

Définition

Un VPN (Virtual Private Network) est une liaison sécurisée entre 2 parties via un réseau public, en général Internet. Cette technique assure l'authentification des 2 parties, l'intégrité des données et le chiffrement de celles-ci.

Les 3 grands cas d'utilisation de VPN sont les suivants :

- Raccordement de télé travailleurs ou travailleurs mobiles. Ceux-ci se raccordent aux ressources de l'entreprise par modem, RNIS ou xDSL
- Interconnexion de succursales. Des sites distants d'une même entreprise partagent les mêmes ressources sans avoir recours à des lignes spécialisées (LS).
- Exploitation de réseaux extranets. Ce segment trouve aussi sa justification dans l'essor du commerce électronique.

Utilité

La principale raison pour implémenter un VPN est l'économie supposée par rapport à tout autre type de connexion. Bien que les VPN nécessitent l'acquisition de produits matériels et logiciels supplémentaires, le coût à terme de ce genre de communication est moindre. L'entreprise ne paye que l'accès à l'Internet via son FAI et non une communication nationale dans le cas d'une liaison RNIS ou un forfait dans le cas d'une Liaison Spécialisée. La technologie VPN procure de même la sécurité lors des connexions d'utilisateurs distants au réseau interne de l'entreprise.

Fonctionnement

L'interconnexion

Une connexion VPN met en jeu les composants suivants :

Serveur VPN

Un ordinateur qui accepte des connexions VPN de clients VPN. Un serveur VPN peut fournir une connexion VPN accès distant ou une connexion VPN routeur à routeur.

Client VPN

Un ordinateur qui initie une connexion VPN vers un serveur VPN. Un client VPN peut être un ordinateur individuel qui obtient une connexion VPN accès distant ou un routeur qui obtient une connexion VPN routeur à routeur.

Tunnel

La portion de connexion dans laquelle les données sont encapsulées.

La connexion VPN

La portion de connexion dans laquelle les données sont chiffrées. Pour des connexions VPN sécurisées, les données sont chiffrées et encapsulées dans la même portion de la connexion.

Note : Il est possible de créer un tunnel et d'envoyer les données dans le tunnel sans chiffrement. Ce n'est pas une connexion VPN car les données privées sont envoyées au travers d'un réseau partagé ou public sous une forme non chiffrée et facilement lisible.

Protocoles

Les premiers standards utilisés furent propriétaires à l'image de L2F (Layer 2 Forwarding) de Cisco et Shiva (Intel), PPTP (Point to Point Tunneling Protocol) de Microsoft et 3Com et L2TP (Layer 2 Tunneling Protocol), fusion des 2 précédents.

Cependant, le standard actuel de niveau 3 est IPsec promulgué par IETF (Internet Engineering Task Force).

Partie serveur

Windows XP vous permet de créer votre propre réseau privé virtuel (VPN). Le but est de permettre de connecter plusieurs postes au travers de l'Internet comme s'ils étaient dans un même réseau local. Une fois connectés par VPN, les postes se comportent alors comme s'ils étaient dans la même pièce, reliés au même hub. Mais la connexion VPN est cryptée, et les données circulent de façon sécurisée. Vous pouvez donc partager des documents, des répertoires, ou des périphériques, comme des imprimantes, par exemple,

Voyons les manipulations :

Dans le menu démarrer, faites "**Connexions**" puis "**Affichez toutes les connexions**".
Double-cliquez sur l'assistant nouvelle connexion

Choisissez **Configurez une connexion avancée**, puis cliquez sur **Suivant**

Choisissez **Accepter les connexions entrantes** puis cliquez sur **Suivant**.

Ne cochez rien sur l'écran Suivant écran et cliquez sur **Suivant**
Sélectionnez les utilisateurs autorisés à venir Se Connecter chez vous.
Une fois le ou les utilisateurs choisis, cliquez sur **Suivant**.

