

AWS 백서

# 확장 가능하고 안전한 다중 VPC AWS 네트워크 인프라 구축



# 확장 가능하고 안전한 다중 VPC AWS 네트워크 인프라 구축: AWS 백서

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon의 상표 및 브랜드 디자인은 Amazon 외 제품 또는 서비스와 함께, 브랜드 이미지를 떨어뜨리거나 고객에게 혼동을 일으킬 수 있는 방식으로 사용할 수 없습니다. Amazon이 소유하지 않은 기타 모든 상표는 Amazon 계열사, 관련 업체 또는 Amazon의 지원 업체 여부에 상관없이 해당 소유자의 자산입니다.

# Table of Contents

요약 및 소개 .....	1
소개 .....	1
IP 주소 계획 및 관리 .....	3
귀사는 Well-Architected입니까? .....	4
VPC에서 VPC로의 연결 .....	5
VPC 피어링 .....	5
AWS Transit Gateway .....	6
트랜짓 VPC 솔루션 .....	8
VPC 피어링과 트랜짓 VPC와 트랜짓 게이트웨이 비교 .....	9
AWS PrivateLink .....	11
VPC 공유 .....	13
프라이빗 NAT 게이트웨이 .....	14
AWS 클라우드 WAN .....	16
Amazon VPC Lattice .....	18
하이브리드 연결 .....	20
VPN .....	20
AWS Direct Connect .....	23
다이렉트 커넥트 연결의 MACsec 보안 .....	26
AWS Direct Connect 레질리언스 권장 사항 .....	27
AWS Direct Connect SiteLink .....	27
중앙 집중식 인터넷 송신 .....	30
중앙 집중식 IPv4 송신을 위한 NAT 게이트웨이 사용 .....	30
높은 가용성 .....	32
보안 .....	33
확장성 .....	33
중앙 집중식 IPv4 송신을 위한 NAT 게이트웨이 사용 AWS Network Firewall .....	33
확장성 .....	35
주요 고려 사항 .....	35
중앙 집중식 IPv4 송신을 위해 Amazon EC2 인스턴스와 함께 NAT 게이트웨이 및 게이트웨이 로 드 밸런서 사용 .....	36
높은 가용성 .....	37
장점 .....	38
주요 고려 사항 .....	38
IPv6용 중앙 집중식 이그레스 .....	38

VPC-VPC 간 및 온프레미스-VPC 트래픽에 대한 중앙 집중식 네트워크 보안 .....	43
중앙 집중식 네트워크 보안 검사 모델 사용 고려 사항 .....	43
중앙 집중식 네트워크 보안을 위해 게이트웨이 로드 밸런서와 Transit Gateway를 함께 사용 .....	45
AWS Network Firewall 및 AWS 게이트웨이 로드 밸런서에 대한 주요 고려 사항 .....	46
중앙 집중식 인바운드 검사 .....	48
AWS WAF 그리고 인터넷을 AWS Firewall Manager 통한 인바운드 트래픽을 검사하는 데 사용 됩니다. ....	48
장점 .....	49
주요 고려 사항 .....	50
타사 어플라이언스를 사용한 중앙 집중식 인바운드 검사 .....	50
장점 .....	51
주요 고려 사항 .....	51
Gateway Load Balancer와 함께 방화벽 어플라이언스를 사용하여 인터넷에서 들어오는 인바운 드 트래픽을 검사합니다. ....	52
중앙 집중식 AWS Network Firewall 인그레스에 사용 .....	53
DPI (딥 패킷 검사) 를 통한 AWS Network Firewall .....	54
중앙 집중식 AWS Network Firewall 인그레스 아키텍처의 주요 고려 사항 .....	54
DNS .....	56
하이브리드 DNS .....	56
Route 53 DNS 방화벽 .....	58
VPC 프라이빗 엔드포인트에 대한 중앙 집중식 액세스 .....	60
인터페이스 VPC 엔드포인트 .....	60
지역 간 엔드포인트 액세스 .....	62
AWS Verified Access .....	64
결론 .....	66
기여자 .....	67
사용 설명서 기록 .....	68
고지 사항 .....	70
.....	lxxi

# 확장 가능하고 안전한 다중 VPC AWS 네트워크 인프라 구축

발행일: 2024년 4월 17일 () [사용 설명서 기록](#)

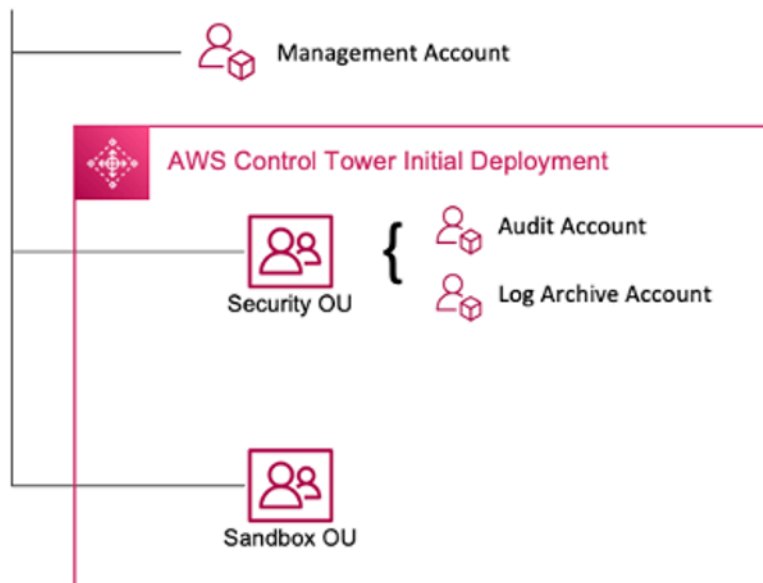
Amazon Web Services (AWS) 고객은 워크로드를 분할하고 설치 공간을 확장하기 위해 수백 개의 계정과 가상 사설 클라우드 (VPC) 를 사용하는 경우가 많습니다. 이러한 수준의 확장으로 인해 리소스 공유, VPC 간 연결, 온프레미스 시설과 VPC 연결과 관련하여 문제가 발생하는 경우가 많습니다.

이 백서에서는 [Amazon Virtual Private Cloud \(Amazon VPC\)](#),,,, [게이트웨이 AWS Direct Connect](#)로드 [밸런서 AWS Transit Gateway](#)[AWS PrivateLink](#), [Amazon Route 53](#)와 같은 AWS 서비스를 사용하여 대규모 네트워크에서 확장 가능하고 안전한 네트워크 아키텍처를 만드는 모범 사례를 설명합니다. [AWS Network Firewall](#) 이 백서는 오버헤드 비용을 낮게 유지하면서 확장성,고가용성 및 보안을 보장하는 등 성장하는 인프라를 관리하기 위한 솔루션을 보여줍니다.

## 소개

AWS 고객은 먼저 권한, 비용, 서비스를 구분하는 관리 경계를 나타내는 단일 AWS 계정에 리소스를 구축하는 것부터 시작합니다. 그러나 고객 조직이 성장함에 따라 비용을 모니터링하고 액세스를 제어하며 보다 쉽게 환경을 관리할 수 있도록 서비스를 더 세분화해야 합니다. 다중 계정 솔루션은 조직 내 IT 서비스 및 사용자를 위한 특정 계정을 제공하여 이러한 문제를 해결합니다. AWS 다음을 포함하여 [AWS Control Tower](#)이 인프라를 관리하고 구성하는 데 사용할 수 있는 여러 도구를 제공합니다.

### Root



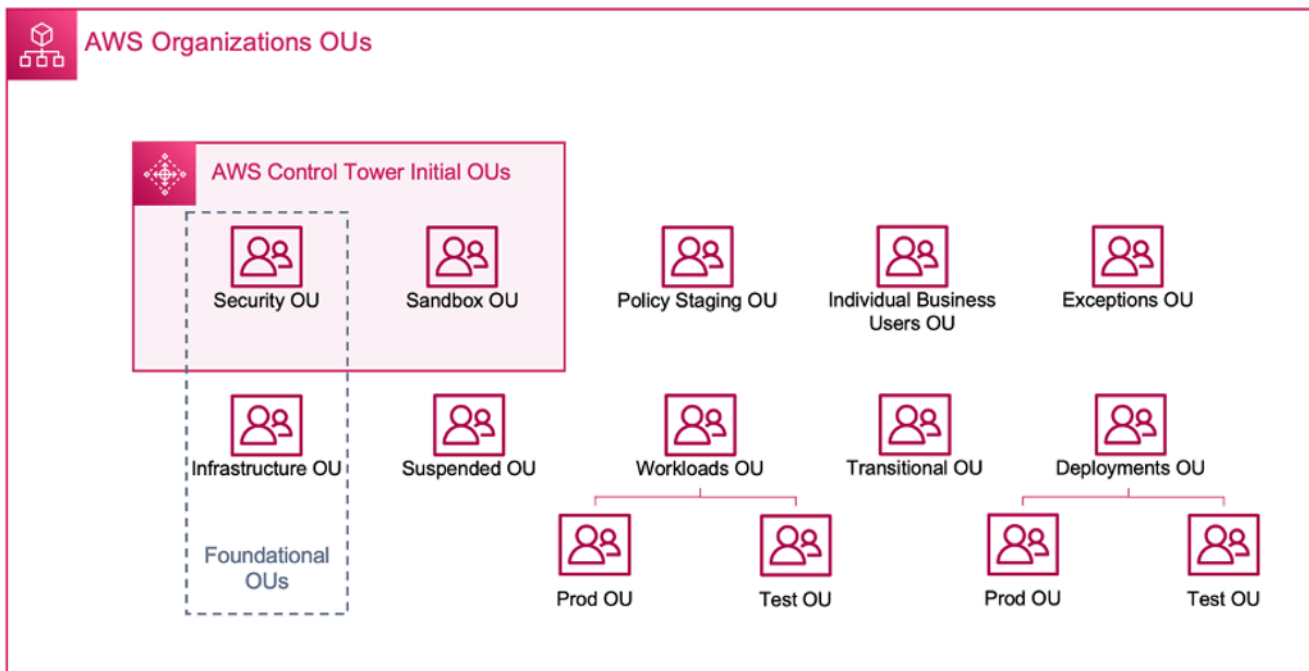
## AWS Control Tower 초기 배포

를 사용하여 다중 계정 환경을 설정하면 다음과 AWS Control Tower같은 두 개의 OU (조직 구성 단위)가 생성됩니다.

- 보안 OU - 이 OU 내에서 두 개의 계정을 AWS Control Tower 생성합니다.
- 로그 아카이브
- 감사 (이 계정은 지침에서 앞서 설명한 보안 도구 계정에 해당합니다.)
- 샌드박스 OU — 이 OU는 내에서 생성된 계정의 기본 대상입니다. AWS Control Tower 여기에는 팀의 허용 가능한 사용 정책에 따라 빌더가 AWS 서비스, 기타 도구 및 서비스를 탐색하고 실험할 수 있는 계정이 포함됩니다.

AWS Control Tower 추가 OU를 만들고, 등록하고, 관리하여 초기 환경을 확장하여 지침을 구현할 수 있습니다.

다음 다이어그램은 에서 처음 배포한 OU를 보여줍니다 AWS Control Tower. 다이어그램에 포함된 모든 권장 OU를 요구 사항에 맞게 구현하도록 AWS 환경을 확장할 수 있습니다.



## AWS 조직 OU

다중 계정 환경 사용에 대한 자세한 내용은 다중 계정을 사용한 AWS Control Tower 환경 구성 백서의 [부록 E](#)를 참조하십시오. AWS

**Note**

이 백서에서 “Control Tower”는 워크로드를 배포하는 확장 가능하고 안전하며 성능이 뛰어난 다중 계정/다중 VPC 설정을 포괄하는 용어입니다. 이 설정은 다양한 도구를 사용하여 구축할 수 있습니다. 다중 계정을 [사용하여 AWS 환경 구성](#) 백서에서 [다중 계정 클라우드 기반의 모범 사례, 설계 원칙 및 이점에 대한 자세한 내용을 확인할 수 있습니다.](#)

대부분의 고객은 먼저 VPC 몇 대를 가지고 인프라를 배포합니다. 고객이 생성하는 VPC의 수는 일반적으로 계정, 사용자, 단계적 환경 (프로덕션, 개발, 테스트 등) 의 수와 관련이 있습니다. 클라우드 사용량이 증가하면 고객이 상호 작용하는 사용자, 사업부, 애플리케이션 및 지역의 수도 증가하여 새로운 VPC가 생성됩니다.

VPC의 수가 증가함에 따라 VPC 간 관리는 고객의 클라우드 네트워크 운영에 필수적입니다. 이 백서는 VPC 간 및 하이브리드 연결의 세 가지 특정 영역에 대한 모범 사례를 다룹니다.

- 네트워크 연결 — VPC와 온프레미스 네트워크를 대규모로 상호 연결합니다.
- 네트워크 보안 — [네트워크 주소 변환 \(NAT\) 게이트웨이, VPC 엔드포인트, 게이트웨이 로드 밸런서 등 인터넷 및 엔드포인트에 액세스하기 위한 중앙 집중식 송신 지점을 구축합니다.](#) [AWS PrivateLink](#) [AWS Network Firewall](#)
- DNS 관리 — Control Tower 및 하이브리드 DNS 내에서 DNS를 해결합니다.

## IP 주소 계획 및 관리

확장 가능한 다중 계정 다중 VPC 네트워크 설계를 구축하려면 IP 주소 계획 및 관리가 필수적입니다. 올바른 IP 주소 지정 체계는 현재와 미래의 네트워킹 요구 사항을 고려해야 합니다. IP 주소 체계 IP는 온프레미스 워크로드와 클라우드 워크로드를 포괄해야 하며 향후 확장 (예: 신규 AWS 리전, 사업부 추가, 인수 합병) 도 가능해야 합니다. 또한 팀이 실수로 중복되는 IP CIDR을 생성하는 일도 방지할 수 있습니다. 분리되거나 연결이 끊긴 워크로드와 같이 중복되는 IP CIDR이 필요한 경우 이 결정은 신중하게 내려야 하며 라우팅, 보안 및 비용에 미치는 영향을 고려해야 합니다. 또한 이러한 예외에 필요한 승인 프로세스를 마련하는 것도 고려해야 할 수 있습니다. 올바른 IP 주소 지정 체계는 네트워크 설계 및 라우팅 구성을 단순화하는 데도 도움이 됩니다.

주요 고려 사항:

- IP 주소 지정 체계 (공용 및 사설 IP 모두) 를 미리 계획하고 IP 주소 관리 도구를 선택하여 모든 워크로드에서 IP 주소 사용을 할당, 관리 및 추적하십시오.

- 계층적이고 요약된 IP 주소 지정 체계를 사용하십시오.
- 환경 AWS 리전, 조직 또는 사업부에 따라 일관된 IP 할당을 계획하세요.
- 온프레미스 및 클라우드 네트워크를 위한 별도의 IP CIDR (IPv4 및 IPv6 모두) 을 지정하십시오.
- 중복되는 IP CIDR을 사전에 방지하고 추적합니다.
- 확장 및 향후 성장에 맞게 IP CIDR 크기를 적절하게 조정하십시오.
- 워크로드에 IPv6 또는 이중 스택 호환성을 지원하여 IP 충돌을 줄이고 IPv4 공간 고갈을 해결하십시오.

Amazon VPC IP 주소 관리자 (IPAM) 를 사용하여 워크로드에 대한 퍼블릭 및 프라이빗 IP 주소 모두의 계획, 추적 및 모니터링을 간소화할 수 있습니다. AWS IPAM을 사용하면 여러 채널에서 IP 주소 공간을 구성, 할당, 모니터링 및 공유할 수 있습니다. AWS 리전 AWS 계정또한 특정 비즈니스 규칙을 사용하여 VPC에 CIDR을 자동으로 할당하는 데도 도움이 됩니다.

[IP 주소 지정 모범 사례와 IPAM을 사용하여 VPC에서 IP 풀을 관리하는 방법을 알아보려면 Amazon VPC IP 주소 관리자 모범 사례, Amazon VPC IP 주소 관리자를 사용한 VPC 및 지역 간 IP 풀 관리 및 AWS Control Tower](#)블로그 게시물의 IP 주소 관리를 참조하십시오. AWS 리전 AWS Control Tower

## 귀사는 Well-Architected입니까?

[AWS Well-Architected 프레임워크](#)는 클라우드에서 시스템을 구축할 때 내리는 결정의 장단점을 이해하는 데 도움이 됩니다. 이 프레임워크를 사용하여 클라우드에서 안정적이고 안전하며 효율적이고 비용 효율적인 시스템을 설계하고 운영하기 위한 아키텍처 모범 사례를 살펴볼 수 있습니다. [AWS Management Console](#)에서 무료로 제공되는 [AWS Well-Architected Tool](#)를 사용하면 각 요소에 대한 일련의 질문에 답하여, 이러한 모범 사례와 비교하여 워크로드를 검토할 수 있습니다.

참조 아키텍처 배포, 다이어그램, 백서 등 클라우드 아키텍처에 대한 더 많은 전문가 지침과 모범 사례를 보려면 [AWS 아키텍처 센터](#)를 참조하세요.



## VPC에서 VPC로의 연결

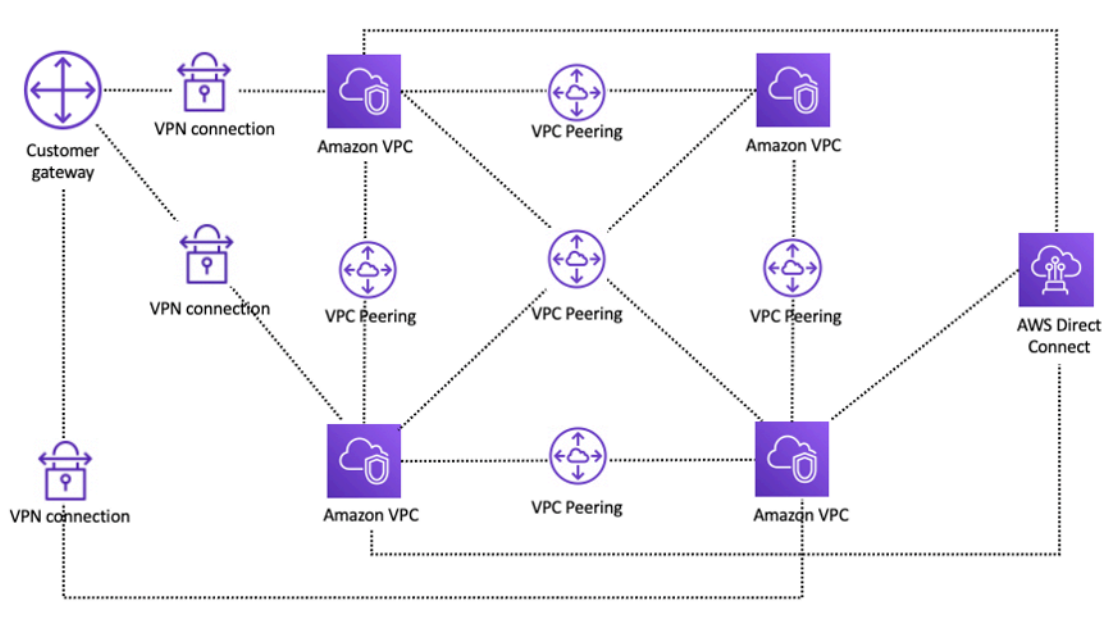
고객은 두 가지 VPC 연결 패턴, 즉 다대다 또는 허브 앤 스포크를 사용하여 다중 VPC 환경을 설정할 수 있습니다. many-to-many 접근 방식에서는 각 VPC 간의 트래픽이 각 VPC 간에 개별적으로 관리됩니다. 이 hub-and-spoke 모델에서는 모든 VPC 간 트래픽이 중앙 리소스를 통해 흐르고, 중앙 리소스는 설정된 규칙에 따라 트래픽을 라우팅합니다.

## VPC 피어링

두 VPC를 연결하는 첫 번째 방법은 VPC 피어링을 사용하는 것입니다. 이 설정에서는 연결을 통해 VPC 간의 완전한 양방향 연결이 가능합니다. 이 피어링 연결은 VPC 간에 트래픽을 라우팅하는 데 사용됩니다. 서로 다른 계정 및 AWS 리전에 있는 VPC도 함께 피어링할 수 있습니다. 가용 영역 내에 있는 VPC 피어링 연결을 통한 모든 데이터 전송은 무료입니다. 가용 영역을 통과하는 VPC 피어링 연결을 통한 모든 데이터 전송에는 표준 리전 내 데이터 전송 요금이 부과됩니다. VPC가 여러 지역에서 피어링되는 경우 표준 지역 간 데이터 전송 요금이 적용됩니다.

VPC 피어링은 point-to-point 연결성이며 전이적 라우팅을 지원하지 않습니다. 예를 들어 VPC A와 VPC B 사이, VPC A와 VPC C 간에 VPC 피어링 연결이 있는 경우 VPC B의 인스턴스는 VPC A를 통해 VPC C에 도달하기 위해 전송할 수 없습니다. VPC B와 VPC C 간에 패킷을 라우팅하려면 직접 VPC 피어링 연결을 만들어야 합니다.

규모에 따라 VPC가 수십 개 또는 수백 개일 때 피어링으로 상호 연결하면 수백 또는 수천 개의 피어링 연결 메시가 생성될 수 있습니다. 연결 수가 많으면 관리 및 확장이 어려울 수 있습니다. 예를 들어, 100 개의 VPC가 있고 둘 사이에 풀 메시 피어링을 설정하려는 경우 4,950개의 피어링 연결  $[n(n-1)/2]$  이 필요합니다. 여기서  $n$  는 총 VPC 수입니다. VPC당 활성 피어링 연결은 최대 125개로 제한됩니다.



## VPC 피어링을 사용한 네트워크 설정

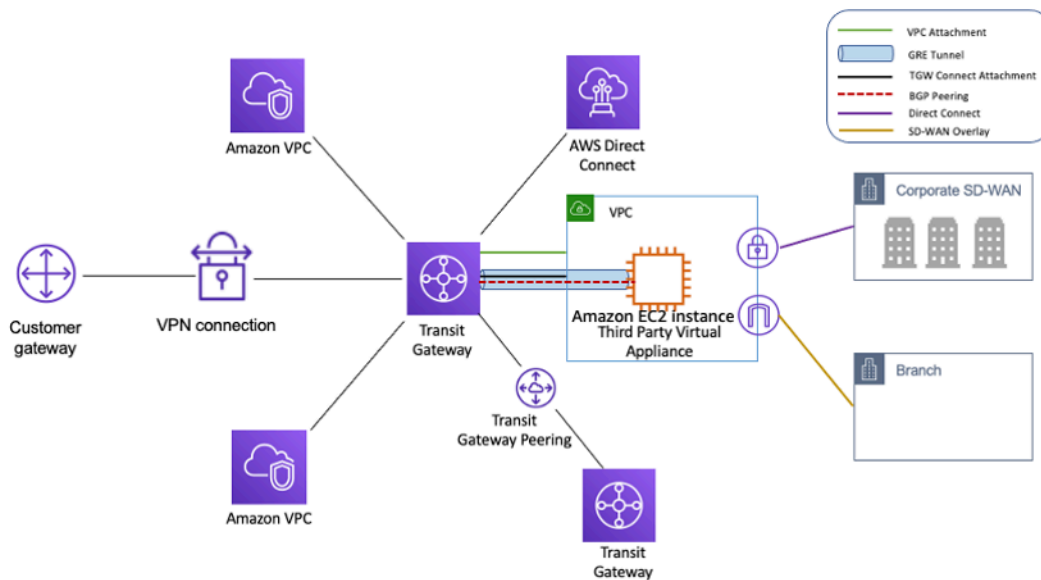
VPC 피어링을 사용하는 경우 각 VPC에 온프레미스 연결 (VPN 및/또는 Direct Connect) 을 설정해야 합니다. 위 그림에 표시된 것처럼 피어링된 VPC의 하이브리드 연결을 사용하여 VPC의 리소스는 온프레미스에 도달할 수 없습니다.

VPC 피어링은 한 VPC의 리소스가 다른 VPC의 리소스와 통신해야 하고, 두 VPC의 환경이 제어 및 보호되며, 연결할 VPC의 수가 10개 미만일 때 가장 잘 사용됩니다 (각 연결을 개별적으로 관리할 수 있음). VPC 피어링은 다른 VPC 간 연결 옵션과 비교할 때 전체 비용이 가장 낮고 총 성능이 가장 높습니다.

## AWS Transit Gateway

[AWS Transit Gateway](#) 타사 가상 어플라이언스를 프로비저닝할 필요 없이 VPC와 온프레미스 네트워크를 완전 관리형 서비스로 연결할 수 있는 허브 및 스포크 디자인을 제공합니다. VPN 오버레이가 필요하지 않으며 고가용성과 확장성을 AWS 관리합니다.

Transit Gateway를 사용하면 고객이 수천 개의 VPC를 연결할 수 있습니다. 모든 하이브리드 연결 (VPN 및 Direct Connect 연결) 을 단일 게이트웨이에 연결하여 조직의 전체 AWS 라우팅 구성을 한 곳에서 통합 및 제어할 수 있습니다 (다음 그림 참조). Transit Gateway는 라우팅 테이블을 사용하여 연결된 모든 스포크 네트워크 간에 트래픽이 라우팅되는 방식을 제어합니다. 이 hub-and-spoke 모델은 VPC가 Transit Gateway 인스턴스에만 연결하여 연결된 네트워크에 액세스하므로 관리를 단순화하고 운영 비용을 절감합니다.



## 허브 및 스포크 디자인 AWS Transit Gateway

Transit Gateway는 지역 리소스이며 같은 AWS 리전지역 내에서 수천 개의 VPC를 연결할 수 있습니다. 하이브리드 연결을 위해 단일 Direct Connect 연결을 통해 여러 게이트웨이를 연결할 수 있습니다. 일반적으로 하나의 Transit Gateway 인스턴스만 사용하여 특정 지역의 모든 VPC 인스턴스를 연결하고 Transit Gateway 라우팅 테이블을 사용하여 필요할 때마다 이들을 격리할 수 있습니다. 단, 트랜짓 게이트웨이는 설계상 가용성이 높도록 설계되었으므로 고가용성을 위해 추가 트랜짓 게이트웨이가 필요하지 않습니다. 중복성을 위해 각 리전에서 단일 게이트웨이를 사용하십시오. 하지만 잘못된 컨피그레이션 폭발 환경을 제한하고 컨트롤 플레인 운영 및 관리를 분리하기 위해 게이트웨이를 여러 개 만드는 것이 좋습니다. ease-of-use

Transit Gateway 피어링으로 고객은 Transit Gateway 인스턴스를 동일 또는 여러 지역 내에서 피어링하여 두 지역 간에 트래픽을 라우팅할 수 있습니다. VPC 피어링과 동일한 기본 인프라를 사용하므로 암호화됩니다. 자세한 내용은 [AWS Transit Gateway 지역 간 피어링을 사용하여 글로벌 네트워크 구축을 참조하십시오. 이제 AWS Transit Gateway는 지역 내 피어링을 지원합니다.](#)

조직의 Transit Gateway 인스턴스를 네트워크 서비스 계정에 배치합니다. 이를 통해 네트워크 서비스 계정을 관리하는 네트워크 엔지니어가 중앙 집중식으로 관리할 수 있습니다. AWS Resource Access Manager (RAM) 를 사용하여 Transit Gateway 인스턴스를 공유하여 동일한 지역 내 AWS 조직의 여러 계정에 있는 VPC를 연결할 수 있습니다. AWS RAM AWS 리소스를 모든 AWS 계정 AWS 조직 또는 AWS 조직 내에서 쉽고 안전하게 공유할 수 있습니다. 자세한 내용은 [중앙 계정 블로그 게시물의 전송 게이트웨이에 대한 AWS Transit Gateway 첨부 자동화를 참조하십시오.](#)

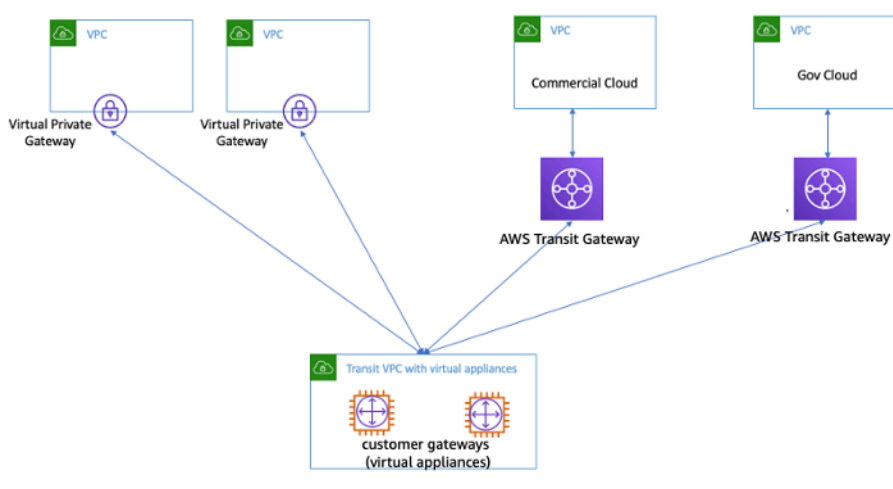
또한 Transit Gateway를 사용하면 SD-WAN 인프라와 Transit Gateway AWS Connect를 사용하여 연결을 설정할 수 있습니다. 동적 라우팅에는 경계 게이트웨이 프로토콜 (BGP) 과 함께 Transit Gateway

Connect 연결을 사용하고 고성능을 위해서는 일반 라우팅 캡슐화 (GRE) 터널 프로토콜과 함께 사용하여 Connect 연결당 최대 20Gbps의 총 대역폭을 제공합니다 (Connect 연결당 최대 4개의 Transit Gateway Connect 피어). Transit Gateway Connect를 사용하면 VPC 연결 또는 연결을 기본 전송 계층으로 사용하여 클라우드에서 실행되는 온프레미스 SD-WAN 인프라 또는 SD-WAN 어플라이언스를 통합할 수 있습니다. AWS Direct Connect 참조 아키텍처 및 자세한 구성은 [AWS Transit Gateway Connect를 통한 SD-WAN 연결 단순화](#)를 참조하십시오.

## 트랜짓 VPC 솔루션

[트랜짓 VPC](#)는 VPC 간 연결을 위한 허브 및 스포크 설계를 도입하여 VPC 피어링과는 다른 방법으로 VPC 간 연결을 만들 수 있습니다. [전송 VPC 네트워크에서는 하나의 중앙 VPC \(허브 VPC\)가 일반적으로 IPsec을 통한 BGP를 활용하는 VPN 연결을 통해 다른 모든 VPC \(스포크 VPC\)와 연결됩니다.](#) 중앙 VPC에는 VPN 오버레이를 사용하여 들어오는 트래픽을 목적지로 라우팅하는 소프트웨어 어플라이언스를 실행하는 Amazon [Elastic Compute Cloud](#) (Amazon EC2) 인스턴스가 포함되어 있습니다. 트랜짓 VPC 피어링에는 다음과 같은 이점이 있습니다.

