Rapport d'exposé

Présentation sur les VPN

Étudiants :

Denis de REYNAL
Jehan-Guillaume de RORTHAIS
Sun Seng TAN

Informatique et Réseaux 3éme année – Février 2004

Table des matières

I - Introduction aux VPNs

Indéniablement, internet est rentré dans nos meurs. A travers, ce réseau informatique, tout un monde parallèle s'est développé : des sites marchands ont fleuris, les services pour les particuliers comme les guides d'itinéraire pour nos voyages nous simplifient bien la vie. Enfin on en vient a échanger des données à travers des programmes d'échange de fichiers et à « chater » entre internautes. Nous retiendrons de tout ça qu'Internet est un véritable outil de communication. A la fois high tech et démodé par sa technique, internet n'a pas su évoluer dans l'utilisation de ses protocoles, la plupart des protocoles utilisés ont plusieurs années d'existence et certains n'ont pas été crée dans une optique ou le réseau prendrait une tel envergure. Les mots de passe traversent ainsi les réseaux en clair, et là où transitent des applications de plus en plus critiques sur le réseau, la sécurité, elle, à peu évolué.

Quand on parle de sécurité, c'est en faisant référence aux pirates, virus, vers, cheval de Troie, etc ... Ils profitent de failles des protocoles, du système, mais surtout du faite que le réseau n'était pas développé dans une optique « sécurité ».

Internet dans ce contexte là n'a pas la vocation d'être une zone sécurisée. La plupart des données y circule à nue. On à alors recours à des algorithmes de cryptage, pour garder nos données confidentielles.

A - Les réseaux privés

Couramment utilisés dans les entreprises, les réseaux privés entreposent souvent des données confidentielles à l'intérieur de l'entreprise. De plus en plus, pour des raisons d'interopérabilité, on y utilise les mêmes protocoles que ceux utilisés dans l'Internet. On appelle alors ces réseaux privés « intranet ». Y sont stockés des serveurs propres à l'entreprise : portails, serveurs de partage de données, etc ... Pour garantir cette confidentialité, le réseau privé est coupé logiquement du réseau internet. En général, les machines se trouvant à l'extérieur du réseau privé ne peut accéder à celui-ci. L'inverse n'étant pas forcément vrai. L'utilisateur au sein d'un réseau privé pourra accéder au réseau internet.

B - Réseau privé virtuel

Le but d'un réseau privé virtuel (Virtual Private Network ou VPN) est de « fournir aux utilisateurs et

administrateurs du système d'information des conditions d'exploitation, d'utilisation et de sécurité à travers un réseau public identiques à celles disponibles sur un réseau privée ». En d'autre terme, on veut regrouper des réseaux privés, séparé par un réseau public (internet) en donnant l'illusion pour l'utilisateur qu'ils ne sont pas séparés, et toute en gardant l'aspect sécurisé qui était assuré par de la coupure logique au réseau internet.

C - Cas d'utilisation

On peut trouver plusieurs cas d'utilisation d'un VPN dont :

- Le Télétravail. Il existe des entreprises sans locaux, ou les employés travaillent chez eux. Quand ce type de travail est possible, pourquoi dépenser plus pour des locaux, des problèmes de transport, etc ... ? Le VPN apporte la possibilité pour tous ses employés de travailler sur un même réseau privé virtuel. Il doit alors évidement disposer d'une connexion internet qui lui permet de travailler à distance, et d'utiliser les différents services du réseau, et même exploiter des outils de travail collaboratif.
- Connexion de sites distants. Pour en entreprise possédant plusieurs sites, il est parfois avantageux de les relier. Une première solution serait d'utiliser une LS. Mais cette solution à un coup, et le VPN ne coûte pas plus que 2 connexion d'accès à internet.

Les nouvelles normes de communication telles que le Wifi ont vu le jour. Cette dernière par exemple, est de plus en plus utilisée, dans les bibliothèques, entreprises ou universités, les réseaux sont accessibles partout. Mais posent des problèmes évidentes de sécurités : le « mur » de sécurité physique que l'on avait à travers l'utilisation de câble n'existe plus. Il est alors simple d'intercepter les flux réseaux qui sont transportés dans les ondes radio. Le réseau privé ne conserve alors plus la confidentialité qu'elle avait. Certes un cryptage est spécifié dans la norme 802.11b, mais n'est pas assez robuste (WEP). C'est pour cette raison que pour des réseaux « sensibles », on à recours aux techniques utilisées par les VPN. Ainsi, il est possible, de manière sécurisée, d'utiliser le réseau sans fil.

D - Présentation des termes

Le VPN est ne représente donc qu'un concept, derrière lui, plusieurs implémentations ont vu le jour, selon l'utilisation que l'on veut en faire, le niveau de sécurité, la taille du réseau, etc ...

Plusieurs moyens techniques peuvent être utilisés et couplés pour mettre en oeuvre des VPN : le chiffrement, l'authentification, le contrôle d'intégrité et les tunnels.

