IWAN および PfRv3 への紹介

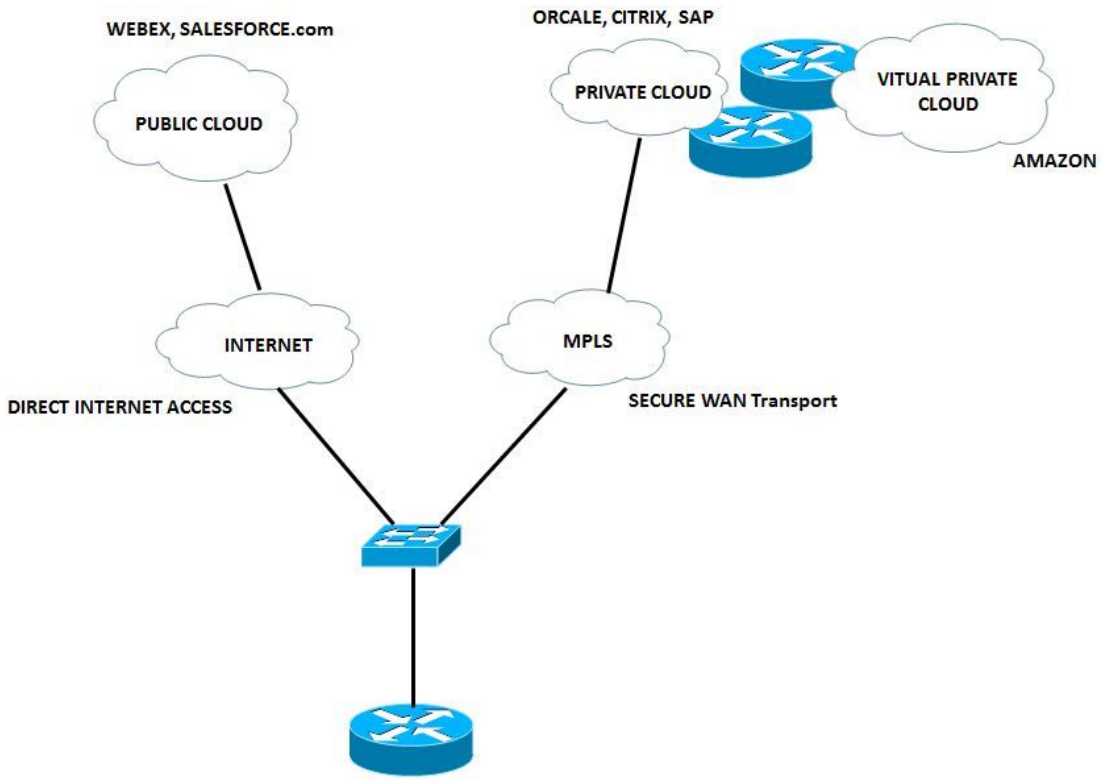
目次

概要

この資料はパフォーマンス ルーティング (PfR) シスコ インテリジェント WAN （ IWAN) および Cisco を記述したものです (PfR) 。

IWAN

また WAN の操業費用を削減するが、コラボレーションおよびクラウド アプリケ– ションパフォーマンスを高める Cisco IWAN はシステムです。 IWAN ソリューションはインターネットおよびブランチの位置にインテリジェント な 経路制御、アプリケーション 最適化およびセキュア接続の転送する依存しない WAN を展開するために検知 する組織に WAN の操業費用を削減する間、設計および実装指導を提供します。 IWAN はコラボレーションまたはクラウド ベースのアプリケーションのパフォーマンス、信頼性、またはセキュリティの侵害なしで帯域幅キャパシティを増加するために事項 WAN および費用効果が高い インターネットサービスを充分に活用します。 組織は公共クラウド アプリケーションに WAN転送として、またダイレクトアクセスのためにインターネットを活用 するために IWAN を使用できます。



R1 は利用可能 なそれへの 2 つのリンク間の比較的選択するために音声およびビデオトラフィックをより少ない遅延、ジッタや損失のベストパスを好みます。 他のトラフィックは帯域幅を最大化するためにバランスをとられるロードです。

現在のパスが低下する場合音声およびビデオは再ルーティングされます（マルチプロトコル ラベル スイッチング（MPLS））そして直接インターネットアクセス（DIA）リンクは選択されます。

IWAN を導入すると次のことが可能になります。

- より少なく重要なデータのためのインターネットとして低価格モードに接続して下さい。
- WAN がアプリケーション 最適化を、インテリジェント な キャッシング使用し、非常に DIA.を保護するようにします。

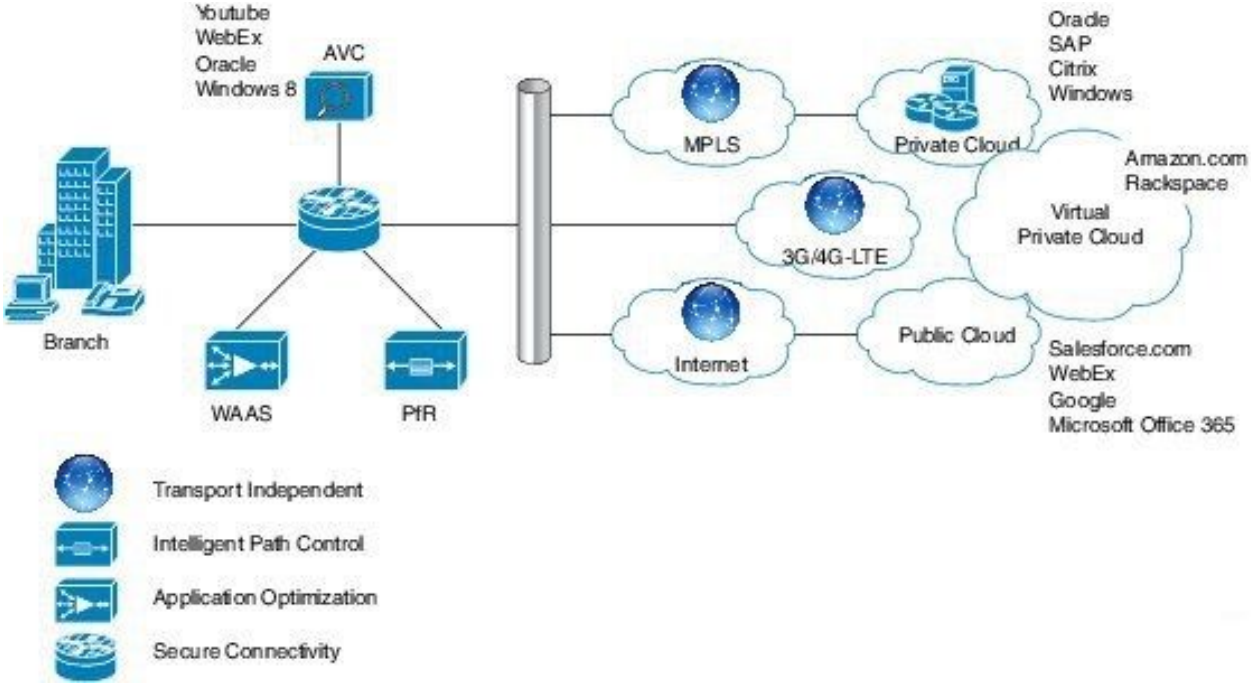
これまでのところ、予想できるパフォーマンスの信頼できる接続を確立する唯一の方法は MPLS か専用回線サービスを使用して private WAN を利用することです。 ただし WAN転送がリモートサイト 接続のための増加する 帯域幅必要条件をサポートすることができるように組織が使用することができるように、キャリア・ベースの MPLS および専用回線サービスは高い常に場合もあり、費用効果が高くない です。 組織はリモートサイトに十分にネットワーク転送を提供している間運営予算案を下げる方法を探します。

IWAN はあらゆる接続上の欠陥のないエクスペリエンスを提供することを組織が可能にすることができます。 Cisco IWAN を使うと、IT 組織は比較的安価の WAN転送 オプションを使うとブランチ オフィス接続にパフォーマンス、セキュリティ、または信頼性に影響を与えないで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。 そして好むモデ

ルを転送する重要ではありません、かどうか MPLS、インターネット、細胞、またはハイブリッド WANアクセス モデル。

この図は IWAN ソリューションのコンポーネントの輪郭を描きます。 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:

- **保護すれば適用範囲が広いトランスポート非依存 設計-** Dynamic Multipoint VPN（DMVPN）IWAN はブロードバンド な MPLS および細胞 3G/4G/LTE を含むあらゆるキャリア サービス サービス上の容易なマルチホーミングに機能を提供します。 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 経路制御-** Cisco PfR によって、このコンポーネントはアプリケーション配信および WAN 効率を改善します。 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 はインテリジェントに 会社の全面的な通信経費を減らすために回線コストに基づいてトラフィックを負荷バランシングするために出力 WAN パスを選択できます。 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： 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 最適化-** Ciscoアプリケーション表示およびコントロール（AVC）はおよび

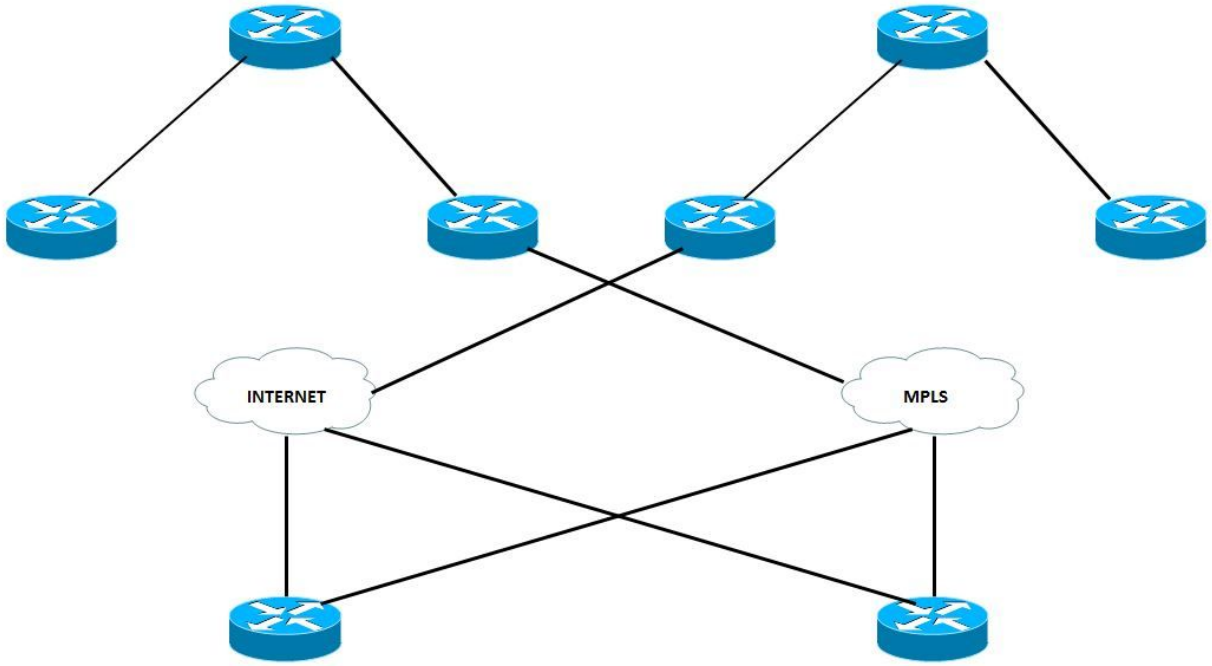
Cisco Wide Area Application Services（WAAS）アプライアンス（WAAS） WAN 上のアプリケ– ションパフォーマンス表示および最適化を提供します。 HTTP（ポート 80）などウェルノウン ポートの再利用が増大したために、アプリケーションの不透明性が高まり、アプリケーションのポートをスタティックに分類することでは対応できなくなっています。 Cisco AVC では、トラフィックのディープ パケット インスペクションによるアプリケーションの識別によって、アプリケーションのパフォーマンスの特定と監視が可能になります。 Network-Based Application 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

- **セキュア接続-**それは WAN を保護し、インターネットにユーザトラフィックを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 がなぜ使用されるか

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 IPユニキャスト、またダイナミック ルーティング プロトコルの使用を含む、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 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 人のプロバイダは使用されます、1 つはプライマリと（MPLS）考慮され、1 はセカンダリ（インターネット）とみなされます。 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。



ダイアグラムに示すように、各ブランチルータは両方のプロバイダに接続されます、1 つはプライマリの他はセカンダリのインターネットです MPLS であり。

トラフィックの種類の依存が、プロバイダのそれぞれトラフィックを送信 するのに使用されています。 たとえば、データは少し優先順位の MPLS およびデータによって高優先順位であるできますインターネット上のルーティングされる送信することができます。 これはより革新的な事業目的でより費用効果が高くさせ、利用可能資源を利用することができます解放します。

転送する 独立 した 設計（二重 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。 同じ設計は設計をトランスポート非依存にする 3G/4G 転送使用することができますまたは MPLS、インターネットに。

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 はここに要約される複数のフェーズを過します:

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 プロトコルおよびマルチキャストのためのサポート
- スポークはハブでフルルーティングテーブルを、要約できます必要としません

DMVPN フェーズ 2 にハブの集約がありません。

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 にダイナミック PBR および正しいネクスト・ホップ情報のパスを実施する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。

PfRv3 はすべての DMVPN フェーズをサポートします。

DMVPN のさらに詳しい詳細については、Cisco IOS DMVPN 概要を参照して下さい。