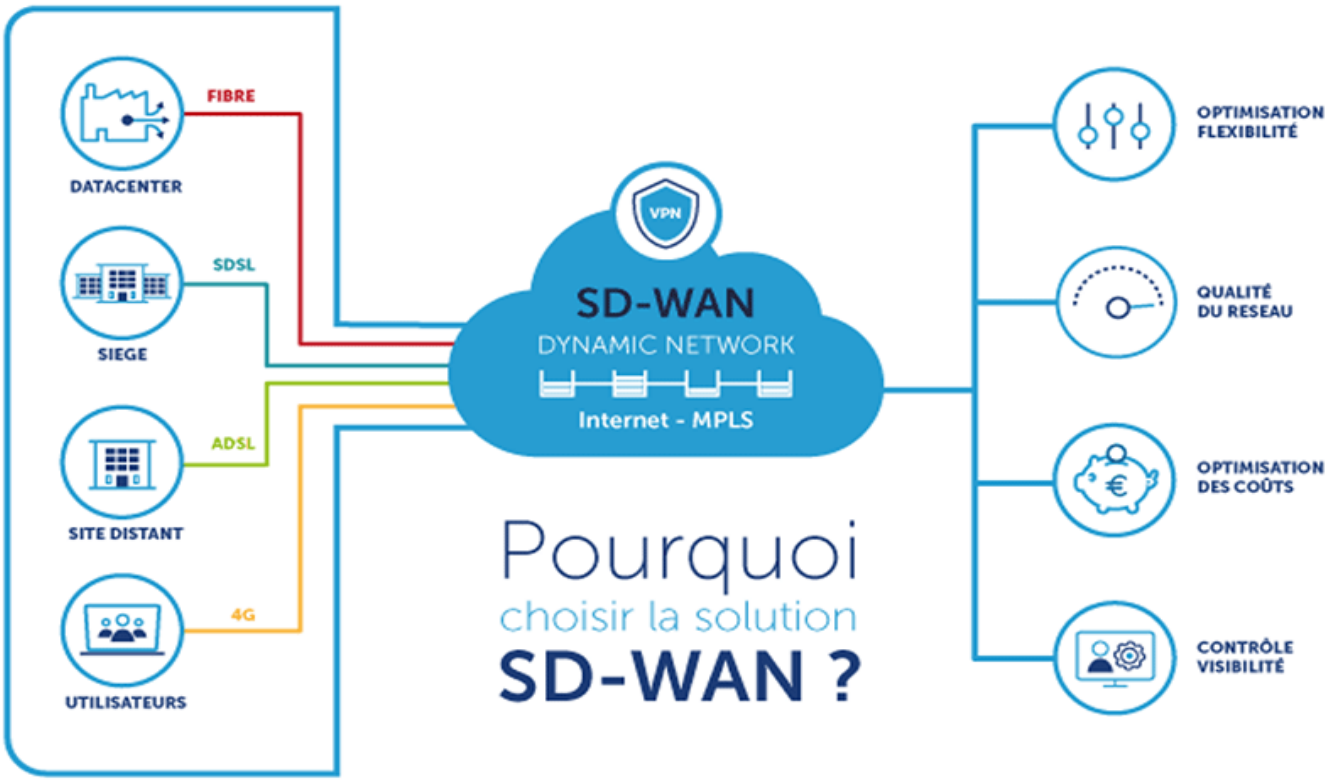
2A CONSULTING

Mise en place d'une Architecture SDWAN



Farah EL BOUMEDIANI 2024

Table des matières

Définition

Le SD-WAN est une version améliorée des WAN existants. Acronyme de Software Defined Wide Area Network soit réseau étendu à définition logicielle en français, le SD-WAN est un système de mise en réseau logiciel ; les administrateurs contrôlent chaque configuration à partir d'un tableau de bord centralisé.

Au lieu d'utiliser des adresses IP pour les réseaux traditionnels ou des étiquettes pour le MPLS, un SD-WAN utilise des informations en temps réel pour déterminer le chemin optimal pour le trafic réseau. Il repose sur une approche de virtualisation du réseau en utilisant des logiciels pour gérer la connectivité et le routage des données.

Pourquoi SD-WAN ?

Avec l'essor des applications cloud, des services de collaboration, et de la connectivité Internet, les entreprises ont connu une augmentation exponentielle des besoins en bande passante et des demandes de performances réseau.