- Chiffrement. Utilisé pour que les données traversant le réseau ne puisse pas être lu par une autre personne. On utilise pour cela notre baguage mathématique et surtout arithmétique. Les deux principaux type de cryptage utilisés sont : le chiffrement asymétrique et symétrique. Le chiffrage symétrique utilisé la même clé pour chiffrer et pour déchiffrer. L'inconvénient, est clair : chaque partie de la communication devra avoir la même clé, et la communiquer à la partie adverse sans que les autres puisses le récupérer. Plusieurs algorithmes de cryptage peuvent être utilisés : DES, AES, RC4/5. Le cryptage asymétrique n'a pas cette inconvénient la : deux clés sont utilisées : une clé publique et une clé privée. La clé public est disponible par tout le monde. Elle sert a crypter des données. Si on veut communiquer avec un autre, on doit récupérer sa clé publique et seul lui pourra la décrypter avec sa clé privé. Bien sur le cryptage et le décryptage se font de manière précise suivant la méthode utilisé. La plus connue est la méthode RSA, acronyme des chercheurs qui ont publiés cette méthode : Rivest, Shamir et Adleman.

  Le chiffrement est utilisé dans le contexte du VPN pour garantir la confidentialité des données circulant sur le réseau publique. En effet, le réseau privé n'est que virtuellement coupé du réseau publique.
- Authentification : On veut garantir qu'a chaque instant de la communication, on parle au bon interlocuteur. Dans le cadre du VPN, on parle des deux passerelles qui sont séparé par internet.
- Contrôle d'intégrité : il garantit que les données transmit entre les interlocuteur n'ont pas été modifié.
- Tunnel : le tunnel consiste à établir un canal entre 2 points sans ce soucier des problématique d'interconnexion (de façon transparente). Nous verrons plus en détail cet aspect important du VPN.

Finalement il n'y a pas qu'une seule façon de déployer un VPN : Dans la plupart des cas, le protocole IPSec est utilisé. Mais il n'est pas le seul. Les spécifications de votre VPN dépendra aussi de l'utilisation que vous allez en faire. C'est pourquoi nous allons dans les chapitres à venir, voir un aperçu des différents solutions existantes en parcourant quelques exemples de tunnel et VPN dit « légers », et enfin nous étudierons plus en détail le protocole IPSec et son déploiement dans un environnement GNU/Linux.

II - Les alternatives : Tunnels et VPN dit « légers »

A - Tunnels et VPN Légers

Le tunnel est une composante indispensable des VPN ; la problématique est la suivante : on veut relier deux réseaux privés qui sont séparés par un réseau publique (internet) de façon transparente pour l'utilisateur. L'utilisateur utilisera ainsi des interfaces réseaux virtuel et aura l'illusion de discuter directement avec le réseau qui se trouve, en fait, de l'autre coté d'Internet. La solution technique utilisée, dans la plupart des cas, pour mettre en oeuvre des tunnels est l'encapsulation de protocole. Technique déjà utilisée par nos fournisseur d'accès à internet, elle sera utilisé dans pas mal de VPN, mais à la différence de nos FAI, l'encapsulation masquera le réseau internet (au lieu du réseau privé du provider). Une autre technique utilisé, est le forwarding de port.

Le concept du tunnel ne sous entend rien concernant le chiffrement ; l'essentiel est de garantir la transparence de la communication entre les 2 réseaux qui ne sont pas directement interconnectés.