- 오버레이 VPN 네트워크를 사용하면 트랜지티브 라우팅이 가능하므로 허브 및 스포크 설계가 가능합니다.
- 허브 트랜짓 VPC의 EC2 인스턴스에서 타사 공급업체 소프트웨어를 사용하는 경우 고급 보안 (계층 7 방화벽/침입 방지 시스템 (IPS) /침입 탐지 시스템 (IDS)) 과 관련된 공급업체 기능을 사용할 수 있습니다. 고객이 온프레미스에서 동일한 소프트웨어를 사용하는 경우 통합 운영/모니터링 환경을 활용할 수 있습니다.
- Transit VPC 아키텍처는 일부 사용 사례에서 필요할 수 있는 연결성을 지원합니다. 예를 들어, AWS GovCloud 인스턴스와 상업 지역 VPC 또는 Transit Gateway 인스턴스를 Transit VPC에 연결하고 두 지역 간의 VPC 간 연결을 활성화할 수 있습니다. 이 옵션을 고려할 때는 보안 및 규정 준수 요구 사항을 평가하십시오. 보안을 강화하기 위해 이 백서 뒷부분에서 설명하는 설계 패턴을 사용하여 중앙 집중식 검사 모델을 배포할 수 있습니다.



### 가상 어플라이언스가 포함된 전송 VPC

Transit VPC에는 인스턴스 크기/패밀리에 따라 EC2에서 타사 공급업체 가상 어플라이언스를 실행하는 데 드는 비용 증가, VPN 연결당 처리량 제한 (VPN 터널당 최대 1.25Gbps), 추가 구성, 관리 및 복원력 오버헤드 (타사 공급업체 가상 어플라이언스를 실행하는 EC2 인스턴스의 HA 및 이중화 관리는 고객 부담) 등 나름의 문제가 있습니다.

## VPC 피어링과 트랜짓 VPC와 트랜짓 게이트웨이 비교

표 1 — 연결성 비교

기준	VPC 피어링	트랜짓 VPC	전송 게이트웨이	PrivateLink	클라우드 WAN	VPC Lattice
범위	지역/글로벌	리전	리전	리전	전 세계	리전
아키텍처	풀 메시	VPN 기반 hub-and-spoke	첨부 파일 기반 hub-and-spoke	제공자 또는 소비자 모델	첨부 파일 기반, 다중 지역	앱 간 연결
Scale	VPC당 125개의 액티브 피어	가상 라우터/EC2에 따라 다름	지역당 5000개의 첨부 파일	제한 없음	코어 네트워킹당 5000개의 첨부 파일	서비스당 500개의 VPC 연결

기준	VPC 피어링	트랜짓 VPC	전송 게이트웨이	PrivateLink	클라우드 WAN	VPC Lattice
분할	보안 그룹	고객 관리	Transit Gateway 라우팅 테이블	세그멘테이션 없음	세그먼트	서비스 및 서비스 네트워크 정책
지연 시간	가장 낮음	VPN 암호화 오버헤드로 인한 추가	추가 Transit Gateway 홉	트래픽은 AWS 백본에 머무므로 고객은 테스트해야 합니다.	Transit Gateway와 동일한 데이터플레인 사용	트래픽은 AWS 백본에 머무므로 고객은 테스트해야 합니다.
대역폭 한도	인스턴스당 한도, 총 한도 없음	크기/패밀리에 따른 EC2 인스턴스 대역폭 제한이 적용됩니다.	최대 100Gbps (버스트) / 첨부 파일	가용 영역당 10Gbps, 최대 100Gbps까지 자동 확장	최대 100Gbps (버스트) / 첨부 파일	가용 영역당 10Gbps
표시 여부	VPC 흐름 로그	VPC 흐름 로그 및 지표 CloudWatch	Transit Gateway 네트워크 관리자, VPC 흐름 로그, 지표 CloudWatch	CloudWatch 메트릭	네트워크 관리자, VPC 흐름 로그, 지표 CloudWatch	CloudWatch 액세스 로그
보안 그룹 상호 참조	지원	지원되지 않음	지원되지 않음	지원되지 않음	지원되지 않음	해당 사항 없음

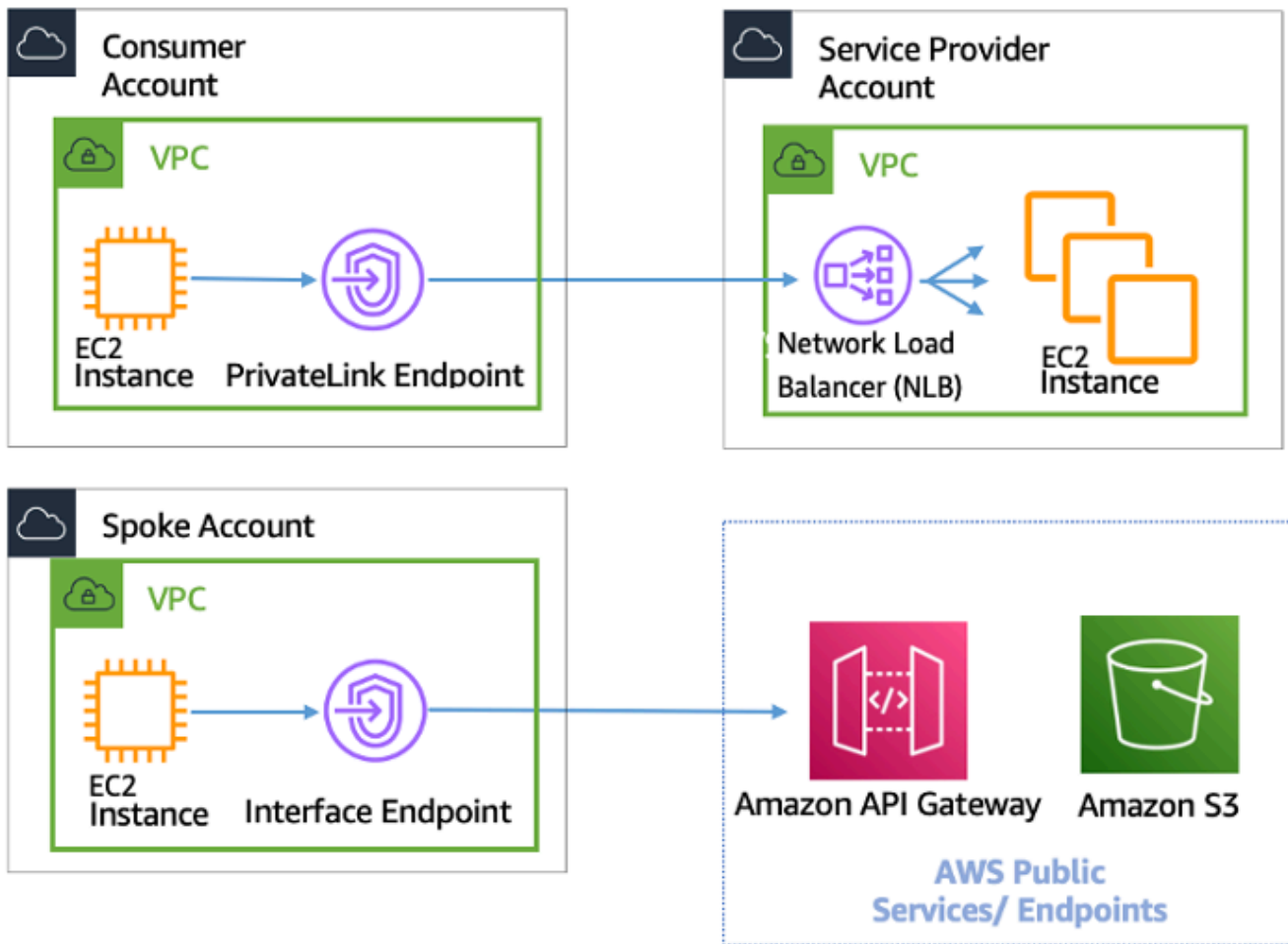
기준	VPC 피어링	트랜짓 VPC	전송 게이트웨이	PrivateLink	클라우드 WAN	VPC Lattice
IPv6 지원	지원	가상 어플라이언스에 따라 다름	지원	지원	지원	지원

## AWS PrivateLink

[AWS PrivateLink](#) 트래픽을 퍼블릭 인터넷에 노출시키지 않고 VPC, AWS 서비스 및 온프레미스 네트워크 간의 프라이빗 연결을 제공합니다. 로 AWS PrivateLink 구동되는 인터페이스 VPC 엔드포인트를 사용하면 다양한 계정 AWS 및 VPC의 다른 서비스에 쉽게 연결하여 네트워크 아키텍처를 크게 단순화할 수 있습니다. 이를 통해 고객은 소비자 VPC만 서비스 공급업체 VPC에 연결을 시작하는 방식으로 한 VPC (서비스 공급업체) 에 있는 서비스/애플리케이션을 다른 VPC (소비자) 에 비공개로 노출할 수 있습니다. AWS 리전 예를 들어 프라이빗 애플리케이션이 서비스 공급업체 API에 액세스할 수 있는 기능을 들 수 있습니다.

사용하려면 AWS PrivateLink VPC에서 애플리케이션을 위한 Network Load Balancer를 생성하고 해당 로드 밸런서를 가리키는 VPC 엔드포인트 서비스 구성을 생성하십시오. 그러면 서비스 소비자가 서비스에 인터페이스 엔드포인트를 생성합니다. 그러면 서비스로 향하는 트래픽의 진입점 역할을 하는 사실 IP 주소를 가진 ENI (Elastic Network Interface) 가 소비자 서브넷에 생성됩니다. 소비자와 서비스는 동일한 VPC에 있지 않아도 됩니다. VPC가 다르면 소비자 및 서비스 공급자 VPC의 IP 주소 범위가 겹칠 수 있습니다. 다른 VPC의 서비스에 액세스하기 위한 인터페이스 VPC 엔드포인트를 생성하는 것 외에도, 다음 그림과 같이 지원되는 [AWS 서비스에](#) 비공개로 액세스하는 인터페이스 VPC 엔드포인트를 생성할 수 있습니다. AWS PrivateLink

애플리케이션 로드 밸런서 (ALB) 를 NLB 대상으로 사용하면 이제 ALB 고급 라우팅 기능을 다음과 결합할 수 있습니다. AWS PrivateLink 참조 아키텍처 및 자세한 구성은 [Network Load Balancer용 애플리케이션 로드 밸런서 유형 대상 그룹을](#) 참조하십시오.



## AWS PrivateLink 다른 VPC 및 AWS 서비스와의 연결용

Transit Gateway와 VPC 피어링 중 하나를 선택하는 AWS PrivateLink 것은 연결에 따라 달라집니다.

- AWS PrivateLink— 하나 이상의 소비자 VPC가 서비스 공급자 VPC 또는 특정 서비스의 특정 서비스나 인스턴스 세트에 단방향으로 액세스할 수 있도록 클라이언트/서버를 설정한 AWS PrivateLink 경우에 사용됩니다. AWS 소비자 VPC에서 액세스 권한을 가진 클라이언트만 서비스 공급자 VPC 또는 서비스의 서비스에 대한 연결을 시작할 수 있습니다. AWS 이는 서비스 공급자와 IP 충돌이 발생하지 않도록 클라이언트 VPC 내에서 ENI를 AWS PrivateLink 사용하기 때문에 두 VPC의 클라이언트와 서버의 IP 주소가 겹치는 경우에도 좋은 옵션입니다. VPC 피어링, VPN, Transit Gateway, 클라우드 WAN 등을 통해 AWS PrivateLink 엔드포인트에 액세스할 수 있습니다. AWS Direct Connect
- VPC 피어링 및 Transit Gateway — VPC 간의 레이어 3 IP 연결을 활성화하려면 VPC 피어링 및 Transit Gateway를 사용합니다.



아키텍처에는 다양한 사용 사례를 충족하기 위해 이러한 기술이 혼합되어 포함됩니다. 이러한 모든 서비스를 결합하여 서로 운영할 수 있습니다. 예를 들어 API 스타일의 클라이언트-서버 연결 AWS PrivateLink 처리, 지역 또는 지역 간 연결 내에서 배치 그룹이 여전히 필요할 수 있는 직접 연결 요구 사항을 처리하기 위한 VPC 피어링, 하이브리드 연결을 위한 에지 통합뿐만 아니라 대규모 VPC의 연결을 단순화하기 위한 Transit Gateway가 필요합니다.

## VPC 공유

VPC 공유는 팀 간 네트워크 격리를 VPC 소유자가 엄격하게 관리할 필요는 없지만 계정 수준의 사용자 및 권한은 엄격하게 관리해야 하는 경우에 유용합니다. [공유 VPC](#)를 사용하면 여러 AWS 계정이 중앙에서 관리되는 공유 Amazon VPC에 애플리케이션 리소스 (예: Amazon EC2 인스턴스)를 생성합니다. 이 모델에서는 VPC를 소유한 계정 (소유자)이 하나 이상의 서브넷을 다른 계정 (참여자)과 공유합니다. 서브넷을 공유한 후 참여자는 공유된 서브넷의 해당 애플리케이션 리소스를 보고, 생성하고, 수정하고, 삭제할 수 있습니다. 참여자는 다른 참여자 또는 VPC 소유자에 속한 리소스를 보거나 수정하거나 삭제할 수 없습니다. 공유 VPC의 리소스 간 보안은 보안 그룹, 네트워크 액세스 제어 목록 (NACL)을 사용하거나 서브넷 간 방화벽을 통해 관리됩니다.

VPC 공유의 이점:

- 단순화된 설계 — VPC 간 연결에 대한 복잡성 없음
- 관리되는 VPC 수가 적음
- 네트워크 팀과 애플리케이션 소유자 간의 직무 분리
- IPv4 주소 활용도 향상
- 비용 절감 — 동일한 가용 영역 내에서 서로 다른 계정에 속하는 인스턴스 간 데이터 전송 요금 없음

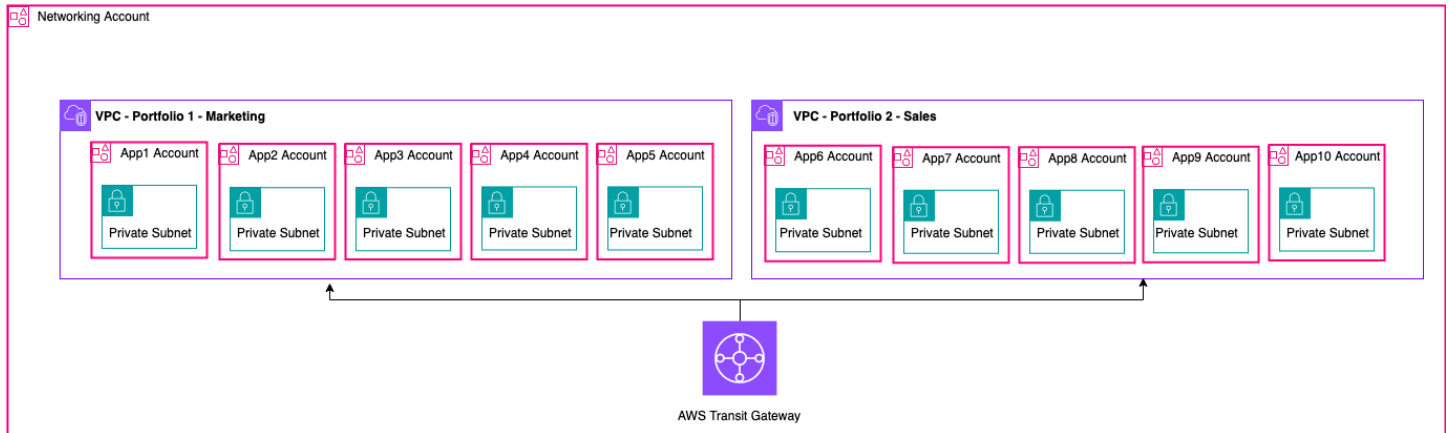
### Note

서브넷을 여러 계정과 공유하는 경우 참가자는 IP 공간과 네트워크 리소스를 공유하므로 참여자가 어느 정도 협력해야 합니다. 필요한 경우 각 참가자 계정마다 다른 서브넷을 공유하도록 선택할 수 있습니다. 참가자당 하나의 서브넷을 통해 네트워크 ACL은 보안 그룹 외에도 네트워크 격리를 제공할 수 있습니다.

대부분의 고객 아키텍처에는 여러 VPC가 포함되며, 이들 중 다수는 둘 이상의 계정과 공유됩니다. Transit Gateway 및 VPC 피어링은 공유 VPC를 연결하는 데 사용할 수 있습니다. 예를 들어 애플리케이션

이션이 10개라고 가정해 보겠습니다. 각 애플리케이션에는 자체 AWS 계정이 필요합니다. 애플리케이션은 두 개의 애플리케이션 포트폴리오로 분류할 수 있습니다 (동일한 포트폴리오 내의 애플리케이션은 네트워킹 요구 사항이 비슷합니다. '마케팅'의 경우 앱 1~5, '세일즈'의 경우 앱 6—10).

애플리케이션 포트폴리오당 VPC 하나 (총 VPC 2개) 를 가질 수 있으며, VPC는 해당 포트폴리오 내의 여러 애플리케이션 소유자 계정과 공유됩니다. 앱 소유자는 각각의 공유 VPC (이 경우 NACL을 사용한 네트워크 경로 분할 및 격리를 위해 서로 다른 서브넷) 에 앱을 배포합니다. 두 개의 공유 VPC는 Transit Gateway를 통해 연결됩니다. 이 설정을 사용하면 다음 그림과 같이 10개의 VPC를 연결해야 했던 것을 단 2개로 줄일 수 있습니다.



## 예제 설정 — 공유 VPC

### Note

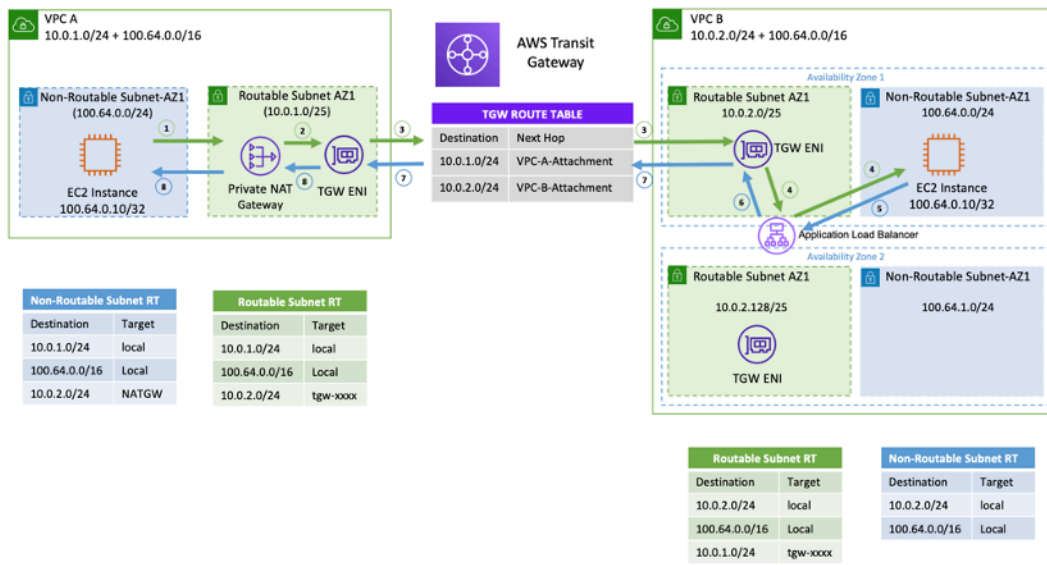
VPC 공유 참여자는 공유 서브넷에서 모든 AWS 리소스를 생성할 수 없습니다. 자세한 내용은 VPC 공유 설명서의 [제한](#) 섹션을 참조하십시오.

VPC 공유의 주요 고려 사항 및 모범 사례에 대한 자세한 내용은 [VPC 공유: 주요 고려 사항 및 모범 사례](#) 블로그 게시물을 참조하십시오.

## 프라이빗 NAT 게이트웨이

팀은 종종 독립적으로 작업하며 프로젝트를 위해 새 VPC를 만들 수 있습니다. 이 VPC에는 클래스가 없는 도메인 간 라우팅 (CIDR) 블록이 겹칠 수 있습니다. 통합을 위해 CIDR이 겹치는 네트워크 간 통신을 지원하고자 할 수 있는데, VPC 피어링 및 Transit Gateway와 같은 기능을 통해서도 이를 달성할 수 없습니다. 프라이빗 NAT 게이트웨이는 이 사용 사례에 도움이 될 수 있습니다. 프라이빗 NAT 게이트웨이는 고유한 프라이빗 IP 주소를 사용하여 중복되는 소스 IP 주소에 대해 소스 NAT를 수행하고, ELB는 중복되는 대상 IP 주소에 대해 대상 NAT를 수행합니다. Transit Gateway 또는 가상 프라이빗 게이

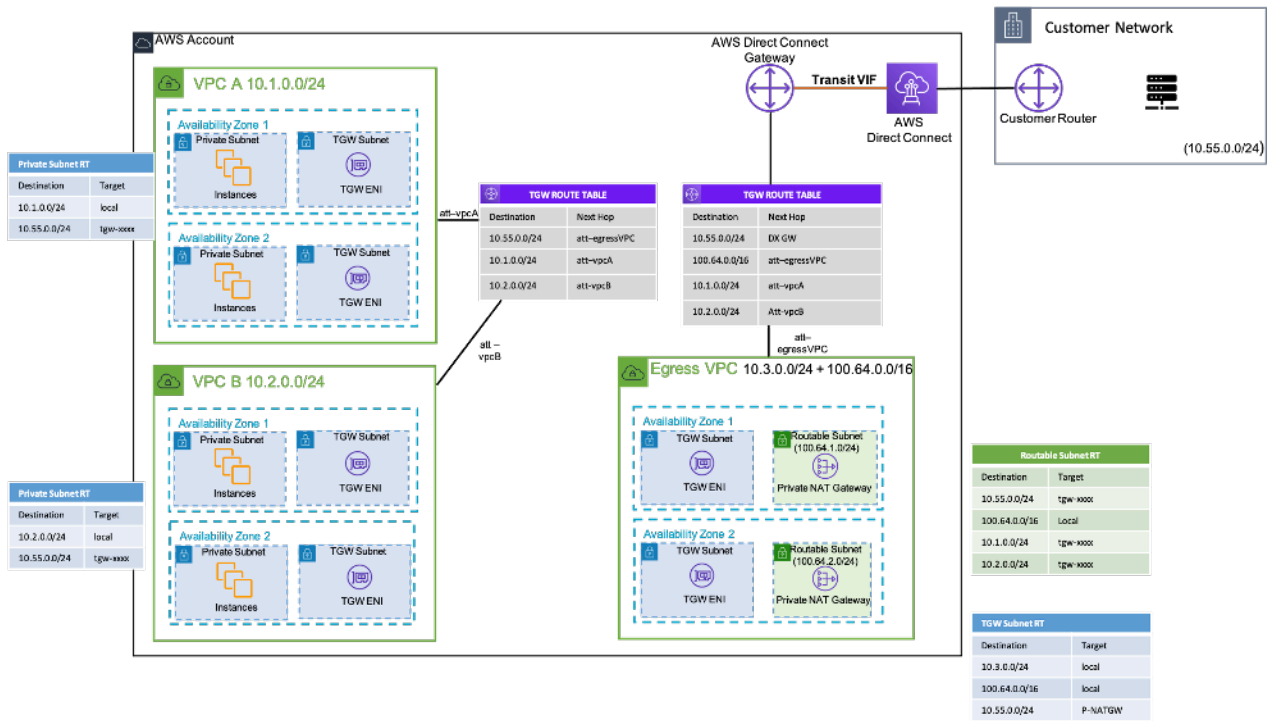
트웨이를 사용하여 프라이빗 NAT 게이트웨이에서 다른 VPC 또는 온프레미스 네트워크로 트래픽을 라우팅할 수 있습니다.



### 예제 설정 — 프라이빗 NAT 게이트웨이

위 그림은 VPC A와 B에 있는 라우팅할 수 없는 (겹치는 CIDR 100.64.0.0/16) 서브넷 두 개를 보여줍니다. 두 서브넷 간에 연결을 설정하기 위해 각각 VPC A와 B에 중복/라우팅이 불가능한 보조 CIDR (라우팅 가능한 서브넷, 및) 을 추가할 수 있습니다. 10.0.1.0/24 10.0.2.0/24 라우팅 가능한 CIDR은 IP 할당을 담당하는 네트워크 관리 팀에서 할당해야 합니다. 프라이빗 NAT 게이트웨이는 IP 주소가 인 VPC A의 라우팅 가능한 서브넷에 추가됩니다. 10.0.1.125 프라이빗 NAT 게이트웨이는 프라이빗 NAT 게이트웨이의 ENI인 VPC A 100.64.0.10 () 10.0.1.125의 라우팅할 수 없는 서브넷에 있는 인스턴스의 요청에 대해 소스 네트워크 주소 변환을 수행합니다. 이제 트래픽은 대상이 인 VPC B ()의 애플리케이션 로드 밸런서 (ALB 10.0.2.10)에 할당된 라우팅 가능한 IP 주소를 가리킬 수 있습니다. 100.64.0.10 트래픽은 Transit Gateway를 통해 라우팅됩니다. 반환 트래픽은 프라이빗 NAT 게이트웨이에 의해 처리되어 연결을 요청한 원래 Amazon EC2 인스턴스로 되돌아갑니다.

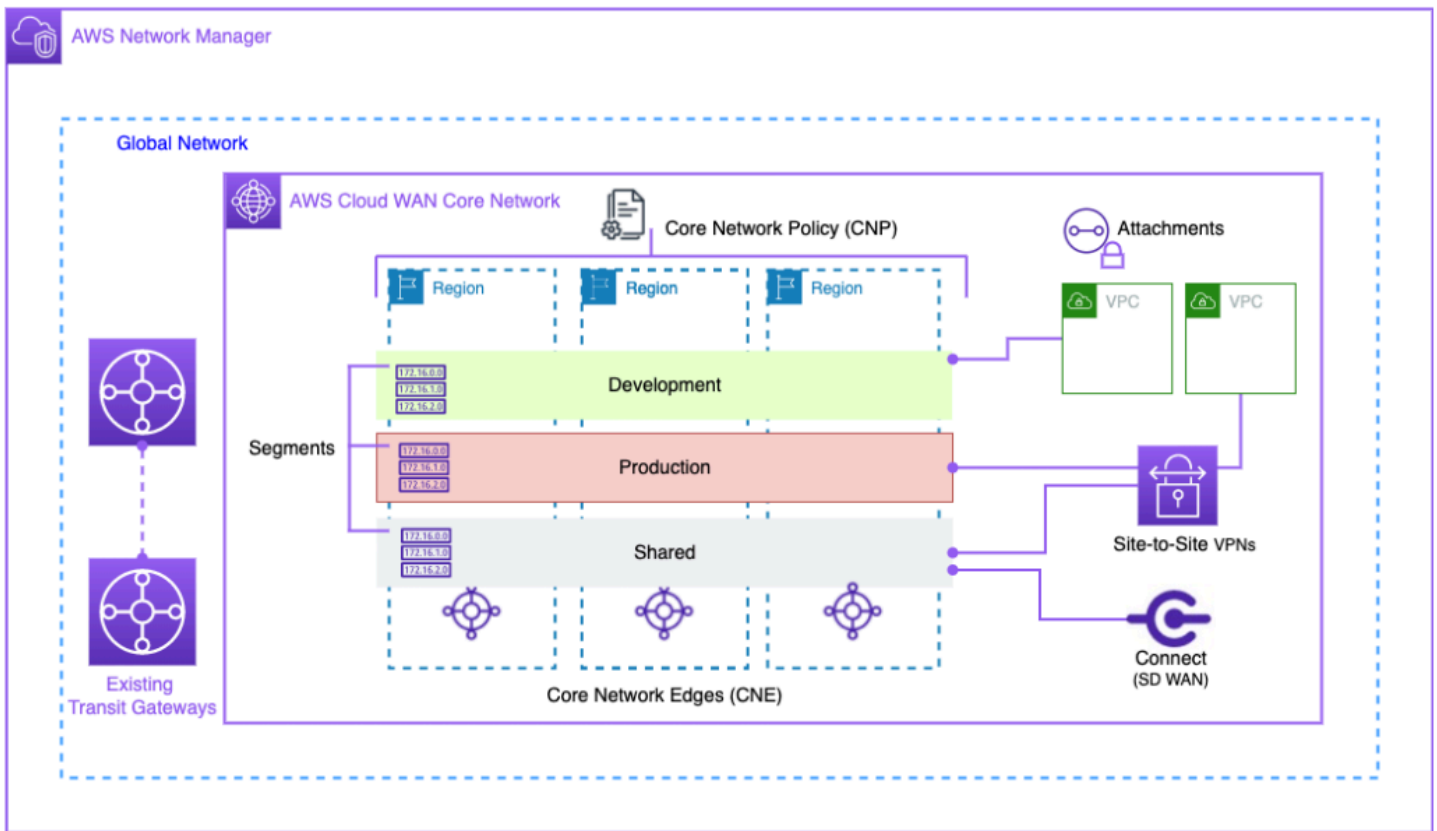
사실 NAT 게이트웨이는 온프레미스 네트워크가 승인된 IP에 대한 액세스를 제한하는 경우에도 사용할 수 있습니다. 규정 준수에 따라 소수의 고객으로 구성된 온프레미스 네트워크는 고객이 소유한 승인된 IP의 제한적이고 연속적인 블록을 통해서만 사실 네트워크 (IGW 제외)와만 통신해야 합니다. 각 인스턴스에 블록과 별도의 IP를 할당하는 대신 프라이빗 NAT 게이트웨이를 사용하여 허용 목록에 있는 각 IP 뒤에 있는 AWS VPC에서 대규모 워크로드를 실행할 수 있습니다. 자세한 내용은 사실 NAT 솔루션으로 [사실 IP 고갈을 해결하는 방법](#) 블로그 게시물을 참조하십시오.



설정 예제 — 사설 NAT 게이트웨이를 사용하여 온프레미스 네트워크에 승인된 IP를 제공하는 방법

## AWS 클라우드 WAN

AWS Cloud WAN은 이전에 트랜짓 게이트웨이, VPC 피어링 및 IPSEC VPN 터널을 통해 가능했던 작업을 네트워크를 연결하는 새로운 방법입니다. 이전에는 하나 이상의 VPC를 구성하고 이전 방법 중 하나로 연결한 다음 IPSEC VPN을 사용하거나 온프레미스 네트워크에 연결했습니다. AWS Direct Connect 한 곳에서는 네트워크 및 보안 상태 구조를 정의하고 다른 곳에서는 네트워크를 정의해야 합니다. 클라우드 WAN을 사용하면 이러한 모든 구조를 한 곳에서 중앙 집중화할 수 있습니다. 정책에 따라 네트워크를 분할하여 누가 누구와 대화할 수 있는지 결정하고, 이러한 세그먼트를 통한 프로덕션 트래픽을 개발 또는 테스트 워크로드 또는 온프레미스 네트워크로부터 분리할 수 있습니다.



## 클라우드 WAN 블록 다이어그램

AWS 네트워크 관리자 사용자 인터페이스 및 API를 통해 글로벌 네트워크를 관리합니다. 글로벌 네트워크는 모든 네트워크 객체의 루트 수준 컨테이너이고, 코어 네트워크는 AWS에서 관리하는 글로벌 네트워크의 일부입니다. 코어 네트워크 정책 (CNP)은 코어 네트워크의 모든 측면을 정의하는 단일 버전의 정책 문서입니다. 첨부 파일은 코어 네트워크에 추가하려는 모든 연결 또는 리소스입니다. 코어 네트워크 에지 (CNE)는 정책을 준수하는 첨부 파일의 로컬 연결 지점입니다. 네트워크 세그먼트는 기본적으로 세그먼트 내에서만 통신을 허용하는 라우팅 도메인입니다.

