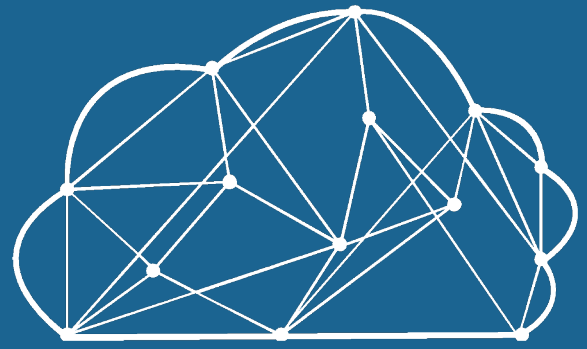
BESPIN GLOBAL



Welcome to AWS

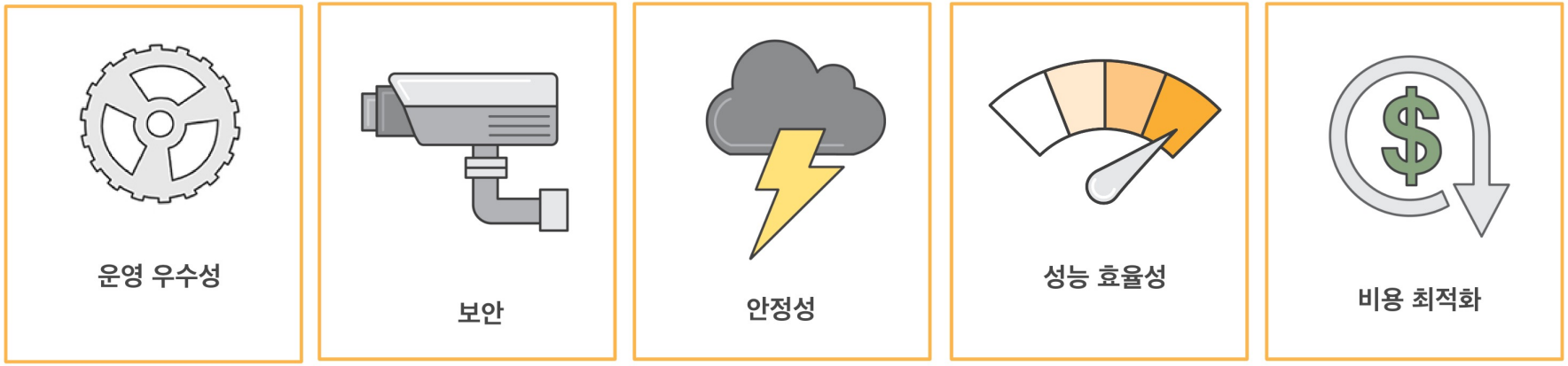
OpsNow ArchOps 심선보(seonbo.shim@bespinglobal.com)

Version 1.0

Welcome

Well-Architected Framework은 무엇인가요?

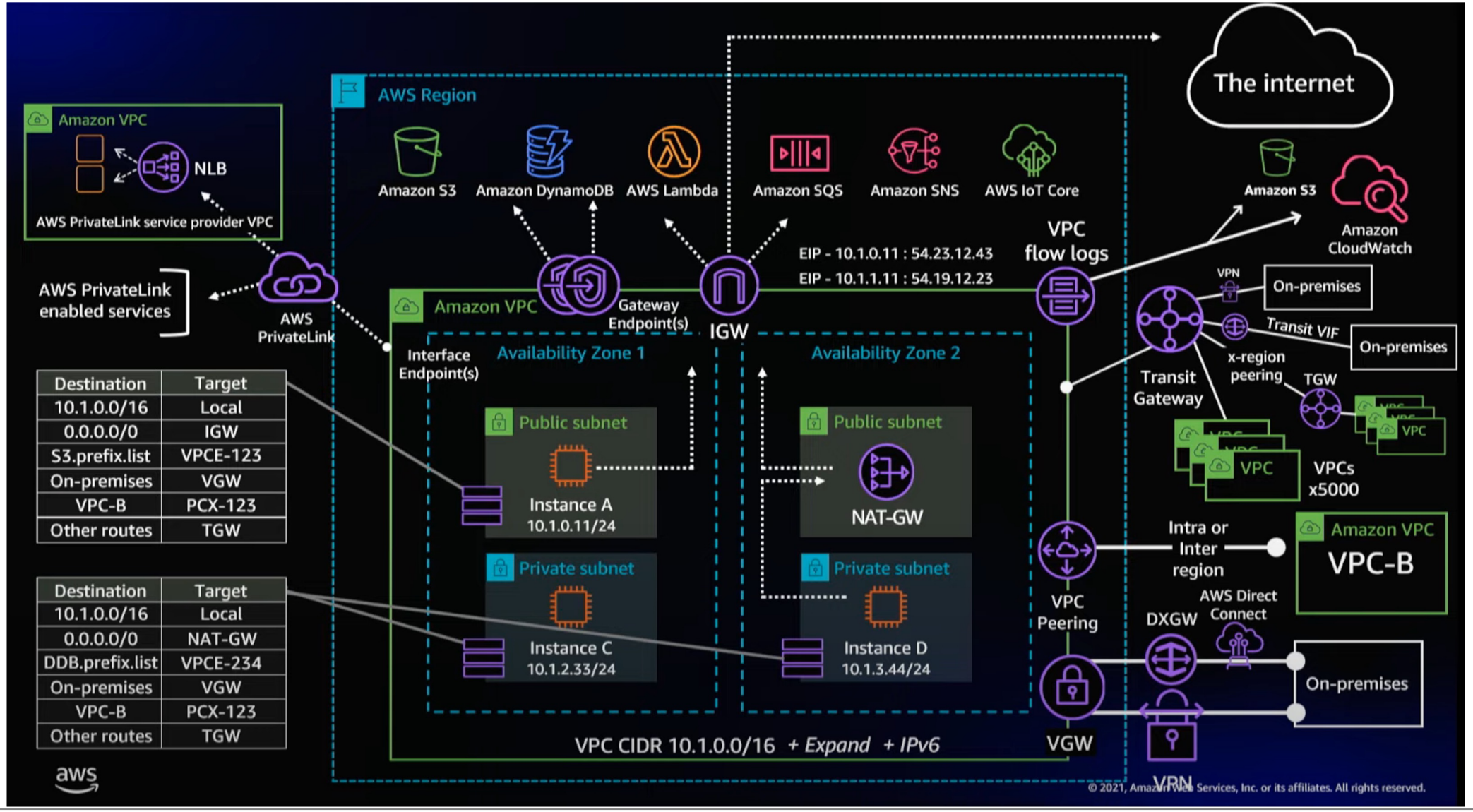
WAF라 함은 고수준의 가이드와 베스트 프랙티스 를 고객 여러분에게 제공하여 보안성, 안정성, 성능 효율성, 비용 최적화, 운영 우수성이 보장되는 어플리케이션을 AWS Cloud상에서 유지할 수 있게 지원합니다.



