aws professional services

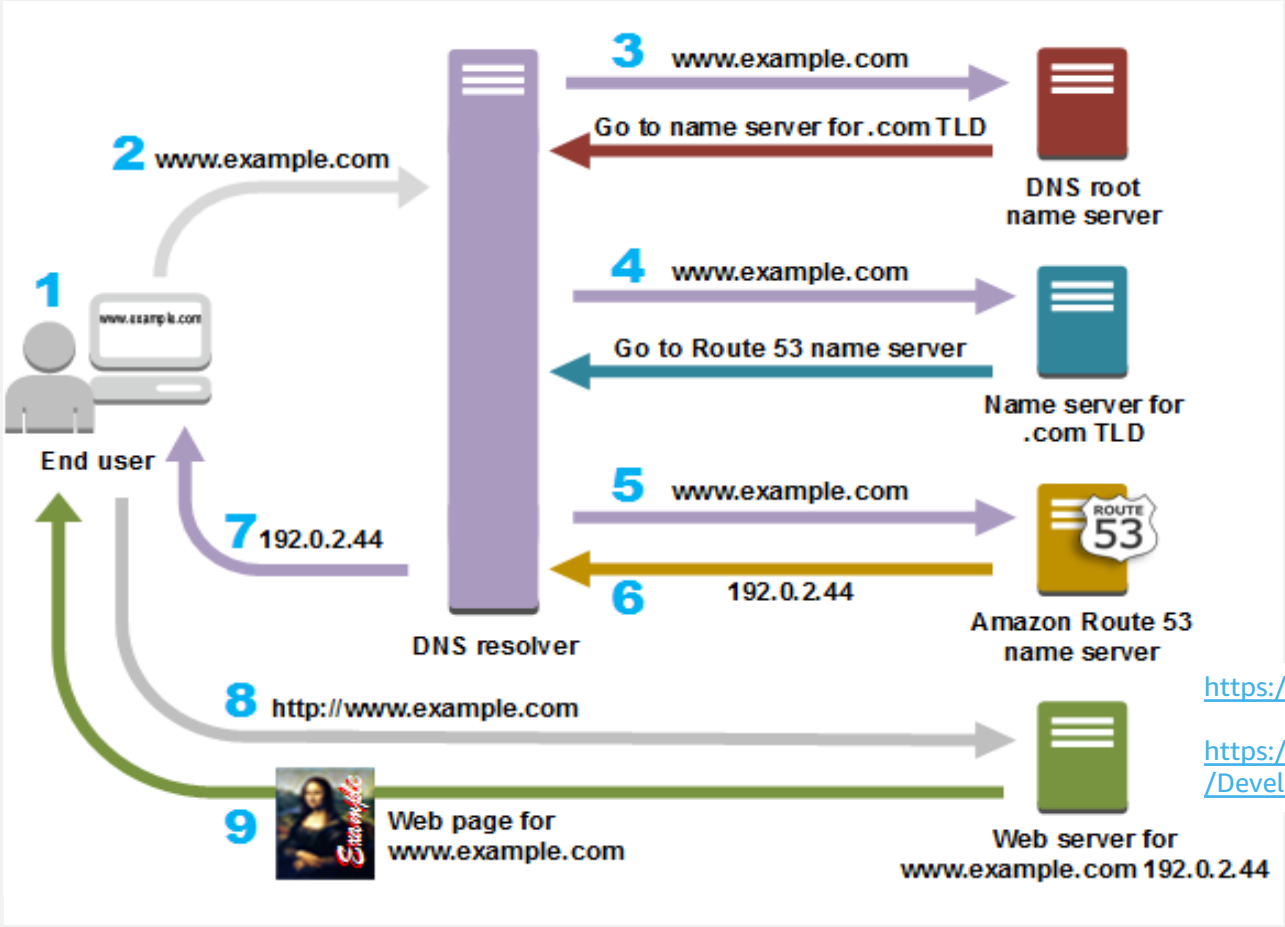
Route 53

ECSA PISAP

AWS Proserve

DNS (Domain Name System)

- DNS는 사람이 읽을 수 있는 도메인 이름 (예: www.example.com)을 컴퓨터가 읽을 수 있는 IP 주소 (예: 192.0.2.44)로 변환해주는 서비스



https://aws.amazon.com/ko/route53/what-is-dns/

https://docs.aws.amazon.com/ko_kr/Route53/latest/DeveloperGuide/welcome-dns-service.html

How DNS works?

```
➜  ~ dig +trace www.example.com

; <<>> DiG 9.10.6 <<>> +trace www.example.com
;; global options: +cmd
.                       66797   IN      NS      a.root-servers.net.
.                       66797   IN      NS      c.root-servers.net.
.                       66797   IN      NS      k.root-servers.net.
.                       66797   IN      NS      m.root-servers.net.
.                       66797   IN      NS      f.root-servers.net.
.                       66797   IN      NS      g.root-servers.net.
.                       66797   IN      NS      j.root-servers.net.
.                       66797   IN      NS      i.root-servers.net.
.                       66797   IN      NS      e.root-servers.net.
.                       66797   IN      NS      b.root-servers.net.
.                       66797   IN      NS      l.root-servers.net.
.                       66797   IN      NS      h.root-servers.net.
.                       66797   IN      NS      d.root-servers.net.
;; Received 228 bytes from 10.148.65.10#53(10.148.65.10) in 16 ms

com.                    172800  IN      NS      m.gtld-servers.net.
com.                    172800  IN      NS      k.gtld-servers.net.
com.                    172800  IN      NS      h.gtld-servers.net.
com.                    172800  IN      NS      b.gtld-servers.net.
com.                    172800  IN      NS      c.gtld-servers.net.
com.                    172800  IN      NS      g.gtld-servers.net.
com.                    172800  IN      NS      j.gtld-servers.net.
com.                    172800  IN      NS      d.gtld-servers.net.
com.                    172800  IN      NS      e.gtld-servers.net.
com.                    172800  IN      NS      i.gtld-servers.net.
com.                    172800  IN      NS      f.gtld-servers.net.
com.                    172800  IN      NS      a.gtld-servers.net.
com.                    172800  IN      NS      l.gtld-servers.net.
com.                    86400   IN      DS      30909 8 2 E2D3C916F6DEEAC73294E8268FB5885044A833FC5459588F4A9184CF C41A5766
com.                    86400   IN      RRSIG   DS 8 1 86400 20230806210000 20230724200000 11019 . kOWTGOfUKcyjkxoM4iTBG7uOizDFp066xEApmKdZt4nnuCl3Pbuc/b/J d0hGjojG
XA99Yl40try363c4QtefgGSwOPQFlrfyh46YPrMT4nAawYTE TZpavnO6Iy7+Y76qSBU0/O7+ZlalkYkp4DJZMDBZmGdqh8W17BVypwYy wpxlWjuq6oW0sX9d4xLu6DlG49/VTJAjfqHPxKtZhjJlArqMQ86h0z60 e
Jp7u86qCs6thhVSBe1MQ/IXYdeOwyvqrI93dl2+5GI8IjC+FVEYjBRF D1Cq3wml4MxfYVQXMnWRTdexWgiX6gQKjk5RBgKpkc06YHWGcZZVJbH5 eDmhEg==
;; Received 1178 bytes from 202.12.27.33#53(m.root-servers.net) in 21 ms

example.com.            172800  IN      NS      a.iana-servers.net.
example.com.            172800  IN      NS      b.iana-servers.net.
example.com.            86400   IN      DS      370 13 2 BE74359954660069D5C63D200C39F5603827D7DD02B56F120EE9F3A8 6764247C
example.com.            86400   IN      RRSIG   DS 8 2 86400 20230728061942 20230721050942 4459 com. TCKxlcmyloez3ZBOtvGKkZpan+xEhG9esV3LKht1yQmYId+7ODVRblDX uoTNHE
kWhItO9w7SuZ4cTybXCOJzEIFsFqSVTxQyZiQGlMbB5Ov23ywj fonPSg9y3dWGZ6DbCYnHxb/aJMS0b+ExwuXYRE5pGVweniAogQ4sWDX4 zsSEVAlk4zsgrEd0sgFARKpvFsDu7uXReUIufckprGBoqA==
;; Received 335 bytes from 192.42.93.30#53(g.gtld-servers.net) in 121 ms

www.example.com.        86400   IN      A       93.184.216.34
www.example.com.        86400   IN      RRSIG   A 13 3 86400 20230811224301 20230721104039 2061 example.com. aCsja3QGMlHPfA+n+DxDDUD0vj1+dueRXoe68INQrB6hLgTcg7ef07b
I 2NkbOIQS1lCL9WMZ2o+nAU4difyz6A==
;; Received 167 bytes from 199.43.135.53#53(a.iana-servers.net) in 256 ms
```

DNS Root Name Server로 질의

DNS Root Name Server에서 받은 응답

.com TLD(Top Level Domain) Name Server에서 받은 응답

최종 권한 Name Server(a.iana-server.net)에서 받은 응답

DNS 서비스 유형

- **Authoritative DNS (= 권한 있는 or 신뢰할 수 있는 DNS)**
  - 도메인에 대한 최종 권한이 있으며, 재귀적 DNS 서버에 IP 주소 정보가 담긴 답을 제공할 책임이 있음
  - **Amazon Route 53** 은 권한 있는 DNS에 해당됨

- **Recursive DNS (= 재귀적 DNS)**
  - 대개 클라이언트는 권한 있는 DNS 서비스에 직접 쿼리를 수행하지 않으며, 대신에 해석기 또는 재귀적 DNS 서비스에 연결하는 것이 일반적임
  - DNS 레코드를 소유하지는 않으나, 사용자를 대신하여 DNS 정보를 가져오는 중개자 역할을 함
  - 캐시된 DNS 정보가 있는 경우, DNS 쿼리의 응답으로 소스 또는 IP 정보를 제공함
  - 캐시된 DNS 정보가 없는 경우, 정보를 찾기 위해 쿼리를 하나 이상의 권한 있는 DNS 서버에 전달

DNS 레코드 유형

유형	설명	기능
A	IPv4 주소 레코드	호스트 이름을 호스트의 IP 주소에 매핑 시 일반적으로 사용되는 32비트 IPv4 주소를 반환
AAAA	IPv6 주소 레코드	호스트 이름을 호스트의 IP 주소에 매핑 시 일반적으로 사용되는 128비트 IPv6 주소를 반환
CNAME	별칭 레코드	하나의 도메인을 다른 도메인으로 연결: 새로운 이름으로 조회를 다시 시도하여 DNS 조회
NS	네임 서버 레코드	호스팅 영역에 대한 권한 있는 이름 서버를 식별 (실제 DNS 레코드를 갖고 있는 서버)
SOA	권한 시작 레코드	DNS 영역에 대한 중요한 정보를 저장: 주 DNS 서버, 도메인 관리자 이메일, 도메인 일련번호, 도메인 업데이트 시간 등

https://docs.aws.amazon.com/ko_kr/Route53/latest/DeveloperGuide/ResourceRecordTypes.html
https://en.wikipedia.org/wiki/List_of_DNS_record_types

Route 53

Amazon Route 53

AWS 관리형 DNS 서비스

- 도메인 등록 대행
- 도메인 이름 확인
- 100% 가용성 SLA
- 글로벌 라우팅 및 정책
  - Health Checks (customer define)
  - DNS Failover
  - Latency Based Routing
  - Geo Based Routing
  - Weighted Round Robin
- 퍼블릭 및 프라이빗 DNS 호스팅 영역 제공

Route53

HostedZone

Route53 Resolver endpoint

Amazon Route 53 Feature

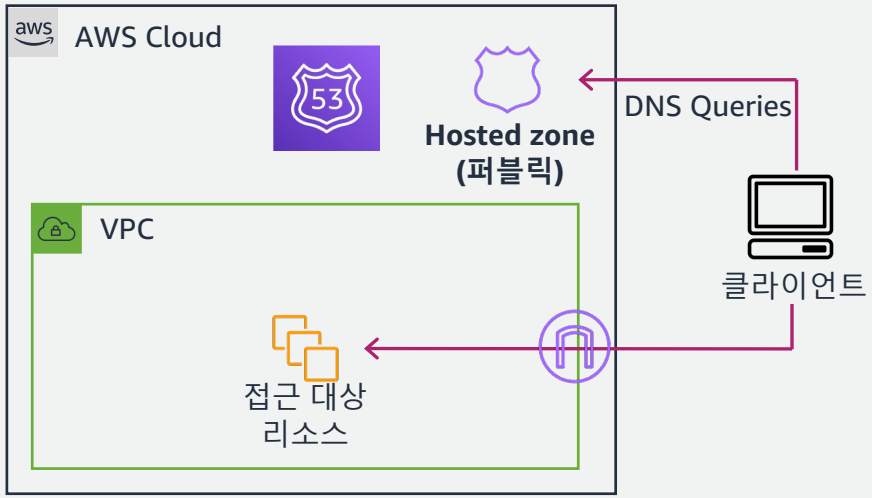
AWS 관리형 DNS 서비스

- Public / Private DNS
- Global Traffic flow
- Route 53 Resolver
- Route 53 Resolver DNS Firewall
- Route 53 Application Recovery Controller
- Health Check & Monitoring
- Domain Registrar (도메인 등록 지원)
- DNSSEC 지원
  (* DNS 트래픽 보호를 위한 프로토콜)

AWS Route 53 퍼블릭 vs 프라이빗 DNS 비교

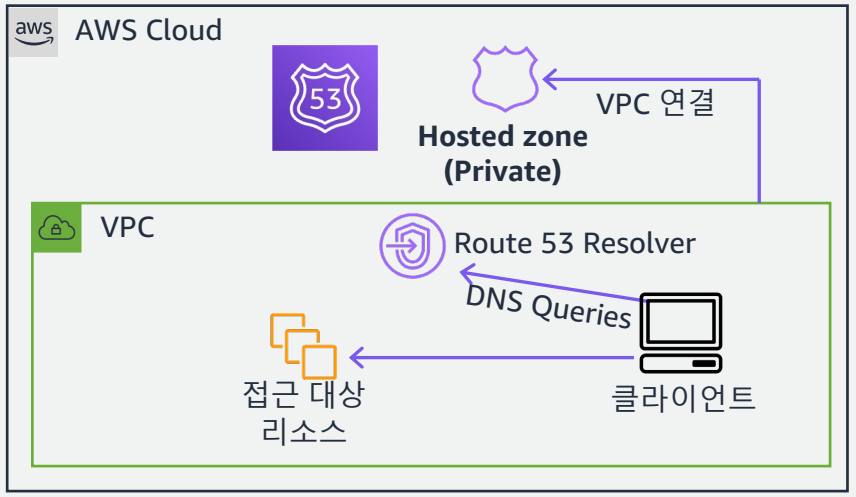
Public Hosted Zones

- Public Domain (도메인 네임 등록)
- 인터넷에서 도메인 정보 해석을 위해 사용
- 인터넷 연결 가능한 리소스로 라우팅
- 글로벌 라우팅 정책 적용



