Network Architecture using AWS VPC PrivateLink

AWS VPC PrivateLink를 이용한 네트워크 구성 전략

박 병진 (Byungjin Park) · 클로드 (Claud) · Site Reliability Engineer @ 당근페이

당근 SRE 밋업 1회

Aug 26, 2021

당근페이

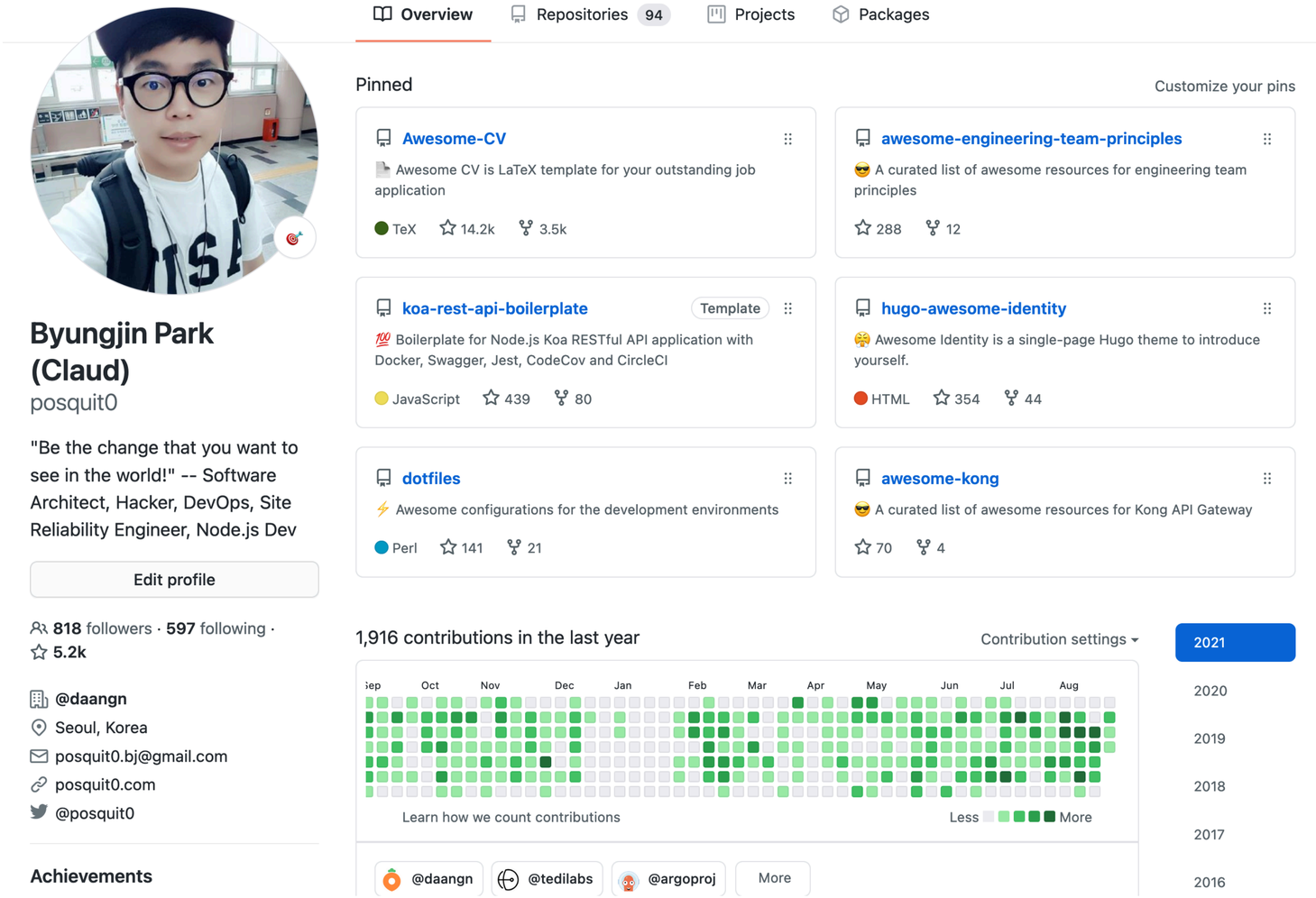
speaker

발표자 소개

박병진 / @posquit0 / 클로드 (Claud)

(현) Site Reliability Engineer @ 당근페이
(전) Director of Infrastructure Division @ 카사코리아
(전) Software Architect @ 옴니어스
(전) Co-founder & Software Engineer @ 카플랫

국제해킹대회 DEFCON CTF 본선 6회 진출
하시코프 한국 사용자 모임 운영
한국의 오픈소스 중 GitHub 10,000개 이상의 스타를 받은 프로젝트



intro

intro

당근페이

당근마켓의 주요 사용자인 지역주민과 동네상권의 불편함을 해결하고자 해요.

당근마켓 플랫폼 내 당근머니를 활용한 간편 송금 제공

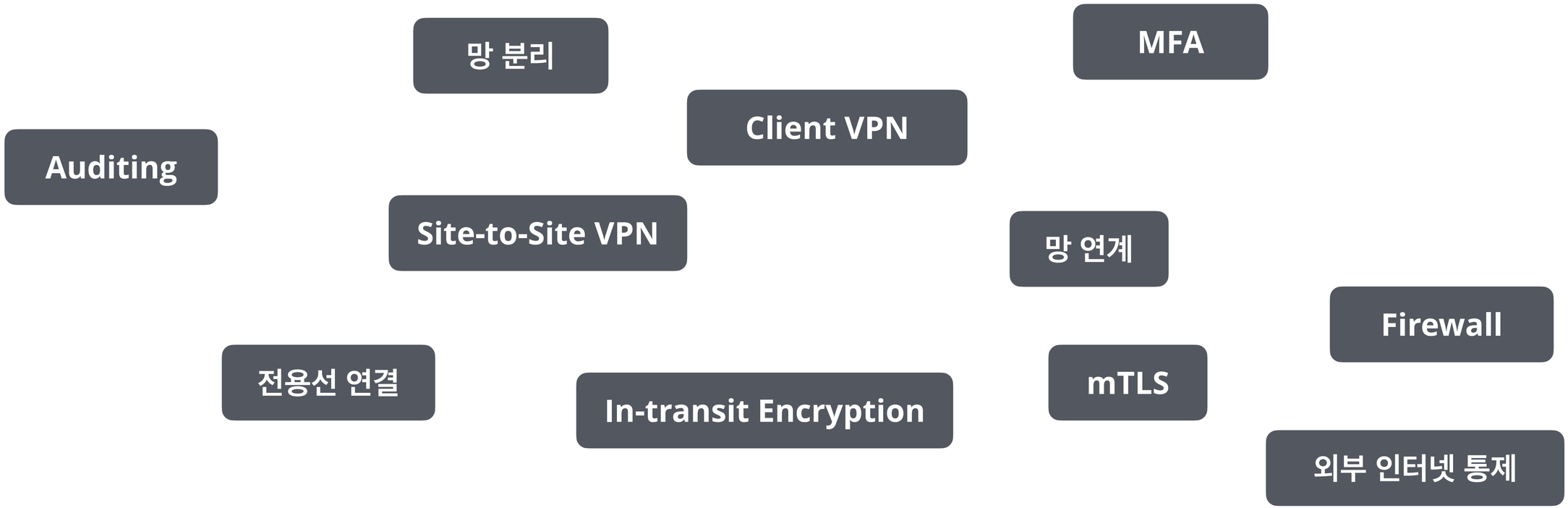
동네상권에서 당근페이 간편결제 제공

당근페이는 당근마켓과 별도 법인으로 전자금융 라이센스 취득 절차를 진행 중에 있어요.

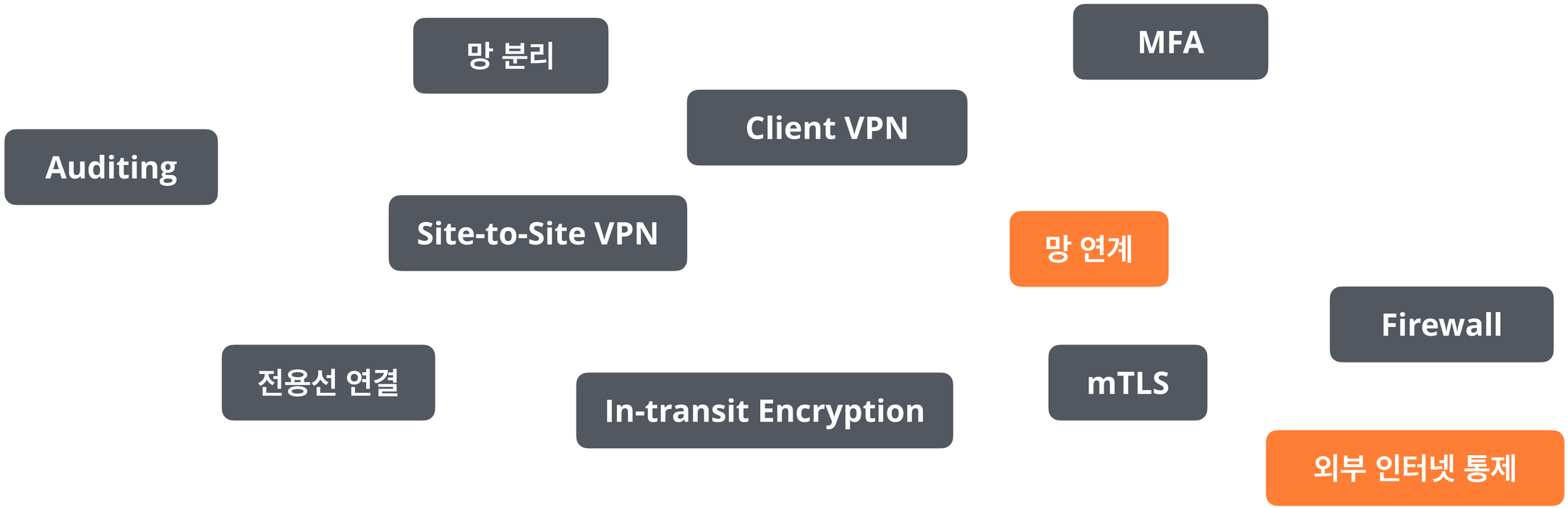
전자금융 서비스 운영에 AWS 클라우드를 사용하기위한 추가 절차 진행중

전자금융감독규정 및 금융권 클라우드 서비스 이용 가이드 등의 컴플라이언스 준수 필요

전자금융업의 네트워크 보안



전자금융업의 네트워크 보안



당근페이

AWS VPC 상의 망 연계 문제

목적에 따라 분리 된 여러 VPC를 어떻게 연결할 수 있을까?