CloudWAN을 사용하려면:

1. AWS Network Manager에서 글로벌 네트워크 및 관련 코어 네트워크를 생성합니다.
2. 세그먼트에 연결하는 데 사용할 세그먼트, ASN 범위 AWS 리전 및 태그를 정의하는 CNP를 생성합니다.
3. 네트워크 정책을 적용합니다.
4. 리소스 액세스 관리자를 사용하여 사용자, 계정 또는 조직과 코어 네트워크를 공유하십시오.
5. 첨부 파일을 만들고 태그를 지정합니다.
6. 코어 네트워크를 포함하도록 연결된 VPC의 경로를 업데이트하십시오.

클라우드 WAN은 AWS 인프라를 전 세계적으로 연결하는 프로세스를 단순화하도록 설계되었습니다. 이를 통해 중앙 집중식 권한 정책으로 트래픽을 분류하고 회사 위치의 기존 인프라를 사용할 수 있습니다. 또한 클라우드 WAN은 VPC, SD-WAN, 클라이언트 VPN, 방화벽, VPN 및 데이터 센터 리소스를 연결하여 클라우드 WAN에 연결합니다. 자세한 내용은 [AWS 클라우드 WAN 블로그 게시물을](#) 참조하십시오.

AWS Cloud WAN은 클라우드와 온 프레미스 환경을 연결하는 통합 네트워크를 지원합니다. 조직은 보안을 위해 차세대 방화벽 (NGFW) 과 침입 방지 시스템 (IPS) 을 사용합니다. [AWS Cloud WAN 및 Transit Gateway 마이그레이션 및 상호 운용성 패턴](#) 블로그 게시물에서는 단일 지역 및 다중 지역 네트워크를 비롯한 Cloud WAN 네트워크의 아웃바운드 네트워크 트래픽을 중앙에서 관리 및 검사하기 위한 아키텍처 패턴을 설명하고 라우팅 테이블을 구성합니다. 이러한 아키텍처는 안전한 클라우드 환경을 유지하면서 데이터와 애플리케이션을 안전하게 유지합니다.

클라우드 WAN에 대한 자세한 내용은 [AWS Cloud WAN 블로그 게시물의 중앙 집중식 아웃바운드 검사 아키텍처](#)를 참조하십시오.

## Amazon VPC Lattice

Amazon VPC Lattice는 다양한 계정과 가상 사설 클라우드에서 서비스를 연결, 모니터링 및 보호하는데 사용되는 완전 관리형 애플리케이션 네트워킹 서비스입니다. VPC Lattice는 논리적 경계 내에서 서비스를 상호 연결하는 데 도움이 되므로 서비스를 효율적으로 관리하고 검색할 수 있습니다.

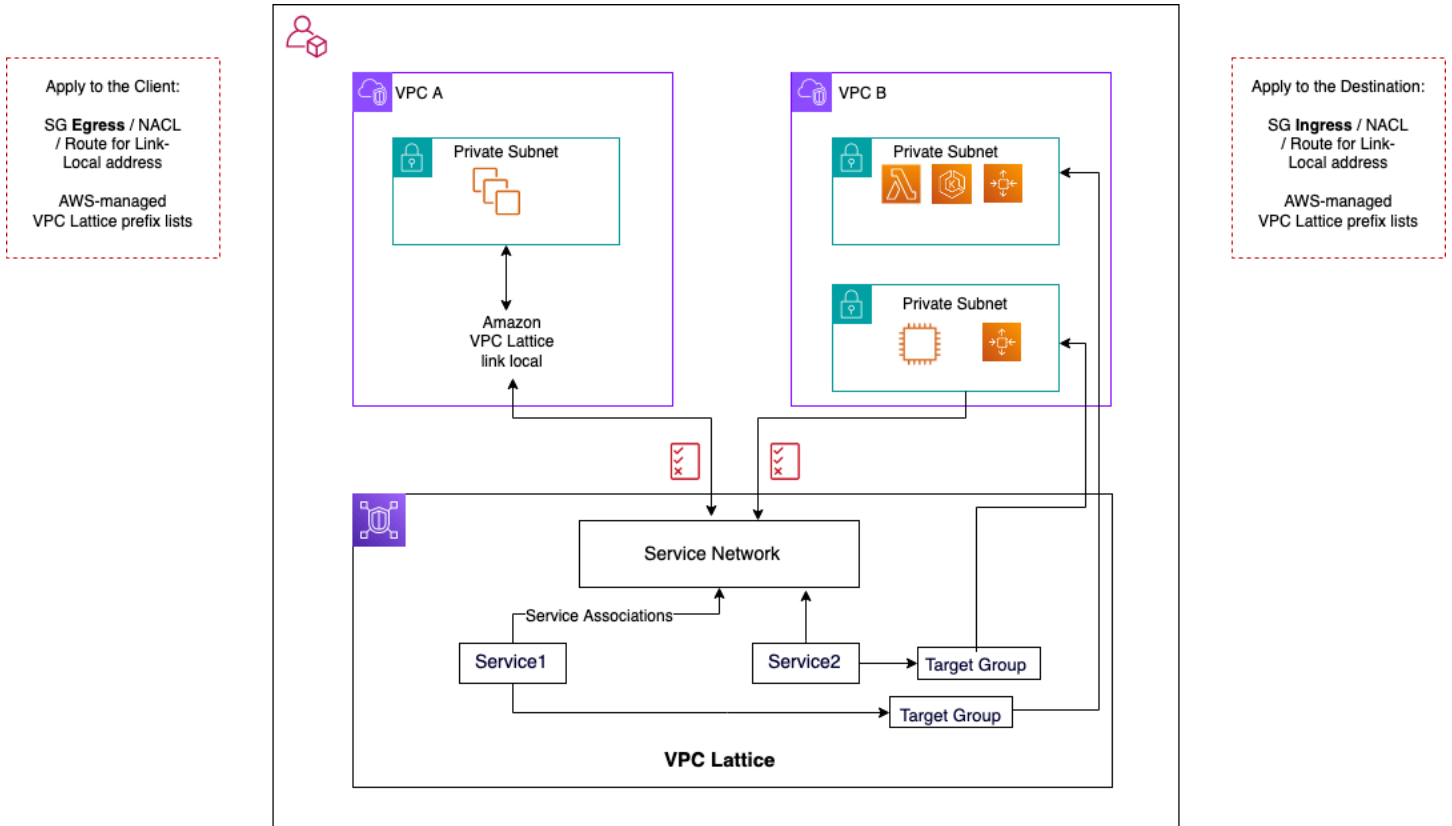
VPC 래티스 구성 요소는 다음과 같이 구성됩니다.

- 서비스 - 인스턴스, 컨테이너 또는 Lambda 함수에서 실행되는 애플리케이션 단위이며 리스너, 규칙 및 대상 그룹으로 구성됩니다.
- 서비스 네트워크 - 서비스 검색 및 연결을 자동으로 구현하고 공통 액세스 및 관찰 가능 정책을 서비스 컬렉션에 적용하는 데 사용되는 논리적 경계입니다.
- 인증 정책 - 요청 수준 인증 및 상황별 권한 부여를 지원하기 위해 서비스 네트워크 또는 개별 서비스와 연결할 수 있는 IAM 리소스 정책입니다.
- 서비스 디렉터리 - 사용자가 소유하고 있거나 AWS Resource Access Manager를 통해 공유된 서비스를 중앙에서 볼 수 있습니다.

VPC 래티스 사용 단계:

1. 서비스 네트워크 생성. 서비스 네트워크는 일반적으로 네트워크 관리자가 전체 액세스 권한을 가진 네트워크 계정에 있습니다. 서비스 네트워크는 조직 내 여러 계정에서 공유할 수 있습니다. 공유는 개별 서비스 또는 전체 서비스 계정에서 수행할 수 있습니다.

2. VPC를 서비스 네트워크에 연결하여 각 VPC의 애플리케이션 네트워킹을 활성화하면 다양한 서비스가 네트워크 내에 등록된 다른 서비스를 사용하기 시작할 수 있습니다. 보안 그룹을 적용하여 트래픽을 제어합니다.
3. 개발자는 서비스를 정의하며, 서비스는 서비스 디렉터리에 채워지고 서비스 네트워크에 등록됩니다. VPC Lattice에는 구성된 모든 서비스의 주소록이 들어 있습니다. 또한 개발자는 블루/그린 배포를 사용하도록 라우팅 정책을 정의할 수 있습니다. 보안은 인증 및 권한 부여 정책이 정의된 서비스 네트워크 수준과 IAM을 사용한 액세스 정책이 구현되는 서비스 수준에서 관리됩니다.



### VPC 래티스 통신 흐름

자세한 내용은 [VPC Lattice](#) 사용 설명서에서 확인할 수 있습니다.

## 하이브리드 커넥티비티

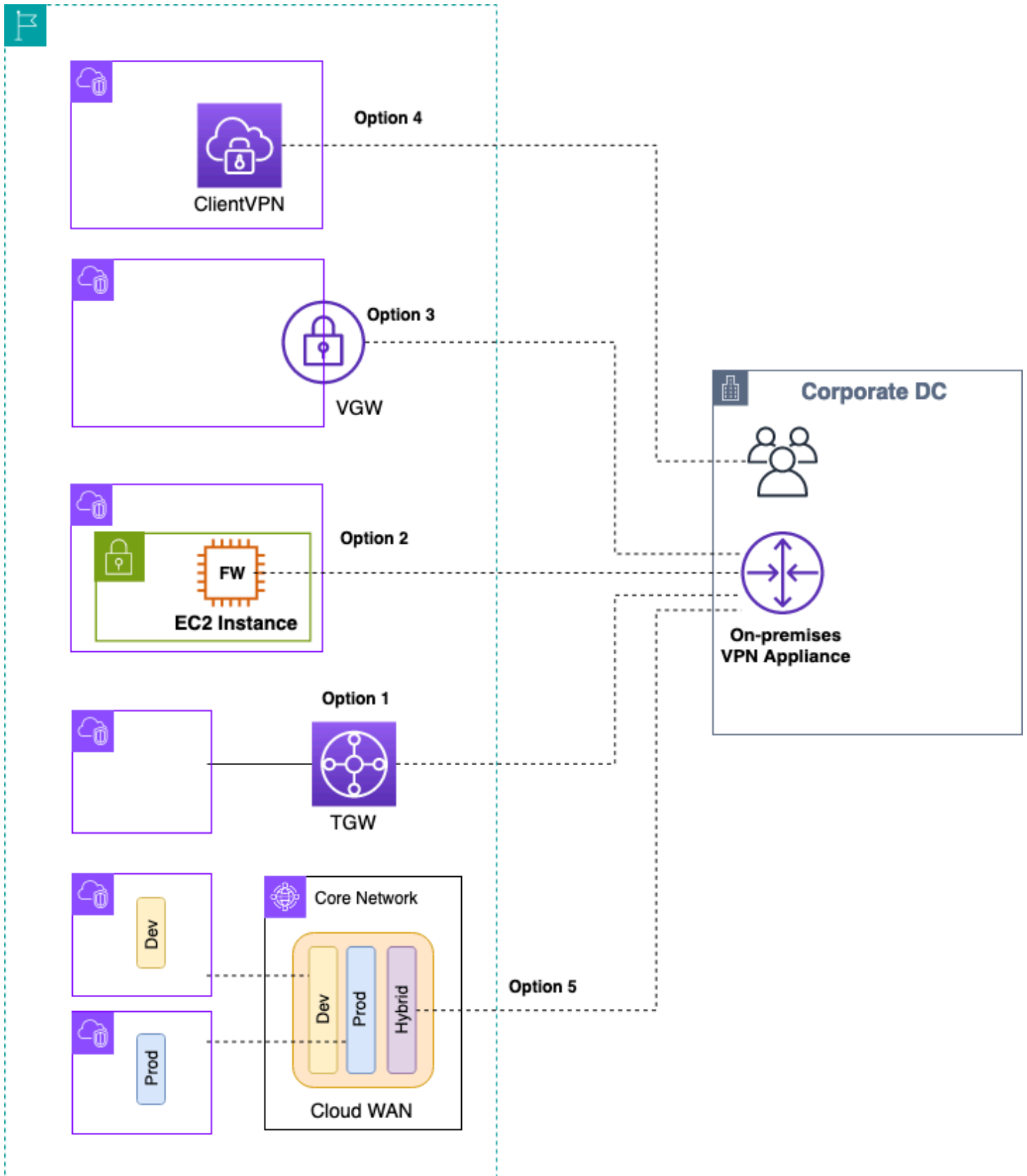
이 섹션에서는 클라우드 리소스를 온프레미스 데이터 센터에 안전하게 연결하는 데 중점을 둡니다. 하이브리드 연결을 활성화하기 위한 세 가지 접근 방식은 다음과 같습니다.

- **One-to-one 연결** — 이 설정에서는 모든 VPC에 대해 VPN 연결 및/또는 Direct Connect 프라이빗 VIF가 생성됩니다. 이는 가상 프라이빗 게이트웨이 (VGW) 를 사용하여 수행됩니다. 이 옵션은 소수의 VPC에 유용하지만 고객이 VPC를 확장함에 따라 VPC별 하이브리드 연결을 관리하기가 어려워질 수 있습니다.
- **엣지 통합** — 이 설정에서 고객은 단일 엔드포인트에서 여러 VPC의 하이브리드 IT 연결을 통합합니다. 모든 VPC는 이러한 하이브리드 연결을 공유합니다. 이는 AWS Transit Gateway 및 게이트웨이를 사용하여 이루어집니다. AWS Direct Connect
- **풀 메시 하이브리드 통합** — 이 설정에서 고객은 기본 제공되는 CloudWAN을 사용하여 단일 엔드포인트에서 여러 VPC에 대한 연결을 통합합니다. AWS Transit Gateway는 하나 이상의 AWS 계정에서 네트워킹하기 위한 완전한 정책 기반 접근 방식이며, 코드로 표시됩니다. 현재 엣지 AWS Direct Connect 연결에 사용하려면 Transit Gateway를 CloudWAN으로 피어링해야 합니다.

## VPN

AWS에 VPN을 설정하는 방법은 여러 가지가 있습니다.



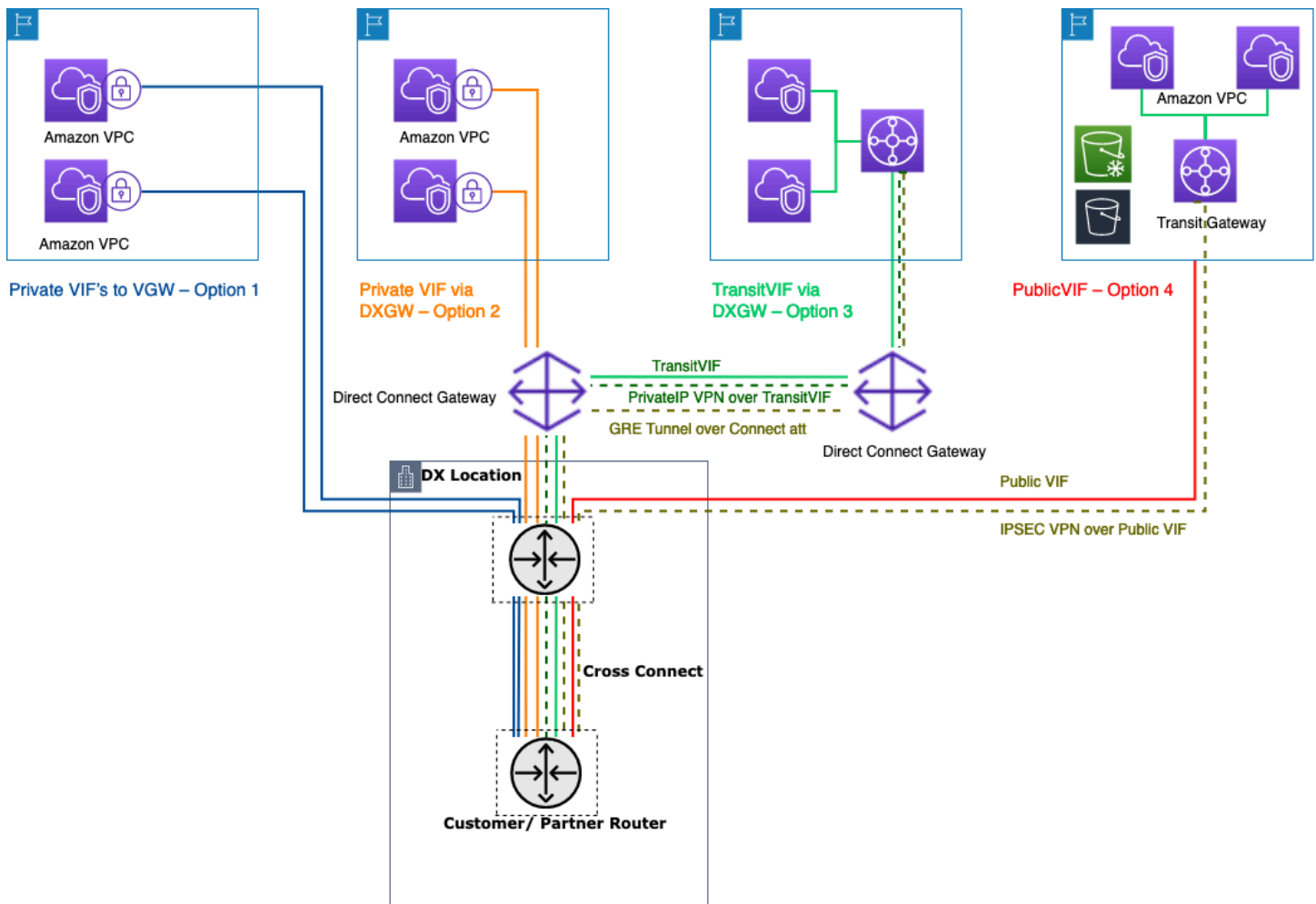


### AWS VPN 옵션

- 옵션 1: Transit Gateway에서 VPN 연결 통합 - 이 옵션은 Transit Gateway의 Transit Gateway VPN 첨부 파일을 활용합니다. Transit Gateway는 site-to-site VPN에 대한 IPsec 종료를 지원합니다. 고객은 Transit Gateway에 VPN 터널을 생성하고 여기에 연결된 VPC에 액세스할 수 있습니다. Transit Gateway는 정적 및 BGP 기반 동적 VPN 연결을 모두 지원합니다. 또한 Transit Gateway는 VPN 연결 시 [동일 비용 다중 경로 \(ECMP\)](#) 를 지원합니다. 각 VPN 연결의 터널당 최대 처리량은 1.25Gbps 입니다. ECMP를 활성화하면 VPN 연결 전반의 처리량을 집계하여 기본 최대 한도인 1.25Gbps 이상으로 확장할 수 있습니다. 이 옵션에서는 [Transit Gateway 요금과 AWS VPN 가격을](#) 모두 지불합니다. AWS는 VPN 연결에 이 옵션을 사용할 것을 권장합니다. 자세한 내용은 [AWS Transit Gateway를 사용하여 VPN 처리량 조정](#) 블로그 게시물을 참조하십시오.
- 옵션 2: Amazon EC2 인스턴스에서 VPN 종료 — 이 옵션은 특정 공급업체 소프트웨어 기능 세트 (예: [Cisco DMVPN 또는 일반 라우팅 캡슐화 \(GRE\)](#)) 를 원하거나 다양한 VPN 배포 전반에서 운영 일관성을 원하는 옛지 케이스에서 고객이 활용할 수 있습니다. 옛지 통합을 위해 전송 VPC 디자인을 사용할 수 있지만, 전송 VPC [VPC에서 VPC로의 연결](#) 섹션의 모든 주요 고려 사항은 하이브리드 VPN 연결에 적용된다는 점을 기억해야 합니다. 고가용성을 관리할 책임은 사용자에게 있으며, EC2 인스턴스뿐 아니라 벤더 소프트웨어 라이선스 및 지원 비용도 지불해야 합니다.
- 옵션 3: 가상 프라이빗 게이트웨이 (VGW) 에서 VPN 종료 — 이 AWS Site-to-Site VPN 서비스 옵션을 one-to-one 사용하면 VPC당 하나의 VPN 연결 (한 쌍의 중복 VPN 터널로 구성) 을 생성하는 연결 설계가 가능합니다. 이는 AWS로의 VPN 연결을 시작하는 좋은 방법이지만, VPC의 수를 확장함에 따라 점점 늘어나는 VPN 연결을 관리하기가 어려워질 수 있습니다. 따라서 Transit Gateway를 활용하는 옛지 통합 설계는 결국 더 나은 옵션이 될 것입니다. VGW에 대한 VPN 처리량은 터널당 1.25Gbps로 제한되며 ECMP 로드 밸런싱은 지원되지 않습니다. 요금 측면에서는 AWS VPN 요금에 대해서만 비용을 지불하고 VGW 실행에는 요금이 부과되지 않습니다. 자세한 내용은 [AWS VPN 요금 및 가상 프라이빗 게이트웨이AWS VPN 이용을](#) 참조하십시오.
- 옵션 4: 클라이언트 VPN 엔드포인트에서 VPN 연결 종료 — AWS Client VPN은 온 프레미스 네트워크의 AWS 리소스 및 리소스에 안전하게 액세스할 수 있게 해주는 관리형 클라이언트 기반 VPN 서비스입니다. 클라이언트 VPN을 사용하면 OpenVPN 또는 AWS에서 제공하는 VPN 클라이언트를 사용하여 어느 위치에서든 리소스에 액세스할 수 있습니다. Client VPN 엔드포인트를 설정하면 클라이언트와 사용자가 연결하여 TLS (전송 계층 보안) VPN 연결을 설정할 수 있습니다. 자세한 내용은 [AWS Client VPN 설명서를 참조하십시오](#).
- 옵션 5: AWS 클라우드 WAN에서 VPN 연결 통합 — 이 옵션은 이 목록의 첫 번째 옵션과 비슷하지만 CloudWAN 패브릭을 사용하여 네트워크 정책 문서를 통해 프로그래밍 방식으로 VPN 연결을 구성합니다.

# AWS Direct Connect

인터넷을 통한 VPN은 시작하기에 좋은 옵션이지만, 프로덕션 트래픽에서는 인터넷 연결이 안정적이지 않을 수 있습니다. 이러한 신뢰성이 낮기 때문에 많은 고객이 선택합니다 [AWS Direct Connect](#). AWS Direct Connect 인터넷을 사용하여 AWS에 연결하는 대신 사용할 수 있는 네트워킹 서비스입니다. 이를 사용하면 AWS Direct Connect 이전에는 인터넷을 통해 전송되었을 데이터가 시설과 AWS 간의 사설 네트워크 연결을 통해 전달됩니다. 많은 상황에서 사설 네트워크 연결은 인터넷 기반 연결보다 비용을 줄이고, 대역폭을 늘리고, 더 일관된 네트워크 경험을 제공할 수 있습니다. VPC에 연결하는 AWS Direct Connect에 사용할 수 있는 몇 가지 방법이 있습니다.



를 사용하여 온프레미스 데이터 센터를 연결하는 방법 AWS Direct Connect

- 옵션 1: VPC에 연결된 VGW에 프라이빗 가상 인터페이스 (VIF) 생성 — Direct Connect 연결당 50개의 VIF를 생성하여 최대 50개의 VPC에 연결할 수 있습니다 (하나의 VIF는 하나의 VPC에 대한 연결을 제공함). VPC당 하나의 BGP 피어링이 있습니다. 이 설정에서의 연결은 Direct Connect 위치가 위

치한 AWS 지역으로 제한됩니다. VIF를 VPC에 one-to-one 매핑하고 글로벌 액세스가 부족하기 때문에 랜딩 존에서 VPC에 액세스하는 데 가장 선호되지 않는 방법입니다.

- 옵션 2: 여러 VGW와 연결된 Direct Connect 게이트웨이에 프라이빗 VIF 생성 (각 VGW는 VPC에 연결됨) — Direct Connect 게이트웨이는 전 세계에서 사용할 수 있는 리소스입니다. 모든 지역에서 Direct Connect 게이트웨이를 생성하고 중국을 포함한 다른 모든 지역에서 액세스할 수 있습니다 GovCloud (중국 제외). Direct Connect 게이트웨이는 단일 프라이빗 VIF를 통해 모든 AWS 계정의 전 세계 최대 20개의 VPC (VGW 이용) 에 연결할 수 있습니다. 랜딩 존이 소수의 VPC (10개 이하 VPC) 로 구성되어 있거나 글로벌 액세스가 필요한 경우 유용한 옵션입니다. Direct Connect 연결당 Direct Connect 게이트웨이당 하나의 BGP 피어링 세션이 있습니다. Direct Connect 게이트웨이는 북쪽/남쪽 트래픽 흐름에만 사용되며 VPC-VPC 연결은 허용하지 않습니다. 자세한 내용은 설명서의 [가상 프라이빗 게이트웨이 연결을](#) 참조하십시오. AWS Direct Connect 이 옵션을 사용하면 Direct Connect 위치가 위치한 AWS 지역에만 연결이 제한되지 않습니다. AWS Direct Connect 게이트웨이는 노스/사우스 트래픽 플로우에만 사용되며 VPC-VPC 연결은 허용하지 않습니다. 이 규칙의 예외는 동일한 게이트웨이 및 동일한 가상 인터페이스에 연결된 VGW가 있는 둘 이상의 VPC에 슈퍼넷을 알리는 경우입니다. AWS Direct Connect 이 경우 VPC는 엔드포인트를 통해 서로 통신할 수 있습니다. AWS Direct Connect 자세한 내용은 [AWS Direct Connect 게이트웨이 설명서를 참조하십시오](#).
- 옵션 3: Transit Gateway와 연결된 Direct Connect 게이트웨이에 전송 VIF 생성 - Transit VIF를 사용하여 Transit Gateway 인스턴스를 Direct Connect 게이트웨이에 연결할 수 있습니다. AWS Direct Connect 이제 모든 포트 속도에 대해 Transit Gateway에 대한 연결을 지원하므로 고속 연결 (1Gbps 이상) 이 필요하지 않은 경우 Transit Gateway 사용자에게 보다 비용 효율적인 선택을 제공합니다. 이를 통해 Transit Gateway에 연결하여 50, 100, 200, 300, 400, 500Mbps의 속도로 다이렉트 커넥트를 사용할 수 있습니다. Transit VIF를 사용하면 단일 전송 VIF 및 BGP 피어링을 통해 다양한 AWS 지역 및 AWS 계정의 AWS Direct Connect 게이트웨이당 최대 6개의 Transit Gateway 인스턴스 (수천 개의 VPC에 연결할 수 있음) 에 온 프레미스 데이터 센터를 연결할 수 있습니다. 이는 여러 VPC를 대규모로 연결하는 옵션 중에서 가장 간단한 설정이지만 [Transit Gateway](#) 할당량을 염두에 두어야 합니다. 한 가지 주요 제한 사항은 Transit Gateway에서 전송 VIF를 통해 온프레미스 라우터로 [200개의 접두사만](#) 알릴 수 있다는 것입니다. 이전 옵션의 경우 Direct Connect 가격을 지불하면 됩니다. 이 옵션의 경우 Transit Gateway 첨부 파일 및 데이터 처리 요금도 지불해야 합니다. 자세한 내용은 [Direct Connect의 Transit Gateway 연결 설명서를 참조하십시오](#).
- 옵션 4: Direct Connect 퍼블릭 VIF를 통해 Transit Gateway에 대한 VPN 연결 생성 — 퍼블릭 VIF를 사용하면 퍼블릭 IP 주소를 사용하여 모든 AWS 퍼블릭 서비스 및 엔드포인트에 액세스할 수 있습니다. Transit Gateway에서 VPN 연결을 생성하면 AWS 측에서 VPN 엔드포인트에 사용할 두 개의 퍼블릭 IP 주소를 얻게 됩니다. 퍼블릭 VIF를 통해 이러한 퍼블릭 IP에 연결할 수 있습니다. 퍼블릭 VIF를 통해 원하는 만큼 많은 Transit Gateway 인스턴스에 대한 VPN 연결을 생성할 수 있습니다. 퍼블릭 VIF를 통해 BGP 피어링을 생성하면 AWS는 [전체 AWS 퍼블릭 IP](#) 범위를 라우터에 알립니다. 특정 트래픽만 허용하려면 (예: VPN 종료 엔드포인트로만 트래픽을 허용) 방화벽 온프레미스 시설을

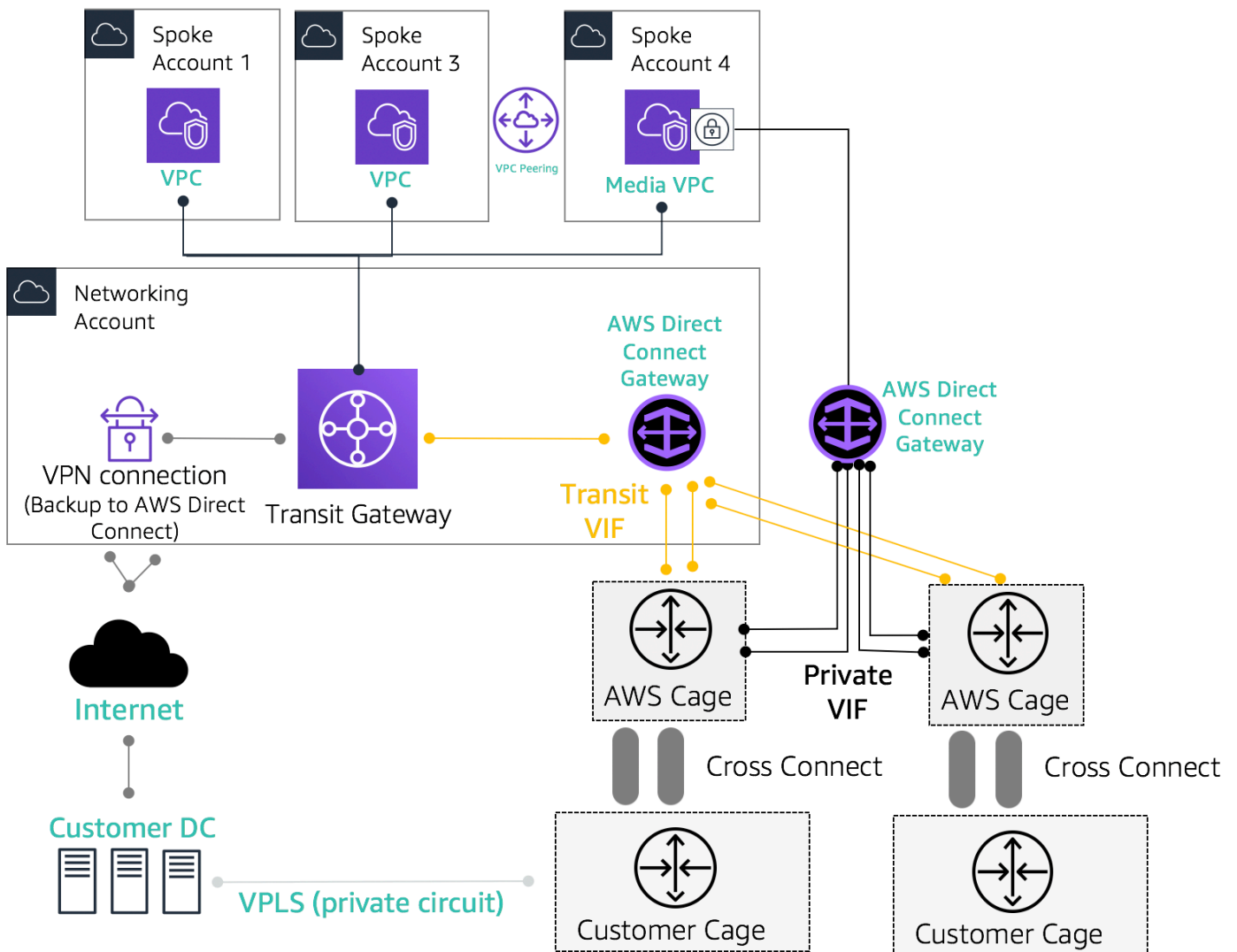
사용하는 것이 좋습니다. 이 옵션은 네트워크 계층에서 Direct Connect를 암호화하는 데 사용할 수 있습니다.

