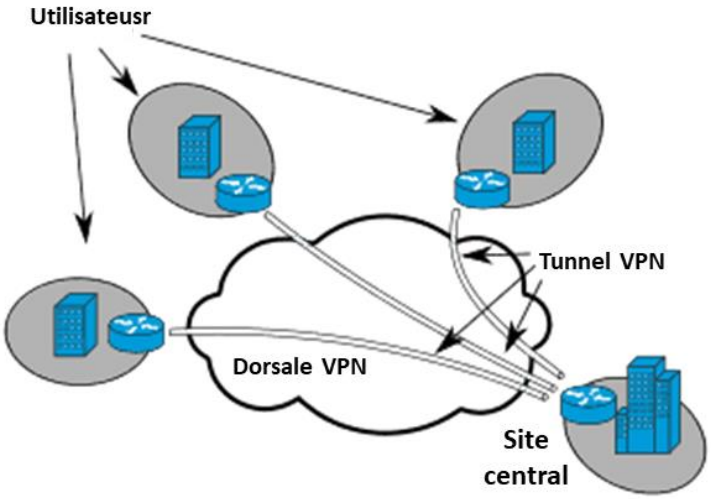
Réseaux VPN

Le **VPN** (Virtual Private Network en anglais) ou **RVP** (réseau virtuel privé en français) est un outil en vogue chez les utilisateurs d'Internet, au bureau comme au domicile. De nombreux utilisateurs n'ont pourtant pas encore connaissance de cette solution aux nombreux atouts en termes de **cybersécurité.**



1 – Introduction au réseau privé virtuel VPN

Les applications et les systèmes distribués font de plus en plus partie intégrante du paysage d'un grand nombre d'entreprises. Ces technologies ont pu se développer grâce aux performances toujours plus importantes des réseaux locaux. Mais le succès de ces applications a fait aussi apparaître un de leur écueil. En effet si les applications distribuées deviennent le principal outil du système d'information de l'entreprise, comment assurer leur accès sécurisé au sein de structures parfois réparties sur de grandes distances géographiques ? Concrètement comment une succursale d'une entreprise peut-elle accéder aux données situées sur un serveur de la maison mère distant de plusieurs milliers de kilomètres ?

Les VPN ont commencé à être mis en place pour répondre à ce type de problématique. Mais d'autres problématiques sont apparues et les VPN ont aujourd'hui pris une place importante dans les réseaux informatique et l'informatique distribuées. Nous verrons ici quelles sont les principales caractéristiques des VPN à travers un certain nombre d'utilisation type. Nous nous intéresserons ensuite aux protocoles permettant leur mise en place.

Opter pour un **VPN** vous permet par exemple de :

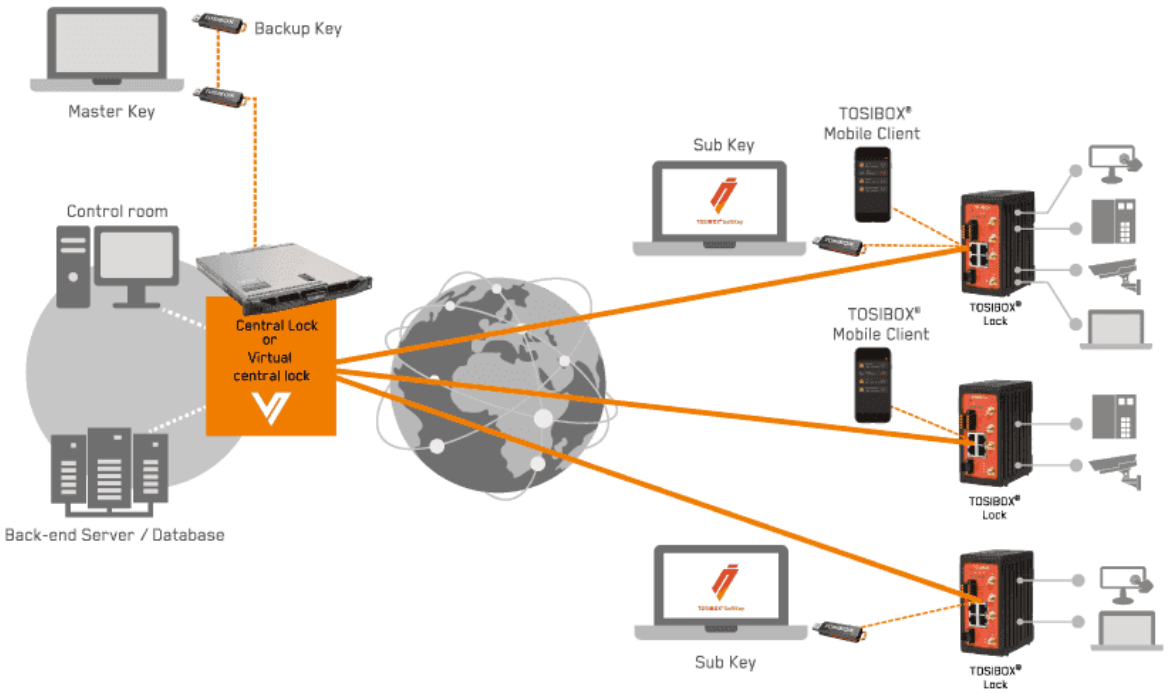
- Sécuriser les connexions sur un ou plusieurs appareils distants
- Protéger les communications
- Accéder à des contenus géolocalisés (chaînes TV étrangères, cybercensure, etc.)

Dans le **domaine industriel** plusieurs usages sont fait des VPN. On retrouvera par exemple:

- Maintenance à distance sécurisée
- Interconnexion de sites distants
- accès à distance à vos équipements de manière sécurisée

- …

Avec l'avènement de l'IoT et des menaces de sécurité, il devient primordial pour les industriels de s'équiper intelligemment de solutions sécurisées.



2 – Principe de fonctionnement du VPN

2.1 – Principe général

Un réseau VPN repose sur un protocole appelé « protocole de tunneling ». Ce protocole permet de faire circuler les informations de l'entreprise de façon cryptée d'un bout à l'autre du tunnel. Ainsi, les utilisateurs ont l'impression de se connecter directement sur le réseau de leur entreprise.

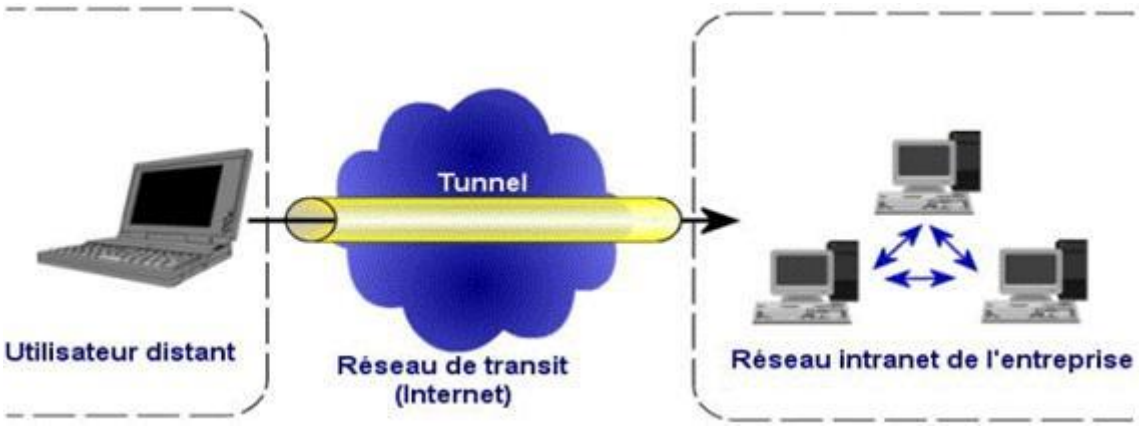
Le principe de tunneling consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Par la suite, la source chiffre les données et les achemine en empruntant Ce chemin virtuel. Afin d'assurer un accès aisé et peu coûteux aux intranets ou aux extranets d'entreprise, les 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 entête. Le tunneling est l'ensemble des processus d'encapsulation, de transmission et de désencapsulassions.

2.2 – Fonctionnalités des VPN

Il existe 3 types standard d'utilisation des VPN. En étudiant ces schémas d'utilisation, il est possible d'isoler les fonctionnalités indispensables des VPN.

2.2.1 – Le VPN d'accès



Le VPN d'accès est utilisé pour permettre à des utilisateurs itinérants d'accéder au réseau privé. L'utilisateur se sert d'une connexion Internet pour établir la connexion VPN. Il existe deux cas:

- L'utilisateur demande au fournisseur d'accès de lui établir une connexion cryptée vers le serveur distant : il communique avec le Nas (Network Access Server) du fournisseur d'accès et c'est le Nas qui établit la connexion cryptée.
- L'utilisateur possède son propre logiciel client pour le VPN auquel cas il établit directement la communication de manière cryptée vers le réseau de l'entreprise.

