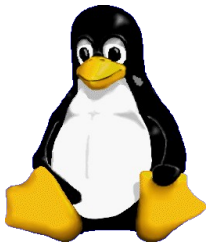


Sécurité GNU/Linux

Virtual Private Network

By ShareVB

Sommaire

I. Le concept de réseau privé virtuel

a) Introduction

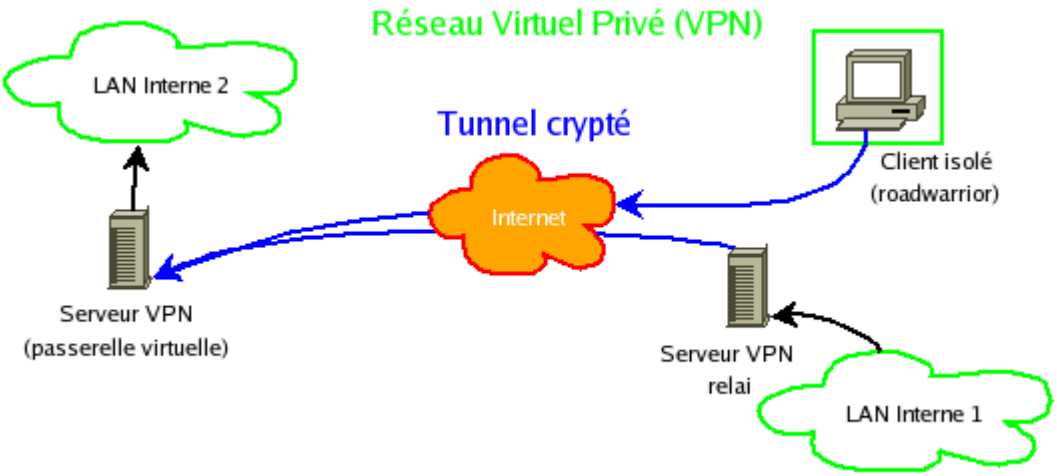
Les réseaux locaux type LAN permettent de faire communiquer les ordinateur d'un site d'une société ensemble. Ces réseaux sont relativement sûr car ils sont quasiment toujours derrière une série de pare-feu ou coupés d'Internet et que le chemin emprunté par les données ne quitte pas l'entreprise et est connu. Ils peuvent toutefois être soumis à des attaques dites du « man-in-the-middle » qui sera l'objet d'un autre document.

Sur Internet, on ne sait pas par où passent les données car les chemins changent. Ces données peuvent donc être écoutées ou interceptées. Il n'est donc pas envisageable de faire connecter deux LAN entre eux par Internet sans moyen de sécuriser le cheminement des données échangées.

Il existe alors deux solutions :

- relier les deux sites par une ligne spécialisée mais hors de prix
- créer un réseau privé virtuel sécurisé autrement dit un VPN. On encapsule (en anglais tunneling) les données dans un tunnel crypté

Voici comment peut se schématiser une Réseau Privé Virtuel ou VPN :



Mais alors pourquoi réseau virtuel privé. Virtuel simplement parce que le VPN relie deux réseaux physiques LAN par une liaison qui n'est pas réellement sûre et surtout pas dédiée à cet usage. Et privé parce que les données sont encryptées et que seuls les deux réseaux se voient mais ne sont pas vus de l'extérieur.

Pour résumé le VPN permet de mettre deux sites en relation de façon sécurisée à très faible coût par une simple connexion Internet. Mais cela se fait au détriment des performances car le passage par Internet est plus lent que sur une liaison dédiée.

b) Un peu plus sur le fonctionnement du VPN

Le VPN repose sur un protocole de tunnelisation qui est un protocole permettant de chiffrer les données par un algorithme cryptographique entre les deux réseaux.

