Introduction à IWAN et PfRv3

Contenu

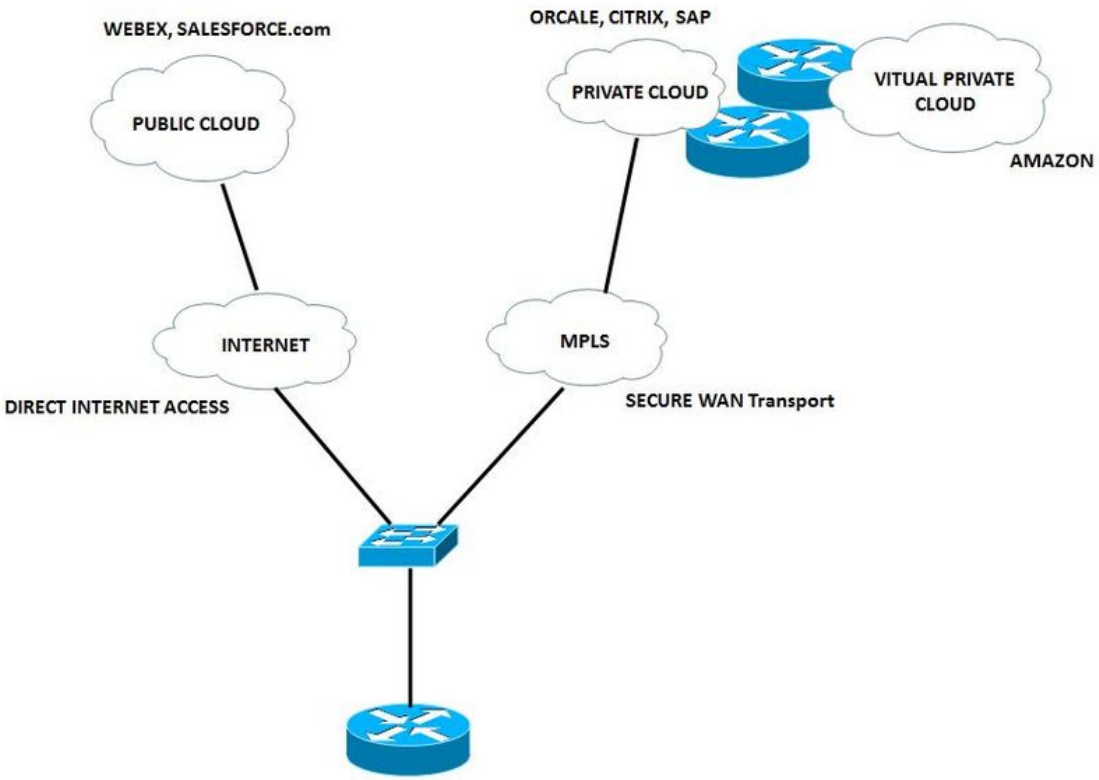
[Introduction](#)
[IWAN](#)
[Pourquoi DMVPN est-il utilisé ?](#)
[Conception indépendante du transport (DMVPN double)](#)
[Résumé de la conception](#)
[Résumé des phases DMVPN](#)

Introduction

Ce document décrit le WAN intelligent de Cisco (IWAN) et le routage des performances de Cisco (PfR).

IWAN

Cisco IWAN est un système qui améliore les performances des applications cloud et de collaboration, tout en réduisant le coût d'exploitation du WAN. La solution IWAN fournit des conseils de conception et de mise en oeuvre aux entreprises qui cherchent à déployer un WAN indépendant du transport avec un contrôle intelligent des chemins, une optimisation des applications et une connectivité sécurisée à Internet et aux filiales, tout en réduisant le coût d'exploitation du WAN. IWAN tire pleinement parti de services Internet haut de gamme et WAN rentables pour augmenter la capacité de bande passante sans compromettre les performances, la fiabilité ou la sécurité des applications de collaboration ou cloud. Les entreprises peuvent utiliser le réseau IWAN afin de tirer parti d'Internet en tant que transport WAN, ainsi que pour accéder directement aux applications de cloud public.