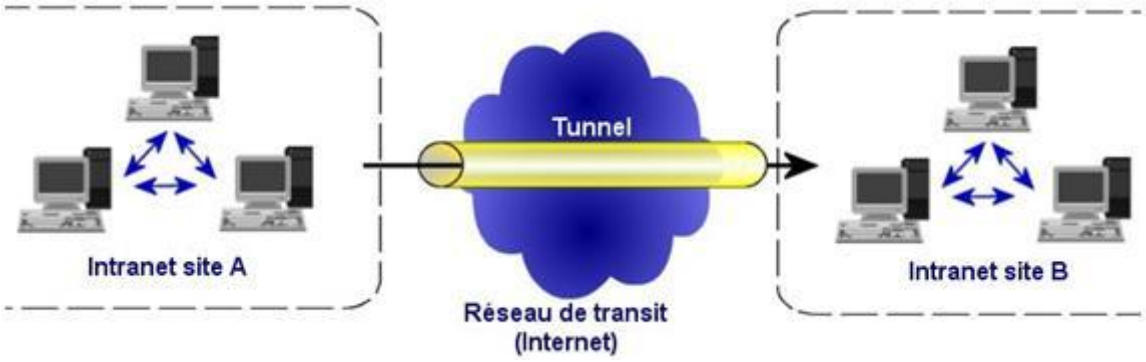
Les deux méthodes possèdent chacune leurs avantages et leurs inconvénients :

- La première permet à l'utilisateur de communiquer sur plusieurs réseaux en créant plusieurs tunnels, mais nécessite un fournisseur d'accès proposant un Nas compatible avec la solution VPN choisie par l'entreprise. De plus, la demande de connexion par le Nas n'est pas cryptée Ce qui peut poser des problèmes de sécurité.
- Sur la deuxième méthode Ce problème disparaît puisque l'intégralité des informations sera cryptée dès l'établissement de la connexion. Par contre, cette solution nécessite que chaque client transporte avec lui le logiciel, lui permettant d'établir une communication cryptée. Nous verrons que pour pallier

Ce problème certaines entreprises mettent en place des VPN à base de SSL, technologie implémentée dans la majorité des navigateurs Internet du marché.

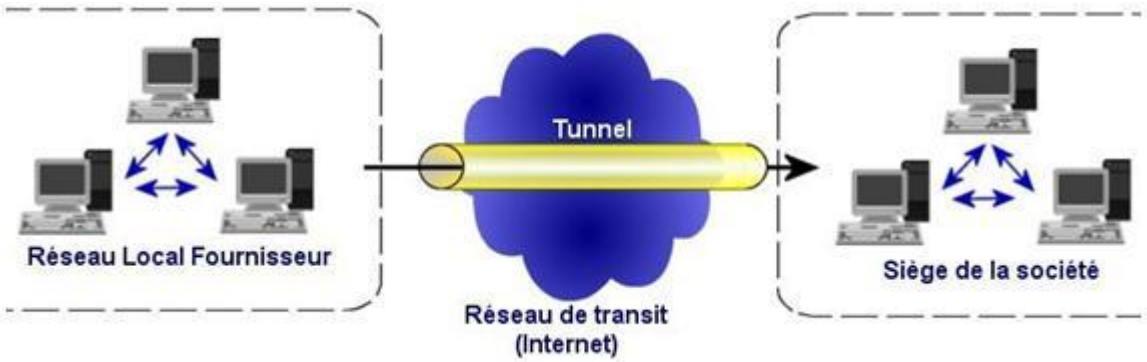
Quelle que soit la méthode de connexion choisie, Ce type d'utilisation montre bien l'importance dans le VPN d'avoir une authentification forte des utilisateurs. Cette authentification peut se faire par une vérification « login / mot de passe », par un algorithme dit « Tokens sécurisés » (utilisation de mots de passe aléatoires) ou par certificats numériques.

2.2.2 – L'intranet VPN



L'intranet VPN est utilisé pour relier au moins deux intranets entre eux. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants. Le plus important dans Ce type de réseau est de garantir la sécurité et l'intégrité des données. Certaines données très sensibles peuvent être amenées à transiter sur le VPN (base de données clients, informations financières…). Des techniques de cryptographie sont mises en oeuvre pour vérifier que les données n'ont pas été altérées. Il s'agit d'une authentification au niveau paquet pour assurer la validité des données, de l'identification de leur source ainsi que leur non-répudiation. La plupart des algorithmes utilisés font appel à des signatures numériques qui sont ajoutées aux paquets. La confidentialité des données est, elle aussi, basée sur des algorithmes de cryptographie. La technologie en la matière est suffisamment avancée pour permettre une sécurité quasi parfaite. Le coût matériel des équipements de cryptage et décryptage ainsi que les limites légales interdisent l'utilisation d'un codage » infaillible « . Généralement pour la confidentialité, le codage en lui-même pourra être moyen à faible, mais sera combiné avec d'autres techniques comme l'encapsulation Ip dans Ip pour assurer une sécurité raisonnable.

2.2.3 – L'extranet VPN



Une entreprise peut utiliser le VPN pour communiquer avec ses clients et ses partenaires. Elle ouvre alors son réseau local à ces derniers. Dans Ce cadre, il est fondamental que l'administrateur du VPN puisse tracer les clients sur le réseau et gérer les droits de chacun sur celui-ci.

2.2.4 – Bilan des caractéristiques fondamentales d'un VPN

Un système de VPN doit pouvoir mettre en oeuvre les fonctionnalités suivantes :

- Authentification d'utilisateur. Seuls les utilisateurs autorisés doivent pouvoir s'identifier sur le réseau virtuel. De plus, un historique des connexions et des actions effectuées sur le réseau doit être conservé.
- Gestion d'adresses. Chaque client sur le réseau doit avoir une adresse privée. Cette adresse privée doit rester confidentielle. Un nouveau client doit pourvoir se connecter facilement au réseau et recevoir une adresse.
- Cryptage des données. Lors de leurs transports sur le réseau public les données doivent être protégées par un cryptage efficace.
- Gestion de clés. Les clés de cryptage pour le client et le serveur doivent pouvoir être générées et régénérées.
- Prise en charge multiprotocole. La solution VPN doit supporter les protocoles les plus utilisés sur les réseaux publics en particulier Ip.

Le VPN est un principe : il ne décrit pas l'implémentation effective de ces caractéristiques. C'est pourquoi il existe plusieurs produits différents sur le marché dont certains sont devenus standard, et même considérés comme des normes.

3 – Protocoles utilisés pour réaliser une connexion VPN

Nous pouvons classer les protocoles que nous allons étudier en deux catégories:

- Les protocoles de niveau 2 comme PPTP et L2TP.
- Les protocoles de niveau 3 comme IPSec ou MPLS.

Il existe en réalité trois protocoles de niveau 2 permettant de réaliser des VPN : PPTP (de Microsoft), L2F (développé par CISCO) et enfin L2TP. Nous

n'évoquerons dans cette étude que PPTP et L2TP : le protocole L2F ayant aujourd'hui quasiment disparut. Le protocole PPTP aurait sans doute lui aussi disparut sans le soutien de Microsoft qui continue à l'intégrer à ses systèmes d'exploitation Windows. L2TP est une évolution de PPTP et de L2F, reprenant les avantages des deux protocoles.

Les protocoles de couche 2 dépendent des fonctionnalités spécifiées pour PPP (Point to Point Protocol), c'est pourquoi nous allons tout d'abord rappeler le fonctionnement de Ce protocole.

3.1 – Rappels sur PPP

PPP (Point to Point Protocol) est un protocole qui permet de transférer des données sur un lien synchrone ou asynchrone. Il est full duplex et garantit l'ordre d'arrivée des paquets. Il encapsule les paquets Ip, Ipx et Netbeui dans des trames PPP, puis transmet ces paquets encapsulés au travers de la liaison point à point. PPP est employé généralement entre un client d'accès à distance et un serveur d'accès réseau (Nas). Le protocole PPP est défini dans la RFC 1661 appuyé de la RFC 2153

3.1.1 – Généralités

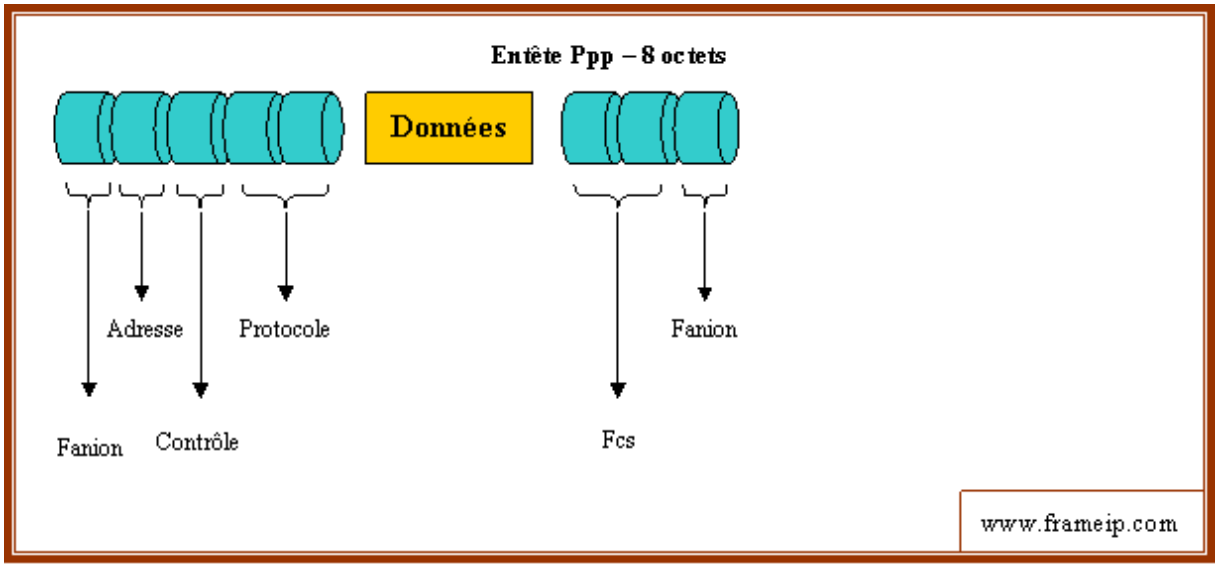
PPP est l'un des deux protocoles issus de la standardisation des communications sur liaisons séries (Slip étant le deuxième). Il permet non seulement l'encapsulation de datagrammes, mais également la résolution de certains problèmes liés aux protocoles réseaux comme l'assignation et la gestion des adresses (Ip, X25 et autres).