VPC

기반 마련

VPC Architecture



Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	IGW
S3.prefix.list	VPCE-123
On-premises	VGW
VPC-B	PCX-123
Other routes	TGW

Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	NAT-GW
DDB.prefix.list	VPCE-234
On-premises	VGW
VPC-B	PCX-123
Other routes	TGW

VPC - CIDR

클래스 A Private 서브넷 대역: 10.0.0.0 - 10.255.255.255 CIDR: 10.0.0.0/8 - 16,777,216

클래스 B Private 서브넷 대역: 172.16.0.0 - 172.31.255.255 CIDR: 172.16.0.0/12 - 1,048,576

클래스 C Private 서브넷 대역: 192.168.0.0 - 192.168.255.255 CIDR: 192.168.0.0/16 - 65,535

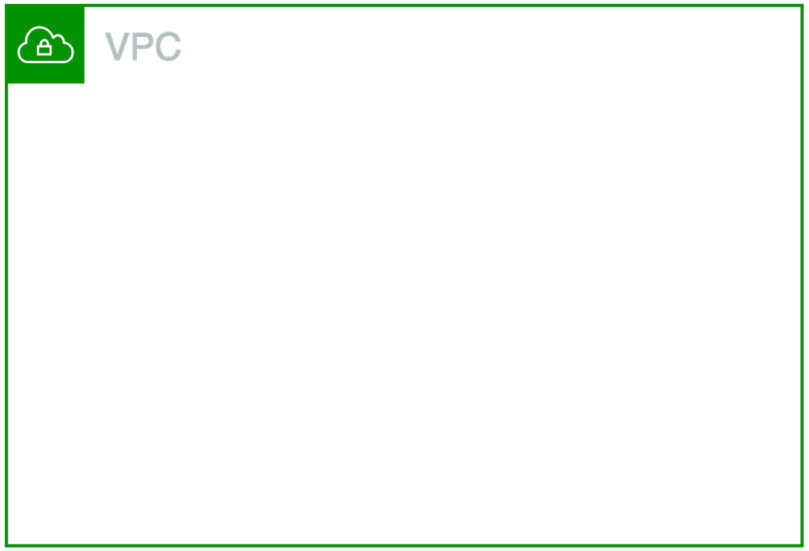
0.0.0.0 => 현재의 네트워크

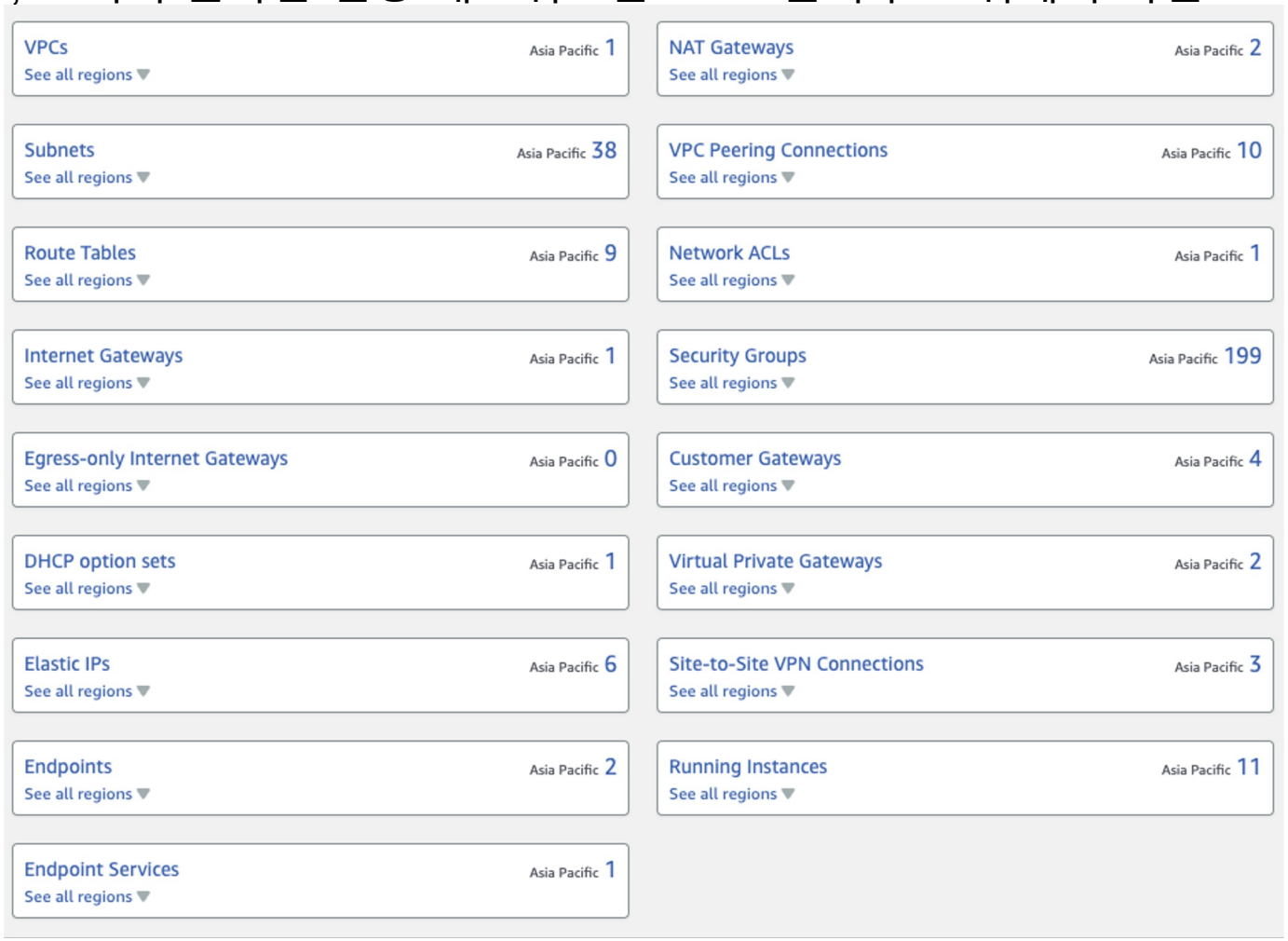
127.0.0.0 => 호스트 자기 자신을 가리키는 Loop Back

172.16.0.0 인 경우 local => VPC 자신을 가리키는 Loop Back

VPC (Virtual Private Cloud)