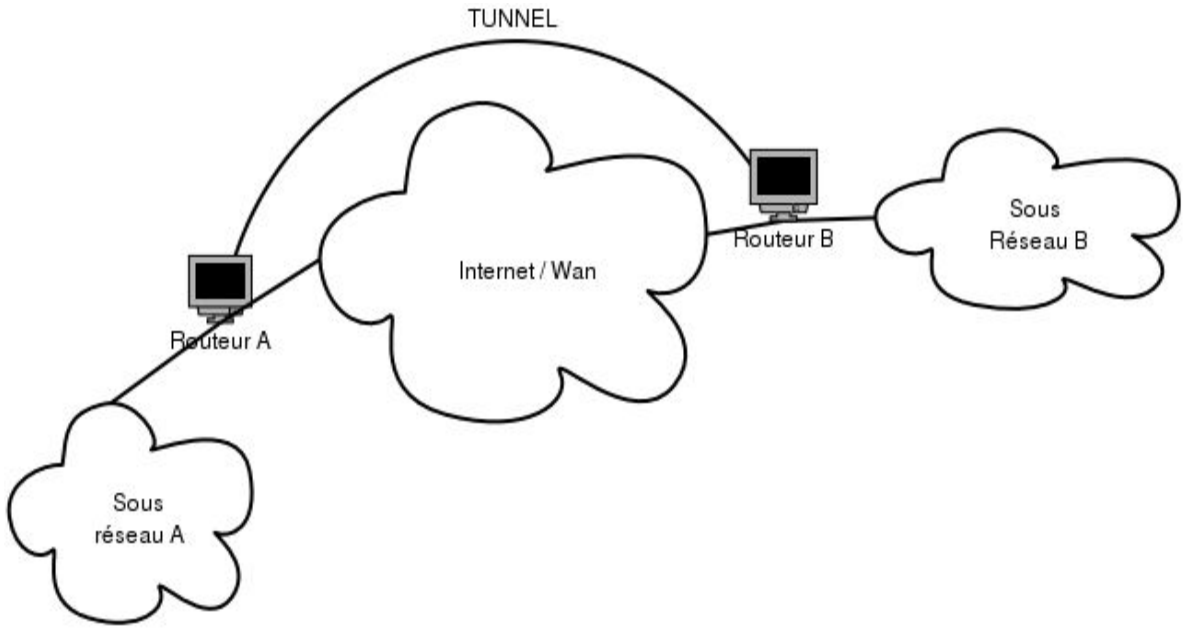


Illustration 1: Tunnel interconnectant le réseau sous réseau A au sous réseau B à travers le réseau Internet.

L'informatique pour les informaticiens ? Sûrement pas ! L'informatique doit être un moyen simple pour n'importe qui d'exploiter les machines. Parallèlement, les VPN que l'on crée doivent être à la mesure des

utilisateurs, personne ne veut passer des nuits à configurer sa passerelle pour mettre en place un simple VPN pour une petite infrastructure. De plus, le VPN n'est pas toujours utilisé pour transféré des données « critiques », une politique de sécurité dure est elle forcément exigée ?

On parle de VPN Légers, car certains moyens techniques n'offrent pas pas toutes les composantes du VPN : sécurité, transparences quand on ne dispose pas de moyens techniques, matériel ou financier de développer?

Finalement pour mettre en place ces alternatives (nous parlons bien d'alternatives à IPSec qui est le plus utilisé pour déployer des VPN) plusieurs solutions existent selon vos besoins.

B - Forwarding de port avec SSH et SSL

1 - Port forwarding

Le principe est est de faire transiter n'importe quel type de donnée IP à travers un canal sécurisé. Considérons 2 passerelles : elles seront configurer de manière à ce que les connections sur un port du premier sont redirigé sur un port d'une machine situé dans le réseau derrière la deuxième passerelle.

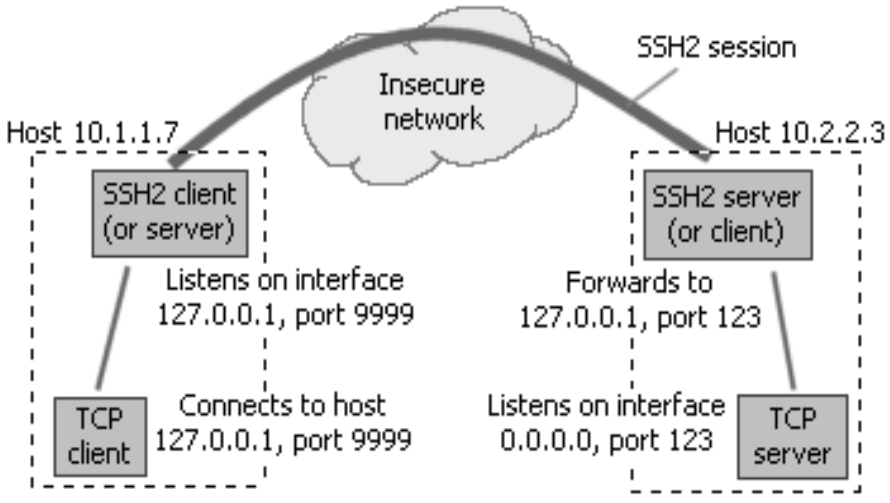


Illustration 2: Exemple de forwarding de port.

Sur ce schéma, le client SSH de l'hôte 10.1.1.7 "forward" les requête qu'il reçoit sur 127.0.0.1:9999 vers le serveur SSH de l'hôte 10.1.1.7 qui lui même forwardera les paquets reçus vers 127.0.0.1:123.

2 - Port forwarding et SSH

SSH est un outils permettant à travers des mécanisme d'authentification, de chiffrement et de compression d'accéder à un shell distant, de transférer des fichiers (scp) et de faire du fowarding de port.

C'est cette dernière fonctionnalité qui nous intéresse, pour cela nous disposons d'un client ssh sur une des passerelles et du serveur sur la deuxième passerelle.

Sur le serveur, on rajoutera la ligne « GatewayPorts yes » au fichier /etc/ssh/sshd_config et sur le client on établira le tunnel par la commande suivante :

```
# ssh -g -L <portSurLeClientSSSH>:<ipDuServeurDistant>:<portDaccèsAuServeurDistant> <ipDuServeurSSH>
```

Si on veut par exemple pourvoir accéder à un serveur web situé sur un serveur du réseau adverse :

```
# ssh -g -L 80:192.168.1.2:80 sunix.homelinux.net
```

192.168.1.2 étant l'adresse du serveur dans le réseau privé adverse, sunix.homelinux.net étant le la passerelle adverse ou se trouve le serveur ssh.

