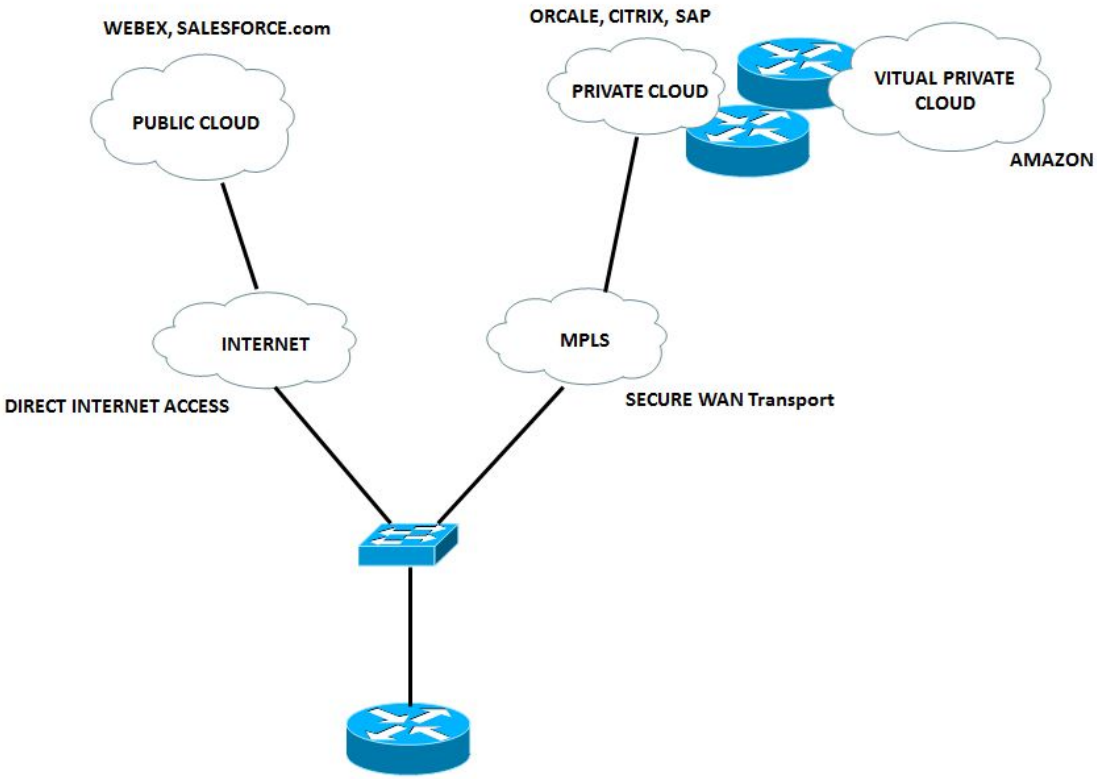
Introduction à IWAN et à PfRv3

Contenu

[Résumé de conception](#)
[Résumé de phase DMVPN](#)
[Cisco relatif prennent en charge des discussions de la Communauté](#)

IWAN

Le WAN intelligent de Cisco (IWAN) est un système qui améliore la performance des applications de Collaboration et de nuage tout en réduisant le coût d'exploitation du WAN. La solution d'IWAN fournit des conseils de conception et réalisation pour des organismes regardant 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 tout en réduisant 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 compromettre la représentation, la fiabilité, ou la Sécurité de la Collaboration ou des applications basées sur nuage. Les organismes peuvent utiliser IWAN pour 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 peu de retard, jitter et/ou perte parmi les deux liens disponibles. L'autre trafic est chargement équilibré pour maximiser la bande passante.

La Voix et le vidéo est reroutée si le degrades(MPLS) en cours de chemin et alors le lien diamètre est choisi.

IWAN vous permet à :

