IWANおよびPfRv3の概要

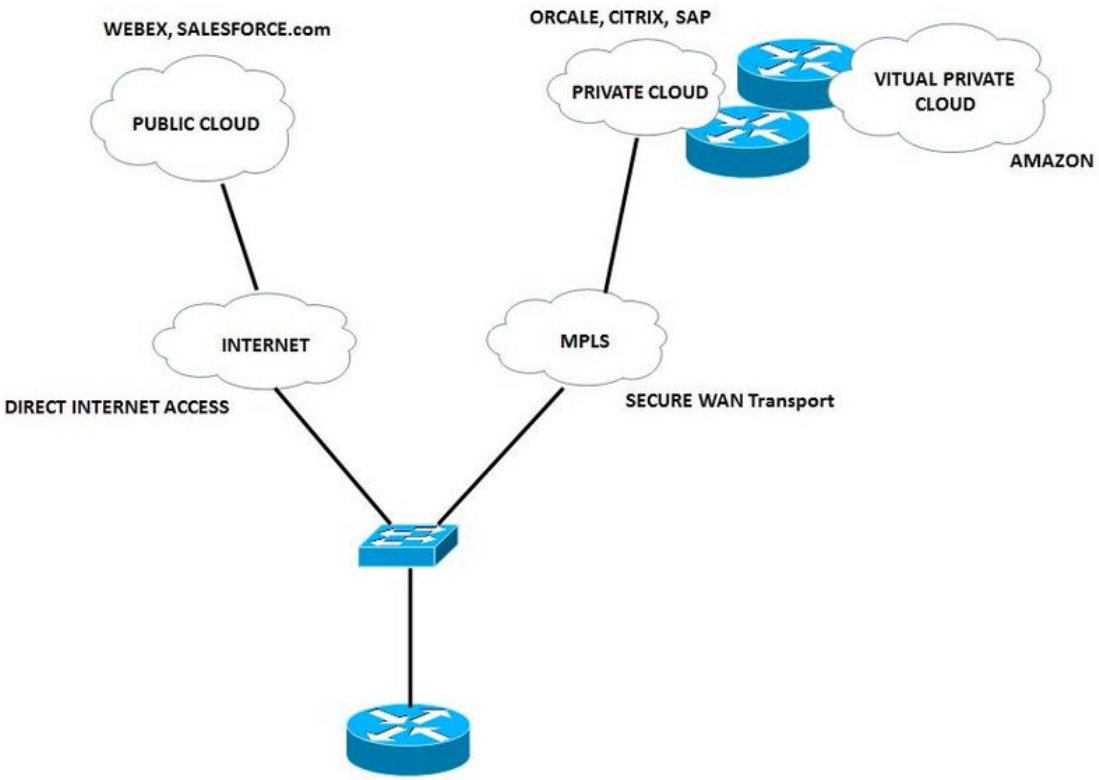
内容

概要

このドキュメントでは、Cisco Intelligent WAN(IWAN)およびCisco Performance Routing(PfR)について説明します。

IWAN

Cisco IWANは、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と同時に、WANの運用コストを削減するシステムです。IWANソリューションは、インテリジェントなパス制御、アプリケーションの最適化、インターネットおよびブランチロケーションへのセキュアな接続を備えたトランスポート非依存WANの導入を目指す組織に設計と実装のガイダンスを提供します。IWANは、プレミアムWANとコスト効率の高いインターネットサービスを最大限に活用し、コラボレーションやクラウドベースアプリケーションのパフォーマンス、信頼性、セキュリティを損なうことなく、帯域幅の容量を増やします。組織は、インターネットをWANトランスポートとして、またパブリッククラウドアプリケーションへの直接アクセスとして活用するために、IWANを使用できます。



R1は、使用可能な2つのリンク間の遅延、ジッタ、損失が比較的少ないベストパスを使用して、音声およびビデオトラフィックを優先します。他のトラフィックは、帯域幅を最大化するためにロードバランシングされます。

現在のパスが劣化した場合(マルチプロトコルラベルスイッチング(MPLS)、音声とビデオが再ルーティングされ、その後でダイレクトインターネットアクセス(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をインターネットとして低コストモードに接続します。
- WANは、アプリケーション最適化、インテリジェントキャッシング、および高度にセキュアなDIAを使用できます。