Ainsi, à partir d'un client web dans notre réseau, on rentrera l'adresse de notre passerelle pour accéder au serveur web.

3 - Port forwarding et SSL

Netscape en 1994, crée le protocole SSL afin de sécuriser les transmissions entre les navigateurs web. Nous pouvons exploiter ce protocole aujourd'hui pour faire du port forwarding, à travers un « wrapper » nommé stunnel : http://www.stunnel.org/. On peut ainsi effectuer le même genre de tunnel grâce à cette outil.

L'avantage de ces solutions est qu'elles présentent tous les composants d'un véritable VPN : authentification, chiffrement des données, tunnel. Néanmoins, elles ont été conçu pour faire transiter des paquets IP. Le deuxième type de solution pour réaliser nos tunnel s'appuie sur l'encapsulation de protocole; ces solutions peuvent être utilisé sur n'importe quel protocole (du moins en théorie).

C - Encapsulation de protocoles

Les protocoles réseaux permettent de transporter des données à travers les réseaux. Et pourquoi se données ne serait pas d'autre paquet réseau qui transporte eux même l'information ? Pourquoi faire ? On se trouve dans la problématique ou on veut créer des tunnels, et on veut donner l'illusion à l'utilisateur qu'il discute directement avec le réseau adverse alors qu'en fait il passe par internet. L'idée de l'encapsulation : l'utilisateur va envoyer des informations à travers une interface réseau virtuel, ces paquets seront encapsulés et transporter à travers un autre réseau puis décapsulé sur le réseau adverse derrière une autre interface virtuelle. Voici quelques exemple de solution utilisant l'encapsulation de protocole :

1 - Ip sur ip

Les tunnels IP sur IP encapsule les paquets IP sur des paquets IP. Ce type de tunnel peut servir à relier deux réseaux non connecté mais relier à internet. L'intérêt, comme dans plupart des tunnels, est de créer une interface réseau virtuel qui accédera virtuellement et directement au réseau adverse. Les paquets utilisés dans cette interface virtuel sera encapsulé.

Son Linux, le module ipip permet de mettre en oeuvre ce mécanisme, cette exemple de script de démarrage permet de mettre en oeuvre un tel réseau : http://www.xs4all.nl/~yskes/howto/linux_ipip_tunnel.htm

2 - IP sur GRE (Generic Routing Encapsulation)

GRE est un protocole développé par Cisco. Le protocole intègre la notion d'encapsulation de protocole. Il permet ainsi de supporter plusieurs types de protocoles pour les transporter sur de l'IP. Il est défini par la RFC 2784.

http://www.routage.org/gre.html

GRE à l'avantage de pouvoir interconnecter des réseaux ip ou non à travers un réseau ip comme internet, on peut notamment faire du tunneling de paquet ipv6 ou multicast sur de l'IP. Il est supporter par un grand nombre de d'appareils, de routeurs, et d'OS. Avec Linux, le module ip_gre permet permet de mettre en place ce genre de tunnel.

On peut mettre en place ce type de tunnel sous Linux à l'aide du module ip_gre et des outils iproute2 qui servent d'interface avec ip_gre.

D - Combiner les deux solutions

PPPD est un démon qui permet d'injecter du trafic au niveau 3 de la couche ISO et les faire transiter à travers un tunnel. On peut également spécifier au démon, les programmes sur lequel le tunnel va transiter. Grâce à cette fonctionnalité, il est alors possible d'utiliser ssh ou stunnel et bénéficier de leurs avantage (authentification, certificat, etc ...).

PPP over SSH, était l'une des première solution VPN mise en place : http://www.tldp.org/HOWTO/VPN-HOWTO/

Pour la mettre en oeuvre, on utilise le démon PPPD couplé avec SSH.

PPP over SSL fonctionne de la même façon, mais avec stunnel.

E - VPN sous Ms Windows.

Par défaut dans tous les Windows, est disponible la solution PPTP (Point to Point Tunneling Protocol) qui permet de déployer des VPN. PPTP encapsule du PPP sur du GRE. Il est généralement couplé avec MS-CHAP pour l'authentification.

Une analyse réalisé par Bruce Schneier et Mudge, démontre les failles de cette solution. La solution à été révisé depuis une autre étude à redémontré que des failles persistait. Pour en savoir plus : http://www.schneier.com

F - Autres solutions

Bien d'autres solutions existent, comme CIPS, ou TUN/TAP. Néanmoins nous n'en parlerons pas plus dans cette article.

Nous avons vu que les VPN peuvent être déployer par des moyens assez divers. Néanmoins les VPN majoritairement utilisé pour traversé le réseau internet qui repose sur IP. IPSec, propose des solutions robustes basées sur la version 4 et intégré dans la version 6 du protocole. Voyons IPSec de plus près.

