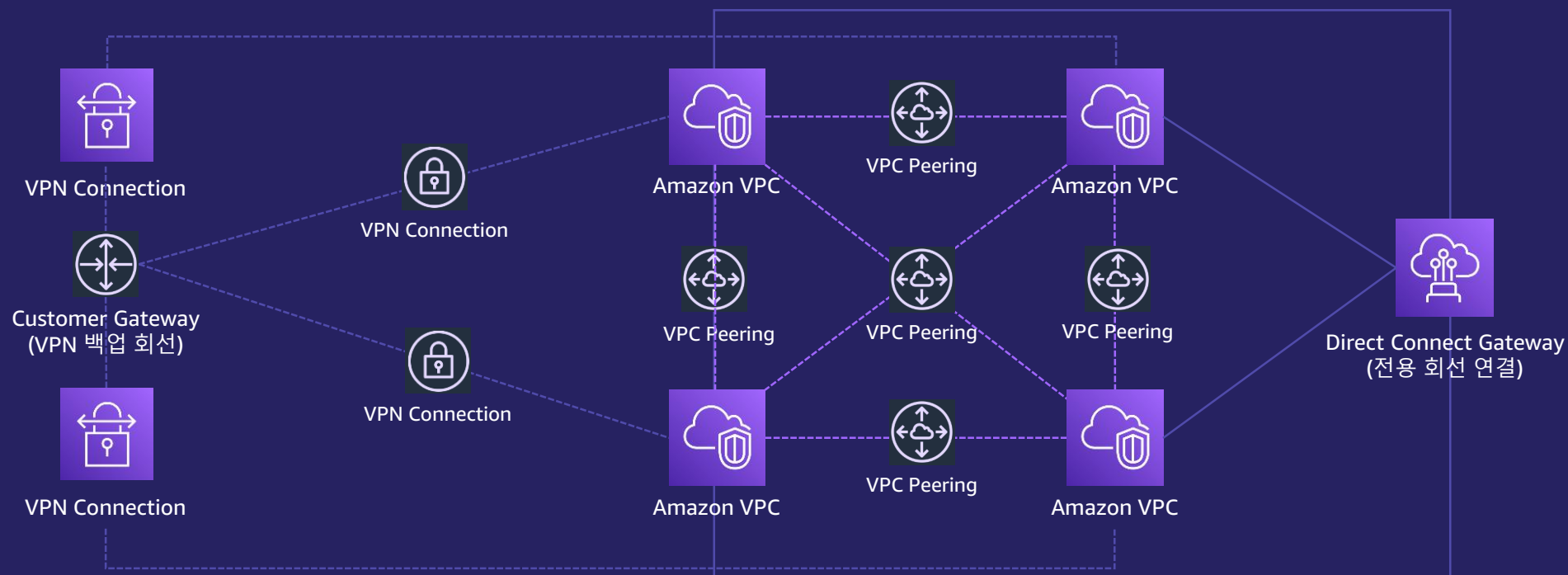


- ❏ VPC 간 완전히 격리된 전용 연결
 - ❏ 서로 다른 리전의 VPC 간 전용 연결
 - ❏ 다른 계정의 VPC 간 전용 연결
- ❏ VPC 간 단일 Peering 만 가능, IP 주소는 중복 불가