Private Hosted Zones

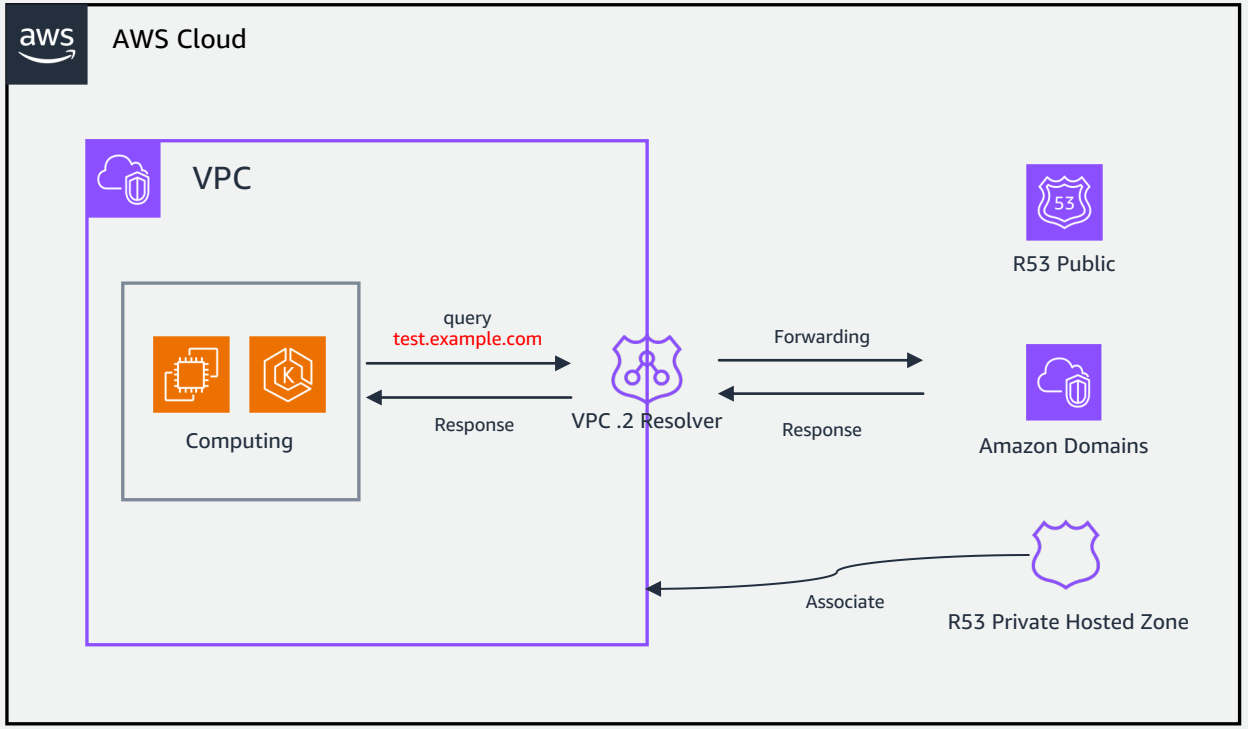
- Private Domain
- VPC 내부 도메인 정보 해석을 위해 사용
- VPC 내부 리소스로 라우팅
- On-premise 사설망과 통합 가능
  (R53 Resolver 엔드포인트, 전달 규칙 이용)



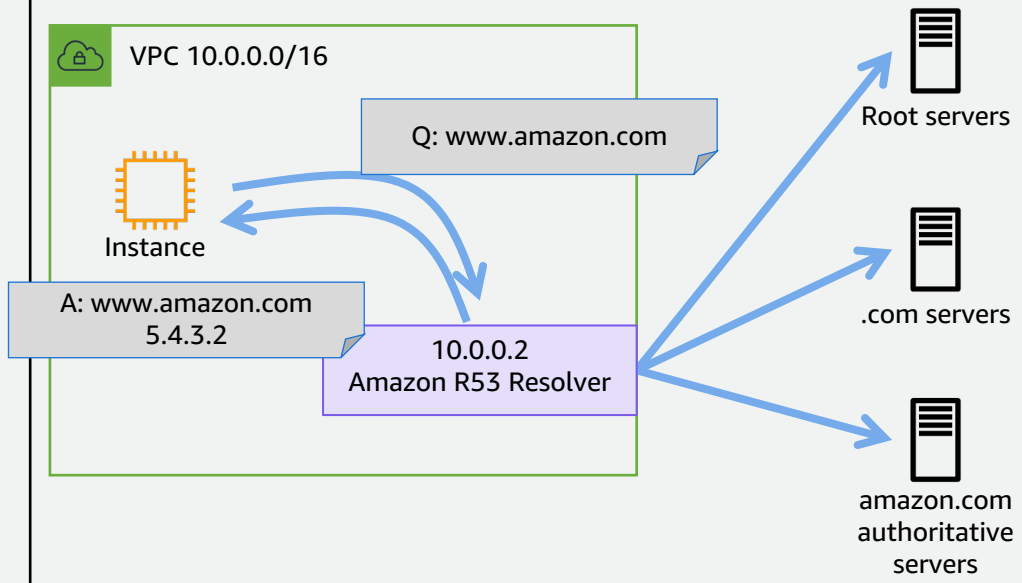
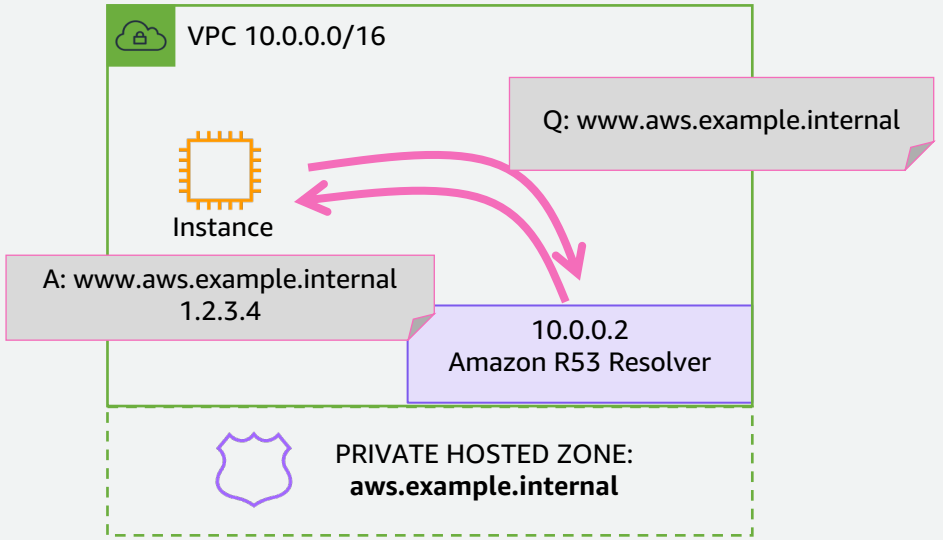
Route 53 Resolver

- Public 레코드, VPC별 DNS 이름, Amazon Route 53 프라이빗 호스팅 영역에 관한 AWS 리소스에 대해서 **DNS 쿼리에 재귀적 응답 제공**
- Route 53 Resolver는 아래 이름으로도 부름:
  - AmazonProvidedDNS
  - VPC Resolver
  - VPC + 2 Resolver
  - **.2 Resolver**

- 모든 VPC에서 기본적으로 사용 가능
- VPC 외부에서는 접근 불가
  (필요 시 Resolver 엔드포인트 사용)



Amazon VPC에서의 DNS 해석 흐름

구분	Public Hosted Zone	Private Hosted Zone
구성도		
특징	• VPC의 Internet Gateway 와 무관 • 기존 도메인 Migration 가능 (기존 호스팅 업체 NS서버 변경 작업) • Sub-Domain 생성 및 권한 위임 가능	• VPC 내부에서만 쿼리 응답 가능 • Public Hosted Zone이 동일하게 존재하는 경우, 응답 처리의 우선 순위 1) Private Hosted Zone > Public Zone 2) more-specific zone

Hybrid DNS

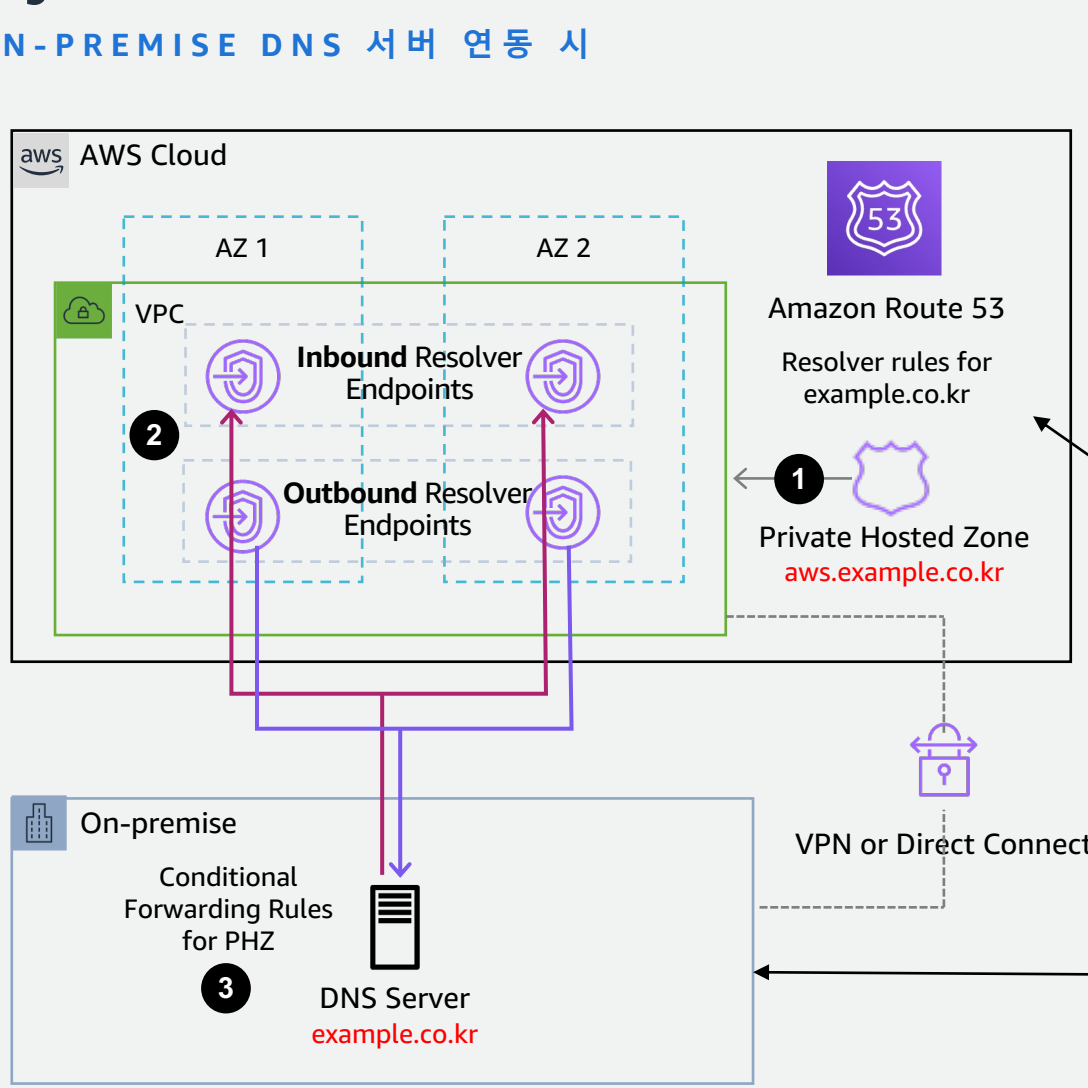
Hybrid DNS on AWS

- AWS와 On-premise를 같이 운영하는 고객사에서 DNS를 Hybrid로 구성하여 사용하고자 하는 경우
- 하이브리드 형태로 운영 시
  - 고객사 IDC 에서 AWS의 일부 도메인 쿼리에 대한 응답을 AWS PHZ로 포워딩 (Inbound)
  - AWS 환경에서 일부 도메인 쿼리에 대한 응답을 Internal DNS로 포워딩 (Outbound)

- Cons : On-premise에서 Resolver 역할의 리소스가 필요, DNS 다중 관리 필요 (On-premise Internal DNS와 Hybrid 구성 체계 수립)
- Props : AWS로 마이그레이션 후 VPC Resolver 활용 및 공유 DNS 환경 구성 가능, Route 53 가용성 활용

Hybrid DNS 아키텍처

ON-PREMISE DNS 서버 연동 시



1) Private Host Zone과 VPC 연결

2) Route53 inbound / outbound endpoint 설정

- Inbound endpoints – On-prem DNS 서버에서, AWS에서 관리하는 도메인 정보를 질의
- Outbound endpoints – AWS에서, On-prem DNS에서 관리하는 도메인 정보를 질의

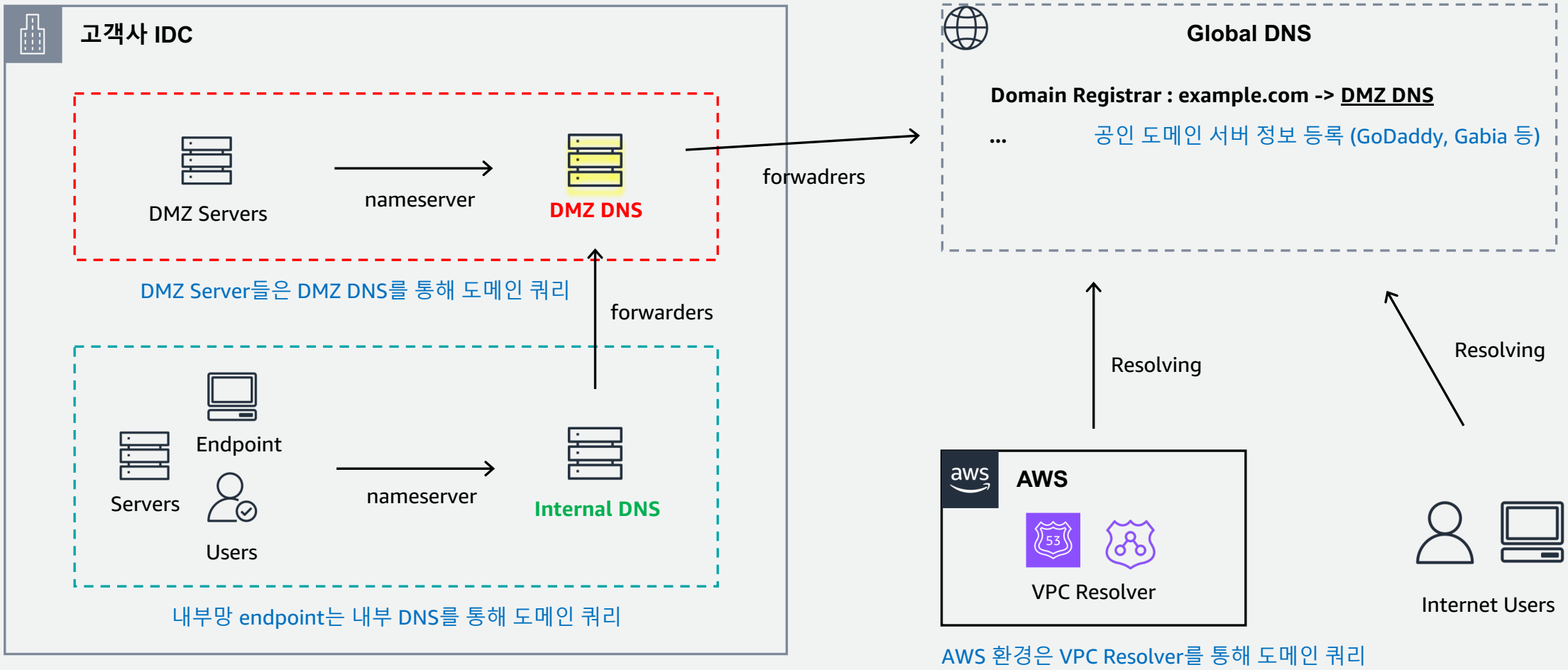
하위 Sub 도메인 관리
- ex) aws.example.co.kr, app1.aws.example.co.kr
- on-prem.example.co.kr -> On-premise DNS IP via Route53 Forwarding Rule