III - IPSec : Présentation globale

A - Présentation

1 - Généralités

IPSec (Internet Protocol Security) a été conçu pour sécuriser les communications réseau à partir de la couche 3 du modèle OSI. Il a été conçus de manière à être supporté par Ipv4 et a été intégré dans le protocole Ipv6.

IPSec n'est pas un remplaçant d'IP mais un complément. Ainsi, il intègre des notions essentielle de sécurité au datagramme IP qui en assureront l'authenticité[1], l'authentification[2] et le cryptage[3]. Pour cela, il fait largement usage de clé de sessions **(voir 4.1.Types de clefs)**

Sa position dans les couche basse du modèle OSI lui permet donc de sécuriser tous type d'applications et protocoles réseaux basée sur IP sans distinction.

IPSec est très largement utilisé pour le déploiement de réseau VPN à travers Internet à petite et grande échelle.

2 - Aspects technique

IPSec est basé sur 2 mécanismes différents assurant les rôles de sécurisation des données : AH (Authentification header) et ESP (Encapsuling Security Payload).

IPSec est largement configurable. Ainsi, chacun des deux mécanismes AH et ESP peuvent être utilisés seuls ou combinés avec le second afin de définir le niveau de sécurité voulu. De plus, il est possible d'indiquer les algorithmes de hachage ou d'encrytion voulu lors d'une communication.

Les clés de session sont de type symétrique (définition manuelles des clés) ou asymétrique (génération automatique des clés). Voir : **4. La gestion des clefs**

1 L'authenticité des données permet d'assurer que les données reçues sont strictement identiques à celles émise.

2 L'authentification permet d'assurer que l'émetteur des données est bien celui qu'il prétend être.

3 Le cryptage permet d'assurer que les données transmise ne seront ni lue ni copier par une tierce personne durant leur acheminement.

L'authentification et l'authenticité des données sont assurée par un mécanisme de hachage des données traitée. si les deux partie de la communication trouve la même signature, c'est qu'ils utilisent bien les même clés de sessions qui ont permis de générer cette même signature des deux coté.

Notons que tous ces choix influencerons sur les performances des transferts.

B - Détails du protocole

Le mécanisme interne d'IPSec est complexe. Le fait que ce protocole soit hautement configurable introduit des notions de gestion et configuration inconnues du monde IP.

1 - Gestion des flux IPSec

Les flux IPSec sont géré unidirectionnellement. Ainsi, une communication bidirectionnelle entre deux machine utilisant IPSec sera définie par diverse processus pour chacun des sens de communication. Les procédés détaillé ci-dessous respectent tout deux cette lois.

a) Security Policy

Une SP défini ce qui doit être traité sur un flux. Comment nous voulons transformer un paquet.

Il y sera indiqué pour un flux donné :

- Les adresses IP de l'émetteur et du récepteur (unicast, mulitcast ou broadcast);
- Par quel protocole il devra être traité (AH ou ESP) ;
- Le mode IPSec à utiliser (tunnel ou transport) ;.
- Le sens de la liaison (entrante ou sortante) ;

Notons qu'une SP ne défini qu'un protocole de traitement à la fois. Pour utiliser AH **ET** ESP sur une communication, deux SP devront être créée.

b) Security Association

Une SA défini comment sera traité le paquet en fonction de sa SP associée. Elle ne sont que la "réalisation" des SP. Elle possède l'ensemble des propriétés de la liaison. Ainsi, elle sera représentée par une structure de donnée contenant les informations suivantes :

- Un compteur permettant de générer les numéros de séquence des entêtes AH et ESP ;
- Un flag (drapeau) permettant d'avertir qu'en cas de dépassement du compteur précédemment décrit, on doit interrompre la communication ;
- Une fenêtre d'anti répétition dans laquelle doit tomber le prochain numéros de séquence ;
- Information sur l'AH : algorithme d'authentification, clefs, durée de bie, etc ;
- Information sur l'ESP : algorithme d'authentification et de chiffrement, clefs, etc ;
- Mode IPSec : tunnel ou transport ;
- Durée de vie de la SA ;
- MTU.

Nous détaillerons les modes d'IPSec dans le prochain chapitre.

Une SA est identifiée à un seul et unique flux unidirectionnel grâce à trois champs :

- L'adresse IP de destination (unicast, multicast ou broadcast);
- Le protocole utilisé, AH ou ESP ;
- Le SPI (Security Parameter Index).

Comme nous pouvons le voir, une SA ne sera associée qu'a un seul des protocole AH ou ESP. si nous voulons protéger un flux avec ces deux protocoles, deux SA devront être créé.

LE SPI est un indice (ou ID) sur 32 bits attribué au SA lors de sa création. Nous verrons plus loin que sa génération dépendra du mode de gestion des clés de sessions. Il sert à distinguer les différentes SA qui aboutissent à une même destination et utilisant le même protocole.

c) Bases de données SPD et SAD

Tout système implémentant IPSec possède donc 2 bases de donnée distinctes dans laquelle ils stockent leurs SP (ici, SPDatabase) et leurs SA (ici, SADatabase).