개발자가 VPC의 Private 영역에 접근할 수 있도록 제공하려면?

AWS VPC에서 인터넷을 통하지 않고 S3, ECR, KMS 등의 서비스를 호출할 수 없을까?

사무실 네트워크와 AWS VPC를 안전하게 연결하고 싶은데?

대외기관과 시스템 연계를 해야하는데 어떻게 하지?

AWS VPC 상의 망 연계 문제

당근페이

목적에 따라 분리 된 여러 VPC를 어떻게 연결할 수 있을까?

개발자가 VPC의 Private 영역에 접근할 수 있도록 제공하려면?

AWS VPC에서 인터넷을 통하지 않고 S3, ECR, KMS 등의 서비스를 호출할 수 없을까?

사무실 네트워크와 AWS VPC를 안전하게 연결하고 싶은데?

대외기관과 시스템 연계를 해야하는데 어떻게 하지?

AWS PrivateLink !!

대외기관 시스템 연계 방법

AWS VPC <=> 온프레미스 상황인 경우

AWS Direct Connect / AWS Site-to-Site VPN / AWS Transit Gateway

Software VPN

AWS VPC <=> AWS VPC 상황인 경우

AWS VPC Peering / **AWS PrivateLink** / AWS Site-to-Site VPN / AWS Transit Gateway

Software VPN

concept

concept

AWS PrivateLink

당근페이

A highly available, scalable technology that enables you to privately connect your VPC to supported AWS services, services hosted by other AWS accounts (VPC endpoint services), and supported AWS Marketplace partner services.

AWS VPC와 대상 서비스 간 안전한 연결을 위한 기술

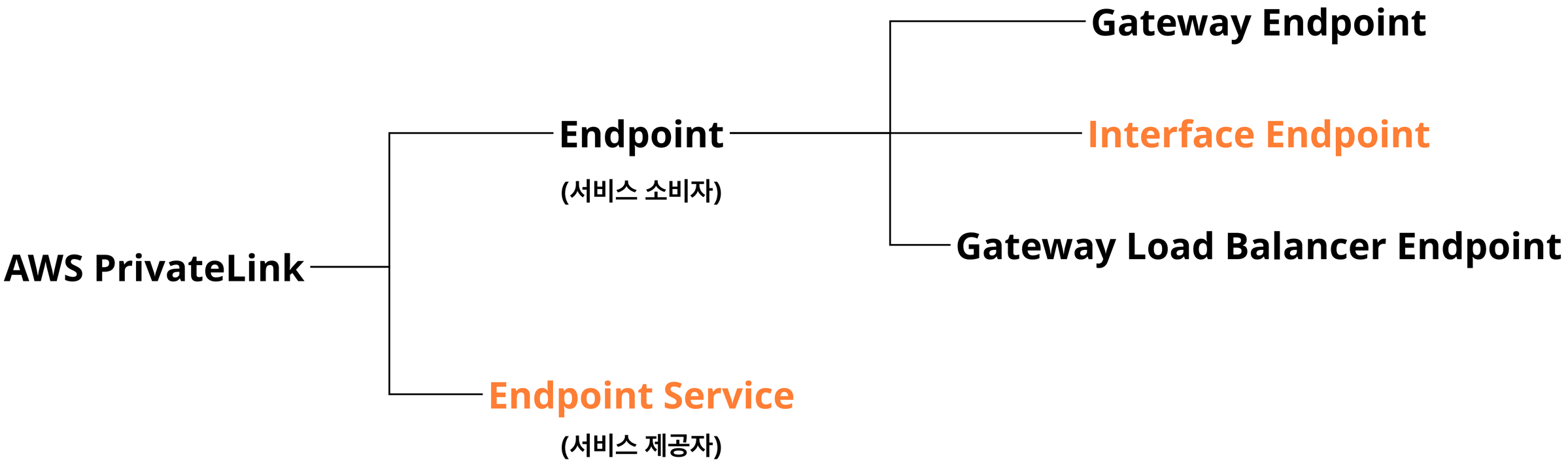
고가용성 (High Availability) 및 **확장성 (Scalability)** 제공

지원하는 대상 서비스

- AWS 서비스 (S3, ECR, KMS 등)
- 다른 AWS 계정 상에서 제공하는 서비스 (VPC Endpoint Service)
- AWS 마켓플레이스 상의 파트너 서비스

concept

PrivateLink 구성요소



게이트웨이 엔드포인트 (Gateway Endpoint)

라우팅 규칙을 통한 AWS 서비스에 사설 접근

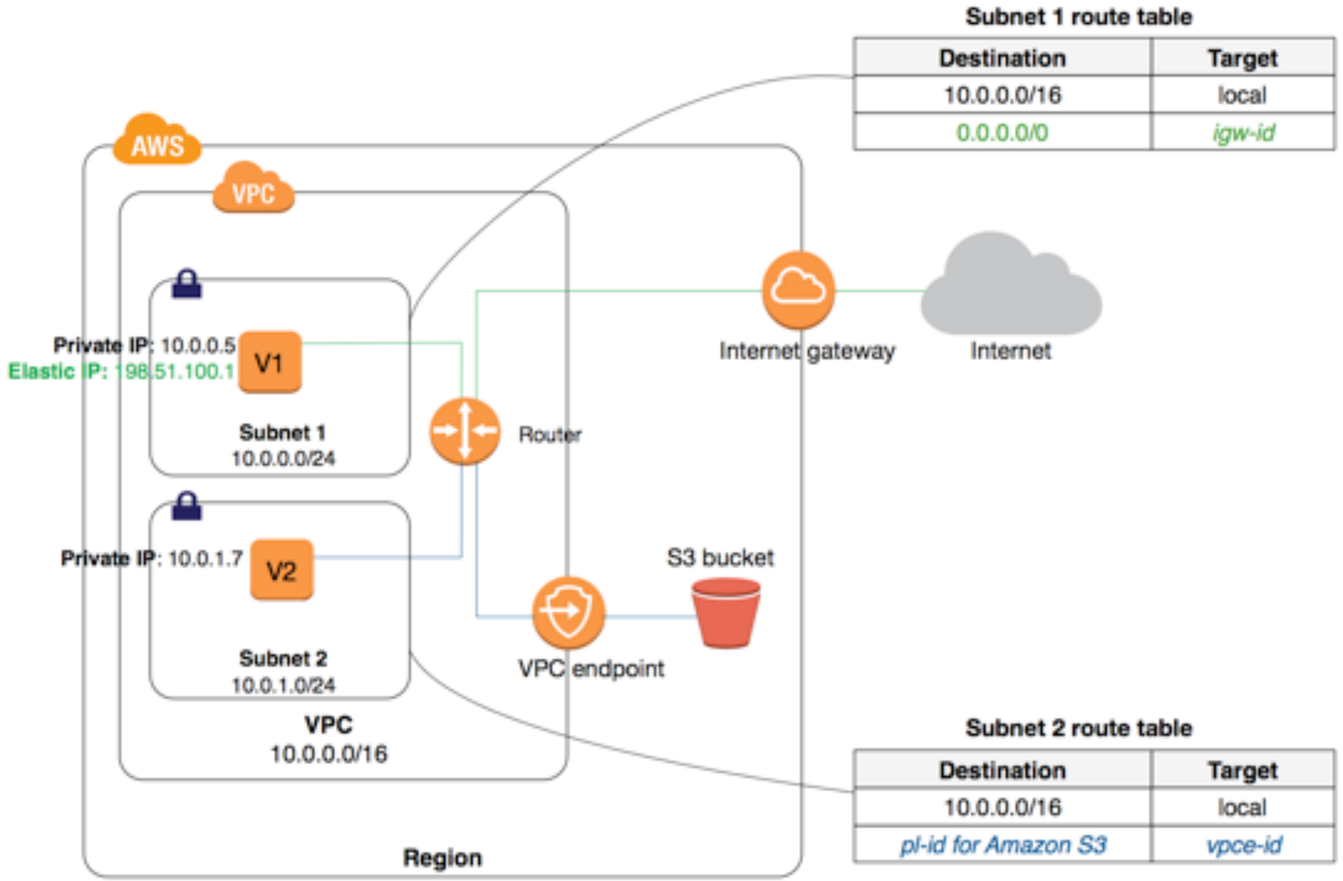
AWS Managed Prefix List를 이용하여 라우팅 규칙 관리
해당 라우팅 규칙이 적용된 서브넷에만 PrivateLink 적용

AWS S3 / DynamoDB 서비스만 지원

그외 서비스는 이용불가

리소스 정책을 통해 세밀한 접근제어 가능

엔드포인트 정책 / S3 버킷 정책 등 활용 가능



당근페이

인터페이스 엔드포인트 (Interface Endpoint)

네트워크 인터페이스를 통해 사설 IP 부여

대상 서비스에 대한 ENI를 원하는 서브넷에 생성 (Multi-AZ 지원)

엔드포인트 도메인 및 사설 도메인 지원

AZ 별 도메인 및 서비스 도메인 기본 제공 / 사설 도메인 (선택)

