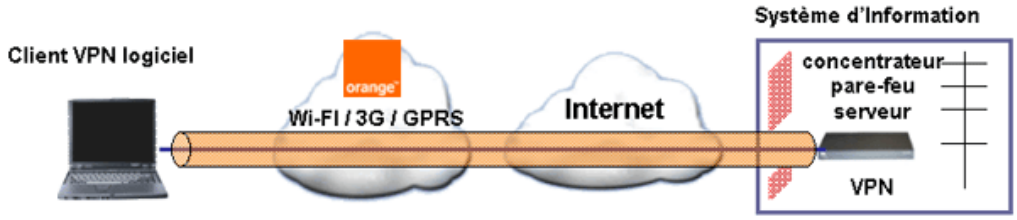
Les VPNs IP Internet : principes et usage nomade

Sommaire

VPN IP Internet

Comme expliqué dans Généralités sur les VPNs, un VPN Internet est caractérisé par le fait que l'infrastructure réseau utilisée en support est le réseau public Internet. Ce type de VPN IP repose en effet sur la création de tunnels virtuels (L2TP, PPTP, IPSec, SSL) sur Internet afin d'isoler les flux échangés entre deux extrémités. La sécurité est alors assurée par les extrémités (client logiciel et passerelle VPN dédiée intégrée soit à un routeur soit à un firewall). Le réseau Internet fonctionnant sur le mode « best effort », il n'y a par contre pas de garantie de qualité de service.



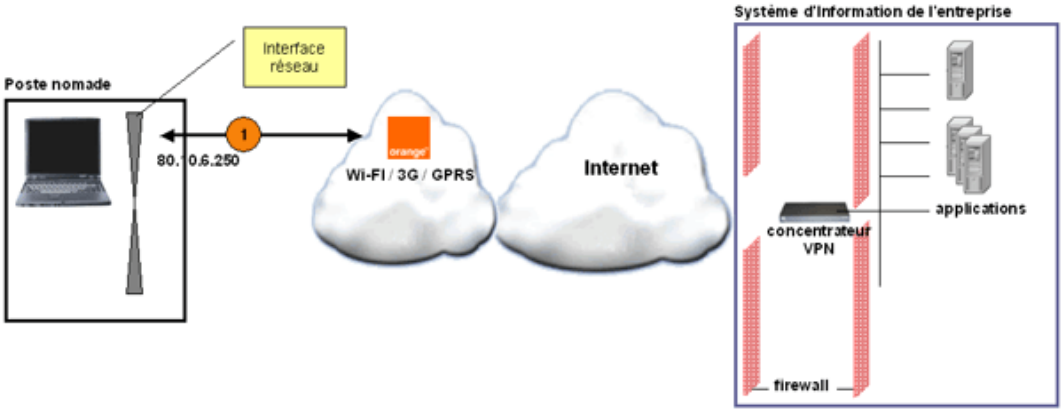
Etapes de connexion en usage nomade

Même si nous avons vu qu'un VPN répond également à d'autres besoins (télémaintenance et interconnexion de sites notamment), le cas d'usage qui nous intéresse ici est l'accès nomade au réseau de l'entreprise.

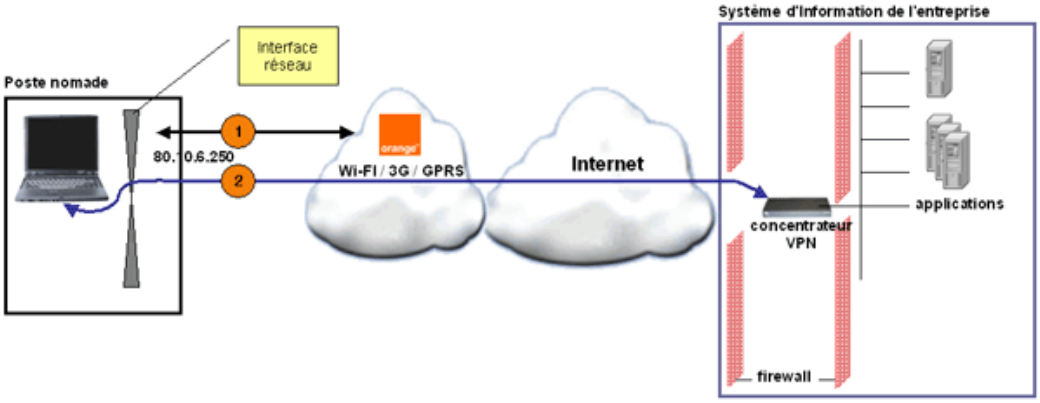
Le processus de connexion décrit ci-dessous peut être transparent ou non selon la solution utilisée et l'utilisation ou non d'un kit de connexion. Il s'applique dans la plupart des cas, sauf https et gateways SSL, qui ne reposent pas sur la mise en place d'une interface virtuelle.

Il consiste pour un collaborateur nomade, à :

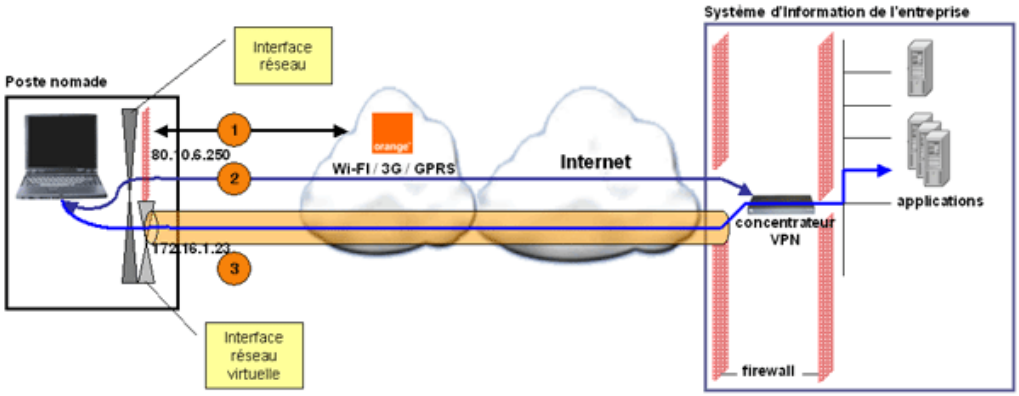
1. Connecter son PC au monde Internet via une solution d’accès mobile Orange. Le PC nomade se voit alors attribuer une adresse IP par le réseau Orange.



2. Etablir un tunnel sécurisé avec le concentrateur VPN du LAN distant en lançant le client logiciel VPN installé et configuré sur son PC. Le client VPN dialogue alors avec l'extrémité VPN située dans le SI, qui lui attribue une adresse IP du réseau privé de l'entreprise une fois que tous les contrôles de sécurité ont été effectués. Cette adresse IP est affectée à une interface réseau virtuelle du poste client.



3. Le client VPN modifie alors les règles de routage afin d'aiguiller les flux vers cette interface. Un firewall est en général lancé en complément pour bloquer tout paquet qui ne proviendrait pas du SI ou au contraire qui partirait du PC nomade vers une destination autre que le concentrateur VPN. La sécurité de l'ensemble est alors optimale.



Une fois le tunnel établi, le PC possède donc une adresse IP délivrée par Orange et une adresse IP du pool de l'entreprise. Tous les échanges entre le PC nomade et le LAN de l'entreprise se font de manière sécurisée dans ce tunnel.

Les services de sécurité offerts

Les services de sécurité offerts par un VPN dépendent bien sûr de la solution choisie mais aussi de la façon dont elle est configurée / utilisée. Les différents services liés au nomadisme et assurés par les VPN sont classiquement : L'authentification : consiste à associer de manière unique une identité à un utilisateur. On regroupe en fait par abus de langage deux fonctions dans le terme unique « authentification » :

- L'identification : consiste à associer une identité numérique présumée à une entité se connectant (utilisateur ou ressource).
- L'authentification : consiste à vérifier et à confirmer que l'entité qui s'est identifiée est bien celle qu'elle prétend être.

La confidentialité : consiste à s'assurer que les données stockées sur une entité ne peuvent être lues que par leur propriétaire et que les messages transmis ne peuvent être lus par qui que ce soit d'autre que l'émetteur et le destinataire lors d'une transmission.

L'intégrité : consiste à s'assurer que des données n'ont pas été modifiées ou supprimées sur leur entité de stockage ou pendant leur transmission sur un réseau, et que les messages qui arrivent à un destinataire sont bien ceux qui ont été envoyés par l'émetteur.