La SPD défini donc le traitement de chaque type de trafic entrant ou sortant, en fonction des émetteurs / récepteurs, selon trois type :

- **DISCARD**, dans ce cas celui-ci sera tout simplement jeté. Il n'est pas autorisé à sortir de la passerelle ni à la traverser ni à être délivré à une quelconque application.
- **BYPASS IPSEC** laisse passer le trafic sans traitement IPSec.
- **APPLY IPSEC** signifie que des services IPSec sont à appliquer à ce trafic.

Pour chaque trafic soumis à des services IPSec, la base SPD possède une référence vers la SA correspondante dans la base SAD. Si cette entrés n'est pas définie, dans le cas d'une gestion dynamique des clés, celle-ci sera alors créée en accord avec la configuration définie par l'administrateur.

2 - Modes d' IPSec

Il existe deux modes d'utilisation d'IPSec : le mode transport et le mode tunnel. La génération des datagrammes sera différente selon le mode utilisé.

a) Mode Transport

Ce mode est utilisé pour créer une communication entre deux hôtes qui supportent IPSec. Une SA est établie entre les deux hôtes. Les entêtes IP ne sont pas modifiées et les protocoles AH et ESP sont intégrés entre cette entête et l'entête du protocole transporté.

Ce mode est souvent utiliser pour sécuriser une connexion Point-To-Point.

b) Mode Tunnel

Ce mode est utiliser pour encapsuler les datagrammes IP dans IPSec. La SA est appliquée sur un tunnel IP. Ainsi, les entêtes IP originales ne sont pas modifiée et un entête propre à IPSec est créée. Ce mode est souvent utilisé pour créer des tunnels entre réseaux LAN distant. Effectivement, il permet de relier deux passerelle étant capable d'utiliser IPSec sans perturber le trafic IP des machines du réseau qui ne sont donc pas forcément prête à utiliser le protocole IPSec.

3 - Détails des protocoles ajoutés

Nous verrons que certains champs sont présent dans les deux protocoles AH et ESP. En cas d'utilisation des deux protocoles pour un même flux de donnée, il n'y aura cependant pas redondance d'information. Effectivement, il faut garder à l'esprit que AH et ESP seront géré séparément par des SA différents.

AH et ESP sont deux protocoles utilisant des clés des sessions utiles à leurs traitement sur le datagramme IP.

a) En-tête AH

AH permet une sécurisation du maximum de données du datagramme IP en assurant l'intégrité des données et leur authentification. Toutes les données ne pourront être sécurisée pour une raison simple : certain champs dans les entêtes sont variables et donc de nature non prédictible. Ces champs pourront donc pas être considéré comme sûr, ce qui en fait le talon d'achille d'AH.

En revanche, il ajoute tout de même un contrôle contre les répétition et de d'intégrité des données sur un mode non connecté (couche IP).

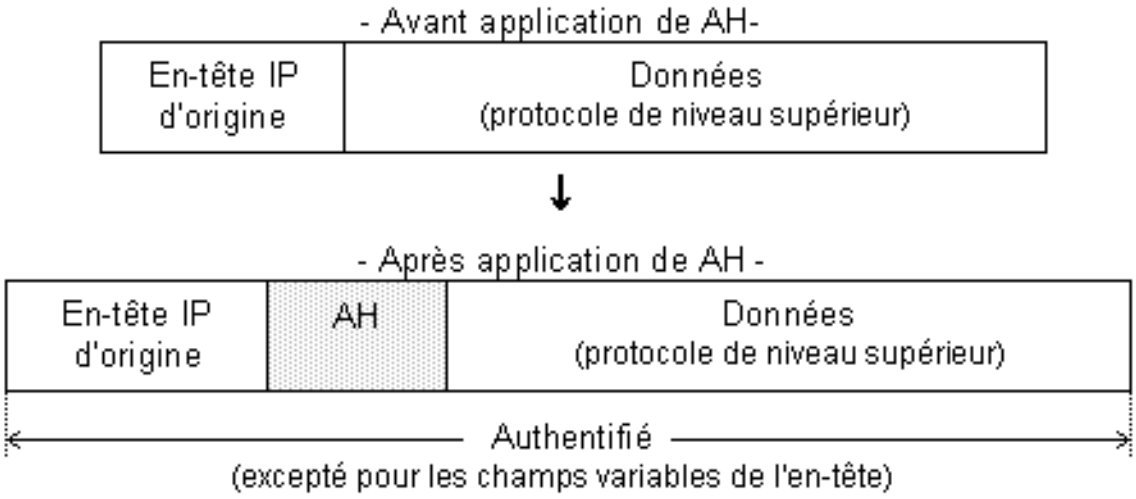


Illustration 3: Intégration d'AH dans un datagramme Ipv4 en mode transport.

