[요약] AWS Summit Korea 2022 - 네트워크

Master Seo

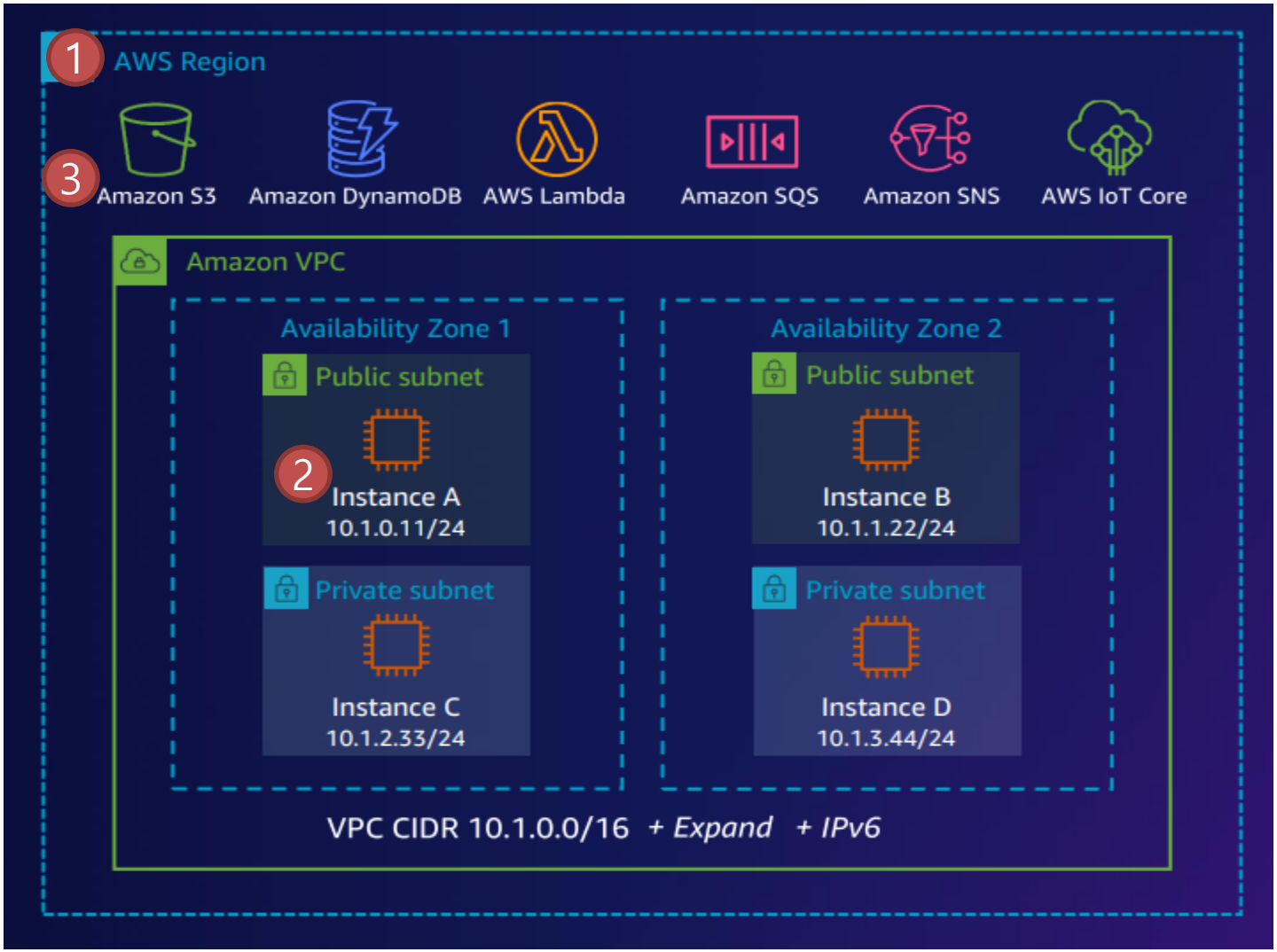
topasvga@naver.com

2022년 10월


내 기술은 모두 한단계 진화한다!