Le contrôle d'accès : consiste à offrir un accès personnalisé aux services ou ressources auxquels un utilisateur a droit sur le système d'information, interdire ceux auxquels il n'a pas droit. Il repose donc sur l'authentification préalable. Le dossier « Sécurité et Nomadisme » disponible sur ce site présente en détail les différentes techniques permettant l'implémentation de ces fonctions (techniques de chiffrement symétrique / asymétrique, algorithmes de chiffrement, certificats, mots de passe, PKI, etc.) :
Dossier « Sécurité et Nomadisme »

Les différentes solutions de VPN Internet

Il existe différentes technologies permettant d'établir des VPN Internet. La liste ci-dessous présente les principaux VPNs :

- PPTP (Point To Point Tunneling Protocol)
- IPSec (IP Security Protocol)
- L2TP / IPSec (Layer 2 Tunneling Protocol)
- SSL (Secure Socket Layer)

Dans le monde du VPN Internet, les solutions à base d'IPSec, apparues après PPTP, sont certainement les plus déployés à ce jour, même si les VPN SSL, actuellement en plein essor, pourraient bien les remplacer à moyen terme dans les entreprises pour l'accès des collaborateurs nomades ou des partenaires, IPSec restant la référence pour l'interconnexion de sites distants.

Les points suivants font une présentation succincte de ces différentes technologies, sur lesquelles nous revenons plus en détail dans les focus de ce dossier VPNs.

VPN IPSec : IP Security Protocol

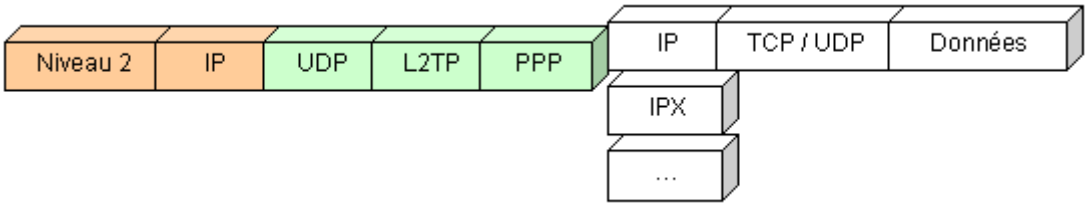
Situé au niveau de la couche réseau (niveau 3), IPSec est une suite de protocoles pour IP développée par l'IETF, conçue pour fournir les services nécessaires à la sécurisation d'échanges de données IP au travers d'un réseau partagé. Véritable extension de IP, IPSec repose sur les protocoles AH (Authentication Header) et ESP (Encapsulation Security Payload).

Outre le niveau de sécurité optimal offert, tout à fait adapté pour des applications sensibles, l'avantage majeur d'IPSec est sa normalisation, même si l'interopérabilité entre solutions de différents éditeurs est loin d'être automatique en pratique du fait des différences d'implémentation entre éditeurs. L'utilisation de L2TP/IPSec permet par ailleurs de transporter les protocoles non IP supportés par L2TP. A noter qu'IPSec est de plus en plus fortement concurrencé par les technologies SSL décrites ci-dessous pour l'accès distant à un réseau privé.

VPN L2TP et L2TP/IPSec : Layer 2 Tunneling Protocol

Combinant les avantages de PPTP et L2F (Layer 2 Forwarding développé par Cisco, qui n'est plus utilisé), L2TP est un protocole de niveau 2 développé conjointement par Cisco Systems, Microsoft, Ascend, 3Com et par d'autres acteurs-clés du marché des réseaux. Il permet l'encapsulation de trames PPP notamment sur un réseau IP, en reposant sur UDP, et donc de

véhiculer IP, IPX, NetBios, etc.



Egalement simple de mise en œuvre, il est à noter que d'un strict point de vue sécurité L2TP seul n'apporte pas grand-chose par rapport à PPTP (mécanismes identiques).