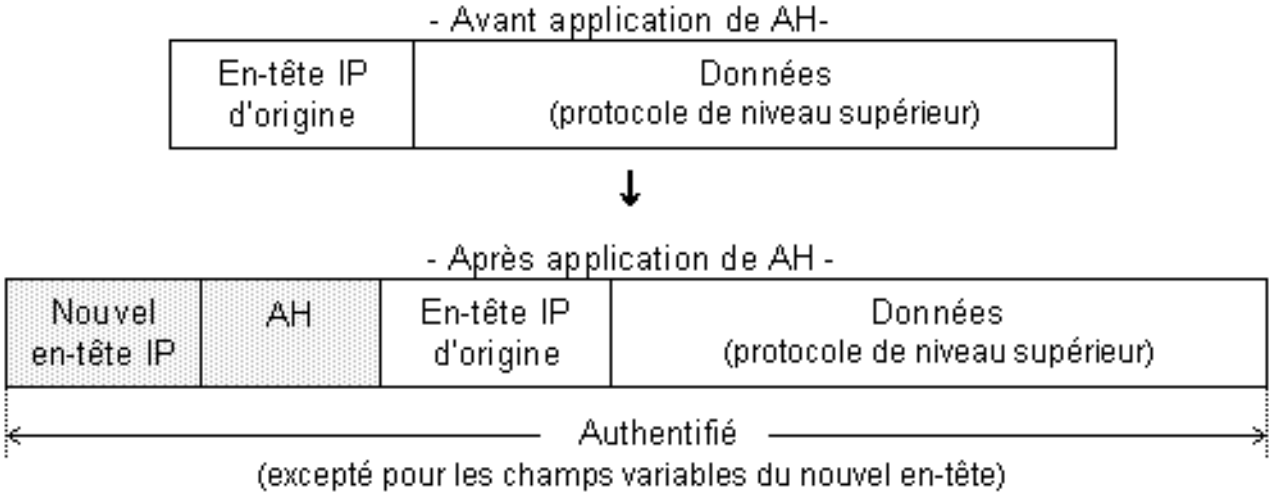


Illustration 4 Intégration d'AH dans un datagramme IPv4 en mode tunnel.

Détails des champs de l'en-tête AH :

8	*16*	*32*
Entête suivante	Longueur des données	Réservé
Security parameters index (SPI)		
Numéros de séquence		
Données Authentification (variable)		

- Entête suivante : ce champs permet de spécifier le type du protocole transporté ;
- Longueur des données : longueur de l'entête AH par facteur de 32-bit, le minimum étant 2 ;
- SPI : index unique définissant la SA pour ce paquet ;
- Numéros de séquence: compteur utile au mécanisme d'anti-répétition ;
- Données Authentification (variable) : champs contenant les signatures de hachages permettant d'authentifier l'émetteur et l'authenticité des données. la taille de ce champs dépend des protocoles de hachage utilisés.

b) Champs ESP

ESP permet la sécurisation des données du datagramme IP par le chiffrement (confidentialité), l'intégrité et l'authentification des données. En mode transport, seuls les données transportées par le datagramme seront protégée, en mode tunnels, ce sera l'intégralité du datagramme qui sera protégé.

L'authentification et l'intégrité des données sont assurés par les même mécanismes que pour AH.

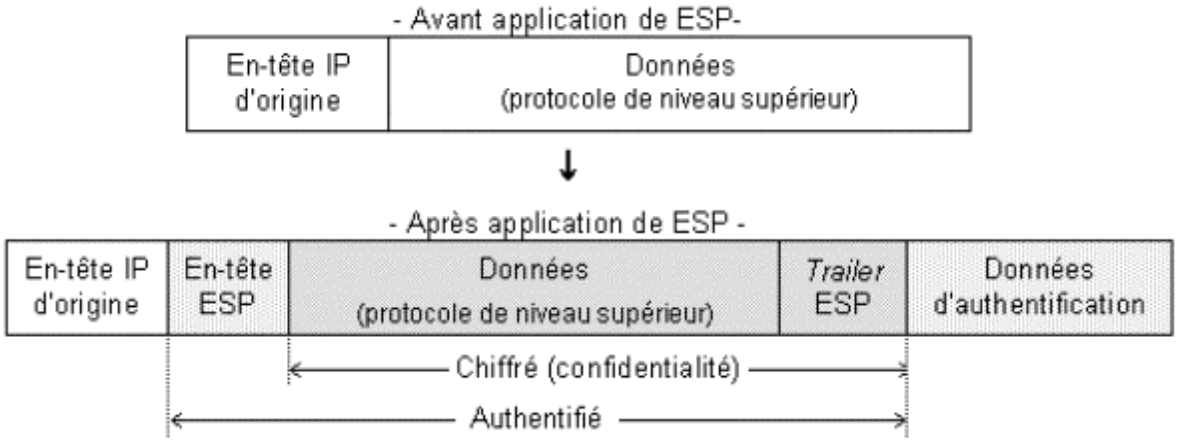


Illustration 5: Intégration d'ESP dans un datagramme Ipv4 en mode transport.