Une connexion PPP est composée principalement de trois parties :

- Une méthode pour encapsuler les datagrammes sur la liaison série. PPP utilise le format de trame Hdlc (Hight Data Level Control) de l'ISO (International Standartization Organisation).
- Un protocole de contrôle de liaison (Lcp – Link Control Protocol) pour établir, configurer et tester la connexion de liaison de données.Plusieurs protocoles de contrôle de réseaux (Ncps – Network trol Protocol) pour établir et configurer les différents protocoles de couche réseau.

- **3.1.2 – Format d'une trame PPP**

-



- **Fanion** – Séparateur de trame égale à la valeur 01111110. Un seul drapeau est nécessaire entre 2 trames.
- **Adresse** – PPP ne permet pas un adressage individuel des stations donc Ce champ doit être à 0xFF (toutes les stations). Toute adresse non reconnue entraînera la destruction de la trame.
- **Contrôle** – Le champ contrôle doit être à 0x03
- **Protocole** – La valeur contenue dans Ce champ doit être impaire (l'octet de poids fort étant pair). Ce champ identifie le protocole encapsulé dans le champ informations de la trame. Les différentes valeurs utilisables sont définies dans la RFC « assign number » et représentent les différents protocoles supportés par PPP (Osi, Ip, Decnet IV, Ipx…), les Ncp associés ainsi que les Lcp.
- **Données** – De longueur comprise entre 0 et 1500 octets, Ce champ contient le datagramme du protocole supérieur indiqué dans le champ « protocole ». Sa longueur est détectée par le drapeau de fin de trame, moins deux octets de contrôle.
- **Fcs (Frame Check Sequence**) – Ce champ contient la valeur du checksum de la trame. PPP vérifie le contenu du Fcs lorsqu'il reçoit un paquet. Le contrôle d'erreur appliqué par PPP est conforme à X25.

- **3.1.3 – Les différentes phases d'une connexion PPP**

Toute connexion PPP commence et finit par une phase dite de « liaison morte ». Dès qu'un événement externe indique que la couche physique est prête, la connexion passe à la phase suivante, à savoir l'établissement de la liaison. Comme PPP doit être supporté par un grand nombre d'environnements, un protocole spécifique a été élaboré et intégré à PPP pour toute la phase de connexion ; il s'agit de Lcp (Link Control Protocol). Lcp est un protocole utilisé pour établir, configurer, tester, et terminer la connexion PPP. Il permet de manipuler des tailles variables de paquets et effectue un certain nombre de tests sur la configuration. Il permet notamment de détecter un lien bouclé sur lui-même.

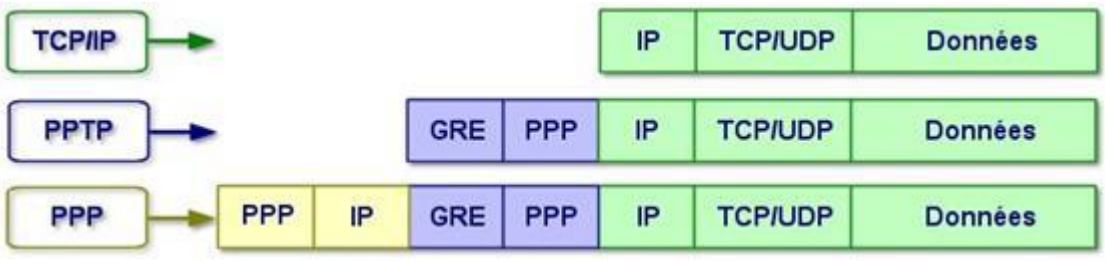
La connexion PPP passe ensuite à une phase d'authentification. Cette étape est facultative et doit être spécifiée lors de la phase précédente

Si l'authentification réussie ou qu'elle n'a pas été demandée, la connexion passe en phase de « Protocole réseau ». C'est lors de cette étape que les différents protocoles réseaux sont configurés. Cette configuration s'effectue séparément pour chaque protocole réseau. Elle est assurée par le protocole de contrôle de réseau (Ncp) approprié. A Ce moment, le transfert des données est possible. Les NPC peuvent à tout moment ouvrir ou fermer une connexion. PPP peut terminer une liaison à tout moment, parce qu'une authentification a échouée, que la qualité de la ligne est mauvaise ou pour toute autre raison. C'est le Lcp qui assure la fermeture de la liaison à l'aide de paquets de terminaison. Les Ncp sont alors informés par PPP de la fermeture de la liaison.

3.2 – Le protocole PPTP

PPTP, définit par la RFC 2637, est un protocole qui utilise une connexion PPP à travers un réseau Ip en créant un réseau privé virtuel (VPN). Microsoft a implémenté ses propres algorithmes afin de l'intégrer dans ses versions de windows. Ainsi, PPTP est une solution très employée dans les produits VPN commerciaux à cause de son intégration au sein des systèmes d'exploitation Windows. PPTP est un protocole de niveau 2 qui permet l'encryptage des données ainsi que leur compression. L'authentification se fait grâce au protocole Ms-Chap de Microsoft qui, après la cryptanalyse de sa version 1, a révélé publiquement des failles importantes. Microsoft a corrigé ces défaillances et propose aujourd'hui une version 2 de Ms-Chap plus sûre. La partie chiffrement des données s'effectue grâce au protocole Mppe (Microsoft Point-to-Point Encryption).

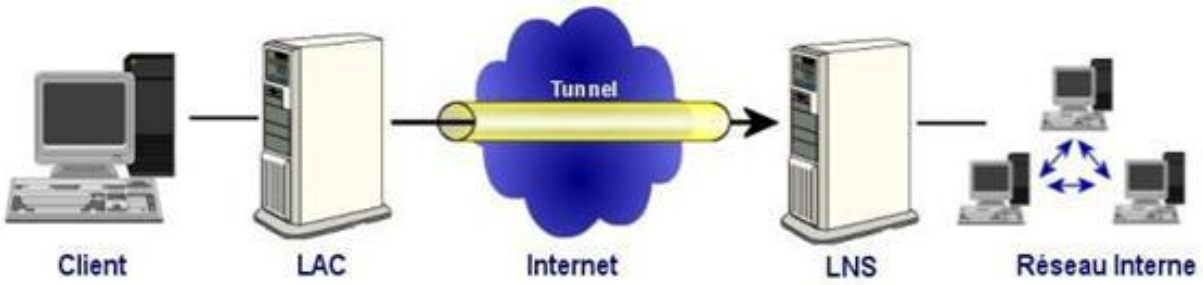
Le principe du protocole PPTP est de créer des paquets sous le protocole PPP et de les encapsuler dans des datagrammes IP. PPTP crée ainsi un tunnel de niveau 3 défini par le protocole Gre (Generic Routing Encapsulation). Le tunnel PPTP se caractérise par une initialisation du client, une connexion de contrôle entre le client et le serveur ainsi que par la clôture du tunnel par le serveur. Lors de l'établissement de la connexion, le client effectue d'abord une connexion avec son fournisseur d'accès Internet. Cette première connexion établie une connexion de type PPP et permet de faire circuler des données sur Internet. Par la suite, une deuxième connexion dial-up est établie. Elle permet d'encapsuler les paquets PPP dans des datagrammes IP. C'est cette deuxième connexion qui forme le tunnel PPTP. Tout trafic client conçu pour Internet emprunte la connexion physique normale, alors que le trafic conçu pour le réseau privé distant, passe par la connexion virtuelle de PPTP



Plusieurs protocoles peuvent être associés à PPTP afin de sécuriser les données ou de les compresser. On retrouve évidement les protocoles développés par Microsoft et cités précédemment. Ainsi, pour le processus d'identification, il est possible d'utiliser les protocoles Pap (Password Authentification Protocol) ou MsChap. Pour l'encryptage des données, il est possible d'utiliser les fonctions de Mppe (Microsoft Point to Point Encryption). Enfin, une compression de bout en bout peut être réalisée par Mppc (Microsoft Point to Point Compression). Ces divers protocoles permettent de réaliser une connexion VPN complète, mais les protocoles suivants permettent un niveau de performance et de fiabilité bien meilleur.

3.3 – Le protocole L2TP

L2TP, définit par la RFC 2661, est issu de la convergence des protocoles PPTP et L2F. Il est actuellement développé et évalué conjointement par **Cisco Systems**, **Microsoft, Ascend, 3Com** ainsi que d'autres acteurs clés du marché des réseaux. Il permet l'encapsulation des paquets PPP au niveau des couches 2 (Frame Relay et Atm) et 3 (Ip). Lorsqu'il est configuré pour transporter les données sur IP, L2TP peut être utilisé pour faire du tunnelling sur Internet. L2TP repose sur deux concepts : les concentrateurs d'accès L2TP (Lac : L2TP Access Concentrator) et les serveurs réseau L2TP (Lns : L2TP Network Server). L2TP n'intègre pas directement de protocole pour le chiffrement des données. C'est pourquoi L'IETF préconise l'utilisation conjointe d'IPSec et L2TP.



3.3.1 – Concentrateurs d'accès L2TP (Lac : L2TP Access Concentrator)

Les périphériques Lac fournissent un support physique aux connexions L2TP. Le trafic étant alors transféré sur les serveurs réseau L2TP. Ces serveurs peuvent s'intégrer à la structure d'un réseau commuté Rtc ou alors à un système d'extrémité PPP prenant en charge le protocole L2TP. Ils assurent le fractionnement en canaux de tous les protocoles basés sur PPP. Le Lac est l'émetteur des appels entrants et le destinataire des appels sortants.