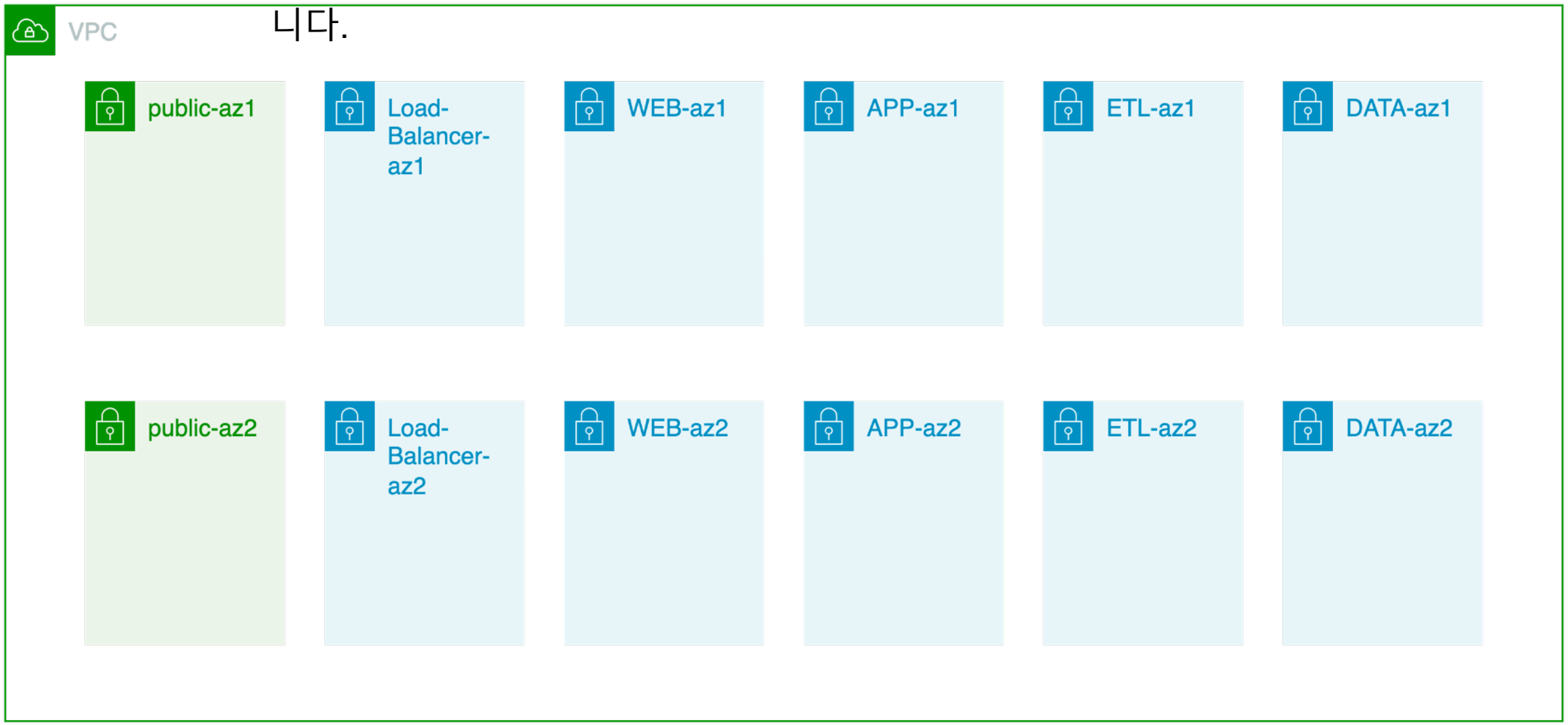
AWS에서 제공하는 가상 네트워킹 환경으로, 고객이 원하는 전용 네트워크를 AWS 클라우드 위에 구축할 수 있도록 해주는 서비스입니다.





VPC - Subnets

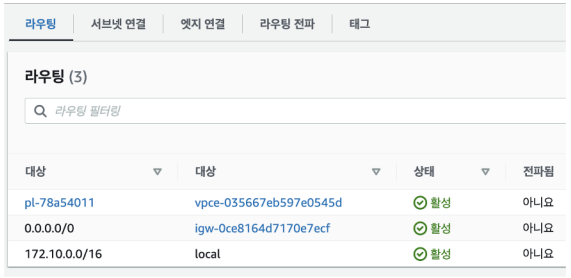
하나의 독립적인 네트워크 공간을 구획하는 네트워크(Subnet) 를 정의하고 그 안에 WEB, API, 데이터베이스, Serverless Lambda 등 컴퓨팅 인스턴스를 배치할 수 있습니다.

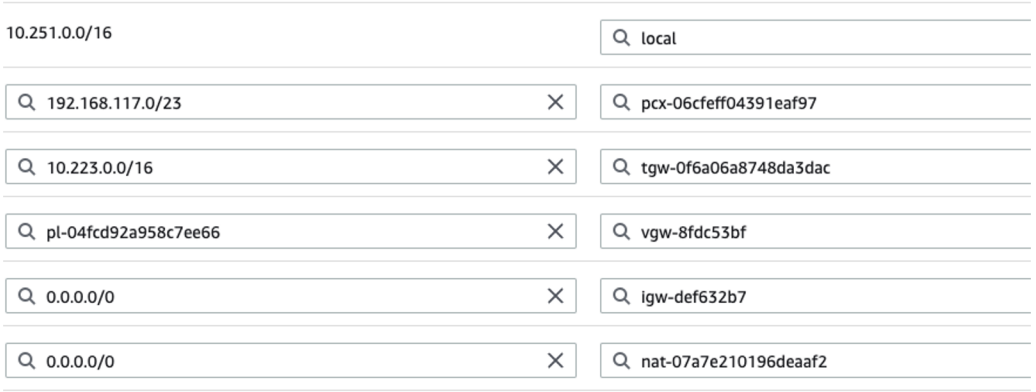


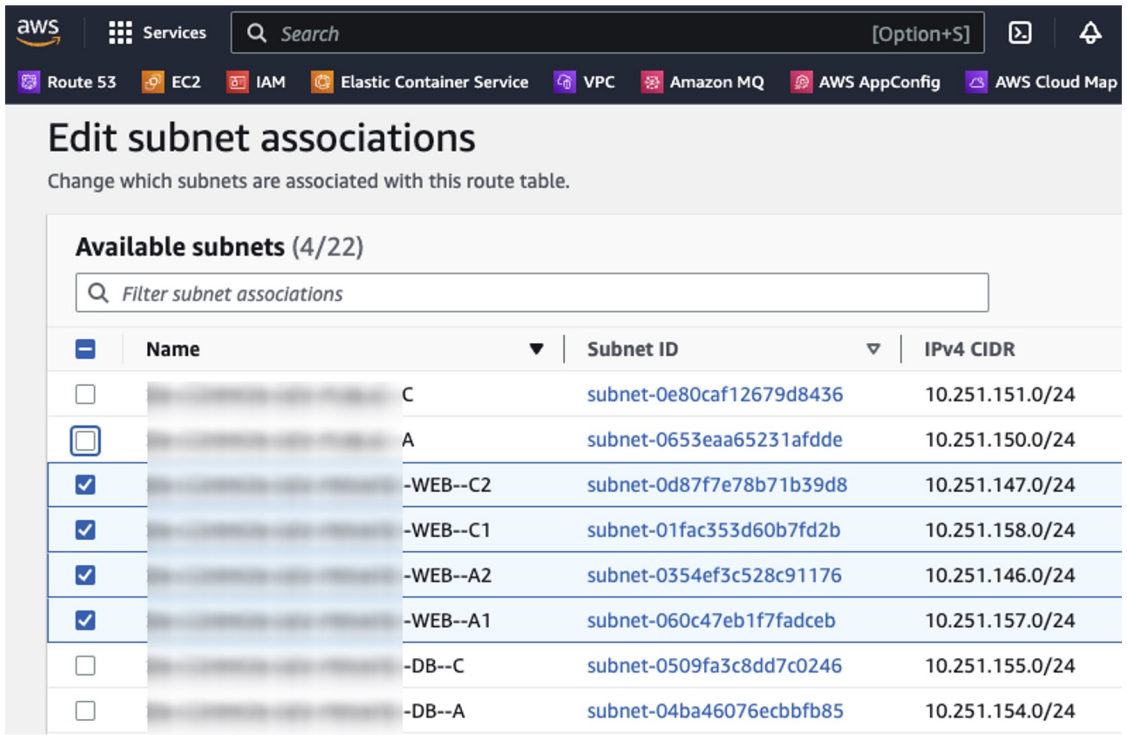
VPC - Route Table

목적지에 정의된 트래픽은 Target 으로 라우팅 되도록 규칙을 정의 합니다.