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	IGW
172.16.0.0/16	PCX

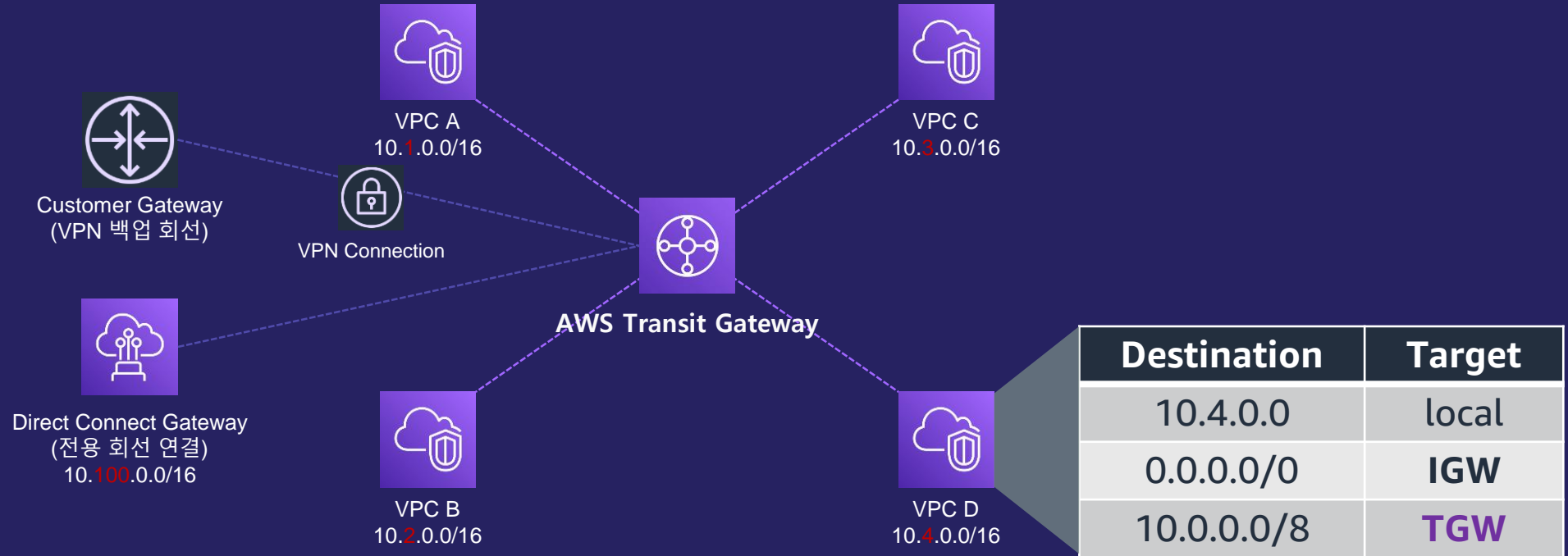
Destination	Target
172.16.0.0/16	local
0.0.0.0/0	IGW
10.0.0.0/16	PCX

VPC간 연결 방법 2 : VPC Peering



- ❏ VPC Peering은 1:1 관계
- ❏ 연결된 VPC 내의 네트워크 인터페이스에서 트래픽이 출발/종료 되어야함
- ❏ Transit 구성을 지원하지 않음