Selon l'ONUG, la technologie SD-WAN offre deux objectifs complémentaires à la connexion Internet pour combler ces besoins :

- Avoir un accès direct aux applications hébergées dans le cloud.
- Offrir un second lien entre le site distant et le site principal ou le Datacenter de l'organisation.

Architecture

Le SD-WAN est l'application de la technologie SDN au réseau étendu. Son principe est donc semblable à cette technologie, reposant sur une approche de virtualisation du réseau en utilisant des logiciels pour gérer la connectivité et le routage des données.

Son architecture repose sur la séparation du plan de contrôle avec le plan de données et se compose de trois couches essentielles. Il s'agit de la périphérie SD-WAN, le contrôleur et l'orchestrateur comme le montre la figure suivante.

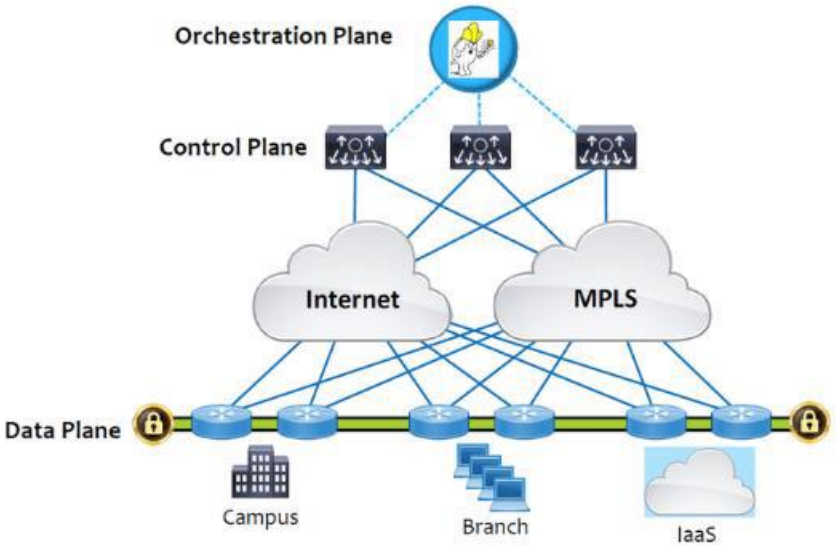


Figure 1 : Architecture de SD-WAN

1. SD-WAN Edge ou Périphérie SD-WAN

Il représente le plan de données de SD-WAN.
Le SD-WAN Edge est donc l'endroit où résident les points de terminaison du réseau c'est-à-dire les points d'extrémité du réseau. Il est constitué de l'ensemble des routeurs physiques ou virtuels gérés par le contrôleur. Concrètement, il peut s'agir de succursales, de centres de données distantes ou de plates-formes cloud.

2. SD-WAN Controller ou Contrôleur SD-WAN

Il correspond au plan de contrôle de SD-WAN.
C'est le cerveau central de l'infrastructure : il centralise la gestion, permettant aux opérateurs d'avoir une vue globale du réseau et définit les politiques que l'orchestrateur doit exécuter.

3. SD-WAN Orchestrator ou Orchestrateur

L'orchestrateur est conçu comme le gestionnaire virtualisé des réseaux. Son rôle consiste à surveiller le trafic et à appliquer des politiques et des protocoles.

Types d'architectures de SD-WAN

SD-WAN représente trois principaux types d'architecture : On-Premises, Cloud-Enabled, et Cloud-Enabled with a Backbone. Ces trois aspects concernent les services spécifiques que le client peut utiliser via la solution SD-WAN.

1. On-Premises SD-WAN (sur site uniquement)

Ce type d'architecture est installé sur site, c'est-à-dire que le dispositif SD-WAN réside sur des machines physiques. Les opérateurs de réseau peuvent accéder et gérer directement le réseau et le matériel sur lequel il réside sans l'implication du cloud pour ses connexions. Cette solution sera pour les informations sensibles qui ne peuvent pas être envoyées sur Internet.

2. Cloud-enabled SD-WANs (architecture adaptée au cloud)

Elle implique l'implication du cloud et de l'Internet. Avec ce type, les SD-WAN sont construits en se connectant à une passerelle cloud virtuelle sur Internet. Cette structure permet de se connecter en réseau aux principaux fournisseurs cloud, tels qu'Amazon Web Services (AWS), Microsoft Office 365 ou Salesforce, et contribue à avoir une meilleure intégration et de meilleures performances avec les applications cloud natives.