Il existe deux types de VPN :

- le VPN d'accès permet à un utilisateur isolé de se connecter dans un réseau local interne (par exemple, de son entreprise). Dans ce cas, il peut avoir son propre client VPN afin de se connecter directement au réseau. Sinon, il doit demander à son FAI de lui fournir un serveur d'accès qui se chargera de la connexion cryptée. Seul problème, la connexion entre l'utilisateur isolé et le serveur d'accès n'est pas crypté.
- l'intranet ou extranet VPN permet de relier deux réseaux LAN entre eux. Dans le cas de l'extranet, il peut s'agir par exemple, d'un réseau d'une société et de ses clients. Dans les deux cas, les deux réseaux doivent se voir comme ci le réseau était en un seul morceau. Par exemple, on peut faire en sorte d'avoir une passerelle dans chaque réseau qui se connecterait ensemble par Internet de façon cryptée et achemineraient donc les données entre les deux réseaux.

c) Les fonctionnalités du VPN en résumé

Le VPN n'est qu'un concept, ce n'est pas une implémentation. Il se caractérise par les obligations

suivantes :

- authentification des entités communicantes : le serveur VPN doit pouvoir être sûr de parler au vrai client VPN et vice-versa
- authentification des utilisateurs : seuls les bonnes personnes doivent pouvoir se connecter au réseau virtuel. On doit aussi pouvoir conserver les logs de connexions
- gestion des adresses : tous les utilisateurs doivent avoir une adresse privée et les nouveau client en obtenir une facilement
- cryptage du tunnel : les données échangées sur Internet doivent être dûment cryptées entre le client VPN et le serveur VPN et vice-versa
- les clés de cryptage doivent être régénérées souvent (automatiquement)
- le VPN dit supporter tous les protocoles afin de réaliser un vrai tunnel comme s'il y avait réellement un câble entre les deux réseaux.

II. Les implémentations historiques de VPN

a) Catégories de protocoles

1) Classement par Niveau OSI

Il existe deux catégories de protocoles VPN :

- Les protocoles nécessitant parfois/souvent du matériel particulier :
  - Les protocoles de niveau 2 (Couche Liaison) dans la pile TCP/IP : PPTP, L2F et L2TP
  - Les protocoles de niveau 3 (Couche Réseau) dans la pile TCP/IP : IPSec
- Les protocoles ne nécessitant qu'une couche logicielle :
  - Les protocoles de niveau 4 (Couche Transport) : OpenVPN en SSL

2) Classement par Système d'exploitation

Voici les protocoles classés par OS :

- Disponibles nativement sous Windows
  - PPTP et IPSec/L2TP
- Protocoles disponibles sous Linux et Windows par logiciel annexe :
  - OpenVPN
- Disponibles sous Linux
  - Tous

b) Les principaux protocoles de VPN

Les principaux protocoles de tunneling VPN sont les suivants :

- PPTP (*Point-to-Point Tunneling Protocol*) est un protocole de niveau 2 développé par Microsoft, 3Com, Ascend, US Robotics et ECI Telematics.
- L2F (*Layer Two Forwarding*) est un protocole de niveau 2 développé par Cisco, Northern Telecom et Shiva. Il est désormais quasi-obsolète
- L2TP (*Layer Two Tunneling Protocol*) est l'aboutissement des travaux de l'*IETF* (RFC 2661) pour faire converger les fonctionnalités de *PPTP* et *L2F*. Il s'agit ainsi d'un protocole de niveau 2 s'appuyant sur PPP.
- **IPSec** est un protocole de niveau 3, issu des travaux de l'IETF, permettant de transporter des données chiffrées pour les réseaux IP.

1) Le protocole PPTP

Le principe du protocole PPTP (RFC2637) (*Point To Point Tunneling Protocol*) est de créer des trames avec le protocole PPP et de les crypter puis de les encapsuler dans un paquet IP.

Cela permet de relier les deux réseaux par une connexion point-à-point *virtuelle* acheminée par une connexion IP sur Internet. Cela fait croire aux deux réseaux qu'ils sont reliés par une ligne directe.