다양한 대상 서비스에 대해 이용 가능

90개 이상의 AWS 서비스 지원

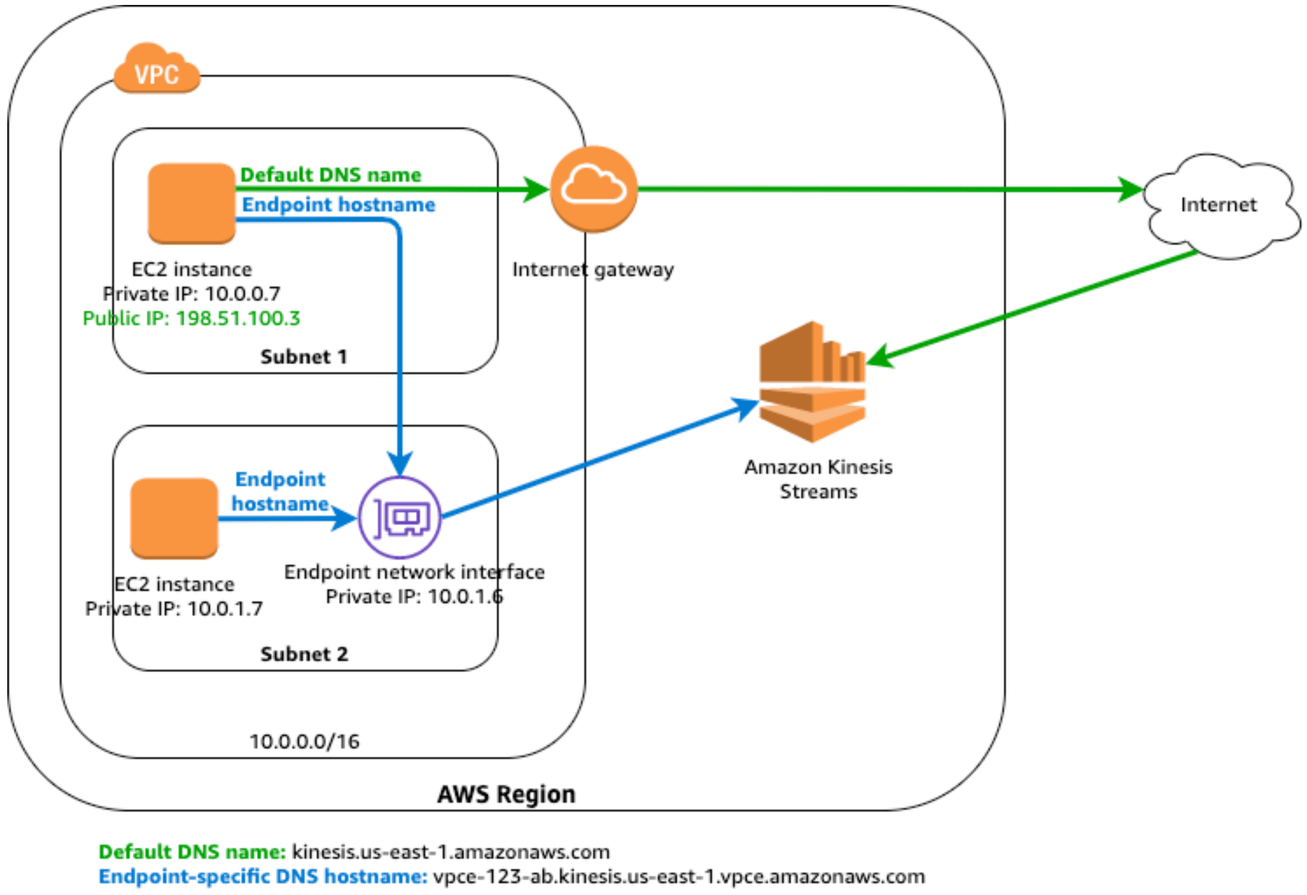
엔드포인트 서비스를 통해 다른 AWS 계정 서비스 연결 지원

AWS 마켓플레이스 서비스 지원

보안그룹과 NACL을 통해 세밀한 접근제어 가능

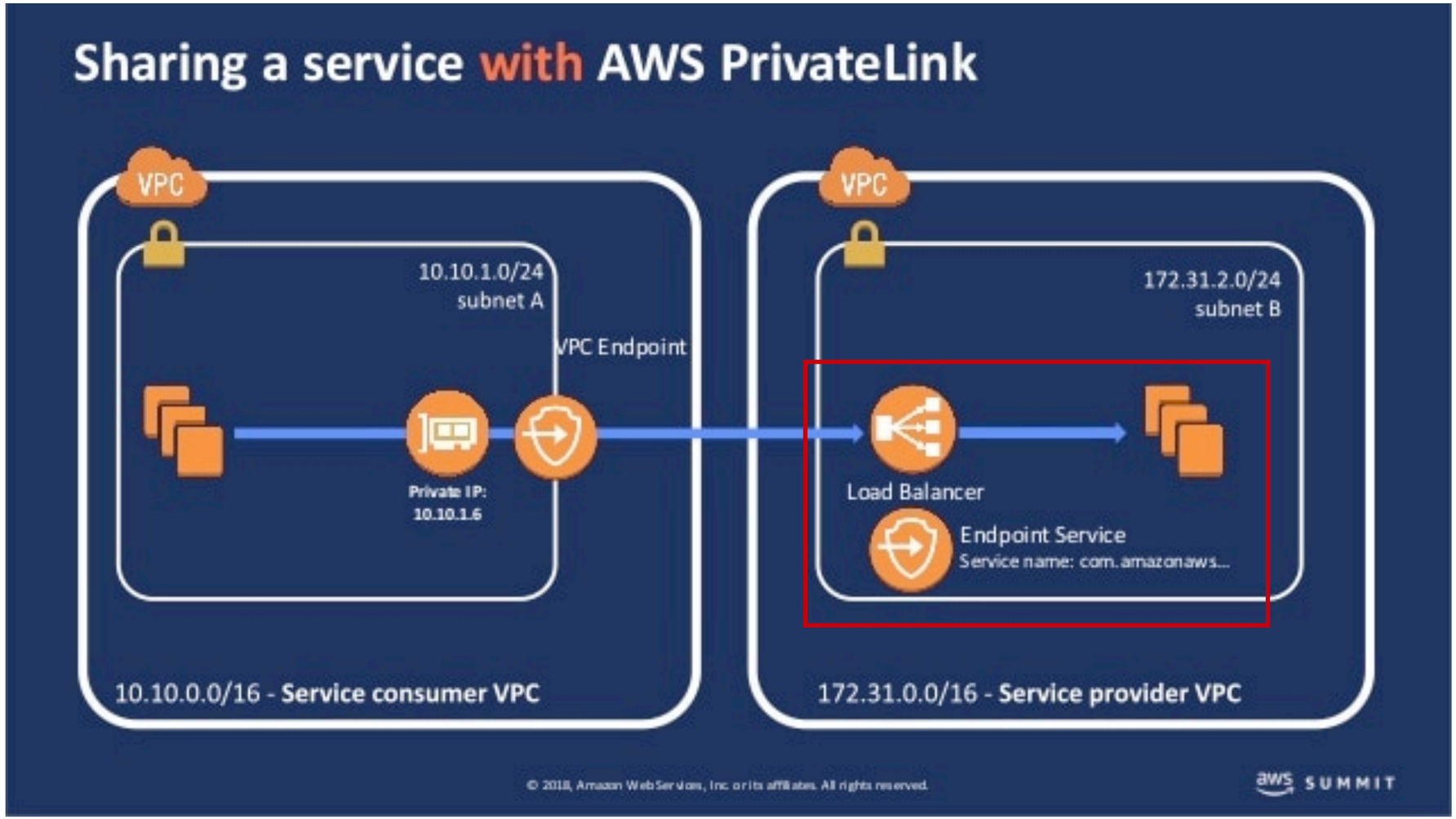
ENI의 보안그룹 및 해당 서브넷의 NACL을 통해 IP 접근제어

엔드포인트 리소스 정책은 특정 AWS 서비스들만 지원



concept

엔드포인트 서비스 (Endpoint Service)



당근페이

엔드포인트 서비스 (Endpoint Service)

다른 AWS 계정에게 서비스 제공 목적

서비스 제공자(Service Provider)

: **네트워크 로드밸런서(NLB)** 혹은 **게이트웨이 로드밸런서(GWLB)**에 대하여 엔드포인트 서비스 생성

서비스 소비자(Service Consumer) / Principal

: **인터페이스 엔드포인트** 혹은 **게이트웨이 로드밸런서 엔드포인트** 생성

사설 도메인 제공 가능

서비스 소비자가 PrivateDNS 기능을 활성화할 경우 해당 사설 도메인을 질의 가능

도메인 소유권 인증 필요

*.company.com 과 같은 와일드카드 도메인 허용

problem solving

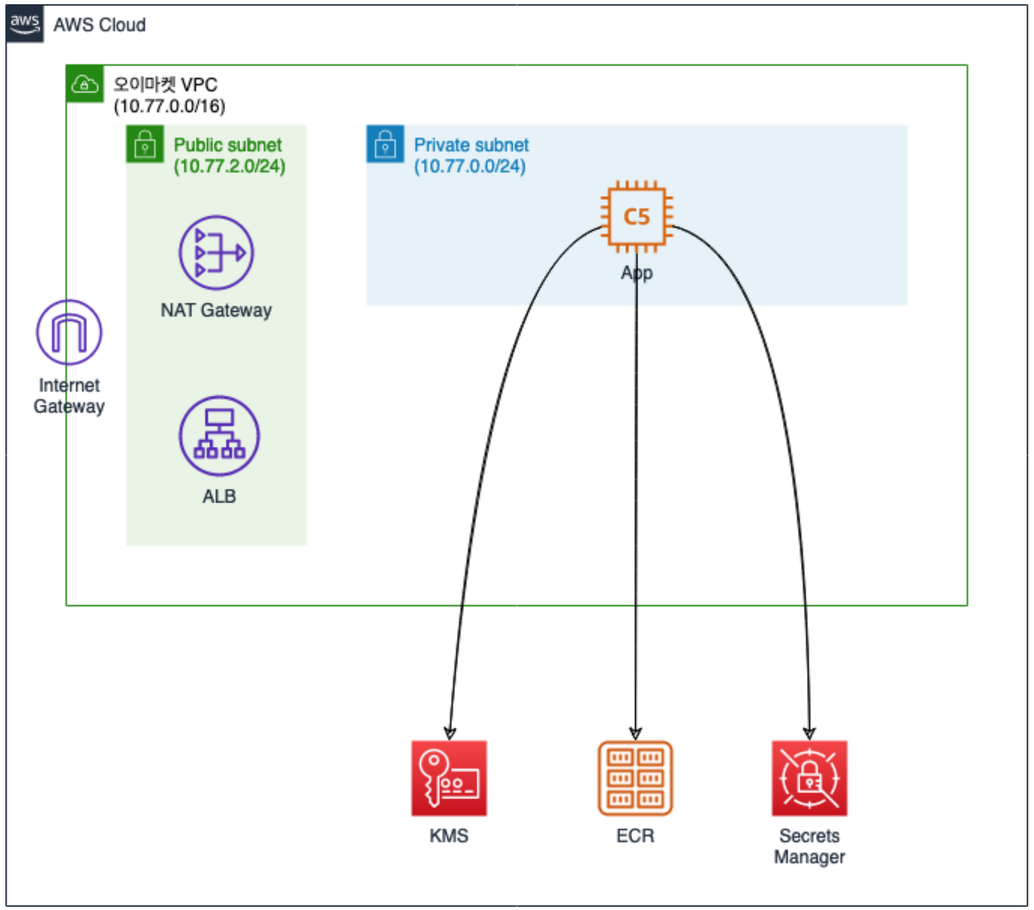
오이마켓 (예시)

