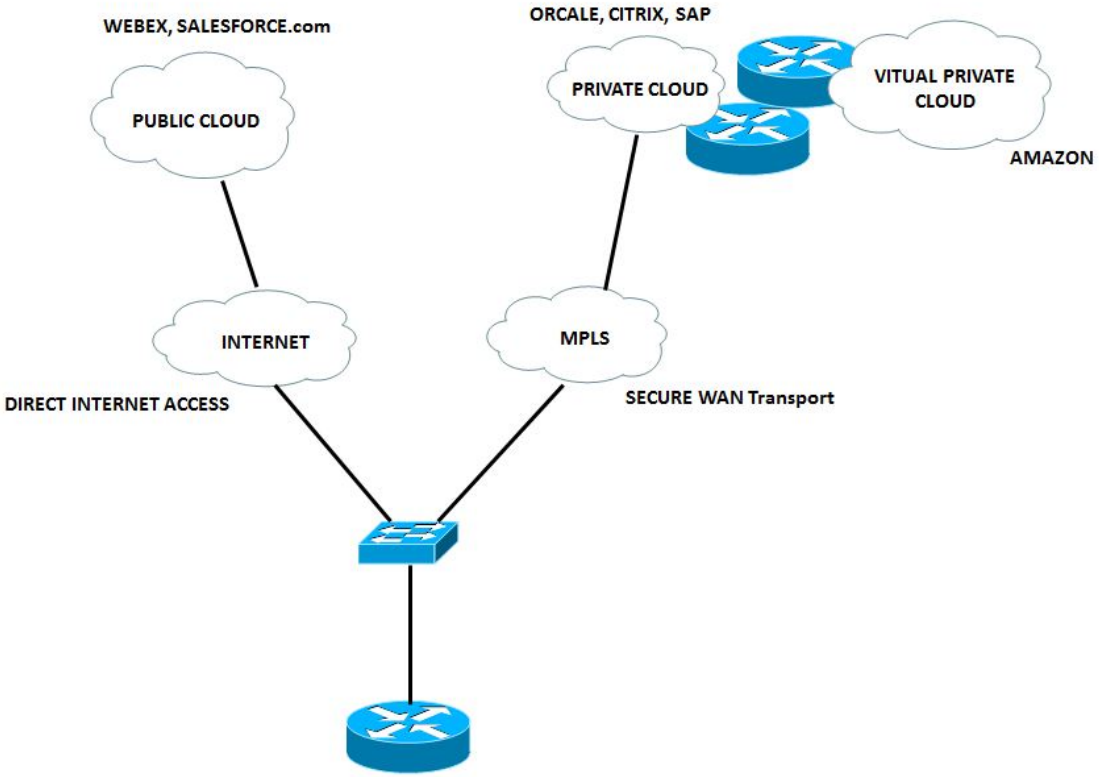
IWAN および PfRv3 の概要

目次

IWAN

シスコ インテリジェント WAN (IWAN) は、WAN の運用コストを削減すると同時にコラボレーションとクラウド アプリケーションのパフォーマンスを向上させるシステムです。 IWAN ソリューションは、WAN の運用コストを抑えると同時に、インテリジェントなパス制御やアプリケーションの最適化、インターネットや拠点へのセキュアな接続機能を備えた独立 WAN の導入を検討している企業に、設計や導入のためのガイドラインを提供します。 IWAN は、コラボレーション アプリケーションやクラウド ベースのアプリケーションのパフォーマンス、信頼性、安全性を損なうことなく、プレミアム WAN とコスト効率に優れたインターネット サービスを最大限活用し、帯域幅キャパシティを増加させます。 組織は、WAN トランスポートとしてインターネットを活用するだけでなく、パブリック クラウド アプリケーションに直接アクセスするために IWAN を使用できます。



R1 は、音声およびビデオ トラフィックを優先し、利用可能な 2 つのリンクのうち、遅延、ジッター、損失が相対的に少ない最良のパスを取ります。 他のトラフィックは、帯域幅を最大限に活用できるようにロード バランシングされます。