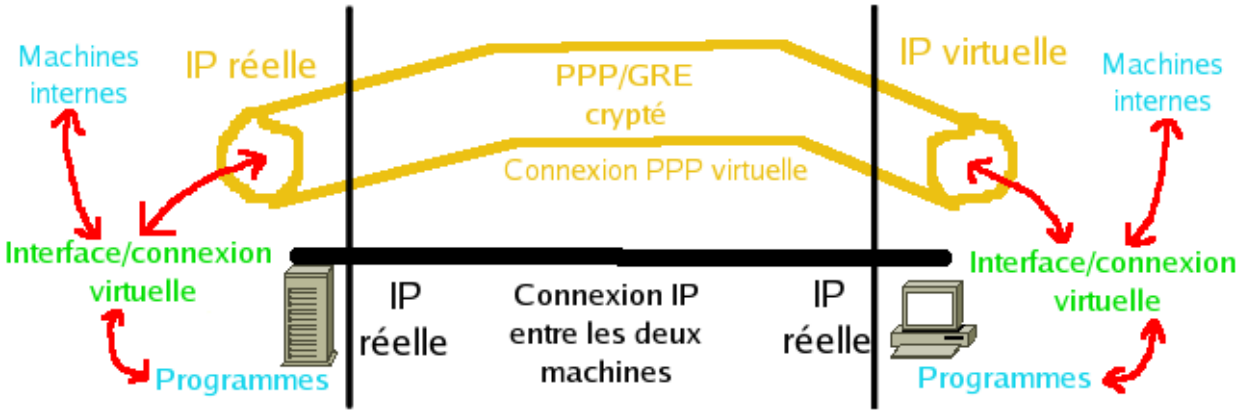
On garde, ainsi les adresses des réseaux physiques dans la trame PPP cryptées et cette trame est acheminée normalement sur Internet vers l'autre réseau.

Il permet les opérations suivantes :

- L'authentification se fait par le protocole MS-CHAP (Challenge Handshake Authentification Protocol) version 2 ou avec le protocole PAP (Password Authentification Protocol)
- L'encryption se fait par le procotole MPPE (Microsoft Point-to-Point Encryption). Cela crée un tunnel de niveau 3 (Réseau) géré par le protocole GRE (Generic Routing Encapsulation).
- La compression peut se faire avec le protocole MPPC (Microsoft Point to Point Compression)
- On peut ajouter autant de protocole que l'on veut dans le protocole PPTP pour l'encryption et la compression des données

La connexion se passe donc ainsi :

- Le client se connecte à Internet par son modem par le protocole PPP (classiquement)
- Le client se connecte alors au serveur VPN par une connexion IP encapsulant les paquets GRE/PPP cryptés. Ainsi cela forme deux connexions l'une sur l'autre
  - la connexion normale à Internet : elle achemine le traffic vers/depuis Internet
  - la connexion virtuelle au dessus de la connexion Internet : elle achemine le traffic vers/depuis le réseaux VPN
- A la fin de la connexion c'est le serveur qui ferme le tunnel



On obtient donc une connexion PPP au dessus de la connexion Internet ou Ethernet qui nous donne accès au serveur VPN pptpd. Cette connexion PPP obtient une IP de la plage définie dans la configuration de pptpd. Sur le serveur, on a une connexion de son IP publique vers l'IP virtuelle du client et sur le client c'est l'inverse.

Voici ce que cela donne avec un ping vers une **machine derrière** le serveur:

- ping

```
11:00:17.003113 IP IP_client > IP_serveur: GREv1, call 128, seq
120, length 101: compressed PPP data
```

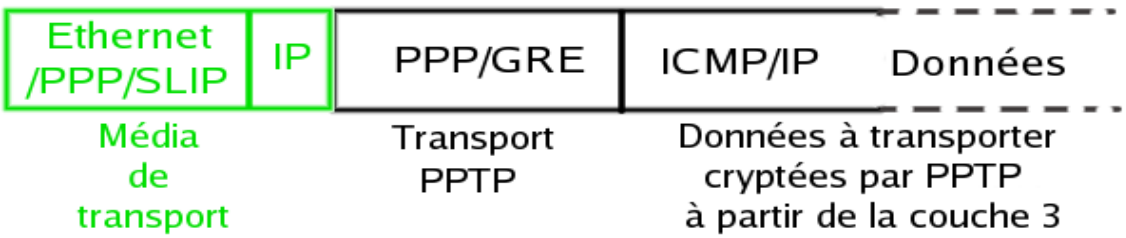
```
11:00:17.503088 IP IP_client > IP_serveur: GREv1, call 128, ack
116, no-payload, length 12
```

- pong

```
11:02:12.840243 IP IP_serveur > IP_client: GREv1, call 0, seq 135,
ack 139, length 105: compressed PPP data
```

On voit donc uniquement les paquets cryptés.