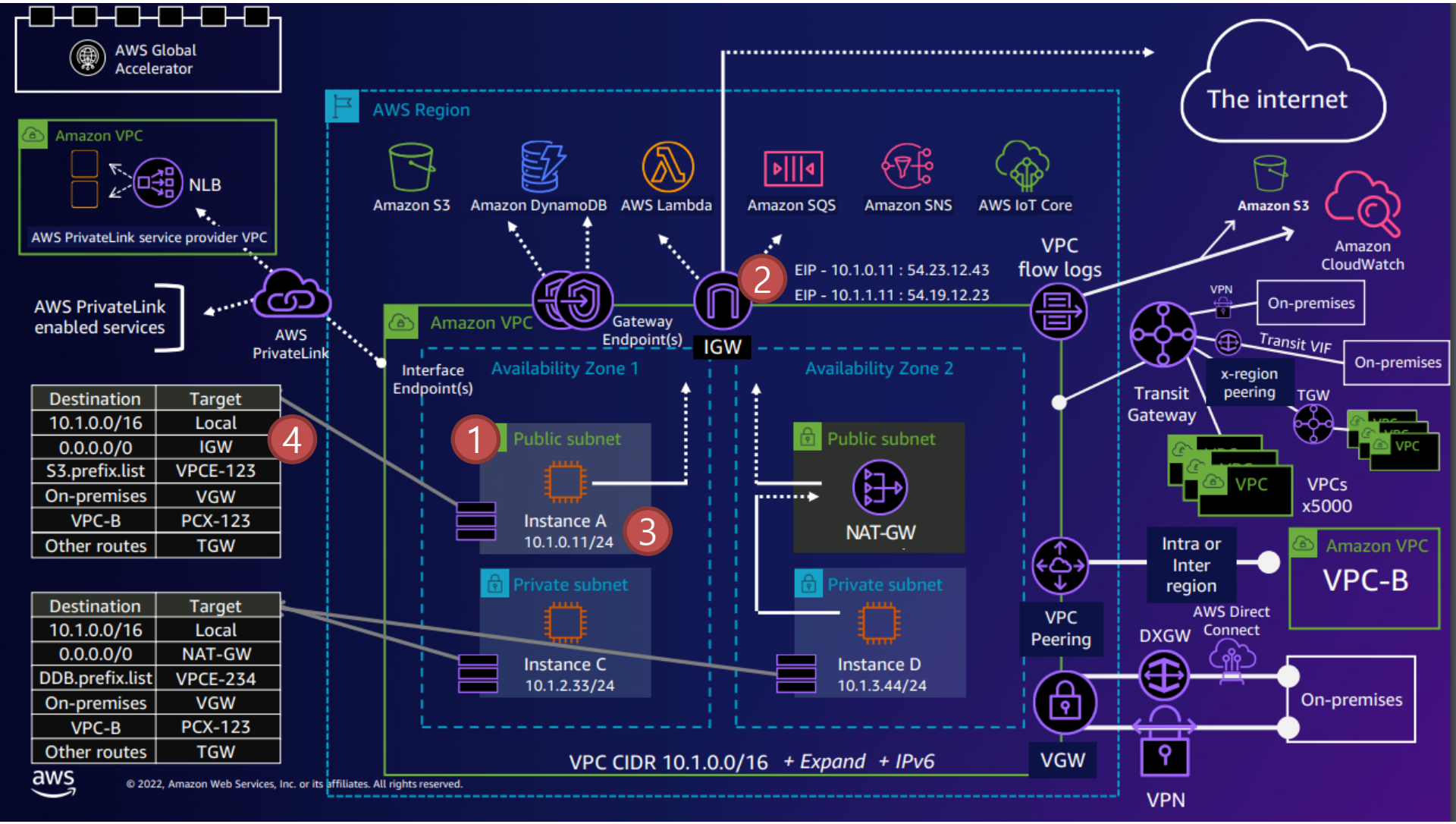
네트워크 아키텍처 목차

1. 리전, PVC , AZ , 서브넷 , VPC 내 서비스, VPC 외부 서비스



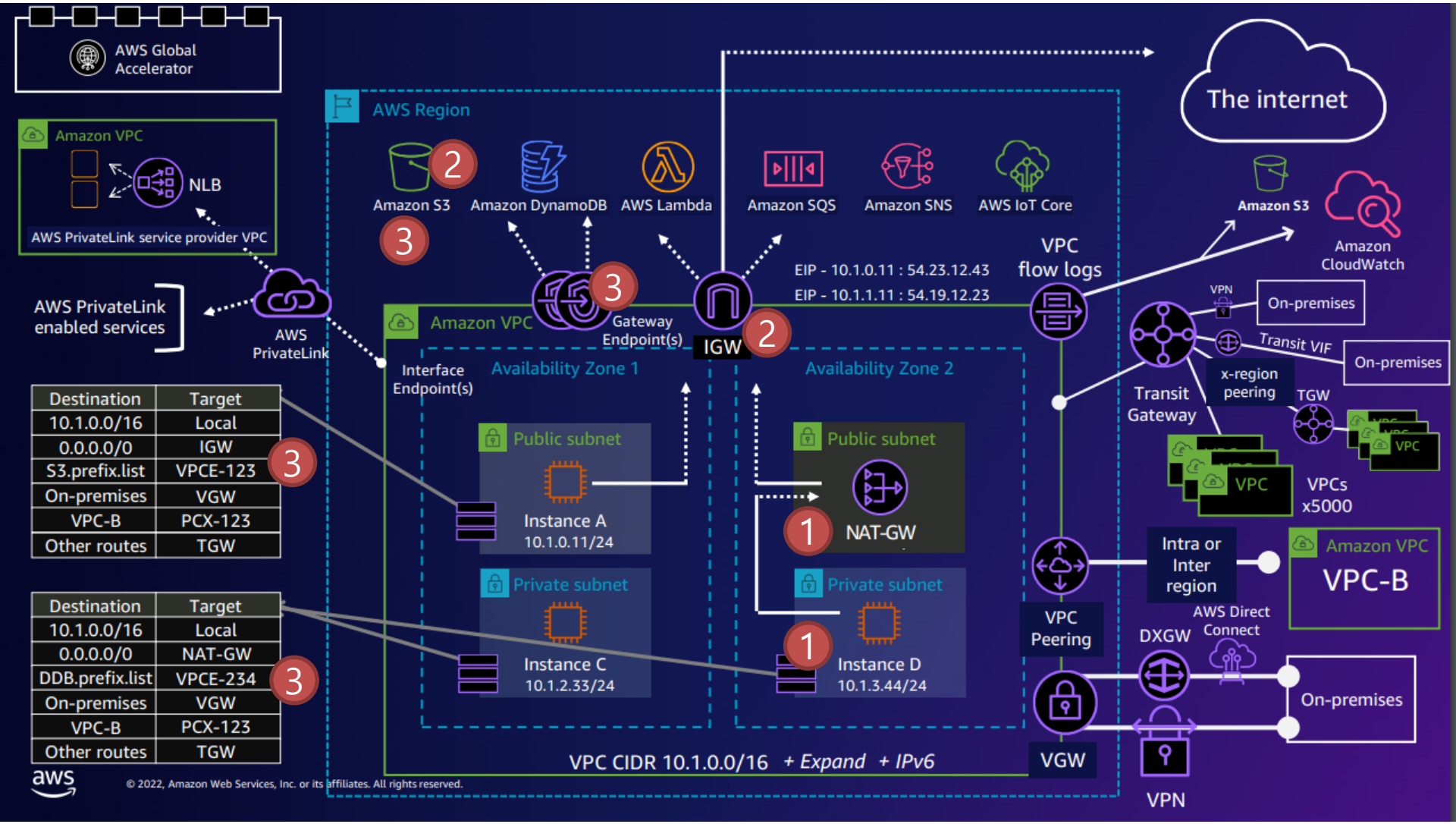
1. 리전 > VPC > AZ1, AZ2 > Pub Subnet > Private Subnet
2. VPC내부서비스와 외부서비스가 있다는 것에 대한 인지
3. VPC외부에 있는 서비스 S3 , Dynamodb , Lambda , IoT Core
4. 보안상 VPC외부 서비스 관리 필요하다. VPC를 통한 S3접근, 람다 VPC에 구축

2. 라우팅, IGW, 1:1NAT, NATGW , S3 endpoint , DX , VPN , Peering ,TGW, Flow-logs,Private-Link, GA



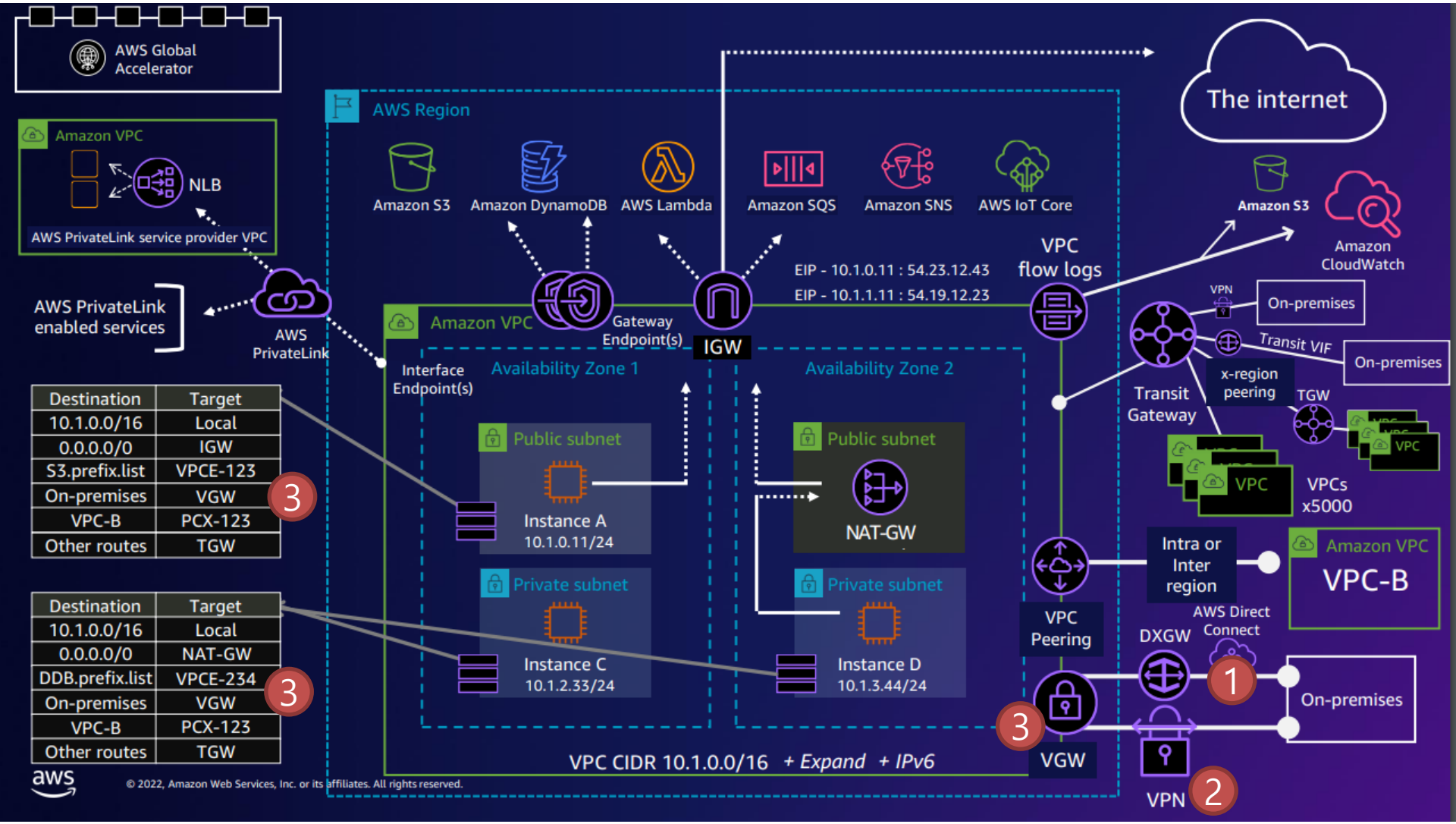
1. 퍼블릭 서브넷과 프라이빗 서브넷
2. 퍼블릭은 공인IP를 매칭시키면 외부에서 접속가능한 네트워크, 프라이빗은 그렇게 안된다.
3. 퍼블릭 서브넷과 프라이빗 서비넷의 구분은 어떻게 하나? 라우팅 테이블
4. 0.0.0.0/0 IGW 가 있는 라우팅 테이블을 서브넷에 적용하면 퍼블릭 서브넷이 된다.

3. 라우팅, IGW, 1:1NAT, NATGW , S3 endpoint , DX , VPN , Peering ,TGW, Flow-logs,Private-Link, GA



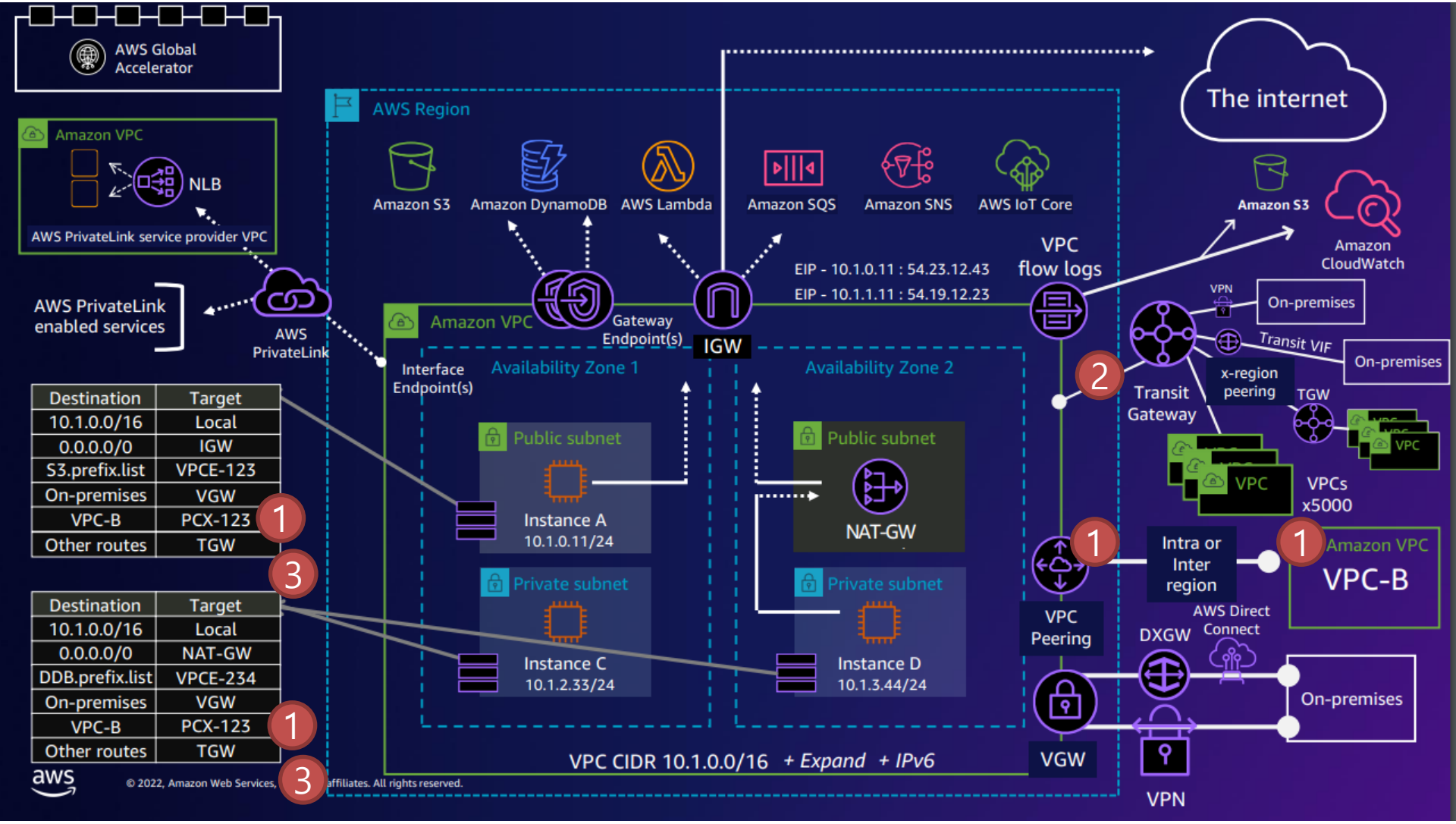
1. 프라이빗 서브넷이 외부 인터넷으로 접속하려면 NAT가 반드시 있어야 한다. NAT는 퍼블릭에 위치한다. 퍼블릭 서브넷만 외부와 통신이 가능하다.
2. 서버에서 S3와 다이나모 디비와 같이 VPC 외부에 서비스와 통신할때는 기본은 IGW를 통해 통신한다.
3. 이 부분은 내부 통신으로 변경하는것은 게이트웨이 엔드포인트 서비스이다. 라우팅 테이블이 추가된다