당근페이

AWS에서 EC2 기반으로 서비스 운영중

서비스 워크로드는 Private 서브넷에서 운영

VPC 외부의 AWS 서비스(KMS, ECR, Secrets Manager) 이용중

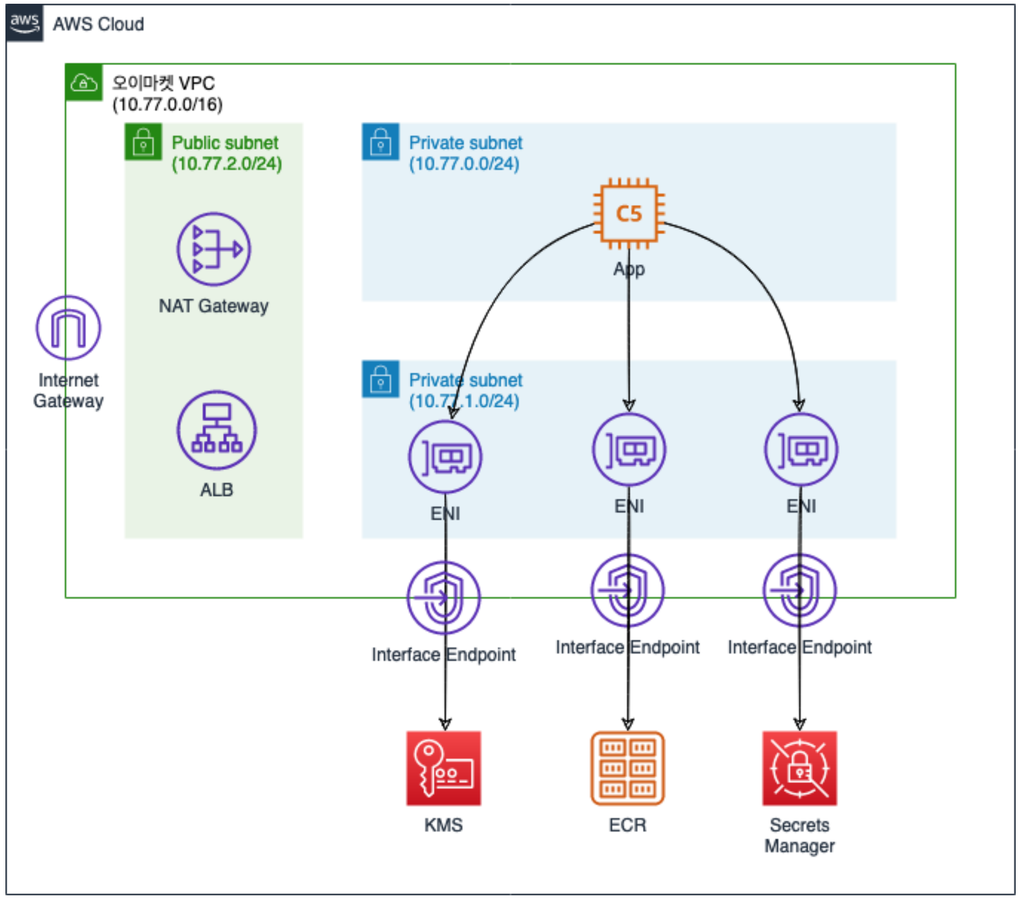


당근페이

1. VPC 상에서 AWS 서비스 통신 문제

"인터넷 망을 통하지 않고 AWS 서비스와 통신해야 합니다."

1. VPC 상에서 AWS 서비스 통신 문제



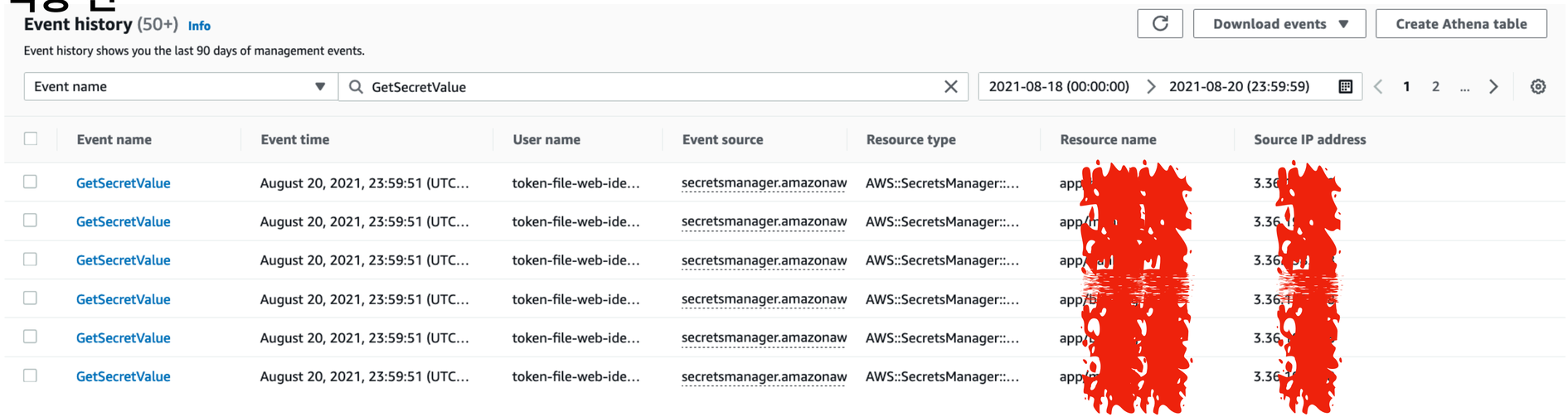
인터페이스 엔드포인트 생성

- AWS 서비스와의 통신이 NAT GW를 거치지 않고 사설 IP로 통신
- 게이트웨이 엔드포인트는 S3, DynamoDB에 대해서만 구성 가능
- 엔드포인트 생성 시 PrivateDNS 기능 활성화
  - PrivateDNS를 활성화하지 않으면 각 서비스(KMS, ECR 등)와 통신 시 엔드포인트 URL 지정 필요

```
$ aws secretsmanager list-secrets –endpoint-url https://vpce-xx.secretsmanager.us-west-2.vpce.amazonaws.com
```

1. VPC 상에서 AWS 서비스 통신 문제

PrivateLink 적용 전



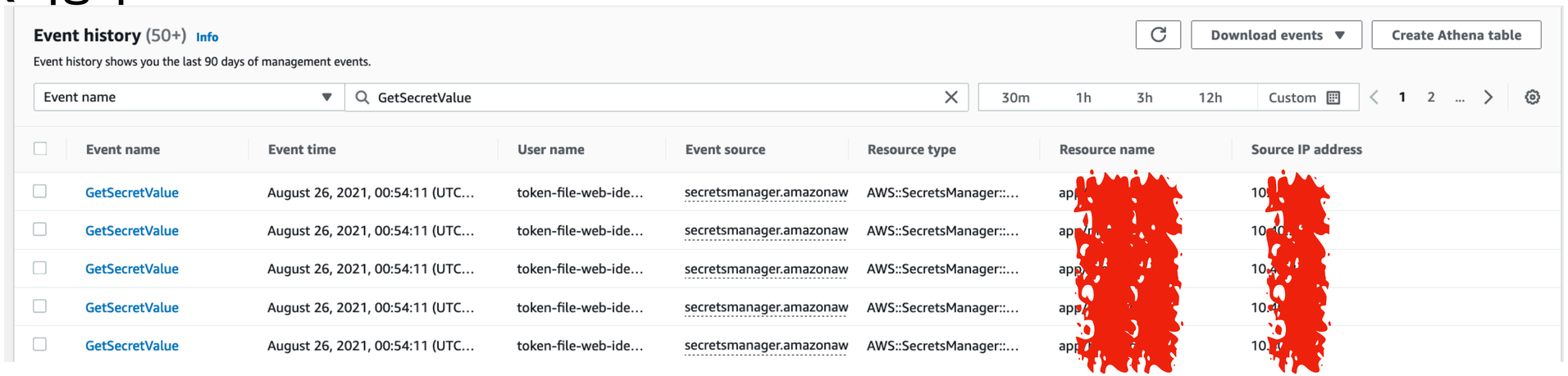
Event history (50+)

Event history shows you the last 90 days of management events.

Event name ▼ | GetSecretValue | 2021-08-18 (00:00:00) > 2021-08-20 (23:59:59)

☐	Event name	Event time	User name	Event source	Resource type	Resource name	Source IP address
☐	GetSecretValue	August 20, 2021, 23:59:51 (UTC...	token-file-web-ide...	secretsmanager.amazonaw	AWS::SecretsManager::...	[redacted]	[redacted]
☐	GetSecretValue	August 20, 2021, 23:59:51 (UTC...	token-file-web-ide...	secretsmanager.amazonaw	AWS::SecretsManager::...	[redacted]	[redacted]
☐	GetSecretValue	August 20, 2021, 23:59:51 (UTC...	token-file-web-ide...	secretsmanager.amazonaw	AWS::SecretsManager::...	[redacted]	[redacted]
☐	GetSecretValue	August 20, 2021, 23:59:51 (UTC...	token-file-web-ide...	secretsmanager.amazonaw	AWS::SecretsManager::...	[redacted]	[redacted]
☐	GetSecretValue	August 20, 2021, 23:59:51 (UTC...	token-file-web-ide...	secretsmanager.amazonaw	AWS::SecretsManager::...	[redacted]	[redacted]
☐	GetSecretValue	August 20, 2021, 23:59:51 (UTC...	token-file-web-ide...	secretsmanager.amazonaw	AWS::SecretsManager::...	[redacted]	[redacted]

PrivateLink 적용 후



Event history (50+)

Event history shows you the last 90 days of management events.