3. Cloud-Enabled with Backbone SD-WAN (architecture hybride)

Ce troisième service est le plus complexe, mais aussi le plus complet. La solution cloud plus réseau principal fournit un boîtier SD-WAN sur site connectant le site de l'entreprise au point de présence réseau le plus proche du fournisseur SD-WAN.

En pratique, il offre une option de sauvegarde supplémentaire en permettant de passer de l'Internet public à une connexion privée. Grâce à ce principe, le réseau résultant est plus robuste aux défaillances et également plus sécurisé.

Principe de fonctionnement

Comme le SD-WAN est une évolution des réseaux WAN existants, son idée maîtresse est de faire abstraire les détails de la couche réseau en donnant aux WAN la possibilité d'utiliser plusieurs types de connexion, comme MPLS, LTE, ethernet, fibre optique ou l'Internet à large bande.

L'abstraction de réseau réside sur la construction de réseaux virtuels par opposition à un itinéraire physique entre deux destinations.

Le réseau SD-WAN est construit en établissant des tunnels cryptés entre les sites. Chaque site doit comporter un dispositif SD-WAN. Une fois connectés, ces dispositifs téléchargent automatiquement une configuration personnalisée et des politiques de trafic.

Les dispositifs SD-WAN choisissent le meilleur chemin pour acheminer le trafic en fonction des statistiques, qui sont calculées instant par instant par le noeud de contrôle principal. Ces opérations de routage et de transfert sont gérées par les trois entités susmentionnées.

En cas de défaillance d'une connexion, l'appareil SD-WAN réagit immédiatement en passant à un autre chemin sans perdre la connectivité.

Zero touch provisionning (ZTP)

Le Zero Touch Provisioning, abrégé ZTP ou provisionnement sans intervention est un processus automatisé qui permet de configurer et de déployer des dispositifs de réseau SD-WAN sans nécessiter d'intervention manuelle. Cette approche simplifie considérablement le déploiement et la gestion du réseau, en particulier dans des environnements où de nombreux dispositifs doivent être configurés et déployés rapidement.

1. Fonctionnement de ZTP

Voici comment le ZTP fonctionne généralement :

- Identification du dispositif : Lorsqu'un dispositif SD-WAN est connecté à un réseau pour la première fois, il envoie généralement des informations d'identification à un contrôleur SD-WAN central ou à un serveur de gestion.

- Attribution automatique d'une configuration : Le contrôleur SD-WAN utilise ces informations d'identification pour attribuer automatiquement une configuration préétablie au dispositif (règles de routage, les politiques de sécurité, les adresses IP, etc.)

- Téléchargement automatique du firmware et des mises à jour : Si nécessaire, le dispositif peut également télécharger automatiquement les mises à jour du firmware ou du logiciel SD-WAN pour garantir qu'il fonctionne avec la dernière version.

- Validation de la connectivité : Lorsque la configuration est appliquée, le dispositif SD-WAN vérifie sa connectivité avec le réseau et peut signaler son état au contrôleur central.

- Opération autonome : Une fois la configuration achevée et la connectivité établie, le dispositif SD-WAN peut fonctionner de manière autonome, en routant le trafic conformément aux règles définies dans sa configuration.

2. Besoins pour la configuration de ZTP

Cette méthode peut différer d'une configuration à l'autre ; néanmoins, les exigences essentielles sont les suivantes :

- Un périphérique réseau avec ZTP

- Un serveur DHCP (Dynamic Host Configuration Protocol) ou un serveur TFTP (Trivial File Transfer Protocol)

- Un serveur de fichiers.

Lorsqu'un périphérique ZTP est mis en marche, il exécute un fichier de démarrage qui configure automatiquement ses paramètres. Le périphérique envoie ensuite une requête DHCP ou TFTP pour récupérer son image et sa configuration à partir d'une source centralisée.

Une fois ces informations téléchargées et exécutées, la configuration du port et l'adresse IP sont automatiquement attribuées.

En fonction des besoins locaux, d'autres paramètres tels que la passerelle, le nom de domaine et l'emplacement du serveur sont également fournis.

Réseau Overlay

1. C'est quoi un réseau overlay ?

En français superposition du réseau, un réseau overlay est une approche de mise en réseau informatique qui consiste à créer une couche de réseau virtuel au-dessus d'un réseau physique.

Cette abstraction de réseau est conçue pour ajouter des fonctionnalités ou des services spécifiques sans modifier la structure sous-jacente du réseau physique.