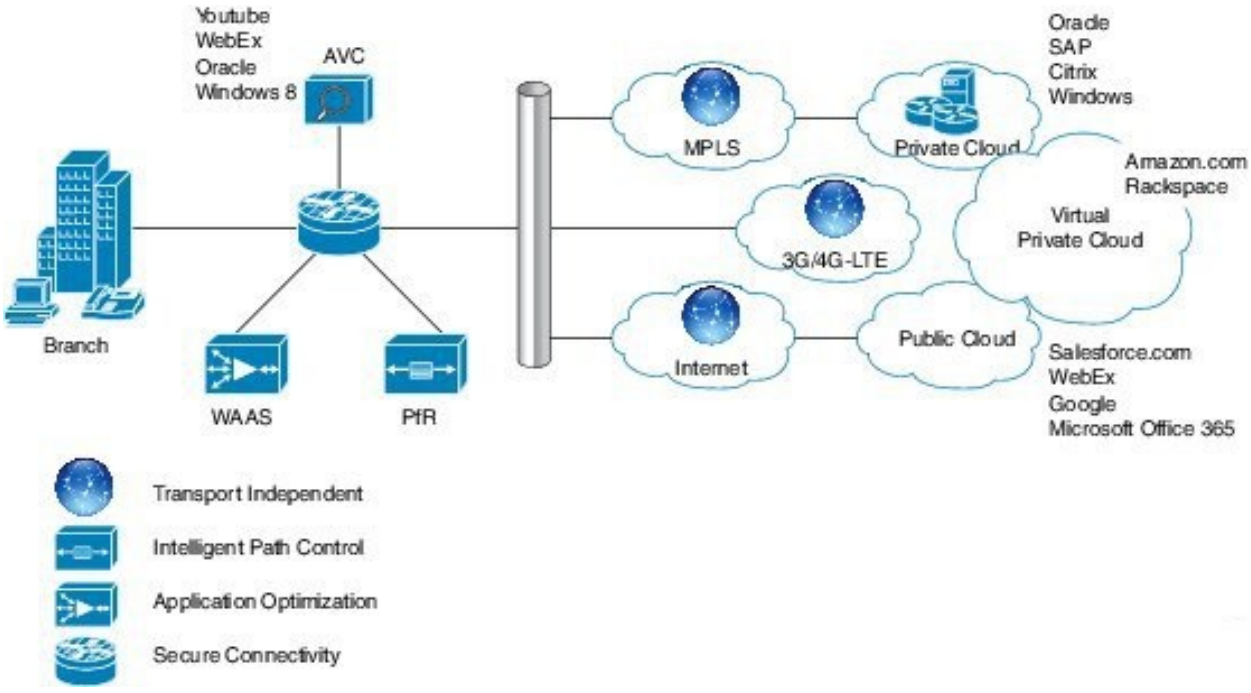
- Connectez à un mode plus peu coûteux comme INTERNET pour des données moins importantes.
- Permet au WAN pour utiliser l'optimisation d'application, mise en cache intelligente, et pour sécuriser fortement l'accès Internet direct.

Jusqu'ici, la seule manière d'obtenir la Connectivité fiable avec la représentation prévisible était de tirer profit d'un WAN privé utilisant le MPLS ou le service de ligne louée. Cependant, le MPLS à fil porteur et le service 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 le budget de fonctionnement tout en convenablement fournissant le transport de réseau pour un site distant.

Le WAN intelligent de Cisco (IWAN) peut permettre à des organismes de fournir une expérience uncompromised au-dessus de n'importe quelle connexion. Avec Cisco IWAN l'organisation informatique peut fournir plus de bande passante à leurs connexions de succursale utilisant des options BLÊMES moins chères de transport sans affecter la représentation, la Sécurité, ou la fiabilité. Avec la solution d'IWAN, le trafic est dynamiquement conduit basé sur l'accord de niveau de service d'application (SLA), le type de point final, et les états de réseau de fournir la meilleure expérience de qualité.

Avec IWAN, vous pouvez rapidement dérouler des applications bande passante-intensives, telles que le vidéo, l'infrastructure de bureau virtuel (VDI), et les services de WiFi d'invité. Et il n'importe pas qui transporte le modèle que vous préférez, si Commutation multiprotocole par étiquette (MPLS), l'Internet, cellulaires, ou un modèle hybride d'accès WAN.

La figure suivante trace les grandes lignes des composants de la solution d'IWAN. Le routage de représentation est un pilier principal de cette initiative :



Les quatre composants du WAN intelligent de Cisco sont :

- **Conception sécurisée et flexible de transport-indépendant** : Utilisant le VPN multipoint dynamique (DMVPN) IWAN fournit des capacités pour le multihébergement facile au-dessus

de n'importe quel opérateur offrant, y compris le Commutation multiprotocole par étiquette (MPLS), la Large bande, et le 3G/4G/LTE cellulaire.
- Technologie : Conception de recouvrement DMVPN/IPsec