Un paquet d'une connexion PPTP ressemble donc à ceci :



Il est encore beaucoup utilisé du fait qu'il est nativement intégré aux systèmes Windows. Mais les protocoles tels que IPSec ou OpenVPN sont bien meilleurs en sécurité et en performances.

Pour plus d'information sur ce type de VPN, voir le tuto qui est consacré à PPTP.

2) Le protocole L2TP

C'est un protocole très proche des protocoles PPTP et L2F et est normalisé dans un RFC. Cette fois les trames PPP sont encapsulées dans le protocole L2TP lui-même et les trames PPP peuvent encapsuler des paquets IP, IPX, NetBIOS ou autre. Il se base aussi souvent sur IPSec.

Il y faut deux types de serveurs pour utiliser L2TP :

- LAC (L2TP Access Concentrator) : concentrateur d'accès L2TP. Il sert à fournir un moyen physique pour se connecter à un ou plusieurs LNS par le protocole L2TP. Il est responsable de l'identification et construit le tunnel vers les LNS. Il se trouve obligatoirement dans l'infrastructure du FAI de chaque utilisateur du VPN. Cela est donc très lourd (et cher) à mettre en place dans la mesure où il faut louer une place dans un serveur de connexion du FAI.
- LNS (L2TP Network Server) : serveur réseau L2TP, il assure la communication entre le réseau auquel il est connecté et les LAC vers lesquels il a un tunnel. Il se trouve généralement dans l'entreprise ou le service auquel appartient l'utilisateur distant.

Plus techniquement, voici l'encapsulation qu'engendre L2TP (de bas en haut, dans le cas d'un HTTP) :

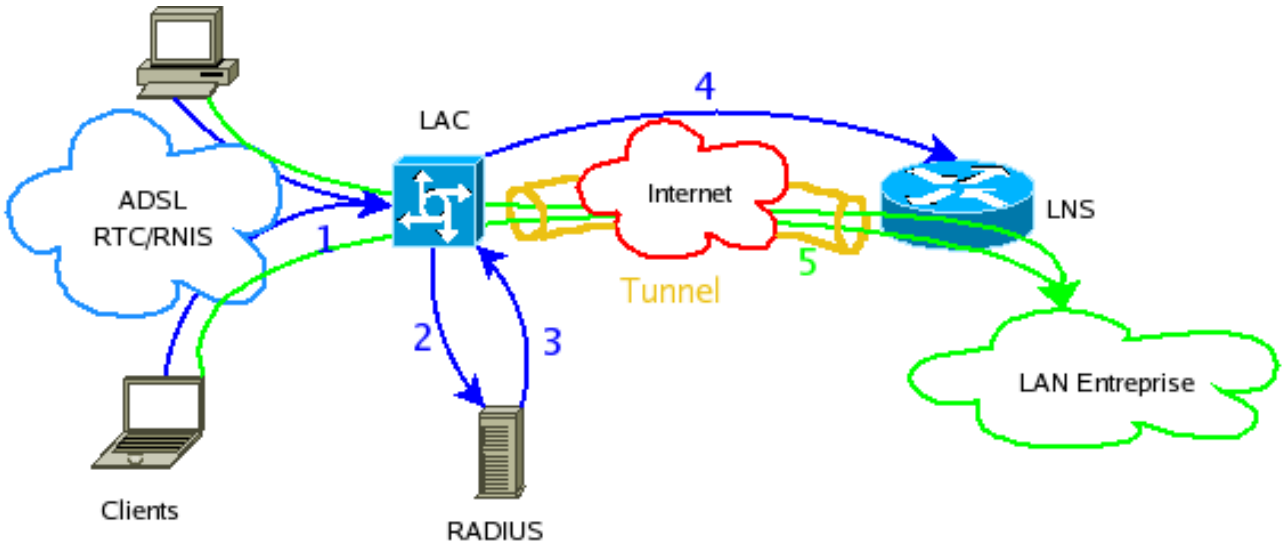
- couche 2 -> IP -> UDP -> L2TP -> PPP -> IP -> TCP -> HTTP

Il est donc relativement lourd, d'autant que les MTU (taille max des paquets) des lignes traversées peuvent générer de la fragmentation. Son seul avantage est de pouvoir terminer une session PPP n'importe quand ce qui permet à un utilisateur mobile de pouvoir se connecter facilement en VPN.

L2TP est encapsulé dans des paquets UDP entre le LAC et le LNS et utilise le port 1701.

La connexion d'un utilisateur se passe donc comme suit :

- 1) Un utilisateur se connecte à un LAC par le biais de sa connexion Internet ou d'un Modem bas débit. Ce LAC fait partie de l'infrastructure du FAI de l'utilisateur.
- 2) Il s'authentifie auprès de ce LAC. Ce dernier transmet les informations de login/mot de passe fournies au serveur RADIUS d'authentification. Ce dernier contient une liste associative login/nom_de_domaine/mot_passe <--> LNS.
- 3) Si le login/mot de passe est valide, cela permet au LAC de connaître le LNS auquel l'utilisateur peut se connecter pour être sur le VPN de son entreprise.
- 4) Si aucun tunnel n'existe entre le LAC et le LNS, un tunnel est créé à l'initiative du LAC
- 5) Une session PPP est créée à l'intérieur de ce tunnel
- L'utilisateur obtient donc une connexion PPP virtuelle entre lui et le réseau de son entreprise.



Pour Linux, il existe l'implémentation RP-L2TP (http://sourceforge.net/projects/rp-l2tp).

Pour plus d'information sur ce type de VPN, voir le tuto qui est consacré à L2TP.

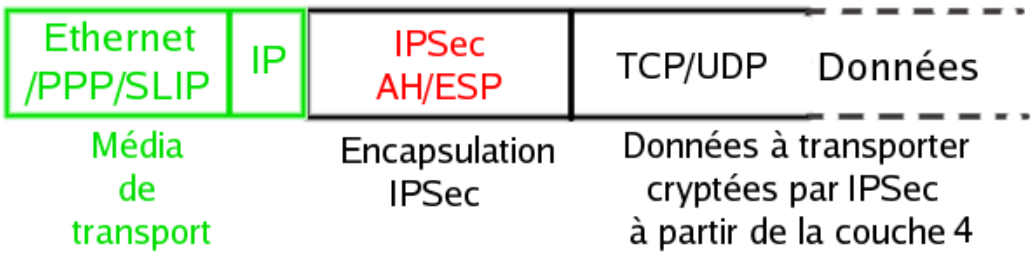
3) Le protocole IPSec

i. Mode de transport

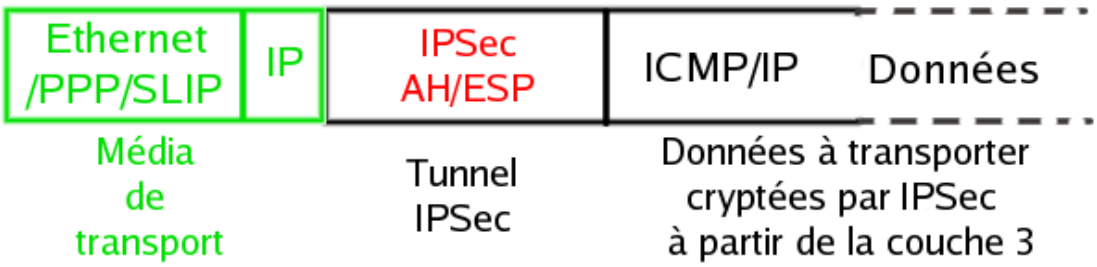
IPSec est un protocole défini par l'IETF permettant de sécuriser les échanges au niveau de la couche réseau. Il s'agit en fait d'un protocole apportant des améliorations au niveau de la sécurité au protocole IP afin de garantir la confidentialité, l'intégrité et l'authentification des échanges.

Il existe deux modes pour IPSec :

- le mode transport permet de protéger principalement les protocoles de niveaux supérieurs :
  - IPSec récupère les données venant de la couche 4 (TCP/transport), les signe et les crypte puis les envoie à la couche 3 (IP/réseau). Cela permet d'être transparent entre la couche TCP et la couche IP et du coup d'être relativement facile à mettre en place.
  - Il y a cependant plusieurs inconvénients :
    - l'entête IP est produite par la couche IP et donc IPSec ne peut pas la contrôler dans ce cas.
    - Il ne peut donc pas masquer les adresses pour faire croire à un réseau LAN virtuel entre les deux LAN reliés
    - cela ne garantie donc pas non plus de ne pas utiliser des options Ips non voulues



- le mode tunnel permet d'encapsuler des datagrammes IP dans des datagrammes IP
  - les paquets descendent dans la pile jusqu'à la couche IP et c'est la couche IP qui passe ses données à la couche IPSec. Il y a donc une entête IP encapsulée dans les données IPSec et une entête IP réelle pour le transport sur Internet (on pourrait imaginer que ce transport se fasse sur de l'IPX ou NetBIOS puisqu'il n'y a pas de contrainte dans ce mode)
  - Cela a beaucoup d'avantages :
    - l'entête IP réelle est produite par la couche IPSec. Cela permet d'encapsuler une entête IP avec des adresses relative au réseau virtuel et en plus de les crypter de façon à être sûr qu'elles ne sont pas modifiées.
    - On a donc des adresses IP virtuelles donc tirant partie au mieux du concept de VPN
    - On a le contrôle total sur l'entête IP produite par IPSec pour encapsuler ses données et son entête IPSec.



ii. Les composantes d'IPSec

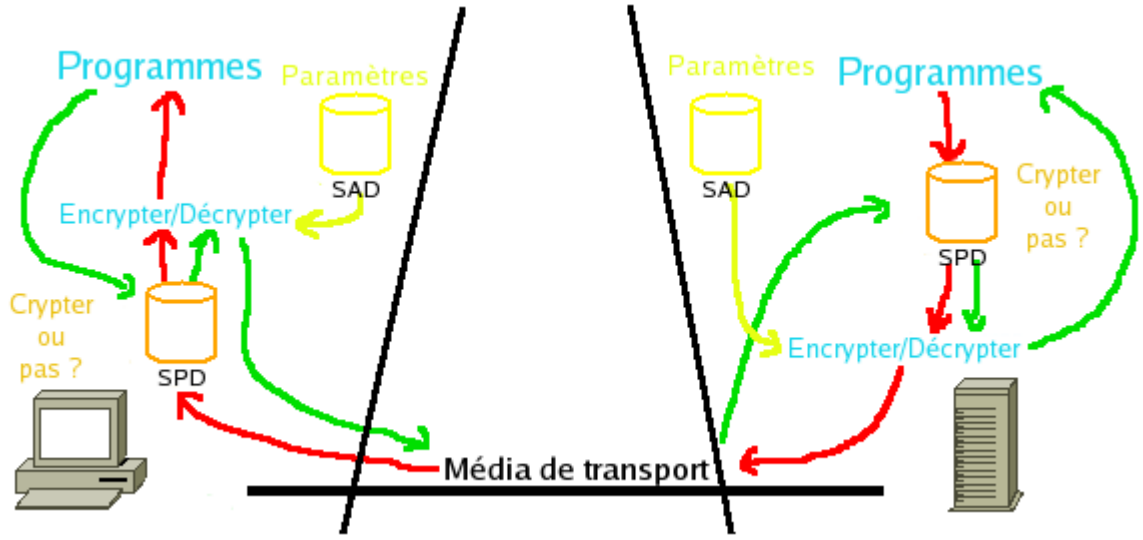
Le protocole IPSec est basé sur quatre modules :