Il permet donc d'améliorer l'évolutivité, les performances et la sécurité de l'infrastructure sous-jacente. Les réseaux overlays sont couramment utilisés dans le domaine de la virtualisation, des réseaux définis par logiciel SDN, SD-WAN et des VPN.

2. SD-WAN Overlay

La superposition SD-WAN est une architecture réseau qui améliore l'infrastructure du réseau étendu WAN traditionnelle en tirant parti des principes de réseau défini par logiciel, le SDN. Dans ce modèle, les applications établissent leur propre réseau overlay, s'affranchissant des contraintes du réseau physique sous-jacent. Ce dernier n'a pour mission que la simple connectivité entre les noeuds d'extrémité des tunnels, et que le réseau d'overlay assure l'intégralité des services.

Ces superpositions de réseaux peuvent reposer à de différentes approches :

- Overlay basé sur des tunnels : encapsulation des trafics dans un tunnel VPN à l'aide des protocoles comme IPSec, GRE, …

- Overlay basé sur des segments : priorisation des trafics en les segmentant en fonction de critères spécifiques tels que le type d'application, le groupe d'utilisateurs ou l'emplacement

- Overlay basé sur des politiques : définition des règles et des politiques en utilisant des algorithmes de routage intelligents

- Overlay hybride : combinaison des avantages des réseaux public et privés permettant aux organisations d'utiliser plusieurs connexions réseau, notamment MPLS, les hauts débits, le LTE, …

- Overlay compatible avec le cloud : connectivité directe et sécurisée entre le réseau SD-WAN et les fournisseurs de services cloud.

Tunnellisation VPN IPsec

La tunnellisation est une composante essentielle des solutions SD-WAN. Elle permet d'acheminer le trafic de manière sécurisée et efficace à travers un réseau étendu WAN en créant des tunnels virtuels pour encapsuler les données.

1. VPN

Le Virtual Private Network ou Réseau Privé Virtuel en français est une technologie permettant à des utilisateurs distants de se connecter à un réseau privé via une connexion publique ou Internet en créant un tunnel de communication sécurisé.

Un tunnel VPN protège donc les données contre toute interception. Il masque l'adresse IP qui permettrait d'identifier un utilisateur lors de sa navigation sur le Web. De plus, lorsque l'utilisateur surfe sur Internet, sa localisation devient celle du serveur emprunté. Nul ne peut l'identifier en raison du tunnel crypté utilisé.

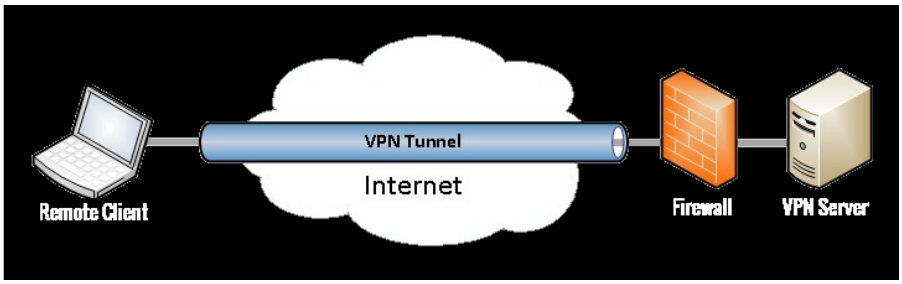


***Figure 2* :** Tunnel VPN

2. VPN IPSec

Un VPN IPSec est un logiciel VPN qui utilise le protocole IPSec pour créer des tunnels chiffrés sur Internet. Il fournit un chiffrement de bout en bout, ce qui signifie que les données sont brouillées sur l'ordinateur et décodées sur le serveur de réception.

3. Le protocole IPSec

IPSec est une combinaison des mots IP (Internet Protocol) et Sec pour security. En une définition simple, IPSec est une suite de protocoles de sécurité de communication utilisés pour sécuriser les échanges de données entre des réseaux privés virtuels ou entre les machines individuelles sur Internet. IL fournit une protection en utilisant des mécanismes de chiffrement, d'authentification, et d'intégrité pour garantir la sécurité des données transitant sur le réseau.

IPSec représente deux modes d'échange :

- Mode transport : seule la charge utile est chiffrée, mais l'en-tête IP d'origine reste inchangé.

- Mode tunnel : Le paquet entier est chiffré. Les datagrammes IP sont encapsulés dans d'autres datagrammes IP, dont le contenu est protégé.

Du point de vue de l'architecture, IPSec est situé au niveau de la couche 3, également connue sous le nom de couche réseau.