R1 préférera que le trafic voix et vidéo emprunte le meilleur chemin avec un délai, une gigue et/ou une perte relativement moindres parmi les deux liaisons qui lui sont disponibles. L'autre trafic est équilibré en charge afin d'optimiser la bande passante.

La voix et la vidéo sont réacheminées si le chemin actuel se dégrade (Multiprotocol Label Switching (MPLS)), puis si la liaison DIA (Direct Internet Access) est choisie.

L'IWAN vous permet de le faire :

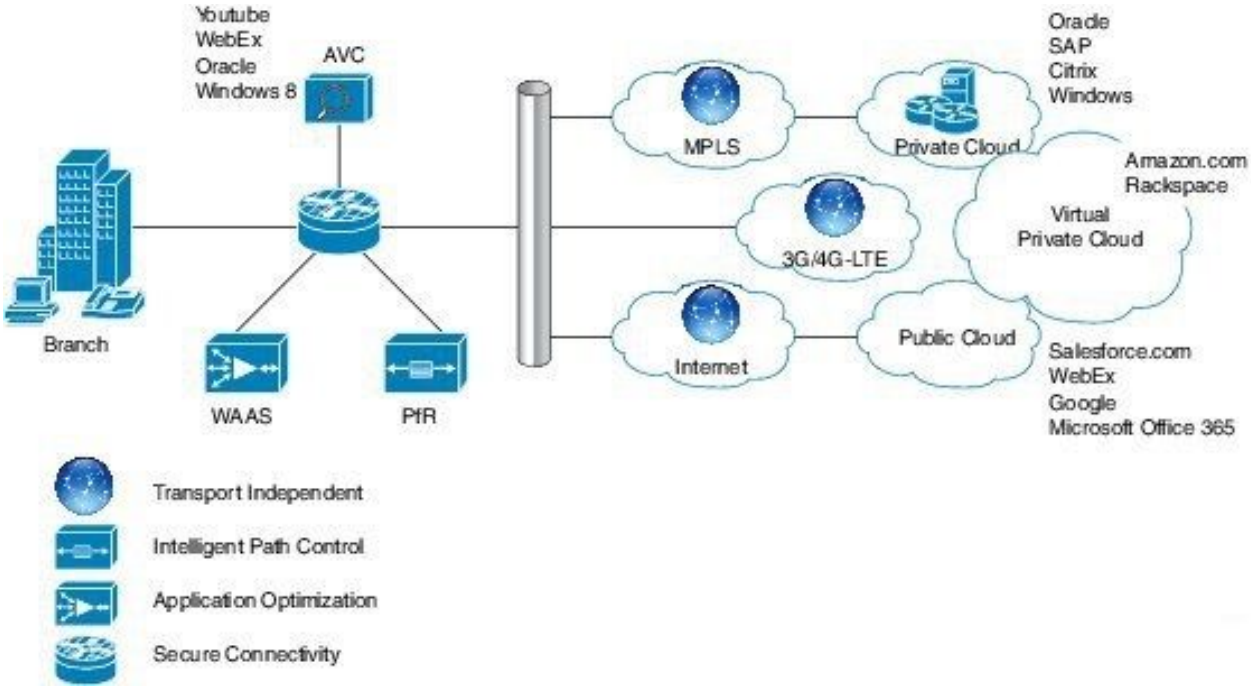
- Connectez-vous à un mode moins coûteux en tant qu'INTERNET pour des données moins importantes.
- Permet au WAN d'utiliser l'optimisation des applications, la mise en cache intelligente et la DIA hautement sécurisée.

