Retrouvez l'ensemble de la documentation technique des réseaux Orange France sur Orange Developer.

Généralités sur les VPNs

Sommaire

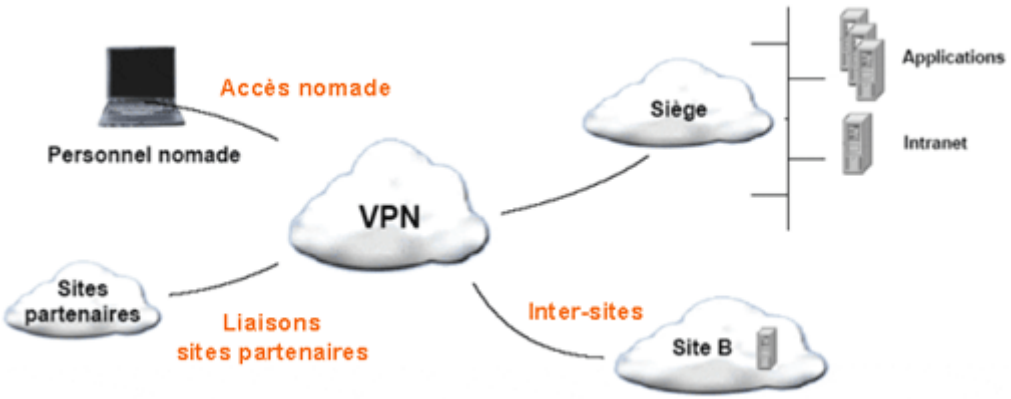
Qu'est-ce qu'un VPN ?

Un VPN est une solution de communication pour laquelle les infrastructures de transport sont partagées entre plusieurs utilisateurs : on parle de réseau privé virtuel (VPN : Virtual Private Network). Plus concrètement, un VPN consiste en un tunnel logique établi entre deux entités, permettant de rendre invisible de l'extérieur les données qui y circulent. Les solutions de type VPN sont à opposer aux réseaux privés (liaisons spécialisées par exemple) où l'entreprise dispose de ressources dédiées sur des infrastructures qui lui sont propres, mais dont elle doit assurer elle-même l'exploitation et la maintenance. Cette dernière approche se justifie de moins en moins avec le développement des VPNs sur infrastructures mutualisées, qui offrent les mêmes fonctions et bénéfices qu'un réseau privé tout en étant plus flexibles et moins chers.

A quoi sert un VPN ?

Un VPN peut être utilisé par une entreprise pour :

- les accès de télémaintenance
- l'interconnexion de ses sites distants
- la communication avec ses clients, fournisseurs ou partenaires
- la connexion des nomades au réseau de l'entreprise



Pour la télémaintenance, les accès sont généralement établis par réseau commuté (modem ou PABX) et par l'utilisation d'un logiciel de prise de contrôle à distance tels que PCANYWHERE ou VNC Viewer. Ces pratiques, utilisées seules, sont dangereuses, car il est assez aisé de pirater un PABX, d'autant plus que l'entreprise ne pensera pas forcément à sécuriser ses accès téléphoniques. Les accès VPN peuvent donc représenter une alternative sécurisée pour maintenir les serveurs à distance. La politique de sécurité choisie s'assurera que seules les machines à maintenir sont accessibles pour les personnes habilitées.

Les VPNs peuvent également être utilisés ***pour interconnecter les sites distants au site central***. A la place de liaisons RNIS ou des LS, coûteuses, une entreprise peut substituer une connexion ADSL et établir un tunnel VPN entre ses sites distants et le site du siège. Le VPN peut par exemple être établi entre les routeurs. Les sites distants utilisent de cette manière un réseau mutualisé (le réseau Internet par exemple) pour venir se connecter au réseau du siège central.

La communication avec ses clients, fournisseurs ou partenaires est également un enjeu fort pour l'entreprise. Une solution de type VPN répond au besoin de partage maitrisé de l'information voire des applications ou processus, permettant de gagner en réactivité et efficacité.

Les VPN sont enfin utilisés ***pour les nomades*** se déplaçant et voulant se connecter au réseau « interne » de l'entreprise. Avec l'utilisation des tunnels VPNs, une simple connexion à Internet suffit. Où qu'il soit, chez un client ou à l'hôtel par exemple, le nomade branche son portable sur Internet, lance son client VPN et demande à établir le tunnel vers son réseau interne. Une fois la connexion établie, il pourra circuler sur le réseau de l'entreprise comme s'il y était physiquement.

Entre quelles extrémités peut être établi un VPN ?

Pour établir un VPN, on a besoin de deux entités aux extrémités du tunnel, qui savent gérer le protocole utilisé pour le VPN.