Event name ▼ | GetSecretValue

☐	Event name	Event time	User name	Event source	Resource type	Resource name	Source IP address
☐	GetSecretValue	August 26, 2021, 00:54:11 (UTC...	token-file-web-ide...	secretsmanager.amazonaw	AWS::SecretsManager::...	[redacted]	[redacted]
☐	GetSecretValue	August 26, 2021, 00:54:11 (UTC...	token-file-web-ide...	secretsmanager.amazonaw	AWS::SecretsManager::...	[redacted]	[redacted]
☐	GetSecretValue	August 26, 2021, 00:54:11 (UTC...	token-file-web-ide...	secretsmanager.amazonaw	AWS::SecretsManager::...	[redacted]	[redacted]
☐	GetSecretValue	August 26, 2021, 00:54:11 (UTC...	token-file-web-ide...	secretsmanager.amazonaw	AWS::SecretsManager::...	[redacted]	[redacted]
☐	GetSecretValue	August 26, 2021, 00:54:11 (UTC...	token-file-web-ide...	secretsmanager.amazonaw	AWS::SecretsManager::...	[redacted]	[redacted]

1. VPC 상에서 AWS 서비스 통신 문제

당근페이

```yaml
vpc_endpoints:
  interface:
  - name: "${vpc}-interface-aws-secrets-manager"
    service_name: "com.amazonaws.ap-northeast-2.secretsmanager"
    subnet_group: "net-private"
    security_groups:
    - endpoint-aws-secrets-manager
    private_dns_enabled: true
  - name: "${vpc}-interface-aws-kms"
    service_name: "com.amazonaws.ap-northeast-2.kms"
    subnet_group: "net-private"
    security_groups:
    - endpoint-aws-kms
    private_dns_enabled: true
```

```hcl
module "vpc_interface_endpoint" {
  source  = "[redacted]/vpc-interface-endpoint"
  version = "[redacted]"

  for_each = {
    for endpoint in local.config.vpc_endpoints.interface :
    endpoint.name => endpoint
  }

  name = each.key

  service_name       = each.value.service_name
  vpc_id             = module.vpc.id
  subnets            = [
    for subnet in try(module.subnet_group[each.value.subnet_group].subnets, []) :
    subnet.id if contains(try(each.value.availability_zone_ids, [subnet.availability_zone_id]), subnet.availability_zone_id)
  ]
  security_group_ids = [
    for security_group in each.value.security_groups :
    local.security_groups[security_group].id
  ]

  private_dns_enabled = try(each.value.private_dns_enabled, false)
  auto_accept         = try(each.value.auto_accept, true)

  notification_configurations = []

  tags = merge(
    local.workspace_tags,
  )
}
```

당근페이

2. AWS를 이용하는 대외기관과 시스템 연계

"대외기관의 API를 이용하고자 합니다. 해당 API는 민감한 데이터가 오가기 때문에 보안이 필요합니다.
만약 이곳도 AWS 상에 서비스를 운영중이라면?"

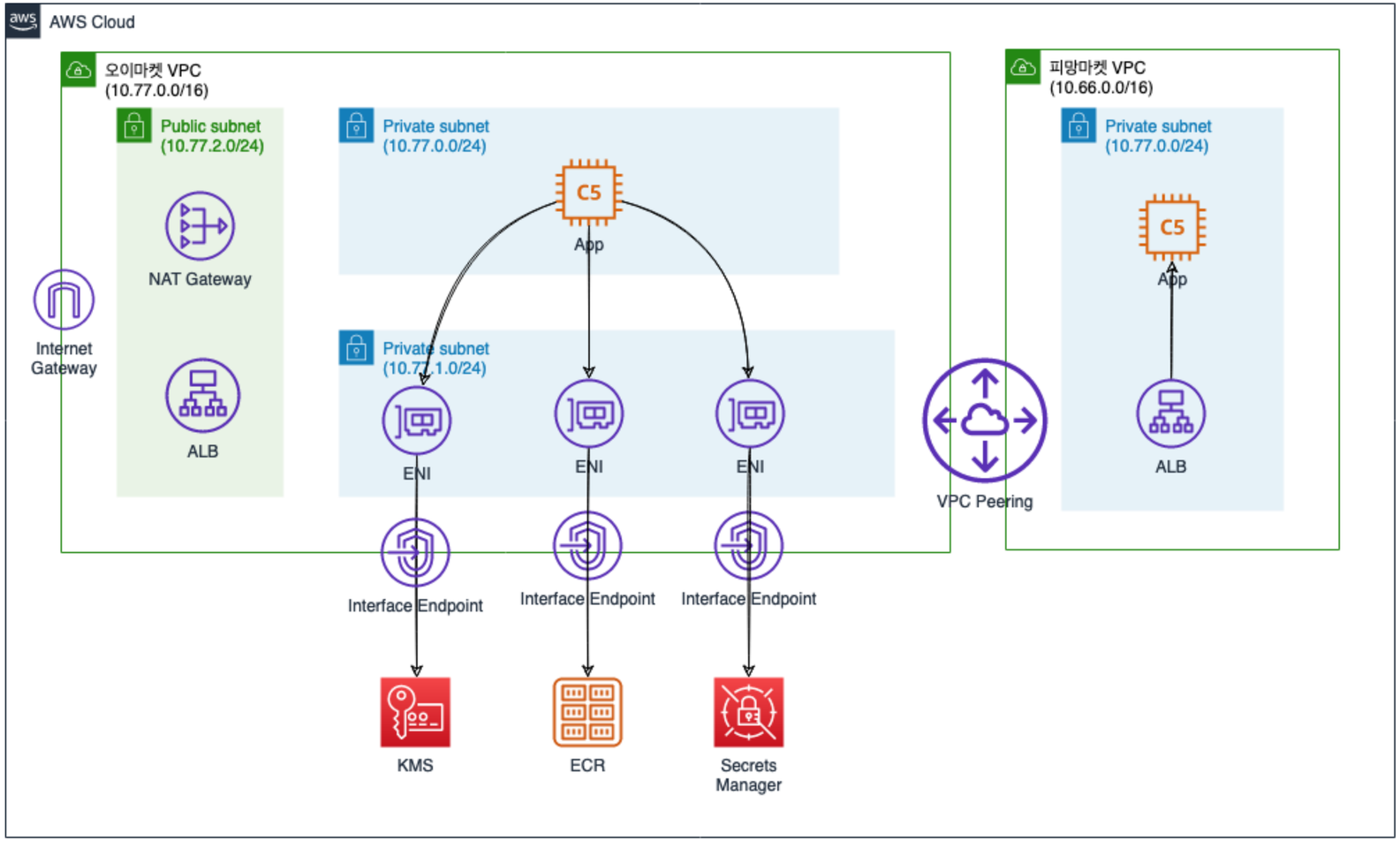
2. AWS를 이용하는 대외기관과 시스템 연계 (VPC Peering)

VPC 정보 노출

서브넷 단위의 연결

유동 IP 환경에서 접근제어가 까다로움

라우트 테이블 / NACL 관리 이슈

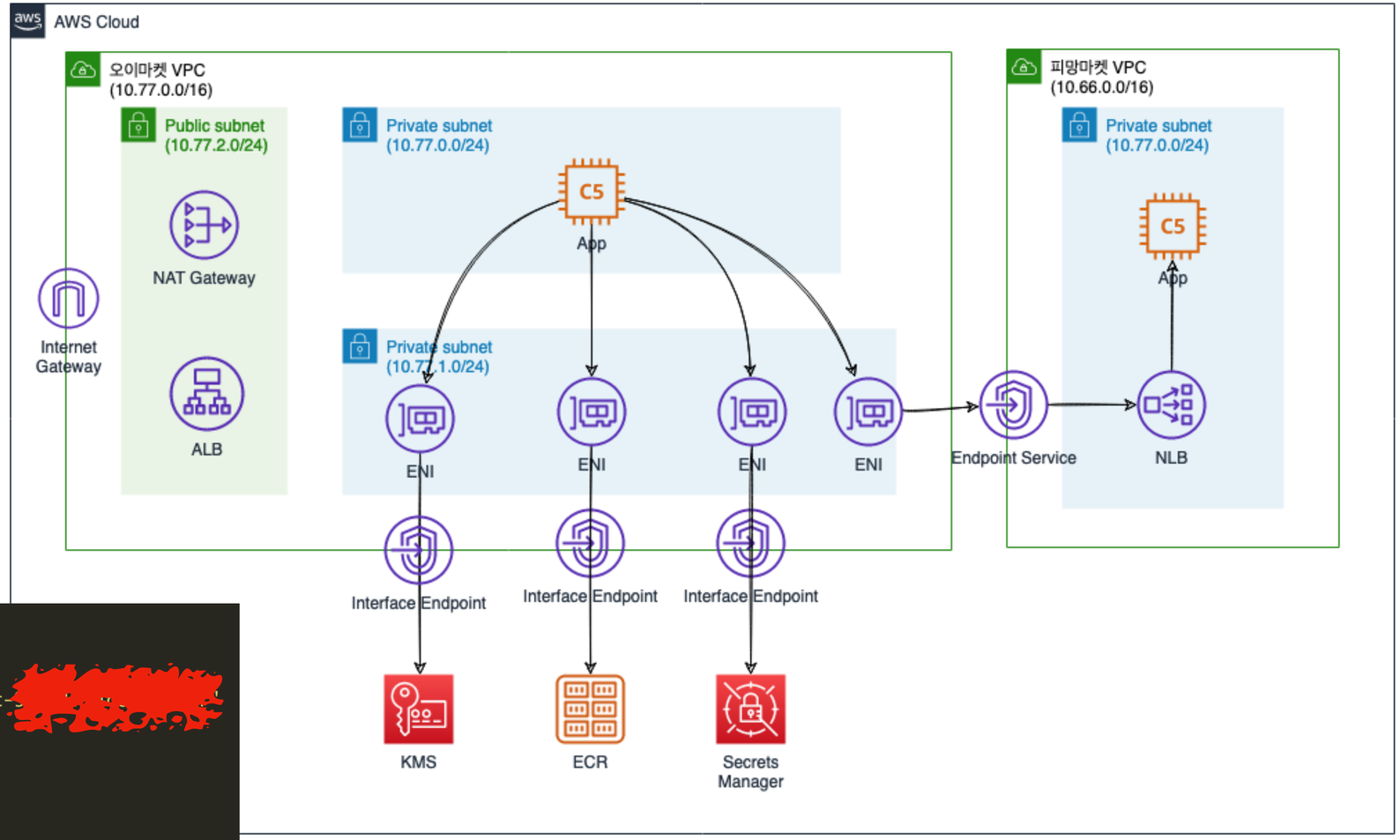


2. AWS를 이용하는 대외기관과 시스템 연계 (PrivateLink)

VPC 정보 노출하지 않음

생성된 ENI의 보안그룹을 통해 접근제어

라우트 테이블 / NACL 관리 이슈 없음




```
vpc_endpoints:
  interface:
  - name: "${vpc}-interface-pimang-api"
    service_name: "com.amazonaws.vpce.ap-northeast-2.vpce-svc-[redacted]"
    subnet_group: net-private-partner
    availability_zone_ids:
    - "${region}-az1"
    - "${region}-az2"
    security_groups:
    - endpoint-pimang-api
```