- *IP Authentification Header* (**AH**) gère
  - l'intégrité : on s'assure que les champs invariants pendant la transmission, dans l'entête IP qui précède l'entête AH et les données
  - l'authentification pour s'assurer que l'émetteur est bien celui qu'il dit être
  - la protection contre le rejeu : un paquet intercepté par un pirate ne peut pas être renvoyé
  - il ne gère pas la confidentialité : les données sont signées mais pas cryptées
- *Encapsulating Security Payload* (**ESP**)
  - en mode transport, il assure
    - confidentialité : les données du datagramme IP encapsulé sont cryptées
    - authentification : on s'assure que les paquets viennent bien de l'hôte avec lequel on communique (qui doit connaître la clé associée à la communication ESP pour s'authentifier)
    - l'unicité optionnelle contre le rejeu des paquets
    - l'intégrité des données transmises
  - en mode tunnel, c'est l'ensemble du datagramme IP encapsulé dans ESP qui est crypté

et subit les vérifications suivantes. On peut donc se passer de AH.

- *Security Assocation* (**SA**) définit l'échange des clés et des paramètres de sécurité. Il existe une SA par sens de communication. Les paramètres de sécurité sont les suivants :
  - protocole AH et/ou ESP
  - mode tunnel ou transport
  - les algo de sécurité utiliser pour encrypter, vérifier l'intégrité
  - les clés utilisées
- La SAD (*Security Association Database*) stocke les SA afin de savoir comment traiter les paquets arrivant ou partant. Elles sont identifiées par des triplets :
  - adresse de destination des paquets
  - identifiant du protocole AH ou ESP utilisé
  - un index des paramètres de sécurité (Security Parameter Index) qui est un champ de 32bits envoyer en clair dans les paquets
- La SPD (Security Policy Database) est la base de configuration de IPSec. Elle permet de dire au noyau quels paquets il doit traiter. C'est à sa charge de savoir avec quel SA il fait le traitement.

En résumé, le SPD indique quels paquets il faut traiter et le SAD indique comment il faut traiter un paquet sélectionné.



iii. L'échange des clés

L'échanges des clés nécessaires au cryptage des données dans IPSec peut se faire de trois façons différentes :

- à la main : pas très pratique
- IKE (Internet Key Exchange) : c'est un protocole développé pour IPSec. ISAKMP (Internet Security Association and Key Management Protocol) en est la base et a pour rôle la création (négociation et mise en place), la modification et la suppression des SA. Elle se compose de deux phases :
  - la première permet de créer un canal sécurisé (par Diffie-Hellman) et authentifié à travers duquel on échange un secret pour dériver les clés utilisées dans la phase 2.

- la seconde permet de mettre en place IPSec avec ses paramètres et une SA par sens de communication. Les données échangées sont protégées par le canal mis en place dans la phase 1.

A l'issue de ces deux phases, le canal IPSec est mis en place.

Pour plus d'informations sur sa configuration, voir le tuto qui est consacré à IPSec.

4) Le protocole MPLS

C'est un protocole développé en partie par Cisco pour faciliter le routage IP par les commutateurs. Il est assez peu employé. Il repose sur la commutation de Label (ce qui n'a rien de particulier au VPN). Le principe est de mettre un entier (le label) entre les couches 2 (liaison) et 3 (réseau) qui évite au routeur de remonter plus haut qu'il n'en a besoin. Ainsi, il a une table pour lui dire « si je reçois un paquet avec le numéro n je le réémet sur ma sortie S avec le label m ». Ceci évite d'avoir besoin de lire l'entête IP et de consulter sa table de routage IP.

Voir aussi Tout sur **Mpls.**

c) L'implémentation OpenVPN

OpenVPN est une solution qui se base sur SSL. Cela permet d'assurer deux choses à la fois, sans avoir besoin de beaucoup de logiciel côté client :

- l'authentification du client et du serveur
- la sécurisation du canal de transmission

Il permet par exemple de résoudre les problèmes de NAT en offrant la même protection qu'IPSec mais sans les contraintes.

Pour plus d'information voir le tuto consacré à OpenVPN.

III. Bibliographie

VPN - Réseaux Privés Virtuels (RPV)

Les Réseaux Privés Virtuels - Vpn

OpenVPN - An Open Source SSL VPN Solution by James Yonan

Réseau privé virtuel - Wikipédia