Si l'utilisateur n'existe pas encore vous pouvez le rajouter en cliquant sur **AJOUTER** et en saisissant les informations demandées puis cliquez sur **OK**.

Choisissez les services, protocoles et clients que vous voulez activez pour cette connexion VPN. Pour la plupart des usages, laissez les choix par défaut. Cliquez ensuite sur **Suivant**.

Pour avoir des précisions sur les différentes options, voici à présent le détail des options

Les options

L'option "Autoriser les correspondants appelant à accéder à mon réseau local" indique si votre poste de travail doit se comporter comme un routeur :

- Si l'option est cochée, l'appelant pourra accéder aux autres postes de votre réseau.
- Si l'option est décochée, l'appelant n'aura accès qu'à votre poste de travail.

- "Attribuer des adresses TCP/IP automatiquement avec le DHCP" permet de faire une demande auprès du serveur DHCP de votre réseau pour une adresse temporaire. Dans un environnement d'entreprise c'est un ou plusieurs serveur DHCP qui se chargent de l'attribution des adresses IP. (voir support sur le service DHCP)

- "Spécifier des adresses TCP/IP" permet d'indiquer une plage d'adresse à utiliser pour les appelants. Cette option est utile lorsqu'il n'y a pas sur le réseau de serveur DHCP.

- "Autoriser l'ordinateur appelant à spécifier sa propre adresse IP" inverse le processus d'attribution de l'adresse. Ce n'est plus votre PC qui attribue une adresse mais l'appelant qui en réclame une. Attention, cette option peut provoquer des conflits d'adresses IP sur votre réseau.

- "Partage de fichiers et d'imprimantes pour les réseaux Microsoft"

Cette ligne donne accès, si elle est cochée, au service "Serveur" de votre PC. Ainsi, l'appelant pourra accéder à vos disques, répertoires, fichiers et imprimantes partagés. Evidemment, avoir accès aux partages n'implique pas avoir les autorisations de les utiliser. Les autorisations sur partage ainsi que les droits NTFS prévalent toujours.

Nota : Il ne faut pas désinstaller de protocole ou de service depuis cet écran. Si vous ne souhaitez pas utiliser une des options, contentez-vous de décocher la case correspondante. Si vous désinstallez une option, vous la désinstallez pour toutes les connexions. Vous pouvez donc perturber le bon fonctionnement d'une connexion nécessitant cette option.

Partie cliente

Voyons les manipulations :

Dans le menu démarrer, Choisissez "**Connexions**" puis "**Affichez toutes les connexions**".

Double-cliquez sur l'assistant nouvelle connexion :

Choisissez **Connexion au réseau d'entreprise**, puis cliquez sur **Suivant**.

En effet, les VPN sont souvent utilisés dans un réseau d'entreprise pour inter-connecter les différents sites sans utiliser de coûteuses liaisons spécialisées.

Choisissez **Connexion réseau privé virtuel** puis cliquez sur **Suivant**.

Pour information, la première option vous sert à vous connecter à un réseau d'entreprise par les réseaux téléphoniques commutés, c'est à dire avec un modem. Bien sur en entreprise, un modem, voir un pool de modem, sont configurés pour accepter les appels entrants.

Saisissez le nom que vous souhaitez attribuer à cette connexion et cliquez sur **Suivant**.

Ce nom est purement informatif, vous pouvez y saisir ce que vous souhaitez. Ex: "Connexion VPN vers Untel"

Vous devez ici saisir l'adresse IP de l'ordinateur à contacter puis cliquez sur **Suivant**.

Il s'agit évidemment de l'adresse IP publique, c'est à dire celle par laquelle l'ordinateur de destination est joignable par internet.

Alors que celle-ci est généralement fixe pour un réseau d'entreprise, pour un particulier ayant l'ADSL, celle-ci change de façon régulière, car l'adresse Ip vous est attribuée via un serveur DHCP (voir cours réseau sur le DHCP). Un bon moyen est alors d'utiliser un service de DNS dynamique tel que DynDns.org.