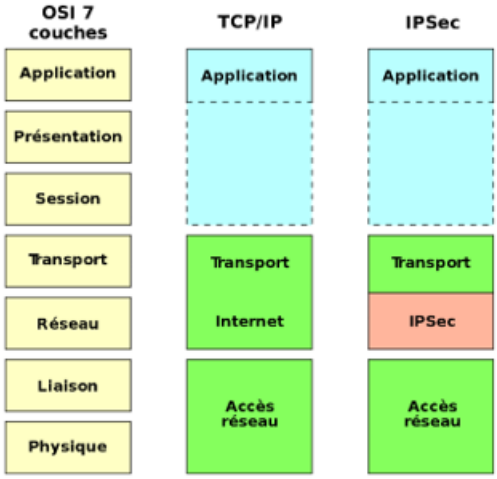


***Figure 3* :** Positionnement protocole IPsec dans le modèle OSI

4. Fonctionnement de la tunnellisation avec IPSec

Lors de l'établissement d'une connexion IPsec, plusieurs opérations sont effectuées :

- Échange de clés : La gestion des clés est le processus permettant de gérer les numéros de clés qui sont nécessaires à l'authentification et au chiffrement.

- Ajout d'en-têtes de paquets : Ces en-têtes contenant les informations d'authentification et de cryptage.

- Authentification : IPsec fournit une authentification pour chaque paquet. Cela garantit que les paquets sont provenus d'une source de confiance et non d'un attaquant.

- Cryptage : Pour que les données envoyées restent ainsi sécurisées et privées, IPsec crypte les charges utiles et l'en-tête IP de chaque paquet.

- Transmission : Les paquets IPsec chiffrés traversent un ou plusieurs réseaux jusqu'à leur destination en utilisant un protocole de transport TCP ou UDP

- Décryptage : A l'autre bout de la communication, les paquets sont décryptés et les applications peuvent maintenant utiliser les données fournies.

5. Les protocoles à la base de IPSec

- Authentication Header (AH)

Le protocole d'en-tête d'authentification (AH) ajoute un en-tête qui contient les données d'authentification de l'expéditeur et protège le contenu du paquet contre toute modification par des parties non autorisées.Elle authentifie, protège en intégrité les datagrammes IP
Cette fonctionnalité est basée sur l'utilisation d'un code d'authentification de message ou MAC (Message Autentication Code).

- Encapsulating Security Protocol (ESP)

Néanmoins, tandis que AH ne fournit pas la confidentialité des données, le protocole ESP quant à lui effectue le chiffrement de l'ensemble du paquet IP : l'en-tête IP et la charge utile. Il offre une sécurité plus complète en fournissant à la fois l'authentification, l'intégrité et la confidentialité des données par l'entremise des algorithmes de chiffrement et d'authentification.

Exemples d'algorithmes de chiffrement et d'authentification utilisés par IPsec encapsulant le protocole ESP et AH : HMAC-SHA1-96 / AES-CBC / DES-CBC / AES-GCM

- Security Association (SA) :

SA désigne un certain nombre de protocoles utilisés pour négocier des clés et des algorithmes de cryptage. L'un des protocoles SA les plus courants est l'échange de clés Internet (IKE). Internet Key Exchange gère l'échange de clés de façon automatique entre les appareils connectés.

Mécanismes de mise en œuvre de SD-WAN

Il désigne l'ensemble des techniques et fonctionnalités utilisées pour déployer et gérer le réseau SD-WAN. Il peut apporter une réponse à de nombreuses problématiques plurisectorielles, grâce aux fonctionnalités suivantes :

- Gestion centralisée

Cette centralisation de contrôleur permet de configurer et surveiller le réseau, ce qui facilite la gestion et la prise de décisions concernant les politiques de routage, la sécurité et la qualité de service.

- Interface conviviale

Les administrateurs utilisent une interface utilisateur simple pour la gestion du réseau.
Cela simplifie la configuration et accélère les cycles de déploiement.