troubleshooting

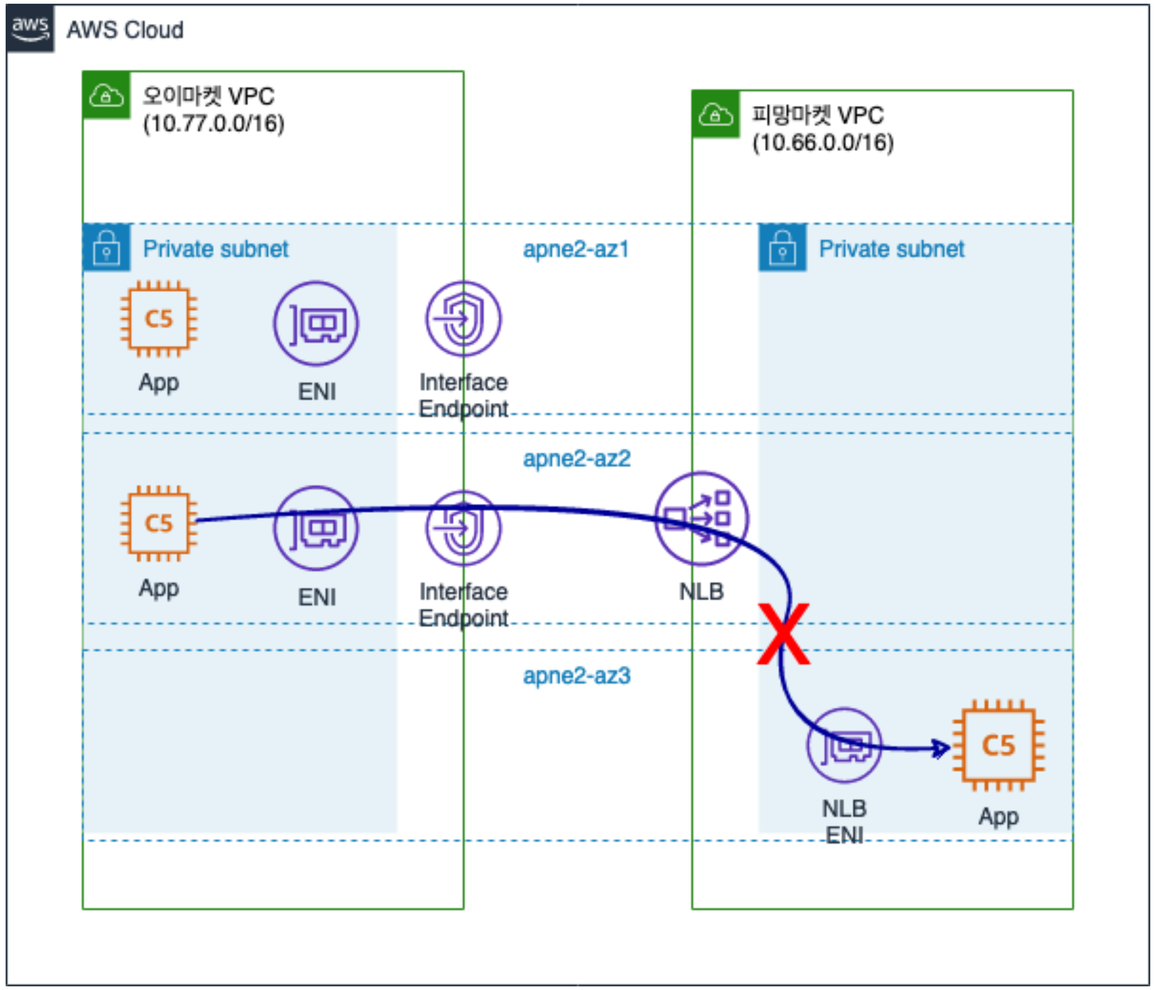
NLB Multi-AZ 이슈

서비스 제공자 AWS
az1 / az2 / az3 가용영역 사용
테스트용 워크로드를 ASG로 1대 구성하였으나 az3에 배포됨

서비스 소비자 AWS
az1 / az2 가용영역 사용

PrivateLink 서비스 제공자가 NLB의
Cross-zone Load Balancing 기능을 비활성화한 경우
서비스 제공자의 az3 워크로드에 트래픽이 전달되지 않아
Empty reply from server 오류 발생

=> 양측의 AZ를 사전에 잘 고려하거나, 크로스 존 기능 활성화 필요



troubleshooting

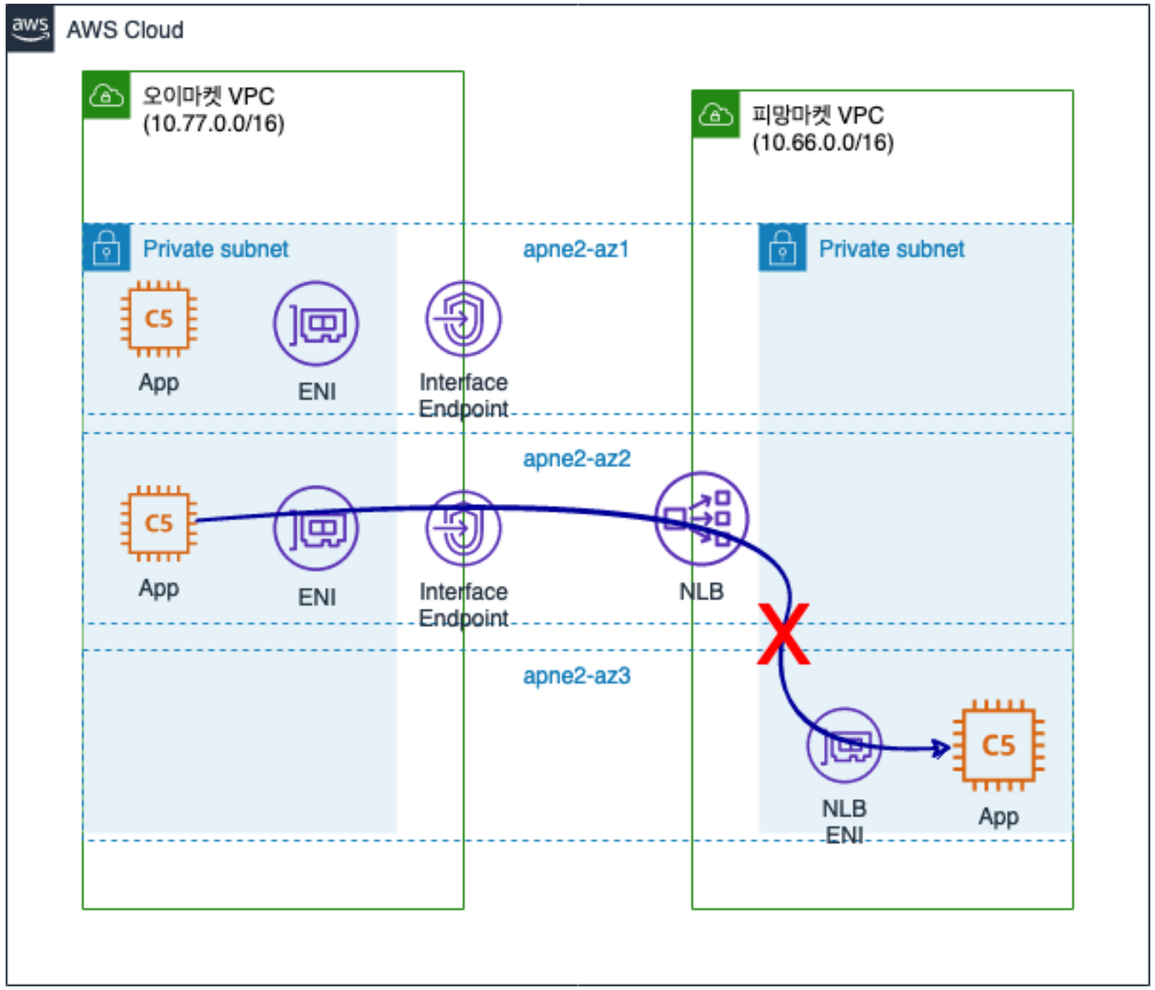
NLB Multi-AZ 이슈

당근페이

Attributes

Deletion protection	Disabled
Cross-zone load balancing	Enabled
Access logs	Disabled