音声とビデオは、現在のパスが品質低下 (MPLS) した場合に再ルーティングされ、その後 DIA リンクが選択されます。

IWAN を導入すると次のことが可能になります。

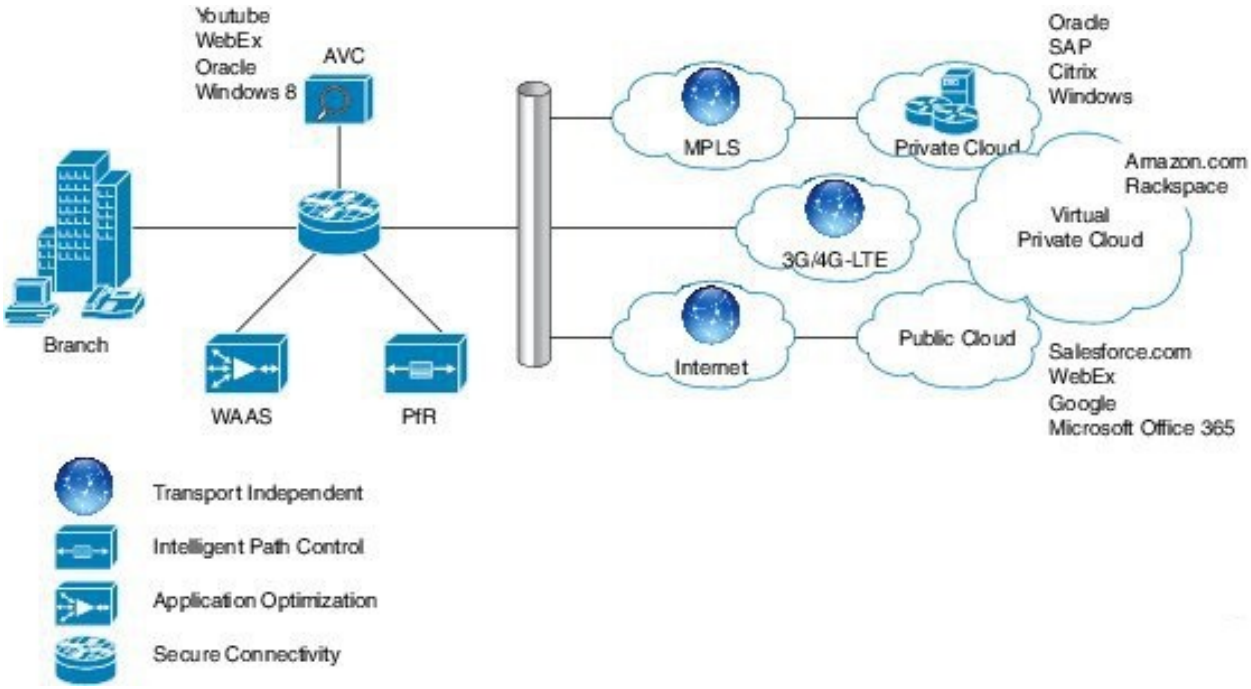
- 重要度の低いデータは、インターネットなどの低コストのモードに接続します。
- アプリケーション最適化、インテリジェント キャッシュ、および高いセキュリティを備えたインターネットへの直接アクセスを WAN で使用できるようにします。

これまでは、パフォーマンスが予測可能で信頼性の高い接続を得るには、MPLS または専用回線サービスによるプライベート WAN を利用するしかありませんでした。 しかしキャリアベースの MPLS や専用回線サービスは、リモートサイト接続のための帯域幅拡大に対応するには高額となる場合があり、WAN トランスポートの手段として、必ずしもコスト効率が高いとは言えません。 組織が求めているのは、リモートサイトに適切なネットワーク トランスポートを提供しながら運用予算を削減する方法です。

