

Les réseaux privés virtuels (VPN)

VPN ont aujourd'hui pris une place importante dans les réseaux informatique et l'informatique distribuée.

1. Définition

Dans les réseaux informatiques et les télécommunications, le réseau privé virtuel (Virtual Private Network en anglais, abrégé en VPN) est vu comme une extension des réseaux locaux et préserve la sécurité logique que l'on peut avoir à l'intérieur d'un réseau local. Il correspond en fait à une interconnexion de réseaux locaux via une technique de « tunnel ».

On parle de VPN lorsqu'un organisme interconnecte ses sites via une infrastructure partagée avec d'autres organismes. Il existe deux types de telles infrastructures partagées : les « publiques » comme Internet et les infrastructures dédiées que mettent en place les opérateurs pour offrir des services de VPN aux entreprises. C'est sur Internet et les infrastructures IP que se sont développées les techniques de « tunnel ».

Historiquement les VPN inter-sites sont apparus avec X.25 sur des infrastructures mises en place par les opérateurs, puis X.25 a été remplacé par le relayage de trames, l'ATM et le MPLS aujourd'hui.

Ce réseau est dit virtuel car il relie deux réseaux « physiques » (réseaux locaux) par une liaison non fiable (Internet), et privé car seuls les ordinateurs des réseaux locaux de part et d'autre du VPN peuvent accéder aux données en clair.

Le VPN est réalisé avec les techniques d'encryptions et d'authentification, en assurant la qualité de services requise par les applications. Il permet l'économie de connexion directe coûteuse

entre les différentes implémentations de l'entreprise, l'accès Internet lui servant à la fois pour la consultation classique des sites Web et pour son réseau privé.

Les VPN sont utilisés pour :

- Réaliser des connexions à distance pour des utilisateurs mobiles ou télétravailleurs.
- Permet d'établir des connexions sécurisées privées (un réseau privé) au travers d'un réseau public comme l'Internet.
- Réaliser des interconnexion Lan to Lan.
- Contrôler l'accès dans un intranet.

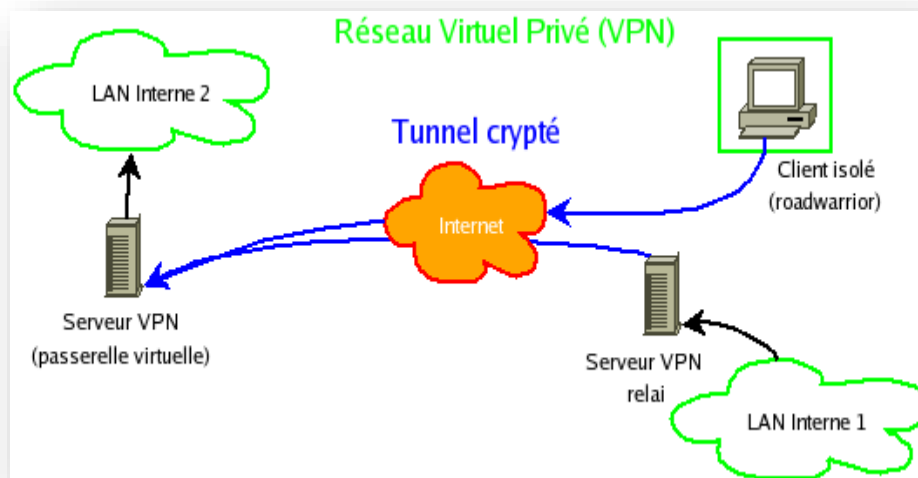


Figure Error! No text of specified style in document.2.Error! No text of specified style in document.1:Un réseau VPN

2. Principe de fonctionnement de VPN

Un VPN repose sur un protocole, appelé protocole de tunnelisation, c'est-à-dire un protocole permettant aux données passant d'une extrémité à l'autre du VPN d'être sécurisées par

des [algorithmes](#) de [cryptographie](#). Le principe de tunneling consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Par la suite, la source chiffre les données et les achemine en empruntant ce chemin virtuel. Afin d'assurer un accès aisé et peu coûteux aux intranets ou aux extranets d'entreprise, les réseaux privés virtuels d'accès simulent un réseau privé, alors qu'ils utilisent en réalité une infrastructure d'accès partagée comme Internet.

Les données à transmettre peuvent être prises en charge par un protocole différent d'IP. Dans Ce cas, le protocole de tunneling encapsule les données en ajoutant un en-tête. Le tunneling est l'ensemble des processus d'encapsulation, de transmission et de dés encapsulation. Ainsi, lorsqu'un système extérieur à un réseau privé (client nomade, agence ou travailleur à domicile) souhaite se connecter au réseau de son entreprise :

- Les paquets (qui contiennent les données) sont chiffrés par le client VPN (selon l'algorithme décidé par les deux interlocuteurs lors de l'établissement du tunnel VPN) et éventuellement signés.
- Ils sont transmis par le biais du réseau transporteur (Internet en général).
- Ils sont reçus par le serveur VPN qui les déchiffre, les traite et regarde si les vérifications requises sont correctes.

3. Les avantages et les inconvénients des VPN

Avantages

Les VPNS présentent les avantages suivants :

- ❖ **La flexibilité** : Dans le cas d'une entreprise ou d'une administration ayant plusieurs localisations, l'ajout d'un nouveau site se fait simplement en le connectant à Internet et en l'incluant sur le VPN d'entreprise. Il sera ainsi très facilement intégré sur l'intranet d'entreprise.

❖ **Réduction de coûts** : Ils permettent de se servir du réseau public Internet ou des réseaux des fournisseurs d'accès en toute sécurité. Ce qui évite la mise en place de liaisons spécialisées chères en termes d'installation et de maintenance.

❖ **Echange d'information facilité** : La mise en place de VPN permet d'accéder aux ressources du réseau local de l'entreprise de manière sécurisée, exactement de la même façon que s'ils se trouvaient dans l'entreprise.

❖ **Mise en place de nouveaux services** : Un bon niveau de sécurité vous autorise à mettre en place des services basés sur l'utilisation d'Internet et à mettre en réseau vos activités.

❖ **Sécurité renforcée** : Un niveau de sécurité élevé est indispensable pour vous garantir contre le vol ou la destruction de données essentielles à votre entreprise.

Les inconvénients

Parmi les désavantages des VPN, on peut citer :

- la disponibilité et les performances des VPN dépendent largement des fournisseurs de services et des sous-traitants. L'entreprise ou l'administration utilisant un VPN ne contrôle en effet pas tous les paramètres nécessaires.
- les standards ne sont pas toujours respectés et les technologies VPN restent dépendantes des équipements utilisés. Il est conseillé d'utiliser les équipements du même constructeur pour assurer le bon fonctionnement du VPN d'entreprise.

la mise en route d'un VPN réclame une forte expertise, et notamment une bonne compréhension de la sécurité informatique et des technologies VPN spécifiques.