Edit attributes



troubleshooting

여러 VPC 운영 시 이슈

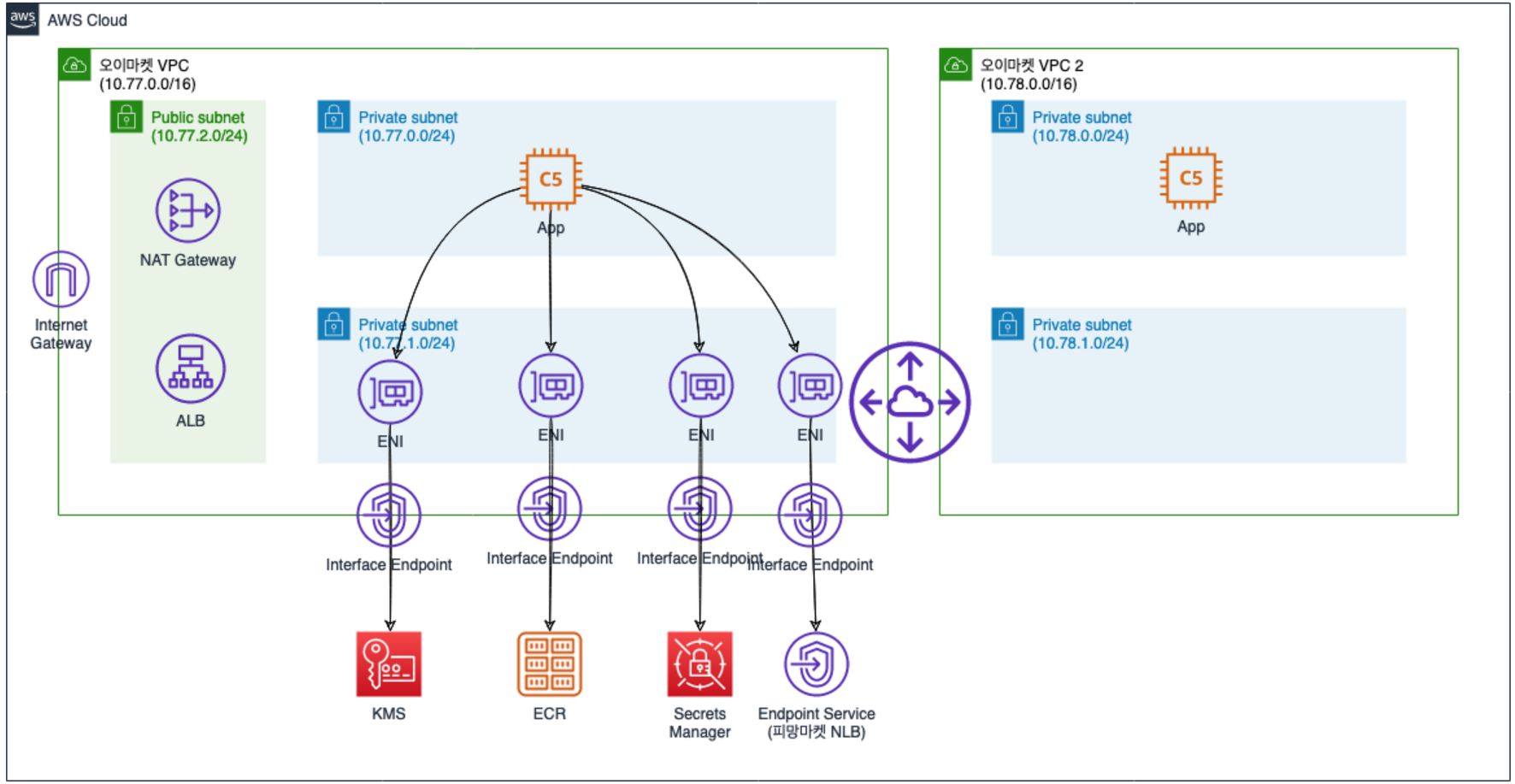
당근페이

"여러 VPC가 해당 서비스에 접근해야 한다면?"

여러 VPC 운영 시 이슈

당근페이

"VPC Peering으로 해결할 수 있지 않을까?"



troubleshooting

여러 VPC 운영 시 이슈

당근페이

"VPC Peering으로 해결할 수 있지 않을까?"

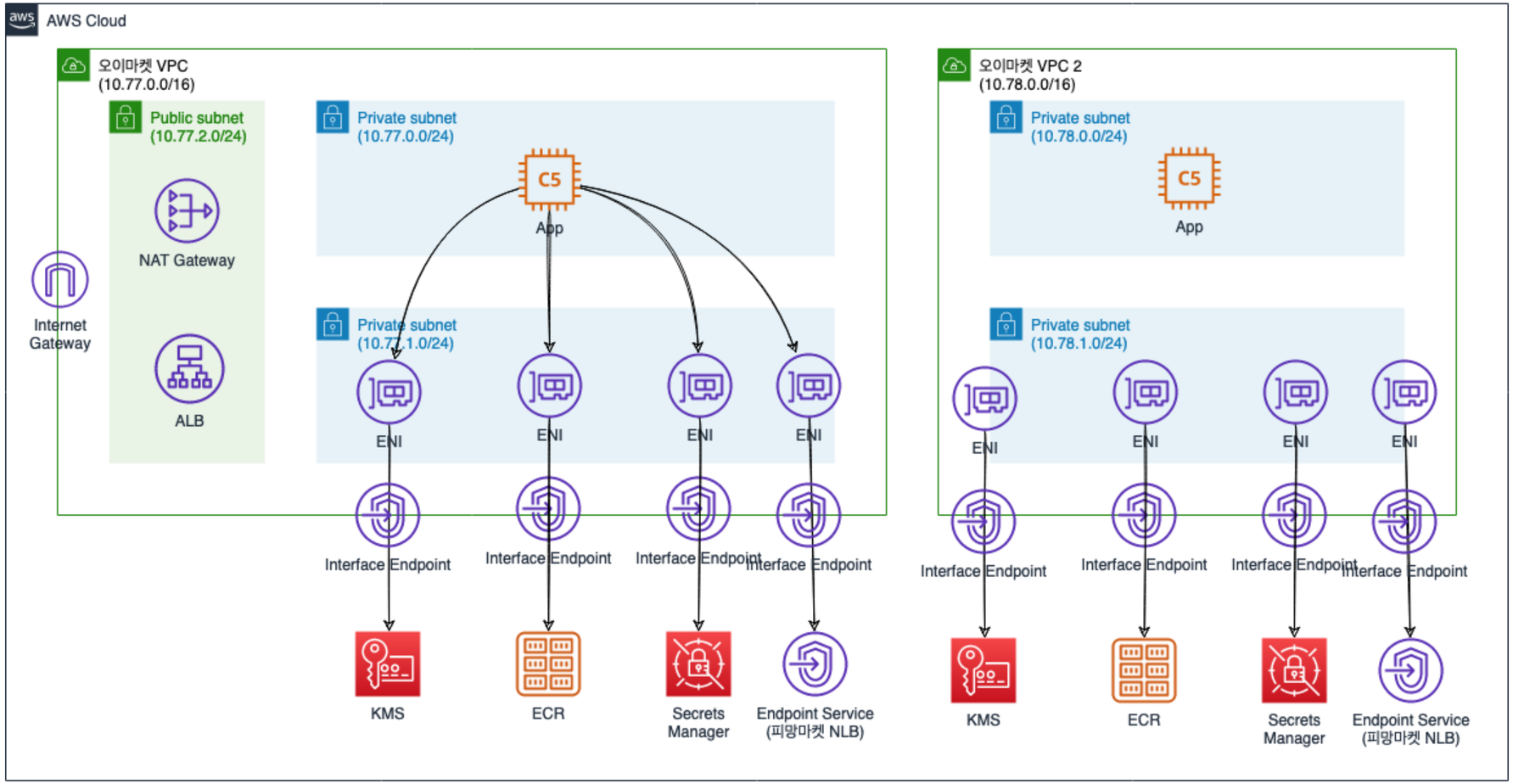
VPC에 ENI가 생성되어 VPC 사설 IP를 할당 받은 상태라 통신 가능
But, 인터페이스 엔드포인트가 제공하는 엔드포인트 도메인과 사설 도메인은 사용 불가

troubleshooting

여러 VPC 운영 시 이슈

당근페이

"그냥 각 VPC마다 중복으로 만들까?"



troubleshooting

여러 VPC 운영 시 이슈

당근페이

"그냥 각 VPC마다 중복으로 만들까?"

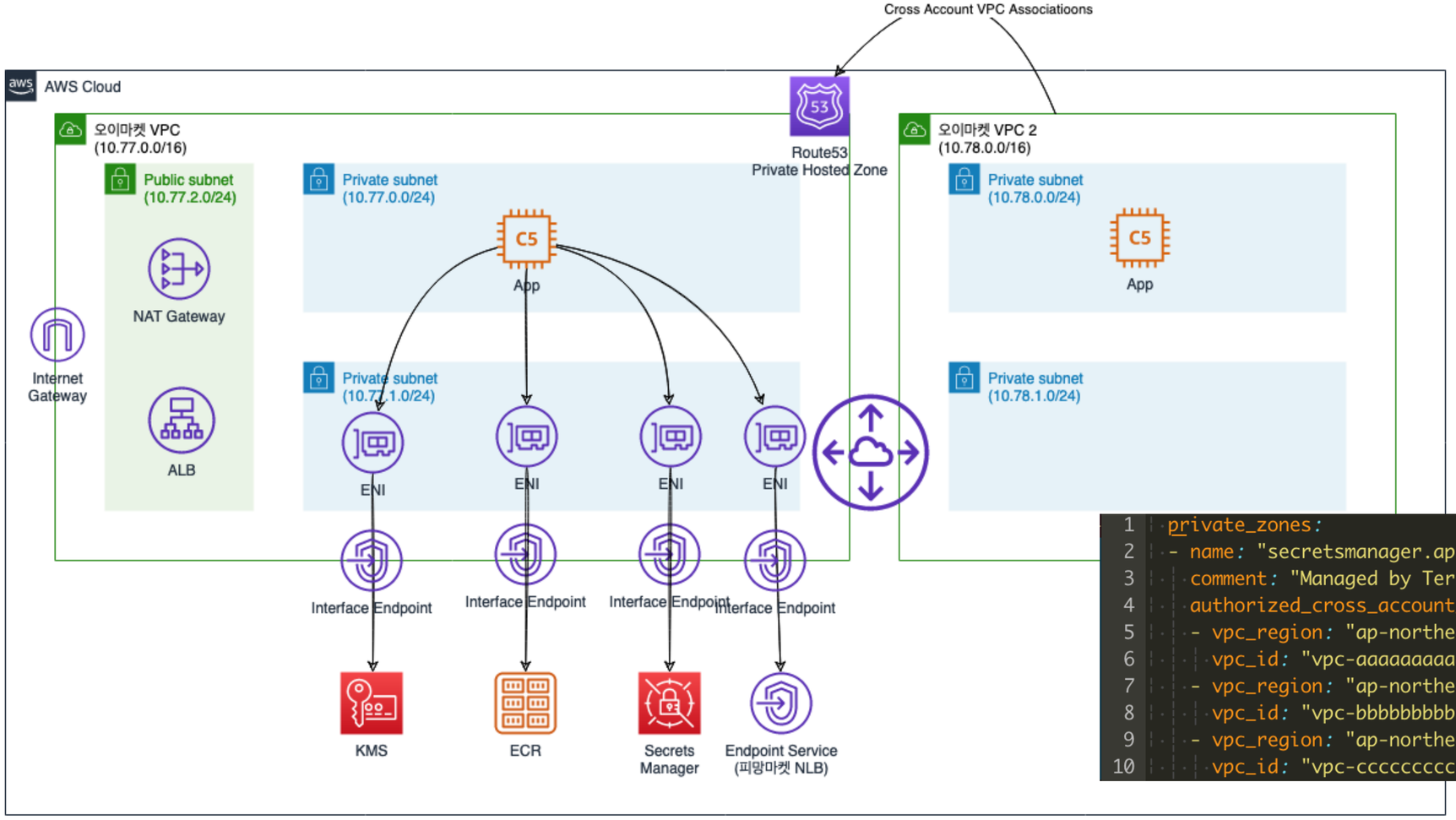
지금 당장 문제 해결은 가능
But, 새로운 VPC가 계속 만들어질 때마다 관리 부담 / 관리포인트가 많아져 확장성이 떨어짐