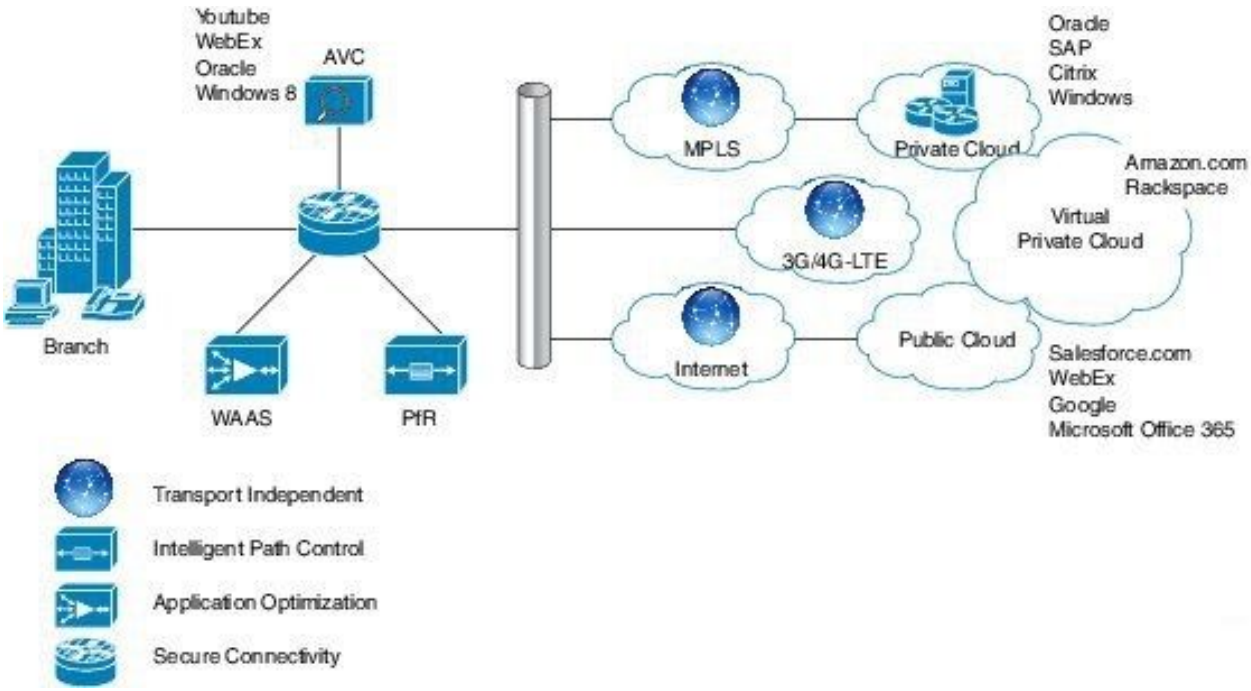
これまでのところ、予測可能なパフォーマンスで信頼性の高い接続を実現する唯一の方法は、MPLSまたは専用回線サービスを使用したプライベートWANを利用することです。ただし、キャリアベースのMPLSおよび専用回線サービスは高価であり、リモートサイト接続の帯域幅要件の増大をサポートするためにWANトランスポートを使用する組織では常にコスト効率が高いとは限りません。企業は、リモートサイトにネットワーク転送を適切に提供しながら、運用予算を削減する方法を探しています。

IWANにより、組織は妥協のないエクスペリエンスをあらゆる接続で提供できます。Cisco IWANにより、IT部門は、パフォーマンス、セキュリティ、信頼性に影響を与えることなく、より安価なWAN転送オプションを使用して、ブランチオフィス接続により多くの帯域幅を提供できます。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。また、MPLS、インターネット、セルラー、ハイブリッドWANアクセスモデルなど、どのトランスポートモデル

を好むかは関係ありません。

この図は、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。



IWANの4つのコンポーネントは次のとおりです。

- **セキュアで柔軟なトランスポート非依存の設計 –** Dynamic Multipoint VPN(DMVPN)IWANは、MPLS、ブロードバンド、およびセルラー3G/4G/LTEを含むキャリアサービス上でマルチホーミングを容易に行える機能を提供します。 テクノロジー：DMVPN/IPsec オーバーレイ設計

- **インテリジェントなパス制御**：シスコPfRを使用すると、アプリケーション配信とWAN効率が向上します。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と、ルータ上のCisco IOS®ソフトウェアでサポートされるプライマリコントローラアプリケーションで構成されます。境界ルータはトラフィックとパス情報を収集し、プライマリコントローラに送信します。プライマリコントローラは、アプリケーション要件に合わせてサービスポリシーを検出して適用します。シスコPfRは、出力WANパスを選択して、回線コストに基づいてトラフィックのロードバランシングをインテリジェントに行うことで、会社の全体的な通信コストを削減できます。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：PfRPfR 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)およびCisco Wide Area Application Services(WAAS)は、WAN上でのアプリケーションパフォーマンスの可視性