Aussi L2TP est-il généralement utilisé sur IPSec (L2TP/IPSec) pour bénéficier de la robustesse des mécanismes d'authentification / chiffrement d'IPSec tout en conservant l'authentification utilisateur et le support non limité à IP permis par L2TP.
Fiche technique : ***Cf*** (Fiche de solution VPN/L2TP/IPSEC) en bas de l'article.
Exemples d'implémentation : ***Cf*** (Configuration VPN L2TP/IPSec sur Pocket PC et usages Remote Desktop et Intranet)

VPN SSL et solutions SSL

Les solutions à base de SSL font actuellement une percée remarquée au sein du marché des VPNs. Elles peuvent être grossièrement partagées en trois en fonction du périmètre d'utilisation, le cas des protocoles sécurisés étant un peu à part :

- Les protocoles sécurisés

HTTPS, POPS, FTPS, etc. sont des exemples d'extensions standardisées de protocoles TCP/IP (HTTP, POP et FTP en l'occurrence), qui implémentent SSL pour faire circuler les données dans un tunnel chiffré. Il s'agit à chaque fois d'un usage monoapplicatif entre un client et un serveur implémentant tous les deux le protocole sécurisé (navigateur web par exemple dans le cas de https).
Fiche technique : Cf (Fiche solution HTTPS) en bas de l'article

- Les solutions de niveau applicatif basées sur une passerelle SSL (ou Gateway SSL)

Sans client spécifique autre qu'un simple navigateur et un client semi léger téléchargé via le navigateur (ActiveX, applet, etc.), ce type de solutions, communément regroupées sous la dénomination "Gateway SSL" est en général porté par des sociétés jeunes ou venant du secteur des applications (Avantail, Whale Communications, etc.).

- Les solutions VPN SSL de niveau réseau

Nécessitant le déploiement d'un client lourd et d'un certificat sur le poste client, ce type de solution est fonctionnellement comparable aux solutions IPSec et fonctionne sur le mécanisme décrit plus haut. Il est souvent porté par les acteurs historiques des solutions réseau (Nortel, Cisco, etc.), mais également Opensource (OpenVPN). ***Une idée reçue*** fréquemment diffusée, mais fausse, est qu'un VPN SSL ne serait capable de protéger que des flux applicatifs entre un utilisateur

distant et une passerelle SSL, par opposition à IPSec qui connecte des machines à des réseaux privés entiers. Cette croyance erronée est probablement due à l'assimilation de SSL aux deux premières catégories listées ci-dessous, l'abus par certains éditeurs du terme générique « VPN » pour désigner leurs solutions, indépendamment du service rendu. Un VPN SSL offrant de la connectivité réseau est en effet tout à fait capable de tunneliser n'importe quel protocole avec des ***fonctionnalités équivalentes à celles offertes par un VPN IPSec***, le chiffrement du tunnel étant basé sur la souche et les librairies de chiffrement SSL/TLS présents sur l'OS plutôt que sur les protocoles et librairies IPSec.
Exemples d'implémentation : Cf (Configuration VPN SSL OpenVPN sur Windows XP)
Le principal avantage d'un VPN SSL réside incontestablement dans sa simplicité, liée à l'usage de protocoles natifs de l'OS et au fait qu'il agit au niveau utilisateur, par opposition à IPSec qui opère au niveau du noyau. Avantage qui devient un inconvénient lorsqu'il s'agit de véhiculer des protocoles très sensibles aux temps de latence du type VoIP ou visio. Il est probable que les solutions de VPN SSL et VPN IPSec coexistent dans les prochaines années en tant que solutions dominantes pour l'accès distant sécurisé sur Internet, avant que les technologies SSL ne prennent vraiment le pas sur IPSec du fait de l'enrichissement progressif des fonctionnalités offertes et de leur intégration dans les passerelles VPN des grands acteurs historiques du marché.

Comparatif des différentes solutions

Le tableau ci-dessous propose une synthèse des forces et faiblesses des différentes solutions.

Solutions	Fonctionnalités	Facilité de mise en oeuvre	Economie de mise en oeuvre	Niveau de Sécurité
HTTPS	*	****	*** ou ****(1)	***
Gateways SSL	**	**	***	***
PPTP	***	***	***	*
VPN IP Sec+L2TP	****	*	*	****
VPN SSL	****	**	**	****

Légende : *: faible **: moyen ***: élevé ****: très élevé
(1) : **** si pas d'achat de certificat délivré par une autorité de certification (ex.Verisign)

Documents joints :

- Fiche Solution VPN L2TP/IPSec
- Configuration VPN L2TP/IPSec sur Pocket PC et usages Remote Desktop et Intranet
- Fiche solution HTTPS
- Configuration VPN SSL OpenVPN sur Windows XP