troubleshooting

여러 VPC 운영 시 이슈

당근페이

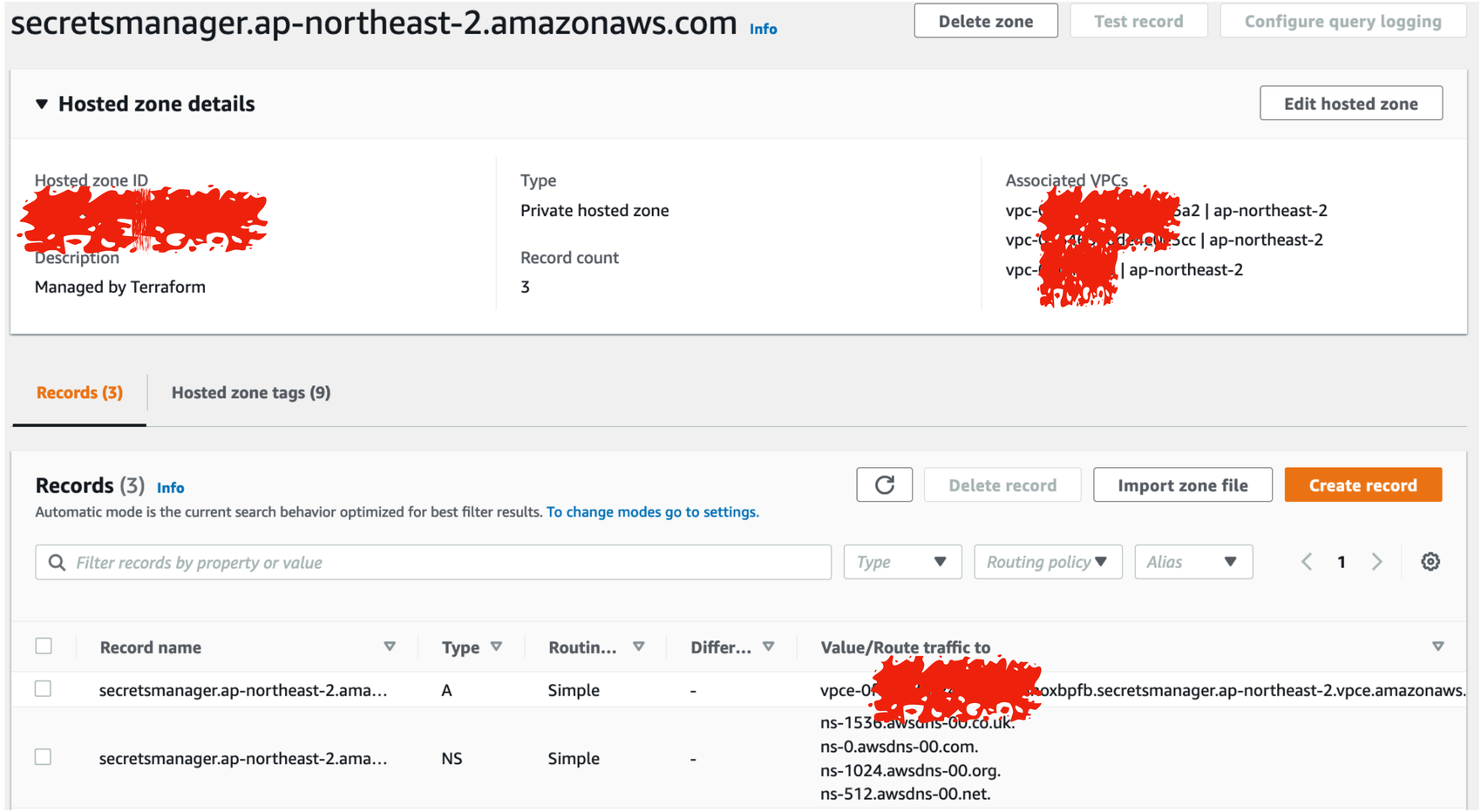
"PrivateDNS의 도메인명을 Route53 Private Hosted Zone을 이용해 직접 호스팅한다면?"




```
private_zones:
- name: "secretsmanager.ap-northeast-2.amazonaws.com"
  comment: "Managed by Terraform"
  authorized_cross_account_vpc_associations:
  - vpc_region: "ap-northeast-2"
    vpc_id: "vpc-aaaaaaaaaaaaaaaaa"
  - vpc_region: "ap-northeast-2"
    vpc_id: "vpc-bbbbbbbbbbbbbbbbb"
  - vpc_region: "ap-northeast-2"
    vpc_id: "vpc-ccccccccccccccccc"
```

여러 VPC 운영 시 이슈

"PrivateDNS의 도메인명을 Route53 Private Hosted Zone을 이용해 직접 호스팅한다면?"



온프레미스 도메인 질의 이슈

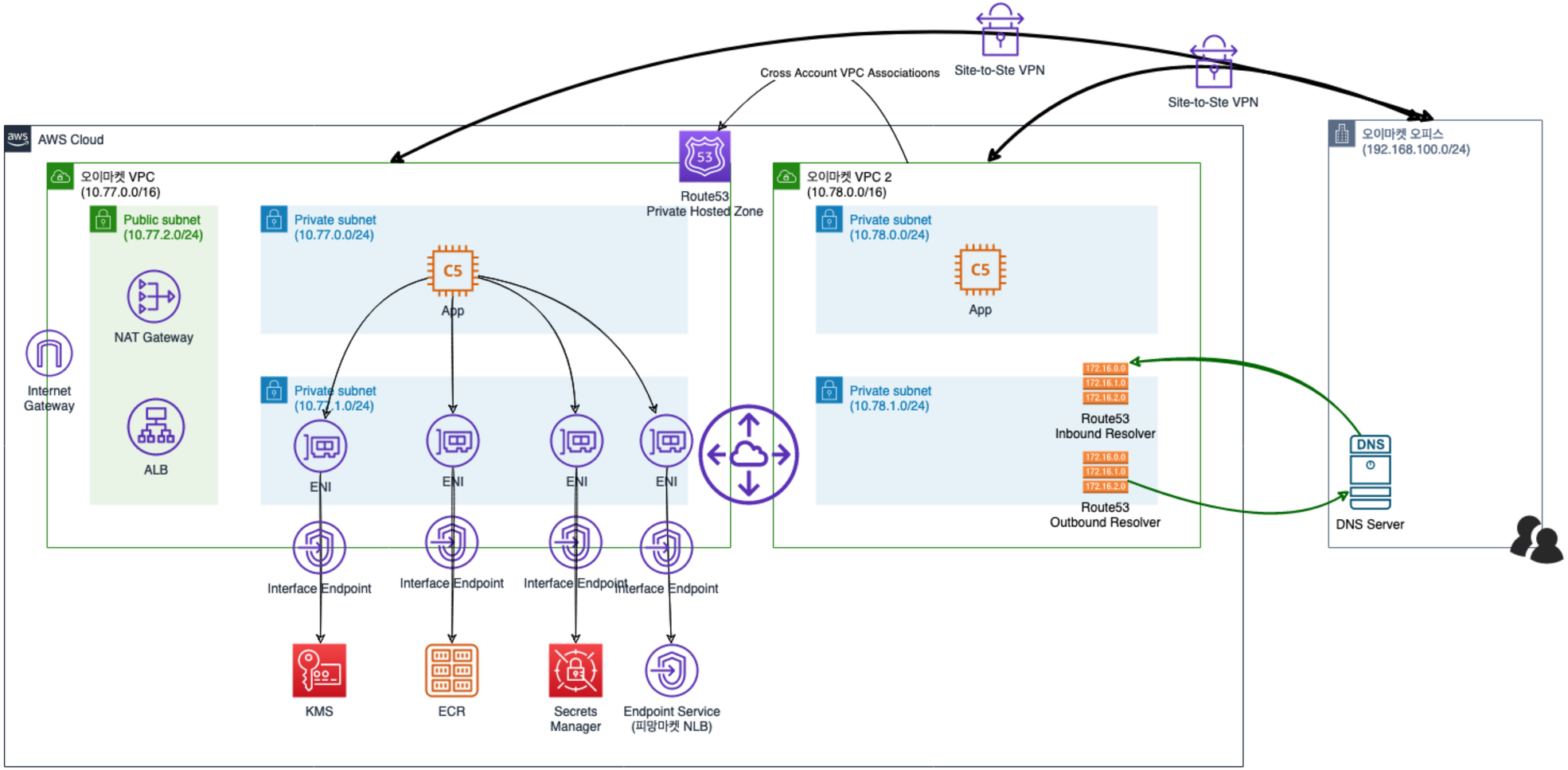
당근페이

"온프레미스 상에서도 도메인 접근이 필요하다면?"

troubleshooting

온프레미스 도메인 질의 이슈

"Route53의 Inbound Resolver를 통해 DNS 요청을 포워딩해보자!"



summary

세 줄 요약

당근페이

AWS PrivateLink를 사용하면 망 연계에 있어 안전하고 확장성 있는 네트워크 구성을 가져 갈 수 있어요.

AWS PrivateLink 서비스 제공자의 AZ 구성과 NLB Cross-zone Load Balancing 옵션을 주의해야 해요.

PrivateLink를 여러 VPC와 온프레미스에 통합 적용하고 싶다면 Route53 기능을 활용할 수 있어요.

마지막으로...

recruiting

당근페이의 초기 정예 멤버로 함께 할 개발자를 찾아요

우리는 이렇게 일해요

수평적인 소통 — 직급 X / 영어이름 / 신뢰와 충돌 / 투명한 정보 공유

자율과 책임 — 능동적 업무 수행 / 자율적 판단

즐겁게 성장 — 나보다 뛰어난 동료 / 팀 워크 / 즐거움

사용자 중심 사고 — 사용자 가치 최우선 / 사용자와 정서적 연결

혜택 및 복지

자유로운 휴가 / 유연 출퇴근 및 재택근무 / 식사 및 다양한 간식 제공

스탠딩 데스크 or 허먼밀러 의자 제공 / 도서 구매 및 교육비 지원

결제/정산팀 서버 개발자 (Java, Kotlin)

당근페이 간편결제 서비스 개발

머니팀 서버 개발자 (Java, Kotlin)

당근머니 및 유저 관리 서비스 개발

데브옵스 엔지니어(?)

4분기 채용 오픈 예정

자세한 내용은 daangn.team을 방문해주세요! :)

Byungjin Park · posquit0.com · posquit0

End of Document

Visit my AMA (https://github.com/posquit0/ama) for any question!