3.3.2 – Serveur réseau L2TP (Lns : L2TP Network Server)

Les serveurs réseau L2TP ou Lns peuvent fonctionner sur toute plate-forme prenant en charge la terminaison PPP. Le Lns gère le protocole L2TP côté serveur. Le protocole L2TP n'utilise qu'un seul support, sur lequel arrivent les

canaux L2TP. C'est pourquoi, les serveurs réseau Lns, ne peuvent avoir qu'une seule interface de réseau local (Lan) ou étendu (Wan). Ils sont cependant capables de terminer les appels en provenance de n'importe quelle interface PPP du concentrateur d'accès Lac : async., Rnis, PPP sur Atm ou PPP sur relais de trame. Le Lns est l'émetteur des appels sortants et le destinataire des appels entrants. C'est le Lns qui sera responsable de l'authentification du tunnel.

3.4 – Le protocole IPSec

IPSec, définit par la **RFC 2401**, est un protocole qui vise à sécuriser l'échange de données au niveau de la couche réseau. Le réseau Ipv4 étant largement déployé et la migration vers Ipv6 étant inévitable, mais néanmoins longue, il est apparu intéressant de développer des techniques de protection des données communes à Ipv4 et Ipv6. Ces mécanismes sont couramment désignés par le terme IPSec pour Ip Security Protocols. IPSec est basé sur deux mécanismes. Le premier, AH, pour Authentification Header vise à assurer l'intégrité et l'authenticité des datagrammes IP. Il ne fournit par contre aucune confidentialité : les données fournies et transmises par Ce « protocole » ne sont pas encodées. Le second, Esp, pour Encapsulating Security Payload peut aussi permettre l'authentification des données mais est principalement utilisé pour le cryptage des informations. Bien qu'indépendants ces deux mécanismes sont presque toujours utilisés conjointement. Enfin, le protocole Ike permet de gérer les échanges ou les associations entre protocoles de sécurité. Avant de décrire ces différents protocoles, nous allons exposer les différents éléments utilisés dans IPSec.

3.4.1 – Vue d'ensemble

Les mécanismes mentionnés ci-dessus font bien sûr appel à la cryptographie et utilisent donc un certain nombre de paramètres (algorithmes de chiffrement utilisés, clefs, mécanismes sélectionnés…) sur lesquels les tiers communicants doivent se mettre d'accord. Afin de gérer ces paramètres, IPSec a recours à la notion d'association de sécurité (Security Association, SA).

Une association de sécurité IPSec est une « connexion » simplexe qui fournit des services de sécurité au trafic qu'elle transporte. On peut aussi la considérer comme une structure de données servant à stocker l'ensemble des paramètres associés à une communication donnée.

Une SA est unidirectionnelle ; en conséquence, protéger les deux sens d'une communication classique requiert deux associations, une dans chaque sens. Les services de sécurité sont fournis par l'utilisation soit de AH soit de Esp. Si AH et Esp sont tout deux appliqués au trafic en question, deux SA (voire plus) sont créées ; on parle alors de paquet (bundle) de SA.

Chaque association est identifiée de manière unique à l'aide d'un triplet composé de:

- L'adresse de destination des paquets,
- L'identifiant du protocole de sécurité utilisé (AH ou Esp),

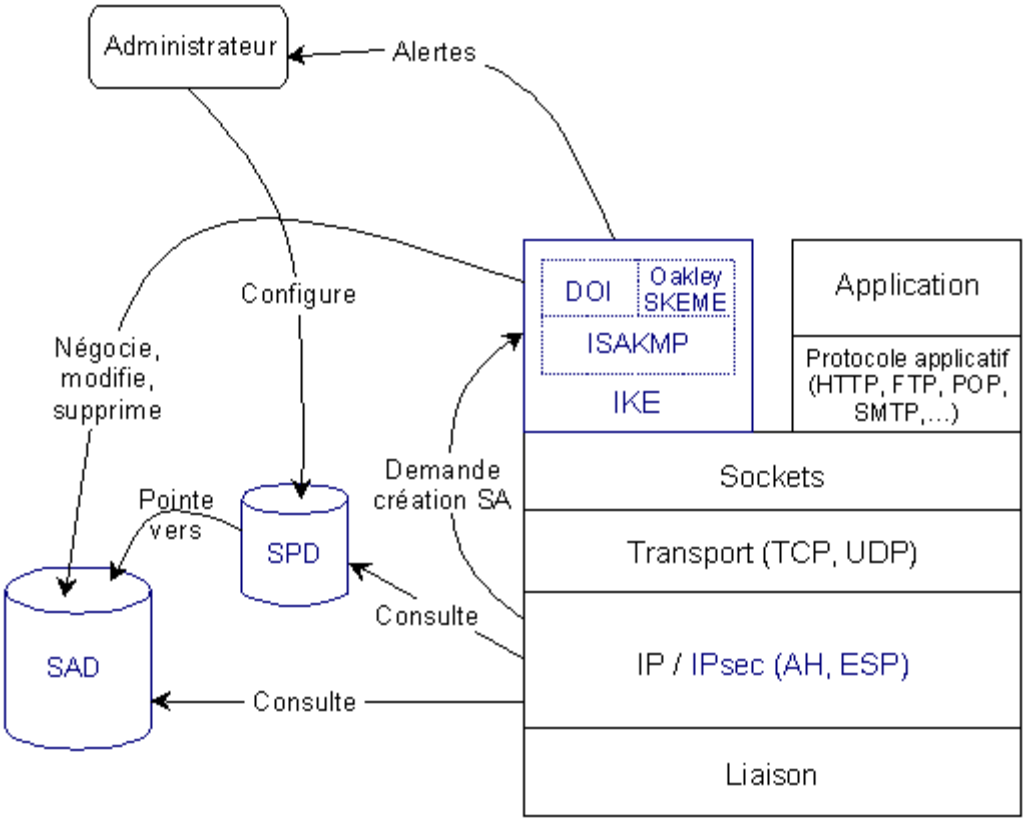
- Un index des paramètres de sécurité (Security Parameter Index, SPI). Un SPI est un bloc de 32 bits inscrit en clair dans l'entête de chaque paquet échangé ; il est choisi par le récepteur.

Pour gérer les associations de sécurités actives, on utilise une « base de données des associations de sécurité » (Security Association Database, SAD). Elle contient tous les paramètres relatifs à chaque SA et sera consultée pour savoir comment traiter chaque paquet reçu ou à émettre.

Les protections offertes par IPSec sont basées sur des choix définis dans une « base de données de politique de sécurité » (Security Policy Database, SPD). Cette base de données est établie et maintenue par un utilisateur, un administrateur système ou une application mise en place par ceux-ci. Elle permet de décider, pour chaque paquet, s'il se verra apporter des services de sécurité, s'il sera autorisé à passer ou rejeté.

3.4.2 – Principe de fonctionnement

Le schéma ci-dessous représente tous les éléments présentés ci-dessus leurs positions et leurs interactions.



On distingue deux situations :

- **Trafic sortant**
  Lorsque la « couche » IPSec reçoit des données à envoyer, elle commence par consulter la base de données des politiques de sécurité (SPD) pour savoir comment traiter ces données. Si cette base lui indique que le trafic doit se voir appliquer des mécanismes de sécurité, elle récupère les

caractéristiques requises pour la SA correspondante et va consulter la base des SA (SAD). Si la SA nécessaire existe déjà, elle est utilisée pour traiter le trafic en question. Dans le cas contraire, IPSec fait appel à IKE pour établir une nouvelle SA avec les caractéristiques requises.

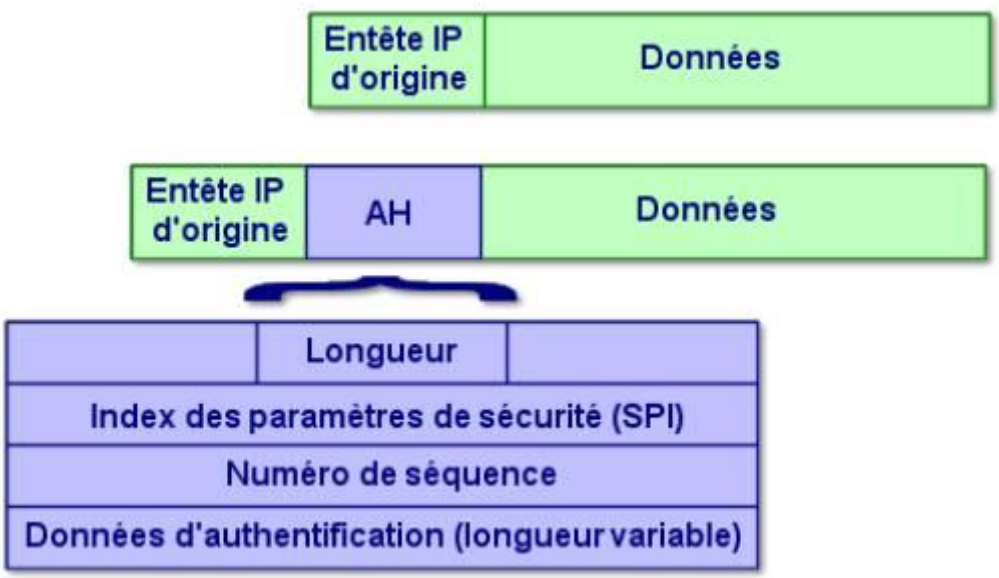
- **Trafic entrant**
  Lorsque la couche IPSec reçoit un paquet en provenance du réseau, elle examine l'entête pour savoir si Ce paquet s'est vu appliquer un ou plusieurs services IPSec et si oui, quelles sont les références de la SA. Elle consulte alors la SAD pour connaître les paramètres à utiliser pour la vérification et/ou le déchiffrement du paquet. Une fois le paquet vérifié et/ou déchiffré, la Spd est consultée pour savoir si l'association de sécurité appliquée au paquet correspondait bien à celle requise par les politiques de sécurité.