- **Contrôle de chemin intelligent : À l'aide du routage de représentation de Cisco (PfR)**, ce composant améliore la distribution d'applications et l'efficacité de WAN. PfR contrôle dynamiquement des décisions d'expédition de paquet de données en regardant le type d'application, la représentation, les stratégies, et l'état de chemin. PfR protège des applications métier contre le WAN aux performances de fluctuation tandis qu'intelligemment le trafic d'Équilibrage de charge au-dessus du chemin en fonction le plus performant sur la stratégie d'application. PfR surveille les performances du réseau - jitter, perte de paquets, retard - et prend des décisions d'expédier des applications stratégiques au-dessus du chemin en fonction le plus performant sur la stratégie d'application. Cisco PfR se compose des Routeurs de cadre qui se connectent au service à large bande, et d'une application de contrôleur principal prise en charge par le logiciel de Cisco IOS® sur un routeur. Les Routeurs de cadre collectent des informations du trafic et de chemin et les envoient au contrôleur principal, qui détecte et impose les stratégies de service pour apparier la condition requise d'application. Cisco PfR peut sélectionner un chemin BLÊME de sortie pour équilibrer la charge intelligemment le trafic basé sur des coûts de circuit, pour réduire les dépenses globales des transmissions d'une société. Le contrôle de chemin intelligent d'IWAN est la clé à fournir un WAN de classe affaires au-dessus du transport d'Internet. Technologie : Routage de représentation (PfR). PfR évolue à une nouvelle release importante appelée le PfRv3.

- **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. Avec des applications devenant due de plus en plus opaque pour augmenter la réutilisation des ports connus tels que le HTTP (port 80), la classification de prise de pression statique de l'application n'est plus suffisante. Cisco AVC fournit à la connaissance d'application l'inspection profonde de paquet du trafic pour identifier et surveiller la représentation des applications. Visibilité et contrôle au niveau application (la couche 7) est fournie par des Technologies AVC telles que la reconnaissance Fondé(e) sur le réseau 2 (NBAR2) d'application, le NetFlow, le Qualité de service (QoS), la supervision des performances, le Medianet, et plus. Technologies : La visibilité d'application et le contrôle (AVC), WAAS, Akamai se connectent

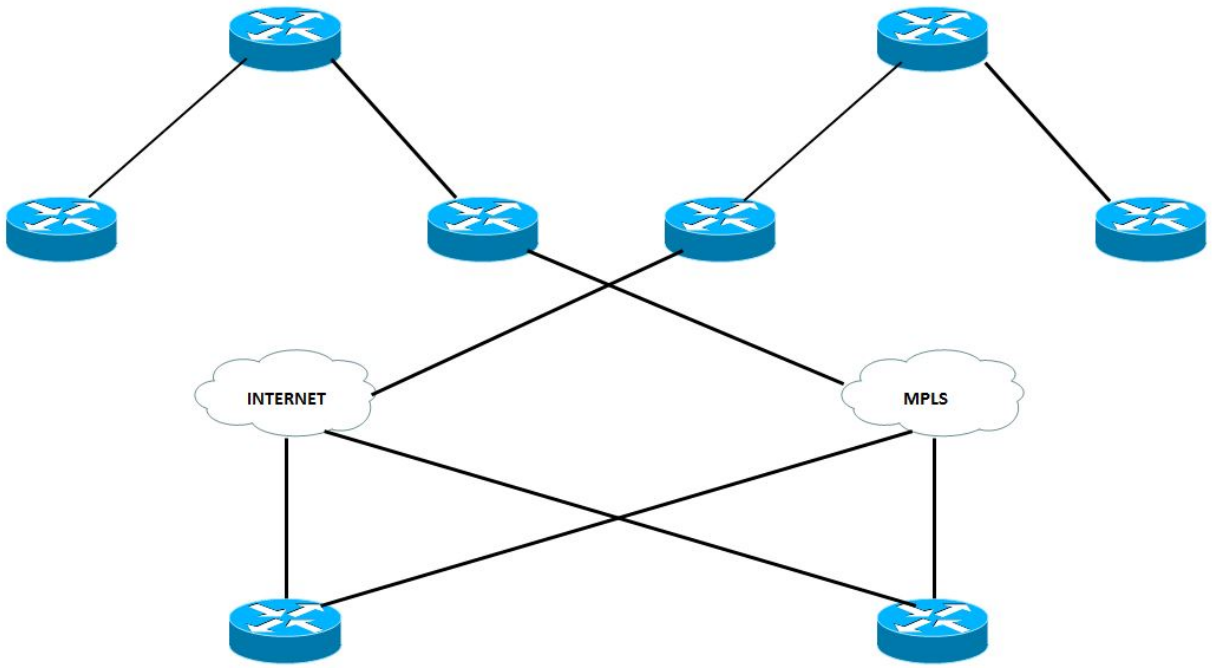
- **Connectivité sécurisée** : Il protège le WAN et débarque le trafic d'utilisateur directement à l'Internet. Le cryptage fort d'IPsec, les Pare-feu basés sur zone, et les Listes d'accès strictes sont utilisés pour protéger le WAN au-dessus de l'Internet public. L'acheminement des utilisateurs de branchement directement à l'Internet améliore la performance des applications publique de nuage tout en réduisant le trafic au-dessus du WAN. Cisco opacifient le service de la sécurité Web (CWS) fournit un proxy basé sur nuage de Web pour gérer centralement et le trafic sécurisé d'utilisateur accédant à l'Internet. Technologies : Cisco IOS Firewall/IPS, sécurité Web de nuage (CWS)