La configuration de base est à présent terminée. Après avoir coché la case pour déposer un icône sur le bureau, vous pouvez cliquer sur **Terminer**.

Vous n'avez plus qu'à saisir le nom d'utilisateur et le mot de passe qui vous ont été fournis par l'administrateur du poste auquel vous voulez vous connecter. Cliquez ensuite sur **Se Connecter**.

Les propriétés

En cliquant sur **Propriétés**, vous aurez accès à toutes les informations que vous aurez saisies, plus quelques paramétrages avancés.

Onglet général

Établir d'abord une autre connexion vous permet de spécifier une relation de dépendance avec une autre connexion. Exemple, vous souhaitez, à travers votre connexion ADSL, établir une connexion VPN. Vous pouvez spécifier que la connexion VPN lancera seule la connexion ADSL si cette dernière n'est pas déjà lancée.

Notez cependant que couper la connexion VPN entraînera la coupure de la connexion liée. Le paramètre est donc plutôt réservé à des usagers peu habitués à jongler entre les connexions et qui préfèrent du "tout automatique".

Onglet gestion de réseau

Type de réseau VPN

Vous pouvez laisser cette option sur automatique. Cependant, il est fort peu probable que le VPN que vous allez contacter fonctionne en L2TP. Vous pouvez donc directement régler le type de VPN sur PPTP. La raison en est la complexité de mise en œuvre de la sécurité IPSec, indispensable au VPN de type L2TP. Ces VPN sont réservés généralement à des organisations importantes en taille et moyens.

Protocole Internet TCP/IP

Par défaut, vous allez recevoir une adresse IP fournie par le VPN serveur. Si vous avez la possibilité de choisir votre propre adresse (cf "Créer un VPN sous XP"), c'est ici que vous devez la spécifier.

Partage de fichiers et d'imprimantes pour les réseaux Microsoft

Cette ligne donne accès, si elle est cochée, au service "Serveur" de votre PC. Ainsi, l'appelé pourra accéder à vos disques, répertoires, fichiers et imprimantes partagés. Évidemment, avoir accès aux partages n'implique pas avoir les autorisations de les utiliser. Les autorisations sur partage ainsi que les droits NTFS prévalent toujours.

Nota :

Vous ne devez pas désinstaller de protocole ou de service depuis cet écran. Si vous ne souhaitez pas utiliser une des options, contentez-vous de décocher la case correspondant. Si vous désinstallez une option, vous la désinstallez pour TOUTES les connexions. Vous pouvez donc perturber le bon fonctionnement de connexion nécessitant cette option.

Onglet avancé

Pare-feu de connexion internet

Tout comme pour une connexion internet classique, vous avez la possibilité de vous protéger en activant le pare-feu. Cependant, alors que cela est indispensable pour une connexion internet, son utilisation dans le cas d'un VPN semble inutile. En effet, c'est vous qui choisissez de rejoindre un réseau privé. Pourquoi donc en fermer les accès ?

Partage de connexion Internet

Vous avez la possibilité de partager l'accès au VPN avec d'autres PC de votre réseau local. Il suffit d'activer l'option et de définir, sur les autres postes de votre réseau local, l'adresse IP LOCALE de ce PC comme étant la passerelle par défaut.

Concernant les firewall et routeurs, le VPN étant de type PPTP, il faut laisser passer les flux sur le port TCP 1723

Pour accéder aux fichiers partagés d'un PC à travers VPN, le plus simple est de taper dans la zone d'adresse de votre navigateur ou de l'explorateur : [\\nomdupc](#)

Pour vous connecter entre vous il faut entrer l'adresse IP du serveur (de l'hôte) dans le champ correspondant,

Attention si vous avez une IP dynamique qui change en fonction de ce qui est paramétré comme durée sur le serveur DHCP,

Ressources :

<http://www.openvpn.se/index.html>

<http://www.dyndns.fr/dyndns.html>

<http://fr.wikipedia.org/wiki/DynDNS>