  Dans le cas où le paquet reçu est un paquet Ip classique, la Spd permet de savoir s'il a néanmoins le droit de passer. Par exemple, les paquets IKE sont une exception. Ils sont traités par Ike, qui peut envoyer des alertes administratives en cas de tentative de connexion infructueuse.

3.4.3 – Le protocole Ah (Authentication Header)

L'absence de confidentialité permet de s'assurer que Ce standard pourra être largement répandu sur Internet, y compris dans les endroits où l'exportation, l'importation ou l'utilisation du chiffrement dans des buts de confidentialité est restreint par la loi.

Son principe est d'adjoindre au datagramme Ip classique un champ supplémentaire permettant à la réception de vérifier l'authenticité des données incluses dans le datagramme. Ce bloc de données est appelé « valeur de vérification d'intégrité » (Intégrity Check Value, Icv). La protection contre le rejet se fait grâce à un numéro de séquence.

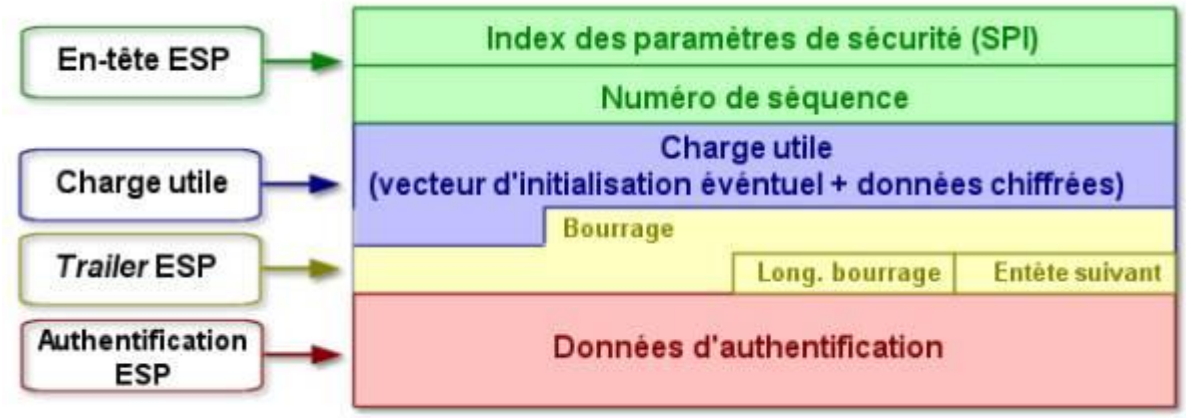


3.4.4 – Protocole Esp (Encapsulating Security Payload)

Esp peut assurer au choix, un ou plusieurs des services suivants :

- Confidentialité (confidentialité des données et protection partielle contre l'analyse du trafic si l'on utilise le mode tunnel).
- Intégrité des données en mode non connecté et authentification de l'origine des données, protection contre le rejeu.

La confidentialité peut être sélectionnée indépendamment des autres services, mais son utilisation sans intégrité/authentification (directement dans Esp ou avec AH) rend le trafic vulnérable à certains types d'attaques actives qui pourraient affaiblir le service de confidentialité



Le champ bourrage peut être nécessaire pour les algorithmes de chiffrement par blocs ou pour aligner le texte chiffré sur une limite de 4 octets.

Les données d'authentification ne sont présentes que si Ce service a été sélectionné.

Voyons maintenant comment est appliquée la confidentialité dans Esp.

L'expéditeur :

- Encapsule, dans le champ « charge utile » de Esp, les données transportées par le datagramme original et éventuellement l'entête IP (mode tunnel).
- Ajoute si nécessaire un bourrage.
- Chiffre le résultat (données, bourrage, champs longueur et entête suivant).
- Ajoute éventuellement des données de synchronisation cryptographiques (vecteur d'initialisation) au début du champ « charge utile ».

3.4.5 – La gestion des clefs pour IPSec : Isakmp et Ike

Les protocoles sécurisés présentés dans les paragraphes précédents ont recours à des algorithmes cryptographiques et ont donc besoin de clefs. Un des problèmes fondamentaux d'utilisation de la cryptographie est la gestion de ces clefs. Le terme

« gestion » recouvre la génération, la distribution, le stockage et la suppression des clefs.

IKE (Internet Key Exchange) est un système développé spécifiquement pour IPSec qui vise à fournir des mécanismes d'authentification et d'échange de clef adaptés à l'ensemble des situations qui peuvent se présenter sur l'Internet. Il est composé de plusieurs éléments : le cadre générique Isakmp et une partie des protocoles Oakley et Skeme. Lorsqu'il est utilisé pour IPSec, IKE est de plus complété par un « domaine d'interprétation » pour IPSec.

3.4.5.1 – Isakmp (Internet Security Association and Key Management Protocol)

sakmp a pour rôle la négociation, l'établissement, la modification et la suppression des associations de sécurité et de leurs attributs. Il pose les bases permettant de construire divers protocoles de gestion des clefs (et plus généralement des associations de sécurité). Il comporte trois aspects principaux :

- Il définit une façon de procéder, en deux étapes appelées phase 1 et phase 2 : dans la première, un certain nombre de paramètres de sécurité propres à Isakmp sont mis en place, afin d'établir entre les deux tiers un canal protégé ; dans un second temps, Ce canal est utilisé pour négocier les associations de sécurité pour les mécanismes de sécurité que l'on souhaite utiliser (AH et Esp par exemple).

- Il définit des formats de messages, par l'intermédiaire de blocs ayant chacun un rôle précis et permettant de former des messages clairs.
- Il présente un certain nombre d'échanges types, composés de tels messages, qui permettant des négociations présentant des propriétés différentes : protection ou non de l'identité, perfect forward secrecy…

Isakmp est décrit dans la RFC 2408

3.4.5.2 Ike (Internet Key Exchange)

IKE utilise **Isakmp** pour construire un protocole pratique. Il comprend quatre modes :

- Le mode principal (Main mode)
- Le mode agressif (Aggressive Mode)
- Le mode rapide (Quick Mode)
- Le mode nouveau groupe (New Groupe Mode)

Main Mode et Aggressive Mode sont utilisés durant la phase 1, Quick Mode est un échange de phase 2. New Group Mode est un peu à part : Ce n'est ni un échange de phase 1, ni un échange de phase 2, mais il ne peut avoir lieu qu'une

fois qu'une SA Isakmp est établie ; il sert à se mettre d'accord sur un nouveau groupe pour de futurs échanges Diffie-Hellman.

a) Phase 1 : Main Mode et Aggressive Mode

Les attributs suivants sont utilisés par Ike et négociés durant la phase 1 : un algorithme de chiffrement, une fonction de hachage, une méthode d'authentification et un groupe pour Diffie-Hellman.

Trois clefs sont générées à l'issue de la phase 1 : une pour le chiffrement, une pour l'authentification et une pour la dérivation d'autres clefs. Ces clefs dépendent des cookies, des aléas échangés et des valeurs publiques Diffie-Hellman ou du secret partagé préalable. Leur calcul fait intervenir la fonction de hachage choisie pour la SA Isakmp et dépend du mode d'authentification choisi. Les formules exactes sont décrites dans la RFC 2409.

b) Phase 2 : Quick Mode

Les messages échangés durant la phase 2 sont protégés en authenticité et en confidentialité grâce aux éléments négociés durant la phase 1. L'authenticité des messages est assurée par l'ajout d'un bloc Hash après l'entête Isakmp et la confidentialité est assurée par le chiffrement de l'ensemble des blocs du message.

Quick Mode est utilisé pour la négociation de SA pour des protocoles de sécurité donnés comme IPSec. Chaque négociation aboutit en fait à deux SA, une dans chaque sens de la communication.

Plus précisément, les échanges composant Ce mode ont le rôle suivant :

- Négocier un ensemble de paramètres IPSec (paquets de SA)
- Échanger des nombres aléatoires, utilisés pour générer une nouvelle clef qui dérive du secret généré en phase 1 avec le protocole Diffie-Hellman. De façon optionnelle, il est possible d'avoir recours à un nouvel échange Diffie-Hellman, afin d'accéder à la propriété de Perfect Forward Secrecy, qui n'est pas fournie si on se contente de générer une nouvelle clef à partir de l'ancienne et des aléas.
- Optionnellement, identifier le trafic que Ce paquet de SA protégera, au moyen de sélecteurs (blocs optionnels IDi et IDr ; en leur absence, les adresses Ip des interlocuteurs sont utilisées).

