

# IWAN 및 PfRv3 소개

## 목차

[소개](#)

[IWAN](#)

[DMVPN을 사용하는 이유](#)

[전송 독립 설계\(듀얼 DMVPN\)](#)

[설계 요약](#)

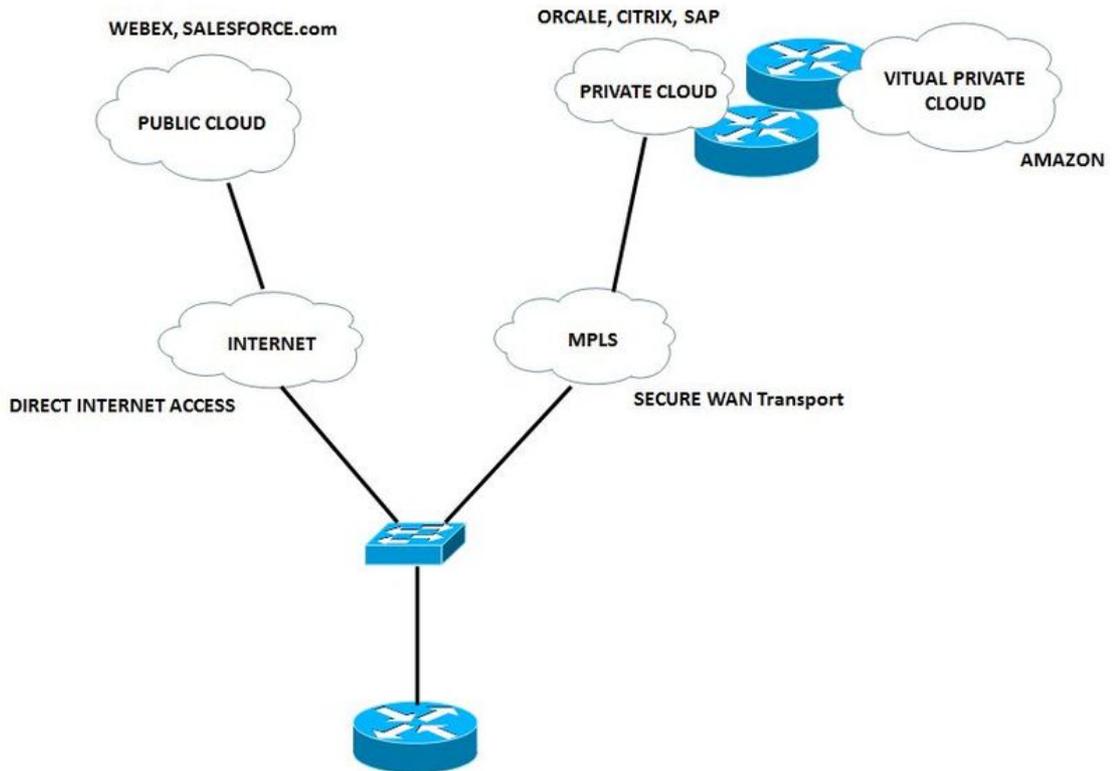
[DMVPN 단계 요약](#)

## 소개

이 문서에서는 Cisco IWAN(Intelligent WAN) 및 Cisco Performance Routing(PfR)에 대해 설명합니다.

## IWAN

Cisco IWAN은 협업 및 클라우드 애플리케이션 성능을 개선하는 동시에 WAN의 운영 비용을 절감하는 시스템입니다. IWAN 솔루션은 지능적인 경로 제어, 애플리케이션 최적화, 인터넷 및 지사 위치에 대한 보안 연결 기능을 갖춘 전송 독립적인 WAN을 구축하려는 조직에 대한 설계 및 구현 지침을 제공하며 WAN의 운영 비용을 절감합니다. IWAN은 프리미엄 WAN과 비용 효율적인 인터넷 서비스를 최대한 활용하여 협업 또는 클라우드 기반 애플리케이션의 성능, 신뢰성 또는 보안의 저하 없이 대역폭 용량을 늘립니다. 조직은 IWAN을 사용하여 인터넷을 WAN 전송으로 활용하고 퍼블릭 클라우드 애플리케이션에 직접 액세스할 수 있습니다.



R1은 음성 및 비디오 트래픽이 사용 가능한 두 링크 중 지연, 지터 및/또는 손실이 상대적으로 적은 상태에서 최상의 경로를 선택하기를 선호합니다. 다른 트래픽은 대역폭을 최대화하기 위해 로드 밸런싱됩니다.

현재 경로가 MPLS(Multiprotocol Label Switching)의 등급을 떨어뜨린 다음 DIA(Direct Internet Access) 링크를 선택하면 음성 및 비디오가 라우팅됩니다.

IWAN을 통해 다음을 수행할 수 있습니다.

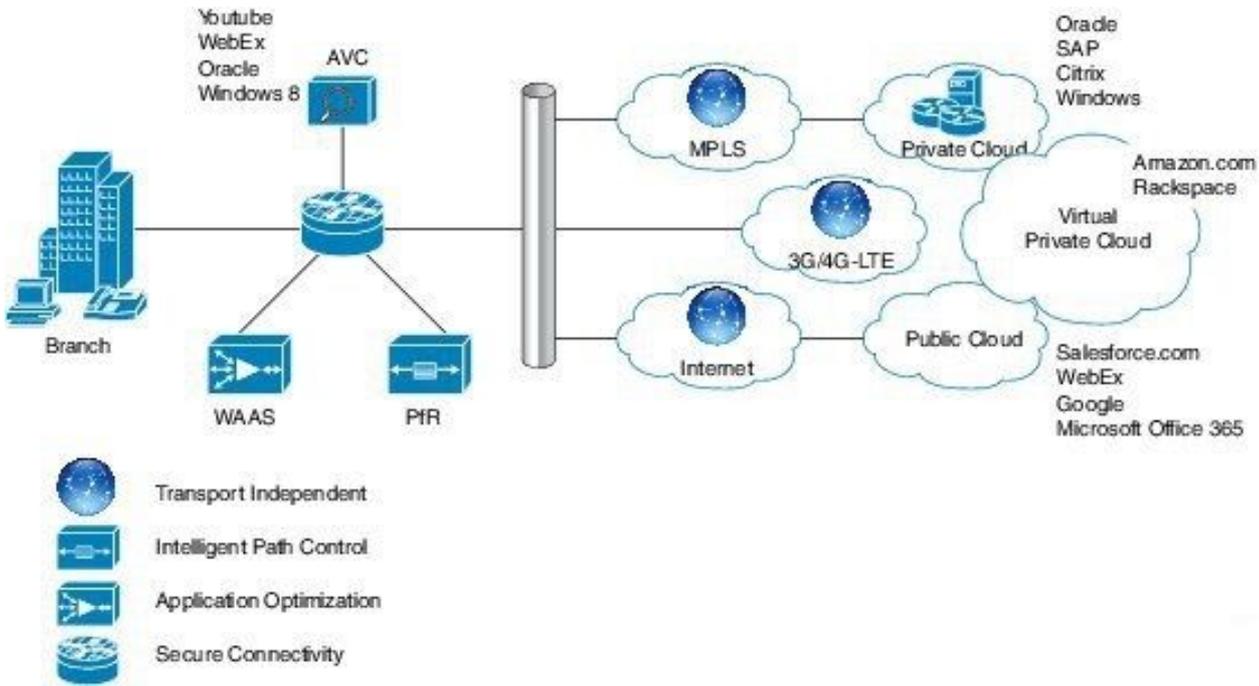
- 덜 중요한 데이터를 위해 더 저렴한 비용으로 인터넷에 연결합니다.
- WAN이 애플리케이션 최적화, 지능형 캐싱 및 매우 안전한 DIA를 사용할 수 있도록 합니다.

지금까지는 예측 가능한 성능을 통해 안정적인 연결을 얻을 수 있는 유일한 방법은 MPLS 또는 임대 회선 서비스를 사용하는 프라이빗 WAN을 활용하는 것입니다. 그러나 통신 사업자 기반 MPLS 및 임대 회선 서비스는 비용이 많이 들고 조직이 원격 사이트 연결에 대한 증가하는 대역폭 요구 사항을 지원하기 위해 WAN 전송에 사용하는 것이 비용 효율적이지 않을 수 있습니다. 조직은 원격 사이트에 대한 네트워크 전송을 적절하게 제공하면서 운영 예산을 줄일 방법을 찾고 있습니다.

IWAN을 통해 조직은 모든 연결에서 최고의 환경을 제공할 수 있습니다. Cisco IWAN을 통해 IT 조직은 성능, 보안 또는 신뢰성에 영향을 주지 않으면서 저렴한 WAN 전송 옵션을 통해 지사 연결에 더 많은 대역폭을 제공할 수 있습니다. IWAN 솔루션을 사용하면 트래픽이 SLA(Application Service-Level Agreement), 엔드포인트 유형 및 네트워크 조건에 따라 동적으로 라우팅되어 최상의 품질 환경을 제공합니다.

IWAN을 사용하면 비디오, VDI(가상 데스크톱 인프라), 게스트 Wi-Fi 서비스 등 대역폭 집약적인 애플리케이션을 신속하게 배포할 수 있습니다. MPLS, 인터넷, 셀룰러, 하이브리드 WAN 액세스 모델 등 어떤 전송 모델을 선호하든 상관없습니다.

이 그림에는 IWAN 솔루션의 구성 요소가 요약되어 있습니다. 성능 라우팅은 이 이니셔티브의 핵심 요소입니다.



IWAN의 4가지 구성 요소는 다음과 같습니다.

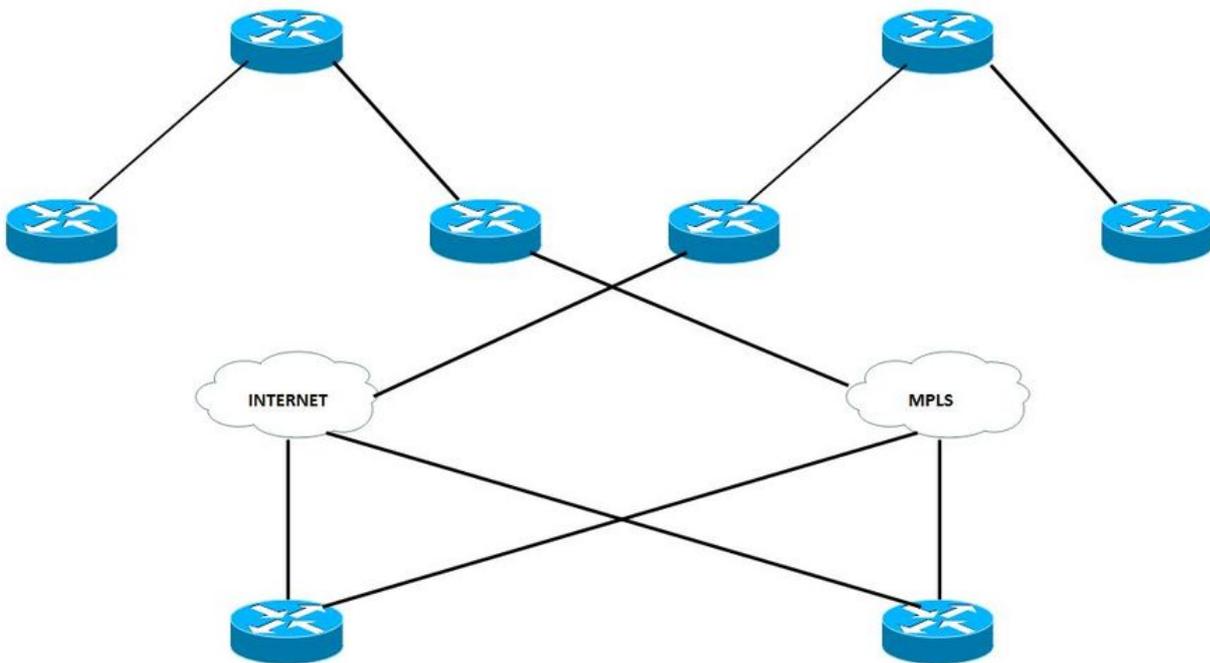
- 안전하고 유연한 전송 독립적 설계** - DMVPN(Dynamic Multipoint VPN) IWAN은 MPLS, 광대역 및 셀룰러 3G/4G/LTE를 포함한 모든 캐리어 서비스 오퍼링을 통해 간편한 멀티 홈 기능을 제공합니다. 기술:DMVPN/IPsec 오버레이 설계
- 지능형 경로 제어** - Cisco PFR을 통해 이 구성 요소는 애플리케이션 전달 및 WAN 효율성을 개선합니다.PFR은 애플리케이션 유형, 성능, 정책 및 경로 상태를 확인하여 데이터 패킷 포워딩 결정을 동적으로 제어합니다.PFR은 애플리케이션 정책에 따라 최상의 수행 경로를 통해 트래픽을 지능적으로 로드 밸런싱하면서 WAN 성능을 변화시키는 것을 비즈니스 애플리케이션을 보호합니다.PFR은 네트워크 성능(지터, 패킷 손실, 지연)을 모니터링하고 애플리케이션 정책에 따라 최상의 수행 경로를 통해 중요한 애플리케이션을 전달하기로 결정합니다.Cisco PFR은 광대역 서비스에 연결하는 보더 라우터와 라우터의 Cisco IOS® Software에서 지원하는 기본 컨트롤러 애플리케이션으로 구성됩니다.보더 라우터는 트래픽과 경로 정보를 수집하고 이를 기본 컨트롤러로 전송합니다. 이 컨트롤러는 애플리케이션 요구 사항에 맞게 서비스 정책을 탐지하고 적용합니다.Cisco PFR은 회사의 전반적인 커뮤니케이션 비용을 줄이기 위해 회로 비용을 기준으로 트래픽을 지능적으로 로드 밸런싱할 이그레스 WAN 경로를 선택할 수 있습니다 .IWAN 지능형 경로 제어는 인터넷 전송을 통해 비즈니스급 WAN을 제공하는 핵심입니다. 기술 :PFR.PFR은 PFRv3라는 주요 새 릴리스로 진화합니다.
- 애플리케이션 최적화** - Cisco AVC(Application Visibility and Control) 및 Cisco WAAS(Wide Area Application Services)는 WAN을 통한 애플리케이션 성능 가시성 및 최적화를 제공합니다 .HTTP(포트 80)와 같이 잘 알려진 포트의 재사용이 증가함에 따라 애플리케이션이 점점 더 불명확해지는 상황에서 애플리케이션의 정적 포트 분류만으로는 충분하지 않습니다.Cisco AVC는 애플리케이션의 성능을 식별하고 모니터링하기 위해 트래픽에 대한 심층 패킷 검사를 통해 애플리케이션 인식을 제공합니다.애플리케이션 레벨(레이어 7)에서의 가시성 및 제어는 NBAR2(Network-Based Application Recognition 2), NetFlow, QoS(Quality of Service), 성능 모니터링, Medianet 등과 같은 AVC 기술을 통해 제공됩니다. 기술:AVC(Application Visibility and Control), WAAS, Akamai Connect
- 보안 연결** - WAN을 보호하고 사용자 트래픽을 인터넷으로 직접 오프로드합니다.강력한 IPsec 암호화, 영역 기반 방화벽 및 엄격한 액세스 목록을 사용하여 공용 인터넷을 통해 WAN을 보호

합니다.지사 사용자를 인터넷에 직접 라우팅하면 퍼블릭 클라우드 애플리케이션 성능이 향상되는 동시에 WAN을 통한 트래픽이 줄어듭니다.Cisco CWS(Cloud Web Security) 서비스는 인터넷에 액세스하는 사용자 트래픽을 중앙 집중식으로 관리하고 보호하는 클라우드 기반 웹 프록시를 제공합니다. 기술:Cisco IOS Firewall/IPS, CWS(Cloud Web Security)

## DMVPN을 사용하는 이유

IWAN은 DMVPN을 기반으로 하는 하이브리드 전송 독립 설계와 함께 규범적 설계를 사용합니다. DMVPN은 MPLS 및 인터넷 전송 전반에 구축됩니다.이렇게 하면 두 전송을 모두 포함하는 단일 라우팅 도메인을 사용하여 라우팅이 크게 간소화됩니다. DMVPN 라우터는 IP 유니캐스트뿐 아니라 동적 라우팅 프로토콜의 사용을 포함하는 IP 멀티캐스트 및 브로드캐스트 트래픽을 지원하는 터널 인터페이스를 사용합니다. 초기 spoke-to-hub 터널이 활성화되면 Site-to-Site IP 트래픽 플로우에 필요한 경우 동적 스포크 투 스포크 터널을 생성할 수 있습니다.

Transport Independent Design은 제공업체당 하나의 DMVPN 클라우드를 기반으로 합니다. 이 설명서에서는 두 개의 제공자를 사용하고, 하나는 기본(MPLS)으로 간주하며, 다른 하나는 보조(인터넷)로 간주됩니다. 브랜치 사이트는 DMVPN 클라우드 모두에 연결되고 두 터널이 모두 가동됩니다.



다이어그램에 나와 있는 것처럼 각 브랜치 라우터는 두 제공자에 연결되며, 하나는 기본 MPLS이고 다른 하나는 보조 인터넷입니다.

트래픽 유형에 따라 각 제공자가 트래픽을 전송하는 데 사용됩니다. 예를 들어, 우선 순위가 더 높은 데이터는 MPLS를 통해 전송할 수 있으며 우선 순위가 더 낮은 데이터는 인터넷을 통해 라우팅할 수 있습니다. 이를 통해 더 비용 효율적으로 사용할 수 있으며, 더 혁신적인 비즈니스 목적으로 가용 리소스를 활용할 수 있습니다.

## 전송 독립 설계(듀얼 DMVPN)

### 설계 요약

이 설계에서는 DMVPN을 최대한 활용하여 일관성 있는 IPsec 오버레이를 위한 액티브-액티브 WAN 경로를 제공합니다. MPLS 및 인터넷 연결은 단일 라우터에서 종료하거나 별도의 두 라우터에서 종료하여 복원력을 강화할 수 있습니다. 동일한 설계를 MPLS, 인터넷 또는 3G/4G 전송에서 사용할 수 있으므로 설계 전송에 독립적입니다.

제공자당 DMVPN 허브(PfRv3 BR)를 사용하고 허브에서 전송하는 것이 좋습니다. 따라서 라우팅 컨피그레이션이 훨씬 쉬워집니다.

DMVPN에서는 DPD(Dead Peer Detection)에 대한 IKEv2(Internet Key Management Protocol version 2) keepalive 간격을 사용해야 합니다. 이는 빠른 재컨버전스를 촉진하고 DMVPN 허브가 다시 로드되는 경우 스포크 등록이 제대로 작동하기 위해 필수적입니다. 이 설계를 통해 스포크는 암호화 피어가 실패했으며 해당 피어가 있는 IKEv2 세션이 오래된 상태임을 탐지하여 새 세션을 생성할 수 있습니다. DPD가 없으면 IPsec SA는 시간 초과(기본값은 60분)여야 하며, 라우터가 새 SA를 재협상할 수 없는 경우 새 IKEv2 세션이 시작됩니다. 최대 대기 시간은 약 60분입니다.

## DMVPN 단계 요약

DMVPN에는 여기에 요약된 여러 단계가 있습니다.

DMVPN 1단계는 허브 및 스포크 기능을 기반으로 합니다.

- 허브의 간소화되고 작은 구성
- 동적으로 CPE(NAT) 지원
- 라우팅 프로토콜 및 멀티캐스트 지원
- 스포크는 전체 라우팅 테이블이 필요하지 않으며 허브에서 요약할 수 있습니다.

DMVPN 2단계에서는 허브에 요약 기능이 없습니다.

각 스포크에는 각 스포크 대상 접두사에 대한 next-hop(스포크 주소)이 있습니다.

PfR에는 동적 PBR 및 올바른 next-hop 정보로 경로를 적용하는 모든 정보가 있습니다.

DMVPN 3단계에서는 경로 요약을 허용합니다.

- 상위 경로 조회를 수행하면 허브에 대한 경로만 사용할 수 있습니다.
- NHRP는 바로 가기 터널을 동적으로 설치하여 RIB/CEF를 채웁니다.
- PfR은 여전히 허브 next-hop 정보를 가지고 있으며 현재 next-hop 변경 사항을 알지 못합니다.

PfRv3는 모든 DMVPN 단계를 지원합니다.

DMVPN에 대한 자세한 내용은 [Cisco IOS DMVPN 개요를 참조하십시오](#).