Jusqu'à présent, le seul moyen d'obtenir une connectivité fiable avec des performances prévisibles est de tirer parti d'un WAN privé utilisant MPLS ou d'un service de ligne louée. Cependant, les services MPLS et de ligne louée basés sur opérateur peuvent être coûteux et ne sont pas toujours rentables pour une entreprise qui utilise le transport WAN pour prendre en charge les besoins croissants en bande passante pour la connectivité des sites distants. Les entreprises cherchent des moyens de réduire leur budget d'exploitation tout en assurant le transport réseau d'un site distant de manière adéquate.

Le réseau IWAN permet aux entreprises de proposer une expérience sans compromis sur n'importe quelle connexion. Avec Cisco IWAN, les départements IT peuvent fournir plus de bande passante à leurs connexions de succursale avec des options de transport WAN moins coûteuses sans affecter les performances, la sécurité ou la fiabilité. Grâce à la solution IWAN, le trafic est routé dynamiquement pour offrir l'expérience de meilleure qualité d'expérience en fonction du contrat par niveau de service d'une application, du type de point d'accès et des conditions du réseau.

Avec IWAN, vous pouvez rapidement déployer des applications gourmandes en bande passante, telles que la vidéo, l'infrastructure de bureau virtuel et les services Wi-Fi pour invités. Et peu importe le modèle de transport que vous préférez, que ce soit MPLS, Internet, cellulaire ou un modèle d'accès WAN hybride.

Cette figure présente les composants de la solution IWAN. Le routage haute performance est le fondement de cette initiative :



Les quatre composants du réseau IWAN sont les suivants :

- **Conception sécurisée et flexible, indépendante du transport :** l'IWAN DMVPN (Dynamic Multipoint VPN) offre des fonctionnalités de multihébergement aisé sur toute offre de services d'opérateur, notamment MPLS, haut débit et 3G/4G/LTE cellulaire. Technologie : Conception par chevauchement DMVPN/IPsec.
- **Contrôle intelligent des chemins -** Avec Cisco PfR, ce composant améliore la livraison des applications et l'efficacité du WAN. Le PfR contrôle de manière dynamique les décisions de transfert des paquets de données en tenant compte du type d'application, des performances, des politiques et de l'état du parcours. Il protège les applications d'exploitation contre les fluctuations des performances du WAN tout en équilibrant intelligemment le trafic vers le parcours le plus efficace en fonction de la politique applicative. Il surveille les performances du réseau – gigue, perte de paquets, retard – et prend les décisions de transférer les applications critiques sur le parcours le plus performant en fonction de la politique applicative. Cisco PfR se compose de routeurs périphériques qui se connectent au service haut débit et d'une application de contrôleur principal prise en charge par le logiciel Cisco IOS® sur un routeur. Les routeurs périphériques collectent les informations de trafic et de chemin et les envoient au contrôleur principal, qui détecte et applique les stratégies de service pour qu'elles correspondent aux exigences de l'application. Cisco PfR peut sélectionner un chemin WAN de sortie pour équilibrer intelligemment la charge du trafic en fonction des coûts de circuit afin de réduire les dépenses globales de communication d'une entreprise. Le contrôle intelligent IWAN est la clé de la fourniture d'un réseau de transport WAN sur Internet de classe professionnelle. Technologie : PfR Une nouvelle version majeure (PfRv3) est en préparation.