연결된 서브넷 “WEB” 은 여기에 정의된 라우팅 규칙을 따릅니다.

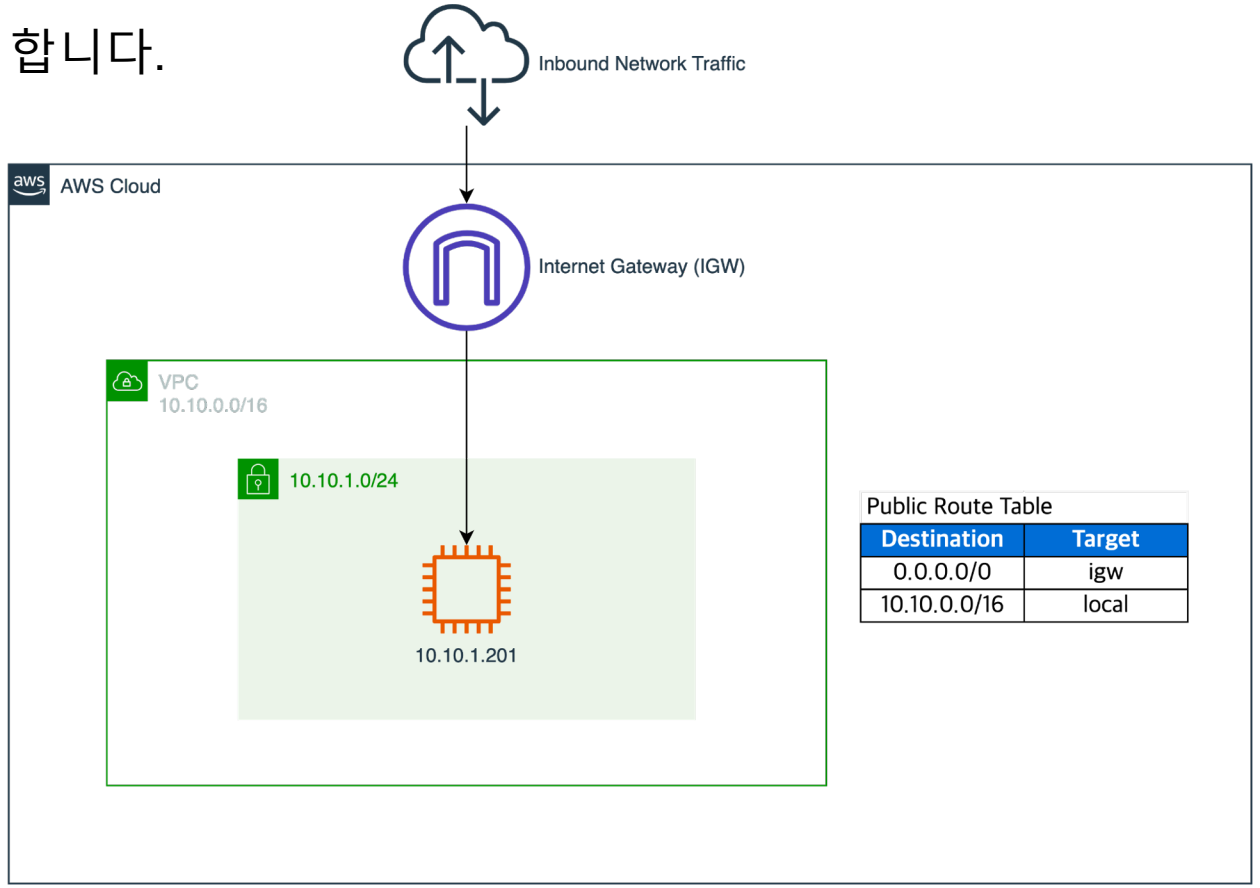






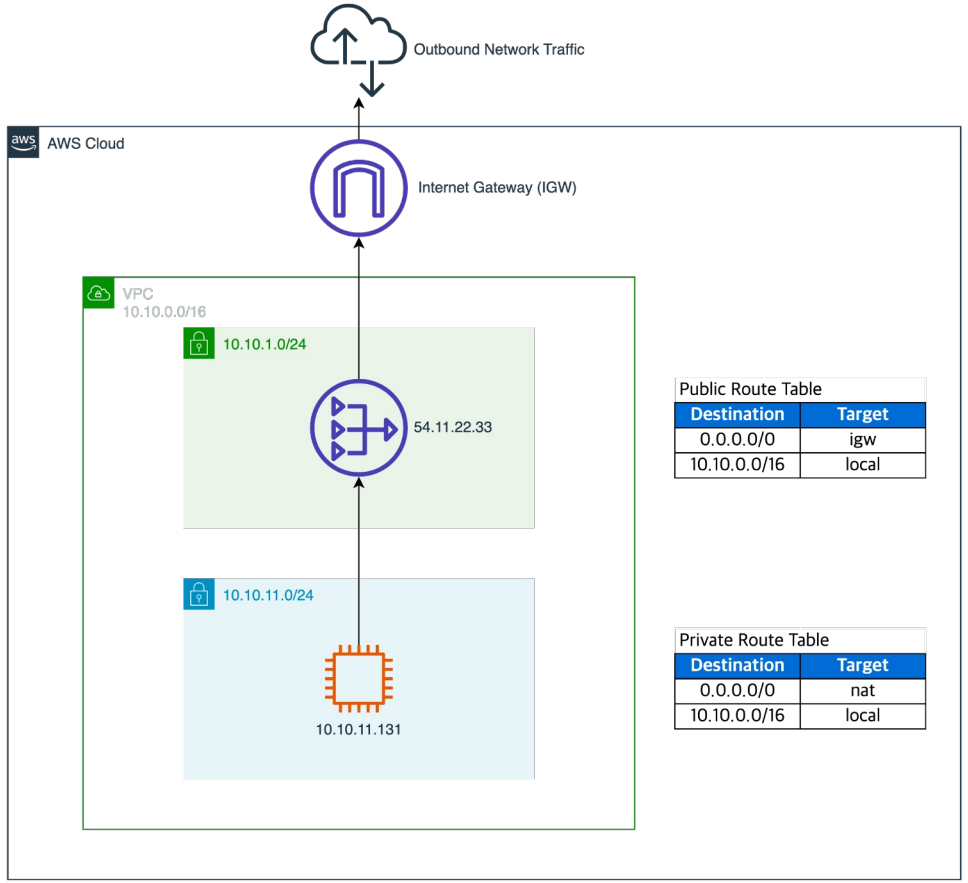
VPC - Internet Gateway

인터넷의 클라이언트(브라우저 및 앱)가 VPC 의 리소스를 액세스 하기 위해선 Internet Gateway 와 구성 되어야 합니다. Internet Gateway 가 Subnet 에 연결되어 있으면 해당 Subnet 은 인터넷과 연결 되므로 Public Subnet 이라고 합니다.