- 옵션 5: 사설 IP VPN을 AWS Direct Connect 사용하여 Transit Gateway에 VPN 연결 생성 — 사설 IP VPN은 고객이 사설 IP 주소를 사용하여 Direct Connect를 통해 AWS 사이트 간 VPN 연결을 배포할 수 있는 기능을 제공합니다. 이 기능을 사용하면 퍼블릭 IP 주소 없이도 Direct Connect 연결을 통해 온프레미스 네트워크와 AWS 간의 트래픽을 암호화할 수 있으므로 보안과 네트워크 프라이버시를 동시에 강화할 수 있습니다. 사설 IP VPN은 Transit VIF에 배포되므로 Transit Gateway를 사용하여 고객 VPC의 중앙 집중식 관리 및 온프레미스 네트워크 연결을 보다 안전하고 사실적이며 확장 가능한 방식으로 관리할 수 있습니다.
- 옵션 6: 트랜짓 VIF를 통해 Transit Gateway에 GRE 터널 생성 — Transit Gateway Connect 연결 유형은 GRE를 지원합니다. Transit Gateway Connect를 사용하면 SD-WAN 네트워크 가상 어플라이언스와 Transit Gateway 간에 IPsec VPN을 설정할 필요 없이 SD-WAN 인프라를 AWS에 기본적으로 연결할 수 있습니다. GRE 터널은 Transit Gateway Connect를 첨부 유형으로 사용하여 전송 VIF를 통해 설정할 수 있으므로 VPN 연결에 비해 더 높은 대역폭 성능을 제공합니다. 자세한 내용은 [AWS Transit Gateway Connect를 통한 SD-WAN 연결 단순화](#) 블로그 게시물을 참조하십시오.

“VIF에서 Direct Connect Gateway로 전송” 옵션은 Direct Connect 연결당 단일 BGP 세션을 사용하여 단일 지점 (Transit Gateway) AWS 리전 에서 특정 항목에 대한 모든 온프레미스 연결을 통합할 수 있기 때문에 최상의 옵션인 것 같습니다. 그러나 이 옵션과 관련된 일부 제한 및 고려 사항으로 인해 랜딩 존 연결 요구 사항에 따라 사설 VIF와 전송 VIF를 함께 사용할 수 있습니다.

다음 그림은 VPC에 연결하는 기본 방법으로 Transit VIF를 사용하고 온프레미스 데이터 센터에서 미디어 VPC로 매우 많은 양의 데이터를 전송해야 하는 엣지 사용 사례에 프라이빗 VIF를 사용하는 샘플 설정을 보여줍니다. 프라이빗 VIF는 Transit Gateway 데이터 처리 요금을 피하기 위해 사용됩니다. [이중화를 극대화하려면](#) 서로 다른 두 Direct Connect 위치에 최소 두 개의 연결을 설치하여 총 네 개의 연결을 사용하는 것이 좋습니다. 연결당 VIF를 하나씩 생성하여 총 4개의 프라이빗 VIF와 4개의 전송 VIF를 생성합니다. 연결에 대한 백업 연결로 VPN을 만들 수도 있습니다. AWS Direct Connect

“트랜짓 VIF를 통해 Transit Gateway에 GRE 터널 생성” 옵션을 사용하면 SD-WAN 인프라를 AWS와 기본적으로 연결할 수 있습니다. 따라서 SD-WAN 네트워크 가상 어플라이언스와 Transit Gateway 간에 IPsec VPN을 설정할 필요가 없습니다.



## 하이브리드 연결을 위한 샘플 참조 아키텍처

네트워크 서비스 계정을 사용하여 네트워크 관리 경계를 지정할 수 있는 Direct Connect 리소스를 만들 수 있습니다. Direct Connect 연결, Direct Connect 게이트웨이 및 트랜짓 게이트웨이는 모두 네트워크 서비스 계정에 있을 수 있습니다. 랜딩 존과 AWS Direct Connect 연결을 공유하려면 Transit Gateway를 다른 AWS RAM 계정과 공유하기만 하면 됩니다.

## 다이렉트 커넥트 연결의 MACsec 보안

[고객은 일부 위치에서 10Gbps 및 100Gbps 전용 연결에 대해 MAC 보안 표준 \(MACsec\) 암호화 \(IEEE 802.1AE\)를 사용하여 Direct Connect 연결을 사용할 수 있습니다. 이 기능을 통해 고객은 계층 2 수준에서 데이터를 보호할 수 있으며 Direct Connect는 point-to-point 암호화를 제공합니다. MACsec Direct Connect 기능을 활성화하려면 \[MACsec 사전 요구 사항을 충족해야\]\(#\) 합니다. MACsec은 링크를 hop-by-](#)

hop 기본적으로 보호하므로 장치가 Direct Connect 장치와 직접 레이어 2 인접성을 가져야 합니다. 라스트 마일 제공업체가 MACsec에서 연결이 제대로 작동하는지 확인하는 데 도움을 줄 수 있습니다. 자세한 내용은 [AWS Direct Connect 연결에 MACsec 보안 추가](#)를 참조하십시오.

## AWS Direct Connect 레질리언스 권장 사항

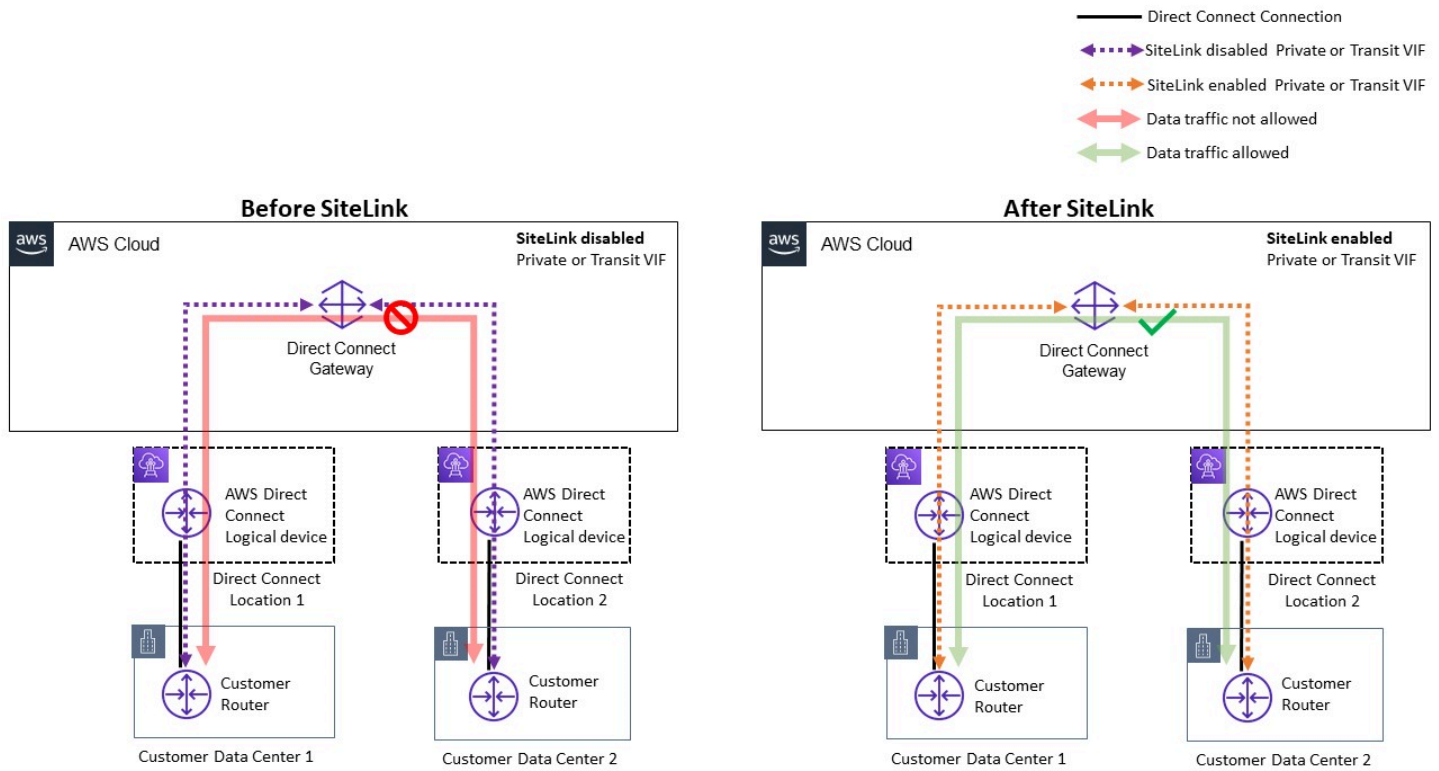
를 AWS Direct Connect 통해 고객은 온프레미스 네트워크에서 Amazon VPC와 AWS 리소스에 매우 탄력적으로 연결할 수 있습니다. 고객이 여러 데이터 센터에서 연결하여 단일 지점의 물리적 위치 장애를 없애는 것이 가장 좋습니다. 또한 워크로드 유형에 따라 고객은 이중화를 위해 둘 이상의 Direct Connect 연결을 사용하는 것이 좋습니다.

또한 AWS는 고객에게 여러 중복 모델이 포함된 연결 마법사를 제공하는 AWS Direct Connect Resiliency Toolkit을 제공합니다. 이를 통해 고객은 서비스 수준 계약 (SLA) 요구 사항에 가장 적합한 모델을 결정하고 그에 따라 Direct Connect 연결을 사용하여 하이브리드 연결을 설계할 수 있습니다. [자세한 내용은 복원력 권장 사항을 참조하십시오.](#) [AWS Direct Connect](#)

## AWS Direct Connect SiteLink

이전에는 다크 파이버 또는 기타 기술인 IPSEC VPN을 통한 직접 회로 구축을 사용하거나 MPLS 또는 기존 T1 회로와 같은 기술을 갖춘 타사 회로 공급자를 사용하여 온프레미스 네트워크에 대한 site-to-site 링크를 구성할 수 있었습니다. MetroEthernet 의 SiteLink 출현으로 이제 고객은 특정 위치에서 종료되는 온-프레미스 위치에 대한 직접 site-to-site 연결을 활성화할 수 있습니다. AWS Direct Connect 회로를 사용하면 트래픽을 VPC를 통해 라우팅할 필요 없이 AWS 지역을 완전히 우회하여 site-to-site 연결을 제공할 수 있습니다.

이제 위치 간 가장 빠른 경로를 통해 데이터를 전송함으로써 글로벌 네트워크의 사무실과 데이터 센터 간에 글로벌하고 안정적인 pay-as-you-go 연결을 구축할 수 있습니다. AWS Direct Connect



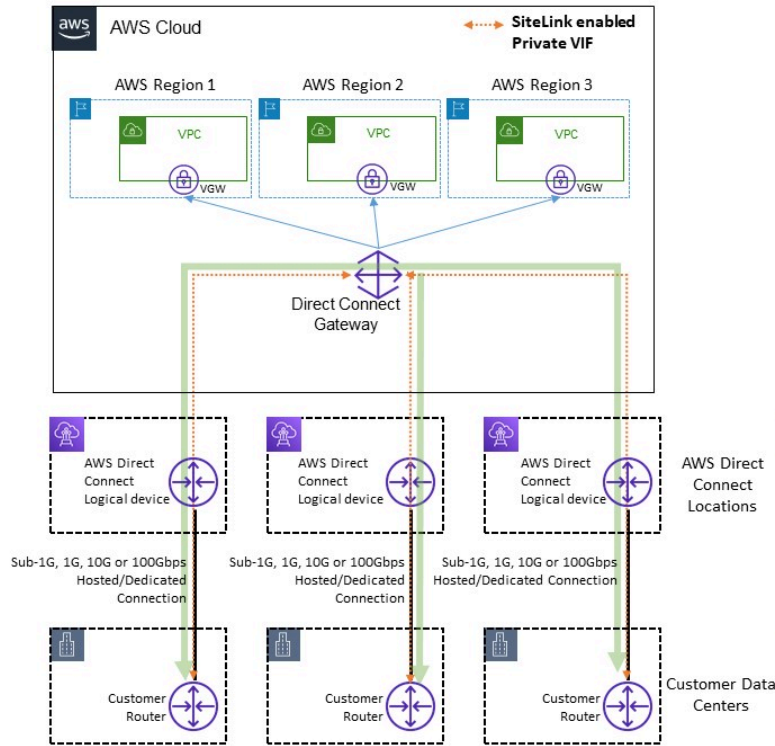
### 에 대한 샘플 참조 아키텍처 AWS Direct Connect SiteLink

를 사용할 SiteLink 때는 먼저 전 세계 100개 이상의 AWS Direct Connect 위치에 있는 온프레미스 네트워크를 AWS에 연결합니다. 그런 다음 해당 연결에 가상 인터페이스 (VIF) 를 생성하고 활성화합니다. SiteLink 모든 VIF가 동일한 AWS Direct Connect 게이트웨이 (DXGW) 에 연결되면 VIF 간에 데이터 전송을 시작할 수 있습니다. 데이터는 빠르고 안전하며 신뢰할 수 있는 AWS 글로벌 네트워크를 사용하여 AWS Direct Connect 위치 간 최단 경로를 따라 목적지에 도달합니다. 리소스가 없어도 사용할 AWS 리전 SiteLink 수 있습니다.

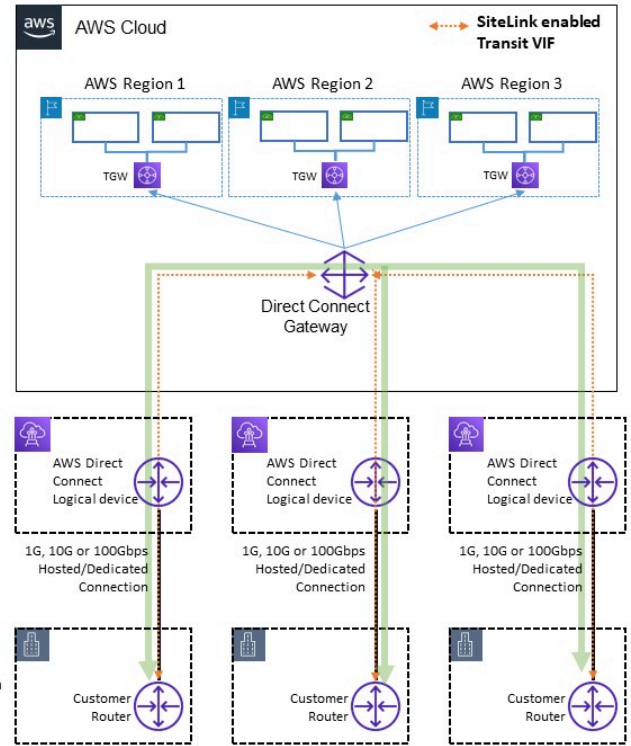
를 통해 DXGW는 SiteLink 활성화된 VIF를 통해 라우터로부터 IPv4/IPv6 접두사를 학습하고 SiteLink, BGP 최적 경로 알고리즘을 실행하고, NextHop AS\_Path와 같은 속성을 업데이트하고, 이러한 BGP 접두사를 해당 DXGW와 관련된 나머지 활성화 VIF에 다시 광고합니다. SiteLink SiteLink VIF에서 사용하지 않도록 설정하면 DXGW는 이 VIF를 통해 학습된 SiteLink 온-프레미스 접두사를 활성화된 다른 VIF에 알리지 않습니다. SiteLink 비활성화된 VIF의 온프레미스 접두사는 DXGW와 연결된 AWS 가상 사설 게이트웨이 (VGW) 또는 TGW (Transit Gateway) 인스턴스와 같은 DXGW 게이트웨이 연결에만 광고됩니다.



Full Mesh Connectivity with Private VIF



Full Mesh Connectivity with Transit VIF



사이트링크는 트래픽 흐름을 허용합니다. 예

SiteLink 고객은 AWS 글로벌 네트워크를 사용하여 높은 대역폭과 짧은 지연 시간으로 원격 위치 간의 기본 또는 보조/백업 연결 역할을 할 수 있으며, 동적 라우팅을 통해 서로 통신할 수 있는 위치 및 AWS 지역 리소스와 통신할 수 있는 위치를 제어할 수 있습니다.

[자세한 내용은 소개를 참조하십시오. AWS Direct Connect SiteLink](#)

## 중앙 집중식 인터넷 송신

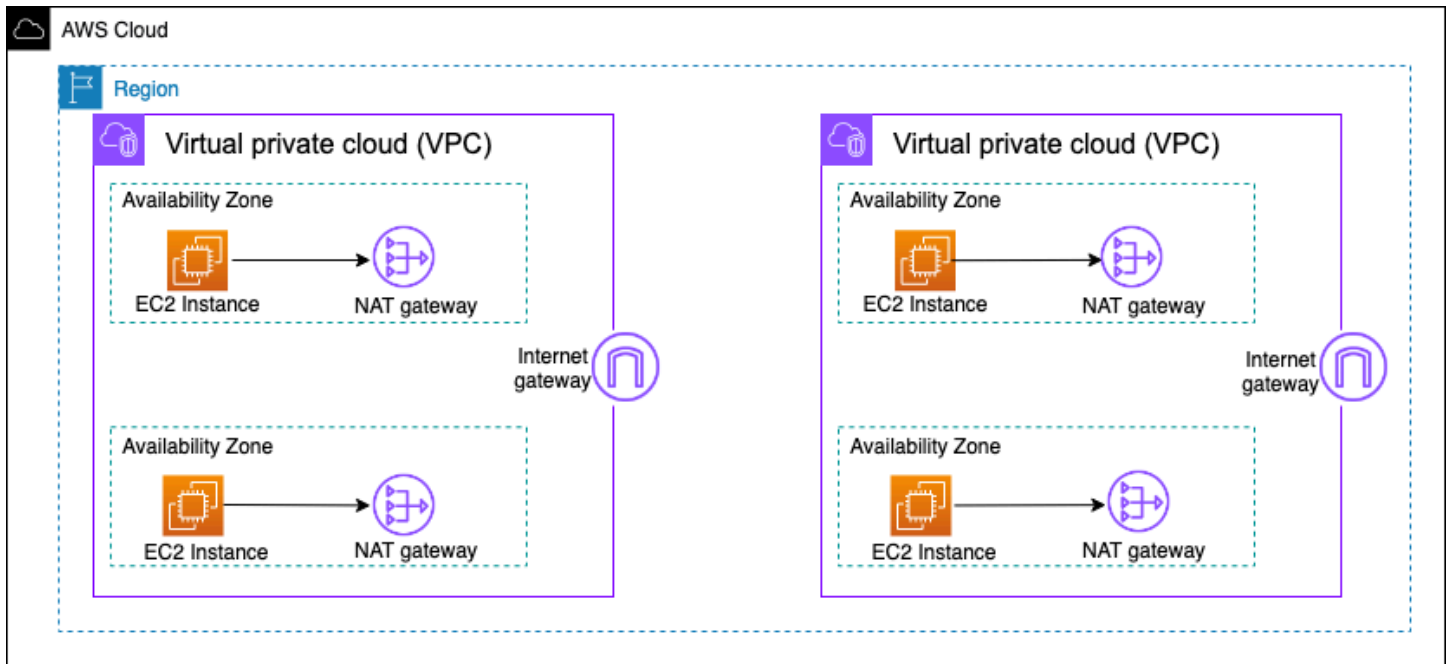
다중 계정 환경에서 애플리케이션을 배포할 때 많은 앱에는 아웃바운드 전용 인터넷 액세스 (예: 라이브러리, 패치 또는 OS 업데이트 다운로드)가 필요합니다. 이는 IPv4 트래픽과 IPv6 트래픽 모두에 적용할 수 있습니다. IPv4의 경우 NAT 게이트웨이 형태의 네트워크 주소 변환 (NAT) (권장)을 통해 이를 달성하거나 Amazon EC2 인스턴스에서 실행되는 자체 관리형 NAT 인스턴스 (모든 송신 인터넷 액세스를 위한 수단으로 사용)를 통해 이를 달성할 수 있습니다. 내부 애플리케이션은 프라이빗 서브넷에 있는 반면, NAT 게이트웨이/Amazon EC2 NAT 인스턴스는 퍼블릭 서브넷에 있습니다. AWS는 NAT 게이트웨이가 더 나은 가용성과 대역폭을 제공하고 관리하는 데 드는 수고도 적기 때문에 NAT 게이트웨이를 사용할 것을 권장합니다. 자세한 내용은 NAT 게이트웨이와 [NAT 인스턴스 비교](#)를 참조하십시오. IPv6 트래픽의 경우 송신 트래픽이 탈중앙화된 방식으로 송신 전용 인터넷 게이트웨이를 통해 각 VPC를 벗어나도록 구성하거나 NAT 인스턴스 또는 프록시 인스턴스를 사용하여 중앙 집중식 VPC로 전송되도록 구성할 수 있습니다. IPv6 패턴은 아래 이 문서의 IPv6 중앙 집중식 송신 섹션에서 설명합니다.

## 중앙 집중식 IPv4 송신을 위한 NAT 게이트웨이 사용

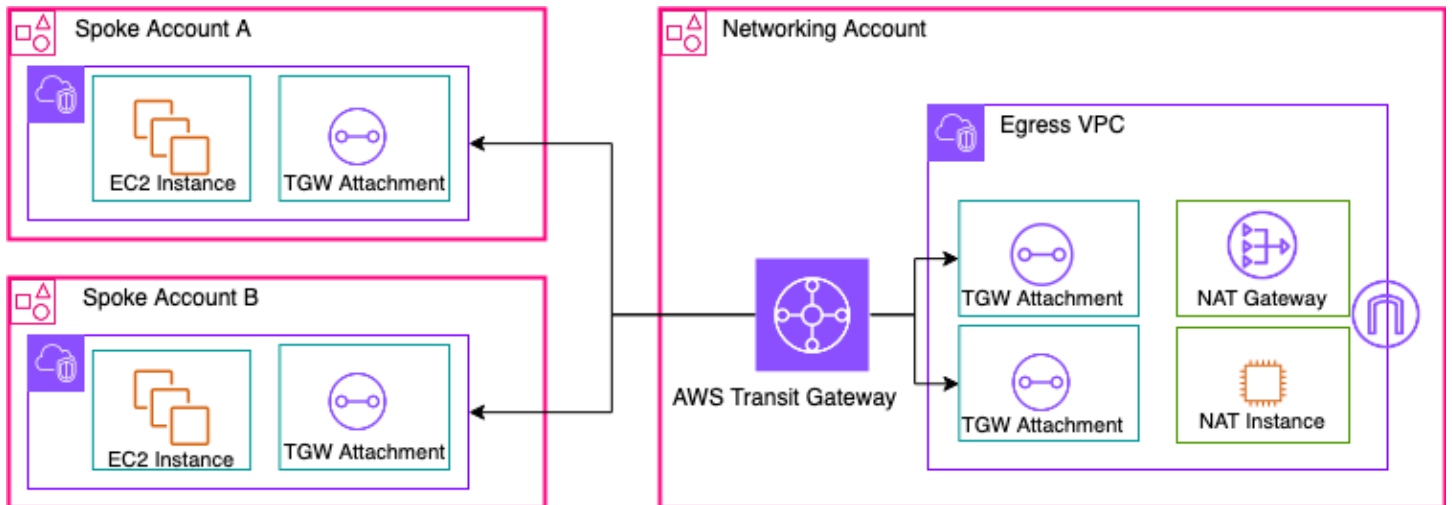
NAT 게이트웨이는 관리형 네트워크 주소 변환 서비스입니다. [모든 스포크 VPC에 NAT 게이트웨이를 배포하는 경우 배포하는 모든 NAT 게이트웨이에 대해 시간당 요금을 지불해야 하므로 비용이 많이 들 수 있습니다 \(Amazon VPC 요금 참조\)](#). NAT 게이트웨이를 중앙 집중화하는 것은 비용 절감을 위한 실행 가능한 옵션이 될 수 있습니다. 중앙 집중화하려면 다음 그림과 같이 네트워크 서비스 계정에서 별도의 이그레스 VPC를 생성하고, 이그레스 VPC에 NAT 게이트웨이를 배포하고, Transit Gateway 또는 CloudWAN을 사용하여 스포크 VPC의 모든 이그레스 트래픽을 이그레스 VPC에 있는 NAT 게이트웨이로 라우팅합니다.

### Note

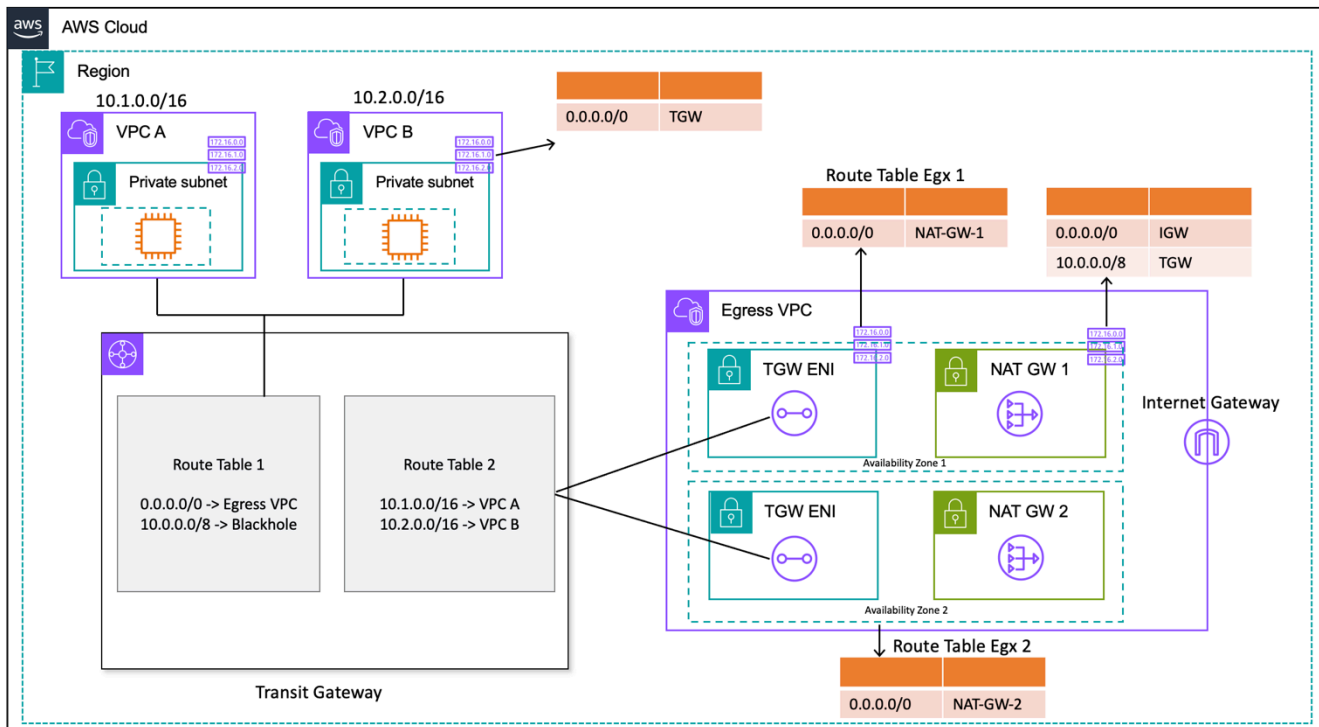
Transit Gateway를 사용하여 NAT 게이트웨이를 중앙 집중화하면 모든 VPC에서 NAT 게이트웨이를 실행하는 분산형 접근 방식에 비해 Transit Gateway 데이터 처리 요금이 추가로 부과됩니다. VPC에서 NAT 게이트웨이를 통해 대량의 데이터를 전송하는 일부 엣지 케이스에서는 Transit Gateway 데이터 처리 요금을 피하기 위해 NAT를 VPC에 로컬로 유지하는 것이 더 비용 효율적인 옵션일 수 있습니다.



### 분산형 고가용성 NAT 게이트웨이 아키텍처



### Transit Gateway를 사용하는 중앙 집중식 NAT 게이트웨이 (개요)



## Transit Gateway를 사용하는 중앙 집중식 NAT 게이트웨이 (라우팅 테이블 설계)

이 설정에서 스포크 VPC 어태치먼트는 라우팅 테이블 1 (RT1) 과 연결되고 라우팅 테이블 2 (RT2) 로 전파됩니다. 두 VPC가 서로 통신하지 못하도록 하는 **블랙홀** 경로가 있습니다. VPC 간 통신을 허용하려면 RT1에서 10.0.0.0/8 -> Blackhole 경로 항목을 제거할 수 있습니다. 이렇게 하면 트랜지트 게이트웨이를 통해 통신할 수 있습니다. 또한 스포크 VPC 연결을 RT1에 전파하여 (또는 하나의 라우팅 테이블을 사용하고 모든 것을 여기에 연결/전파할 수 있음) Transit Gateway를 사용하여 VPC 간에 직접 트래픽 흐름을 가능하게 할 수 있습니다.

모든 트래픽이 이그레스 VPC를 가리키는 고정 경로를 RT1에 추가합니다. 이러한 고정 경로 때문에 Transit Gateway는 이그레스 VPC의 ENI를 통해 모든 인터넷 트래픽을 전송합니다. 이그레스 VPC에 들어가면 트래픽은 이러한 Transit Gateway ENI가 있는 서브넷 라우팅 테이블에 정의된 경로를 따릅니다. 모든 트래픽이 동일한 가용 영역의 해당 NAT 게이트웨이를 가리키는 경로를 서브넷 라우팅 테이블에 추가하여 교차 가용 영역 (AZ) 트래픽을 최소화합니다. NAT 게이트웨이 서브넷 라우팅 테이블에는 인터넷 게이트웨이 (IGW) 가 다음 홉으로 사용됩니다. 반환 트래픽이 다시 흐르도록 하려면 NAT 게이트웨이 서브넷 라우팅 테이블에 모든 스포크 VPC 바운드 트래픽을 Transit Gateway를 다음 홉으로 가리키는 고정 라우팅 테이블 항목을 추가해야 합니다.

## 높은 가용성

고가용성을 위해서는 NAT 게이트웨이를 두 개 이상 (가용 영역당 하나씩) 사용해야 합니다. NAT 게이트웨이를 사용할 수 없는 경우 영향을 받는 NAT 게이트웨이를 통과하는 해당 가용 영역에서 트래픽이

삭제될 수 있습니다. 하나의 가용 영역을 사용할 수 없는 경우 해당 가용 영역의 NAT 게이트웨이와 함께 Transit Gateway 엔드포인트에 장애가 발생하고 모든 트래픽이 다른 가용 영역의 Transit Gateway 및 NAT 게이트웨이 엔드포인트를 통해 흐릅니다.