AWS Transit Gateway



- 수많은 VPC를 쉽고 자유롭게 연결
- 지점/지사 네트워크를 손쉽게 단순하게 통합
- 라우팅 도메인을 활용한 다양한 구성

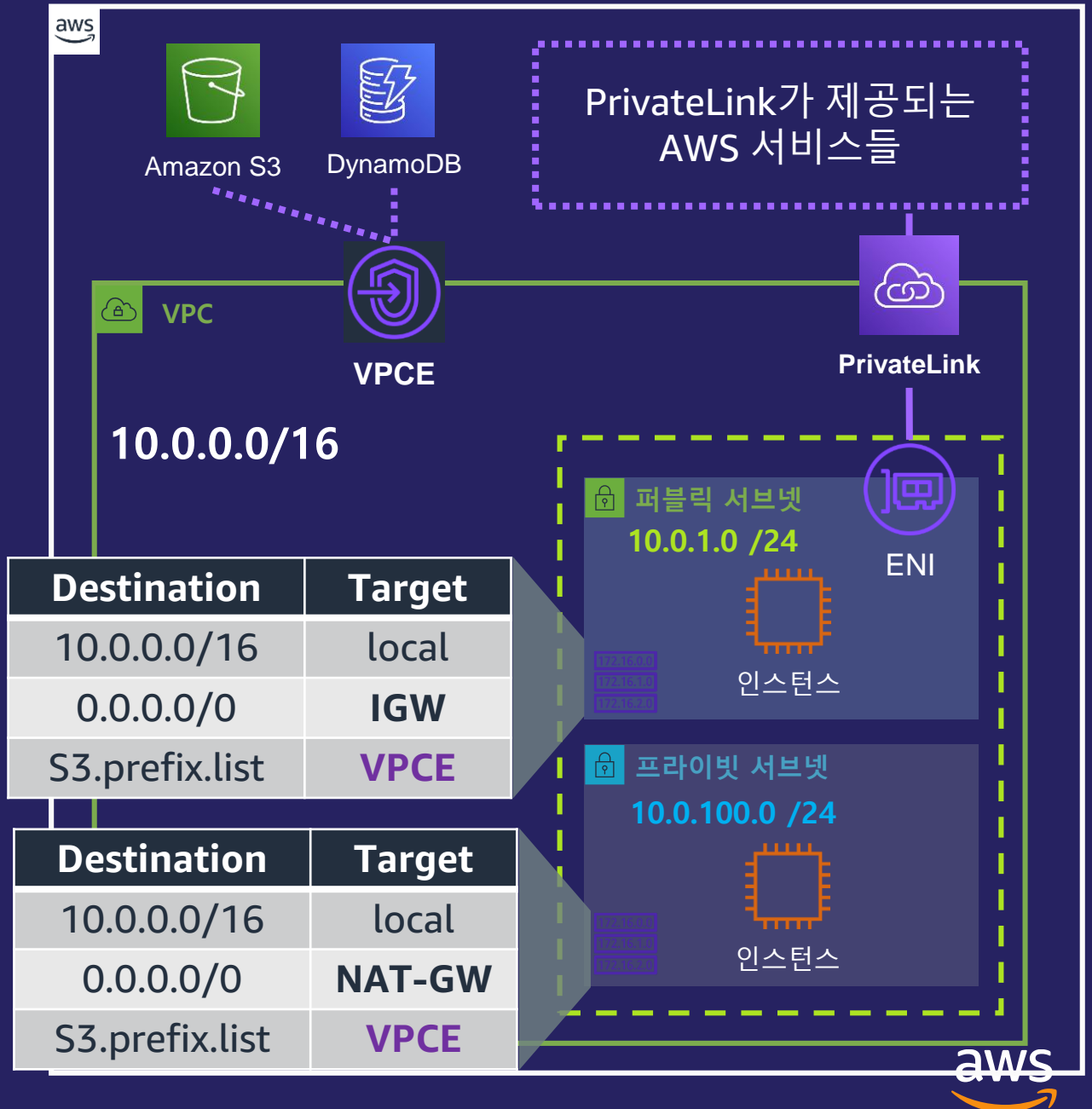
네트워크 관련 추가 서비스



VPC Endpoint 1

엔드 포인트

- 인터넷을 경유하지 않고 AWS 서비스 사용
- VPC와 해당 자원 간 전용 연결
(NAT이나 IGW 불필요)



VPC Endpoint 2

엔드 포인트 종류

게이트웨이 엔드포인트

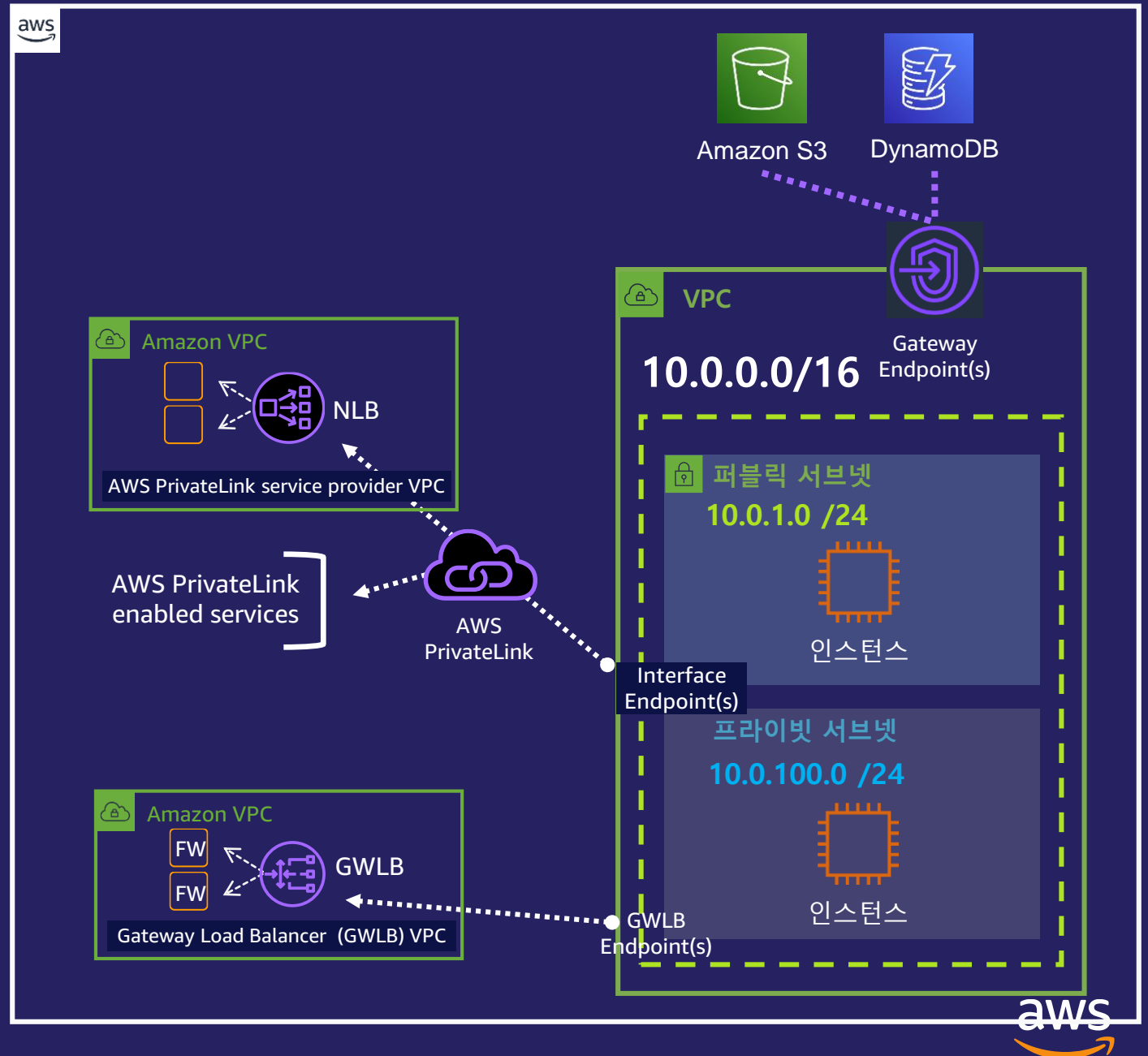
대상 : S3, Dynamo DB

인터페이스 엔드포인트

대상 : 다양한 AWS 서비스들

게이트웨이 로드밸런서 엔드포인트

대상 : 게이트웨이 로드밸런서



VPC flow logs

CloudWatch > Log Groups > /aws/vpc/demo > eni-08ab0ff5bdf9923a5-all

Expand all

Filter events

Message	Account ID	ENI ID	Source IP	Dest. IP	Source Port	Dest. Port	Protocol	Packets	Bytes	Start & End Time
No older events found at the moment. Retry.										
2 48 [REDACTED] 3 eni-08 [REDACTED] 5 83.234.179.125 172.31.22.145 59003 80 6 3 140 1565072998 1565073000 REJECT OK										
2 48 [REDACTED] 3 eni-08 [REDACTED] 5 91.189.89.198 172.31.22.145 123 45139 17 1 76 1565073020 1565073037 ACCEPT OK										
2 48 [REDACTED] 3 eni-08 [REDACTED] 5 82.151.107.126 172.31.22.145 54553 80 6 1 60 1565073020 1565073037 REJECT OK										
2 48 [REDACTED] 3 eni-08 [REDACTED] 5 37.208.66.136 172.31.22.145 57975 80 6 4 240 1565073020 1565073037 REJECT OK										

- ❏ VPC, 서브넷, EC2 인스턴스 ENI 단위로 적용 가능한 패킷 헤더 및 기타 메타데이터 수집
- ❏ 생성되는 모든 패킷에 대한 정보를 S3 또는 CloudWatch Logs에 기록
- ❏ 로깅할 트래픽 선택 가능
 - ❏ 필터 종류 : 수락된 트래픽, 거부된 트래픽, 둘 다 수집
- ❏ 최대 집계 간격 1분 또는 10분 단위로 선택 가능

Traffic Mirroring



- ❏ 대규모 트래픽 실시간 네트워크 모니터링
- ❏ 원본 인스턴스 패킷을 대상 네트워크 인터페이스 또는 네트워크 로드 밸런서로 복제
- ❏ 미러링 트래픽 선택 가능
 - ❏ 필터 종류 : 트래픽 방향, 프로토콜, 포트 및 IP 범위
- ❏ 오픈소스 혹은 AWS 파트너 솔루션 설치



더 나은 세미나를 위해
여러분의 의견을 남겨주세요!

▶ 질문에 대한 답변 드립니다.



Thank you!