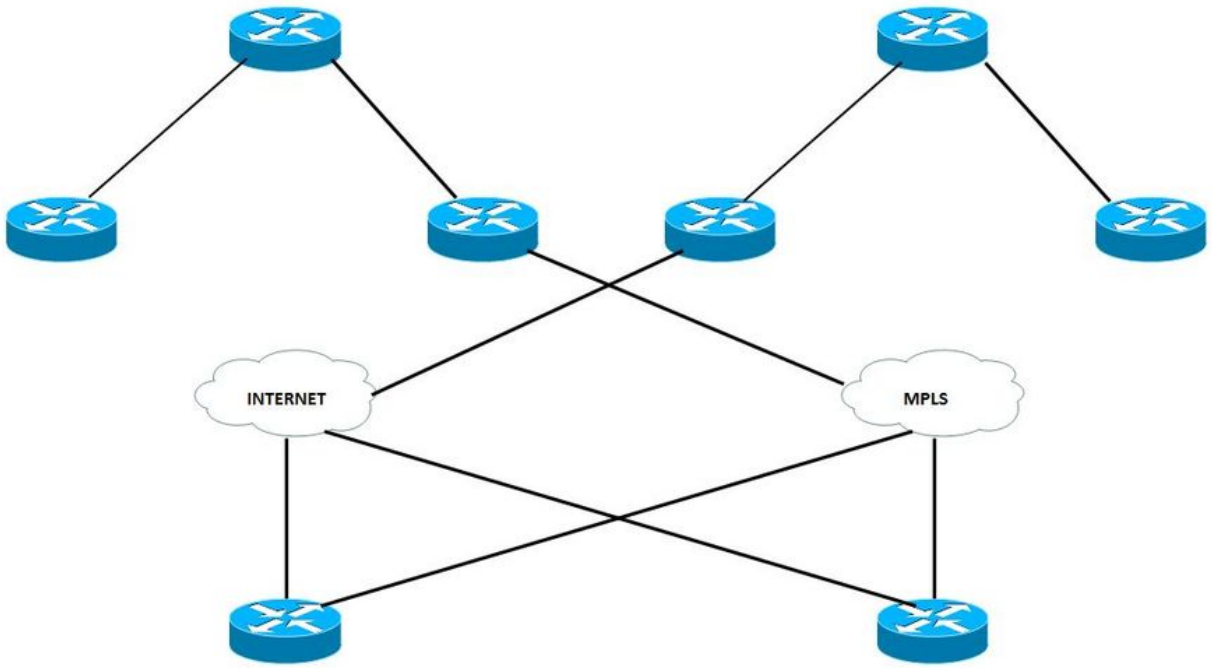
- **Optimisation des applications :** Cisco Application Visibility and Control (AVC) et Cisco Wide Area Application Services (WAAS) offrent une visibilité et une optimisation des performances des applications sur le WAN. Les applications devenant de plus en plus opaques en raison de la réutilisation croissante de ports bien connus (tels que le HTTP sur le port 80), la classification statique des ports des applications n'est plus suffisante. Les outils AVC fournissent une sensibilisation aux applications avec une inspection approfondie des paquets de trafic pour identifier et surveiller les performances des applications. La visibilité et le contrôle au niveau de l'application (couche 7) sont assurés par des technologies AVC telles que Network-Based Application Recognition 2 (NBAR2), NetFlow, qualité de service (QoS), la surveillance des performances, Medianet, et plus. Technologies : AVC, WAAS, Akamai Connect.

- **Connectivité sécurisée :** elle protège le WAN et décharge le trafic utilisateur directement sur Internet. Elle utilise un chiffrement IPsec puissant, des pare-feu basés sur des zones et des listes d'accès strictes pour protéger le WAN de l'Internet public. Le routage direct des utilisateurs des filiales/succursales vers Internet améliore la performance des applications infonuagiques publiques tout en réduisant le trafic sur le réseau étendu. Le service Cisco Cloud Web Security (CWS) fournit un proxy Web infonuagique pour gérer et sécuriser de manière centralisée le trafic des utilisateurs accédant à Internet. Technologies : Cisco IOS Firewall/IPS, Cloud Web Security (CWS).

Pourquoi DMVPN est-il utilisé ?

L'IWAN utilise une conception normative hybride indépendante du mode de transmission basée sur le VPN multipoint dynamique (DMVPN). Ce DMVPN est déployé sur MPLS et Internet Transport, ce qui simplifie grandement le routage en utilisant un seul domaine de routage qui englobe les deux transmissions. Les routeurs DMVPN utilisent des interfaces de tunnel qui prennent en charge la monodiffusion IP ainsi que le trafic de multidiffusion et de diffusion IP, ce qui inclut l'utilisation de protocoles de routage dynamique. Après l'activation du tunnel initial reliant le point central aux points d'accès, il est possible de créer des tunnels dynamiques entre les points d'accès lorsque les flux de trafic IP de site à site l'exigent.