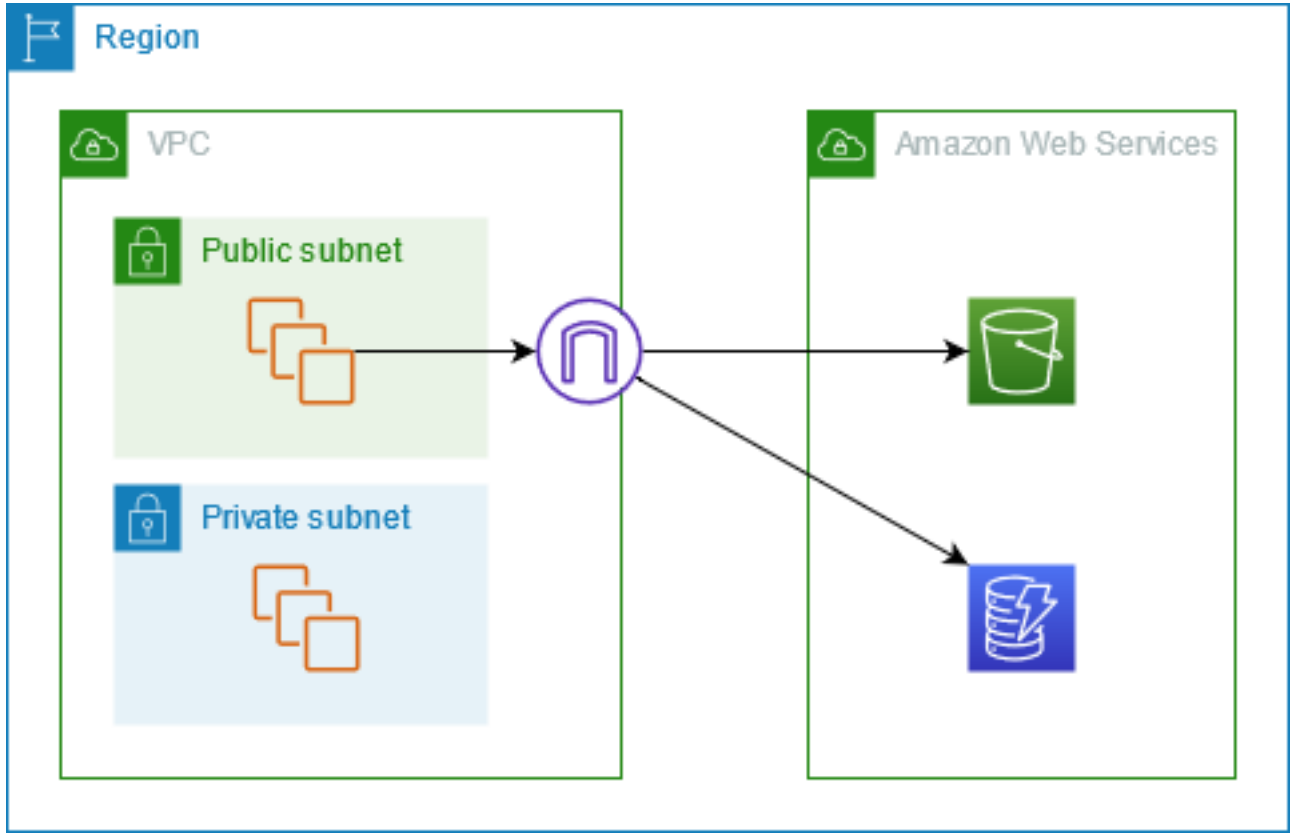


VPC - NAT(Network Address Translation) Gateway

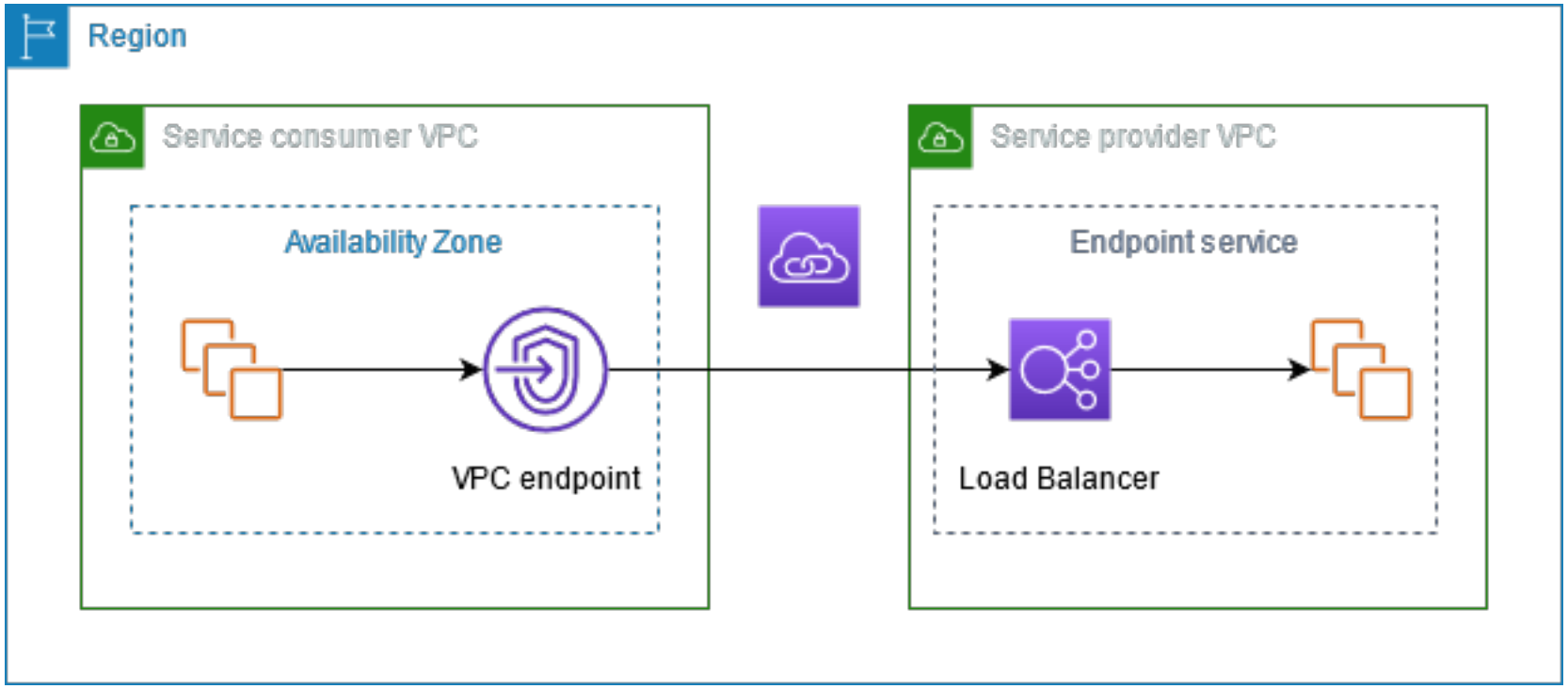
프라이빗 서브넷의 인스턴스가 인터넷에 접속하거나 인터넷에서 프라이빗 서브넷의 인스턴스 접속을 가능하게 합니다. 이를 위해 Private / Public 네트워크 연결을 위해 IP 주소를 변환합니다.



