Introduction à IWAN et à PfRv3

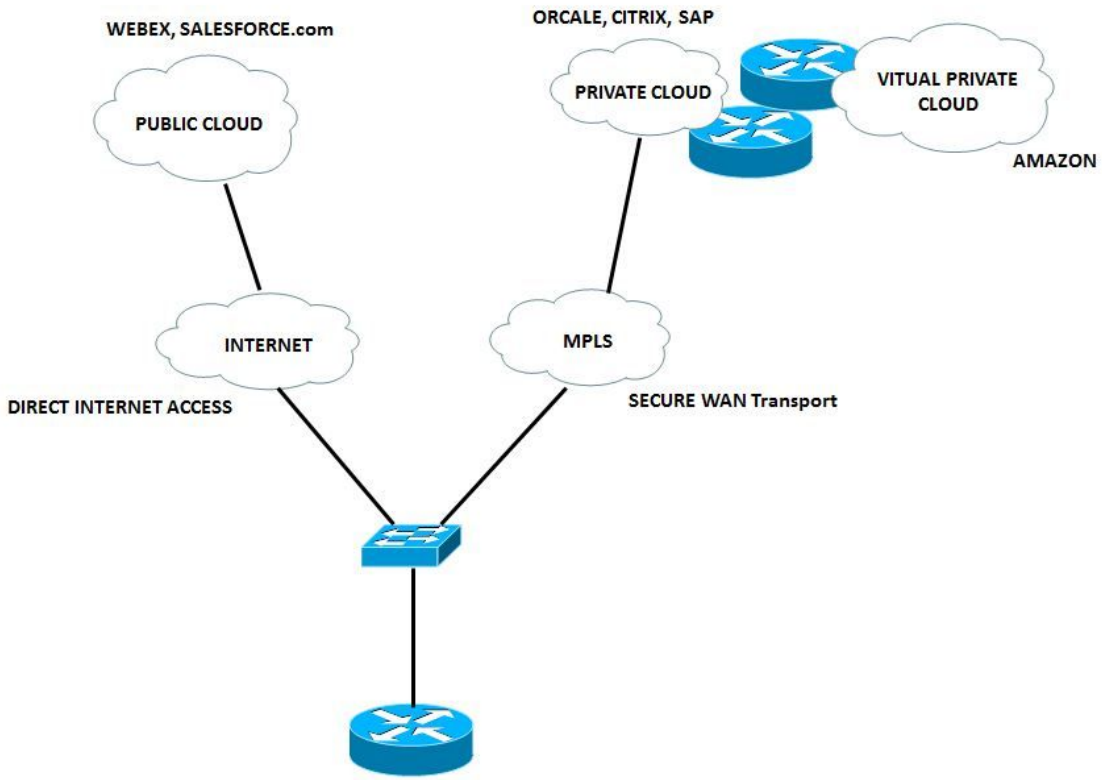
Contenu

Introduction

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

IWAN

Cisco IWAN est un système qui améliore la performance des applications de Collaboration et de nuage, alors qu'elle réduit également le coût d'exploitation du WAN. La solution d'IWAN fournit des conseils de conception et réalisation pour les organismes qui regardent pour déployer un WAN indépendant de transport avec le contrôle de chemin intelligent, l'optimisation d'application, et la connectivité sécurisée vers l'Internet et les filiales tandis qu'il réduit le coût d'exploitation du WAN. IWAN profite pleinement de WAN de la meilleure qualité et de services Internet rentables pour augmenter la capacité de bande passante sans compromission dans la représentation, la fiabilité, ou la Sécurité de la Collaboration ou des applications basées sur nuage. Les organismes peuvent utiliser IWAN afin d'accroître l'Internet comme transport BLÊME, aussi bien que pour l'accès direct aux applications publiques de nuage.



R1 préférera le trafic de Voix et de vidéo pour lui prendre le meilleur chemin avec relativement moins de retard, de jitter et/ou de perte parmi les deux liens disponibles. L'autre trafic est chargement équilibré afin de maximiser la bande passante.

La Voix et le vidéo est reroutée si le chemin en cours dégrade (le Commutation multiprotocole par étiquette (MPLS)) et alors le lien direct de l'accès Internet (diamètre) est choisi.