4. 라우팅, IGW, 1:1NAT, NATGW , S3 endpoint , DX , VPN , Peering ,TGW, Flow-logs,Private-Link, GA



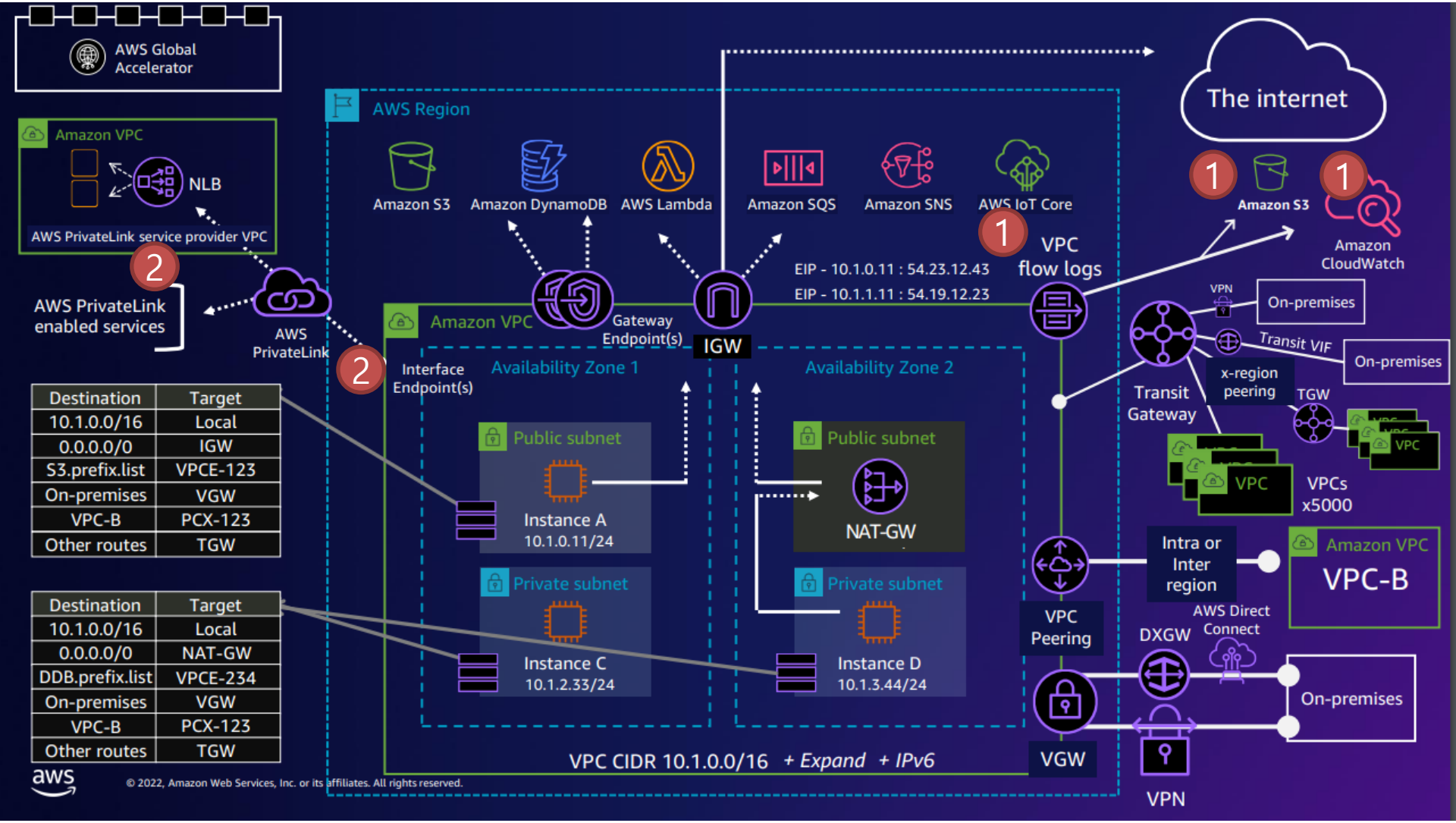
1. AWS VPC와 온프라미스를 연결하는 방법은 Site to Site VPN을 연결하거나, 전용선을 연결하는 AWS Direct Connect 서비스 2가지 이다.
2. 다이렉트 컨넥트 서비스는 고가이므로 일반적으로 Site to Site VPN을 사용한다.
3. VPC에 있는 서버에서 온프라미스로 가려면 가상게이트웨이(VGW)를 통해 가면 된다. 전용선 또는 VPN연결후

5. 라우팅, IGW, 1:1NAT, NATGW , S3 endpoint , DX , VPN , Peering ,TGW, Flow-logs,Private-Link, GA



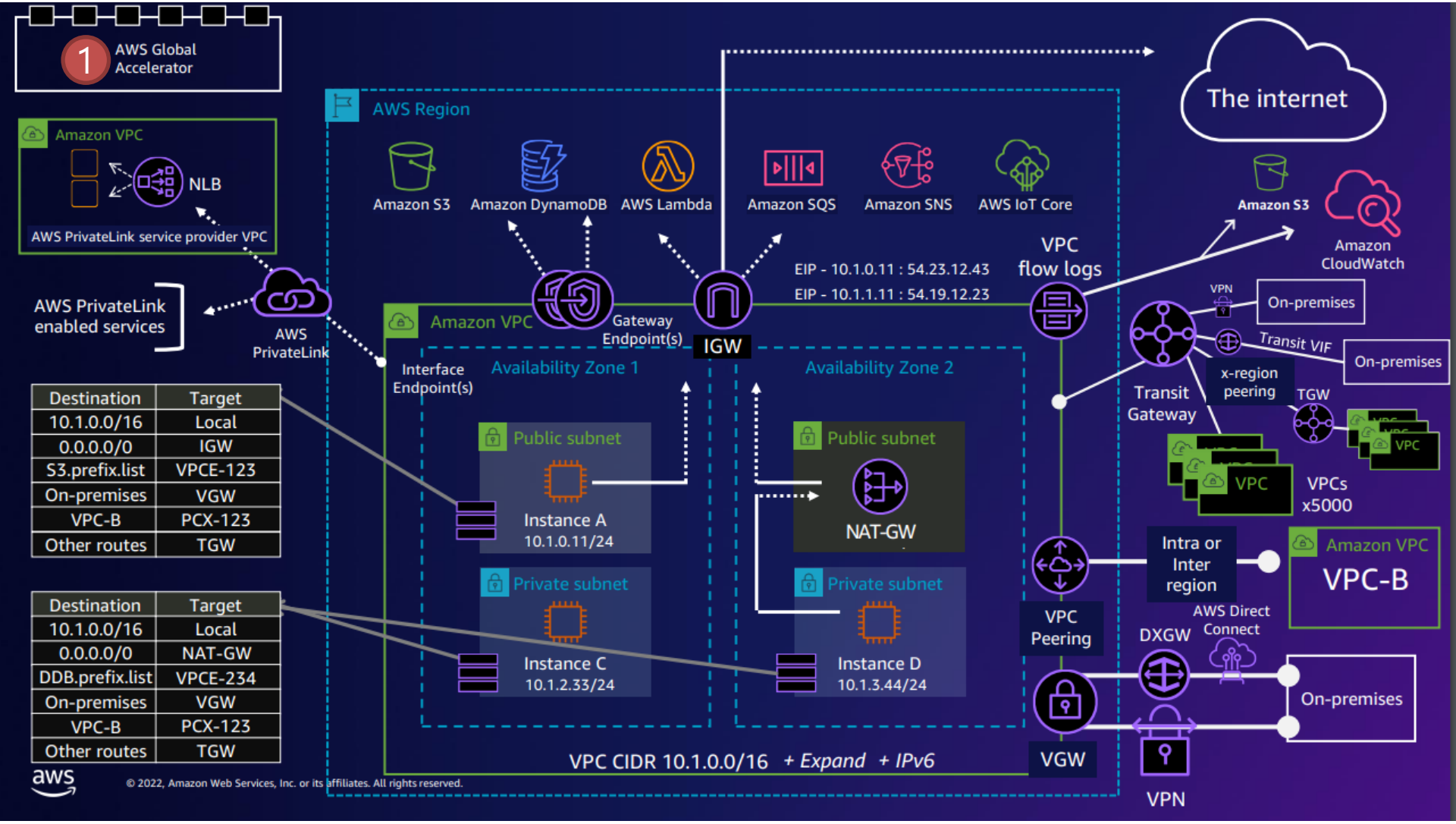
1. VPC피어링은 다른 AWS VPC 인 VPC-B로 가려면 VPC-B블럭에 대해 피어링연결로 라우팅 잡아줘야한다.PCX-123
2. 트랜짓 게이트웨이를 통해서 온프라미스와 VPC를 연결할수 있다. 온프라미스는 전용선과 VPN연결이 되어야 한다.
3. 트랜짓 게이트웨이에서 라우팅을 잡아주어야 해당 네트워크로 간다.