VPC - VPC Gateway Endpoint (S3, DynamoDB)



VPC - VPC Interface Endpoint



VPC 네트워크 보안

Security Group

VPC - Security Group

Inbound rules (38)

Manage tags | Edit inbound rule

Filter security group rules

1

Name	Security group rule...	IP versi...	Type	Protocol	Port range	Source
–	sgr-059f0e89d7e029396	–	Custom TCP	TCP	8090	sg-08ae03a797671e141 / mea-mc1p-costetl-gbs-sg
–	sgr-0083d1a6e2b996...	–	Custom TCP	TCP	8080 - 9140	sg-0082195a3348a76b2 / mea-mc1p-padm-web-sg
–	sgr-0de033955244c19...	–	Custom TCP	TCP	8080 - 9140	sg-05e24f6cca54d0da4 / mea-mc1p-awsbatch-sg
–	sgr-0722c20f3b286641f	–	Custom TCP	TCP	8080 - 9140	sg-02dec432baa99a4da / mea-mc1p-openapi-cost-sg
–	sgr-0f662d71b6d8cda6c	–	Custom TCP	TCP	8080 - 9140	sg-0133e3d77fe169a72 / mea-mc1p-orgtree-web-sg
–	sgr-0252a7051c1624f69	–	Custom TCP	TCP	8080 - 9140	sg-08f2ff09ea8750742 / mea-mc1p-cost-admin-sg
–	sgr-0c4cec8f38973ffc6	–	Custom TCP	TCP	8080 - 9140	sg-0ecd7327ebc46dfa1 / mea-mc1p-cre-api-sg
–	sgr-09868cf5d6c43709b	–	Custom TCP	TCP	8080 - 9000	sg-0b0a0a36b4e778803 / mea-mc1p-gbs-batch-sg
–	sgr-0da29e69b3036c5...	–	Custom TCP	TCP	8080 - 9140	sg-0f3b606a4caa3b6ef / mea-mc1p-gov-web-sg
–	sgr-0778e735b9168e...	–	Custom TCP	TCP	8080 - 9140	sg-0ae1393ed026c2006 / mea-mc1p-cre-web-sg
–	sgr-034116d2510642...	–	Custom TCP	TCP	8080 - 9140	sg-0eb9dff81d5c9e1a6 / mea-mc1p-svcgrp-batch-sg
–	sgr-0d35de0fb4c856171	–	Custom TCP	TCP	8080 - 9140	sg-0596485f903dacbcc / mea-mc1p-cost-web-sg
–	sgr-0c773b1be596bd7...	–	Custom TCP	TCP	8080 - 9140	sg-0ff610a58c0913829 / mea-mc1p-assetaws-proc...
–	sgr-0baac1234a602c315	–	Custom TCP	TCP	8080 - 9140	sg-0fb17e30397164ce5 / mea-mc1p-kpi-web-sg
–	sgr-0421f94fd12c3bc90	–	Custom TCP	TCP	8080 - 9140	sg-0c7a328aafce2b331 / mea-mc1p-kpi-api-sg
–	sgr-0213c72d71049344f	–	Custom TCP	TCP	8080 - 9140	sg-0d7e5952f23530923 / mea-mc1p-sso-web-sg
–	sgr-0536cb44d7cd96ef3	–	Custom TCP	TCP	8080 - 9140	sg-028455757ec331912 / mea-mc1p-padm-api-sg

VPC - Security Group

Inbound rules | Outbound rules | Tags

Outbound rules (13)