## 보안

원본 인스턴스의 보안 그룹, Transit Gateway 라우팅 테이블의 블랙홀 경로, NAT 게이트웨이가 위치한 서브넷의 네트워크 ACL을 신뢰할 수 있습니다. 예를 들어 고객은 NAT 게이트웨이 퍼블릭 서브넷의 ACL을 사용하여 원본 또는 대상 IP 주소를 허용하거나 차단할 수 있습니다. 또는 이 요구 사항을 충족하기 위해 다음 섹션에서 설명하는 중앙 집중식 AWS Network Firewall 송신을 위해 NAT Gateway와 함께 사용할 수 있습니다.

## 확장성

단일 NAT 게이트웨이는 각 고유 대상에 할당된 IP 주소당 최대 55,000개의 동시 연결을 지원할 수 있습니다. 할당량 조정을 요청하여 최대 8개의 할당된 IP 주소를 허용하여 단일 대상 IP 및 포트에 440,000개의 동시 연결을 허용할 수 있습니다. NAT 게이트웨이는 5Gbps의 대역폭을 제공하며 자동으로 100Gbps로 확장됩니다. Transit Gateway는 일반적으로 로드 밸런서 역할을 하지 않으며 여러 가용 영역의 NAT 게이트웨이에 트래픽을 균등하게 분배하지 않습니다. Transit Gateway를 통한 트래픽은 가능한 경우 가용 영역 내에 유지됩니다. 트래픽을 시작하는 Amazon EC2 인스턴스가 가용 영역 1에 있는 경우, 트래픽은 송신 VPC의 동일한 가용 영역 1에 있는 Transit Gateway Elastic network 인터페이스를 빠져나가 Elastic Network 인터페이스가 있는 서브넷 라우팅 테이블을 기반으로 다음 홉으로 이동합니다. 전체 규칙 목록은 Amazon Virtual Private Cloud 설명서에서 [NAT 게이트웨이를](#) 참조하십시오.

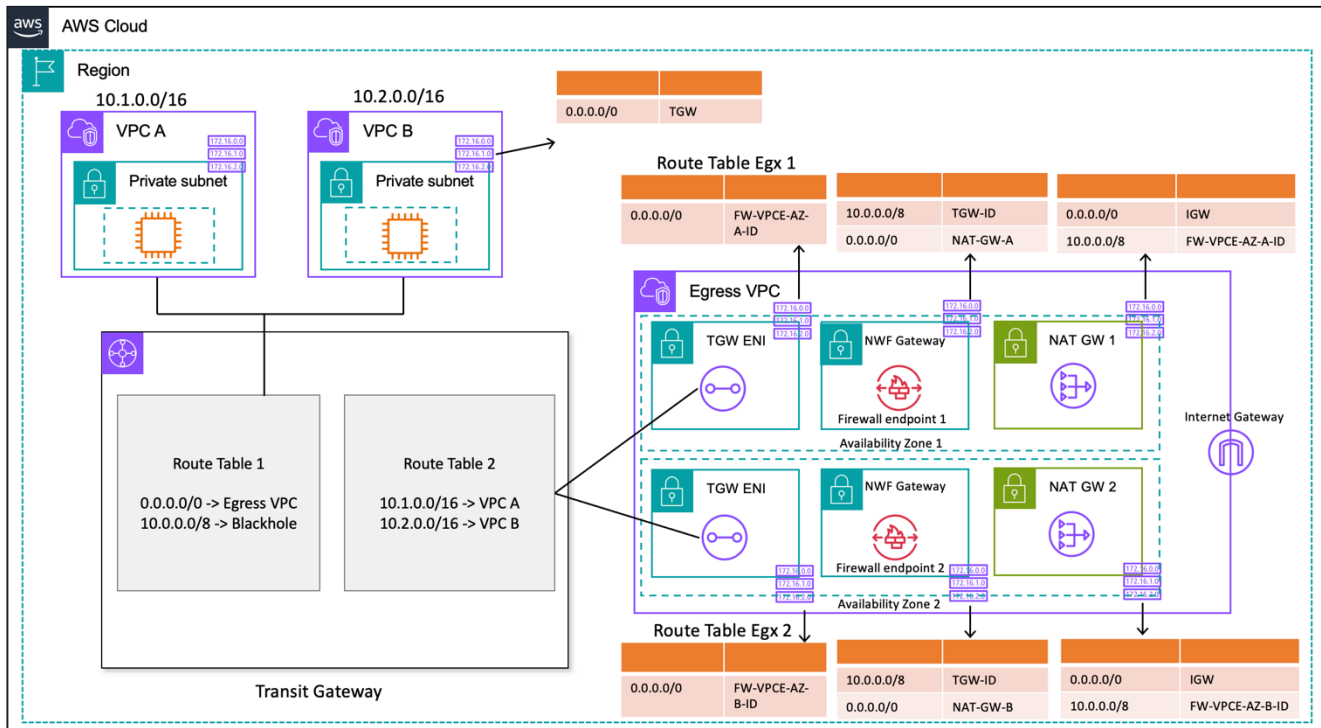
자세한 내용은 [AWS Transit Gateway를 사용하여 여러 VPC에서 단일 인터넷 출구 만들기](#) 블로그 게시물을 참조하십시오.

## 중앙 집중식 IPv4 송신을 AWS Network Firewall 위한 NAT 게이트웨이가 사용

아웃바운드 트래픽을 검사하고 필터링하려면 AWS Network Firewall을 중앙 집중식 송신 아키텍처에 NAT 게이트웨이와 통합할 수 있습니다. AWS Network Firewall 모든 VPC에 필수적인 네트워크 보호를 쉽게 배포할 수 있게 해주는 관리형 서비스입니다. 전체 VPC의 계층 3-7 네트워크 트래픽에 대한 제어 및 가시성을 제공합니다. URL/도메인 이름, IP 주소, 콘텐츠 기반 아웃바운드 트래픽 필터링을 통해 가능한 데이터 손실을 막고, 규정 준수 요구 사항을 충족하고, 알려진 멀웨어 통신을 차단할 수 있습니다. AWS Network Firewall 알려진 불량 IP 주소 또는 잘못된 도메인 이름으로 향하는 네트워크 트래

픽을 필터링할 수 있는 수천 개의 규칙을 지원합니다. 오픈 소스 규칙 세트를 가져오거나 Suricata 규칙 구문을 사용하여 자체 IPS (침입 방지 시스템) 규칙을 작성하여 Suricata IPS 규칙을 AWS Network Firewall 서비스의 일부로 사용할 수도 있습니다. AWS Network Firewall 또한 AWS 파트너가 제공하는 호환 가능한 규칙을 가져올 수 있습니다.

검사가 포함된 중앙 집중식 이그레스 아키텍처에서 AWS Network Firewall 엔드포인트는 이그레스 VPC의 트랜짓 게이트웨이 첨부 파일 서브넷 라우팅 테이블의 기본 라우팅 테이블 대상입니다. 스포크 VPC와 인터넷 간의 트래픽은 다음 다이어그램에 표시된 AWS Network Firewall 대로 검사됩니다.



### NAT 게이트웨이를 통한 AWS Network Firewall 중앙 집중식 이그레스 (라우팅 테이블 디자인)

Transit Gateway를 사용한 중앙 집중식 배포 모델의 경우 AWS는 여러 가용 AWS Network Firewall 영역에 엔드포인트를 배포할 것을 권장합니다. 위 다이어그램에서 볼 수 있듯이 고객이 워크로드를 실행하는 각 가용 영역에는 방화벽 엔드포인트가 하나씩 있어야 합니다. 방화벽 AWS Network Firewall 서브넷은 방화벽 서브넷 내의 소스 또는 대상으로부터 오는 트래픽을 검사할 수 없으므로 방화벽 서브넷에는 다른 트래픽이 포함되지 않는 것이 좋습니다.

이전 설정과 마찬가지로 스포크 VPC 연결은 라우팅 테이블 1 (RT1) 과 연결되고 라우팅 테이블 2 (RT2) 로 전파됩니다. 두 VPC가 서로 통신할 수 없도록 블랙홀 경로가 명시적으로 추가되었습니다.

모든 트래픽이 이그레스 VPC를 가리키는 RT1의 기본 경로를 계속 사용하십시오. Transit Gateway는 모든 트래픽 흐름을 이그레스 VPC의 두 가용 영역 중 하나로 전달합니다. 트래픽이 이그레스 VPC의 Transit Gateway eNI 중 하나에 도달하면 해당 가용 영역의 AWS Network Firewall 엔드포인트 중 하나

로 트래픽을 전달하는 기본 경로에 도달하게 됩니다. AWS Network Firewall 그러면 기본 경로를 사용하여 NAT 게이트웨이로 트래픽을 전달하기 전에 설정한 규칙에 따라 트래픽을 검사합니다.

이 경우에는 첨부 파일 간에 트래픽을 전송하지 않으므로 Transit Gateway 어플라이언스 모드가 필요하지 않습니다.

### Note

AWS Network Firewall 네트워크 주소 변환을 대신 수행하지 않습니다. 이 기능은 NAT 게이트웨이를 통해 트래픽을 검사한 후 NAT 게이트웨이에서 처리합니다. AWS Network Firewall이 경우에는 반환 트래픽이 기본적으로 NATGW IP로 전달되므로 인그레스 라우팅이 필요하지 않습니다.

Transit Gateway를 사용하고 있기 때문에 여기서는 NAT 게이트웨이보다 먼저 방화벽을 배치할 수 있습니다. 이 모델에서 방화벽은 Transit Gateway 뒤에 있는 소스 IP를 볼 수 있습니다.

단일 VPC에서 이 작업을 수행했다면 동일한 VPC에 있는 서브넷 간 트래픽을 검사할 수 있는 향상된 VPC 라우팅 기능을 사용할 수 있습니다. 자세한 [내용은 VPC 라우팅 개선 기능이 AWS Network Firewall 포함된 배포 모델](#) 블로그 게시물을 참조하십시오.

## 확장성

AWS Network Firewall 트래픽 부하에 따라 방화벽 용량을 자동으로 늘리거나 줄일 수 있으므로 안정적이고 예측 가능한 성능을 유지하여 비용을 최소화할 수 있습니다. AWS Network Firewall 수만 개의 방화벽 규칙을 지원하도록 설계되었으며 가용 영역당 처리량을 최대 100Gbps까지 확장할 수 있습니다.

## 주요 고려 사항

- [각 방화벽 엔드포인트는 약 100Gbps의 트래픽을 처리할 수 있습니다. 더 높은 버스트 또는 지속적인 처리량이 필요한 경우 AWS Support에 문의하십시오.](#)
- [Network Firewall과 함께 AWS 계정에 NAT 게이트웨이를 생성하기로 선택한 경우, 방화벽에 청구되는 GB당 처리 및 사용 시간을 one-to-one 기준으로 표준 NAT 게이트웨이 처리 및 시간당 사용 요금이 면제됩니다.](#)
- Transit Gateway AWS Firewall Manager 없이 분산 방화벽 엔드포인트를 사용하는 것도 고려해 볼 수 있습니다.
- 순서가 중요하므로 네트워크 액세스 제어 목록과 마찬가지로 프로덕션 환경으로 이동하기 전에 방화벽 규칙을 테스트하십시오.

- 심층 검사를 위해서는 고급 수리카타 규칙이 필요합니다. 네트워크 방화벽은 유입 및 송신 트래픽에 대한 암호화된 트래픽 검사를 지원합니다.
- HOME\_NET 규칙 그룹 변수는 Stateful 엔진에서 처리할 수 있는 소스 IP 범위를 정의했습니다. 중앙 집중식 접근 방식을 사용하는 경우 Transit Gateway에 연결된 모든 추가 VPC CIDR을 추가하여 처리할 수 있도록 해야 합니다. HOME\_NET 규칙 그룹 변수에 대한 자세한 내용은 [Network Firewall 설명서를](#) 참조하십시오.
- 직무 위임에 따라 액세스를 분리하려면 Transit Gateway와 이그레스 VPC를 별도의 네트워크 서비스 계정에 배포하는 것을 고려해 보십시오. 예를 들어 네트워크 관리자만 네트워크 서비스 계정에 액세스할 수 있습니다.
- 이 모델의 배포 및 관리를 단순화하기 위해 사용할 AWS Network Firewall 수 있습니다. AWS Firewall Manager Firewall Manager를 사용하면 중앙 위치에서 생성한 보호 기능을 여러 계정에 자동으로 적용하여 다양한 방화벽을 중앙에서 관리할 수 있습니다. Firewall Manager는 네트워크 방화벽에 대한 분산 및 중앙 집중식 배포 모델을 모두 지원합니다. 자세한 내용은 블로그 게시물을 [사용하여 AWS Network Firewall 배포하는 방법을](#) 참조하십시오 AWS Firewall Manager.

## 중앙 집중식 IPv4 송신을 위해 Amazon EC2 인스턴스와 함께 NAT 게이트웨이 및 게이트웨이 로드 밸런서 사용

종료 지점으로 소프트웨어 기반 가상 어플라이언스 (Amazon EC2) 를 사용하는 것은 AWS Partner Network NAT 게이트웨이 AWS Marketplace 설정과 비슷합니다. 이 옵션은 다양한 공급업체 제품의 고급 계층 7 방화벽/침입 방지/탐지 시스템 (IPS/IDS) 및 심층 패킷 검사 기능을 사용하려는 경우 사용할 수 있습니다.

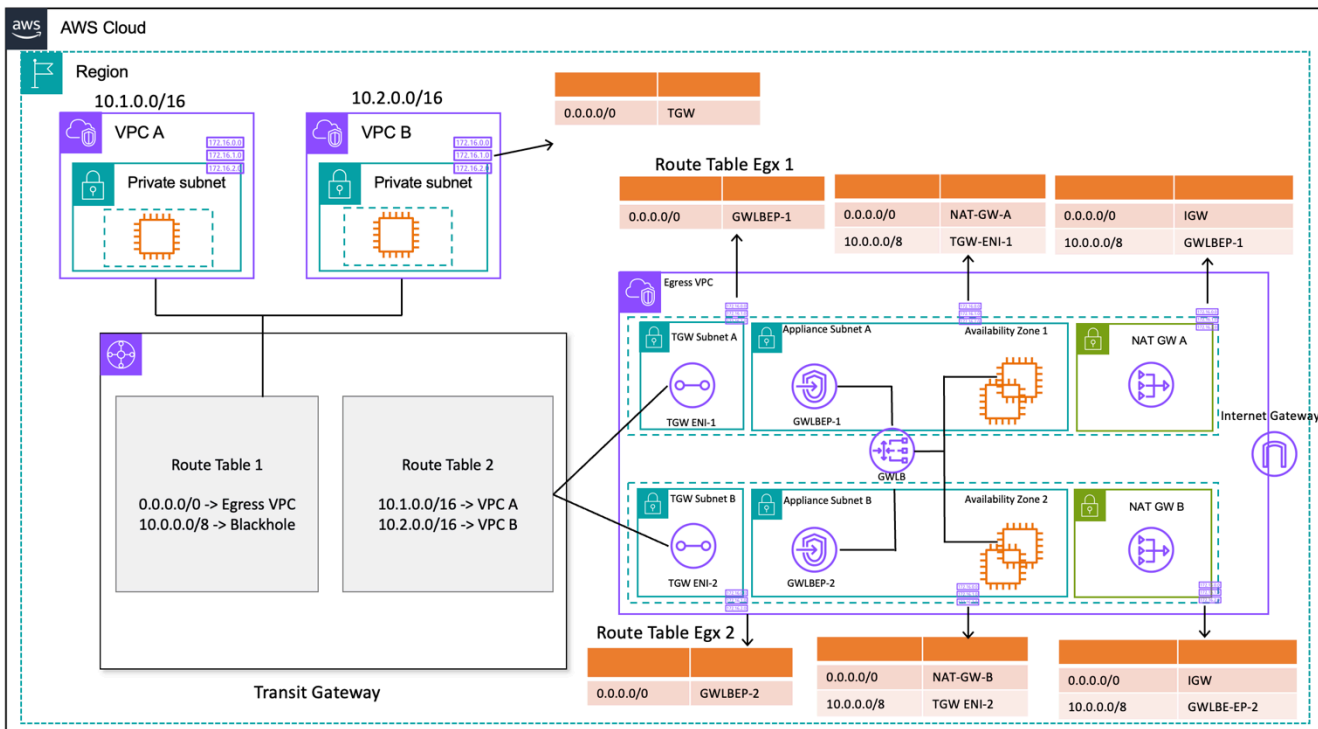
다음 그림에서는 NAT 게이트웨이 외에도 GWLB (Gateway Load Balancer) 위의 EC2 인스턴스를 사용하여 가상 어플라이언스를 배포합니다. 이 설정에서는 GWLB, 게이트웨이 로드 밸런서 엔드포인트 (GWLBE), 가상 어플라이언스 및 NAT 게이트웨이가 VPC 연결을 사용하여 Transit Gateway에 연결되는 중앙 집중식 VPC에 배포됩니다. 또한 스포크 VPC는 VPC 연결을 사용하여 Transit Gateway에 연결됩니다. GWLBE는 라우팅 가능한 대상이므로 Transit Gateway에서 오가는 트래픽을 GWLB 위의 대상으로 구성된 가상 어플릿으로 라우팅할 수 있습니다. GWLB는 a 역할을 bump-in-the-wire 하며 모든 레이어 3 트래픽을 타사 가상 어플라이언스를 통해 투명하게 전달하므로 트래픽의 소스와 목적지는 보이지 않습니다. 따라서 이 아키텍처를 사용하면 Transit Gateway를 통과하는 모든 송신 트래픽을 중앙에서 검사할 수 있습니다.

트래픽이 VPC의 애플리케이션에서 인터넷으로 이동하고 이 설정을 통해 다시 돌아오는 방식에 대한 자세한 내용은 [AWS Gateway Load Balancer AWS Transit Gateway 및 를 사용한 중앙 집중식 검사 아키텍처](#)를 참조하십시오.



Transit Gateway에서 어플라이언스 모드를 활성화하여 가상 어플라이언스를 통한 흐름 대칭을 유지할 수 있습니다. 즉, 양방향 트래픽은 흐름의 수명 기간 동안 동일한 어플라이언스와 가용 영역을 통해 라우팅됩니다. 이 설정은 심층 패킷 검사를 수행하는 스테이트풀 방화벽에 특히 중요합니다. 어플라이언스 모드를 활성화하면 대칭을 유지하기 위해 트래픽이 올바른 어플라이언스로 강제로 돌아오도록 SNAT (소스 네트워크 주소 변환)와 같은 복잡한 해결 방법을 사용할 필요가 없습니다. 자세한 내용은 [내용은 게이트웨이 Load Balancer 배포 모범 사례를](#) 참조하십시오.

또한 송신 검사를 지원하는 Transit Gateway 없이 GWLB 엔드포인트를 분산 방식으로 배포할 수 있습니다. [AWS Gateway Load Balancer 소개: 지원되는 아키텍처 패턴 블로그 게시물에서 이 아키텍처 패턴에](#) 대해 자세히 알아보십시오.



게이트웨이 로드 밸런서 및 EC2 인스턴스를 사용한 중앙 집중식 송신 (라우팅 테이블 설계)

## 높은 가용성

AWS는 가용성을 높이기 위해 여러 가용 영역에 게이트웨이 로드 밸런서와 가상 어플라이언스를 배포할 것을 권장합니다.

Gateway Load Balancer는 상태 점검을 수행하여 가상 어플라이언스 장애를 탐지할 수 있습니다. 어플라이언스가 비정상인 경우 GWLB는 새 플로우를 정상 어플라이언스로 다시 라우팅합니다. 기존 흐름은 대상의 상태에 관계없이 항상 동일한 대상으로 이동합니다. 이렇게 하면 연결 드레이닝이 가능하고 어플라이언스의 CPU 스파이크로 인한 상태 점검 실패를 수용할 수 있습니다. 자세한 내용은 블로그 [게이트웨이 로드 밸런서 및 EC2 인스턴스를 사용한 중앙 집중식 송신 \(라우팅 테이블 설계\)](#)를 참조하십시오.

시물의 [Gateway Load Balancer 배포 모범 사례의 섹션 4: 어플라이언스 및 가용 영역 장애 시나리오](#) 이해를 참조하십시오. 게이트웨이 로드 밸런서는 자동 스케일링 그룹을 대상으로 사용할 수 있습니다. 이 이점을 통해 어플라이언스 플릿의 가용성 및 확장성을 관리하는 번거로움을 덜 수 있습니다.

## 장점

Gateway Load Balancer 및 Gateway Load Balancer 엔드포인트에 AWS PrivateLink의해 구동되므로 공용 인터넷을 통과할 필요 없이 VPC 경계를 넘어 안전하게 트래픽을 교환할 수 있습니다.

Gateway Load Balancer는 가상 보안 어플라이언스를 관리, 배포, 확장하는 차별화되지 않은 부담을 없애주어 중요한 일에 집중할 수 있도록 하는 관리형 서비스입니다. Gateway Load Balancer는 방화벽 스택을 엔드포인트 서비스로 노출하여 고객이 방화벽을 사용하여 구독하도록 할 수 있습니다. [AWS Marketplace](#) 이를 서비스형 방화벽 (FWaaS) 이라고 하며, 배포가 간소화되고 BGP 및 ECMP를 사용하여 여러 Amazon EC2 인스턴스에 트래픽을 분산할 필요가 없습니다.

## 주요 고려 사항

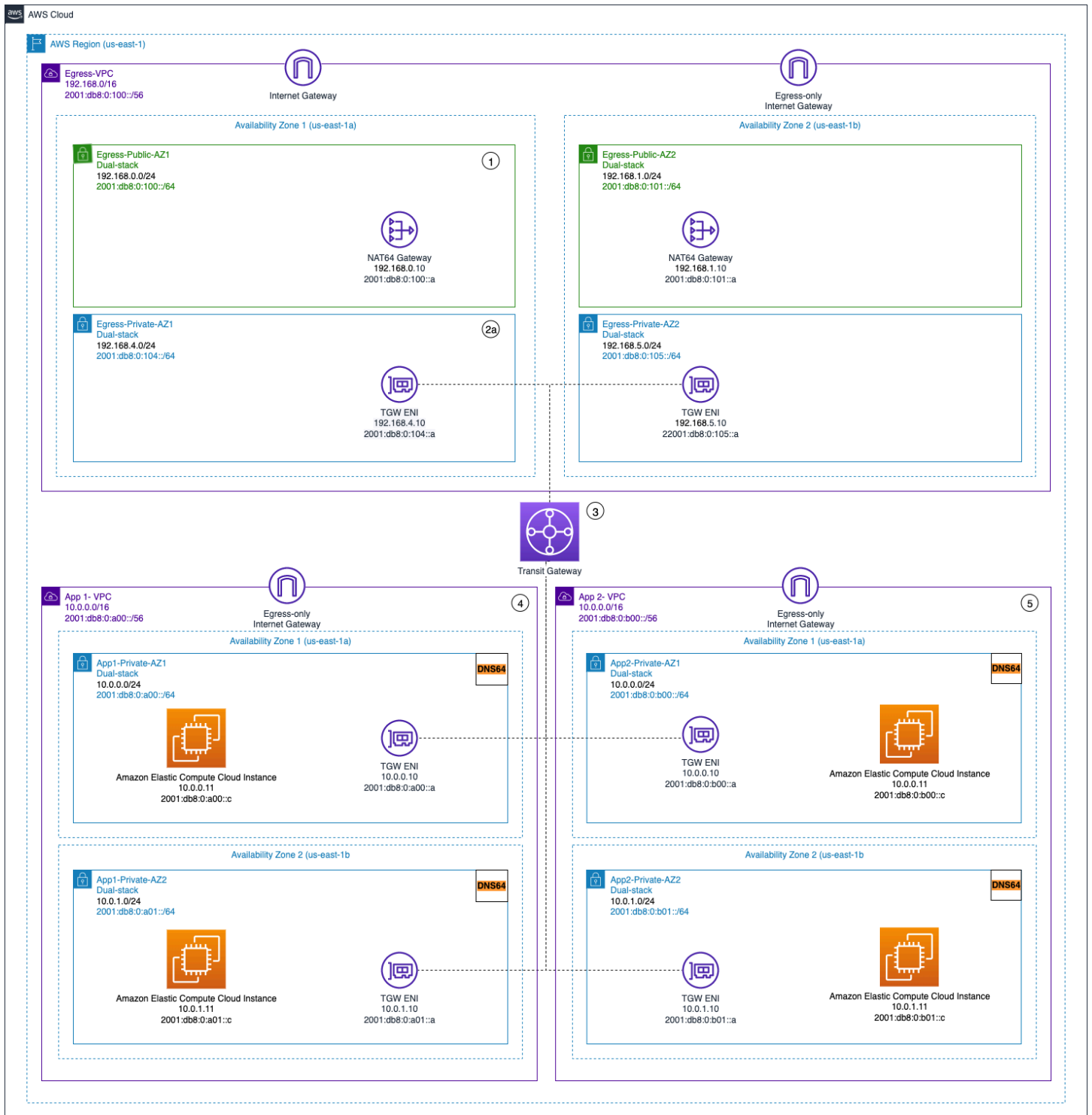
- 어플라이언스가 GWLB와 통합하려면 [제네바 캡슐화 프로토콜](#)을 지원해야 합니다.
- 일부 타사 어플라이언스는 SNAT 및 오버레이 라우팅 ([2-arm 모드](#)) 을 지원할 수 있으므로 비용 절감을 위해 NAT 게이트웨이를 만들 필요가 없습니다. 하지만 벤더 지원 및 구현에 따라 다르므로 이 모드를 사용하기 전에 원하는 AWS 파트너와 상의하십시오.
- [GWLB 유휴 타임아웃](#)을 기록해 두십시오. 이로 인해 클라이언트의 연결 제한 시간이 초과될 수 있습니다. 클라이언트, 서버, 방화벽 및 OS 수준에서 타임아웃을 조정하여 이를 방지할 수 있습니다. 자세한 내용은 [Gateway Load Balancer 배포 모범 사례 블로그 게시물에서 수명이 긴 TCP 흐름을 지원하기 위한](#) 섹션 1: TCP 연결 유지 또는 제한 시간 값 조정을 참조하십시오.
- GWLBE는 전원이 공급되므로 요금이 부과됩니다. AWS PrivateLink [AWS PrivateLink 가격](#) 페이지에서 자세히 알아볼 수 있습니다. Transit Gateway와 함께 중앙 집중식 모델을 사용하는 경우 TGW 데이터 처리 요금이 적용됩니다.
- 업무 위임 (예: 네트워크 관리자만 네트워크 서비스 계정에 액세스할 수 있음) 에 따라 액세스를 분리하려면 Transit Gateway와 이그레스 VPC를 별도의 네트워크 서비스 계정에 배포하는 것을 고려해 보십시오.

## IPv6용 중앙 집중식 이그레스

중앙 집중식 IPv4 송신을 사용하는 이중 스택 배포에서 IPv6 송신을 지원하려면 다음 두 패턴 중 하나를 선택해야 합니다.

- 중앙 집중식 IPv4 송신 및 분산형 IPv6 송신
- 중앙 집중식 IPv4 송신 및 중앙 집중식 IPv6 송신

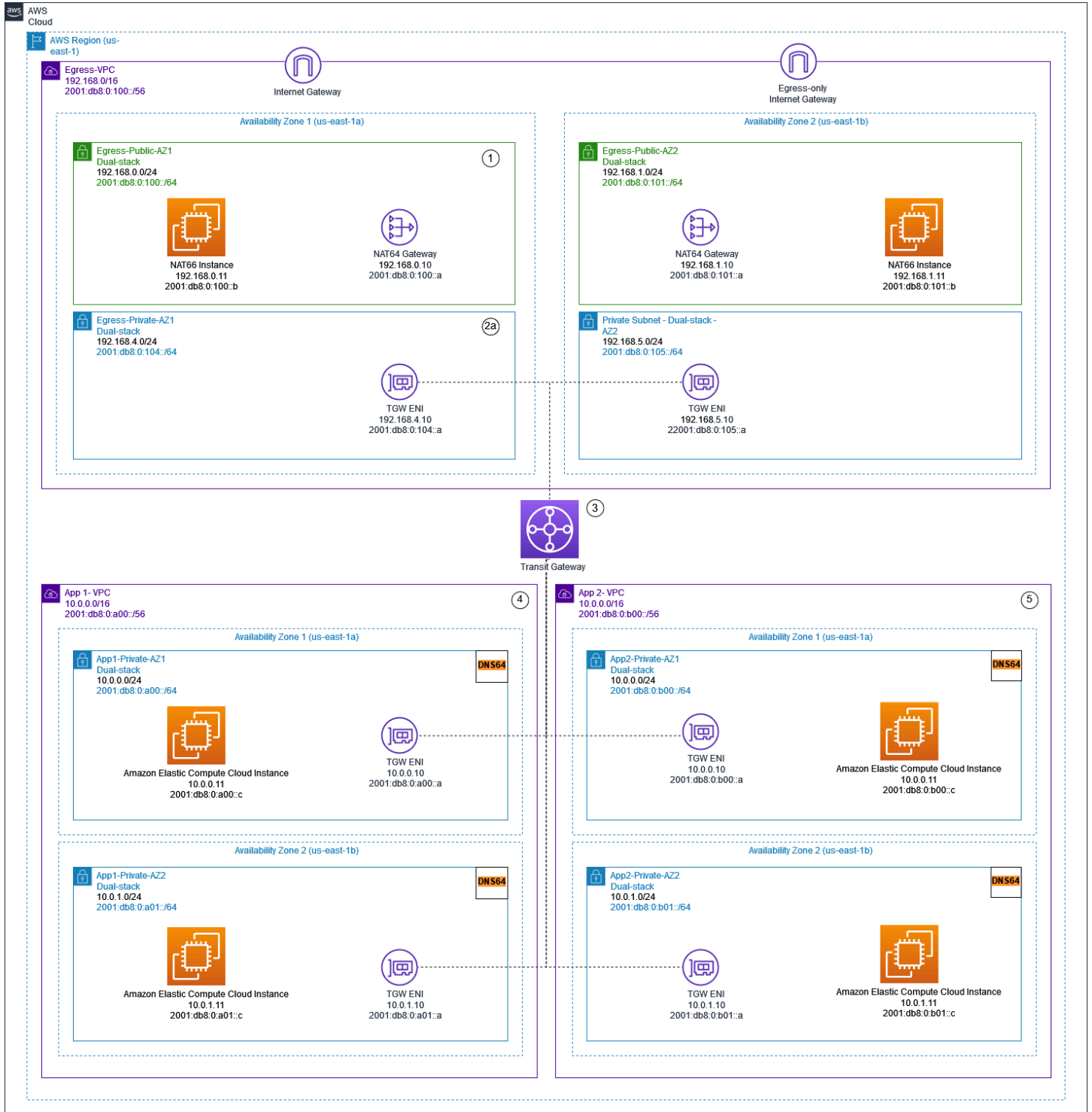
다음 다이어그램에 표시된 첫 번째 패턴에서는 외부 전용 인터넷 게이트웨이가 각 스포크 VPC에 배포됩니다. 외부 전용 인터넷 게이트웨이는 수평적으로 확장되고 이중화된고가용성 게이트웨이로, VPC 내부 인스턴스로부터 IPv6를 통한 아웃바운드 통신을 허용합니다. 인터넷이 인스턴스와의 IPv6 연결을 시작하지 못하게 합니다. 외부 전용 인터넷 게이트웨이는 요금이 부과되지 않습니다. 이 배포 모델에서는 IPv6 트래픽이 각 VPC의 외부 전용 인터넷 게이트웨이에서 나오고 IPv4 트래픽은 배포된 중앙 집중식 NAT 게이트웨이를 통해 흐릅니다.