シスコ インテリジェント WAN（IWAN）の導入により、組織はどのような接続環境でも妥協のないエクスペリエンスを提供できるようになります。 Cisco IWAN では、パフォーマンス、セキュリティ、および信頼性を損なわずに低コストの WAN トランスポート オプションを利用できるため、ブランチ オフィス接続の帯域幅を増やすことが可能です。 IWAN ソリューションにより、トラフィックはアプリケーション サービスレベル契約（SLA）、エンドポイント タイプ、およびネットワークの状態に基づいて動的にルーティングされ、最適な品質が提供されます。

IWAN を使用すると、ビデオ、仮想デスクトップ インフラストラクチャ（VDI）、ゲスト Wi-Fi サービスなど、帯域幅の負荷の高いアプリケーションでも迅速に展開できます。 さらに、マルチプロトコル ラベル スイッチング（MPLS）、インターネット、セルラー、またはハイブリッド WAN アクセス モデルなど、あらゆるトランスポート モデルを使用できます。

次の図は、IWAN ソリューションのコンポーネントの概要を示しています。 パフォーマンス ルーティングは、この構想を支える重要な要素です。



シスコ インテリジェント WAN には次の 4 つの特長があります。

- **安全で柔軟な、トランスポートに依存しない設計**： Dynamic Multipoint VPN（DMVPN）を使用することで、マルチプロトコル ラベル スイッチング（MPLS）、ブロードバンド、セルラー 3G/4G/LTE など、あらゆるキャリア サービスでマルチホーミング機能が簡単に実現します。

- テクノロジー： DMVPN/IPsec オーバーレイ設計

- **インテリジェント パス制御： Cisco Performance Routing（PfR）**を使用することで、このコンポーネントでのアプリケーション配信と WAN の効率性が向上します。 PfR は、アプリケーションのタイプ、パフォーマンス、ポリシー、およびパスのステータスに基づいて、データ パケット転送の決定を動的に制御します。 PfR は、アプリケーション ポリシーに基づき、パフォーマンスが最良のパス上でインテリジェントにトラフィックのロードバランシングを実現するだけでなく、WAN のパフォーマンスの変動からビジネス アプリケーションを保護します。 PfR はネットワーク パフォーマンス（ジッター、パケット損失、遅延）を監視し、アプリケーション ポリシーに基づいて、重要なアプリケーションを最もパフォーマンスに優れたパスを利用して転送するよう決定します。 Cisco PfR は、ブロードバンド サービスに接続するボーダルータ（BR）、およびルータ上の Cisco IOS® ソフトウェアでサポートされるマスター コントローラ アプリケーションで構成されます。 ボーダルータは、トラフィックとパスの情報を収集してマスター コントローラに送信します。マスター コントローラは、アプリケーションの要件に合わせて、サービス ポリシーを適用します。 Cisco PfR では、回線コストに基づいてインテリジェントにロード バランシングされたトラフィックに対して出力側 WAN パスを選択し、全社的な通信費用を削減できます。 IWAN のインテリジェントなパス制御は、インターネット トランスポートでビジネスクラスの WAN を実現する鍵になります。 テクノロジー： パフォーマンス ルーティング（PfR）。 PfR は、PfRv3 と呼ばれる主要な新リリースに進化します。

- **アプリケーションの最適化**： Cisco Application Visibility and Control（AVC）と Cisco Wide Area Application Services（WAAS）は、WAN におけるアプリケーション パフォーマンスの可視化と最適化を実現します。 HTTP（ポート 80）などウェルノウン ポートの再利用が増大したために、アプリケーションの不透明性が高まり、アプリケーションのポートをスタティックに分類することでは対応できなくなっています。 Cisco AVC では、トラフィックのディープ パケット インスペクションによるアプリケーションの識別によって、アプリケーションのパフォーマンスの特定と監視が可能になります。 Network-Based Application Recognition 2（NBAR2）、NetFlow、Quality of Service（QoS）、パフォーマンス モニタリング、メディアネットなどの AVC テクノロジーを通じて、アプリケーション レベル（レイヤ 7）での可視性や制御を提供します。 テクノロジー： Application Visibility and Control（AVC）、WAAS、Akamai Connect

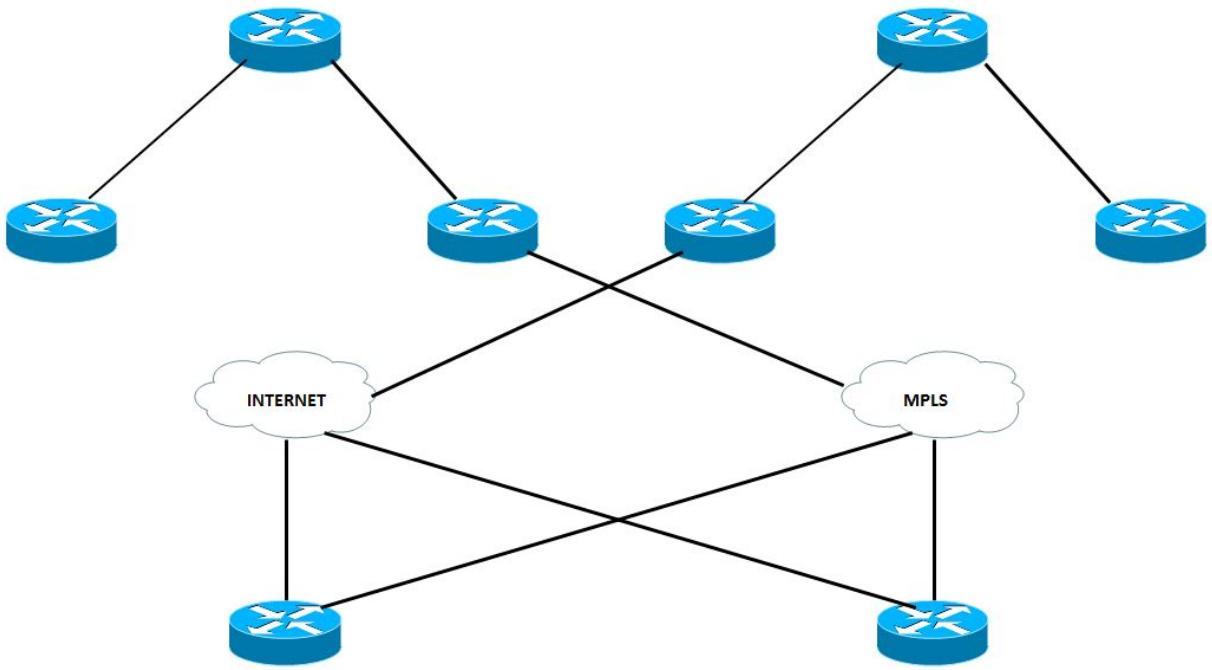
- **セキュアな接続**： これによって WAN を保護し、ユーザ トラフィックをインターネットに直接オフロードできます。 強力な IPsec 暗号化、ゾーンベース ファイアウォール、そして厳格なアクセス リストによって、パブリック インターネットを利用した WAN が保護されます。ブランチのユーザをインターネットに直接ルーティングすることで、WAN のトラフィックが軽減され、パブリック クラウド アプリケーションのパフォーマンスが向上します。 Cisco Cloud Web Security（CWS）サービスは、インターネットにアクセスするユーザ トラフィックの一元的な管理とセキュリティ保護が可能な、クラウドベースの Web プロキシを提供します。 テクノロジー： Cisco IOS Firewall/IPS、Cloud Web Security（CWS）

DMVPN が使用されている理由

IWANは、DMVPN に基づいて、ハイブリッド トランスポートに依存しない設計と規範的なデザインを使用しています。 DMVPN は、MPLS とインターネット トランスポート全体に配備されています。 これは、両方の転送を含む単一のルーティング ドメインを使用して、ルーティングを大幅に簡素化します。 DMVPN ルータは、ダイナミック ルーティング プロトコルの使用を含め、IP ユニキャスト、IP マルチキャスト、およびブロードキャスト トラフィックをサポートするトンネル インターフェイスを使用します。 最初のスポークとハブ間のトンネルがアクティブになる

と、サイト間 IP トラフィック フローで必要な場合に動的なスポーク間トンネルを作成できるようになります。

トランスポート非依存の設計は、プロバイダーごとに 1 つの VPN クラウドに基づいています。このガイドでは 2 つのプロバイダーが使用され、1 つはプライマリ（MPLS）と見なされ、1 つはセカンダリ（インターネット）と見なされて使用されます。 ブランチ サイトは両方の DMVPN クラウドに接続され、両方のトンネルは起動しています。



上記の図で示されるように、各ブランチ ルータは両方のプロバイダーに接続され、1 つはプライマリである MPLS で、他方はセカンダリであるインターネットです。

トラフィックの種類によって、それぞれのプロバイダーがトラフィックを送信するために使用されます。 次に、例を示します。 高い優先度のデータは MPLS を介して送信でき、低い優先度のデータはインターネットを介してルーティングできます。これにより、費用対効果をより高くし、空いているリソースをより革新的なビジネス上の目的のために利用できます。

設計の概要

設計は、一貫性のある IPsec オーバーレイのために、DMVPN を最大限に活用するアクティブ-アクティブの WAN パスを提供します。 MPLS とインターネット接続は、単一のルータ上で終端させるか、追加の復元力を目的とした 2 つの別々のルータ上で終端させることができます。 同じ設計は、MPLS、インターネット、または 3G/4G トランスポート上で使用することができ、トランスポートに依存しない設計を実現します。

ハブのプロバイダーとトランスポートごとに、DMVPN ハブ（PfRv3 BR）を使用することをお勧めします。 これにより、ルーティング設定がさらに容易になります。

DMVPN では、Dead Peer Detection（DPD; デッドピア検出）用に、Internet Key Management Protocol バージョン 2（IKEv2）キープアライブ インターバルが必要になります。DPD は、DMVPN ハブが再起動された場合に高速の再コンバージェンスを促進し、スポーク登録が正常に

機能するために不可欠です。 この設計では、スポークが暗号化ピアの障害と、そのピアを使用する IKEv2 セッションが古くなったことを検出でき、それによって新しい IKEv2 セッションを作成できます。 DPD がないと、IPsec の SA がタイムアウトし（デフォルトでは 60 分）、ルータが新しい SA を再ネゴシエーションできない場合には新しい IKEv2 セッションが開始されます。 最大待機時間は約 60 分です。

DMVPN フェーズの概要

DMVPN には、次のように集約された複数のフェーズがあります。

DMVPN フェーズ 1 は、ハブとスポーク機能に基づいています。

- ハブ上の、簡素化されたより小規模な構成
- 動的にアドレスされた CPE（NAT）のサポート
- ルーティング プロトコルとマルチキャストをサポートします。
- スポークはハブに集約でき、完全なルーティング テーブルを必要としません。

DMVPN フェーズ 2 は、ハブには集約されていません。

各スポークには、各スポークの宛先プレフィックスのためのネクストホップ（スポーク アドレス）があります。

PfR には、動的 PBR や適切なネクストホップ情報など、パスを適用するためのすべての情報があります。

DMVPN フェーズ 3 は、ルートの集約を可能にします。

- 親ルート検索が実行される場合、ハブへのルートのみが利用可能です。
- NHRP は動的にショートカット トンネルをインストールして、RIB/CEF への入力を行います。
- PfR はまだハブのネクストホップ情報を持っており、現時点ではネクストホップの変更を認識しません。

PfRv 3 は、すべての DMVPN フェーズをサポートします。

DMVPN の詳細については、次のリンクを参照してください。

http://www.cisco.com/c/dam/en/us/products/collateral/security/dynamic-multipoint-vpn-dmvpn/DMVPN_Overview.pdf