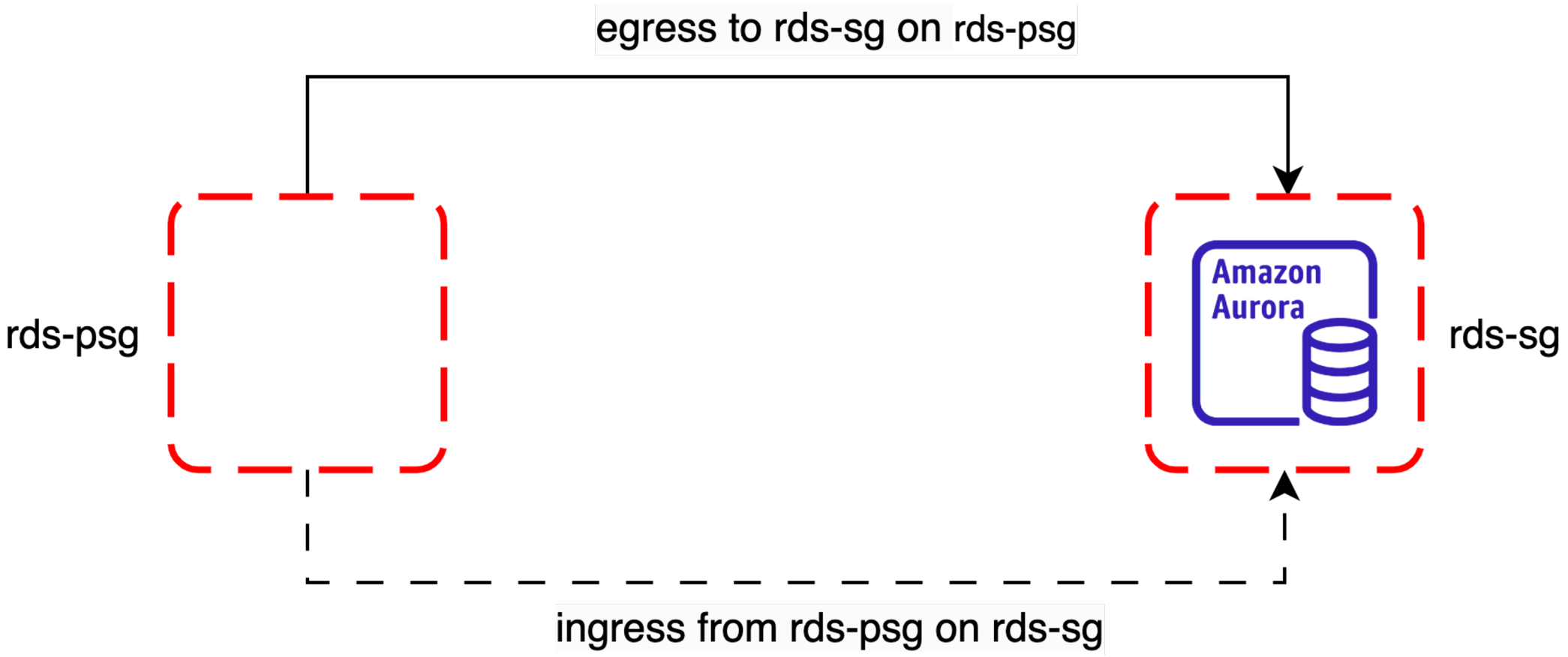
Manage tags | Edit outbound rules

Filter security group rules

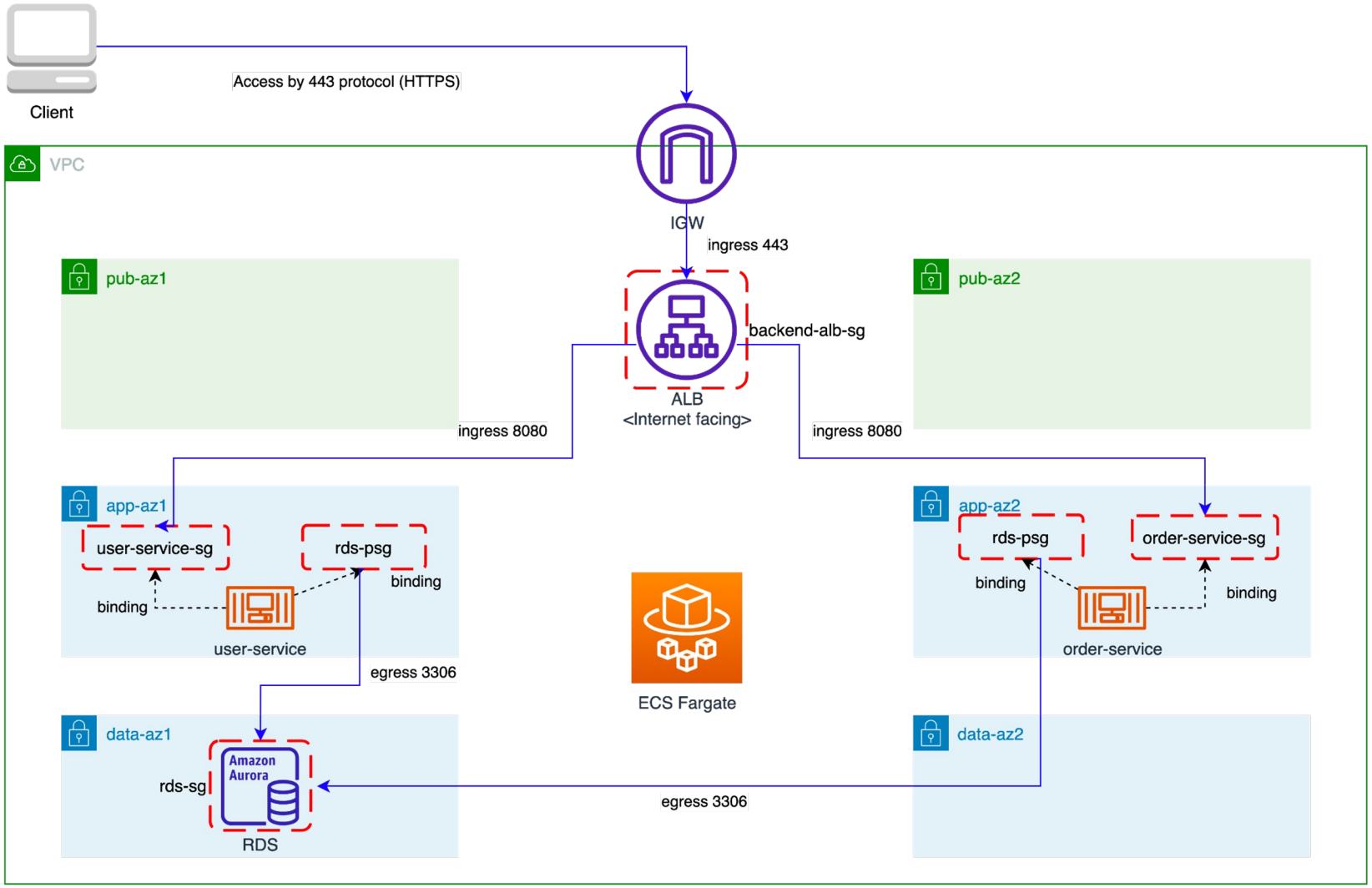
1

Name	Security group rule...	IP versi...	Type	Protocol	Port ra...	Destination	Description
–	sgr-0d10cfe0159e9c392	–	Custom TCP	TCP	8080	sg-0ae12eae9d9cd0cb0 / mea-mc1p-earth-api-sg	mea-mc1p-earth-api
–	sgr-0460a1c2693b8a5...	–	Custom TCP	TCP	8080	sg-0c7a328aafce2b331 / mea-mc1p-kpi-api-sg	mea-mc1p-kpi-api
–	sgr-0e82631321a032f05	–	Custom TCP	TCP	9081	sg-014ba9581c8d73918 / mea-mc1p-costopt-api-sg	mea-mc1p-costopt-api
–	sgr-029f04d4ad1da1078	–	Custom TCP	TCP	9031	sg-0ecd7327ebc46dfa1 / mea-mc1p-cre-api-sg	mea-mc1p-cre-api
–	sgr-0f09dd54c76957e93	–	Custom TCP	TCP	8080	sg-0b0a0a36b4e778803 / mea-mc1p-gbs-batch-sg	mea-mc1p-gbs-batch
–	sgr-03694440fa72a0ba1	–	Custom TCP	TCP	8080	sg-06f97d9cd13cf6df9 / mea-mc1p-costdis-api-sg	mea-mc1p-costdis-api
–	sgr-0e5d9fd6b80cdd564	–	Custom TCP	TCP	8080	sg-0550c1f5f962c9369 / mea-mc1p-portal-app-clssg	mea-mc1p-portal-api
–	sgr-047a85ccdb3f90b43	–	Custom TCP	TCP	9135	sg-028455757ec331912 / mea-mc1p-padm-api-sg	mea-mc1p-padm-api
–	sgr-0f5a2c5cd8f2cfbd2	–	Custom TCP	TCP	8080	sg-0e85235a0a0f48b5c / mea-mc1p-adm-api-sg	mea-mc1p-adm-api
–	sgr-04a8ad0b745c93c10	–	Custom TCP	TCP	8080	sg-0089ed68091ffddad / mea-mc1p-cost-api-sg	mea-mc1p-cost-api
–	sgr-0906ab7e430700...	–	Custom TCP	TCP	9111	sg-0a18bbca1a7bf0416 / mea-mc1p-orgtree-api-sg	mea-mc1p-orgtree-api
–	sgr-022754229e6d1f3a5	–	Custom TCP	TCP	9091	sg-0837c5cf6e8178321 / mea-mc1p-gov-api-sg	mea-mc1p-gov-api
–	sgr-0619be6796245c1...	–	Custom TCP	TCP	8080	sg-0f5f5e895c3e5ba74 / mea-mc1p-asset-apiv2-sg	mea-mc1p-asset-apiv2

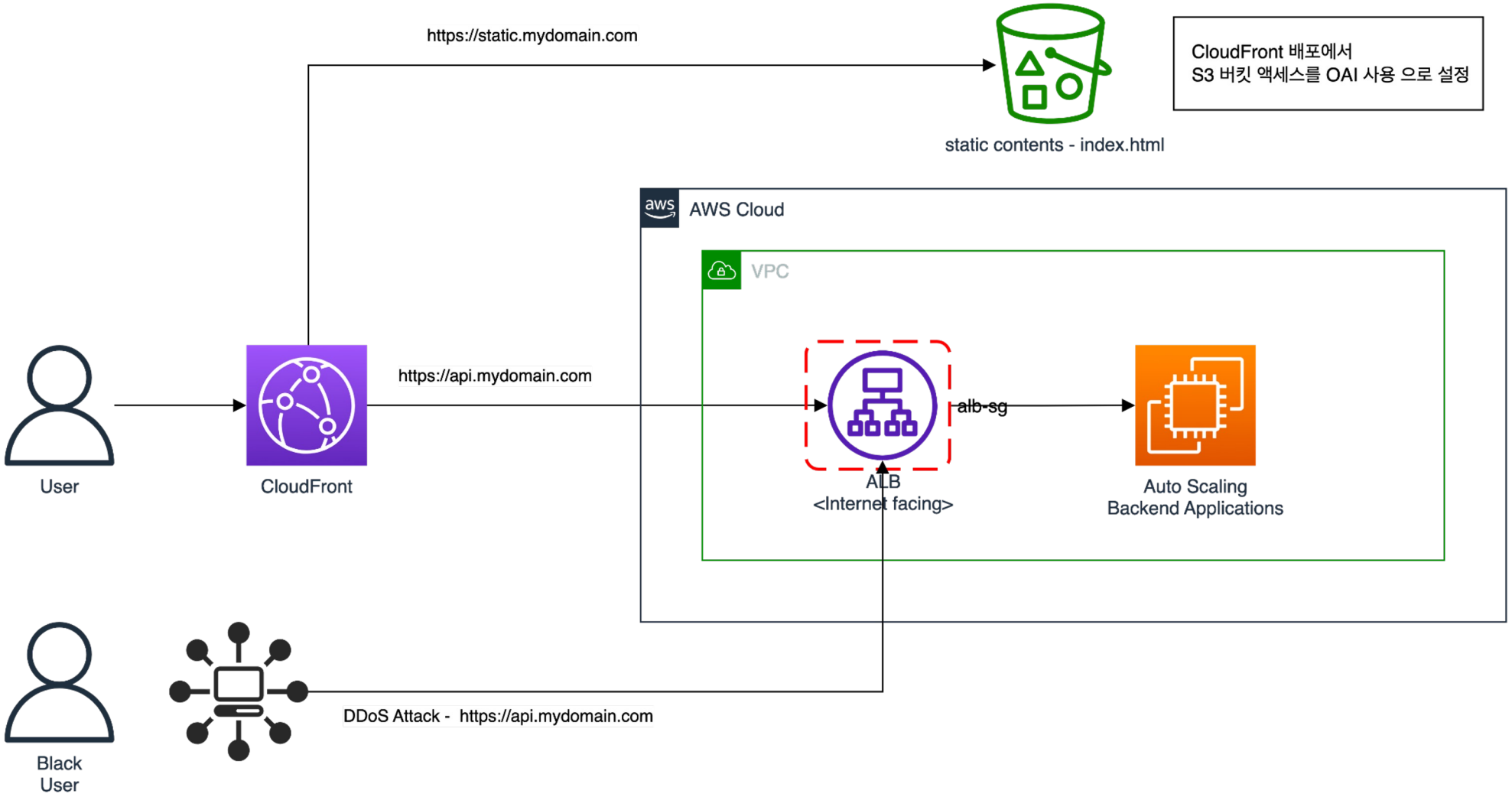
VPC - Security Group



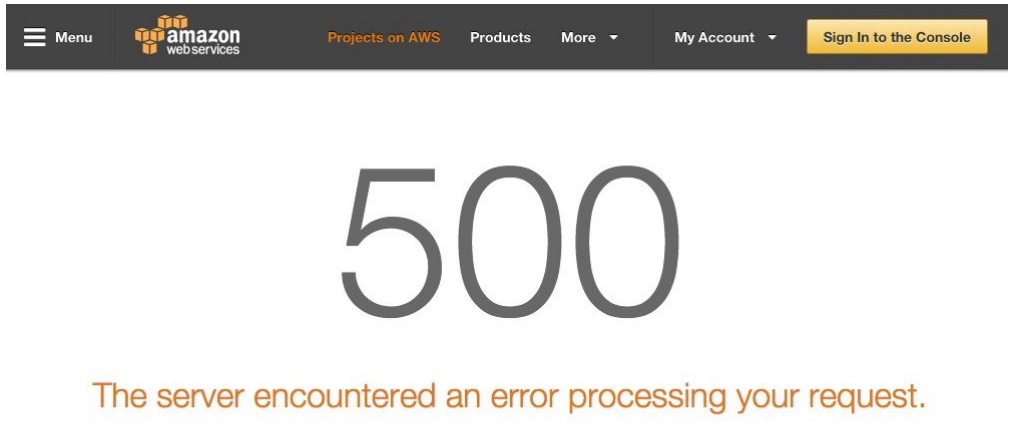
Advanced Security Group Practice



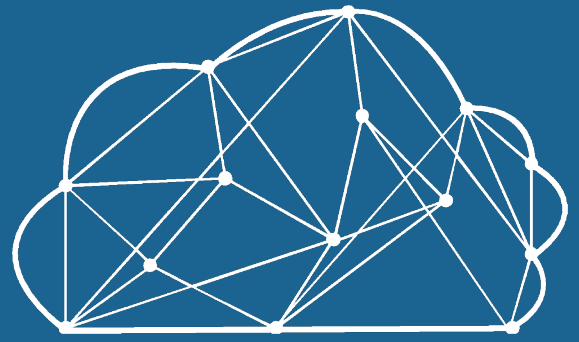
Advanced Security Policy for Service



VPC - 네트워크에서 발생하는 트러블 유형



외부 네트워크 구간	내부 네트워크 구간
• 보안그룹 • 애플리케이션 자체 문제(health 체크 등) • ELB 리스너 및 RULE 우선순위 • R53 Public 레코드 • WAF • 라우팅테이블 • ACM 인증서 문제 • DNS 방화벽 • IGW – 엣지 • NACL • NAT • 인스턴스 자체 방화벽	• 보안그룹 • 애플리케이션 자체 문제(health 체크 등) • R53 Private 레코드 • ELB 리스너 및 RULE 우선순위 • 라우팅테이블 • VPC Endpoint • NACL • 인스턴스 자체 방화벽



감사합니다

BESPIN GLOBAL