6. 라우팅, IGW, 1:1NAT, NATGW , S3 endpoint , DX , VPN , Peering ,TGW, Flow-logs,Private-Link, GA



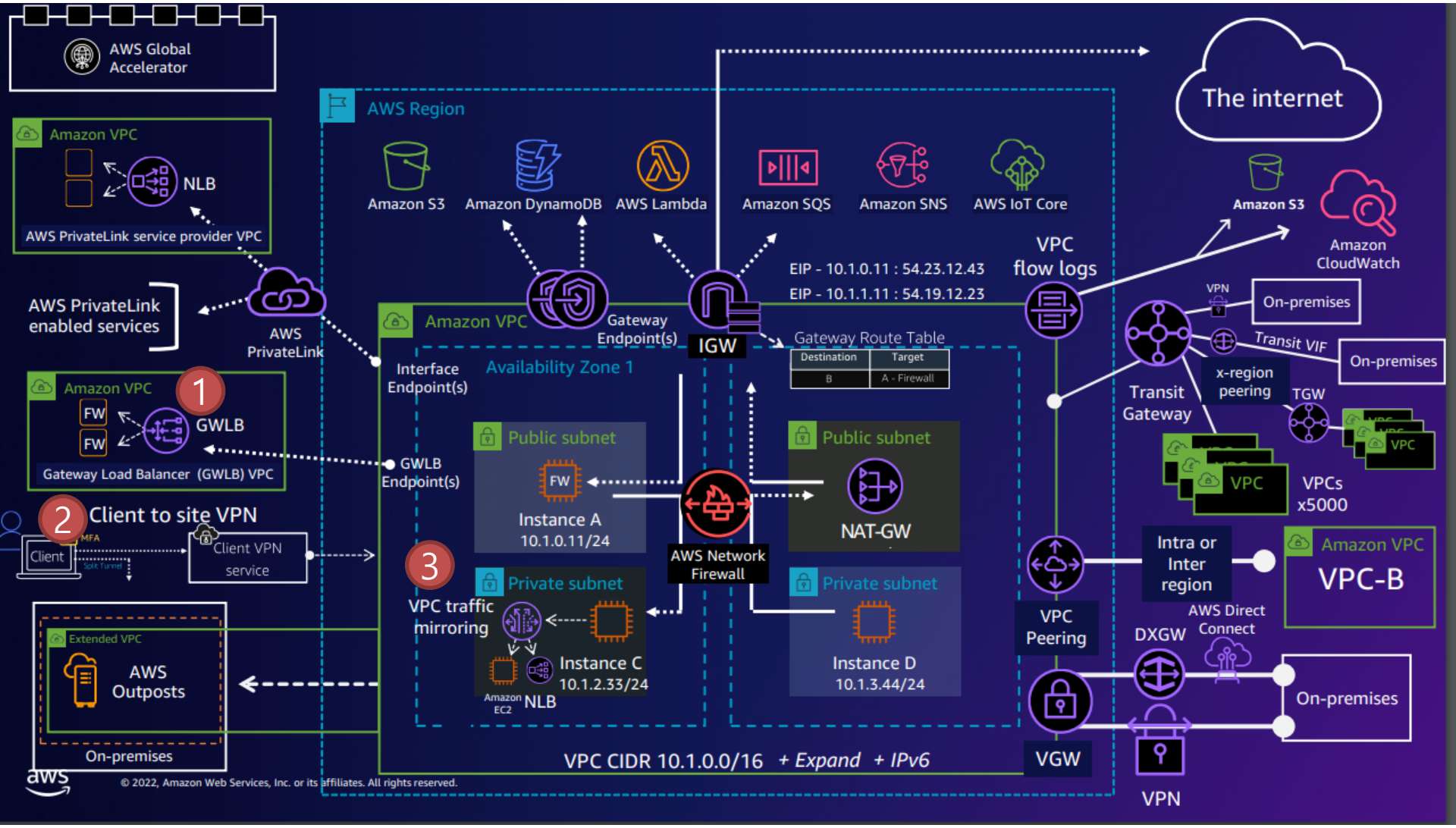
1. VPC에 VPC Flow logs설정을 통해 외부에서 VPC내부 서버로 접속로그나 내부에서 외부로 연결 로그를 남길수 있다.
2. VPC에서 인터페이스 엔드포인드, 엔드포인트 서비스(프라이빗 링크)를 통해서도 내부 통신으로 외부 리소스와 연결할 수 있다. 이 경우 인터페이스를 추가해 사용하는것이라 라우팅테이블은 없다.

7. 라우팅, IGW, 1:1NAT, NATGW , S3 endpoint , DX , VPN , Peering ,TGW, Flow-logs,Private-Link, GA



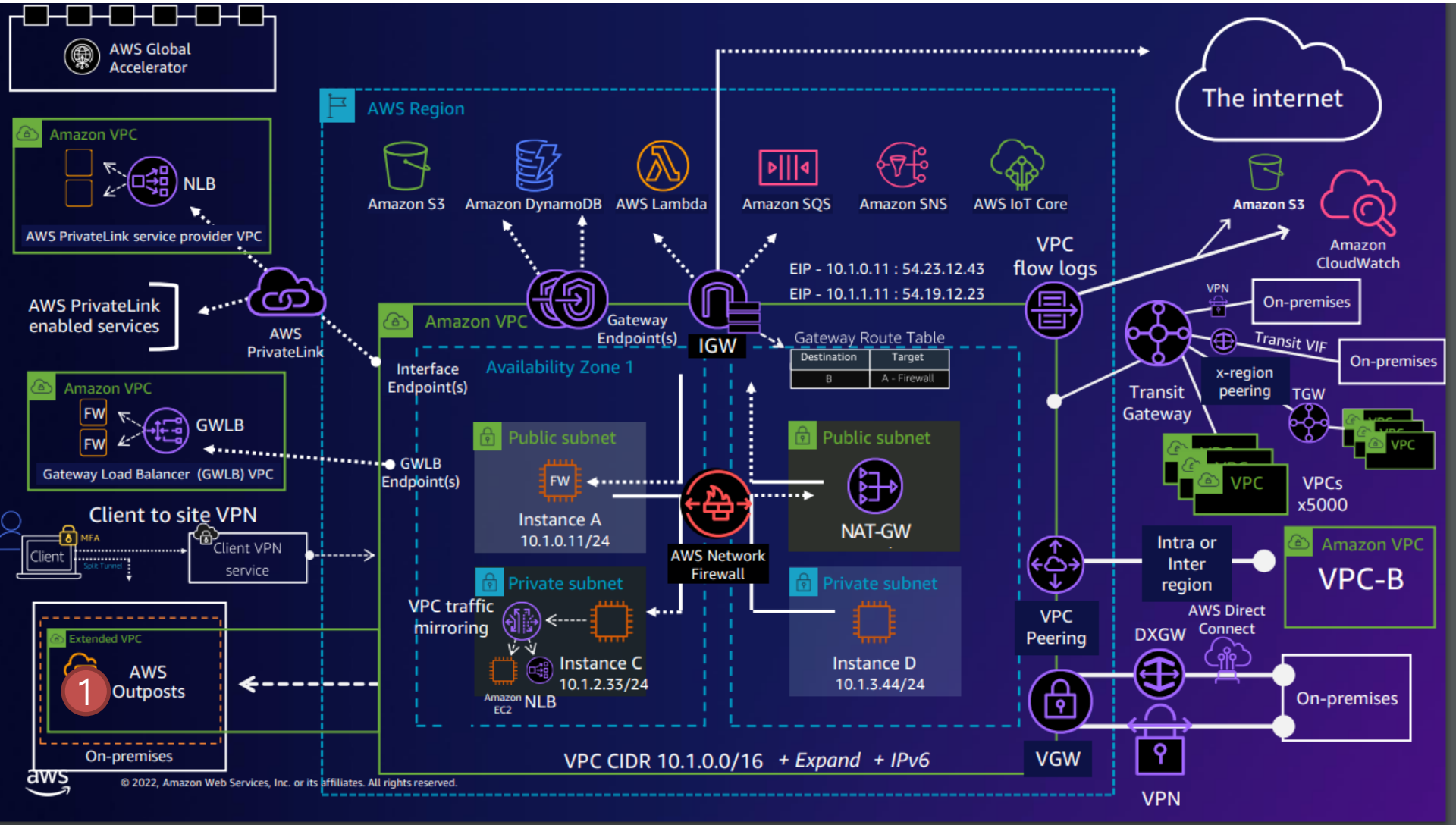
1. Global Accelerator를 사용하면 해외에서 가까운 지역으로 접속하게 해준다.
2. 고정 IP 2개를 제공 받으며 접속을 빠르게 할수 있는 서비스이다.

8. 게이트웨이 로드밸런서, 네트워크 파이어월, 클라이언트 VPN, VPC미러링



1. 게이트웨이 로드밸런서 GWLB - 인그레스 라우팅 설정(IGW Ingress)로 AWS Network Firewall 등 보안장비 구축시 사용하는 로드밸런서.
2. 클라이언트 VPN은 PC에서 VPC내 서버로 직접 접속할수 있게 해준다.
3. VPC 미러링-Nitron System만 지원, 같은 계정 or 원격지 목적지 다른 계정 지정, 침해 서버 점검하는 것.

9. Outposts(온프레미스로 확장)



1. AWS Outposts는 온프렘에 AWS 환경을 연장한 것이다. 온프렘에 AWS서버 랙을 가져다 놓고 AWS를 사용할수 있다.

10. VPC MSR(MORE SPECIFIC ROUTE) - VPC 내부에서 App Sunet ->DB Subnet간 보안존을 거치도록 한다.

VPC MSR: VPC 내부에서 보안 존 디자인

NEW!

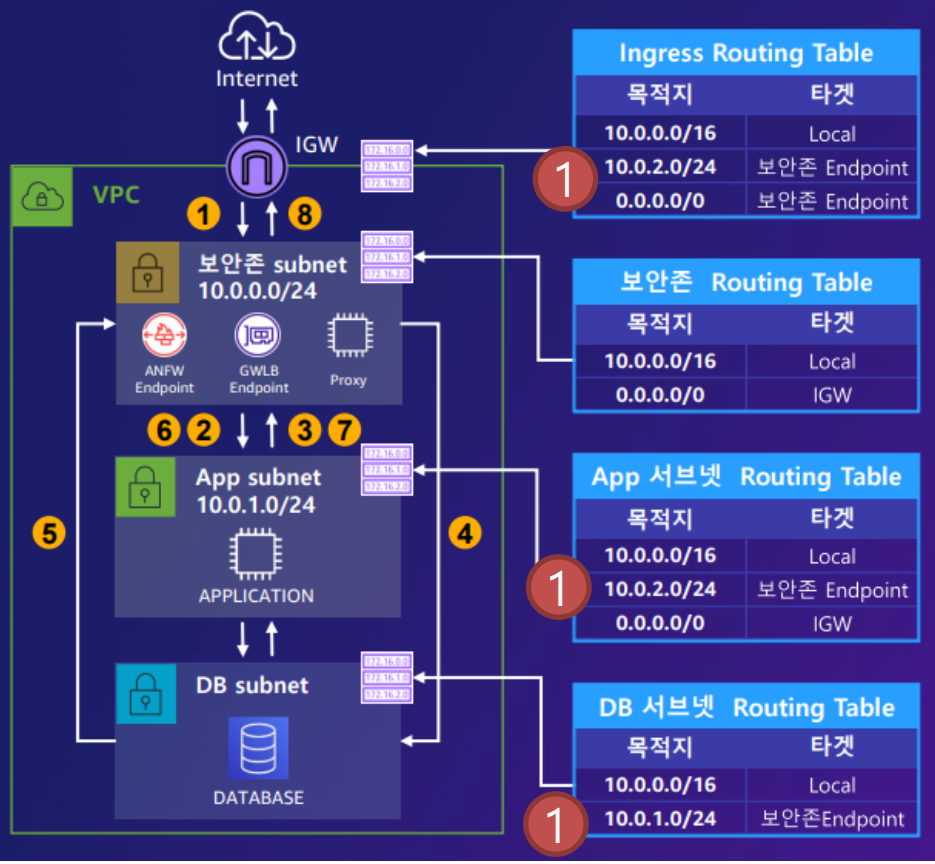
MSR(MORE SPECIFIC ROUTE) 기반의 VPC 내부 라우팅 변경

기술 배경

- VPC MSR (More Specific Route)
- 보안을 위한 VPC 내부의 트래픽 우회 경로 필요

상세 기술

- VPC 내부 기본 라우팅 보다 상세 라우팅 우선 처리
- VPC 내부에서 보안/트래픽 검사를 위한 우회
- VPC 내부 ANFW, GWLB 등의 보안 서브넷 구성



1. 보안을 위해 필요. 기본 VPC 10.0.0.0/16은 서브넷간 기본적으로 서로 통신이 됨.
2. VPC 서브넷간 보안존을 거치도록 하는 법이 필요
3. Pub,Pri,DB = 10.0.0.0/24 10.0.1.0/24 , 10.0.2.0/24 구축
4. 인그레스 라우팅 , 각 서브넷 라우팅 필요

11. S3 PrivateLink - IGW, Endpoint 연결, 라우팅 필요 / VPC interface Endpoint 제공으로 라우팅 없이 접근

S3를 위한 PrivateLink 디자인

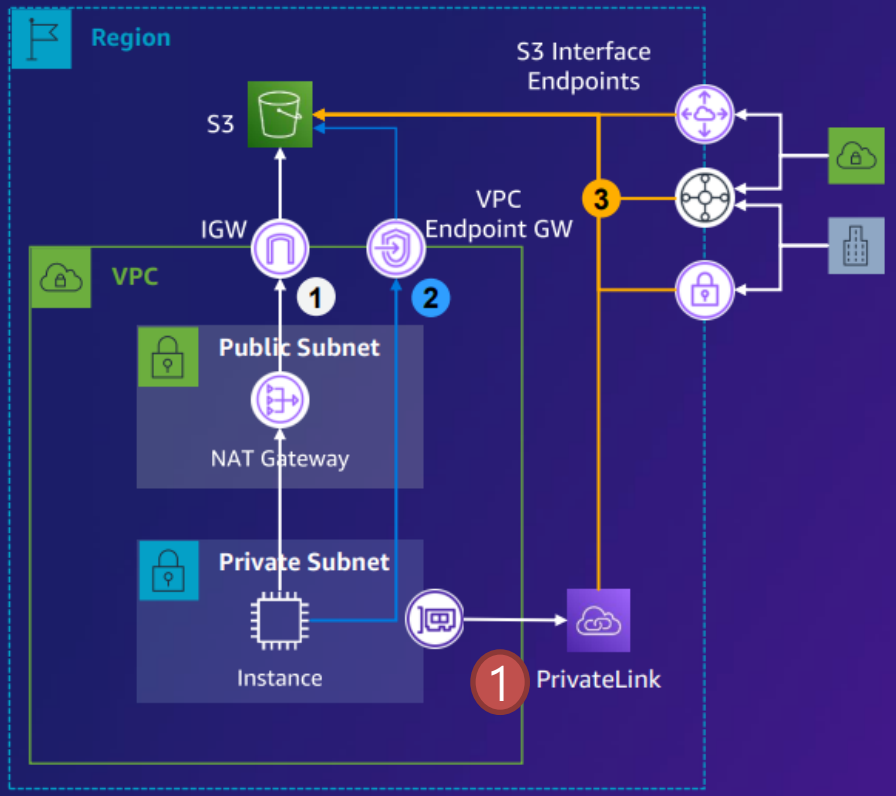
온프렘에서 편리하게 접근하기 위한 S3 PRIVATELINK 지원

기술 배경

- S3 PrivateLink
- 온프렘 환경에서 손쉬운 S3 접근 방법 요구.
- VPC 내부에서 S3 접근을 위한 편의성 요구.

상세 기술

- VPC Interface Endpoint 기반의 S3 접근
- DX, VPN , VPC 내부등에서 Private IP로 S3 접근
- 운영의 복잡성 제거



- ✓ VPC에서 라우팅 없이 S3 접근, 손쉬운 접근 필요. Private Link , 인터페이스로 S3에 접근한다.
- ✓ S3가 Private Link를 지원하게 되었다.

12. Private NAT 디자인 - VPC와 온프렘간 사설IP로 통신

Private NAT 디자인

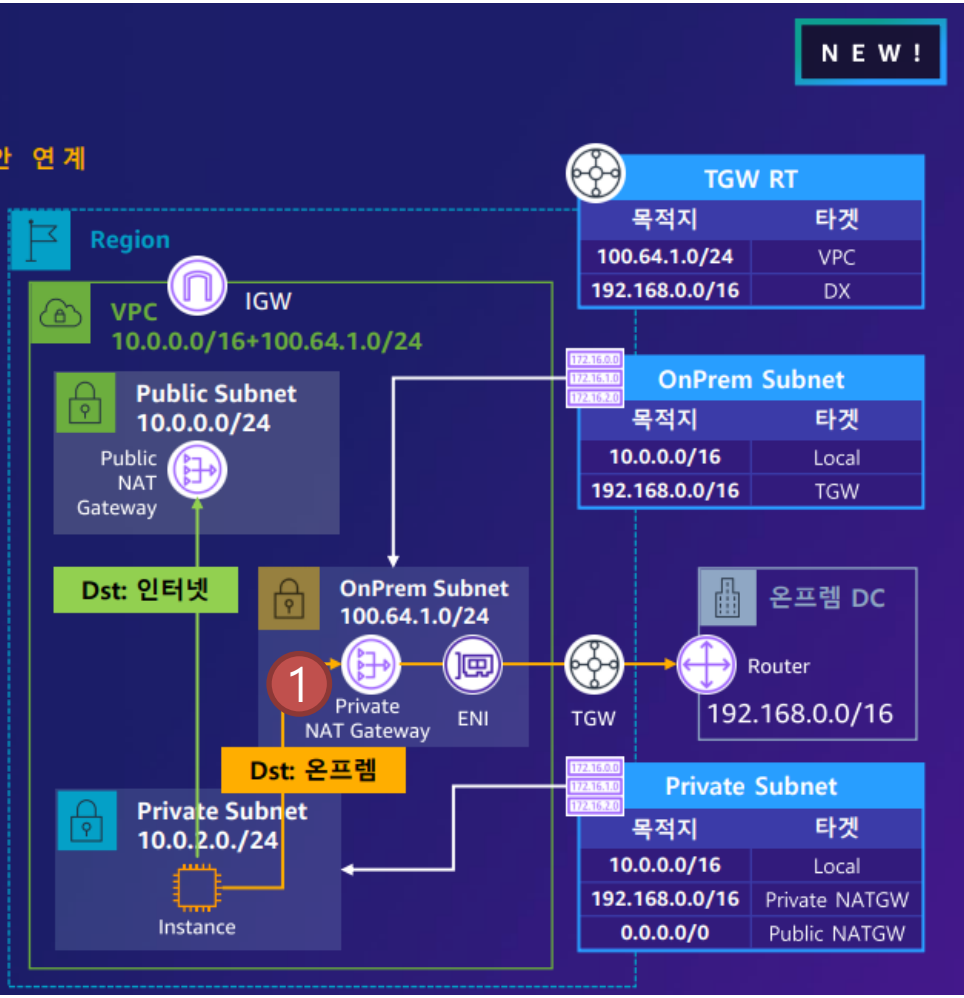
NAT GATEWAY를 통한 PRIVATE NAT 구성으로 ONPREM 보안 연계

기술 배경

- NAT Gateway Private NAT
- 온프렘 환경과 연동시 보안을 위한 고정 사설 IP 필요.

상세 기술

- IGW가 없는 서브넷에 NAT Gateway 배치
- NAT Gateway가 CIRD 주소 기반의 NAT 처리
- OnPrem과 연동시 사설 IP 기반 보안 강화 가능



1. VPC에서 온프렘 연동시 보안을 위해 고정 사설IP 필요
2. 온프렘 192.168.0.0/16이라 가정
3. vpc, pub , pri , 온프렘 서브넷
4. Pri 라우팅, 온프렘 서브넷 라우팅, TGW라우팅 작성 필요

13. NLB생성하고 ALB를 타켓그룹으로 지정- ALB가 동적 IP를 사용할때 , 고정IP를 요구할때 사용

NLB 를 위한 ALB Target Group 디자인

NEW!