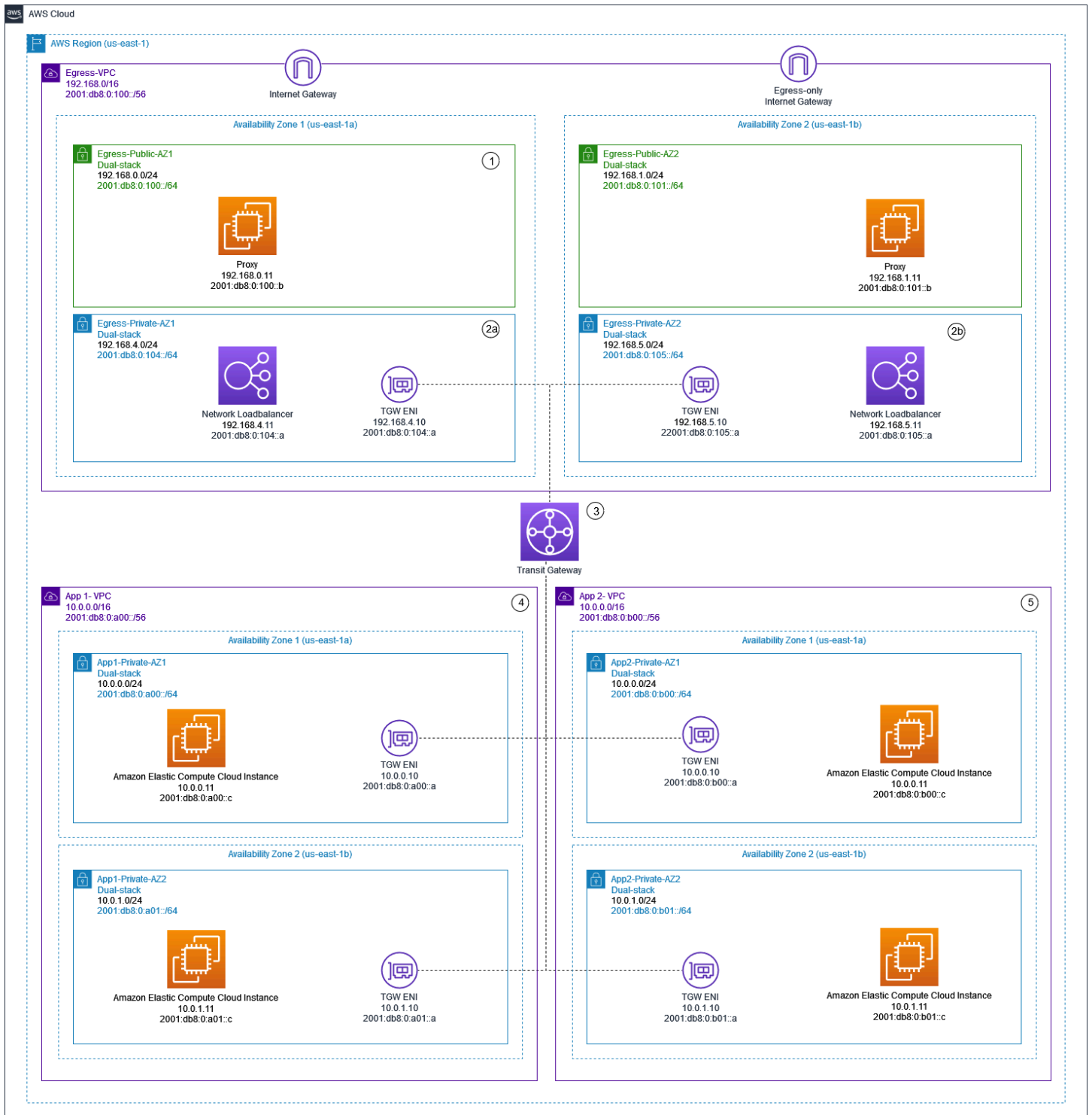
### 중앙 집중식 IPv4 송신 및 분산형 아웃바운드 전용 IPv6 송신

다음 다이어그램에 표시된 두 번째 패턴에서는 인스턴스의 송신 IPv6 트래픽이 중앙 집중식 VPC로 전송됩니다. 이는 NAT66 인스턴스 및 NAT 게이트웨이와 함께 IPv6에서 IPv6으로의 네트워크 접두사 변환 (NPTv6) 을 사용하거나 프록시 인스턴스 및 Network Load Balancer를 사용하여 수행할 수 있습니

다. 이 패턴은 아웃바운드 트래픽에 대한 중앙 집중식 트래픽 검사가 필요하고 각 스포크 VPC에서 수행할 수 없는 경우에 적용할 수 있습니다.



NAT 게이트웨이와 NAT66 인스턴스를 사용하는 중앙 집중식 IPv6 송신



프록시 인스턴스와 Network Load Balancer를 사용하는 중앙 집중식 IPv4 및 IPv6 송신

[AWS 기반 IPv6 백서](#)는 중앙 집중식 IPv6 송신 패턴을 설명합니다. IPv6 송신 패턴은 특수 고려 사항, 샘플 솔루션 및 다이어그램과 함께 [이중 스택 IPv4 및 IPv6 VPC의 중앙 집중식 아웃바운드 인터넷 트래픽 블로그](#)에 자세히 설명되어 있습니다.

# VPC-VPC 간 및 온프레미스-VPC 트래픽에 대한 중앙 집중식 네트워크 보안

고객이 다중 계정 환경 내에 계층 3-7 방화벽/IPS/ID를 구현하여 VPC 간 (동서 트래픽) 또는 온프레미스 데이터 센터와 VPC (남북 트래픽) 간의 트래픽 흐름을 검사하려는 시나리오가 있을 수 있습니다. 이는 사용 사례 및 요구 사항에 따라 다양한 방법으로 달성할 수 있습니다. 예를 들어 게이트웨이 Load Balancer, Network Firewall, Transit VPC를 통합하거나 트랜짓 게이트웨이와 함께 중앙 집중식 아키텍처를 사용할 수 있습니다. 이러한 시나리오는 다음 섹션에서 설명합니다.

## 중앙 집중식 네트워크 보안 검사 모델 사용 고려 사항

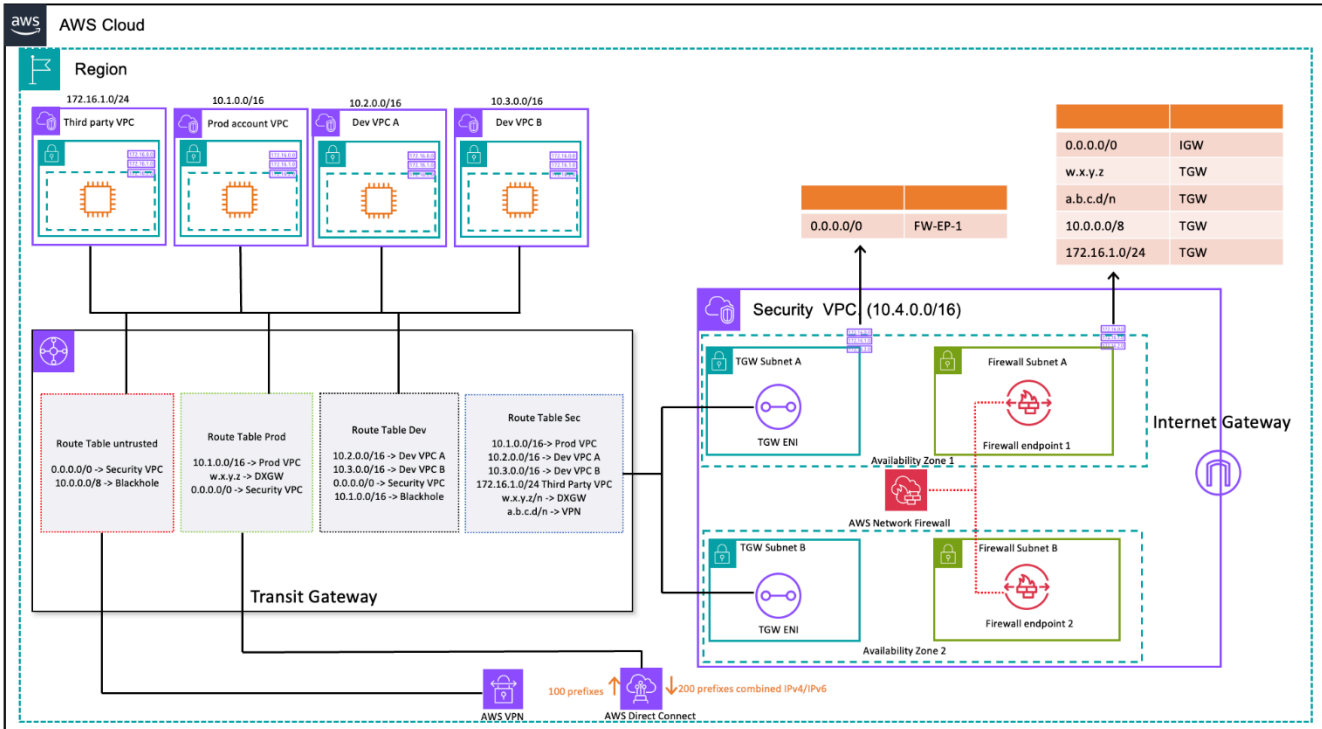
비용을 줄이려면 사용자 AWS Network Firewall 또는 게이트웨이 Load Balancer를 통해 전달되는 트래픽을 선별해야 합니다. 한 가지 해결 방법은 보안 영역을 정의하고 신뢰할 수 없는 영역 간의 트래픽을 검사하는 것입니다. 신뢰할 수 없는 영역은 타사에서 관리하는 원격 사이트, 제어/신뢰할 수 없는 공급업체 VPC 또는 다른 환경에 비해 보안 규칙이 더 완화된 샌드박스/개발 VPC일 수 있습니다. 이 예시에는 네 개의 영역이 있습니다.

- 신뢰할 수 없는 영역 — '신뢰할 수 없는 원격 사이트로 연결되는 VPN' 또는 타사 공급업체 VPC로 들어오는 모든 트래픽을 위한 것입니다.
- 프로덕션 (Prod) 영역 — 여기에는 프로덕션 VPC와 온프레미스 고객 DC의 트래픽이 포함됩니다.
- 개발 (개발) 영역 - 여기에는 두 개발 VPC의 트래픽이 포함됩니다.
- 보안 (Sec) 영역 - 방화벽 구성 요소인 Network Firewall 또는 게이트웨이 Load Balancer를 포함합니다.

이 설정에는 네 개의 보안 영역이 있지만 보안 영역이 더 있을 수도 있습니다. 여러 라우팅 테이블과 블랙홀 경로를 사용하여 보안을 격리하고 트래픽 흐름을 최적화할 수 있습니다. 적절한 영역 집합을 선택하는 것은 전반적인 랜딩 존 설계 전략 (계정 구조, VPC 설계) 에 따라 달라집니다. 영역을 만들어 사업부 (BU), 애플리케이션, 환경 등을 분리할 수 있습니다.

VPC-VPC, 영역 간 트래픽 및 VPC-온프레미스 트래픽을 검사하고 필터링하려는 경우 중앙 집중식 아키텍처에 Transit Gateway를 통합할 수 있습니다. AWS Network Firewall 의 hub-and-spoke 모델을 사용하면 중앙 집중식 배포 모델을 구현할 수 있습니다. AWS Transit Gateway AWS Network Firewall 는 별도의 보안 VPC에 배포됩니다. 별도의 보안 VPC는 검사를 관리하기 위한 단순하고 중앙화된 접근 방식을 제공합니다. 이러한 VPC 아키텍처는 AWS Network Firewall 소스 및 대상 IP 가시성을 제공합니

다. 소스 IP와 대상 IP가 모두 보존됩니다. 이 보안 VPC는 각 가용 영역에 있는 두 개의 서브넷으로 구성되어 있습니다. 즉, 한 서브넷은 AWS Transit Gateway 연결 전용이고 다른 서브넷은 방화벽 엔드포인트 전용입니다. Network Firewall은 엔드포인트와 동일한 서브넷의 트래픽을 검사할 수 없으므로 이 VPC의 서브넷에는 엔드포인트만 AWS Network Firewall 포함되어야 합니다. Network Firewall을 사용하여 중앙에서 트래픽을 검사하면 인그레스 트래픽에 대해 딥 패킷 검사 (DPI) 를 수행할 수 있습니다. DPI 패턴은 이 백서의 중앙 인바운드 검사 섹션에서 자세히 설명합니다.



### Transit Gateway를 사용한 VPC 간 및 온프레미스에서 VPC로의 트래픽 검사 및 (라우팅 테이블 설계) AWS Network Firewall

검사가 포함된 중앙 집중식 아키텍처에서 Transit Gateway 서브넷에는 트래픽이 동일한 가용 영역 내의 방화벽 엔드포인트로 전달되도록 하기 위해 별도의 VPC 라우팅 테이블이 필요합니다. 반환 트래픽의 경우 Transit Gateway로 향하는 기본 경로를 포함하는 단일 VPC 라우팅 테이블이 구성됩니다. AWS Transit Gateway 에서 트래픽을 검사한 후 동일한 가용 영역에 있는 트래픽으로 반환됩니다. AWS Network Firewall이는 Transit Gateway의 어플라이언스 모드 기능 때문에 가능합니다. Transit Gateway의 어플라이언스 모드 기능은 보안 AWS Network Firewall VPC 내에서 상태 저장 트래픽 검사 기능을 갖추는 데도 도움이 됩니다.

트랜지트 게이트웨이에 어플라이언스 모드를 활성화하면 전체 연결 수명 동안 플로우 해시 알고리즘을 사용하여 단일 네트워크 인터페이스를 선택합니다. Transit Gateway는 반환 트래픽에 대해 동일한 네트워크 인터페이스를 사용합니다. 이렇게 하면 양방향 트래픽이 대칭적으로 라우팅됩니다. 즉, 트래픽 흐름은 수명이 다할 때까지 VPC 연결의 동일한 가용 영역을 통해 라우팅됩니다. 어플라이언스 모드에



대한 자세한 내용은 Amazon VPC [설명서의 스테이트풀 어플라이언스 및 어플라이언스 모드를](#) 참조하십시오.

Transit Gateway를 사용하는 AWS Network Firewall 보안 VPC의 다양한 배포 옵션에 대해서는 [AWS Network Firewall의 배포 모델](#) 블로그 게시물을 참조하십시오.

## 중앙 집중식 네트워크 보안을 위해 게이트웨이 로드 밸런서와 Transit Gateway를 함께 사용

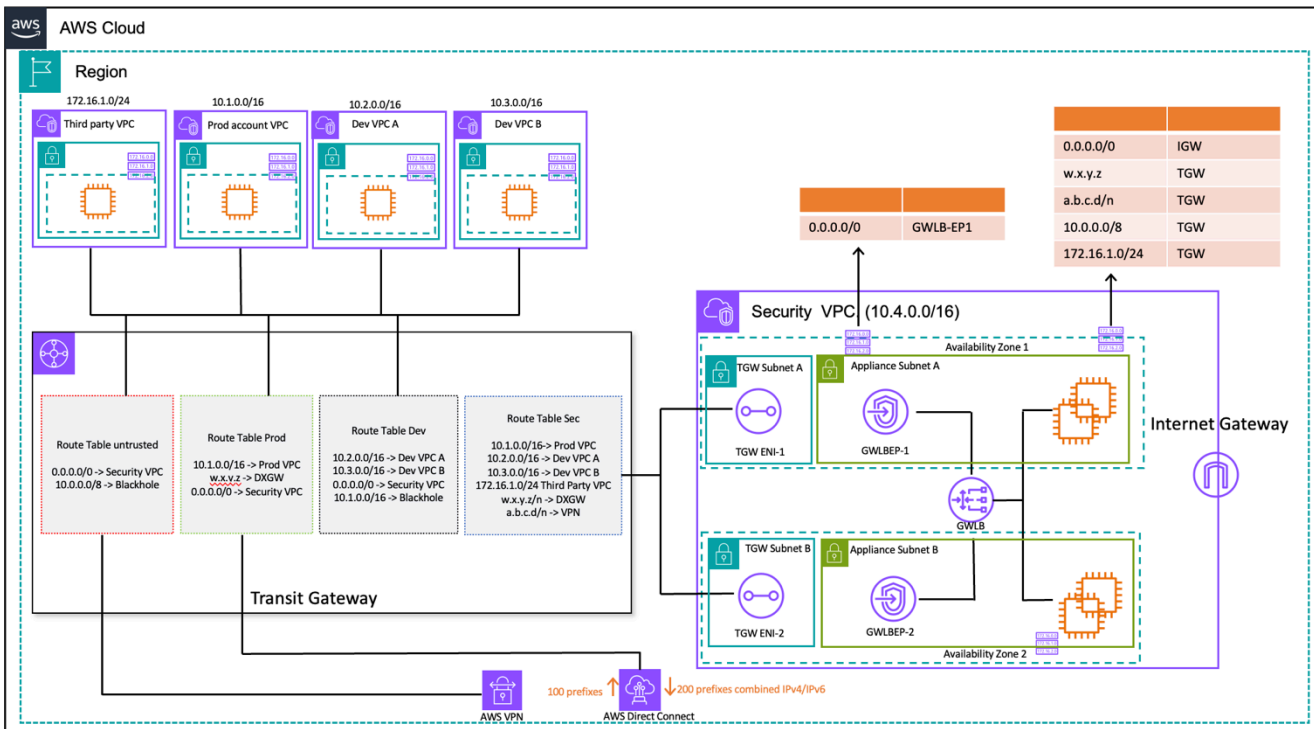
고객은 트래픽 필터링을 처리하고 보안 검사 기능을 제공하기 위해 가상 어플라이언스를 통합하기를 원하는 경우가 많습니다. 이러한 사용 사례에서는 Gateway Load Balancer, 가상 어플라이언스 및 Transit Gateway를 통합하여 VPC 간 및 VPC 트래픽을 검사하기 위한 중앙 집중식 아키텍처를 배포할 수 있습니다. to-on-premises

게이트웨이 로드 밸런서는 가상 어플라이언스와 함께 별도의 보안 VPC에 배포됩니다. 트래픽을 검사할 가상 어플라이언스는 Gateway Load Balancer 뒤의 대상으로 구성됩니다. Gateway Load Balancer 엔드포인트는 라우팅 가능한 대상이므로 고객은 Transit Gateway에서 오가는 트래픽을 가상 어플라이언스 플릿으로 라우팅할 수 있습니다. 흐름 대칭을 보장하기 위해 Transit Gateway에서 어플라이언스 모드가 활성화되어 있습니다.

각 스포크 VPC에는 Transit Gateway와 연결된 라우팅 테이블이 있으며, 이 라우팅 테이블에는 보안 VPC 연결에 대한 기본 경로가 다음 흐름으로 사용됩니다.

중앙 집중식 보안 VPC는 Gateway Load Balancer 엔드포인트와 가상 어플라이언스가 있는 각 가용 영역의 어플라이언스 서브넷으로 구성됩니다. 또한 다음 그림과 같이 각 가용 영역에 Transit Gateway 연결용 서브넷이 있습니다.

Gateway Load Balancer 및 Transit Gateway를 사용한 중앙 집중식 보안 검사에 대한 자세한 내용은 [AWS Gateway Load Balancer를 사용한 중앙 집중식 검사 아키텍처 및 블로그](#) 게시물을 참조하십시오.



Transit Gateway 및 AWS 게이트웨이 로드 밸런서를 사용한 on-premises-to VPC 간 및 -VPC 트래픽 검사 (라우팅 테이블 설계)

## AWS Network Firewall 및 AWS 게이트웨이 로드 밸런서에 대한 주요 고려 사항

- 동서 검사를 수행할 때는 Transit Gateway에서 어플라이언스 모드를 활성화해야 합니다.
- [AWS Transit Gateway 지역 간 피어링을 AWS 리전](#) 사용하여 다른 모델에 대한 트래픽 검사를 위해 동일한 모델을 배포할 수 있습니다.
- 기본적으로 가용 영역에 배포된 각 Gateway Load Balancer는 동일한 가용 영역 내의 등록된 대상에만 트래픽을 분산합니다. 이를 가용 영역 어피니티라고 합니다. [영역 간 로드 밸런싱을 활성화하면](#) Gateway Load Balancer는 활성화된 모든 가용 영역의 등록된 모든 대상 및 정상 대상에 트래픽을 분산합니다. 모든 가용 영역의 모든 대상이 비정상이면 Gateway Load Balancer가 열리지 않습니다. 자세한 내용은 [Gateway Load Balancer 배포 모범 사례 블로그 게시물의 섹션 4: 어플라이언스 및 가용 영역 장애 시나리오](#) 이해를 참조하십시오.
- 다중 지역 배포의 경우 각 로컬 지역에 별도의 검사 VPC를 설정하여 지역 간 종속성을 피하고 관련 데이터 전송 비용을 줄이는 것이 좋습니다. AWS 검사를 다른 지역으로 중앙 집중화하는 대신 로컬 지역의 트래픽을 검사해야 합니다.

- 다중 지역 배포에서 EC2 기반 HA (고가용성) 쌍을 추가로 실행하는 데 드는 비용은 합산될 수 있습니다. 자세한 내용은 [Gateway Load Balancer 배포 모범 사례](#) 블로그 게시물을 참조하십시오.

## AWS Network Firewall 게이트웨이 로드 밸런서와 비교

표 2 — 게이트웨이 로드 밸런서와 AWS Network Firewall 비교

기준	AWS Network Firewall	Gateway Load Balancer
사용 사례	Suricata와 호환되는 침입 탐지 및 방지 서비스 기능을 갖춘 스테이트풀 관리형 네트워크 방화벽.	타사 가상 어플라이언스를 쉽게 배포, 확장 및 관리할 수 있는 관리형 서비스
복잡성	AWS 매니지드 서비스. AWS 서비스의 확장성 및 가용성을 처리합니다.	AWS 관리형 서비스. AWS 게이트웨이 로드 밸런서 서비스의 확장성과 가용성을 처리합니다. 고객은 Gateway Load Balancer 기반 가상 어플라이언스의 규모 조정 및 가용성을 관리할 책임이 있습니다.
규모 조정	AWS Network Firewall 엔드포인트는 에 의해 AWS PrivateLink구동됩니다. Network Firewall은 방화벽 엔드포인트당 최대 100Gbps의 네트워크 트래픽을 지원합니다.	게이트웨이 로드 밸런서 엔드포인트는 엔드포인트당 최대 100Gbps의 최대 대역폭을 지원합니다.
비용	AWS Network Firewall 엔드포인트 비용+데이터 처리 요금	게이트웨이 로드 밸런서 + 게이트웨이 로드 밸런서 엔드포인트 + 가상 어플라이언스 + 데이터 처리 요금

## 중앙 집중식 인바운드 검사

인터넷 연결 애플리케이션은 그 특성상 공격 범위가 더 크고 대부분의 다른 유형의 애플리케이션이 직면하지 않아도 되는 위협 범주에 노출됩니다. 이러한 유형의 애플리케이션에 대한 공격으로부터 필요한 보호를 확보하고 영향 노출 영역을 최소화하는 것은 모든 보안 전략의 핵심입니다.

랜딩 존에 애플리케이션을 배포하면 사용자는 공용 인터넷 (예: CDN (Content Delivery Network) 또는 공용 웹 애플리케이션을 통해 공용 로드 밸런서, API 게이트웨이 또는 인터넷 게이트웨이를 통해 직접 많은 앱에 액세스하게 됩니다. 이 경우 인바운드 애플리케이션 검사를 위한 AWS 웹 애플리케이션 방화벽 (AWS WAF) 을 사용하거나 Gateway Load Balancer 또는 IDS/IPS 인바운드 검사를 사용하여 워크로드와 애플리케이션을 보호할 수 있습니다. AWS Network Firewall

랜딩 존에 애플리케이션을 계속 배포하면서 인바운드 인터넷 트래픽을 검사해야 할 필요가 생길 수 있습니다. 타사 방화벽 어플라이언스를 실행하는 Gateway Load Balancer를 사용하거나 오픈 소스 Suricata 규칙을 사용하는 고급 DPI 및 IDS/IPS 기능을 사용하여 분산, 중앙 집중식 AWS Network Firewall 또는 복합 검사 아키텍처를 사용하는 등 다양한 방법으로 이를 달성할 수 있습니다. 이 섹션에서는 Gateway Load Balancer와 AWS Network Firewall 트래픽 라우팅을 위한 중앙 허브 AWS Transit Gateway 역할을 사용하는 중앙 집중식 배포에 대해 다룹니다.

## AWS WAF 인터넷에서 들어오는 인바운드 트래픽을 검사하는 데도 AWS Firewall Manager 사용됩니다.

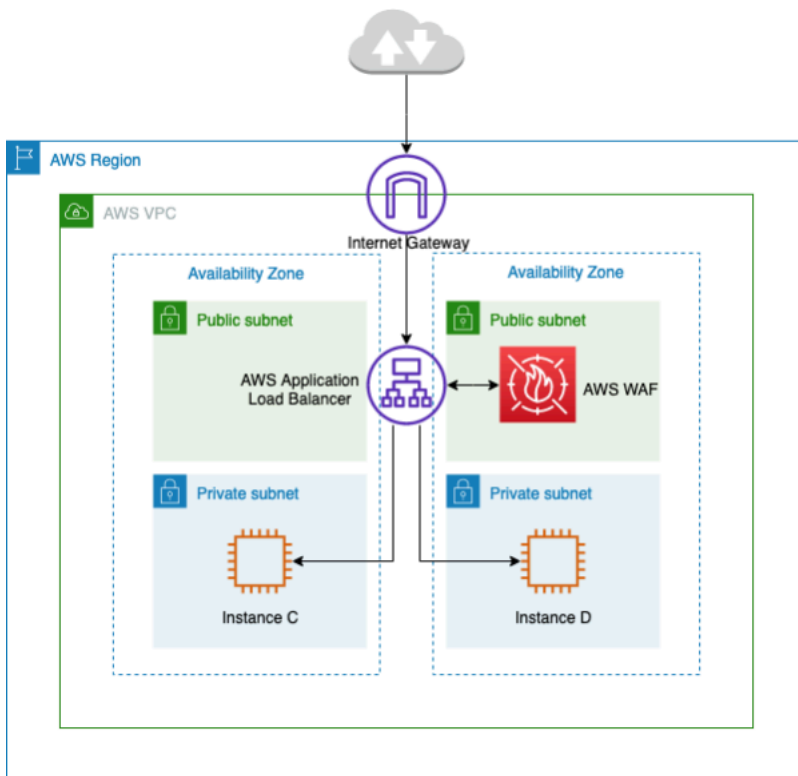
AWS WAF 가용성에 영향을 미치거나 보안을 손상시키거나 리소스를 과도하게 소비할 수 있는 일반적인 웹 공격 및 봇으로부터 웹 애플리케이션 또는 API를 보호하는 데 도움이 되는 웹 애플리케이션 방화벽입니다. AWS WAF 봇 트래픽을 제어하고 SQL 삽입 또는 XSS (Cross-Site Scripting) 와 같은 일반적인 공격 패턴을 차단하는 보안 규칙을 만들 수 있으므로 트래픽이 애플리케이션에 도달하는 방식을 제어할 수 있습니다. 특정 트래픽 패턴을 필터링하는 규칙을 사용자 지정할 수도 있습니다.

AWS WAF Amazon에서 CDN 솔루션, 웹 서버 앞에 있는 애플리케이션 로드 밸런서, REST API용 Amazon API Gateway 또는 AWS AppSync GraphQL API의 CloudFront 일부로 배포할 수 있습니다.

배포한 후에는 시각적 규칙 작성기 AWS WAF, JSON으로 작성된 코드, 에서 유지 관리하는 관리형 규칙을 사용하여 자체 트래픽 필터 규칙을 생성하거나 에서 제공하는 AWS타사 규칙을 구독할 수 있습니다. AWS Marketplace이러한 규칙은 지정된 패턴을 기준으로 트래픽을 평가하여 원치 않는 트래픽을 필터링할 수 있습니다. 또한 CloudWatch Amazon을 사용하여 들어오는 트래픽 지표 및 로깅을 모니터링할 수 있습니다.

에서 모든 계정과 애플리케이션을 중앙 집중식으로 AWS Organizations 관리하려면 다음을 사용할 수 있습니다 AWS Firewall Manager. AWS Firewall Manager 방화벽 규칙을 중앙에서 구성하고 관리할 수 있는 보안 관리 서비스입니다. 새 애플리케이션이 생성되면 AWS Firewall Manager 공통 보안 규칙을 적용하여 새 애플리케이션과 리소스를 손쉽게 규정을 준수할 수 있습니다.

를 사용하면 애플리케이션 로드 밸런서 AWS Firewall Manager, API Gateway 인스턴스 및 Amazon CloudFront 배포에 대한 AWS WAF 규칙을 쉽게 롤아웃할 수 있습니다. AWS Firewall Manager for 와 AWS Managed Rules 통합되어 사전 구성되고 큐레이션된 AWS WAF 규칙을 애플리케이션에 쉽게 배포할 수 있습니다. AWS WAF 중앙 관리에 대한 자세한 내용은 중앙 관리 AWS WAF [AWS WAF \(API v2\) 및 대규모 관리](#)를 참조하십시오. AWS Firewall Manager AWS Managed Rules AWS Firewall Manager



를 사용한 중앙 집중식 인바운드 트래픽 검사 AWS WAF

이전 아키텍처에서는 애플리케이션이 프라이빗 서브넷의 여러 가용 영역에 있는 Amazon EC2 인스턴스에서 실행됩니다. Amazon EC2 인스턴스 앞에 공개 애플리케이션 로드 밸런서 (ALB) 가 배포되어 서로 다른 대상 간에 요청을 로드 밸런싱합니다. ALB와 AWS WAF 연결되어 있습니다.

## 장점

- [AWS WAF Bot Control](#)을 사용하면 애플리케이션에 대한 일반적이고 널리 퍼지는 봇 트래픽을 파악하고 제어할 수 있습니다.