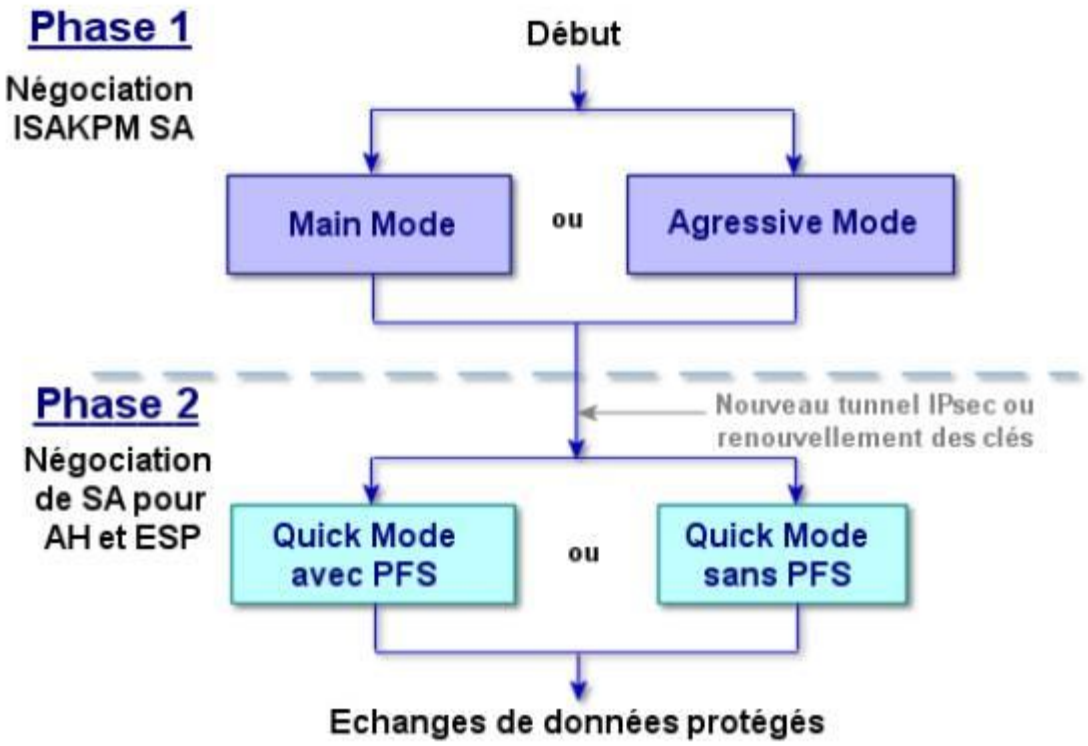
c) Les groupes : New Groupe Mode

Le groupe à utiliser pour Diffie-Hellman peut être négocié, par le biais du bloc SA, soit au cours du Main Mode, soit ultérieurement par le biais du New Group Mode. Dans les deux cas, il existe deux façons de désigner le groupe à utiliser :

- Donner la référence d'un groupe prédéfini : il en existe actuellement quatre, les quatre groupes Oakley (deux groupes MODP et deux groupes EC2N).
- Donner les caractéristiques du groupe souhaité : type de groupe (MODP, ECP, EC2N), nombre premier ou polynôme irréductible, générateurs…

d) Phases et modes

Au final, le déroulement d'une négociation IKE suit le diagramme suivant :

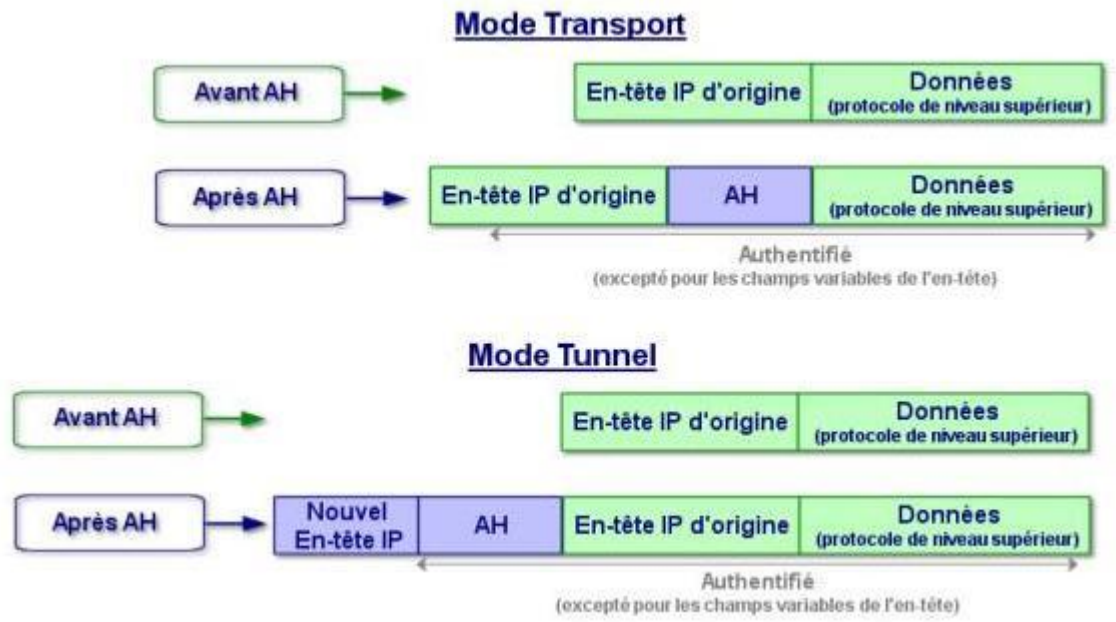


3.4.6 – Les deux modes de fonctionnement de IPSec

e mode transport prend un flux de niveau transport (couche de niveau 4 du modèle OSI) et réalise les mécanismes de signature et de chiffrement puis transmet les données à la couche Ip. Dans Ce mode, l'insertion de la couche IPSec est transparente entre Tcp et Ip. Tcp envoie ses données vers IPSec comme il les enverrait vers IPv4.

L'inconvénient de Ce mode réside dans le fait que l'entête extérieur est produit par la couche Ip c'est-à-dire sans masquage d'adresse. De plus, le fait de terminer les traitements par la couche Ip ne permet pas de garantir la non-utilisation des options Ip potentiellement dangereuses. L'intérêt de Ce mode réside dans une relative facilité de mise en oeuvre.

Dans le mode tunnel, les données envoyées par l'application traversent la pile de protocole jusqu'à la couche Ip incluse, puis sont envoyées vers le module IPSec. L'encapsulation IPSec en mode tunnel permet le masquage d'adresses. Le mode tunnel est utilisé entre deux passerelles de sécurité (routeur, firewall, …) alors que le mode transport se situe entre deux hôtes.



3.5 – Le protocole MPLS

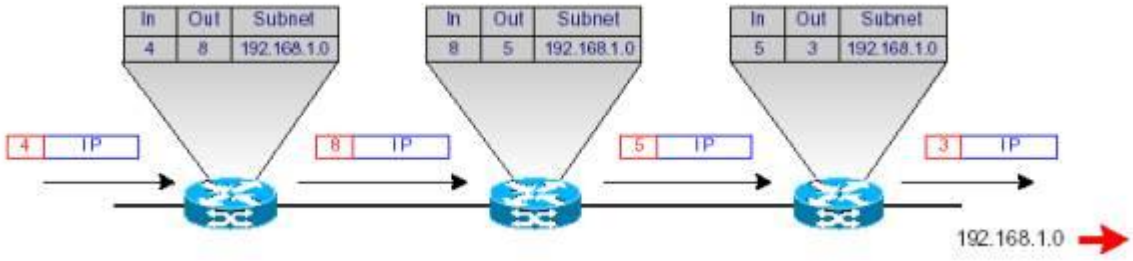
Le protocole MPLS est un brillant rejeton du « tout ip ». Il se présente comme une solution aux problèmes de routage des datagrammes Ip véhiculés sur Internet. Le principe de routage sur Internet repose sur des tables de routage. Pour chaque paquet les routeurs, afin de déterminer le prochain saut, doivent analyser l'adresse de destination du paquet contenu dans l'entête de niveau 3. Puis il consulte sa table de routage pour déterminer sur quelle interface doit sortir le paquet. Ce mécanisme de recherche dans la table de routage est consommateur de temps Cpu et avec la croissance de la taille des réseaux ces dernières années, les tables de routage des routeurs ont constamment augmenté. Le protocole MPLS fut initialement développé pour donner une plus grande puissance aux commutateurs Ip, mais avec l'avènement de techniques de commutation comme Cef (Cisco Express Forwarding) et la mise au point de nouveaux Asic (Application Specific Interface Circuits), les routeurs Ip ont vu leurs performances augmenter sans le recours à MPLS.

3.5.1 – Principe de fonctionnement de MPLS

Le principe de base de MPLS est la commutation de labels. Ces labels, simples nombres entiers, sont insérés entre les entêtes de niveaux 2 et 3, les routeurs permutant alors ces labels tout au long du réseau jusqu'à destination, sans avoir besoin de consulter l'entête Ip et leur table de routage.

3.5.1.1 – Commutation par labels

Cette technique de commutation par labels est appelée Label Swapping. MPLS permet de définir des piles de labels (label stack), dont l'intérêt apparaîtra avec les VPN. Les routeurs réalisant les opérations de label swapping sont appelés Lsr pour Label Switch Routers.



Les routeurs MPLS situés à la périphérie du réseau (Edge Lsr), qui possèdent à la fois des interfaces Ip traditionnelles et des interfaces connectées au backbone MPLS, sont chargés d'imposer ou de retirer les labels des paquets Ip qui les traversent. Les routeurs d'entrée, qui imposent les labels, sont appelés Ingress Lsr, tandis que les routeurs de sortie, qui retirent les labels, sont appelés Egress Lsr.

3 .5.1.2 – Classification des paquets

A l'entrée du réseau MPLS, les paquets Ip sont classés dans des Fec (Forwarding Equivalent Classes). Des paquets appartenant à une même Fec suivront le même chemin et auront la même méthode de forwarding. Typiquement, les Fec sont des préfixes Ip appris par l'Igp tournant sur le backbone MPLS, mais peuvent aussi être définis par des informations de Qos (Quality Of Services). La classification des paquets s'effectue à l'entrée du backbone MPLS, par les Ingress Lsr. A l'intérieur du backbone MPLS, les paquets sont label-switchés, et aucune reclassification des paquets n'a lieu. Chaque Lsr affecte un label local, qui sera utilisé en entrée, pour chacune de ses Fec et le propage à ses voisins. Les Lsr voisins sont appris grâce à l'Igp. L'ensemble des Lsr utilisés pour une Fec, constituant un chemin à travers le réseau, est appelé Label Switch Path (Lsp). Il existe un Lsp pour chaque Fec et les Lsp sont unidirectionnels.