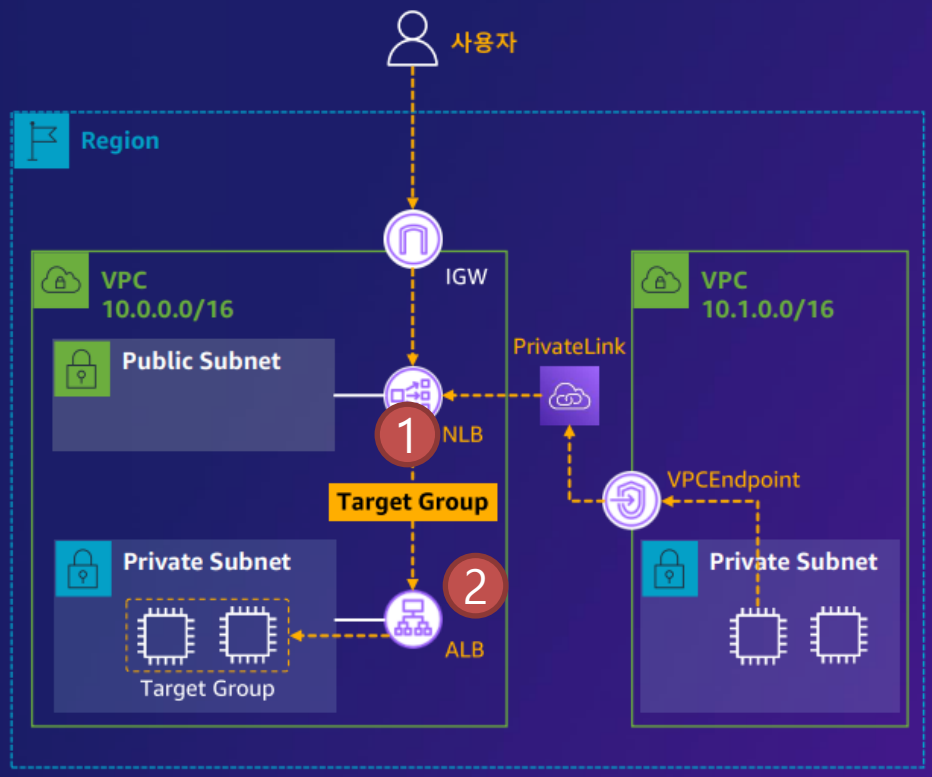
고정 IP 요구를 위한 NLB 기반 ALB TARGET GROUP

기술 배경

- NLB를 위한 ALB Target Group
- ALB의 동적 IP 주소 할당으로 인한 관리 어려움 호소

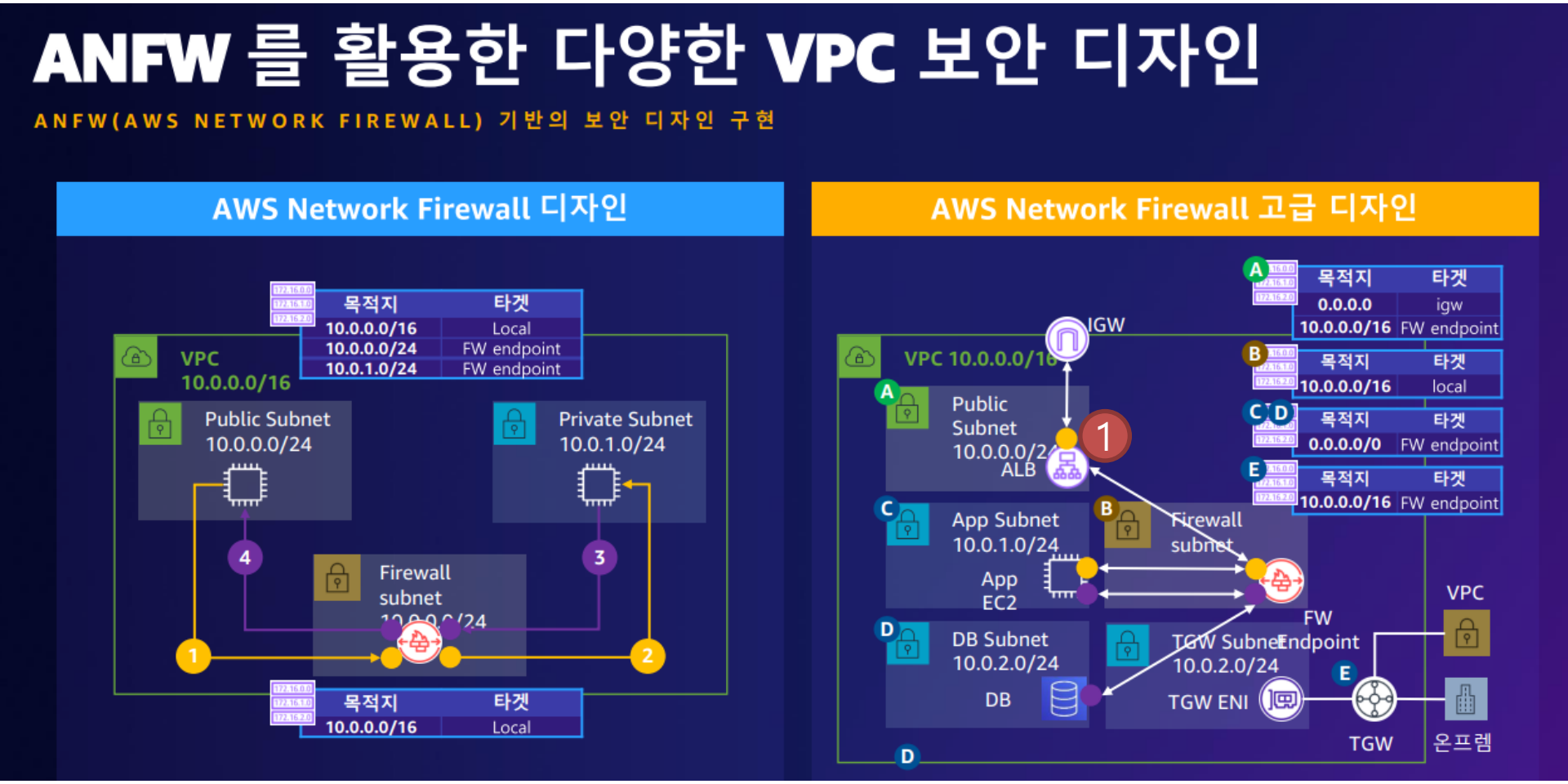
상세 기술

- NLB의 고정 IP를 기반으로 ALB 와 연계
- ALB가 NLB의 타겟그룹으로 동작
- VPC PrivateLink 구성 지원



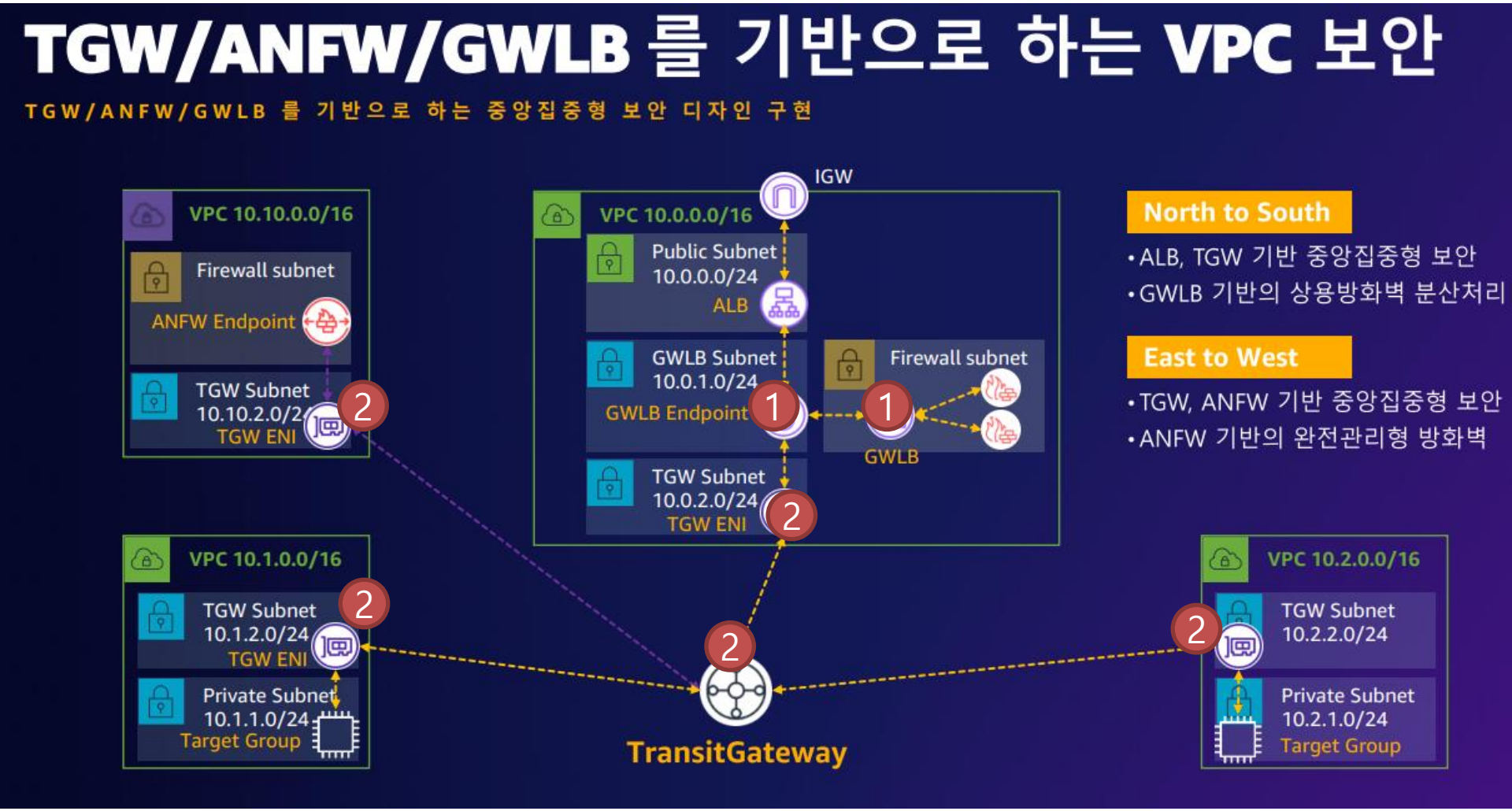
1. ALB의 동적 IP 주소 할당으로 인한 관리 어려움 호소
2. NLB 고정IP를 기반으로 ALB를 연계
3. ALB가 NLB를 추가함으로 고정 IP로 로드밸런서 사용 가능해짐

14. ANFW 아키 – AWS Network Firewall 고급 디자인



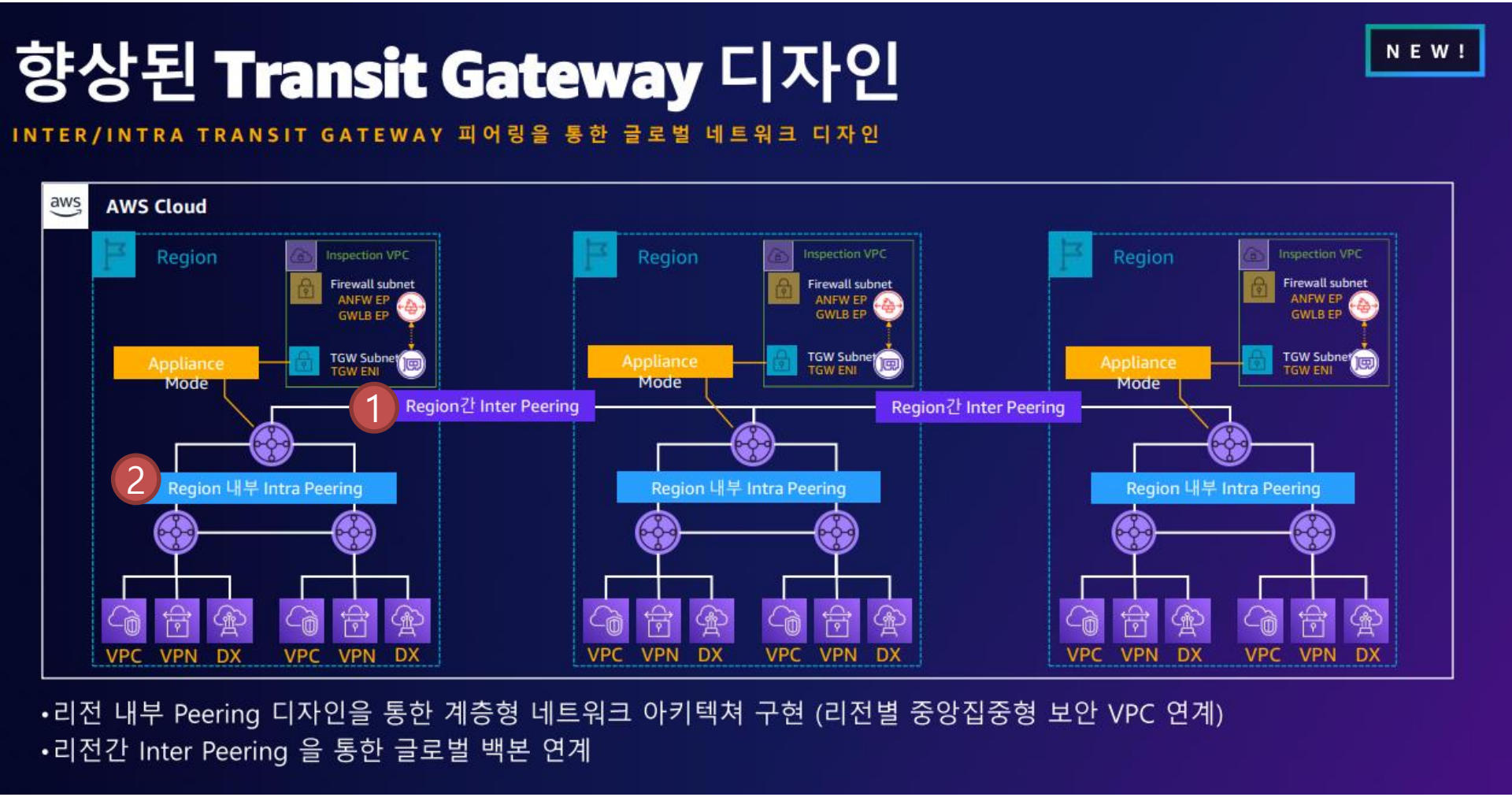
1. VPC , pub , pri , db , firewal subnet 생성
2. 모든 서브넷은 firewal Subnet을 거친다
3. 각 서브넷의 라우팅 테이블 작성
4. Firewall이 VPC내에 존재하는 경우 아키

15. TGW / ANFW / GWLB 아키 - 여러 VPC를 사용하는 경우



1. TGW는 TGW 서브넷을 만든다.
2. Firewall은 Firewall 서브넷과 GWLB 서브넷이 필요하다.
3. VPC , pub, gwlb subnet , firewal , TGW Subnet

16. TGW - VPC 외부와 리전간 통신, 변경전 : 리전 내 TGW연동 불가 , 변경후 : 리전 내 TGW피어링 가능



1. 리전간 인터넷 피어링 가능
2. 리전내 TGW Peering이 가능해짐. 기존엔 리전내 피어링이 안되었음.

17. DirectConnect MACSec 기반 전용선 암호화 - AWS와 온프렘간 전용선 연결시, 암호화 가능

DirectConnect MACSec 기반 전용선 암호화

NEW!

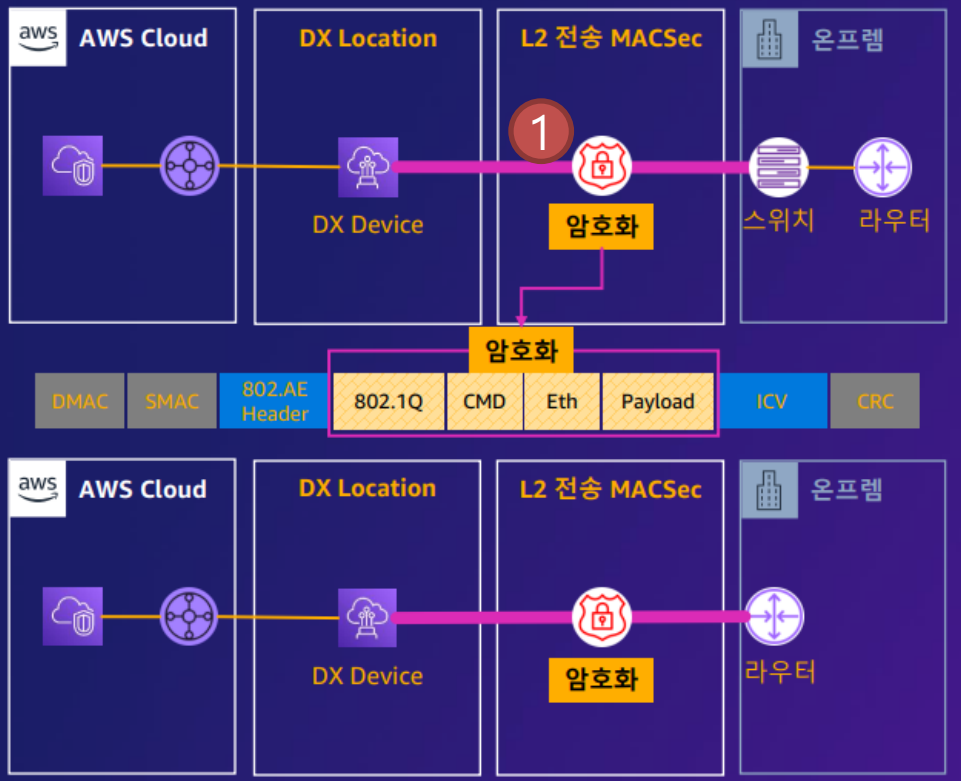
하이테크, 금융, 공공 등 산업군을 위한 전용선 암호화

기술 배경

- DX MACSec 기반 암호화
- 특정 산업군에서 DX 전용선 암호화 기반 보안 요구

상세 기술

- DX 네트워크 – 온프렘 스위치, 라우터간 암호화
- L2 전송 계층 기반의 암호화를 통한 하이테크, 금융, 공공 산업군의 데이터 전송 암호화
- 기업 고객들의 보안성 강화



- AWS Cloud -----DX location --------L2 전송 MACSec 암호화-------- 온프렘

18. DX SiteLink - 가까운 DX POP에 연결하여 AWS 글로벌 백본 연결 가능

DX SiteLink 기반의 AWS 글로벌 백본 디자인

NEW!