Ces entités peuvent être les suivantes :

- Un routeur
- Un pare-feu qui sait gérer les VPN : pratiquement tous les pare-feu aujourd'hui prétendent savoir gérer les VPN, mais il faut faire attention à la baisse de performances engendrée
- Un concentrateur VPN qui est une boîte noire spécialement conçue pour recevoir des tunnels VPN
- Un serveur logiciel VPN qui joue le même rôle qu'un concentrateur VPN. Certaines solutions sont gratuites et/ou intégrées dans le système d'exploitation. Les solutions payantes offrent souvent des fonctionnalités de sécurité supplémentaires
- Un client logiciel VPN qui permet d'établir un tunnel vers un routeur, un pare-feu, un concentrateur ou un serveur. Certains clients VPN sont gratuits et d'autres sont payants. Les versions payantes incluent dans la plupart des cas des fonctionnalités de sécurité améliorées qui garantissent que la politique de sécurité choisie n'est pas changée par l'utilisateur

Un tunnel peut donc être établi entre deux routeurs, entre deux pare-feu, entre un routeur et un concentrateur, entre un client et un pare-feu, etc.

Ces éléments doivent être inter opérables entre eux, c'est-à-dire qu'ils doivent supporter la même version du protocole utilisé pour le VPN avec la même interprétation des standards associés. Peu importe ensuite les types de réseaux sur lequel transite le tunnel et les équipements qu'il rencontre sur son chemin.

Quels sont les différents types de VPN ?

Plusieurs technologies permettent de constituer un réseau VPN : les technologies traditionnelles ATM et Frame Relay permettent d'isoler et de gérer de manière indépendante, sur une même infrastructure physique, des flux générés par des entités différentes *(**VPN ATM** et **VPN Frame Relay**).*

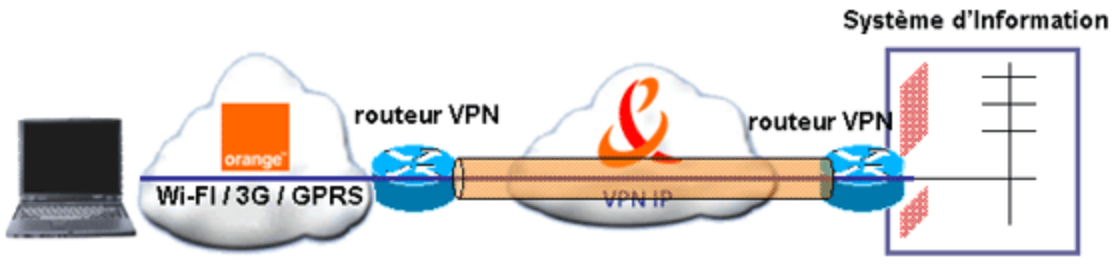
Un VPN utilisant un ***réseau IP mutualisé**,* maîtrisé ou non, comme réseau support est quant à lui appelé ***VPN IP**.* Le marché des VPNs est aujourd'hui dominé par ce dernier type de VPN du fait de la convergence vers le monde IP et de la réduction des coûts qu'il induit.

VPNs IP : VPN IP Opérateur et VPN IP Internet

On distingue deux types de VPN IP, en fonction de l'infrastructure de transport sur laquelle il s'appuie :

- Les VPNs IP « opérateurs » ou « privés »

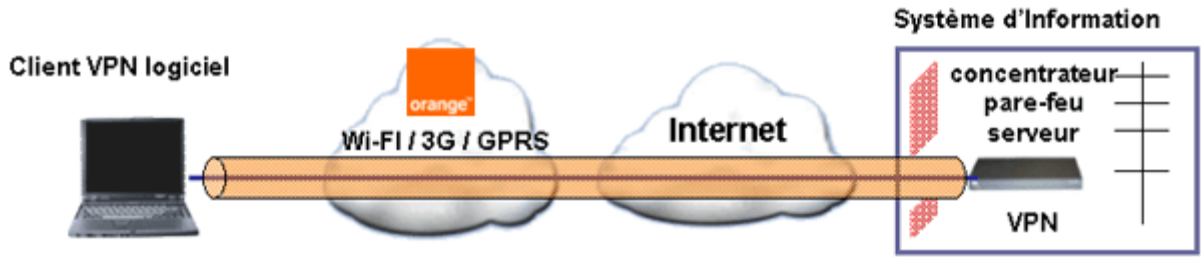
Dans le cas d'un VPN opérateur, le réseau utilisé est basé sur les infrastructures IP privées et managées d'un opérateur de télécommunications et permettent un transport direct et natif des flux IP. La sécurité et la qualité de service sont alors assurés par le réseau de l'opérateur (technologies ***MPLS*** ou ***IPSec***). Les VPNs IP opérateurs cumulent les avantages du protocole IP et ceux des VPN traditionnels comme le Frame Relay (sécurité et classes de service).



Ce type de VPN est à la base des offres d'Orange Business Service de type "Business VPN" et de l'option "Secure Mobile Access Intranet" pour les accès mobiles.

- Les VPNs IP « Internet »

L'infrastructure réseau utilisée est le réseau public Internet. Ce type de VPN IP repose sur la création de tunnels virtuels (***L2TP, PPTP, IPSec, SSL***) sur le réseau public 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 aucune garantie de qualité de service.



L'objet de ce dossier est de présenter les différents protocoles et solutions de type VPN IP Internet à la disposition des entreprises pour isoler et sécuriser les flux de bout en bout entre les terminaux mobiles de leur flotte et leur SI. Nous ne rentrerons donc pas ici dans le détail des VPNs opérateurs, le choix de la technologie et la gestion étant dans ce cas assuré par l'opérateur.