L'IWAN vous permet de le faire :

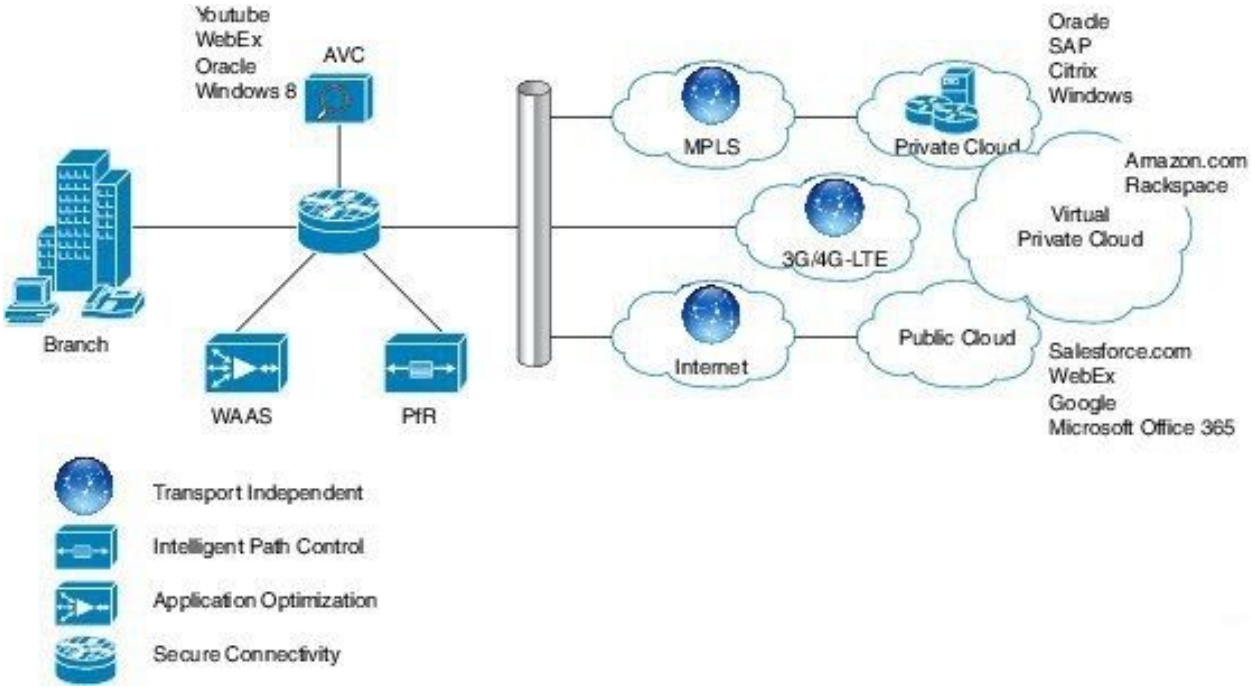
- Connectez à un mode plus peu coûteux comme INTERNET pour des données moins importantes.
- Permet au WAN pour utiliser l'optimisation d'application, mise en cache intelligente, et pour sécuriser fortement le diamètre.

Jusqu'ici, la seule manière d'obtenir la Connectivité fiable avec la représentation prévisible est de tirer profit d'un WAN privé utilisant le MPLS ou un service de ligne louée. Cependant, le MPLS à fil porteur et les services de ligne louée peuvent être chers et ne sont pas toujours rentables pour qu'une organisation l'utilise pour que le transport BLÊME prenne en charge des bandes passantes nécessaires croissantes pour la Connectivité de site distant. Les organismes recherchent des manières de diminuer leur budget de fonctionnement tout en convenablement fournissant le transport de réseau pour un site distant.

IWAN peut permettre à des organismes de fournir une expérience uncompromised au-dessus de n'importe quelle connexion. Avec Cisco IWAN, les organismes informatiques peuvent fournir plus de bande passante à leurs connexions de succursale en options BLÊMES moins chères de transport sans affecter la représentation, 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 il n'importe pas qui transporte le modèle que vous préférez, si MPLS, l'Internet, cellulaires, ou un modèle hybride d'accès WAN.

Cette figure trace les grandes lignes des composants de la solution d'IWAN. Le routage haute performance est le fondement de cette initiative :



Les quatre composants d'IWAN sont :

- **Conception sécurisée et flexible de transport-indépendant -** Le VPN multipoint dynamique (DMVPN) IWAN fournit des capacités pour le multihébergement facile au-dessus de n'importe quel opérateur offrant, qui inclut le MPLS, la Large bande, et le 3G/4G/LTE cellulaire. Technologie : Conception par chevauchement DMVPN/IPsec.

- **Contrôle de chemin intelligent -** Avec Cisco PfR, ce composant améliore la distribution d'applications et l'efficacité de 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. Il se compose de routeurs frontaliers qui se connectent au service large bande et d'une application de contrôle central prise en charge par le logiciel Cisco IOS® sur un routeur. Ces routeurs frontaliers recueillent les renseignements sur le trafic et les parcours d'accès et les envoient au contrôleur central, qui détecte et applique les politiques de service en fonction des exigences des applications. Cisco PfR peut sélectionner un chemin BLÊME de sortie pour équilibrer la charge intelligemment le trafic basé sur des coûts de circuit afin de réduire les dépenses globales des transmissions d'une société. 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.