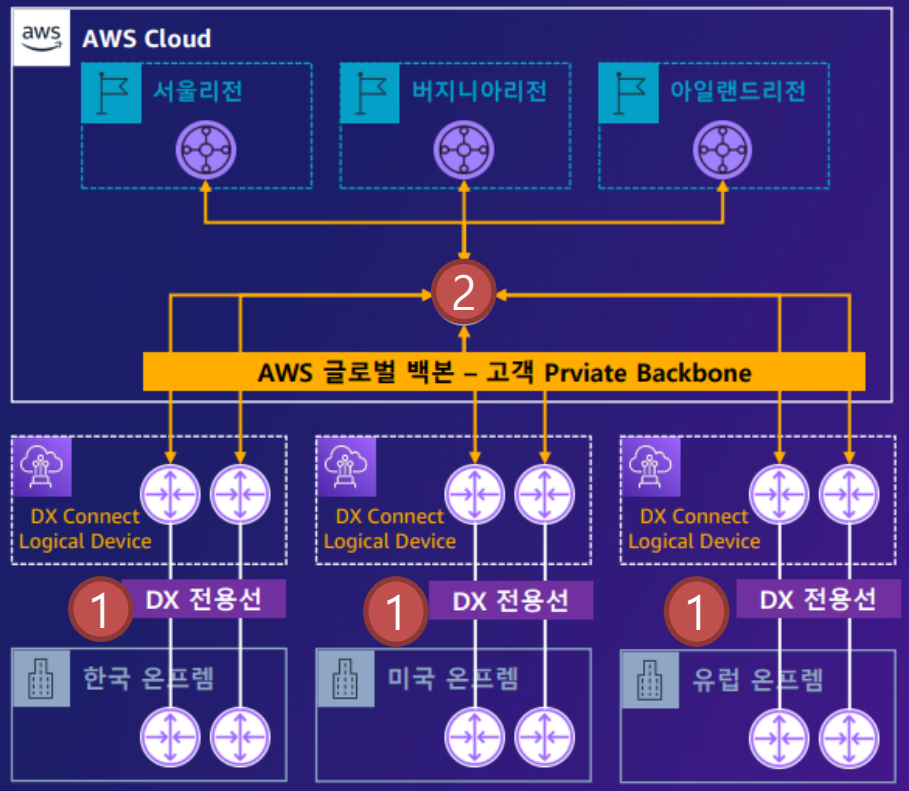
DIRECT CONNECT SITELINK 기반의 글로벌 백본을 통한 온프렘 네트워크 처리

기술 배경

- DX SiteLink 기반 TransitRouting
- 글로벌 비지니스 고객을 위한 해외 거점 네트워크의 AWS DXGW Trasit Routing 요구

상세 기술

- DX 전용선 사용 고객들이 , 각 거점 오피스 간 해외 전용선을 사용하지 않고 AWS 백본을 통한 연결
- 해외 전용선 비용 대폭 절감.



- AWS Cloud -----DX Connect ---------- 온프렘

19. AWS CloudWAN으로 글로벌 백본 연결

CloudWAN 기반의 완전관리형 WAN 서비스

NEW!

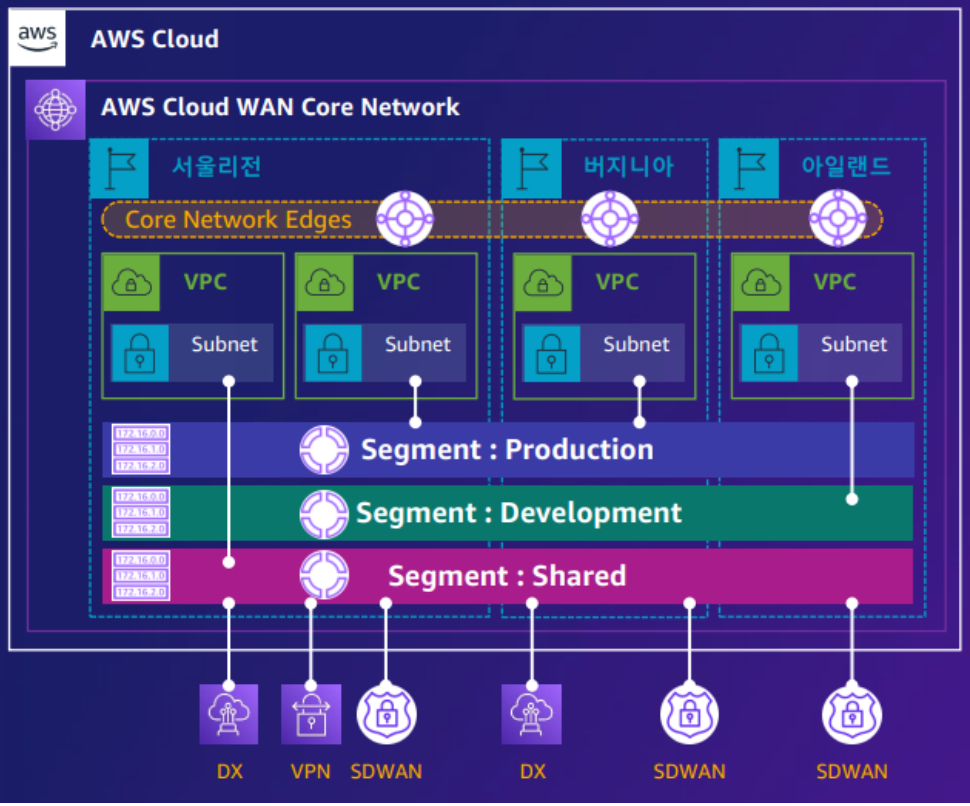
CLOUDWAN 기반의 글로벌 백본 세그먼트 디자인

기술 배경

- AWS CloudWAN 을 통한 글로벌 백본 연결
- 다양한 AWS 네트워크 연결 방법의 관리의 편의성 요구와 보안 강화 요구

상세 기술

- CloudWAN 기반의 네트워크 연결 통합
- Segment 기능을 통한 WAN 가상화 및 보안 적용
- CloudWAN 기반의 동적 라우팅 지원으로
- 관리의 편의성 향상



- ✓ **CloudWAN으로 글로벌 백본 연결 가능**
- ✓ **Shared와 연결**

20. Network Manager(CloudWAN지원) , VPC IP Address Manager , VPC Network Access Analyzer

새로운 네트워크 관리/분석 도구

Network Manager

- 통합 네트워크 모니터링
- 글로벌 네트워크 가시성
- SD WAN 통합

네트워크 구성 관리

VPC IP Address Manager

- VPC IP 주소 통합 관리
- IP 주소구성,모니터링, 감사
- 관리적 부담 및 오류 제거

IP 주소 관리

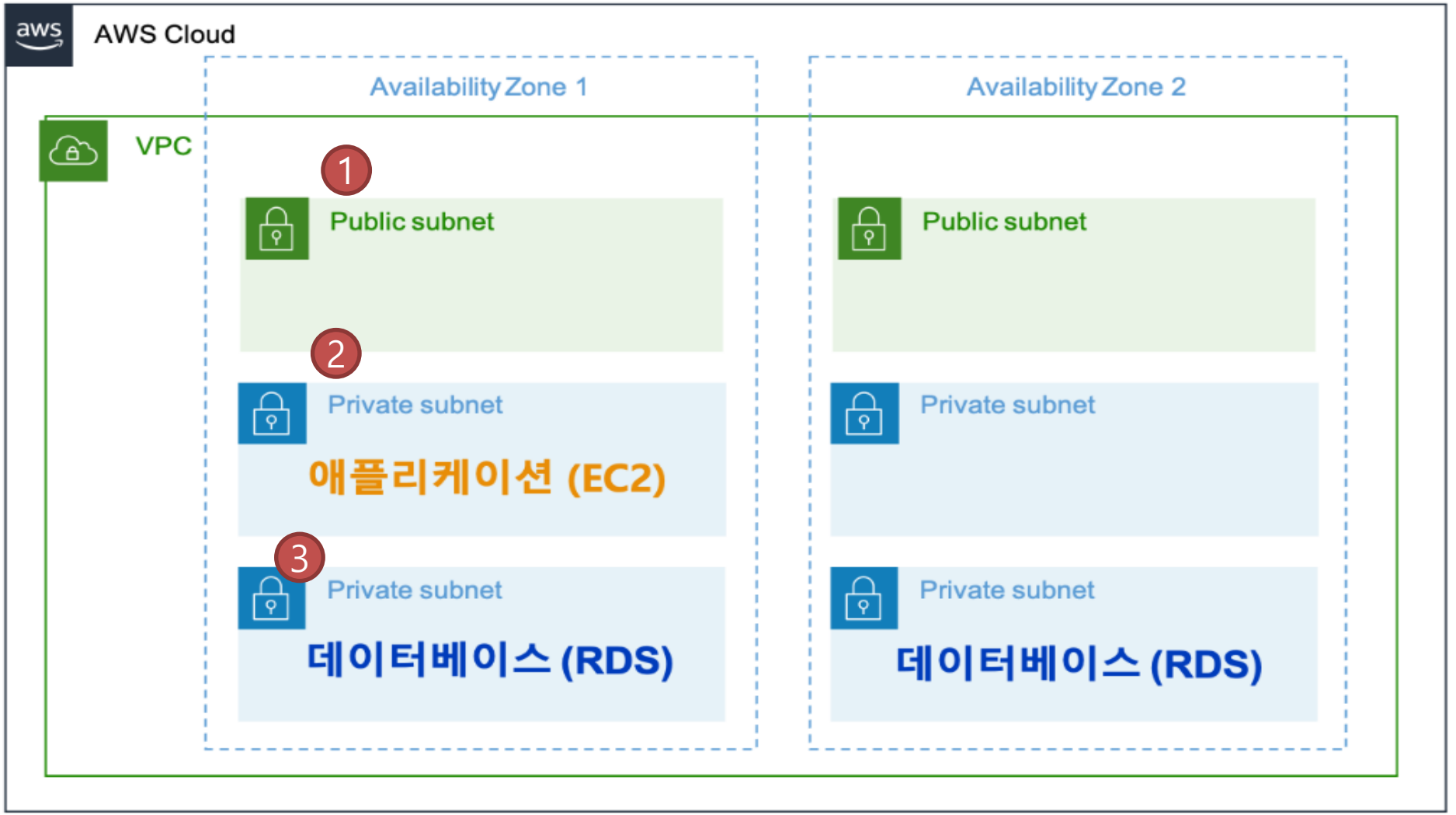
VPC
Network Access Analyzer

- 중요자원에 대한 네트워크 액세스 파악
- 보안 요구 위반 네트워크 액세스 식별
- 규정 준수 확인 자동화

VPC 네트워크 접근 분석기

- ✓ **Network Manager – Up/Down 확인가능**
- ✓ **IPAM**
- ✓ **VPC > 네트워크 분석 > 네트워크 액세스 분석기 > 분석 - 분석 결과**

21. 실무에서 VPC


AWS Cloud
Availability Zone 1
Availability Zone 2
VPC
1
Public subnet
Public subnet
2
Private subnet
애플리케이션 (EC2)
Private subnet
3
Private subnet
데이터베이스 (RDS)
Private subnet
데이터베이스 (RDS)

질문 ?

topasvga@naver.com

감사합니다.