- [Managed AWS WAF Rules for](#) 를 사용하면 빠르게 시작하고 일반적인 위협으로부터 웹 애플리케이션 또는 API를 보호할 수 있습니다. 개방형 웹 응용 프로그램 보안 프로젝트 (OWASP) 10대 보안 위협, Joomla와 같은 콘텐츠 관리 시스템 (CMS) 관련 위협, 새로 등장하는 일반적인 취약성 및 노출 (CVE) 등 문제를 해결하는 규칙 유형 등 다양한 규칙 유형 중에서 선택할 수 있습니다. WordPress 관리형 규칙은 새로운 문제가 발생하면 자동으로 업데이트되므로 애플리케이션 구축에 더 많은 시간을 할애할 수 있습니다.
- AWS WAF 관리형 서비스이므로 이 아키텍처에서는 검사를 위한 어플라이언스가 필요하지 않습니다. 또한 [Amazon Data Firehose](#)를 통해 거의 실시간으로 로그를 제공합니다. AWS WAF 웹 트래픽에 대한 가시성을 거의 실시간으로 제공하여 Amazon에서 새 규칙이나 알림을 생성하는 데 사용할 수 있습니다. CloudWatch

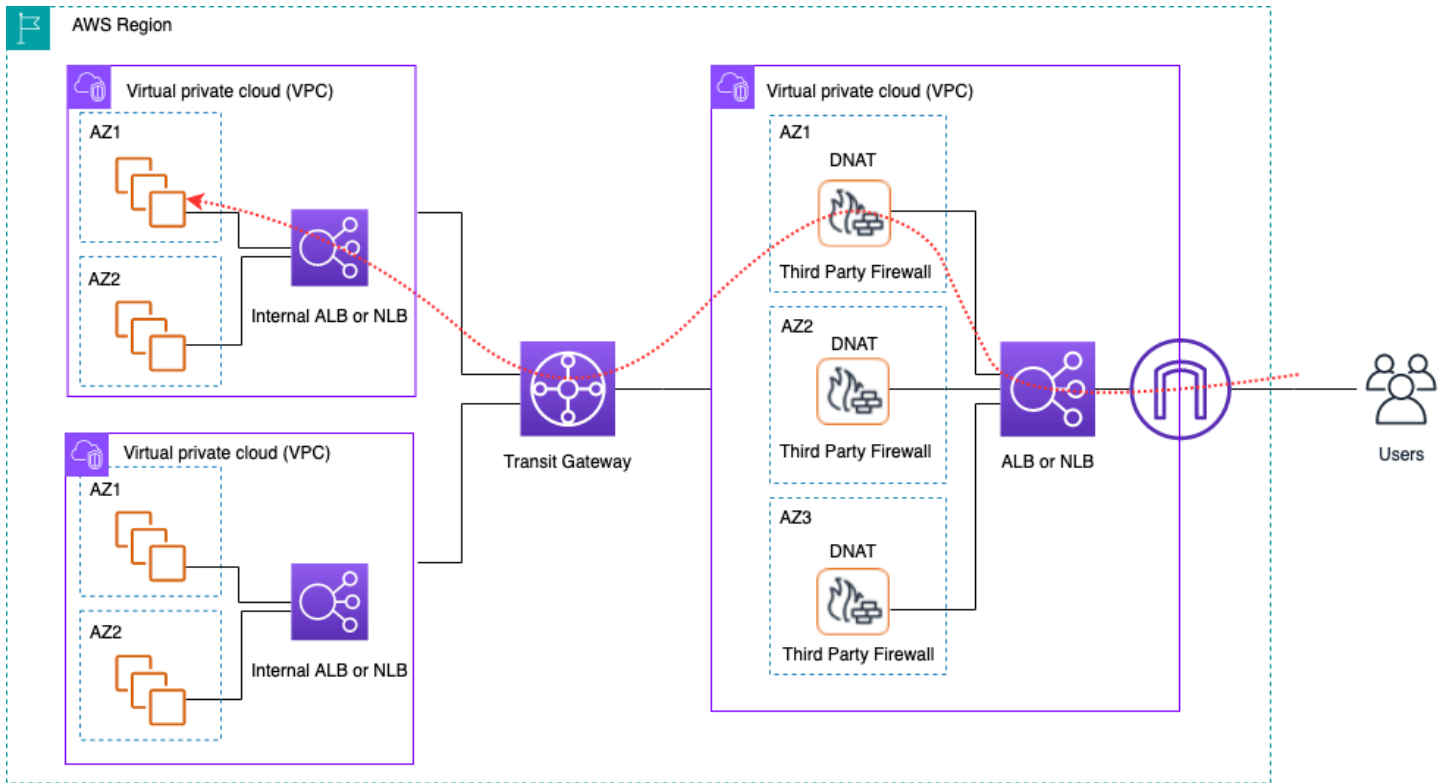
## 주요 고려 사항

- 이 아키텍처는 ALB별, 배포 및 API Gateway에 AWS WAF 통합되므로 HTTP 헤더 검사 및 분산 검사에 가장 적합합니다. CloudFront AWS WAF 요청 본문을 기록하지 않습니다.
- 두 번째 ALB 세트 (있는 경우) 로 이동하는 트래픽은 동일한 AWS WAF 인스턴스에서 검사되지 않을 수 있습니다. 두 번째 ALB 세트에 새 요청이 전송되기 때문입니다.

## 타사 어플라이언스를 사용한 중앙 집중식 인바운드 검사

이 아키텍처 설계 패턴에서는 별도의 검사 VPC의 애플리케이션/네트워크 로드 밸런서와 같은 Elastic Load Balancer (ELB) 뒤의 여러 가용 영역에 Amazon EC2에 타사 방화벽 어플라이언스를 배포합니다.

검사 VPC는 다른 스포크 VPC와 함께 Transit Gateway를 통해 VPC 첨부 파일로 함께 연결됩니다. 스포크 VPC의 애플리케이션은 애플리케이션 유형에 따라 ALB 또는 NLB일 수 있는 내부 ELB에 의해 프론트엔드입니다. 인터넷을 통해 클라이언트는 트래픽을 방화벽 어플라이언스 중 하나로 라우팅하는 검사 VPC에 있는 외부 ELB의 DNS에 연결합니다. 방화벽은 트래픽을 검사한 다음 다음 그림과 같이 내부 ELB의 DNS를 사용하여 Transit Gateway를 통해 트래픽을 스포크 VPC로 라우팅합니다. 타사 어플라이언스를 사용한 인바운드 보안 검사에 대한 자세한 내용은 [타사 방화벽 어플라이언스를 AWS 환경에 통합하는 방법](#) 블로그 게시물을 참조하십시오.



타사 어플라이언스 및 ELB를 사용한 중앙 집중식 인그레스 트래픽 검사

## 장점

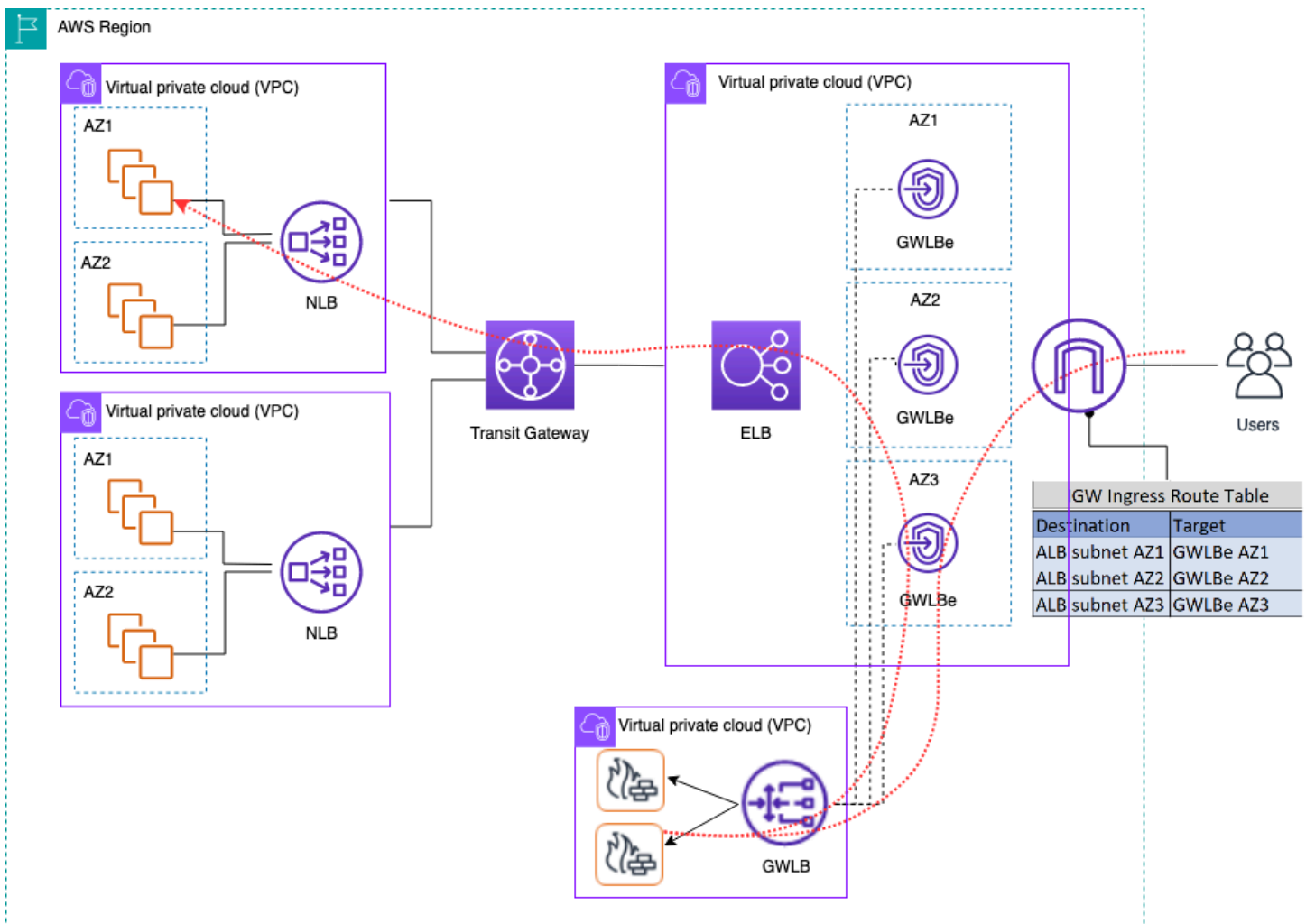
- 이 아키텍처는 타사 방화벽 어플라이언스를 통해 제공되는 검사 및 고급 검사 기능을 위한 모든 애플리케이션 유형을 지원할 수 있습니다.
- 이 패턴은 방화벽 어플라이언스에서 스포크 VPC로의 DNS 기반 라우팅을 지원하므로 Spoke VPC의 애플리케이션을 ELB를 기반으로 독립적으로 확장할 수 있습니다.
- Auto Scaling을 ELB와 함께 사용하여 검사 VPC에서 방화벽 어플라이언스를 확장할 수 있습니다.

## 주요 고려 사항

- 고가용성을 위해서는 가용 영역 전체에 여러 방화벽 어플라이언스를 배포해야 합니다.
- 흐름 대칭을 유지하려면 방화벽을 소스 NAT로 구성하고 수행해야 합니다. 즉, 클라이언트 IP 주소가 애플리케이션에 표시되지 않습니다.
- 네트워크 서비스 계정에 Transit Gateway 및 검사 VPC를 배포해 보십시오.
- 추가 타사 공급업체 방화벽 라이선스/지원 비용. Amazon EC2 요금은 인스턴스 유형에 따라 달라집니다.

## Gateway Load Balancer와 함께 방화벽 어플라이언스를 사용하여 인터넷에서 들어오는 인바운드 트래픽을 검사합니다.

고객은 심층 방어 전략의 일환으로 타사 차세대 방화벽 (NGFW) 및 IPS (침입 방지 시스템) 를 사용합니다. 일반적으로 이들은 전용 하드웨어 또는 소프트웨어/가상 어플라이언스인 경우가 많습니다. Gateway Load Balancer를 사용하면 다음 그림과 같이 이러한 가상 어플라이언스를 수평적으로 확장하여 VPC에서 들어오고 VPC로 들어오는 트래픽을 검사할 수 있습니다.



### Gateway Load Balancer와 함께 방화벽 어플라이언스를 사용한 중앙 집중식 인그레스 트래픽 검사

이전 아키텍처에서 Gateway Load Balancer 엔드포인트는 별도의 엣지 VPC의 각 가용 영역에 배포되었습니다. 차세대 방화벽, 침입 방지 시스템 등은 중앙 집중식 어플라이언스 VPC의 Gateway Load Balancer 뒤에 배포됩니다. 이 어플라이언스 VPC는 스포크 VPC와 동일한 AWS 계정 또는 다른 AWS 계정에 있을 수 있습니다. 가상 어플라이언스는 Auto Scaling 그룹을 사용하도록 구성할 수 있으며 Gateway Load Balancer에 자동으로 등록되므로 보안 계층의 자동 확장이 가능합니다.

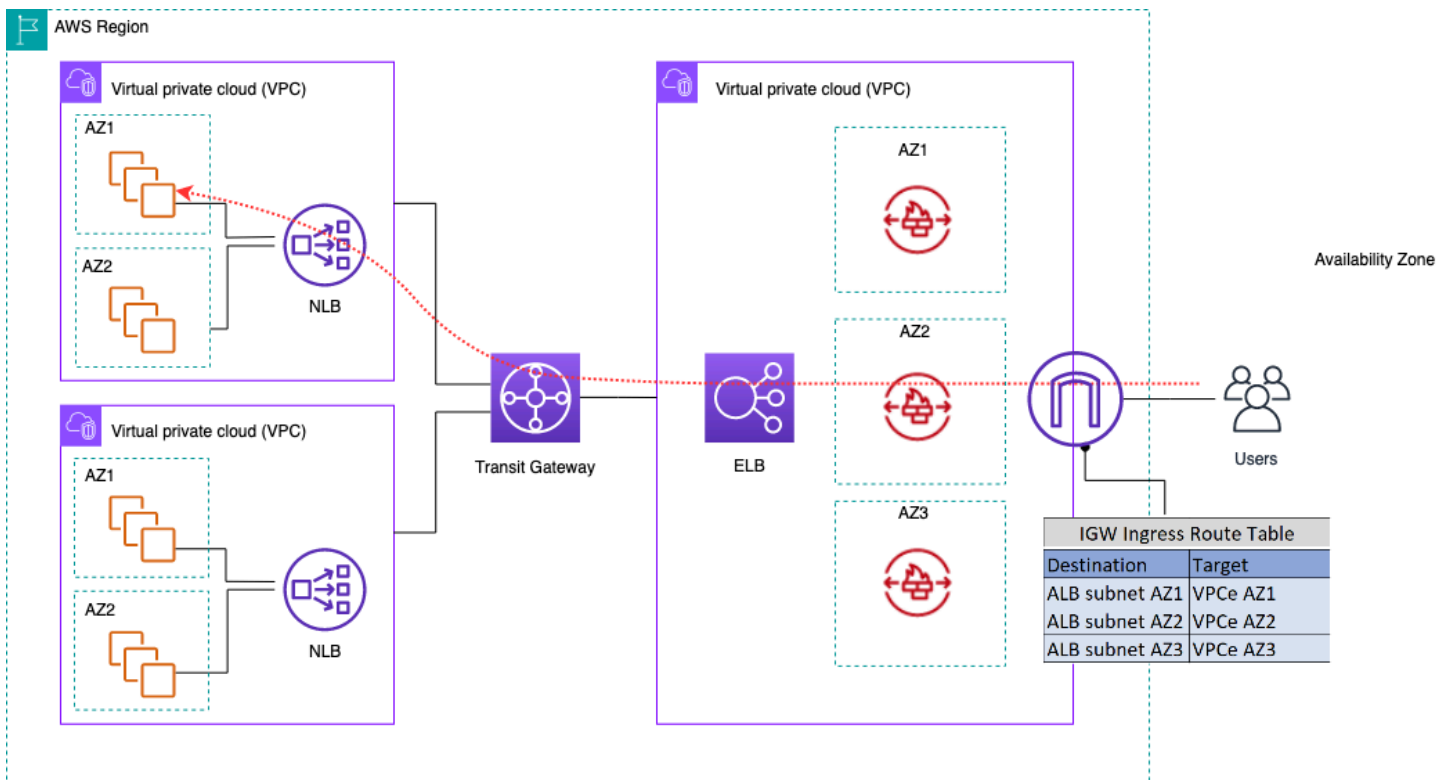


이러한 가상 어플라이언스는 IGW (Internet Gateway) 를 통해 관리 인터페이스에 액세스하거나 어플라이언스 VPC의 배스천 호스트 설정을 사용하여 관리할 수 있습니다.

VPC 인그레스 라우팅 기능을 사용하면 인터넷의 인바운드 트래픽을 Gateway Load Balancer 뒤의 방화벽 어플라이언스로 라우팅하도록 엣지 라우팅 테이블이 업데이트됩니다. 검사된 트래픽은 게이트웨이 로드 밸런서 엔드포인트를 통해 대상 VPC 인스턴스로 라우팅됩니다. [AWS 게이트웨이 로드 밸런서를 사용하는 다양한 방법에 대한 자세한 내용은 게이트웨이 로드 밸런서 소개: 지원되는 아키텍처 패턴 블로그 게시물을 참조하십시오.](#)

## 중앙 집중식 AWS Network Firewall 수신에 사용

이 아키텍처에서는 인그레스 트래픽이 나머지 VPC에 AWS Network Firewall 도달하기 전에 검사됩니다. 이 설정에서는 트래픽이 Edge VPC에 배포된 모든 방화벽 엔드포인트 간에 분할됩니다. 방화벽 엔드포인트와 Transit Gateway 서브넷 사이에 퍼블릭 서브넷을 배포합니다. 스포크 VPC에 IP 대상을 포함하는 ALB 또는 NLB를 사용할 수 있으며 그 뒤에 있는 대상에 대한 Auto Scaling을 처리할 수 있습니다.



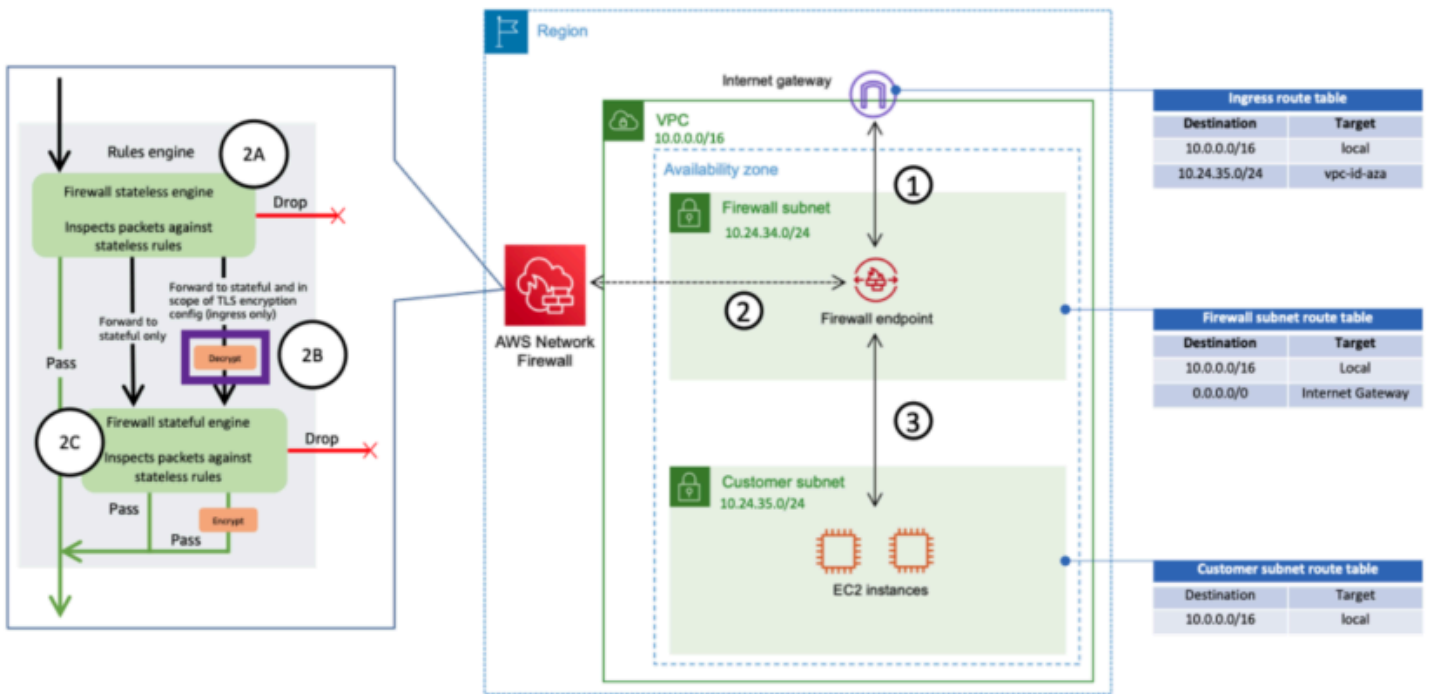
### AWS Network Firewall을 사용한 인그레스 트래픽 검사

이 모델의 배포 및 관리를 단순화하기 위해 사용할 AWS Firewall Manager 수 있습니다. AWS Network Firewall Firewall Manager를 사용하면 중앙 위치에서 생성한 보호 기능을 여러 계정에 자동으로 적

용하여 다양한 방화벽을 중앙에서 관리할 수 있습니다. Firewall Manager는 네트워크 방화벽에 대한 분산 및 중앙 집중식 배포 모델을 모두 지원합니다. 모델을 자세히 설명하는 블로그 게시물 [[블 AWS Network Firewall 사용하여 AWS Firewall Manager 배포하는 방법](#)] 을 참조하십시오.

## DPI (딥 패킷 검사) 를 통한 AWS Network Firewall

Network Firewall은 인그레스 트래픽에 대해 딥 패킷 검사 (DPI) 를 수행할 수 있습니다. Network Firewall은 (ACM) 에 저장된 TLS AWS Certificate Manager (전송 계층 보안) 인증서를 사용하여 패킷을 복호화하고, DPI를 수행하고, 패킷을 재암호화할 수 있습니다. 네트워크 방화벽으로 DPI를 설정할 때는 몇 가지 고려할 사항이 있습니다. 먼저, 신뢰할 수 있는 TLS 인증서를 ACM에 저장해야 합니다. 둘째, 복호화 및 재암호화를 위해 패킷을 올바르게 전송하도록 Network Firewall 규칙을 구성해야 합니다. [암호화된 트래픽에 대한 자세한 내용은 블로그 게시물 TLS 검사 구성을](#) 참조하십시오. AWS Network Firewall



DPI와 함께 Network Firewall을 사용한 인그레스 트래픽 검사

## 중앙 집중식 AWS Network Firewall 인그레스 아키텍처의 주요 고려사항

- Edge VPC의 Elastic Load Balancing은 호스트 이름이 아닌 대상 유형으로만 IP 주소를 사용할 수 있습니다. 위 그림에서 대상은 스포크 VPC에 있는 Network Load Balancer의 프라이빗 IP입니다. 엣지 VPC에서 ELB 뒤에 있는 IP 타겟을 사용하면 Auto Scaling이 손실됩니다.
- 방화벽 AWS Firewall Manager 엔드포인트를 단일 창으로 사용하는 것을 고려해 보십시오.

- 이 배포 모델은 엣지 VPC에 진입하는 즉시 트래픽 검사를 사용하므로 검사 아키텍처의 전체 비용을 줄일 수 있습니다.

## DNS

기본 VPC를 제외하고 VPC로 인스턴스를 시작하면 VPC에 지정한 DNS 속성 및 인스턴스에 퍼블릭 IPv4 주소가 있는지 여부에 따라 인스턴스에 프라이빗 DNS 호스트 이름 (및 퍼블릭 [DNS](#) 호스트 이름)을 AWS 제공합니다. `enableDnsSupport` 속성이 `true` 설정되면 Route 53 리졸버로부터 VPC 내의 DNS 확인을 가져옵니다 (VPC CIDR에 대한 +2 IP 오프셋). 기본적으로 Route 53 리졸버는 EC2 인스턴스 또는 Elastic Load Balancing 로드 밸런서의 도메인 이름과 같은 VPC 도메인 이름에 대한 DNS 쿼리에 응답합니다. VPC 피어링을 사용하면 한 VPC의 호스트가 퍼블릭 DNS 호스트 이름을 피어링된 VPC의 인스턴스에 대한 프라이빗 IP 주소로 확인할 수 있습니다. 단, 그렇게 하는 옵션이 활성화되어 있어야 합니다. 를 통해 연결된 VPC에도 동일하게 적용됩니다. AWS Transit Gateway 자세한 내용은 [VPC 피어링 연결에 대한 DNS 확인 지원 활성화](#)를 참조하십시오.

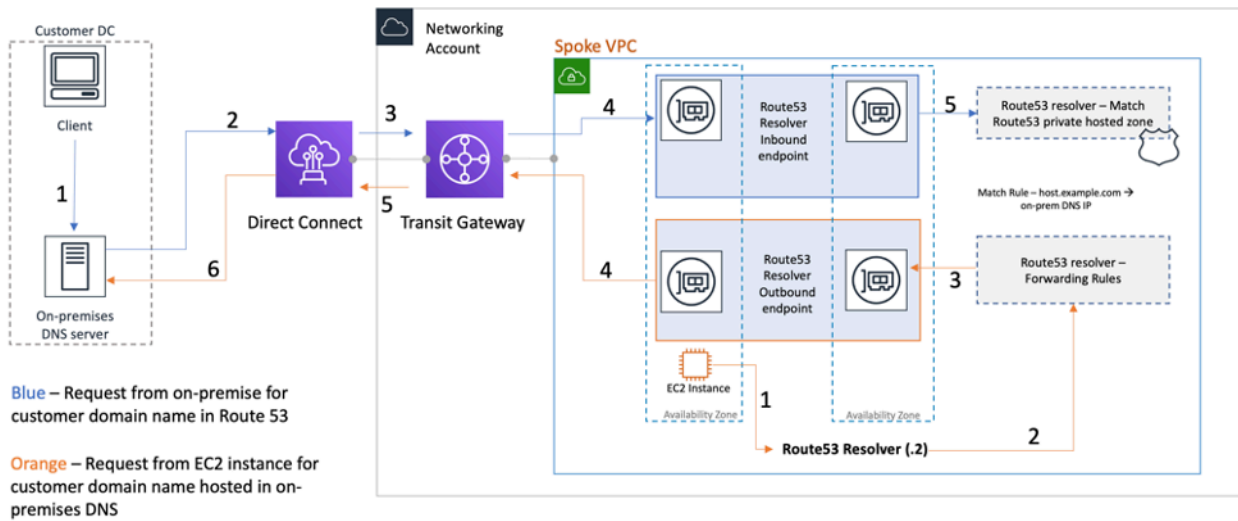
인스턴스를 사용자 지정 도메인 이름에 매핑하려는 경우 [Amazon Route 53](#)을 사용하여 사용자 지정 DNS-IP 매핑 레코드를 생성할 수 있습니다. Amazon Route 53 호스팅 영역은 Amazon Route 53이 도메인 및 해당 하위 도메인에 대한 DNS 쿼리에 응답하기를 원하는 방식에 대한 정보를 보관하는 컨테이너입니다. 퍼블릭 호스팅 영역에는 퍼블릭 인터넷을 통해 확인할 수 있는 DNS 정보가 포함되어 있는 반면, 프라이빗 호스팅 영역은 특정 프라이빗 호스팅 영역에 연결된 VPC에만 정보를 제공하는 특정 구현입니다. 여러 VPC 또는 계정이 있는 랜딩 존 설정에서는 단일 프라이빗 호스팅 영역을 AWS 계정 및 지역 전체에 걸쳐 여러 VPC와 연결할 수 있습니다 ([SDK/CLI/API에서만](#) 가능). VPC의 최종 호스트는 각각의 Route 53 리졸버 IP (VPC CIDR 오프셋 +2) 를 DNS 쿼리용 네임 서버로 사용합니다. VPC의 Route 53 리졸버는 VPC 내 리소스로부터의 DNS 쿼리만 받아들입니다.

## 하이브리드 DNS

DNS는 애플리케이션이 의존하는 호스트 이름-IP 주소 해상도를 제공하므로 하이브리드 또는 기타 인프라의 중요한 구성 요소입니다. 하이브리드 환경을 구현하는 고객은 일반적으로 이미 DNS 확인 시스템을 갖추고 있으며 현재 시스템과 함께 작동하는 DNS 솔루션을 원합니다. VPN 또는 온프레미스 네트워크에서는 네이티브 Route 53 리졸버 (기본 VPC CIDR의 2배 이상) 에 연결할 수 없습니다. AWS Direct Connect 따라서 AWS 리전의 VPC용 DNS를 네트워크의 DNS와 통합할 때는 Route 53 Resolver 인바운드 엔드포인트 (VPC에 전달하는 DNS 쿼리용) 와 Route 53 Resolver 아웃바운드 엔드포인트 (VPC에서 네트워크로 전달하는 쿼리용) 가 필요합니다.

다음 그림에 표시된 것처럼 VPC의 Amazon EC2 인스턴스에서 수신한 쿼리를 네트워크의 DNS 서버로 전달하도록 아웃바운드 Resolver 엔드포인트를 구성할 수 있습니다. VPC에서 온 프레미스 네트워크로 선택한 쿼리를 전달하려면 전달하려는 DNS 쿼리의 도메인 이름 (예: `example.com`) 과 쿼리를 전달하려는 네트워크 상의 DNS 확인자의 IP 주소를 지정하는 Route 53 Resolver 규칙을 생성합니다. 온

프리미스 네트워크에서 Route 53 호스팅 영역으로의 인바운드 쿼리의 경우 네트워크의 DNS 서버가 지정된 VPC의 인바운드 Resolver 엔드포인트로 쿼리를 전달할 수 있습니다.

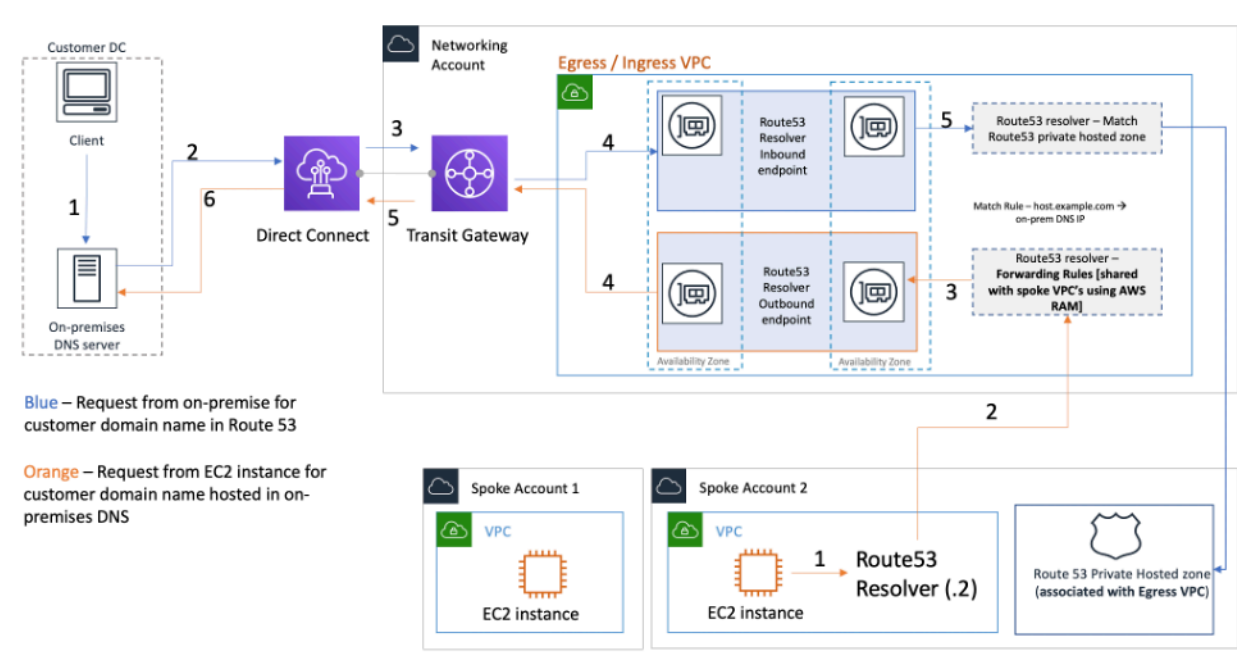


### Route 53 리졸버를 사용한 하이브리드 DNS 해결

이렇게 하면 온 프레미스 DNS 해석기가 Amazon EC2 인스턴스 또는 해당 VPC와 연결된 Route 53 프라이빗 호스팅 영역의 레코드와 같은 AWS 리소스의 도메인 이름을 쉽게 확인할 수 있습니다. 또한 Route 53 Resolver 엔드포인트는 ENI당 초당 최대 약 10,000개의 쿼리를 처리할 수 있으므로 훨씬 더 큰 DNS 쿼리 볼륨으로 쉽게 확장할 수 있습니다. 자세한 내용은 [내용은 Amazon Route 53 설명서의 리졸버 모범 사례를](#) 참조하십시오.