3) On-premise DNS Server

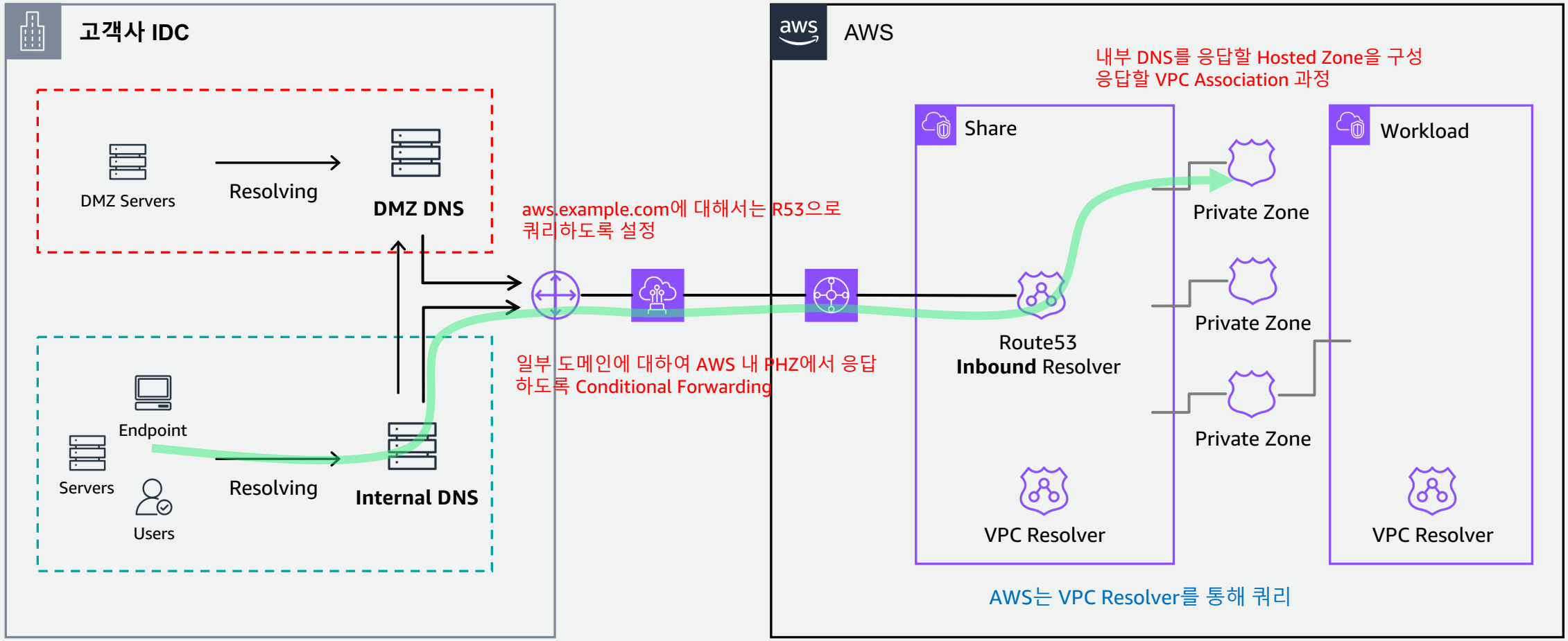
- Conditional forwarding rules – On-prem DNS 서버에서, AWS 호스팅 도메인에 대한 요청을 inbound endpoint로 보낼 때 사용

상위 Main 도메인 관리
- example.co.kr Hosted Zone & Record 관리
- AWS 하위 subdomain Conditional Forwarder설정
  .aws.example.co.kr -> Inbound Resolver Endpoint Via DX

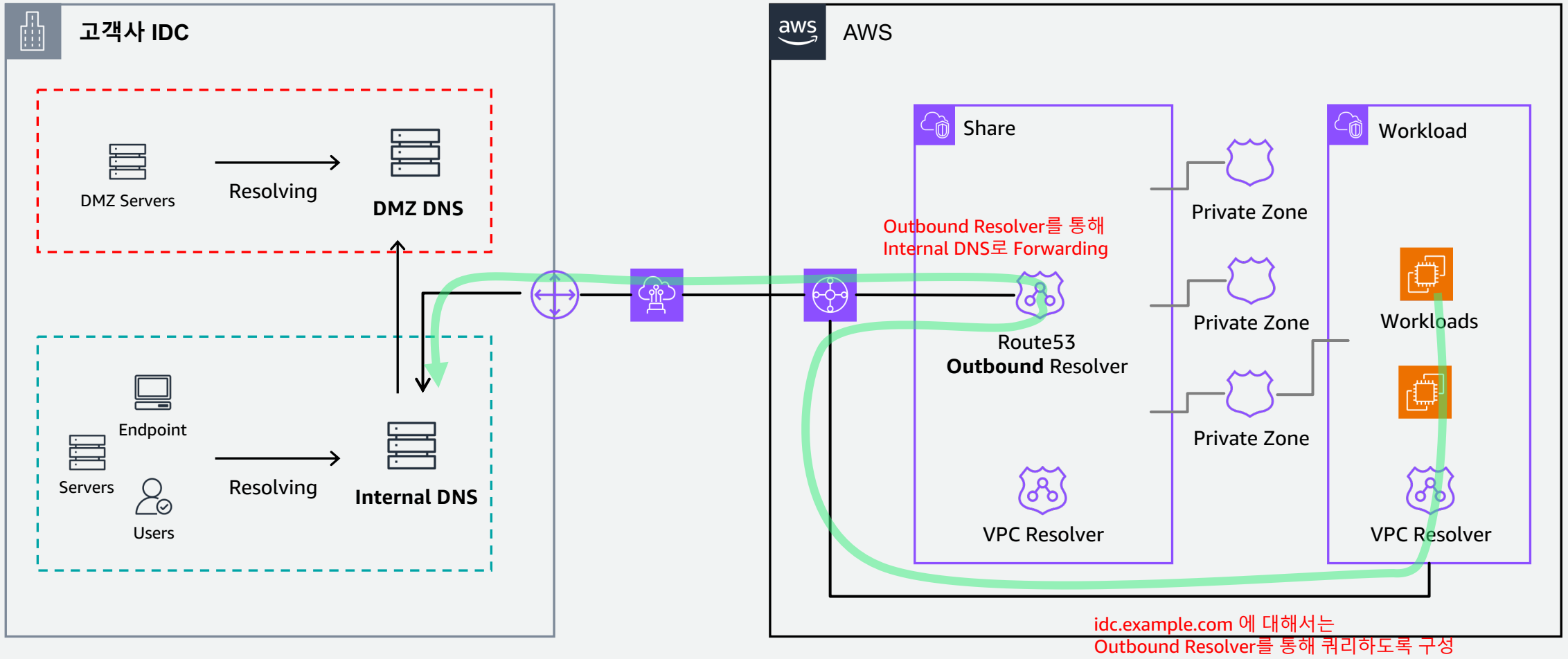
DNS 구성 예시 – Customer Usecase



Internal DNS 구성 (Hybrid - Inbound)



Internal DNS 구성 (Hybrid - Outbound)



Further Reading

Hybrid Cloud DNS Options for Amazon VPC

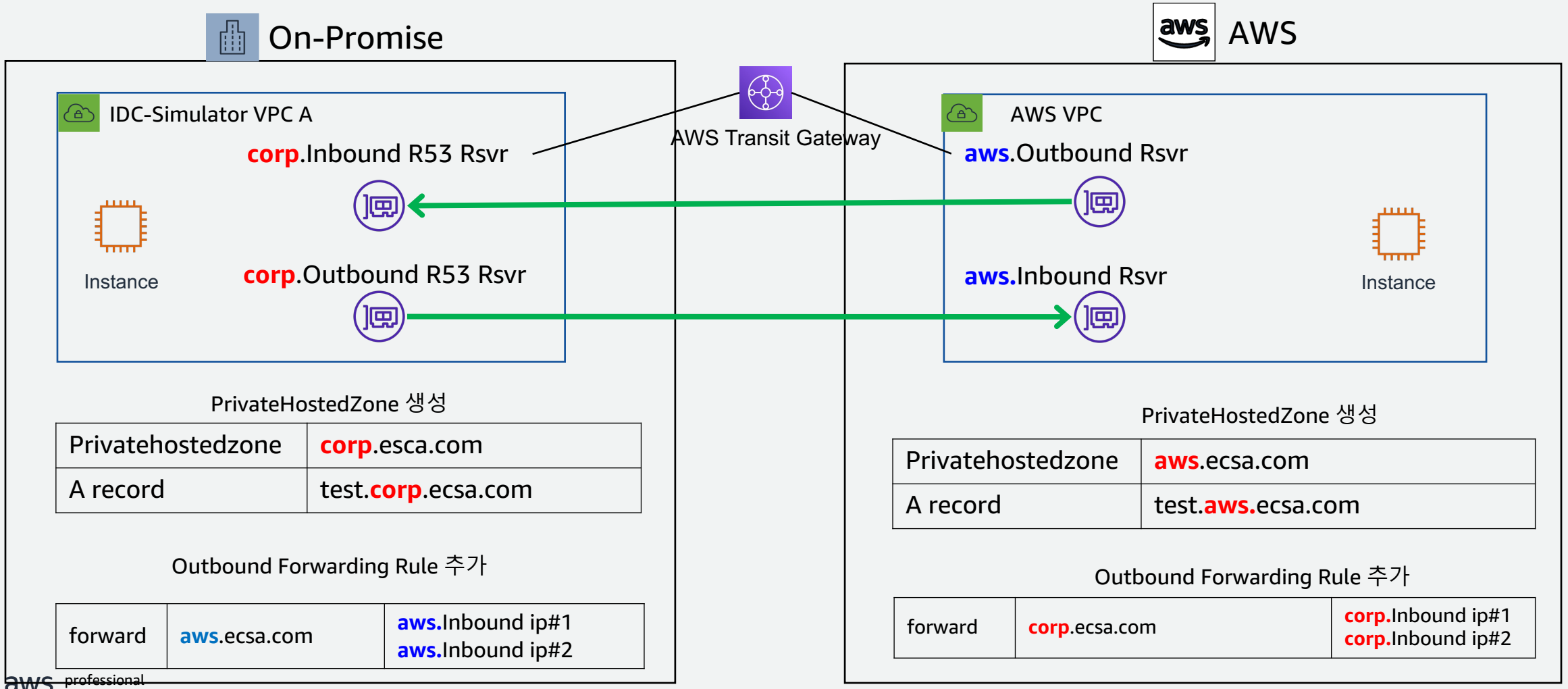
Using Route 53 Private Hosted Zones for Cross-account Multi-region Architectures – **[Blog]**

Simplify DNS management in a multi-account environment with Route 53 Resolver – **[Blog]**

실습 – In/Outbound Resolver

실습) Inbound, Outbound Resolver 사용

Onpremise 환경을 가정한 VPC와, AWS VPC를 2개 구성하여 Resolver를 간략하게 구성해봅니다.



PrivateHostedZone 생성

Privatehostedzone	corp.esca.com
A record	test.corp.ecsa.com

Outbound Forwarding Rule 추가

forward	aws.ecsa.com	aws.Inbound ip#1 aws.Inbound ip#2

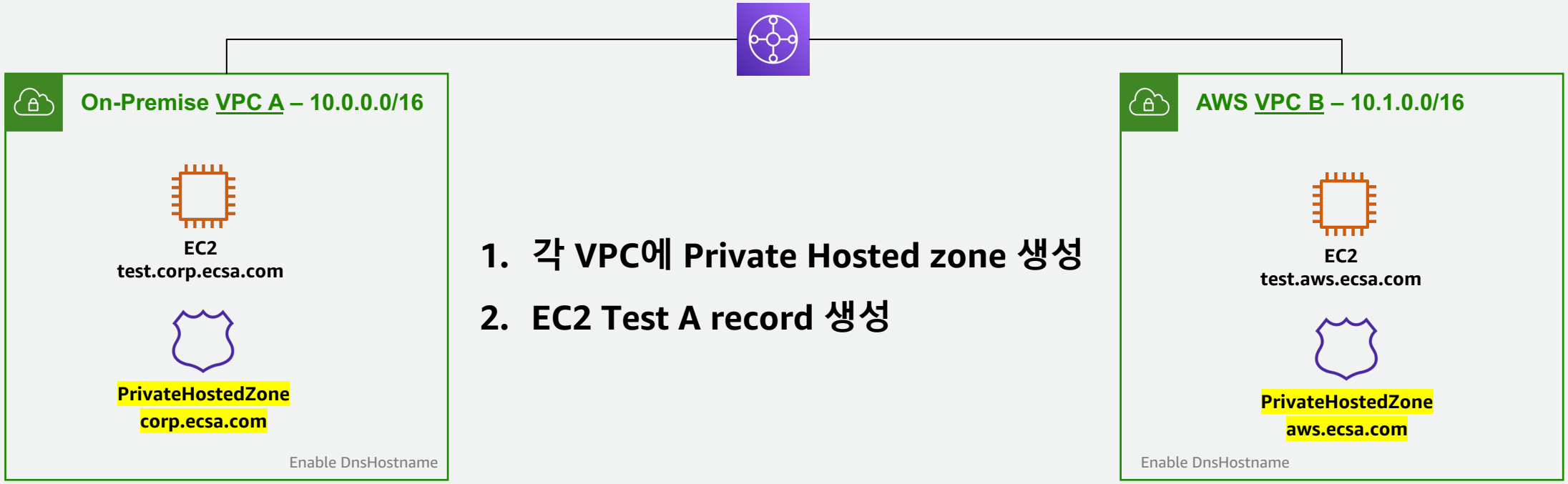
PrivateHostedZone 생성

Privatehostedzone	aws.ecsa.com
A record	test.aws.ecsa.com

Outbound Forwarding Rule 추가

forward	corp.ecsa.com	corp.Inbound ip#1 corp.Inbound ip#2

Step 1. Create PrivateHosted Zone

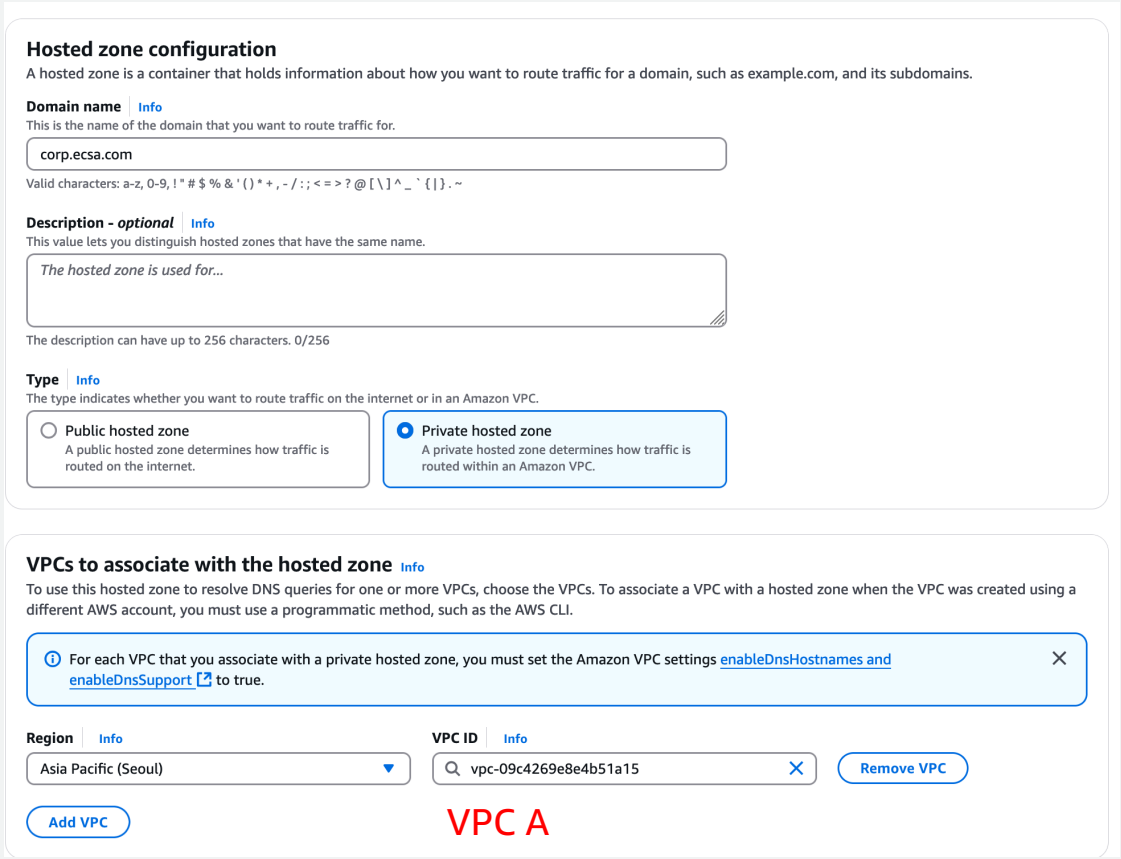


For each VPC that you associate with a private hosted zone, you must set the Amazon VPC settings enableDnsHostnames and enableDnsSupport to true.