- Routage intelligent et dynamique

Le SD-WAN utilise des algorithmes intelligents pour sélectionner automatiquement les meilleures liaisons pour acheminer le trafic en fonction des politiques définies. Ces algorithmes prennent en compte plusieurs facteurs, dont les performances des liens, la latence, la bande passante …

- Priorisation ou segmentation de trafic

Elle permet de diviser les paquets en différentes classes de services en fonction de leurs exigences en matière de qualité de service (QoS). Cette fonctionnalité permet d'améliorer les performances de certaines applications sensibles à la perte et au temps d'attente, par exemple le protocole VoIP (Voice over Internet Protocol), la visioconférence, la vidéo en temps réel…

- Redondance

En collectant des informations granulaires sur le chemin WAN, SD-WAN met en oeuvre des mécanismes de redondance pour assurer la continuité de service en cas de défaillance. Lorsqu'une liaison échoue ou connaît une dégradation des performances, le SD-WAN peut rapidement basculer le trafic vers une autre sans affecter de manière significative l'expérience utilisateur.

- Optimisation du trafic

Elle est une fonctionnalité essentielle de SD-WAN, visant à améliorer les performances et l'efficacité de la bande passante.

- Accès direct au cloud

Comme la transformation numérique pousse davantage de services vers le cloud, le SD-WAN offre un accès direct aux applications cloud critiques pour les utilisateurs situés loin du siège social.

- Mise en place de sécurité avancée

Pour protéger les données transitant sur le réseau, SD-WAN intègre des fonctionnalités de sécurité avancée : chiffrement, pare-feu, VPN…

Fournisseurs SD-WAN

Pléthorique, l'offre SD-WAN ? Les estimations de Gartner vont dans ce sens. Il compte actuellement de nombreux fournisseurs de SD-WAN sur le marché, chacun offrant des solutions variées pour répondre aux besoins spécifiques des entreprises.

Les offreurs sont jugés sur les deux axes suivants :

- Vision : centré sur les stratégies sectorielle, géographique, commerciale, marketing.

- Exécution : centré sur la capacité à répondre effectivement à la demande c'est-à-dire l'expérience client, la performance avant-vente, la qualité des produits et des services.

Le cabinet américain Gartner recense environ 70 fournisseurs. Il en classe les meilleurs dans son Magic Quadrant sur l'infrastructure WAN Edge c'est-à-dire dédié au segment de marché dont six qui creusent l'écart.

La figure suivante nous montre les fournisseurs de solutions SD-WAN retenus dans le rapport du Gartner en 2022

Figure 4 **:** Rappot Gartner - Magic Quadrant sur l'infrastructure WAN Edge

Selon ce rapport de Gartner en 2022, les six fournisseurs suivants sont classés comme leaders dans le domaine des solutions SD-WAN qui sont inchangés depuis la précédente édition :

- Fortinet reste en tête sur l'axe de l'exécution

- VMware et Palo Alto Networks sur celui de la vision, rejoint toutefois à égalité par. –

- Cisco, HPE (Aruba) et Versa Networks spécialiste indépendant du SD-WAN et du SASE

Pour notre projet, nous avons choisi spécifiquement la solution Fortinet.

Avantages de SD-WAN

Une solution flexible et évolutive fournissant des performances élevées, Le SD-WAN répond aux besoins des utilisateurs, tout en offrant de nombreux autres avantages :

- Coûts de connectivité minimisés
- Économie sur le long terme
- Meilleure performance du réseau
- Flexibilité
- Agilité améliorée
- Gain de temps en termes de déploiement et configuration
- Réduction de la complexité du réseau
- Facilité de gestion de ressources

Cas d'utilisation de SD-WAN

SD-WAN est adapté à de diverses applications dans des scénarios et environnements du réseau étendu :

- Connectivité de succursales et sites distants : Pour les réseaux d'entreprises multisites qui ont des bureaux distants et des sites géographiquement dispersés
- Connexion au cloud : pour les entreprises utilisant des services et des applications basées sur le cloud par la possibilité d'avoir un accès direct
- Pour les réseaux hybrides : mise en oeuvre de réseaux combinant des connexions MPLS, Internet, LTE
- Migration de MPLS : cette application pourrait être remplacement ou complément du MPLS pour objectif d'avoir un coût réduit et une flexibilité
- Mobilité et télétravail : Accès pour les travailleurs mobiles et aux employés en télétravail avec une connectivité sécurisée

Conclusion

La transition du MPLS au SD-WAN marque une évolution significative dans la gestion des réseaux WAN. Cette transformation majeure offre aux entreprises une connectivité accrue, plus flexible, économique et facile à gérer, tout en maintenant la pertinence du MPLS pour les applications sensibles. Il est évident que l'adoption judicieuse de cette innovation, le SD-WAN, peut considérablement améliorer les performances des réseaux et renforcer la compétitivité en informatique d'entreprise en évolution constante.