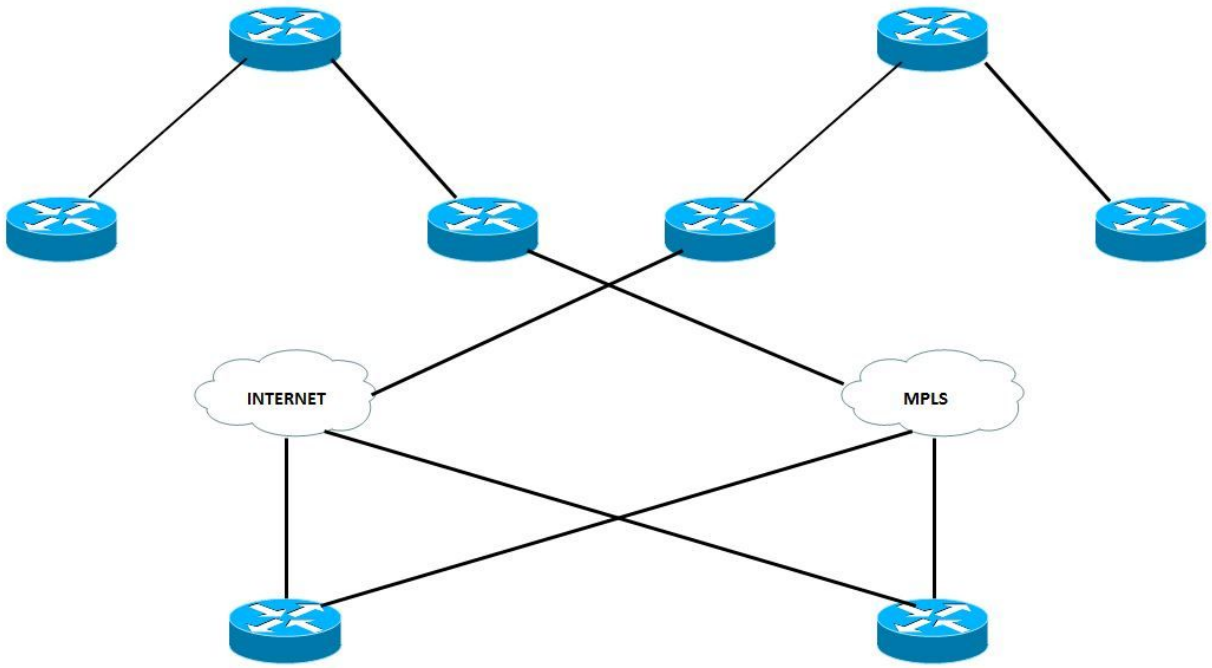
- **Optimisation d'application -** La visibilité d'application de Cisco et le contrôle (AVC) et le Cisco Wide Area Application Services (WAAS) fournissent la visibilité et l'optimisation de performance des applications au-dessus du WAN. Les applications devenant de plus en plus opaques en raison de la 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 débarque le trafic d'utilisateur directement à l'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 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 les interfaces de tunnel qui prennent en charge l'unicast sur IP aussi bien que le Protocole IP Multicast et le trafic d'émission, qui inclut l'utilisation des 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. De ce guide deux des fournisseurs sont utilisés, on est considéré le primaire (MPLS), et on est considéré le secondaire (Internet). Les sites des filiales/succursales sont reliés aux deux nuages DMVPN et les deux tunnels sont en place.



Suivant les indications du diagramme, chaque routeur secondaire est connecté les aux deux les fournisseurs, on est le MPLS qui est primaire et autre est l'INTERNET qui est secondaire.

La personne à charge sur le type de trafic, chacun des fournisseurs est utilisée pour envoyer le trafic. Par exemple, des données qui sont de haute priorité peuvent être envoyées par le MPLS et les données avec peu de priorité peuvent être conduites au-dessus de l'INTERNET. Ceci le rend plus rentable et libère des ressources disponibles peut être utilisé pour des buts commerciaux plus innovateurs.

Conception indépendante de transport (doubles DMVPN)

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 au-dessus du MPLS, de l'Internet, ou des transports 3G/4G, qui fait l'indépendant de transport de conception.

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 a les plusieurs phases qui sont récapitulées 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)
- Soutien des protocoles de routage et de Multidiffusion
- Les rais n'ont pas besoin de la pleine table de routage, peuvent récapituler sur le hub

Le Phase 2 DMVPN n'a aucune récapitulation sur le hub.

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

PfR a toutes les informations pour imposer le chemin avec PBR dynamique et les informations correctes de prochain-saut.

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 DMVPN.

Pour plus d'informations sur DMVPN, voir l'aperçu du Cisco IOS DMVPN.