랜딩 존의 모든 VPC에 Route 53 리졸버 엔드포인트를 생성하는 것은 권장되지 않습니다. 중앙 송신 VPC (네트워크 서비스 계정) 에 중앙 집중화하십시오. 이 접근 방식을 사용하면 비용을 낮추면서 관리 용이성을 높일 수 있습니다 (생성한 각 인바운드/아웃바운드 리졸버 엔드포인트에 대해 시간당 요금이 부과됨). 중앙 인바운드 및 아웃바운드 엔드포인트를 나머지 랜딩 존과 공유합니다.

- 아웃바운드 해결 - 네트워크 서비스 계정을 사용하여 리졸버 규칙 (온프레미스 DNS 서버로 전달되는 DNS 쿼리를 기반으로 함) 을 작성합니다. 리소스 액세스 관리자 (RAM) 를 사용하여 이러한 Route 53 리졸버 규칙을 여러 계정과 공유하고 계정의 VPC와 연결할 수 있습니다. 스포크 VPC의 EC2 인스턴스는 Route 53 리졸버에 DNS 쿼리를 전송할 수 있으며, Route 53 리졸버 서비스는 이그레스 VPC의 아웃바운드 Route 53 리졸버 엔드포인트를 통해 이러한 쿼리를 온프레미스 DNS 서버로 전달합니다. 스포크 VPC를 이그레스 VPC에 피어링하거나 Transit Gateway를 통해 연결할 필요가 없습니다. 아웃바운드 리졸버 엔드포인트의 IP를 스포크 VPC의 기본 DNS로 사용하지 마십시오. 스포크 VPC는 VPC에서 Route 53 리졸버 (VPC CIDR을 오프셋하기 위해) 를 사용해야 합니다.



### 수신/송신 VPC의 Route 53 리졸버 엔드포인트 중앙 집중화

- 인바운드 DNS 확인 — 중앙 집중식 VPC에 Route 53 Resolver 인바운드 엔드포인트를 생성하고 랜딩 존의 모든 프라이빗 호스팅 영역을 이 중앙 집중식 VPC와 연결합니다. 자세한 내용은 프라이빗 호스팅 영역에 더 많은 VPC [연결을 참조하십시오](#). VPC와 연결된 여러 프라이빗 호스팅 영역 (PHZ)은 겹칠 수 없습니다. 위 그림에서 볼 수 있듯이 PHZ와 중앙 집중식 VPC를 연결하면 온프레미스 서버가 중앙 집중식 VPC의 인바운드 엔드포인트를 사용하여 중앙 VPC와 연결된 프라이빗 호스팅 영역의 모든 항목에 대한 DNS를 확인할 수 있습니다. 하이브리드 DNS 설정에 대한 자세한 내용은 [Amazon Route 53 및 AWS Transit Gateway를 사용한 하이브리드 클라우드의 중앙 집중식 DNS 관리 및 Amazon VPC용 하이브리드 클라우드 DNS 옵션을 참조하십시오](#).

## Route 53 DNS 방화벽

Amazon Route 53 Resolver DNS 방화벽은 VPC의 아웃바운드 DNS 트래픽을 필터링하고 규제하는 데 도움이 됩니다. DNS 방화벽의 주요 용도는 VPC의 리소스가 조직이 신뢰하는 사이트에 대해서만 아웃바운드 DNS 요청을 할 수 있도록 하는 도메인 이름 허용 목록을 정의하여 데이터의 데이터 유출을 방지하는 것입니다. 또한 고객은 VPC 내 리소스가 DNS를 통해 통신하는 것을 원하지 않는 도메인에 대한 차단 목록을 만들 수 있습니다. Amazon Route 53 Resolver DNS 방화벽에는 다음과 같은 기능이 있습니다.

고객은 규칙을 만들어 DNS 쿼리에 응답하는 방법을 정의할 수 있습니다. 도메인 이름에 대해 정의할 수 있는 작업에는 NODATA, OVERRIDE 등이 포함됩니다 NXDOMAIN.

고객은 허용 목록과 거부 목록 모두에 대한 알림을 생성하여 규칙 활동을 모니터링할 수 있습니다. 이 기능은 고객이 규칙을 프로덕션 환경으로 전환하기 전에 테스트하려는 경우에 유용할 수 있습니다.

자세한 내용은 [Amazon VPC용 Amazon Route 53 Resolver DNS 방화벽 시작 방법](#) 블로그 게시물을 참조하십시오.

## VPC 프라이빗 엔드포인트에 대한 중앙 집중식 액세스

VPC 엔드포인트를 사용하면 인터넷 게이트웨이 또는 NAT 디바이스, VPN 연결 또는 연결 없이 VPC를 지원되는 AWS 서비스에 비공개로 연결할 수 있습니다. AWS Direct Connect 따라서 VPC가 퍼블릭 인터넷에 노출되지 않습니다. VPC의 인스턴스는 이 인터페이스 엔드포인트를 사용하여 AWS 서비스 엔드포인트와 통신하는 데 퍼블릭 IP 주소가 필요하지 않습니다. VPC와 다른 서비스 간의 트래픽은 AWS 네트워크 백본을 벗어나지 않습니다. VPC 엔드포인트는 가상 디바이스입니다. 수평으로 확장된 고가용성 중복 VPC 구성 요소입니다. 현재 두 가지 유형의 엔드포인트, 즉 인터페이스 엔드포인트(구동)와 게이트웨이 엔드포인트를 프로비저닝할 수 있습니다. [AWS PrivateLink 게이트웨이 엔드포인트](#)를 사용하여 Amazon S3 및 Amazon DynamoDB 서비스에 비공개로 액세스할 수 있습니다. 게이트웨이 엔드포인트 사용에 따르는 추가 요금은 없습니다. 데이터 전송 및 리소스 사용량에 대한 표준 요금이 그대로 적용됩니다.

### 인터페이스 VPC 엔드포인트

[인터페이스 엔드포인트](#)는 지원되는 서비스로 향하는 트래픽의 진입점 역할을 하는 사설 IP 주소를 가진 하나 이상의 엘라스틱 네트워크 인터페이스로 구성됩니다. AWS 인터페이스 엔드포인트를 프로비저닝하면 데이터 처리 요금과 함께 엔드포인트를 실행하는 1시간마다 비용이 발생합니다. 기본적으로 서비스에 액세스하려는 모든 VPC에 인터페이스 엔드포인트를 생성합니다. AWS 이는 고객이 여러 VPC에서 특정 AWS 서비스와 상호 작용하기를 원하는 랜딩 존 설정에서 비용이 많이 들고 관리하기 어려울 수 있습니다. 이를 방지하기 위해 인터페이스 엔드포인트를 중앙 집중식 VPC에서 호스팅할 수 있습니다. 모든 스포크 VPC는 Transit Gateway를 통해 이러한 중앙 집중식 엔드포인트를 사용합니다.

AWS 서비스에 VPC 엔드포인트를 생성할 때 프라이빗 DNS를 활성화할 수 있습니다. 이 설정이 활성화되면 공용 AWS 서비스 엔드포인트를 인터페이스 엔드포인트의 사설 IP로 확인할 수 있는 AWS 관리형 Route 53 프라이빗 호스팅 영역 (PHZ)이 생성됩니다. 관리형 PHZ는 인터페이스 엔드포인트가 있는 VPC 내에서만 작동합니다. 설정에서 스포크 VPC가 중앙 집중식 VPC에 호스팅된 VPC 엔드포인트 DNS를 확인할 수 있도록 하려는 경우 관리형 PHZ는 작동하지 않습니다. 이 문제를 해결하려면 인터페이스 엔드포인트 생성 시 프라이빗 DNS를 자동으로 생성하는 옵션을 비활성화하세요. 다음으로 [Route 53 PHZ를 수동으로 생성하고](#) 인터페이스 엔드포인트를 가리키는 전체 AWS 서비스 엔드포인트 이름이 포함된 Alias 레코드를 추가합니다.

1. 콘솔에 로그인하고 Route 53 서비스로 이동합니다.
2. 프라이빗 호스팅 영역을 선택하고 레코드 생성으로 이동합니다.
3. 레코드 이름 필드를 채우고 레코드 유형을 A로 선택한 다음 별칭을 활성화합니다.



4. Route Traffic to 섹션에서 트래픽을 전송할 서비스를 선택하고 드롭다운 목록에서 지역을 선택합니다.
5. 적절한 라우팅 정책을 선택하고 대상 상태 평가 옵션을 활성화했는지 확인하십시오.

이 프라이빗 호스팅 영역을 랜딩 존 내의 다른 VPC와 [연결합니다](#). 이 구성을 통해 스포크 VPC는 중앙 집중식 VPC의 인터페이스 엔드포인트에 대한 풀 서비스 엔드포인트 이름을 확인할 수 있습니다.

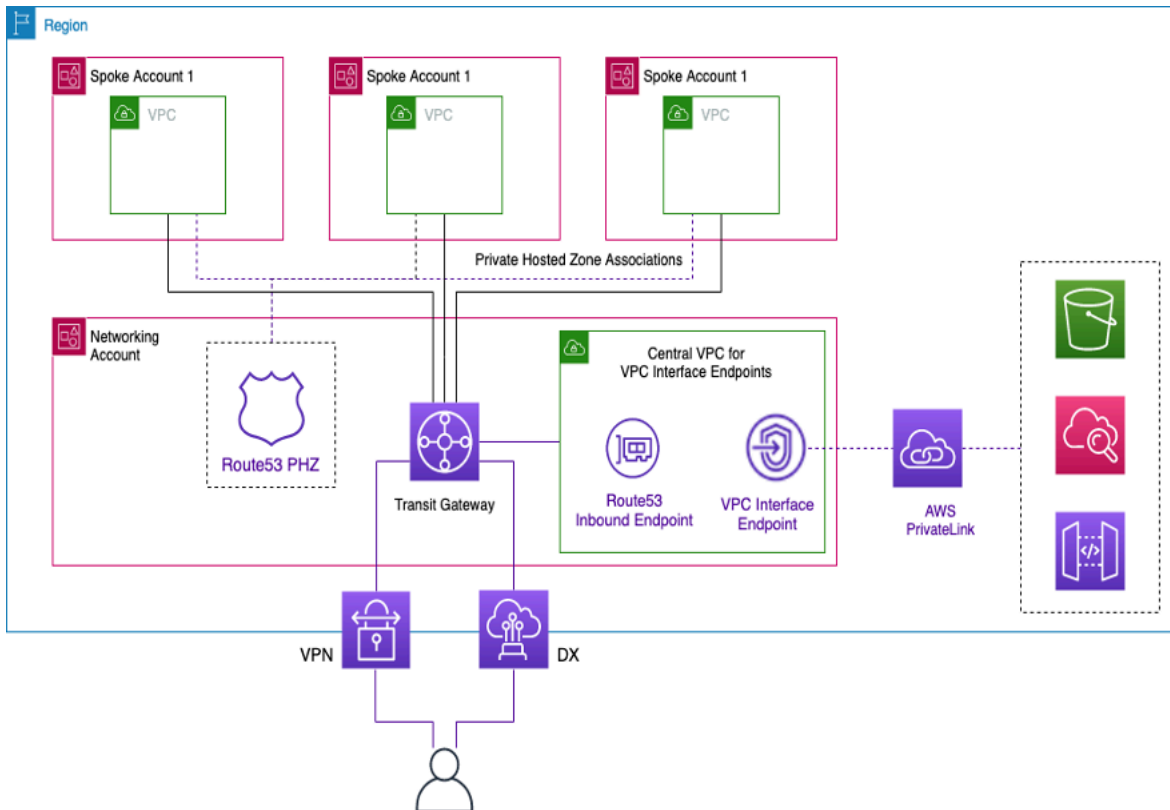
#### Note

공유 프라이빗 호스팅 영역에 액세스하려면 스포크 VPC의 호스트가 해당 VPC의 Route 53 Resolver IP를 사용해야 합니다. 또한 온프레미스 네트워크에서 VPN 및 Direct Connect를 통해 인터페이스 엔드포인트에 액세스할 수 있습니다. 조건부 전달 규칙을 사용하여 풀 서비스 엔드포인트 이름에 대한 모든 DNS 트래픽을 Route 53 Resolver 인바운드 엔드포인트로 전송하면 프라이빗 호스팅 영역에 따라 DNS 요청이 해결됩니다.

다음 그림에서 Transit Gateway는 스포크 VPC에서 중앙 집중식 인터페이스 엔드포인트로의 트래픽 흐름을 지원합니다. 네트워크 서비스 계정에서 VPC 엔드포인트와 프라이빗 호스팅 영역을 생성하고 이를 스포크 계정의 스포크 VPC와 공유합니다. 다른 VPC와 엔드포인트 정보를 공유하는 방법에 대한 자세한 내용은 [AWS Transit Gateway와 AWS PrivateLink Amazon Route 53 리졸버 통합](#) 블로그 게시물을 참조하십시오.

#### Note

분산 VPC 엔드포인트 접근 방식, 즉 VPC당 엔드포인트를 사용하면 VPC 엔드포인트에 최소 권한 정책을 적용할 수 있습니다. 중앙 집중식 접근 방식에서는 단일 엔드포인트에서 모든 스포크 VPC 액세스에 대한 정책을 적용하고 관리합니다. VPC의 수가 증가함에 따라 단일 정책 문서로 최소 권한을 유지하는 것이 복잡해질 수 있습니다. 또한 단일 정책 문서로 인해 폭발 반경이 더 커집니다. 또한 [정책 문서의 크기 \(20,480자\)](#) 도 제한됩니다.



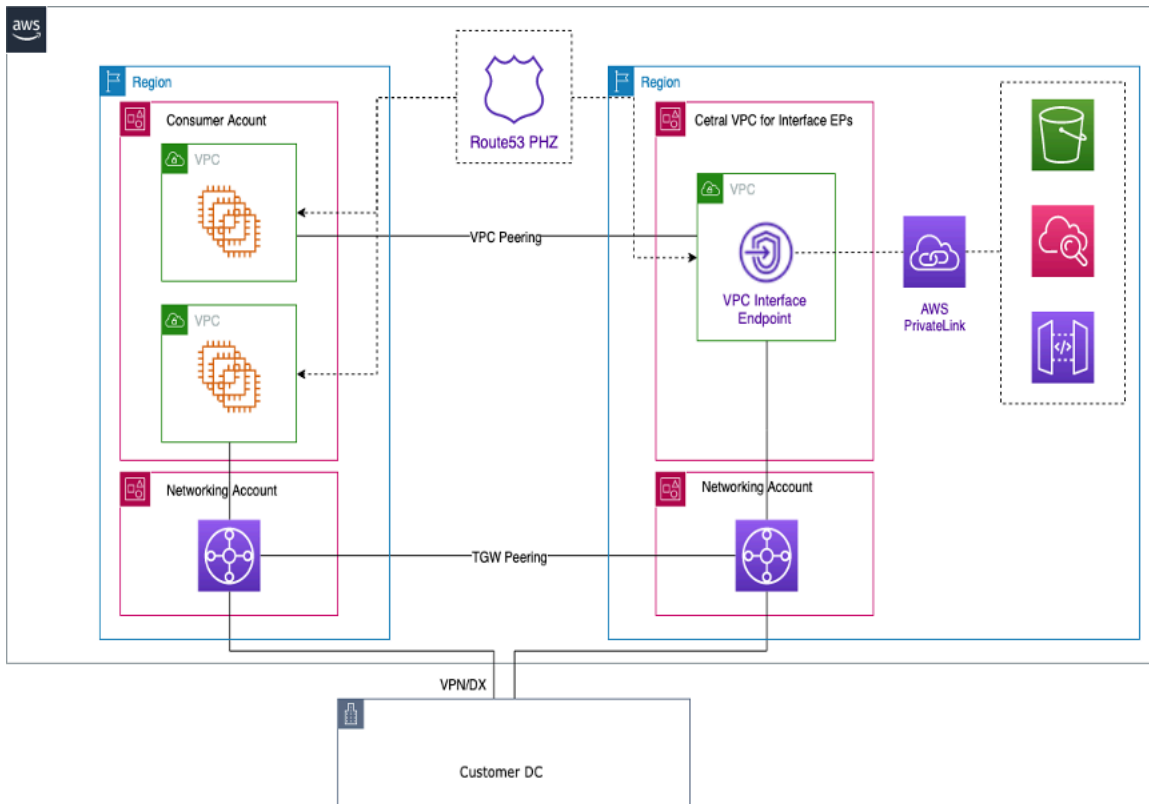
인터페이스 VPC 엔드포인트 중앙 집중화

## 리전 간 엔드포인트 액세스

공통 VPC 엔드포인트를 공유하는 서로 다른 지역에 여러 VPC를 설정하려면 앞서 설명한 대로 PHZ를 사용하십시오. 각 지역의 두 VPC는 엔드포인트의 별칭을 사용하여 PHZ와 연결됩니다. 다중 지역 아키텍처에서 VPC 간에 트래픽을 라우팅하려면 각 지역의 Transit Gateway를 함께 피어링해야 합니다. 자세한 내용은 다음 블로그를 참조하십시오. [교차 계정 다중 지역 아키텍처를 위한 Route 53 프라이빗 호스팅 영역 사용](#).

트랜짓 게이트웨이 또는 VPC 피어링을 사용하여 서로 다른 지역의 VPC를 서로 라우팅할 수 있습니다. [트랜짓 게이트웨이 피어링에 대해서는 다음 문서를 사용하십시오. 트랜짓 게이트웨이 피어링 첨부 파일](#).

이 예제에서 VPC us-west-1 지역의 Amazon EC2 인스턴스는 PHZ를 사용하여 지역 내 엔드포인트의 사설 IP 주소를 가져오고 Transit Gateway 피어링 또는 us-west-2 VPC 피어링을 통해 지역 VPC로 트래픽을 라우팅합니다. us-west-2 이 아키텍처를 사용하면 트래픽이 AWS 네트워크 내에 남아 있어 EC2 인스턴스가 인터넷을 거치지 않고 VPC 서비스에 us-west-2 안전하게 액세스할 수 있습니다. us-west-1



## 다중 지역 VPC 엔드포인트

### Note

리전 간 엔드포인트에 액세스할 때는 리전 간 데이터 전송 요금이 적용됩니다.

위 그림을 참조하면 리전의 VPC에 엔드포인트 서비스가 생성됩니다. us-west-2 이 엔드포인트 서비스는 해당 지역의 AWS 서비스에 대한 액세스를 제공합니다. 다른 지역 (예:us-east-1) 의 인스턴스가 해당 지역의 엔드포인트에 액세스하려면 원하는 VPC 엔드포인트의 별칭을 사용하여 PHZ에 주소 레코드를 생성해야 합니다. us-west-2

먼저, 각 지역의 VPC가 생성한 PHZ와 연결되어 있는지 확인하십시오.

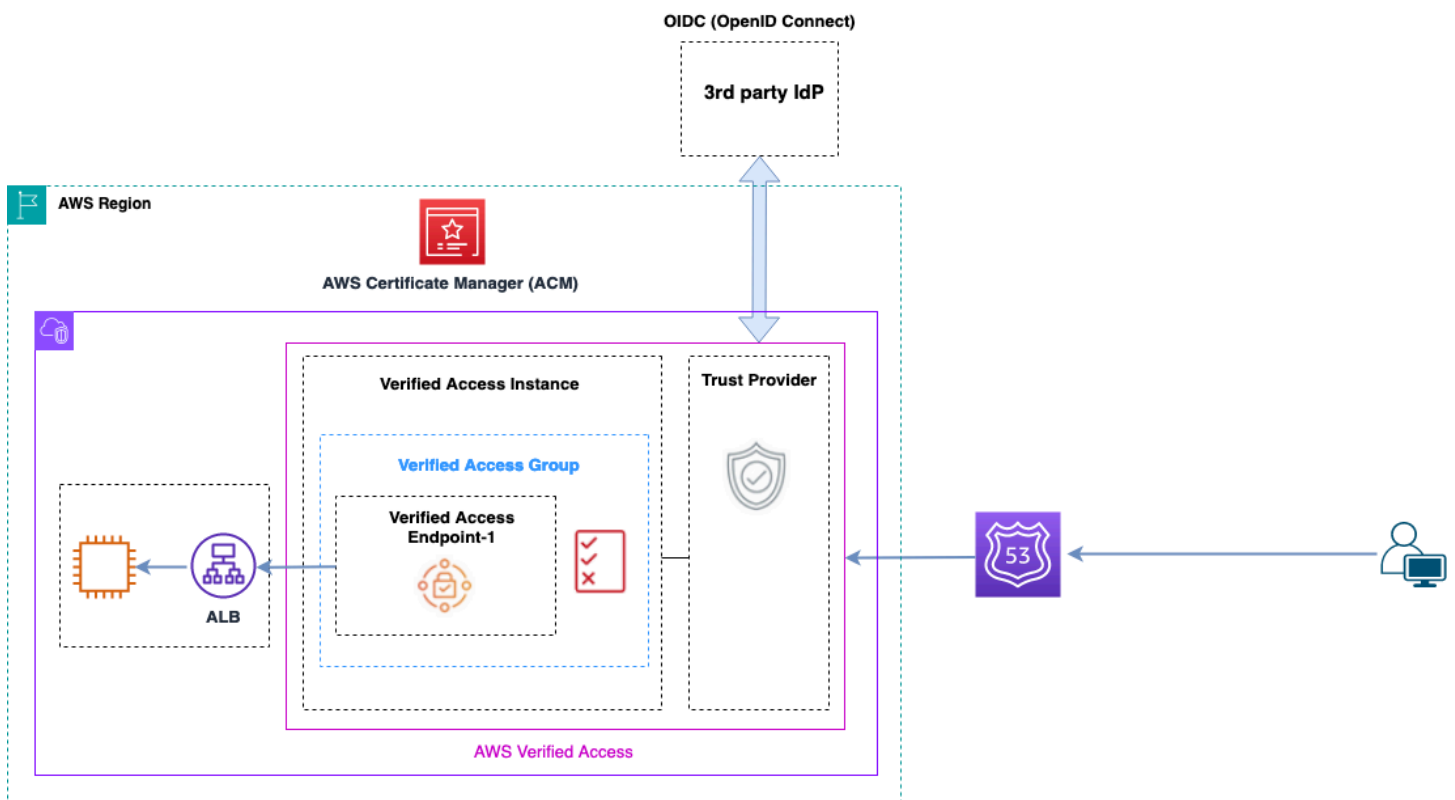
여러 가용 영역에 엔드포인트를 배포할 때 DNS에서 반환되는 엔드포인트의 IP 주소는 할당된 가용 영역의 모든 서브넷에서 가져온 것입니다.

엔드포인트를 호출할 때는 PHZ에 있는 FQDN (정규화된 도메인 이름) 을 사용하십시오.

## AWS Verified Access

AWS Verified Access VPN 없이 사설망의 애플리케이션에 안전하게 액세스할 수 있습니다. ID, 장치, 위치와 같은 요청을 실시간으로 평가합니다. 이 서비스는 애플리케이션 정책에 따라 액세스 권한을 부여하고 조직의 보안을 개선하여 사용자를 연결합니다. Verified Access는 ID를 인식하는 역방향 프록시 역할을 하여 개인 애플리케이션에 대한 액세스를 제공합니다. 해당하는 경우 사용자 ID 및 장치 상태는 트래픽을 애플리케이션으로 라우팅하기 전에 수행됩니다.

다음은 Verified Access의 중요한 개요를 설명하는 다이어그램입니다. 사용자가 애플리케이션 액세스 요청을 보냅니다. Verified Access는 그룹에 대한 액세스 정책 및 애플리케이션별 엔드포인트 정책을 기준으로 요청을 평가합니다. 액세스가 허용되면 해당 요청이 엔드포인트를 통해 애플리케이션에 전송됩니다.



### 검증된 액세스 개요

AWS Verified Access 아키텍처의 주요 구성 요소는 다음과 같습니다.

- **Verified Access 인스턴스** - 인스턴스는 애플리케이션 요청을 평가하여 보안 요구 사항이 충족되는 경우에만 액세스를 부여합니다.
- **Verified Access 엔드포인트** - 각 엔드포인트는 애플리케이션을 나타냅니다. 엔드포인트는 NLB, ALB 또는 네트워크 인터페이스일 수 있습니다.

- Verified-Access 그룹 – Verified-Access 엔드포인트의 모음입니다. 정책 관리를 단순화하려면 보안 요구 사항이 비슷한 애플리케이션의 엔드포인트를 그룹화하는 것이 좋습니다.
- 액세스 정책 - 애플리케이션에 대한 액세스를 허용할지 거부할지를 결정하는 사용자 정의 규칙 집합입니다.
- 신뢰 제공자 - Verified Access는 사용자 ID 및 장치 보안 상태를 쉽게 관리할 수 있는 서비스입니다. 타사 신뢰 제공자 AWS 모두와 호환되므로 각 Verified Access 인스턴스에 하나 이상의 신뢰 공급자를 연결해야 합니다. 이러한 각 인스턴스에는 단일 ID 신뢰 공급자뿐만 아니라 여러 장치 신뢰 공급자가 포함될 수 있습니다.
- 신뢰 데이터 — 응용 프로그램 요청이 수신될 때마다 신뢰 제공자가 Verified Access에 보내는 보안 데이터 (예: 사용자의 이메일 주소 또는 사용자가 속한 그룹) 를 액세스 정책에 따라 평가합니다.

자세한 내용은 [Verified Access 블로그 게시물에서](#) 확인할 수 있습니다.

## 결론

AWS 랜딩 존에서 애플리케이션 사용량을 AWS 확장하고 애플리케이션을 배포하면 VPC와 네트워킹 구성 요소의 수가 늘어납니다. 이 백서에서는 이렇게 성장하는 인프라를 관리하여 비용을 낮게 유지하면서 확장성, 고가용성 및 보안을 보장하는 방법을 설명했습니다. Transit Gateway, 공유 VPC, AWS Direct Connect VPC 엔드포인트, 게이트웨이 로드 밸런서, AWS Network Firewall Amazon Route 53 및 타사 소프트웨어 어플라이언스와 같은 서비스를 사용할 때는 올바른 설계 결정을 내리는 것이 매우 중요합니다. 각 접근 방식의 주요 고려 사항을 이해하고 요구 사항부터 거꾸로 검토하여 자신에게 가장 적합한 옵션 또는 옵션 조합을 분석하는 것이 중요합니다.

# 기여자

다음 개인이 이 문서에 기여했습니다.

- 소하이브 타히르, 솔루션스 아키텍트, Amazon Web Services
- 시린 밤바니, 솔루션스 아키텍트, Amazon Web Services
- 쿠날 판사리, 솔루션스 아키텍트, Amazon Web Services
- 에릭 바스케즈, 솔루션스 아키텍트, Amazon Web Services
- 투샤르 재그데일, 솔루션스 아키텍트, Amazon Web Services
- 아미어 샤리프, 솔루션스 아키텍트, Amazon Web Services
- 글렌 데이비스, 솔루션스 아키텍트, Amazon Web Services
- 닉 나이브턴, 솔루션스 아키텍트, Amazon Web Services
- 싯다르타 차우한, 아마존 웹 서비스 수석 솔루션 아키텍트

## 문서 이력

이 백서에 대한 업데이트 알림을 받으려면 RSS 피드를 구독하면 됩니다.

변경 사항	설명	날짜
<a href="#">메이저 업데이트</a>	CloudWAN, Amazon VPC Lattice, ENA 익스프레스, 하 이브리드 연결, AWS Direct Connect 사이트링크, 딥 패킷 검사 등에 대한 변경 사항이 백서 전체에 걸쳐 업데이트되었습니다. AWS Verified Access	2024년 4월 17일
<a href="#">마이너 업데이트</a>	다이어그램을 보다 일관되게 업데이트하고, 사설 IP VPN을 포함하도록 DX 연결 옵션을 업데이트했으며, 전체적으로 사소한 변경 사항이 많았습니다.	2023년 7월 6일
<a href="#">마이너 업데이트</a>	AWS Control Tower 정보 업데이트, 다양한 서비스에 대한 새로운 처리량 제한 반영, NAT 게이트웨이 다이어그램 업데이트, 중앙 집중식 송신을 위한 보안 섹션 업데이트	2023년 4월 4일
<a href="#">마이너 업데이트</a>	섹션 추가: 지역 간 엔드포인트 액세스.	2022년 7월 19일
<a href="#">메이저 업데이트</a>	Transit Gateway Connect로 Transit Gateway 섹션 업데이트, 트랜짓 VPC AWS Direct Connect 섹션 업데이트, MACsec 및 복원력 권장 사항으로 섹션 업데이트, 섹션 업데이트 AWS PrivateLink VPC 피	2022년 2월 22일



어링과 트랜짓 VPC와 Transit Gateway 비교 표 추가, 중앙 집중식 인바운드 검사 섹션 추가, VPC의 VPC 간 및 VPC-온프레미스의 VPC에 대한 중앙 집중식 네트워크 보안 및 Gateway Load Balancer 설계 패턴을 AWS Network Firewall 통한 중앙 집중식 인터넷 송신을 업데이트하고 프라이빗 NAT 게이트웨이 및 Amazon Route 53 DNS 방화벽 섹션을 추가했습니다.

### [마이너 업데이트](#)

Transit Gateway와 VPC 피어링 섹션 업데이트

2021년 4월 2일

### [백서 업데이트](#)

그림 7에 표시된 옵션과 일치하도록 텍스트를 수정했습니다.

2020년 6월 10일

### [최초 게시](#)

백서가 게시되었습니다.

2019년 11월 15일

## 고지 사항

고객은 본 문서에 포함된 정보를 독자적으로 평가할 책임이 있습니다. 본 문서는 (a) 정보 제공만을 위한 것이며, (b) 사전 고지 없이 변경될 수 있는 현재의 AWS 제품 제공 서비스 및 사례를 보여 주며, (c) AWS 및 자회사, 공급업체 또는 라이선스 제공자로부터 어떠한 약정 또는 보증도 하지 않습니다. AWS 제품 또는 서비스는 명시적이든 묵시적이든 어떠한 종류의 보증, 진술 또는 조건 없이 '있는 그대로' 제공됩니다. 고객에 대한 AWS의 책임과 법적 책임은 AWS 계약서에 준하며 본 문서는 AWS와 고객 간의 계약에 포함되지 않고 계약을 변경하지도 않습니다.

© 2019 Amazon Web Services, Inc. or its affiliates. All rights reserved.

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.