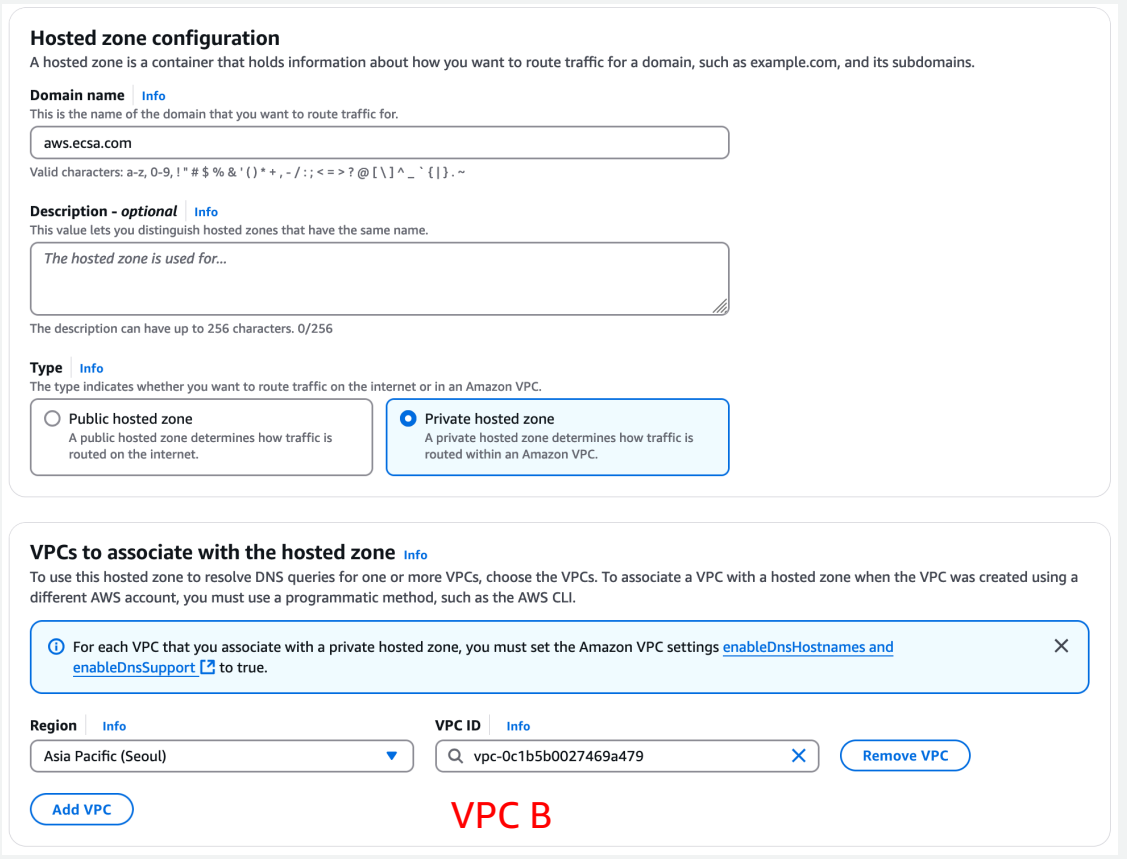
Step 1-1. Create PrivateHosted Zone

Route53에서 다음의 2개 Private Hosted Zone을 생성합니다.

corp.ecsa.com

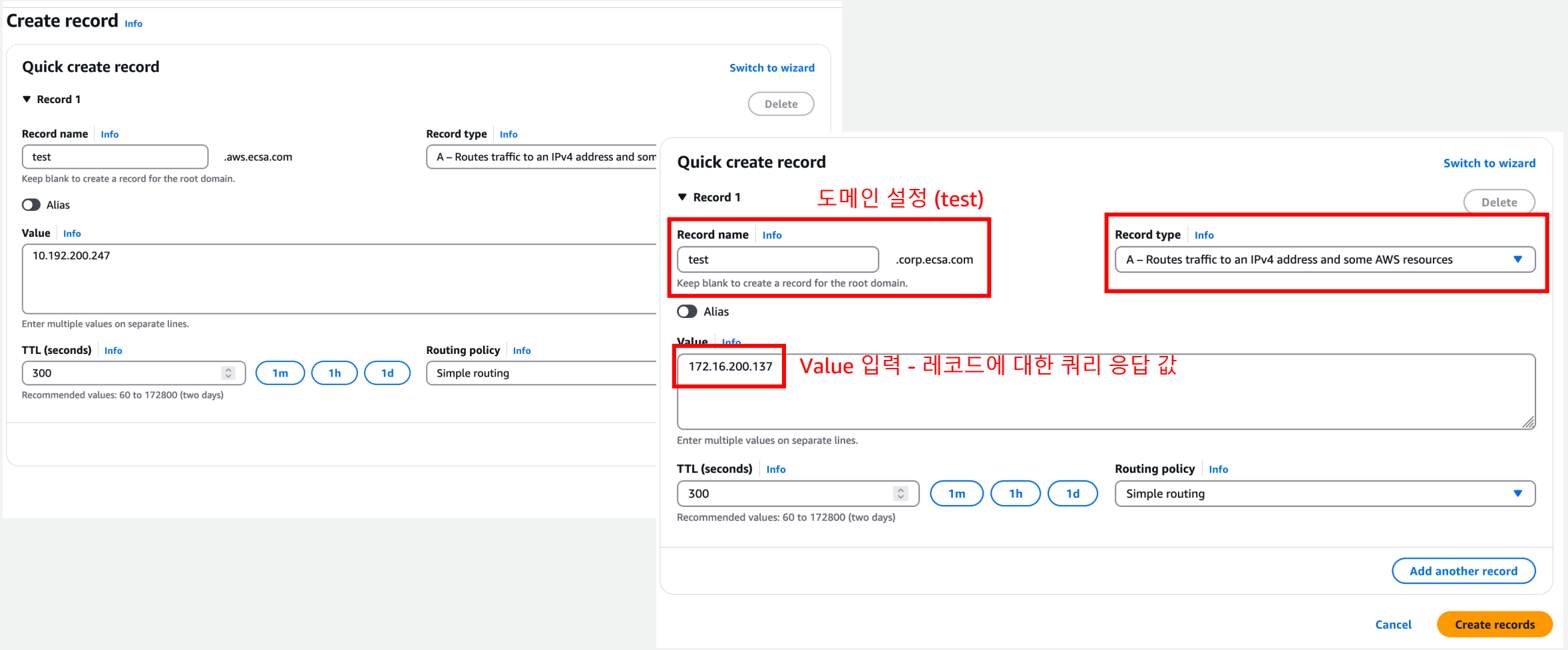


aws.ecsa.com



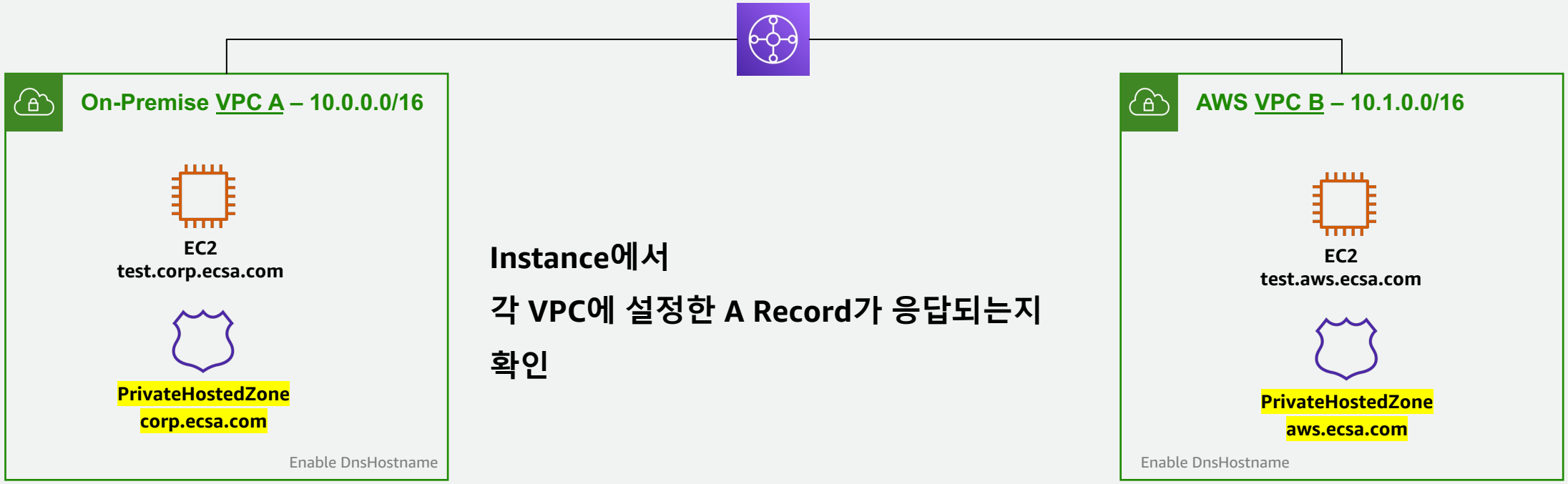
Step 1-2. Create A Records in PHZ

생성된 PHZ에 A Record를 생성합니다.



Step 1-3. PHZ Test

각 VPC 내 정의된 레코드가 질의되는지 확인




```
sh-5.2$ nslookup test.corp.ecsa.com
Server:         10.1.0.2
Address:        10.1.0.2#53

** server can't find test.corp.ecsa.com: NXDOMAIN
```

아직 CORP 쪽으로는
질의할 수 없음

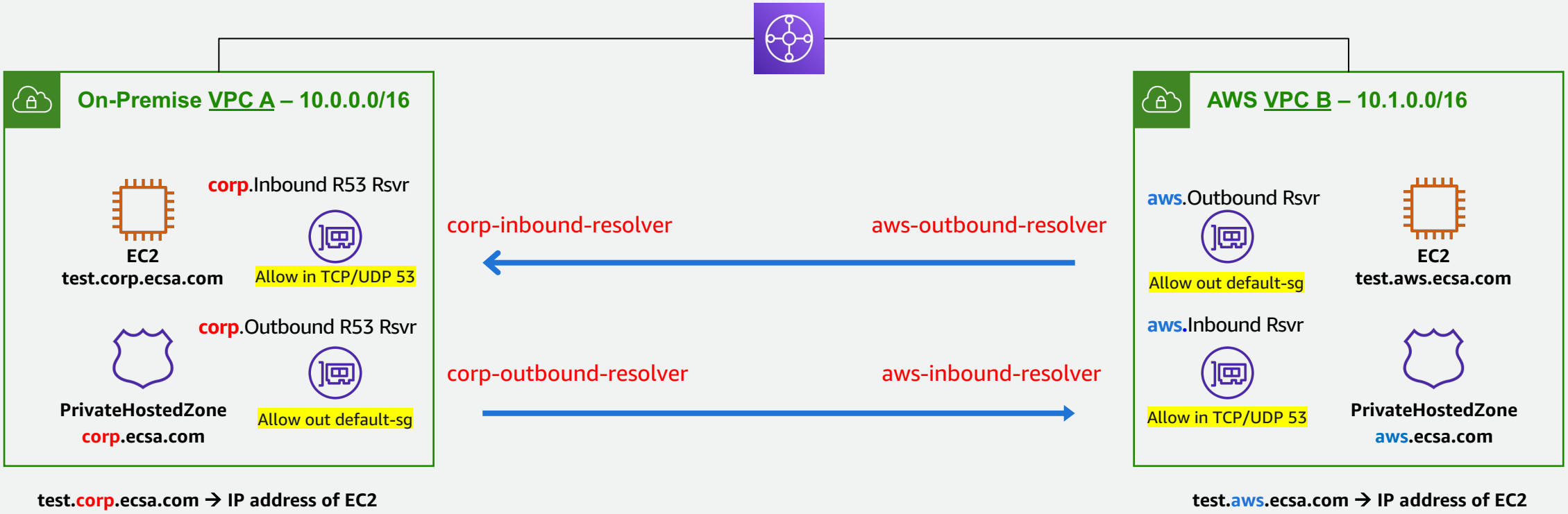
```
sh-5.2$ nslookup test.corp.ecsa.com
Server:         10.0.0.2
Address:        10.0.0.2#53

Non-authoritative answer:
Name:   test.corp.ecsa.com
Address: 10.0.1.100
```

OK!

Step 2. Inbound, Outbound Resolver

각 VPC에 Inbound, Outbound Resolver를 생성합니다.

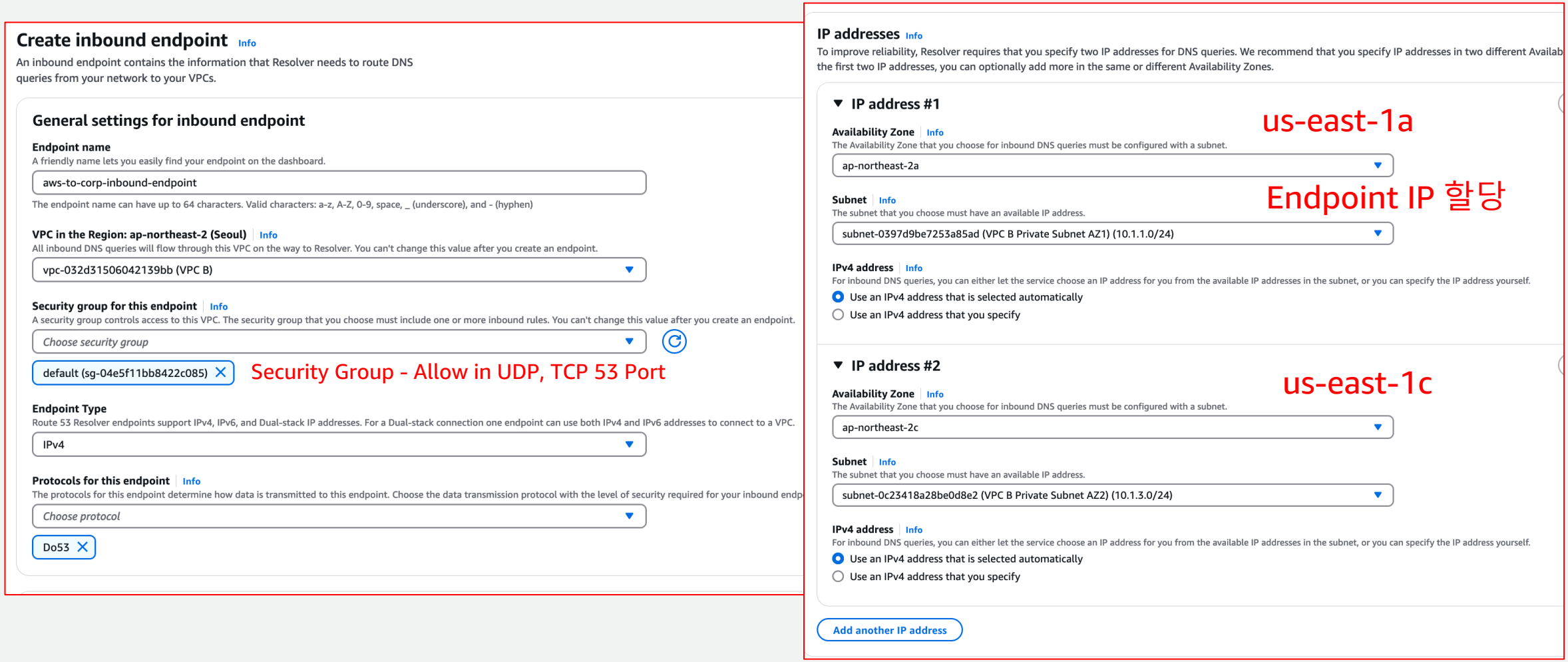


Inbound rules must allow TCP and UDP access on port 53

Outbound rules must allow TCP and UDP access on the port that you're using for DNS queries on your network

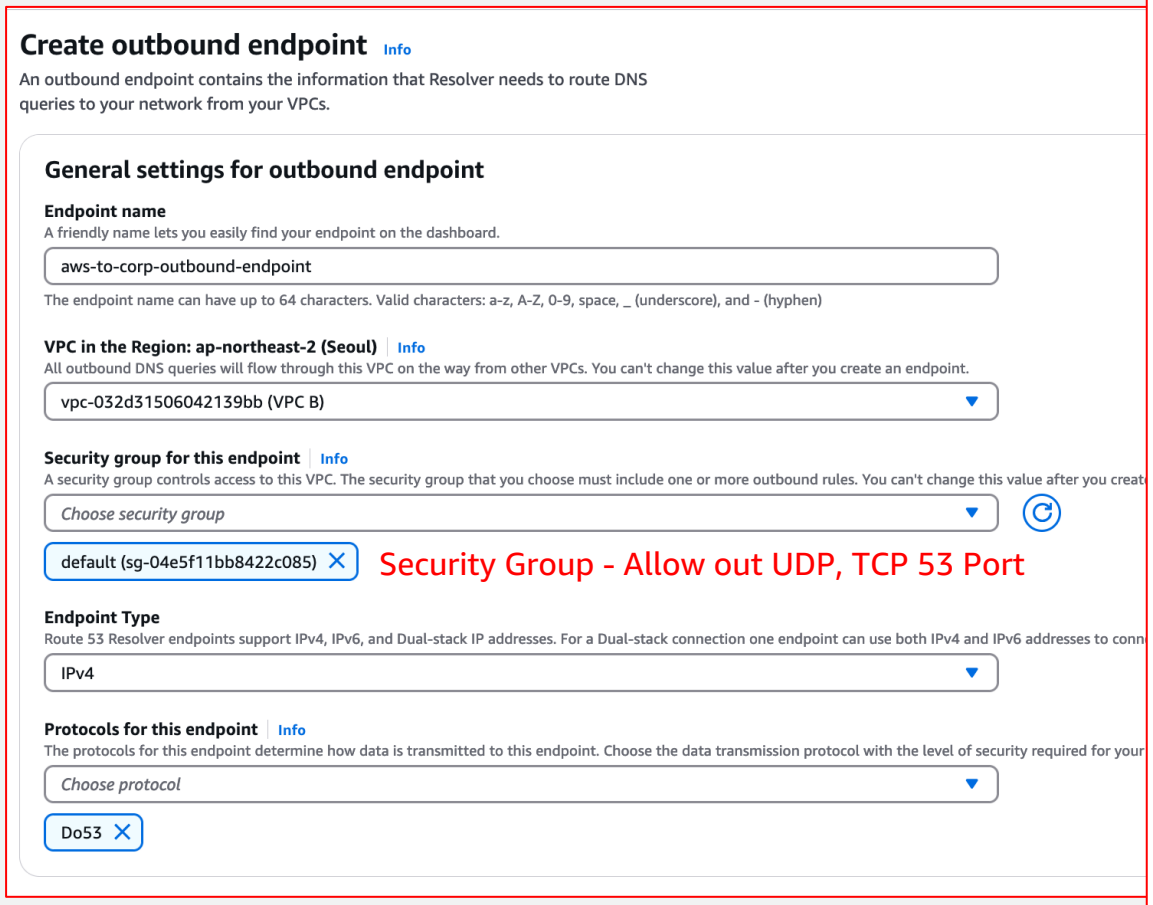
Step 2-1. Create Inbound Resolver

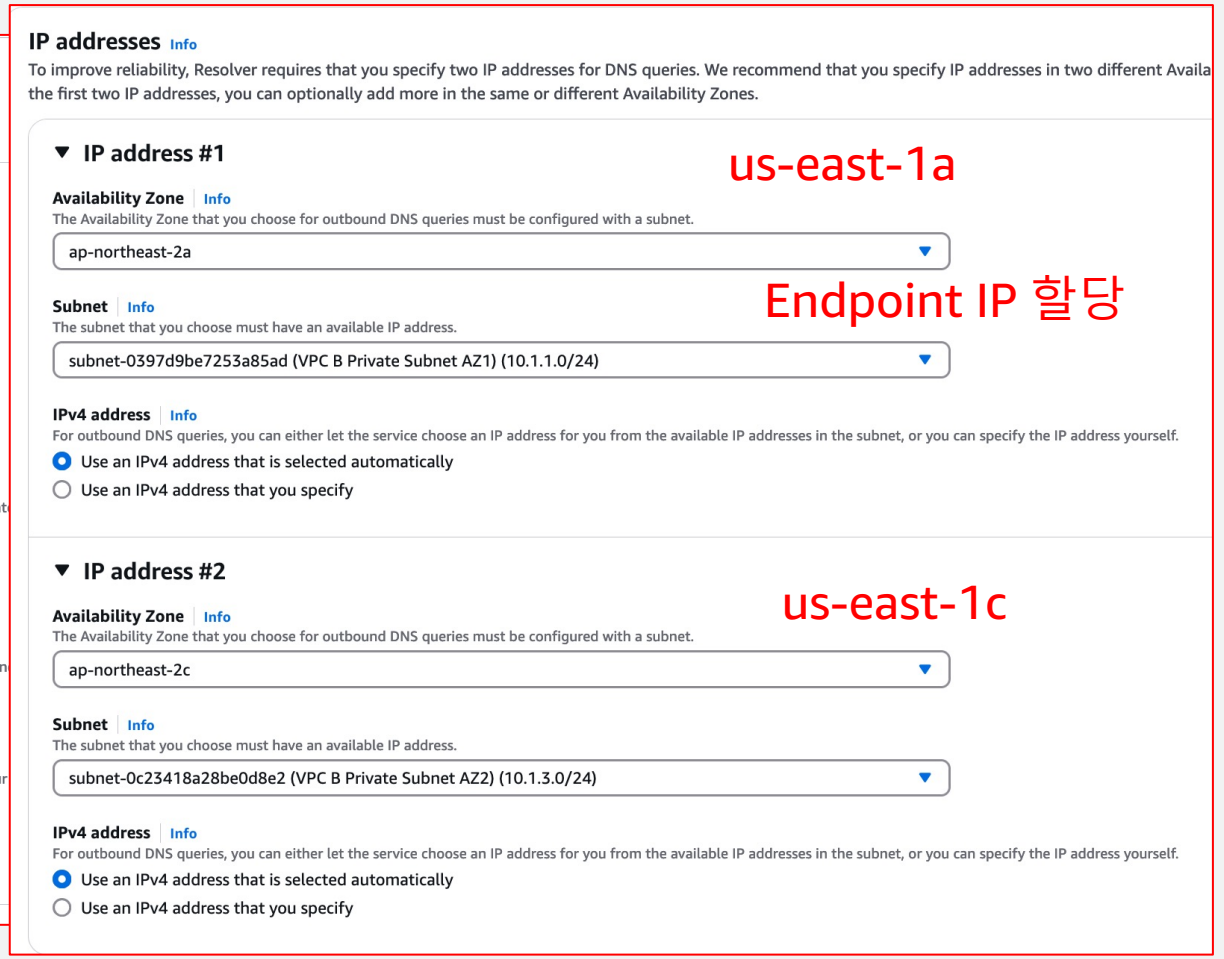
각 VPC에 대한 Route53 Inbound Endpoint를 생성합니다.



Step 2-2. Create Outbound Resolver

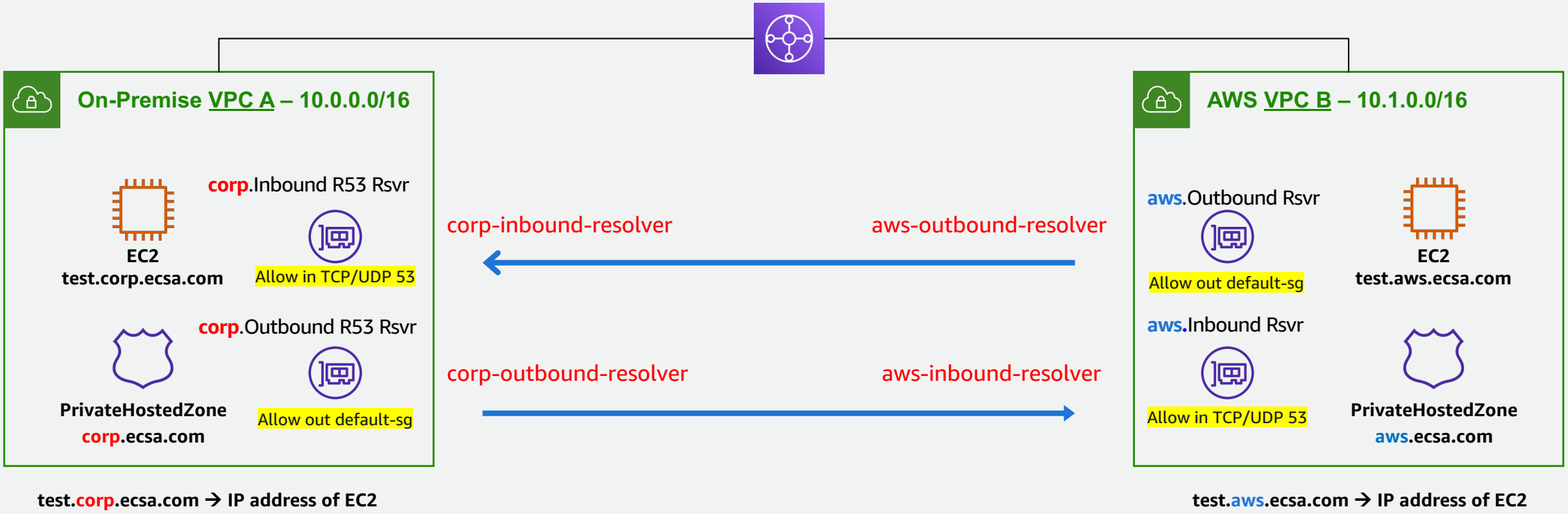
각 VPC에 대한 Route53 Outbound Endpoint를 생성합니다.





Step 3. Resolver Rule

각 VPC에 Inbound, Outbound Resolver를 생성합니다.

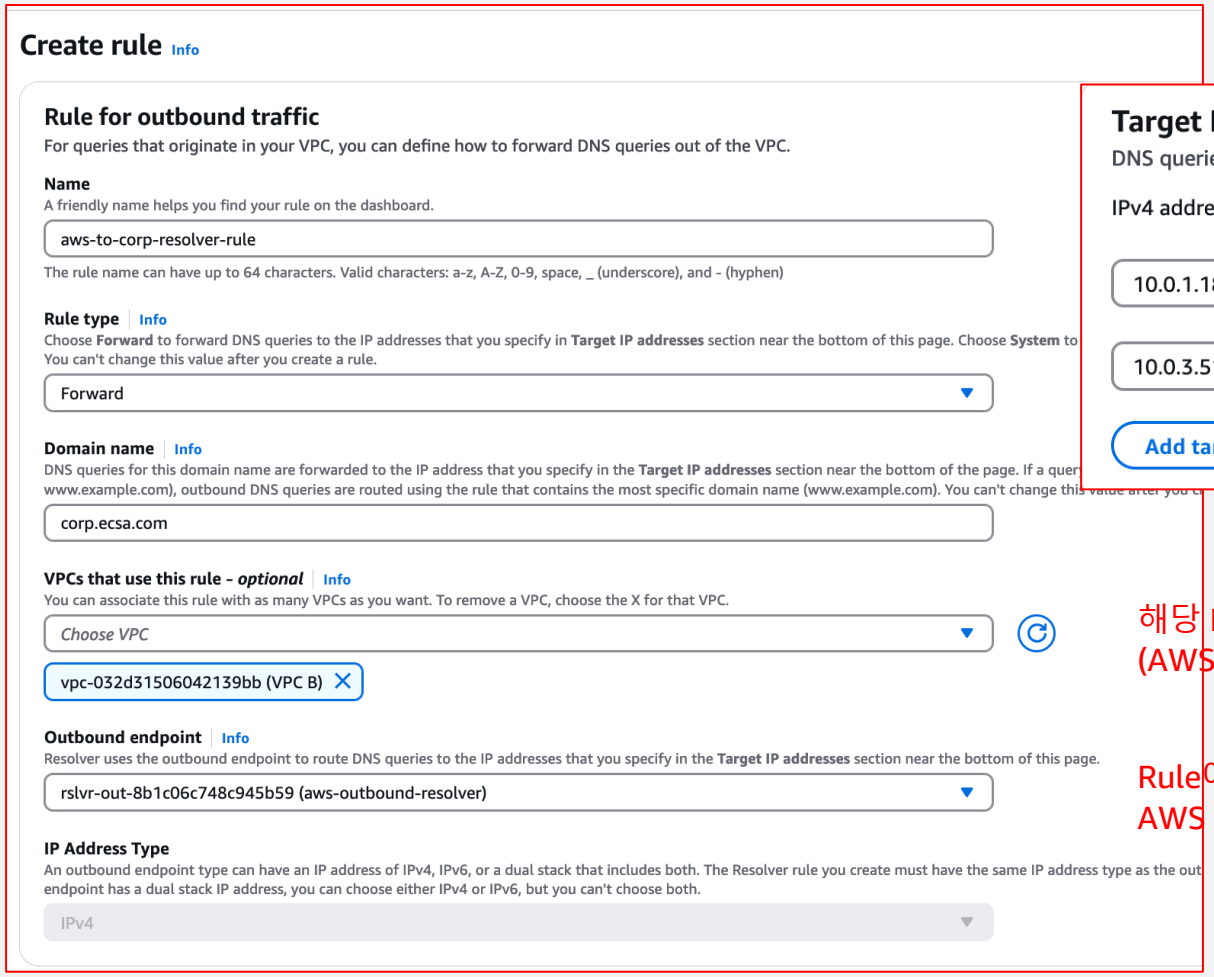


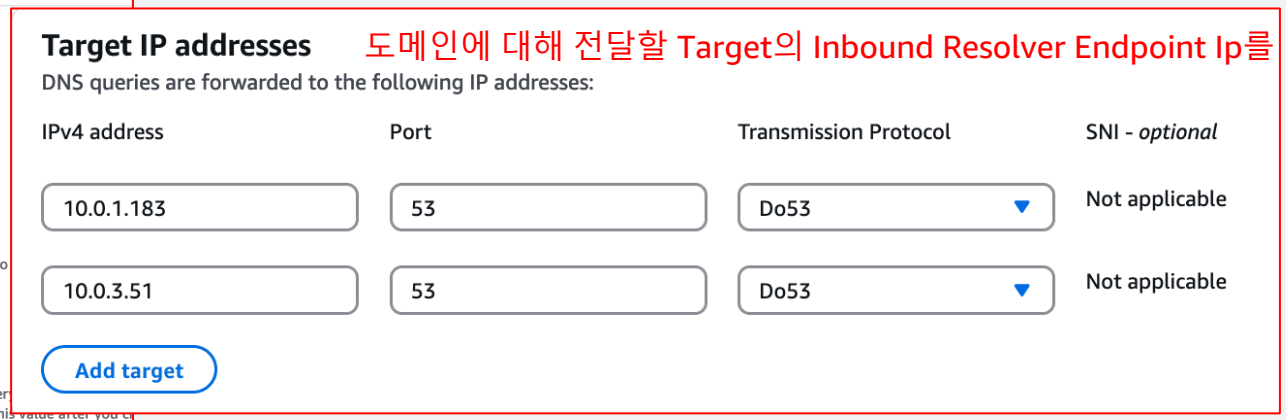
** Security Group - Inbound rules must allow TCP and UDP access on port 53

Outbound rules must allow TCP and UDP access on the port that you're using for DNS queries on your network

Step 3-1. Create Resolver Rule

Resolver Rule 생성 – AWS VPC에서 Corp VPC로 Conditional Forwarding 생성 조건 설정



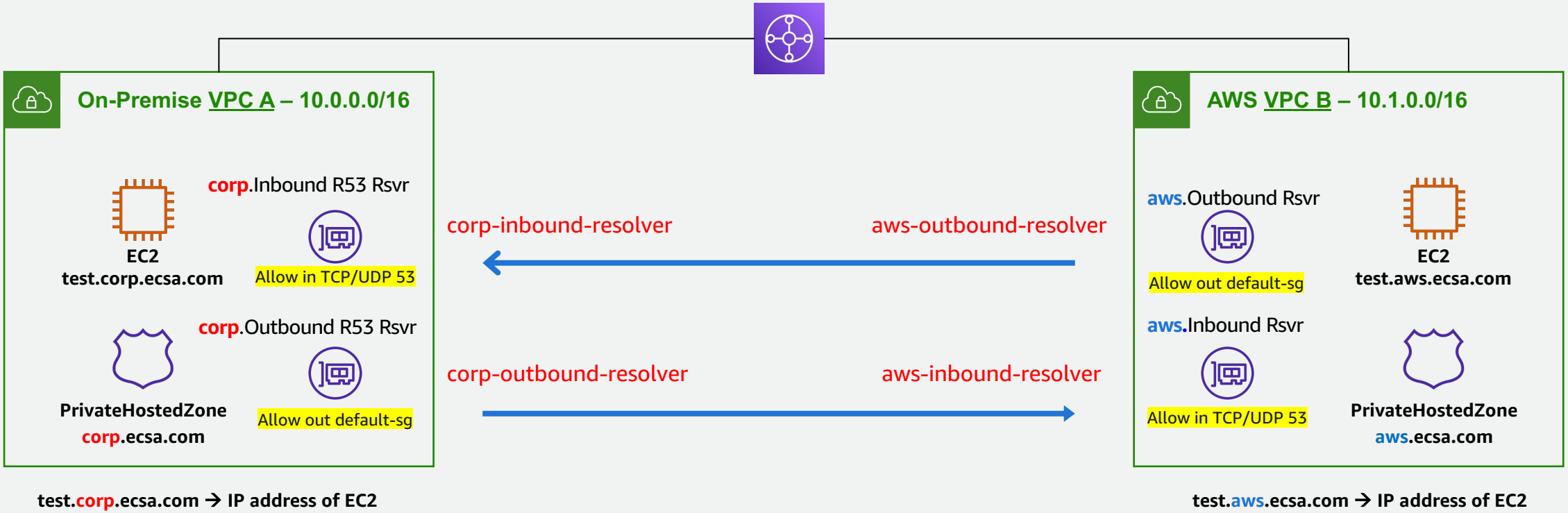


해당 Rule이 적용될 VPC 선택
(AWS VPC에서 CORP로 가기 위한 조건 설정이므로 AWS VPC 선택)

Rule에 해당될 경우 전달될 Endpoint 선택
AWS VPC에 생성했던 Outbound Endpoint

Step 4. Test!

상호 질의가 가능한지 확인

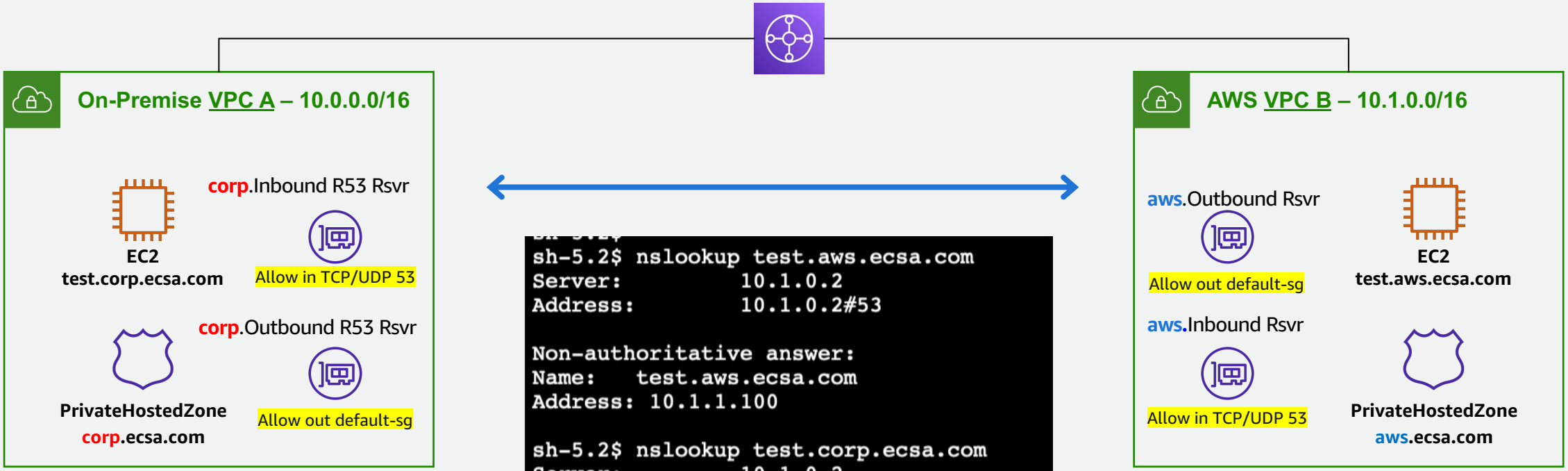


Inbound rules must allow TCP and UDP access on port 53

Outbound rules must allow TCP and UDP access on the port that you're using for DNS queries on your network

Step 4-1. Test!

상호 질의가 가능한지 확인



OK!

Appendix
Centralized VPC Endpoint

VPC Endpoint

AWS 서비스에 접근하려면..

```
sh-5.2$ nslookup kms.ap-northeast-2.amazonaws.com
Server:         10.1.0.2
Address:        10.1.0.2#53

Non-authoritative answer:
Name:   kms.ap-northeast-2.amazonaws.com
Address: 52.95.192.102
```

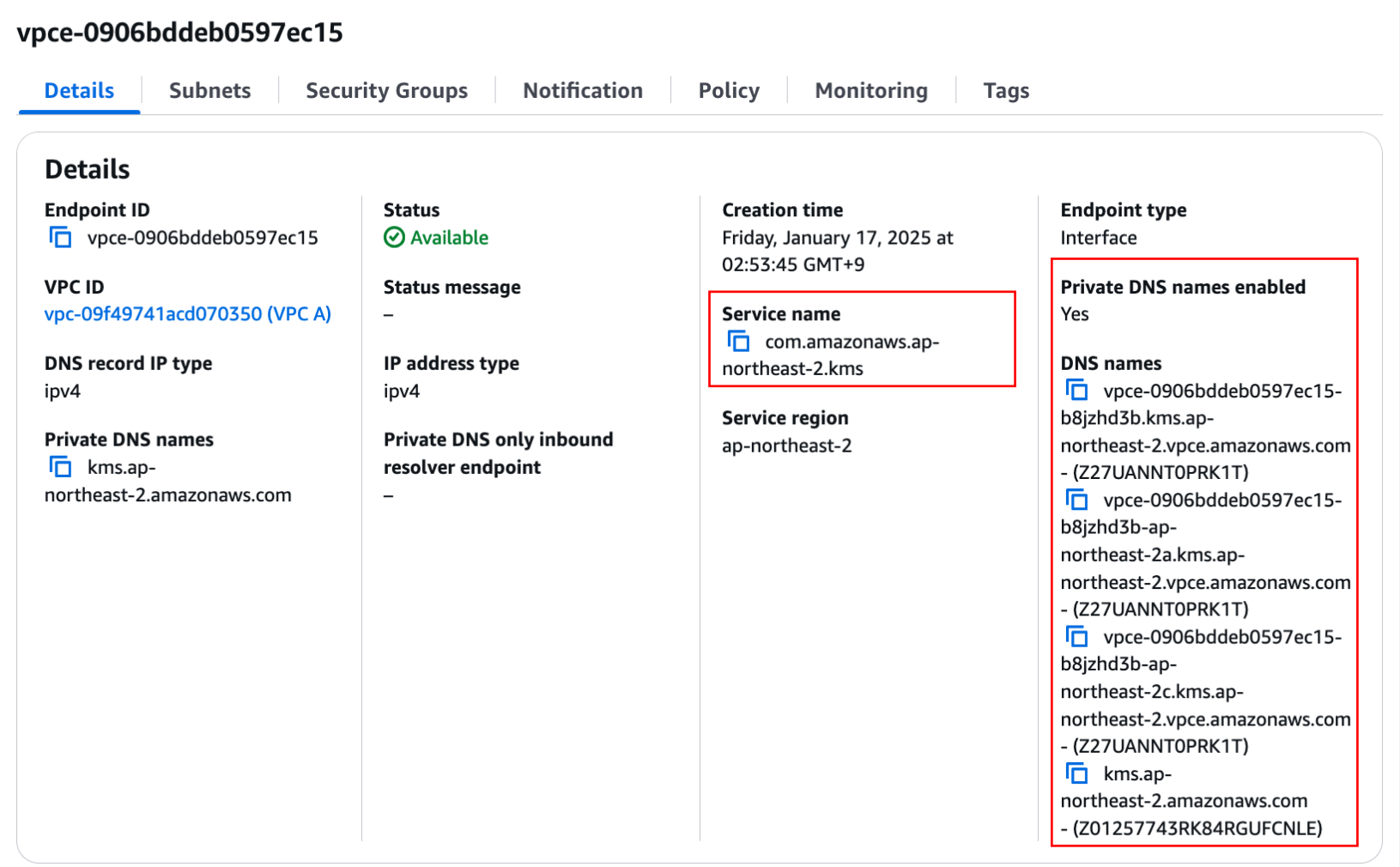
인터넷 IP

VPC Endpoint IP

```
sh-5.2$ nslookup kms.ap-northeast-2.amazonaws.com
Server:         10.0.0.2
Address:        10.0.0.2#53

Non-authoritative answer:
Name:   kms.ap-northeast-2.amazonaws.com
Address: 10.0.3.65
Name:   kms.ap-northeast-2.amazonaws.com
Address: 10.0.1.207
```

VPC Endpoint

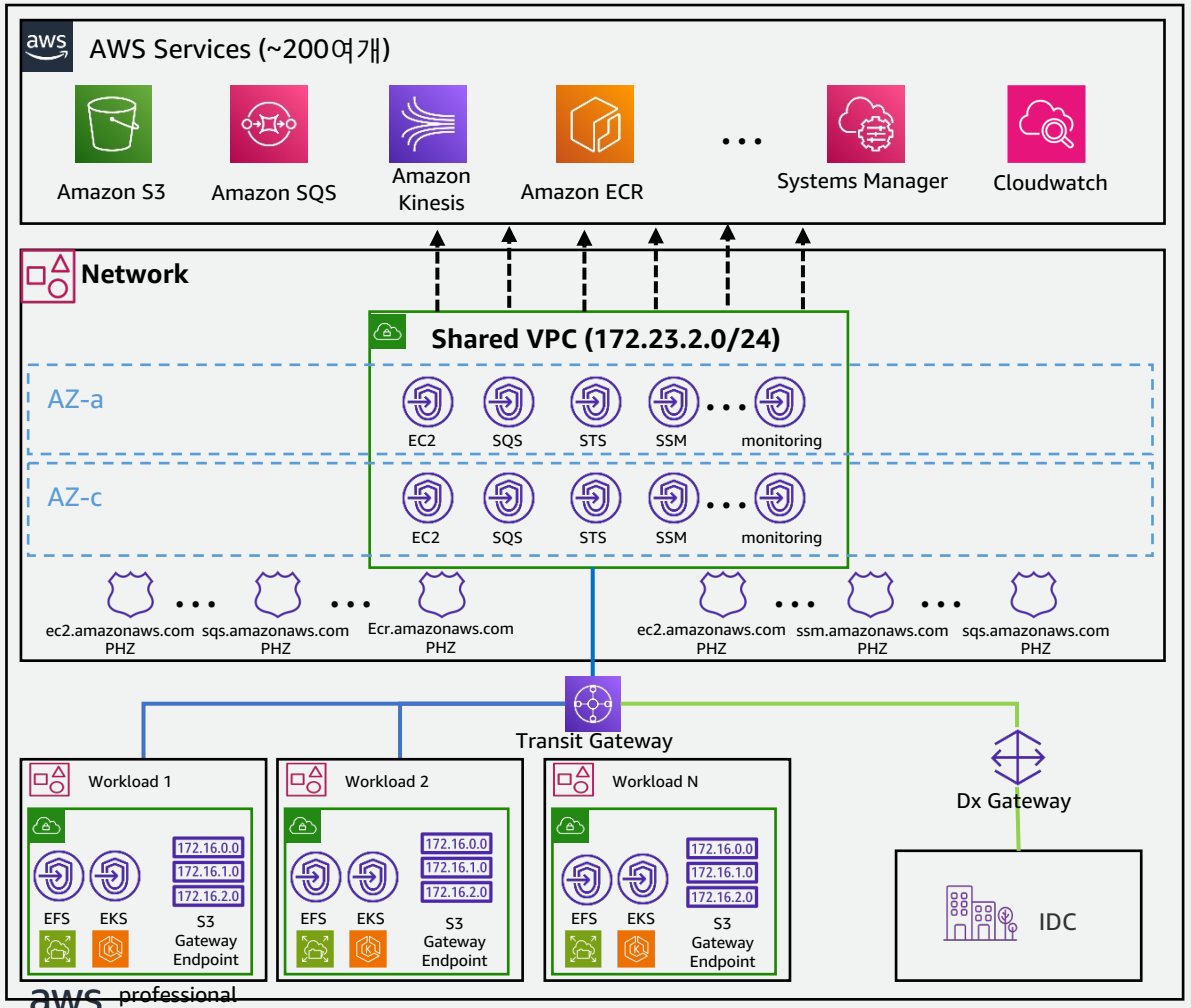


VPC Interface Endpoint를 구성하면

AWS가 Background에서 Service Domain에 대한 PHZ를 생성하여 VPC에 Associate 해준다!

VPC Endpoint 구성 사례

Topology



Design/Deployment

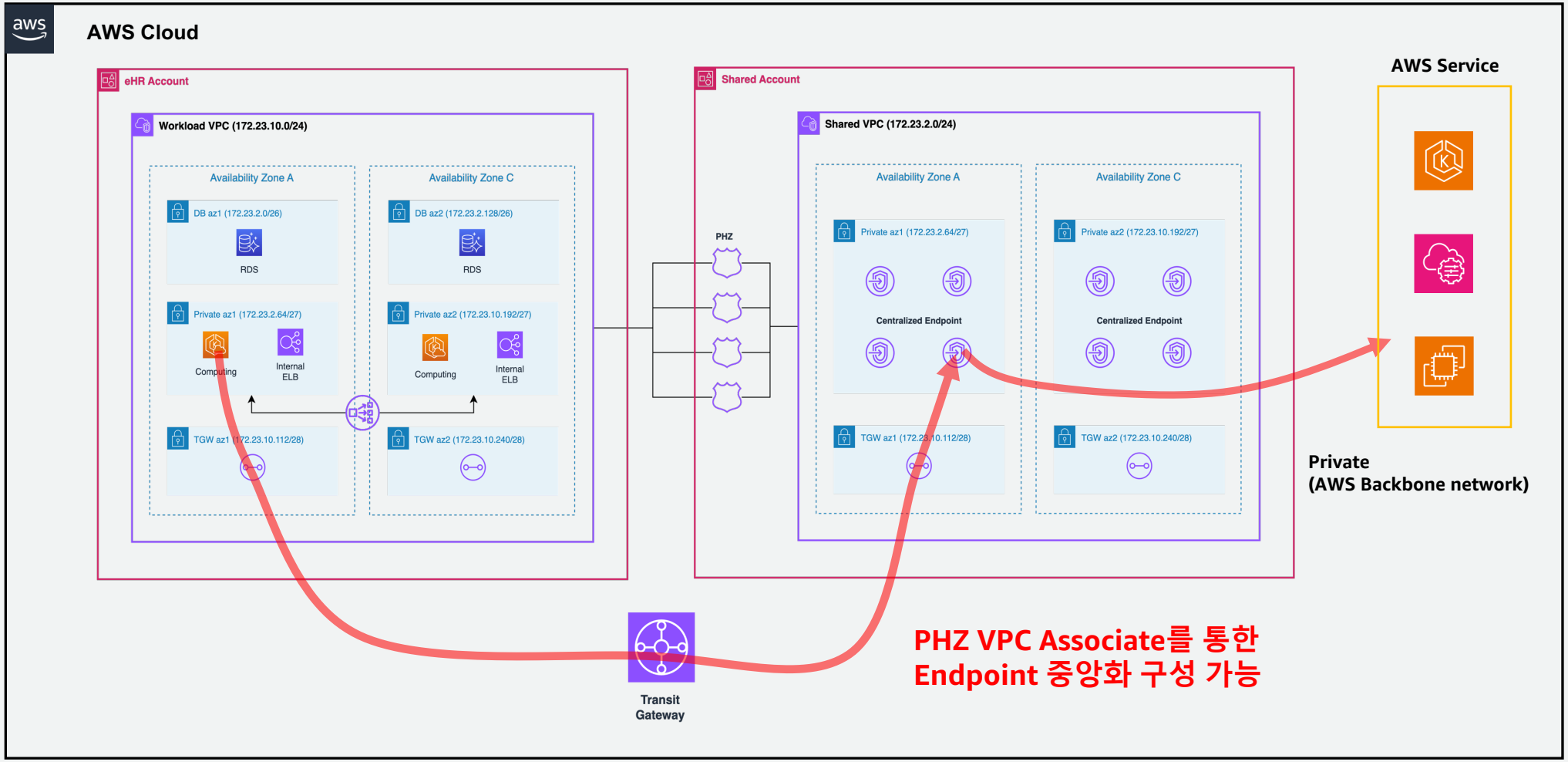
- 모델 선정 : **Hybrid (중앙형 + 분산형)**
- Endpoint 선정 기준 :

※ Gateway Endpoint 활용 (S3)

  - 분산형 : Traffic 발생량이 많은 endpoints (EFS, EKS, S3, RDS)
    대량의 Traffic으로 인해 TGW 비용 증가 방지
  - 중앙형 : 분산형 외 (EC2, STS, SSM, Cloudwatch..etc)
    소량의 Traffic 대비 많은 Endpoint 비용 발생 방지

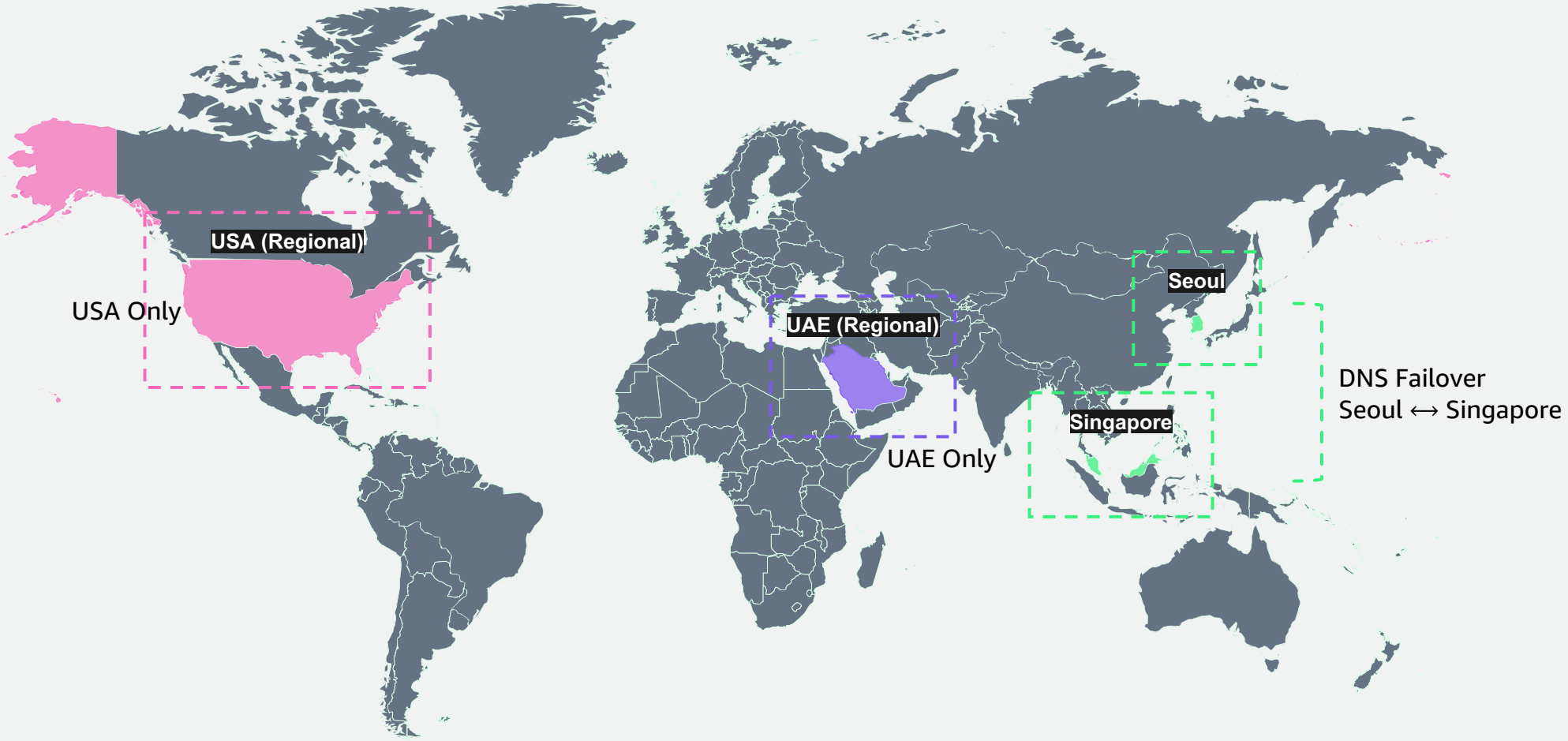
- **Account 선택 : Shared Account**
- **배포 VPC : Shared VPC**
- 확장성 : AZ 분리, endpoint 증설 가능 (Route53 활용)
  - Route53 PHZ Cross Account Association & Alias Record
- Endpoint 모니터링 방안
  - 필요 시 VPCFlow & Cloudwatch를 활용 가능

PHZ를 이용한 Centralized Endpoint 구성 예시



Appendix
Global Route 53 Usecases

Public Domain Concepts



Route53 Health Check

Route53에서 제공하는 Domain health check 기능

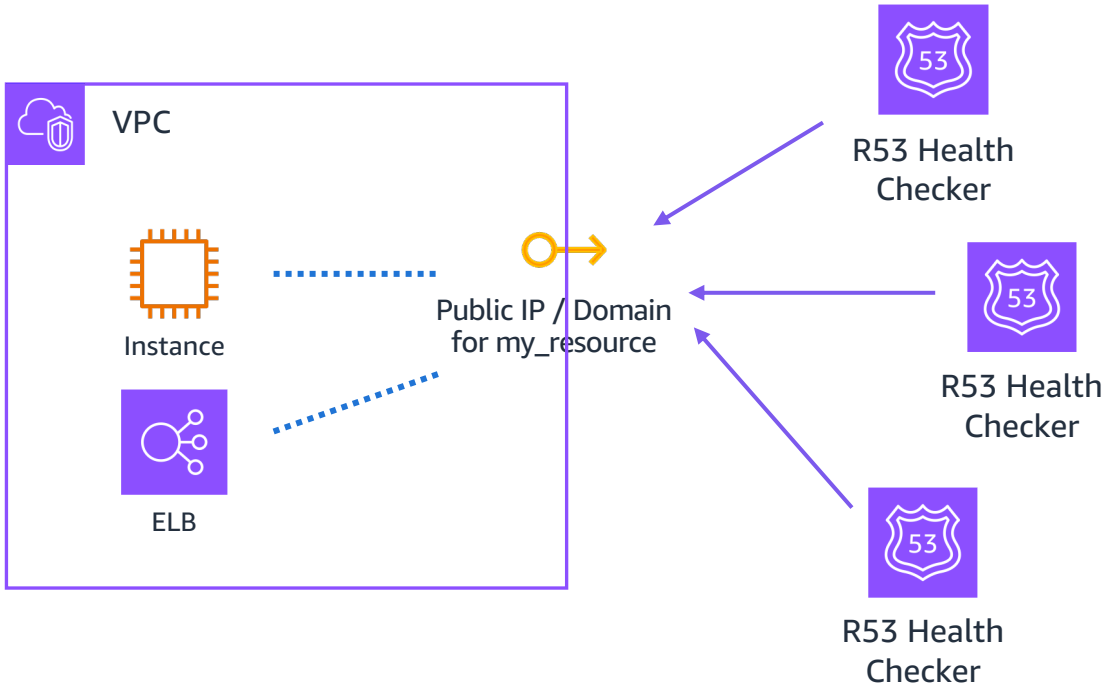
- Failover Rule 설정 시 Evaluate Health check 용도
- 해당 도메인에 대한 모니터링 용도

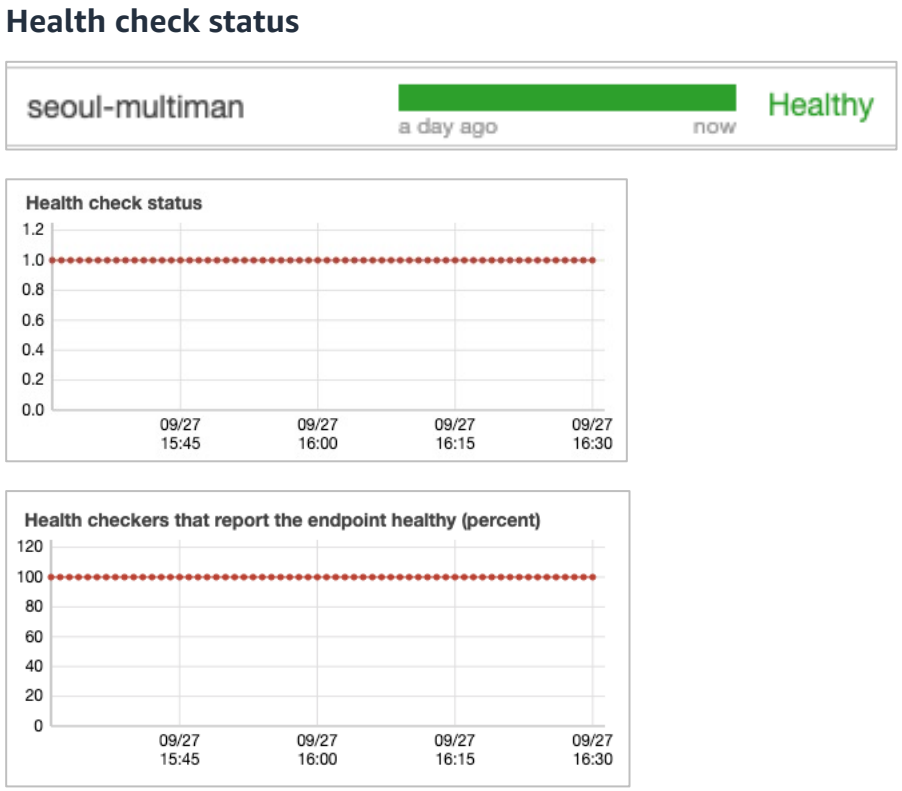
1. **Endpoint Monitoring**
   - IP Address, Domain Name
   - Endpoint는 IP, Port, Path까지 지정하여 모니터링 (Health Page)

2. **Status of other health checks (calculated health check)**
   - 다른 Route53 Health Check를 Reference
   - 1개 이상의 Health Check를 Composite 하여 구성

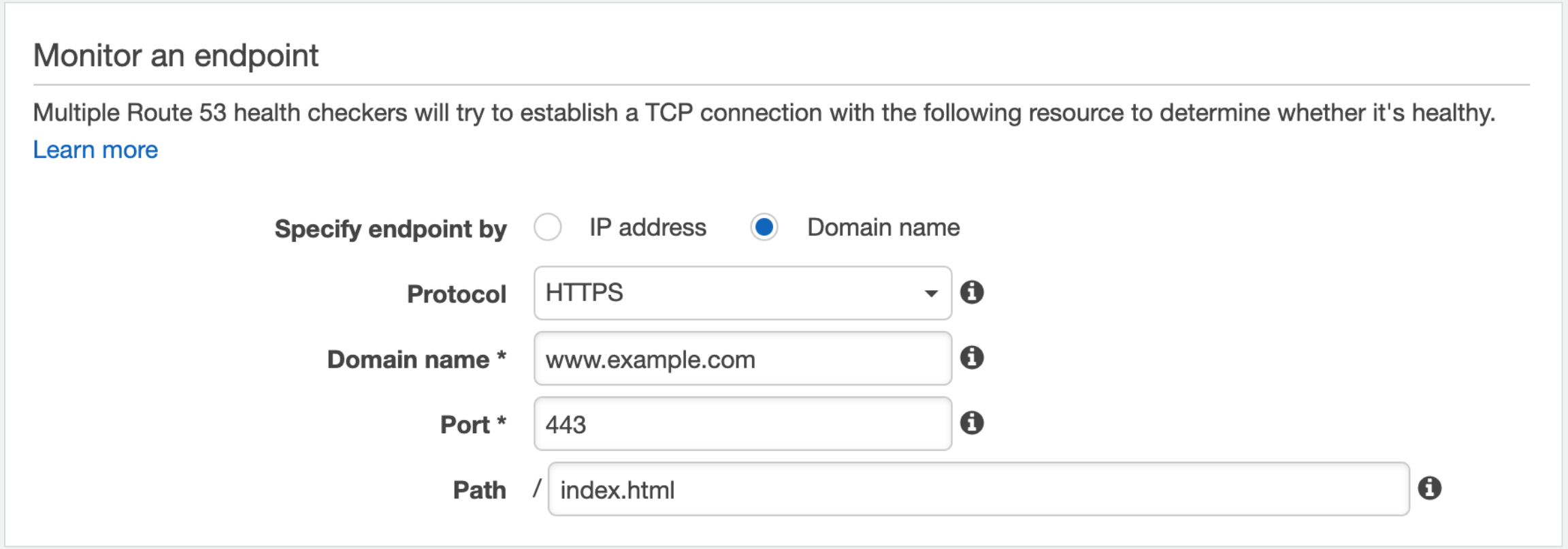
3. **State of Cloudwatch Alarm**
   - CloudWatch Alarm Reference

Route 53 Health Check - Endpoint Monitoring





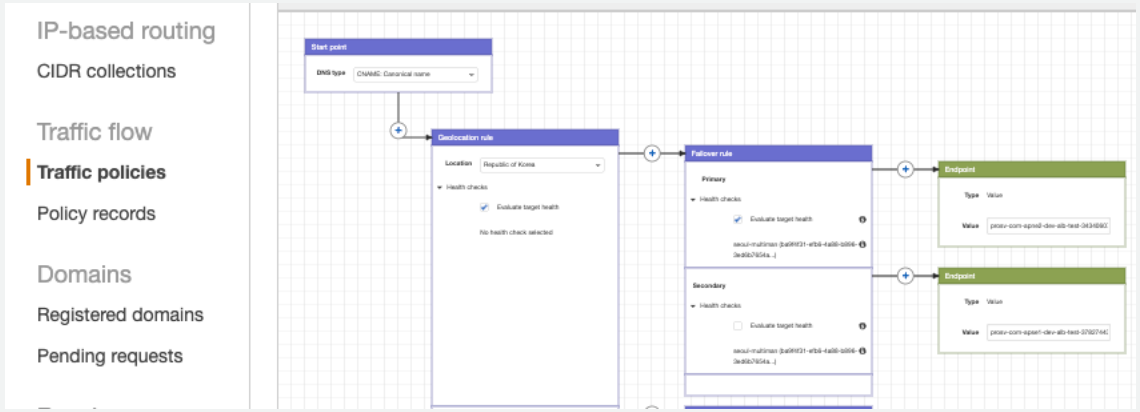
Route 53 Health Check - Endpoint Monitoring



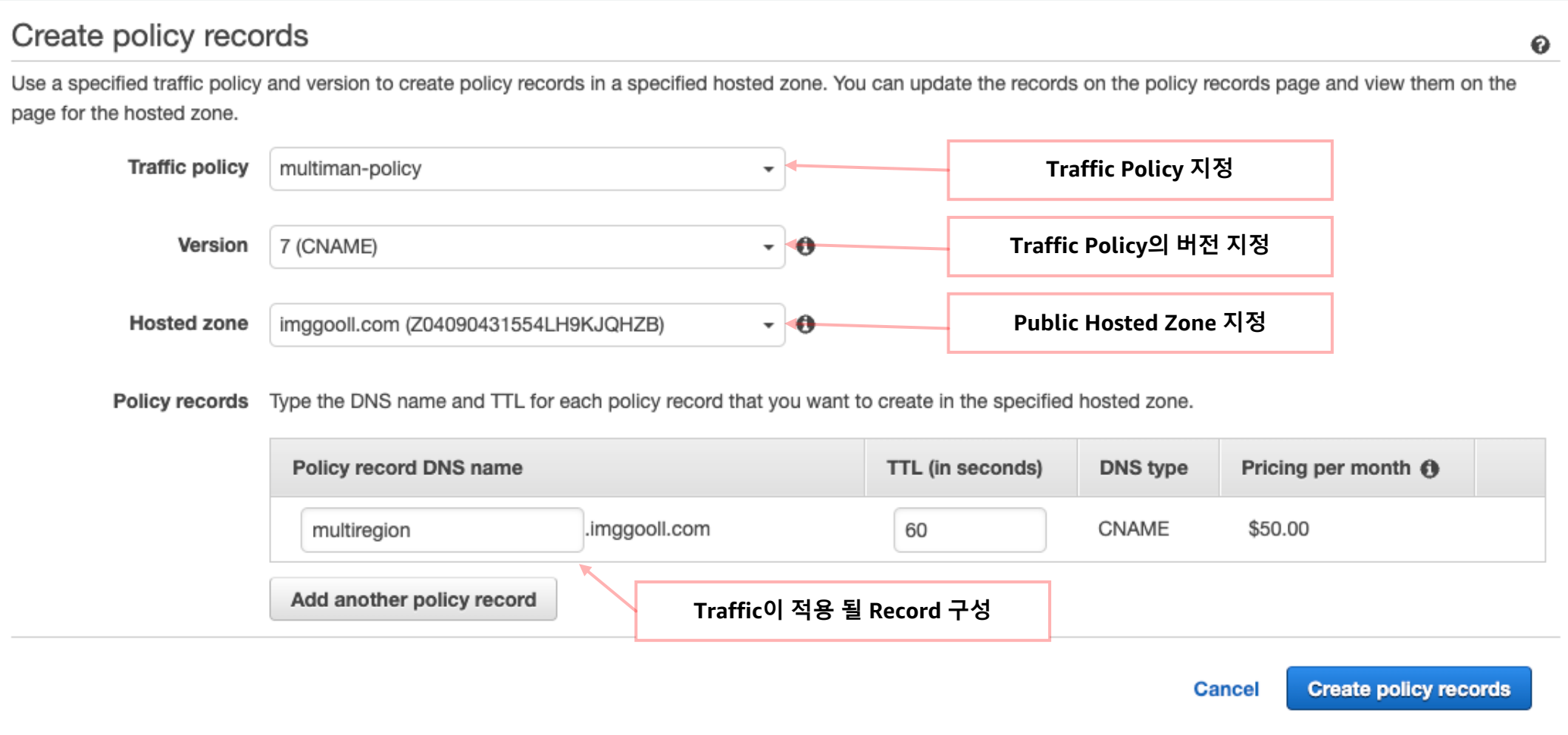
Traffic Policy & Policy Record

- Traffic Policy를 통한 동일한 도메인에 대해 복잡한 구성으로 레코드를 유지 관리
- Traffic Policy - Record는 쿼리 시 해당 레코드를 트래픽 정책 구성을 기반으로 응답
- 각 Policy는 Visual Editor를 통해 Tree를 생성 및 관리할 수 있으며, 버저닝 기본 지원으로 버전 롤백 가능
- Traffic Policy는 지정된 Policy Record와 연결되며, 연결 구성 당 월 50$의 고정 비용이 부과
  - 연결되지 않은 Policy 및 Record에 대해서는 비용 부과되지 않음

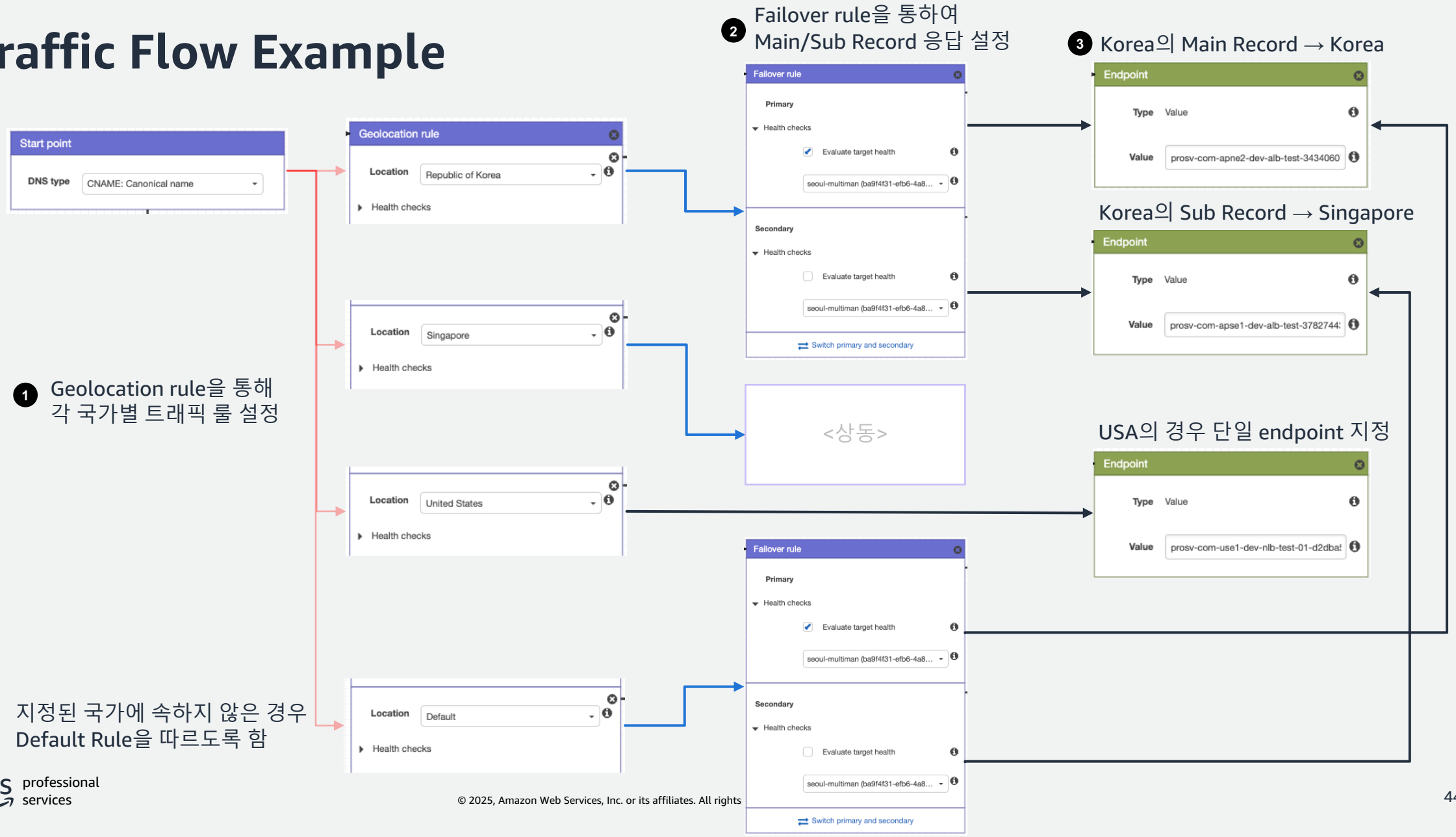
- Ex) www.example.com Record에 대한 Traffic policy 생성
  - 서울에서 접근 시 서울 리전의 서비스 ELB 응답
    - 서울의 ELB 혹은 HealthCheck가 Fail인 경우 DR의 ELB 응답
  - USA에서 접근 시 US 리전의 서비스 ELB 응답
    - USA의 HealthCheck가 Fail이더라도 다른 레코드를 응답하지 않음



Traffic Policy & Policy Record



Traffic Flow Example



Route 53 Record Routing Policy

- Traffic Flow로 구성한 트래픽 정책을 Route 53 레코드로 정의하는 방법
- Failover, Geolocation Rule 레코드 정의를 통한 도메인 Flow 구성

Concepts example

- **service.test.com - Geolocation Seoul**
  - Failover Domain Primary / Secondary (A Alias Record)
    - Failover Domain Primary -> Seoul Public NLB IP (A Record)
    - Failover Domain Secondary -> Singapore Public NLB IP (A Record)
- **service.test.com - Geolocation Singapore**
  - Failover Domain Primary / Secondary (A Alias Record)
    - Failover Domain Primary -> Singapore Public NLB IP (A Record)
    - Failover Domain Secondary -> Seoul Public NLB IP (A Record)
- **service.test.com - Geolocation Virginia - Regional**
  - Virginia Public NLB CNAME

Geolocation

Failover

Route 53 Record Routing Policy

Geolocation Rule

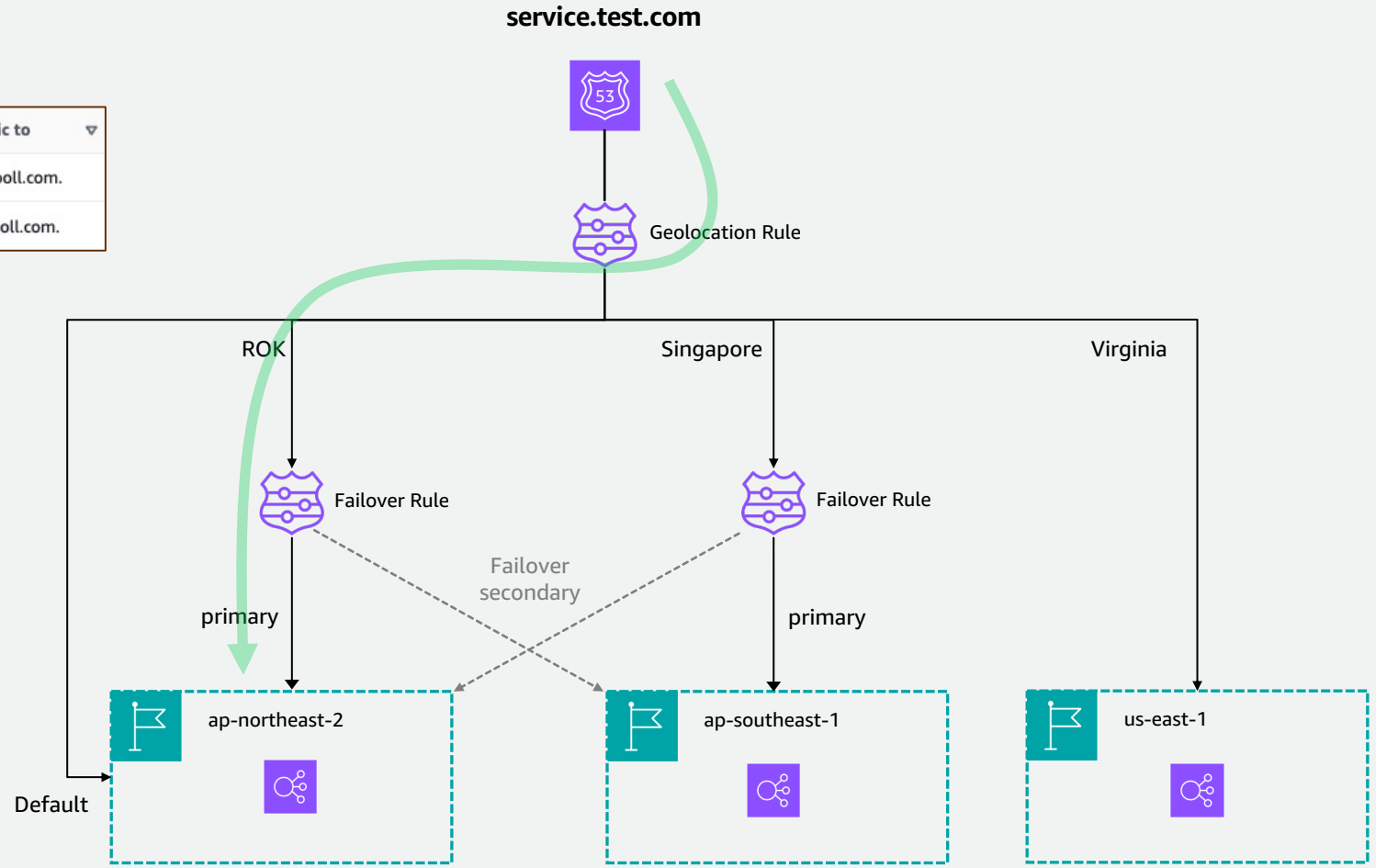
Record name	Routing ...	Differentiator	Value/Route traffic to
multigeo.imggooll.com	Geolocation	Republic of Korea	apne2-swift.imggooll.com.
multigeo.imggooll.com	Geolocation	Singapore	apse1-swift.imggooll.com.

Failover Rule - RoK

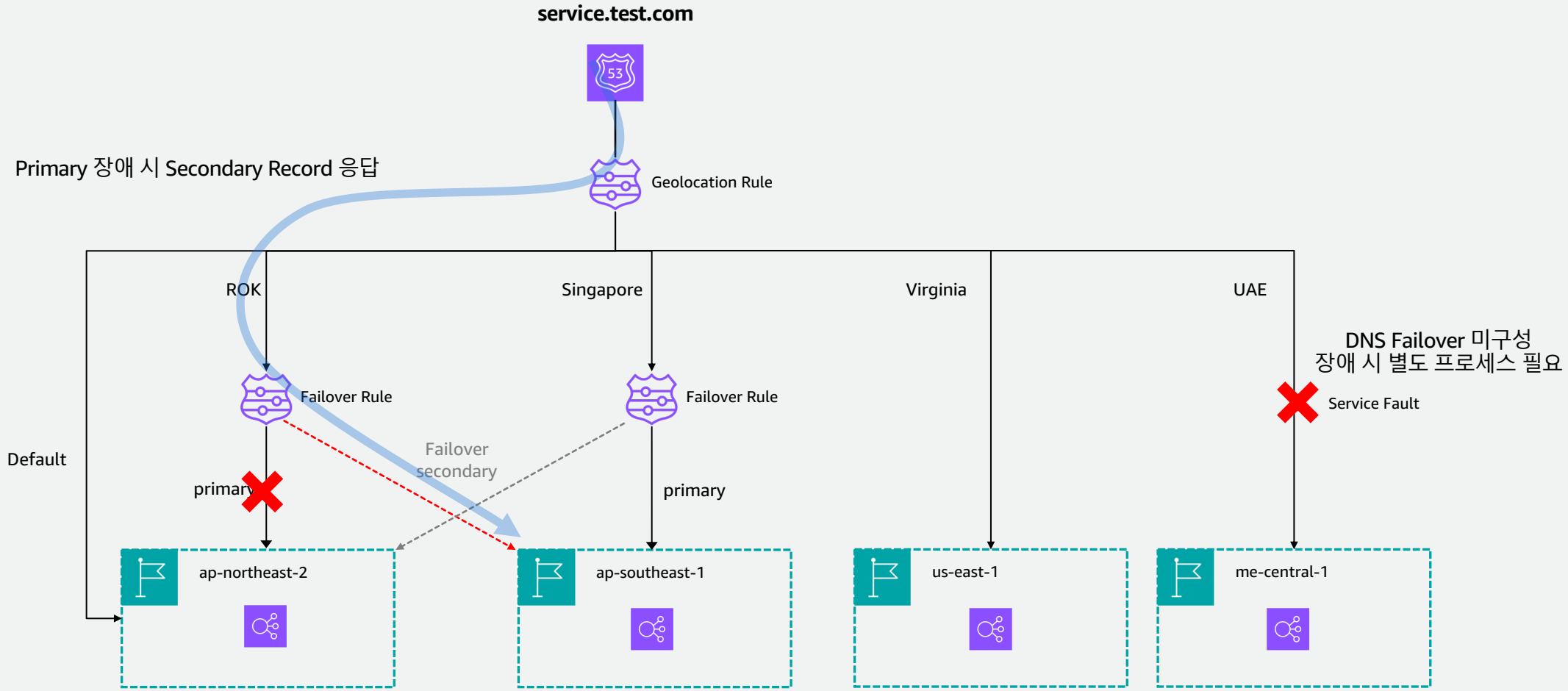
Record name	Routin...	Differentiator	Value/...
apne2-swift.imggooll.com	Failover	Primary	52.79.107...
apne2-swift.imggooll.com	Failover	Secondary	18.138.69...

Failover Rule - singapore

Record name	Routin...	Differentiator	Value/...
apse1-swift.imggooll.com	Failover	Primary	18.138.69...
apse1-swift.imggooll.com	Failover	Secondary	52.79.107...



Route 53 Record Routing Policy



aws professional services

Thank you!