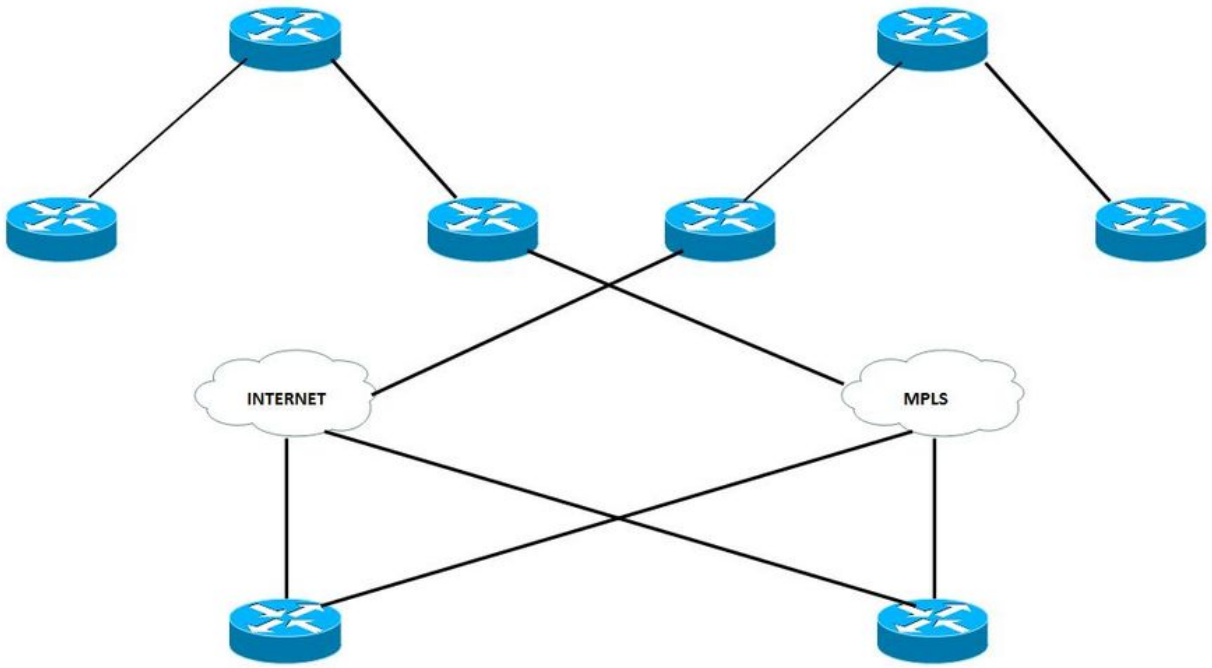
と最適化を提供します。HTTP（ポート 80）などウェルノウン ポートの再利用が増大したために、アプリケーションの不透明性が高まり、アプリケーションのポートをスタティックに分類することでは対応できなくなっています。Cisco AVC では、トラフィックのディープ パケット インスペクションによるアプリケーションの識別によって、アプリケーションのパフォーマンスの特定と監視が可能になります。Network-Based Application Recognition 2（NBAR2）、NetFlow、Quality of Service（QoS）、パフォーマンス モニタリング、メディアネットなどの AVC 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**: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します。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を使用する理由

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む、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つのプロバイダーを使用し、1つはプライマリ(MPLS)、もう1つはセカンダリ（インターネット）と見なされます。 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。



図に示すように、各ブランチルータは両方のプロバイダーに接続されています。1つはプライマリMPLSで、もう1つはセカンダリINTERNETです。

トラフィックのタイプに応じて、各プロバイダーがトラフィックの送信に使用されます。たとえば、優先順位の高いデータはMPLSを介して送信でき、優先順位の低いデータはインターネット経由でルーティングできます。これにより、コスト効率が向上し、利用可能なリソースを解放して、より革新的なビジネス目的で利用できます。

トランスポート非依存設計（デュアルDMVPN）

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。同じ設計をMPLS、インターネット、または3G/4Gトランスポートで使用できるため、トランスポートに依存しません。

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、次に示す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のサポート
- スポークは完全なルーティングテーブルを必要とせず、ハブで集約できる

DMVPNフェーズ2には、ハブでの集約はありません。

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、ダイナミックPBRと正しいネクストホップ情報を使用してパスを適用するためのすべての情報が含まれています。

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。

PfRv3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、『Cisco IOS DMVPNの概要』を参照してください。