3.5.2 – Utilisation du MPLS pour les VPN

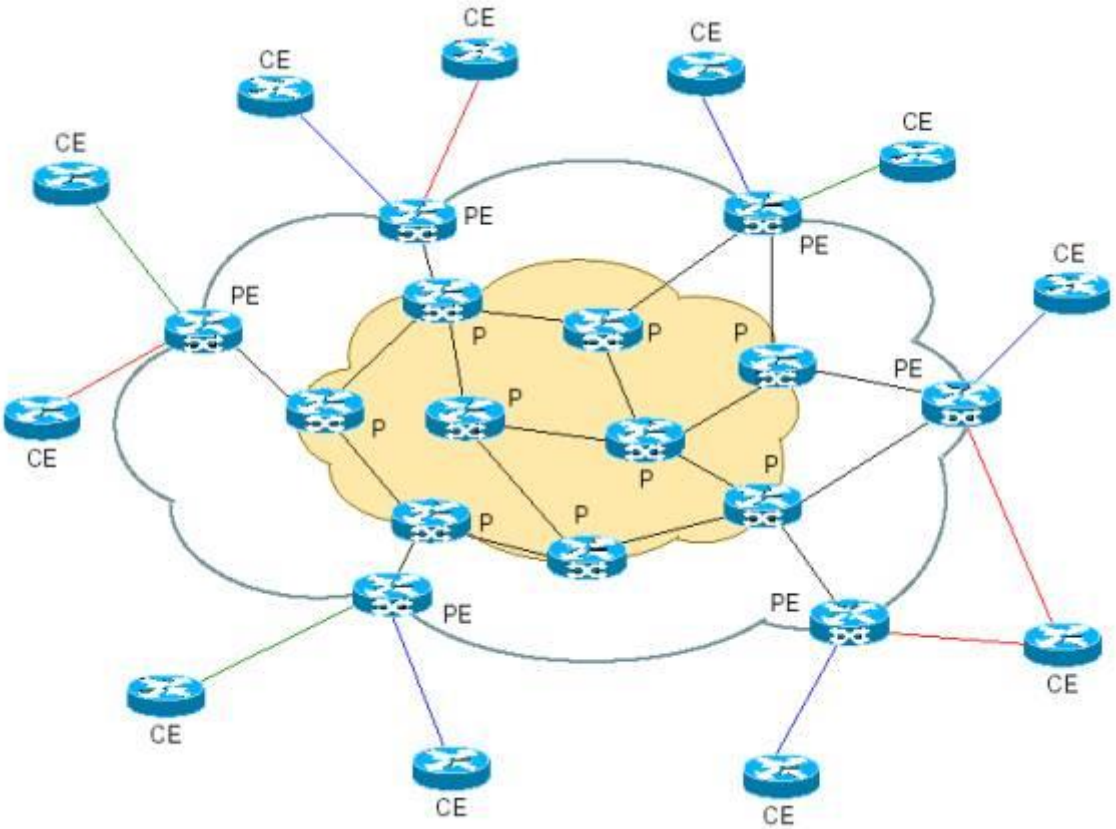
Pour satisfaire les besoins des opérateurs de services VPN, la gestion de VPN-IP à l'aide des protocoles MPLS a été définie dans une spécification référencée RFC 2547. Des tunnels sont créés entre des routeurs MPLS de périphérie appartenant à l'opérateur et dédiés à des groupes fermés d'usagers particuliers, qui constituent des VPN. Dans l'optique MPLS/VPN, un VPN est un ensemble de sites placés sous la même autorité administrative, ou groupés suivant un intérêt particulier.

3.5.2.1 – Routeurs P, Pe et Ce

ne terminologie particulière est employée pour désigner les routeurs (en fonction de leur rôle) dans un environnement MPLS / VPN :

- P (Provider) : ces routeurs, composant le coeur du backbone MPLS, n'ont aucune connaissance de la notion de VPN. Ils se contentent d'acheminer les données grâce à la commutation de labels ;
- Pe (Provider Edge) : ces routeurs sont situés à la frontière du backbone MPLS et ont par définition une ou plusieurs interfaces reliées à des routeurs clients ;
- Ce (Customer Edge) : ces routeurs appartiennent au client et n'ont aucune connaissance des VPN ou même de la notion de label. Tout routeur « traditionnel » peut être un routeur Ce, quel que soit son type ou la version d'OS utilisée.

Le schéma ci-dessous montre l'emplacement de ces routeurs dans une architecture MPLS :



3.5.2.2 – Routeurs Virtuels : VRF

La notion même de VPN implique l'isolation du trafic entre sites clients n'appartenant pas aux mêmes VPN. Pour réaliser cette séparation, les routeurs Pe ont la capacité de gérer plusieurs tables de routage grâce à la notion de Vrf (VPN Routing and Forwarding). Une Vrf est constituée d'une table de routage, d'une Fib (Forwarding Information Base) et d'une table Cef spécifiques, indépendantes des autres Vrf et de la table de routage globale. Chaque Vrf est désignée par un nom (par ex. RED, GREEN, etc.) sur les routeurs Pe. Les noms

sont affectés localement et n'ont aucune signification vis-à-vis des autres routeurs.

Chaque interface de Pe, reliée à un site client, est rattachée à une Vrf particulière. Lors de la réception de paquets Ip sur une interface client, le routeur Pe procède à un examen de la table de routage de la Vrf à laquelle est rattachée l'interface et donc ne consulte pas sa table de routage globale. Cette possibilité d'utiliser plusieurs tables de routage indépendantes permet de gérer un plan d'adressage par sites, même en cas de recouvrement d'adresses entre VPN différents.

3.5.3 – Sécurité

La séparation des flux entre clients sur des routeurs mutualisés supportant MPLS est assurée par le fait que seul la découverte du réseau se fait au niveau de la couche 3 et qu'ensuite le routage des paquets est effectué en s'appuyant uniquement sur le mécanisme des labels (intermédiaire entre la couche 2 et la couche 3).

Le niveau de sécurité est le même que celui de Frame Relay avec les Dlci au niveau 2.

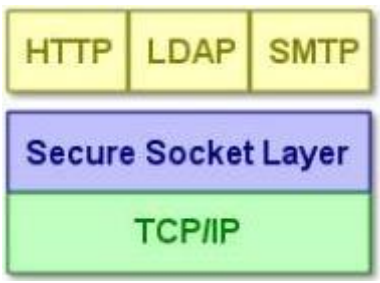
Le déni de service est en général effectué au niveau 3 (Ip). Ici, les paquets seront quand même routés jusqu'au destinataire au travers du réseau MPLS en s'appuyant sur les LSPs.

3.6 – Le protocole SSL

Récemment arrivé dans le monde des VPN, les **VPN à base de SSL** présente une alternative séduisante face aux technologies contraignantes que sont les VPN présentés jusque ici. Les VPN SSL présentent en effet le gros avantage de ne pas nécessiter du coté client plus qu'un navigateur Internet classique. En effet le protocole SSL utilisé pour la sécurisation des échanges commerciaux sur Internet est implémenté en standard dans les navigateurs modernes.

SSL est un protocole de couche 4 (niveau transport) utilisé par une application pour établir un canal de communication sécurisé avec une autre application.

SSL a deux grandes fonctionnalités : l'authentification du serveur et du client à l'établissement de la connexion et le chiffrement des données durant la connexion.



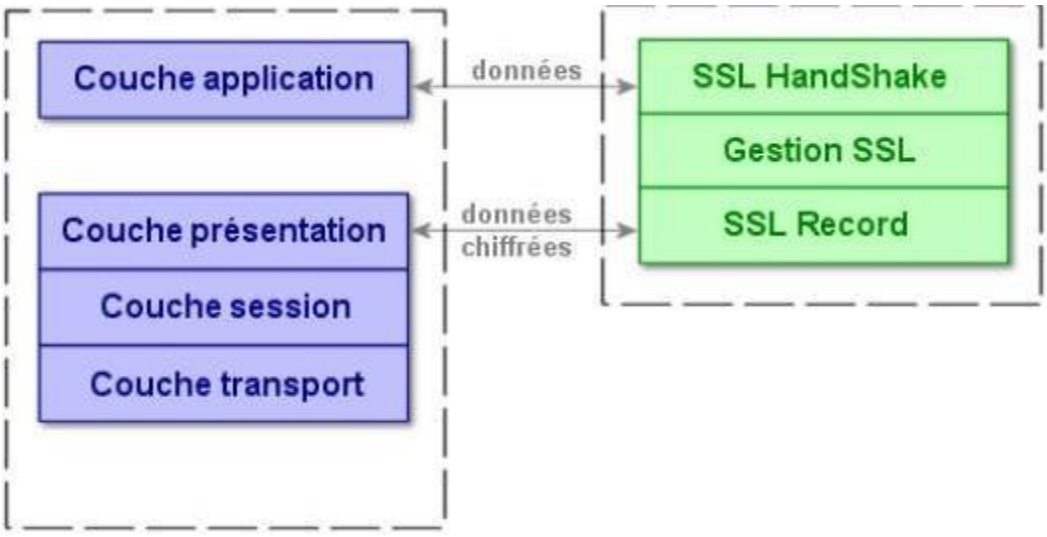
3.6.1 – Fonctionnement

Le protocole SSL Handshake débute une communication SSL. Suite à la requête du client, le serveur envoie son certificat ainsi que la liste des algorithmes qu'il souhaite utiliser. Le client commence par vérifier la validité du certificat du serveur. Cela se fait à l'aide de la clé publique de l'autorité de certification contenue dans le navigateur du client. Le client vérifie aussi la date de validité du certificat et peut également consulter une CRL (Certificate Revocation List). Si toutes les vérifications sont passées, le client génère une clé symétrique et l'envoie au serveur. Le serveur peut alors envoyer un test au client, que le client doit signer avec sa clé privée correspondant à son propre certificat. Ceci est fait de façon à Ce que le serveur puisse authentifier le client.