La conception indépendante du mode de transmission utilise un nuage DMVPN pour chaque fournisseur. Dans ce guide, deux fournisseurs sont utilisés, un est considéré comme étant le principal (MPLS) et l'autre comme le secondaire (Internet). Les sites des filiales/succursales sont reliés aux deux nuages DMVPN et les deux tunnels sont en place.



Comme le montre le schéma, chaque routeur Branch est connecté aux deux fournisseurs, l'un étant MPLS principal et l'autre étant INTERNET secondaire.

Selon le type de trafic, chaque fournisseur est utilisé pour envoyer le trafic. Par exemple, les données de priorité supérieure peuvent être envoyées via MPLS et les données de priorité moindre peuvent être acheminées via INTERNET. Il est ainsi plus rentable et les ressources disponibles peuvent être utilisées à des fins commerciales plus innovantes.

Conception indépendante du transport (DMVPN double)

Résumé de la conception

La conception offre des parcours WAN actifs-actifs qui tirent pleinement parti du DMVPN pour une superposition IPsec cohérente. Les connexions MPLS et Internet peuvent être acheminées à un seul routeur ou sur deux routeurs distincts pour plus de résilience. La même conception peut être utilisée sur les transports MPLS, Internet ou 3G/4G, ce qui rend le transport de conception indépendant.

Il est recommandé d'utiliser un point central DMVPN par fournisseur (PfRv3 BR) pour les transmissions, car cela facilite la configuration du routage.

DMVPN nécessite l'utilisation des intervalles « Keepalive » de la version 2 de l'Internet Key Management Protocol (IKEv2) pour la détection de pair hors ligne (DPD); ceci est essentiel pour faciliter une reconvergence rapide et pour que l'enregistrement des points d'accès fonctionne correctement au cas où un point central DMVPN est réinitialisé. Cette conception permet à un point d'accès de détecter qu'un pair de cryptage a échoué et que la session IKEv2 avec ce pair est périmée, ce qui permet d'en créer une nouvelle. Sans DPD, l'AS IPsec doit attendre la fin de son délai (la valeur par défaut est de 60 minutes) et lorsque le routeur ne peut pas renégocier une nouvelle AS, une nouvelle session IKEv2 est lancée. Le temps d'attente maximal est d'environ 60 minutes.

Résumé des phases DMVPN

DMVPN comporte plusieurs phases résumées ici :

La phase 1 du DMVPN est basée sur un réseau en étoile.

- Configuration réduite et simplifiée sur le point central
- Prise en charge de l’équipement des locaux d’abonné avec adressage dynamique (NAT)
- Prise en charge des protocoles de routage et de la multidiffusion
- Les rayons n'ont pas besoin d'une table de routage complète, peuvent être récapitulés sur le concentrateur

La phase 2 du DMVPN ne comporte aucun résumé sur le concentrateur.

chaque préfixe de destination indique l’adresse du prochain point d’accès sur le parcours.

PfR dispose de toutes les informations nécessaires pour appliquer le chemin avec un PBR dynamique et les informations de tronçon suivant correctes.

La phase 3 du DMVPN permet la synthèse du routage :

- Seul le parcours vers le point central est disponible lorsqu’on recherche le routage original.
- Le protocole NHRP installe un tunnel de raccourci lorsque requis et fournit donc les renseignements pour la base RIB/CEF.
- Le routage haute performance dispose des renseignements sur le prochain saut mais n’est pas au courant de changements pour ce saut.

PfRv3 prend en charge toutes les phases du DMVPN.

Pour plus d'informations sur DMVPN, consultez Présentation de Cisco IOS DMVPN.