POURQUOI DMVPN EST UTILISÉ

IWAN utilise une conception normative avec une conception indépendante de transport hybride basée sur DMVPN. DMVPN est déployé à travers le MPLS et le transport d'Internet. Ceci simplifie considérablement le routage à l'aide d'un routing domain simple qui entoure les deux transports.

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, y compris l'utilisation des protocoles de routage dynamique. Après que le tunnel initial de rai-à-hub soit en activité, il est possible de créer les tunnels dynamiques de spoke-to-spoke quand les écoulements du trafic IP de site à site l'exigent.

La conception indépendante de transport est basée sur un nuage DMVPN par fournisseur. De ce guide deux des fournisseurs sont utilisés, on étant considéré en tant que primaire (MPLS), et un considéré en tant que secondaire (Internet). Des filiales sont connectées aux deux nuages DMVPN et les deux tunnels sont.



Suivant les indications du diagramme ci-dessus, 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.

Selon le type de trafic, chacun du fournisseur est utilisé pour envoyer le trafic. 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 des ressources disponibles libres peuvent être utilisées pour des buts commerciaux plus innovateurs.

Résumé de conception

La conception fournit les chemins BLÊMES actif-actifs qui profitent pleinement de DMVPN pour à recouvrement cohérent d'IPsec. Le MPLS et les connexions Internet peuvent être terminés sur un routeur unique, ou être terminés sur deux Routeurs distincts pour la résilience supplémentaire. La même conception peut être utilisée au-dessus du MPLS, de l'Internet, ou des transports 3G/4G, faisant l'indépendant de transport de conception.

Il est recommandé pour utiliser un hub DMVPN (BR PfRv3) par fournisseur et transport sur le hub. Il facilite la configuration de routage beaucoup.

DMVPN exige l'utilisation des intervalles de keepalive de la version 2 de protocole de gestion de clé Internet (IKEv2) pour Dead Peer Detection (DPD), qui est essentielle pour faciliter la reconvergence rapide et pour que l'enregistrement de rai fonctionne correctement au cas où un hub DMVPN serait rechargé. Cette conception active a parlé pour la détecter qu'un homologue de chiffrement a manqué et que la session IKEv2 avec ce pair est éventée, qui permet alors un neuf à créer. Sans DPD, IPsec SA doit chronométrer (le par défaut est de 60 minutes) et quand le routeur ne peut pas renégocier nouvelle SA, une nouvelle session IKEv2 est initiée. Le temps d'attente maximum est approximativement 60 minutes.

Résumé de phase DMVPN

DMVPN a les plusieurs phases qui sont récapitulées ci-dessous :

Le Phase 1 DMVPN est basé sur la fonctionnalité de hub and spoke.

- Configuration simplifiée et plus petite sur des Concentrateurs
- Le support a dynamiquement adressé CPEs (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 rai a le prochain-saut (adresse de rai) pour chaque préfixe de destination de rai.

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

DMVPN phase3 permet le résumé du routage :

- Quand la consultation de route parent est exécutée, seulement l'artère au hub est disponible.
- Le NHRP installe dynamiquement le tunnel raccourci et par conséquent remplit RIB/CEF.
- PfR a les informations de prochain-saut de hub et est toujours actuellement inconscient de la modification de prochain-saut.

PfRv3 prend en charge toutes les phases DMVPN.

Pour plus d'informations sur DMVPN, référez-vous s'il vous plaît au lien :

http://www.cisco.com/c/dam/en/us/products/collateral/security/dynamic-multipoint-vpn-dmvpn/DMVPN_Overview.pdf