De nombreux paramètres sont échangés durant cette phase : type de clé, valeur de la clé, algorithme de chiffrage …

La phase suivante consiste en l'échange de données cryptées (protocole SSL Records). Les clés générées avec le protocole Handshake sont utilisées pour garantir l'intégrité et la confidentialité des données échangées. Les différentes phases du protocole sont :

- Segmentation des paquets en paquets de taille fixe
- Compression (mais peu implémenté dans la réalité)
- Ajout du résultat de la fonction de hachage composé de la clé de cryptage, du numéro de message, de la longueur du message, de données …
- Chiffrement des paquets et du résultat du hachage à l'aide de la clé symétrique générée lors du Handshake.
- Ajout d'un entête SSL au paquet



4 – Comparaison des différents protocoles

Chaque protocole présenté permet de réaliser des solutions performantes de VPN. Nous allons ici aborder les points forts et les points faibles de chacun de ses protocoles.

4.1 – VPN-SSL, une nouveauté marketing ?

Présentée comme la solution miracle pour permettre aux itinérants de se connecter aux applications réparties de l'entreprise les VPN-SSL souffrent de problèmes principalement liés aux navigateurs web utilisés.

Le but d'utiliser des navigateurs web est de permettre aux utilisateurs d'utiliser un outil dont ils ont l'habitude et qui ne nécessite pas de configuration supplémentaire. Cependant lorsqu'un certificat expire l'utilisateur doit aller manuellement le renouveler. Cette opération peut poser problème aux utilisateurs novices. De plus sur la majorité des navigateurs web la consultation des listes de certificats révoqués n'est pas activée par défaut : toute la sécurité de SSL reposant sur ces certificats ceci pose un grave problème de sécurité.

Rien n'empêche de plus le client de télécharger une version modifiée de son navigateur pour pouvoir utiliser de nouvelles fonctionnalités (skins, plugins…). Rien ne certifie que le navigateur n'a pas été modifié et que son autorité de certification en soit bien une.

Enfin Un autre problème lié à l'utilisation de navigateurs web comme base au VPN est leur spécificité au monde web. En effet par défaut un navigateur n'interceptera que des communication Https ou éventuellement Ftps. Toutes les communications venant d'autre type d'applications (MS Outlook, ou une base de données par exemple) ne sont pas supportées. Ce problème est généralement contourné par l'exécution d'une applet Java dédiée dans le navigateur. Mais ceci implique également la maintenance de cette applet (s'assurer que le client possède la bonne version, qu'il peut la re-télécharger au besoin)

L'idée suivant laquelle le navigateur web est une plate-forme idéale pour réaliser des accès VPN est donc sérieusement à nuancer.

4.2 – PPTP

PPTP présente l'avantage d'être complètement intégré dans les environnements Windows. Ceci signifie en particulier que l'accès au réseau local distant pourra se faire via le système d'authentification de Windows NT : RADIUS et sa gestion de droits et de groupe. Cependant comme beaucoup de produit Microsoft la sécurité est le point faible du produit :

- Mauvaise gestion des mots de passe dans les environnements mixtes win 95/NT

- Faiblesses dans la génération des clés de session : réalisé à partir d'un hachage du mot de passe au lieu d'être entièrement générées au hasard. (facilite les attaques « force brute »)
- Faiblesses cryptographiques du protocole MsCHAP 1 corrigées dans la version 2 mais aucun contrôle sur cette version n'a été effectué par une entité indépendante.
- Identification des paquets non implémentée : vulnérabilité aux attaques de type « spoofing »

4.3 – L2TP / IPSec

Les mécanismes de sécurité mis en place dans IPSec sont plus robustes et plus reconnus que ceux mis en place par Microsoft dans PPTP. Par défaut le protocole L2TP utilise le protocole IPSec. Cependant si le serveur distant ne le supporte pas L2TP pourra utiliser un autre protocole de sécurité. Il convient donc de s'assurer que l'ensemble des équipements d'un VPN L2TP implémente bien le protocole IPSec.

IPSec ne permet d'identifier que des machines et non pas des utilisateurs. Ceci est particulièrement problématique pour les utilisateurs itinérants. Il faut donc prévoir un service d'authentification des utilisateurs. Dans le cas de connexion dial-up c'est l'identifiant de connexion qui sera utilisé pour authentifier l'utilisateur. Mais dans le cas de connexion via Internet il faudra prévoir une phase d'authentification supplémentaire à l'établissement du tunnel.

D'autre part IPSec n'offre aucun mécanisme de Qos Ce qui limite ses applications : toutes les applications de voix sur Ip ou de vidéo sur Ip sont impossibles ou seront amenées à être complètement dépendantes des conditions de traffic sur l'internet public.

Enfin IPSec à cause de la lourdeur des opérations de cryptage/décryptage réduit les performances globales des réseaux. L'achat de périphériques dédiés, coûteux est souvent indispensable.

4.4 – MPLS

MPLS est aujourd'hui la solution apparaissant comme la plus mature du marché. La possibilité d'obtenir une Qos garantie par contrat est un élément qui pèse fortement dans la balance des décideurs. Cependant, seuls des opérateurs spécialisés fournissent Ce service Ce qui peut poser de nouveaux problèmes. Tout d'abord, Ce sont ces opérateurs de services qui fixent les prix. Ce prix inclus forcement une marge pour le fournisseur de service. D'autre part certaines entreprise ne souhaitent pas sous traiter leurs communications à un seul opérateur. En effet l'explosion de la bulle boursière autour des valeurs technologiques a suscité une vague de faillite d'opérateurs réseaux et de nombreuses entreprises ont vu leurs connexions coupées du jour au

lendemain. Ce risque est aujourd'hui fortement pris en compte par les décideurs informatiques. Cependant utiliser plusieurs opérateurs pour la gestion du VPN complique d'autant la gestion et la configuration de celui-ci.

Enfin l'étendu d'un VPN-MPLS est aujourd'hui limité par la capacité de l'opérateur de service à couvrir de vastes zones géographiques.

4.5 – MPLS / IPSec

- **Qualité de service**
  - MPLS : Permet d'attribuer des priorités au trafic par le biais de classes de service
  - IPSec : Le transfert se faisant sur l'Internet public, permet seulement un service « best effort »
- **Coût**
  - MPLS : Inférieur à celui des réseaux Frame Relay et Atm mais supérieur à celui des autres VPN IP.
  - IPSec : Faible grâce au transfert via le domaine Internet public
- **Sécurité**
  - MPLS : Comparable à la sécurité offerte par les réseaux Atm et Frame Relay existants.
  - IPSec : Sécurité totale grâce à la combinaison de certificats numériques et de Pki pour l'authentification ainsi qu'à une série d'options de cryptage, triple DES et AES notamment
- **Applications compatibles**
  - MPLS : Toutes les applications, y compris les logiciels d'entreprise vitaux exigeant une qualité de service élevée et une faible latence et les applications en temps réel (vidéo et voix sur IP)
  - IPSec : Accès à distance et nomade sécurisé. Applications sous IP, notamment courrier électronique et Internet. Inadapté au trafic en temps réel ou à priorité élevée
- **Etendue**
  - MPLS : Dépend du réseau MPLS du fournisseur de services
  - IPSec : Très vaste puisque repose sur l'accès à Internet
- **Evolutivité**
  - MPLS : Evolutivité élevée puisque n'exige pas une interconnexion d'égal à égal entre les sites et que les déploiements standard peuvent prendre en charge plusieurs dizaines de milliers de connexions par VPN

- IPSec : Les déploiements les plus vastes exigent une planification soigneuse pour répondre notamment aux problèmes d'interconnexion site à site et de peering

- **Frais de gestion du réseau**
  - MPLS : Aucun traitement exigé par le routage
  - IPSec : Traitements supplémentaires pour le cryptage et le décryptage
- **Vitesse de déploiement**
  - MPLS : Le fournisseur de services doit déployer un routeur MPLS en bordure de réseau pour permettre l'accès client
  - IPSec : Possibilité d'utiliser l'infrastructure du réseau Ip existant
- **Prise en charge par le client**
  - MPLS : Non requise. Le MPLS est une technologie réseau
  - IPSec : Logiciels ou matériels client requis

5 – Conclusion

Cette étude des solutions VPN, met en évidence une forte concurrence entres les différents protocoles pouvant être utilisés. Néanmoins, il est possible de distinguer deux rivaux sortant leurs épingles du jeu, à savoir IPSec et MPLS. Ce dernier est supérieur sur bien des points, mais il assure, en outre, simultanément, la séparation des flux et leur confidentialité. Le développement rapide du marché pourrait bien cependant donner l'avantage au second. En effet, la mise en place de VPN par Ip entre généralement dans une politique de réduction des coûts liés à l'infrastructure réseau des entreprises. Les VPN sur Ip permettent en effet de se passer des liaisons louées de type Atm ou Frame Relay. Le coût des VPN Ip est actuellement assez intéressant pour motiver de nombreuses entreprises à franchir le pas. A performance égales un VPN MPLS coûte deux fois moins cher qu'une ligne Atm. Mais si les solutions à base de MPLS prennent actuellement le devant face aux technologies IPSec c'est principalement grâce à l'intégration possible de solution de téléphonie sur IP. La qualité de service offerte par le MPLS autorise en effet Ce type d'utilisation. Le marché des VPN profite donc de l'engouement actuel pour ces technologies qui permettent elles aussi de réduire les coût des infrastructures de communication. Les VPN sont donc amenés à prendre de plus en plus de place dans les réseaux informatiques.

Annexe : Documents associ&s

Sur le site :

- Technologie : 2023 - VPN2023 : Classements de VPN commerciaux
- Technologie 2009- VPN pour les nuls , principes,mise en œuvre,outils open source

Bibliographie

- **Frameip.com** - https://www.frameip.com/vpn/?video=220#video-220

: