Introdução a IWAN e PfRv3

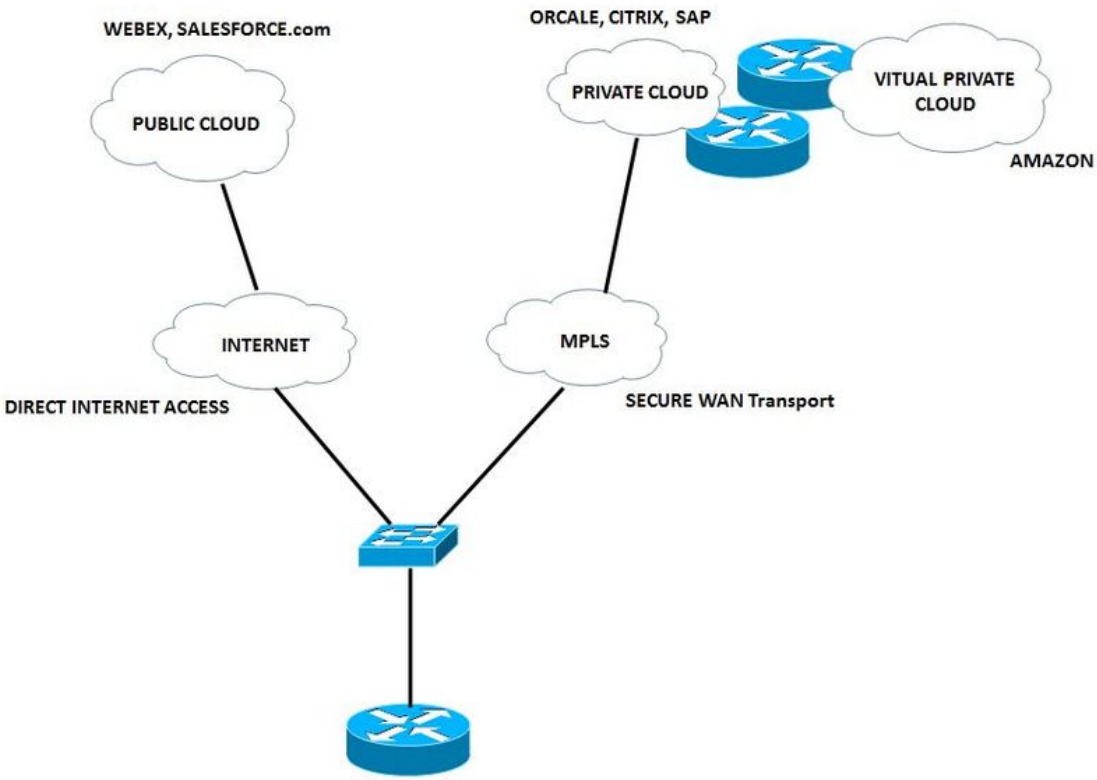
Contents

Introduction

Este documento descreve o Cisco Intelligent WAN (IWAN) e o Cisco Performance Routing (PfR).

IWAN

A Cisco IWAN é um sistema que melhora a colaboração e o desempenho dos aplicativos em nuvem, enquanto também reduz o custo operacional da WAN. A solução IWAN fornece orientação de projeto e implementação para organizações que procuram implantar uma WAN independente de transporte com controle de caminho inteligente, otimização de aplicativos e conectividade segura para a Internet e filiais, enquanto reduz o custo operacional da WAN. A IWAN aproveita totalmente a WAN premium e os serviços de Internet econômicos para aumentar a capacidade de largura de banda sem comprometer o desempenho, a confiabilidade ou a segurança de aplicativos baseados em nuvem ou de colaboração. As organizações podem usar a IWAN para aproveitar a Internet como transporte de WAN, bem como para acesso direto a aplicativos de nuvem pública.



R1 preferirá que o tráfego de voz e vídeo siga o melhor caminho com um atraso, instabilidade e/ou perda relativamente menor entre os dois links disponíveis para ele. Outro tráfego tem balanceamento de carga para maximizar a largura de banda.

Voz e vídeo são redirecionados se o caminho atual se degrada (Multiprotocol Label Switching (MPLS)) e então o link Direct Internet Access (DIA) é escolhido.

A IWAN permite que você:

- Conecte-se a um modo de custo mais baixo como INTERNET para obter dados menos importantes.
- Permite que a WAN use otimização de aplicativos, cache inteligente e DIA altamente segura.

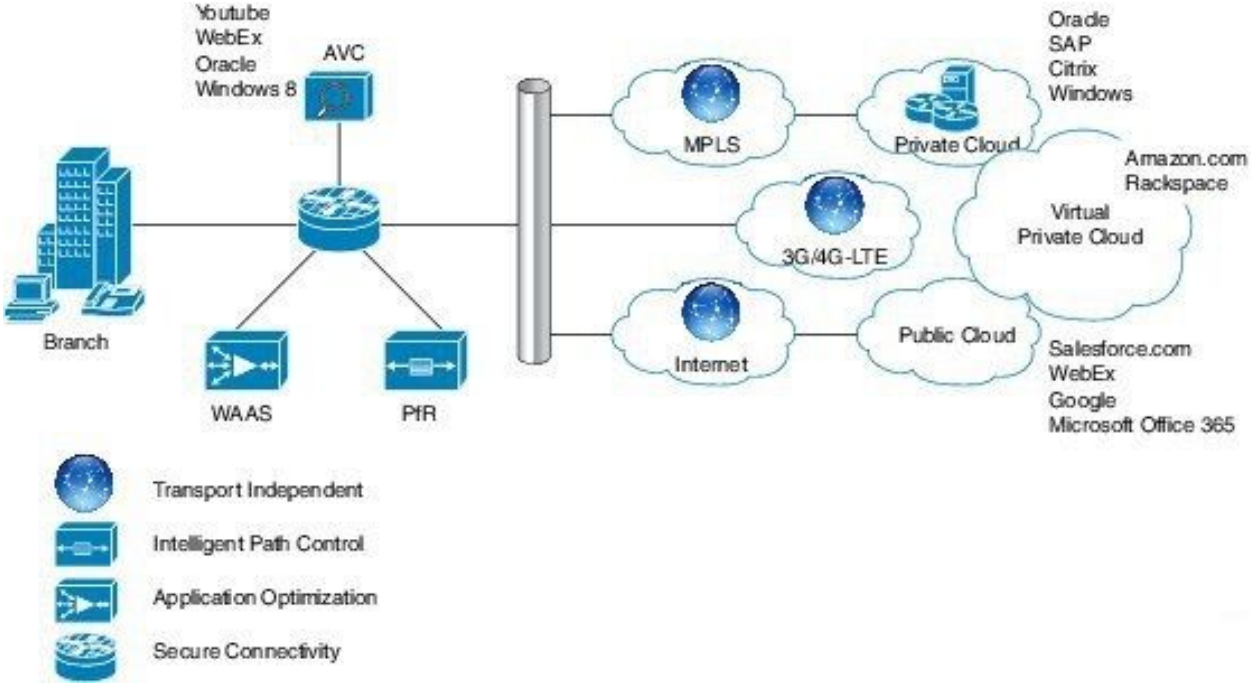
Até agora, a única maneira de obter conectividade confiável com desempenho previsível é aproveitar uma WAN privada usando MPLS ou um serviço de linha alugada. No entanto, os serviços de MPLS e linhas alugadas baseados em operadora podem ser caros e nem sempre são econômicos para uma empresa usar para transporte de WAN para suportar os crescentes requisitos de largura de banda para conectividade de local remoto. As organizações buscam maneiras de reduzir seu orçamento operacional e, ao mesmo tempo, fornecer adequadamente o transporte de rede para um local remoto.

A IWAN pode permitir que as empresas ofereçam uma experiência perfeita em qualquer conexão. Com a Cisco IWAN, as organizações de TI podem fornecer mais largura de banda para suas conexões de filial com opções de transporte de WAN mais baratas, sem afetar o desempenho, a segurança ou a confiabilidade. Com a solução IWAN, o tráfego é roteado dinamicamente dependendo do acordo de nível de serviço (SLA) do aplicativo, do tipo de endpoint e das condições de rede para fornecer a melhor experiência de qualidade.

Com a IWAN, você pode implantar rapidamente os aplicativos de uso intensivo da largura de banda, como vídeo, infraestrutura de desktops virtuais (VDI) e serviços de Wi-Fi para convidados.

E não importa qual modelo de transporte você prefere, seja MPLS, Internet, celular ou um modelo de acesso híbrido à WAN.

Esta figura descreve os componentes da solução IWAN. O roteamento de desempenho é um pilar fundamental dessa iniciativa:



Os quatro componentes da IWAN são:

- **Design seguro e flexível independente de transporte -** A DMVPN (Dynamic Multipoint VPN) IWAN fornece recursos para multihoming fácil sobre qualquer oferta de serviço de portadora, que inclui MPLS, banda larga e 3G/4G/LTE de celular. Tecnologia: Design de sobreposição DMVPN/IPsec

- **Controle de caminho inteligente -** Com o Cisco PfR, esse componente melhora o fornecimento de aplicativos e a eficiência da WAN. O PfR controla dinamicamente as decisões de encaminhamento de pacotes de dados ao observar o tipo de aplicação, o desempenho, as políticas e o status do caminho. O PfR protege os aplicativos de negócios do desempenho da WAN flutuante, enquanto faz o inteligente balanceamento de carga do tráfego no melhor caminho de desempenho com base na política do aplicativo. O PfR monitora o desempenho da rede (instabilidade, perda de pacotes, atraso) e toma decisões para encaminhar aplicativos críticos no melhor caminho de desempenho com base na política do aplicativo. O Cisco PfR consiste em roteadores de borda que se conectam ao serviço de banda larga e um aplicativo controlador primário suportado pelo software Cisco IOS® em um roteador. Os roteadores de borda coletam informações de tráfego e caminho e as enviam ao controlador principal, que detecta e aplica as políticas de serviço para corresponder ao requisito do aplicativo. O Cisco PfR pode selecionar um caminho de WAN de saída para balancear a carga de tráfego de forma inteligente com base nos custos de circuito para reduzir as despesas gerais de comunicação de uma empresa. O controle de caminho inteligente da IWAN é a chave para fornecer uma WAN de classe empresarial no transporte da Internet. Tecnologia: PfR O PfR evolui para uma nova grande versão chamada PfRv3.

- **Otimização de aplicativos -** O Cisco Application Visibility and Control (AVC) e o Cisco Wide

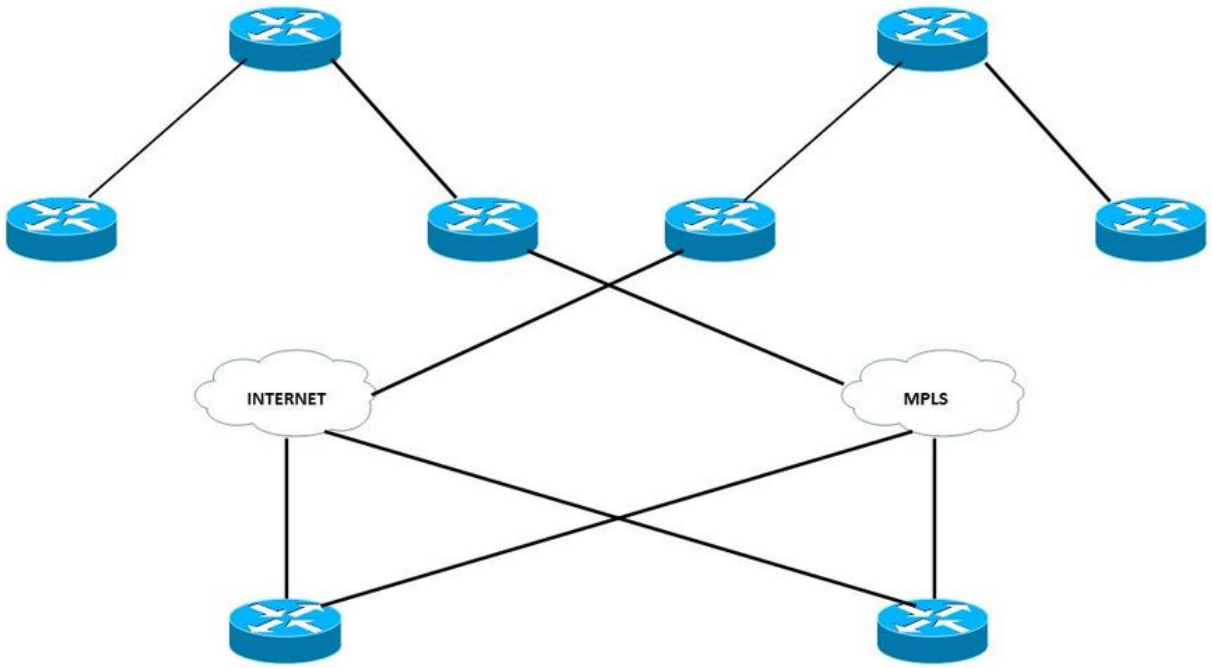
Area Application Services (WAAS) fornecem visibilidade e otimização do desempenho de aplicativos na WAN. Com aplicações cada vez mais opacas devido ao aumento da reutilização de portas conhecidas como HTTP (porta 80), a classificação de porta estática da aplicação não é mais suficiente. O Cisco AVC fornece reconhecimento de aplicativos com inspeção profunda de pacotes de tráfego para identificar e monitorar o desempenho dos aplicativos. A visibilidade e o controle no nível do aplicativo (camada 7) são fornecidos por meio de tecnologias AVC, como reconhecimento de aplicativo baseado na rede 2 (NBAR2), NetFlow, qualidade de serviço (QoS), monitoramento de desempenho, Medianet e mais. Tecnologias: Application Visibility and Control (AVC), WAAS, Akamai Connect

- **Conectividade segura -** Protege a WAN e descarrega o tráfego do usuário diretamente para a Internet. Criptografia IPsec forte, firewalls baseados em zona e listas de acesso restritas são usados para proteger a WAN na Internet pública. O roteamento de usuários de filiais diretamente para a Internet melhora o desempenho de aplicações em nuvem pública, reduzindo o tráfego na WAN. O serviço Cisco Cloud Web Security (CWS) fornece um proxy da Web baseado em nuvem para gerenciar e proteger de forma centralizada o tráfego de usuários que acessam a Internet. Tecnologias: Cisco IOS Firewall/IPS, Cloud Web Security (CWS)

Por que o DMVPN é usado

A IWAN usa um design prescritivo com um design independente de transporte híbrido com base no DMVPN. O DMVPN é implantado em MPLS e Internet Transport. Isso simplifica muito o roteamento usando um único domínio de roteamento que abrange os dois transportes. Os roteadores DMVPN usam interfaces de túnel que suportam unicast IP, bem como tráfego multicast e de broadcast IP, o que inclui o uso de protocolos de roteamento dinâmico. Após a ativação do túnel spoke-to-hub inicial, é possível criar túneis spoke-to-spoke dinâmicos quando os fluxos de tráfego IP de local para local exigirem isso.

O design independente de transporte é baseado em uma nuvem DMVPN por provedor. Neste guia, dois provedores são usados, um é considerado o principal (MPLS) e um é considerado o secundário (Internet). Os sites de filiais estão conectados às duas nuvens DMVPN e os dois túneis estão ativos.



Como mostrado no diagrama, cada roteador da filial é conectado aos dois provedores, um é o MPLS, que é primário e outro é a INTERNET, que é secundária.

Dependendo do tipo de tráfego, cada provedor é usado para enviar o tráfego. Por exemplo, os dados de maior prioridade podem ser enviados através do MPLS e os dados com menor prioridade podem ser roteados pela INTERNET. Isso o torna mais econômico e os recursos disponíveis livres podem ser utilizados para fins comerciais mais inovadores.

Design independente de transporte (DMVPN dupla)

Resumo do design

O design fornece caminhos WAN ativa-ativa que aproveitam ao máximo o DMVPN para uma sobreposição de IPsec confiável. O MPLS e as conexões com a Internet podem ser encerrados em um único roteador ou em dois roteadores separados para resiliência adicional. O mesmo design pode ser usado em transportes de MPLS, Internet ou 3G/4G, o que torna o projeto independente de transporte.

Recomenda-se usar um hub DMVPN (PfRv3 BR) por provedor e transportar no hub. Isso torna a configuração de roteamento muito mais fácil.

O DMVPN requer o uso de intervalos keepalive do Internet Key Management Protocol versão 2 (IKEv2) para Dead Peer Detection (DPD), que é essencial para facilitar a rápida reconvergência e para que o registro do spoke funcione corretamente caso um hub DMVPN seja recarregado. Esse design permite que um spoke detecte que o par da criptografia falhou e que a sessão IKEv2 com esse par está interrompida, o que possibilita que uma nova seja criada. Sem o DPD, a SA do IPsec deve expirar (o padrão é de 60 minutos) e quando o roteador não conseguir renegociar uma nova SA, uma nova sessão IKEv2 será iniciada. O tempo de espera máximo é de aproximadamente 60 minutos.

Resumo da fase de DMVPN

O DMVPN tem várias fases resumidas aqui:

A fase 1 do DMVPN é baseada na funcionalidade Hub e Spoke.

- Configuração simplificada e menor em hubs
- Suporte a CPEs endereçados dinamicamente (NAT)
- Suporte para protocolos de roteamento e multicast
- Spokes não precisam de tabela de roteamento completa, podem resumir no hub

A fase 2 do DMVPN não tem resumo no hub.

Cada spoke tem o próximo salto (endereço spoke) para cada prefixo de destino do spoke.

O PfR tem todas as informações para aplicar o caminho com o PBR dinâmico e as informações corretas do próximo salto.

A fase 3 do DMVPN permite o resumo de rotas:

- Quando a pesquisa de rota pai é executada, somente a rota para o hub está disponível.
- O NHRP instala dinamicamente o túnel de atalho e, portanto, preenche o RIB/CEF.
- O PfR ainda tem as informações do próximo salto do hub e atualmente não está ciente da mudança do próximo salto.

O PfRv3 é compatível com todas as fases do DMVPN.

Para obter mais informações sobre DMVPN, consulte Visão geral do Cisco IOS DMVPN.