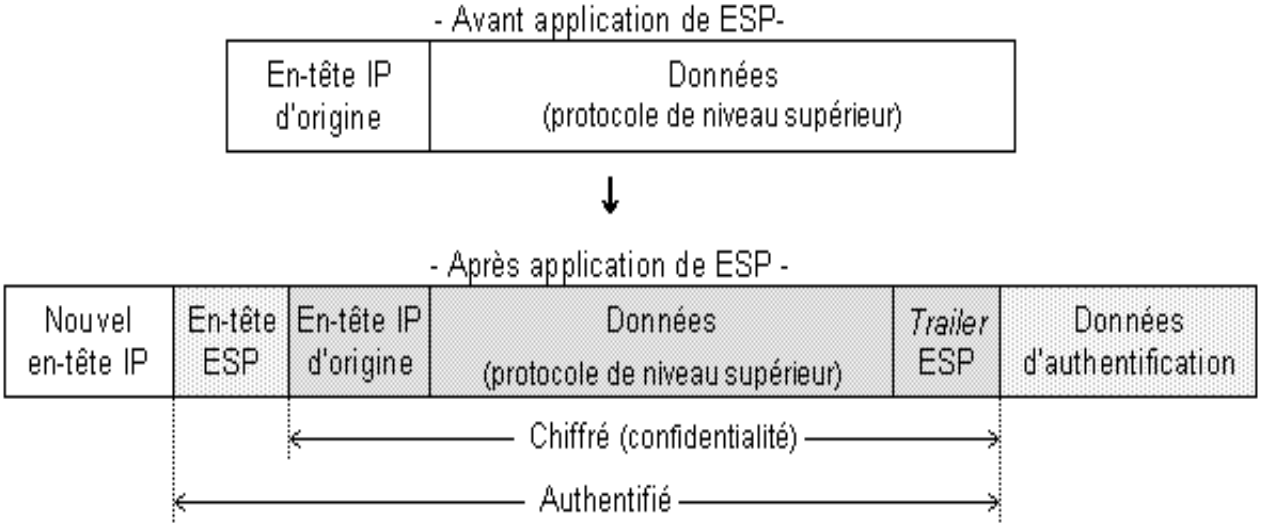


Illustration 6 Illustration 5: Intégration d'ESP dans un datagramme Ipv4 en mode tunnel.

Détails des champs du protocole ESP :

16	*24*	*32*
Security association identifier (SPI)		
Numéros de séquence		
Données		
Bourrage (0-255 octets)		
	Taille du bourrage	Entête souvante
Données Authentification (variable)		

- SPI : index unique définissant la SA pour ce paquet ;
- Numéros de séquence: compteur utile au mécanisme d'anti-répétition ;
- Données : donnée du protocole de couche supérieure ;
- Bourrage : sert à l'encryption des données. Certains protocoles nécessitent une certaine taille afin d'être plus efficace et/ou applicable ;
- Taille du bourrage : indique la taille du bourrage ;
- Entête suivante : ce champs permet de spécifier le type du protocole transporté ;
- Données Authentification (variable) : champs contenant les signatures de hachages permettant d'authentifier l'émetteur et l'authenticité des données. la taille de ce champs dépend des protocoles de hachage et d'encryption utilisés.

Tous les processus que nous venons de découvrir son donc basé sur des mécanisme de cryptage et de hachage complexe qui utilisent des clés de longueurs variable. Avant d'utiliser un VPN, il faut donc s'intéresser à la gestion de ses clés.

IV - Gestion des clefs IPSec

A - Les différents types de clefs

- **Clefs de chiffrement de clefs**
  Ces clefs sont utilisées afin de chiffrer d'autres clefs et ont généralement une durée de vie longue. Les clefs étant des valeurs aléatoires, l'utilisation d'autres clefs pour les chiffrer rend les attaques par cryptanalyse (tentatives de déchiffrement du message) plus difficiles à leur niveau. La cryptographie à clef publique est souvent utilisée pour le transport de clefs, en chiffrant la clef à transporter à l'aide d'une clef publique.

- **Clefs maîtresses**
  Les clefs maîtresses sont des clefs qui ne servent pas à chiffrer mais uniquement à générer d'autres clefs par dérivation. Une clef maîtresse peut ainsi être utilisée, par exemple, pour générer deux clefs : une pour le chiffrement et une pour la signature.

- **Clefs de session ou de chiffrement de données**
  Ces clefs, contrairement aux précédentes, servent à chiffrer des données.

B - PKI - Public Key Infrastructure

De nombreuses applications et protocoles utilisent le cryptage à chef publiques sur d'importants réseaux. Il est nécessaire de pouvoir gérer dans ce cas un nombre important de clefs publiques. Pour cela, on a recours à des Infrastructures à Clefs Publiques, ou PKI (Public Key Infrastructure). Ces infrastructures se basent généralement sur des autorités de certification (CA : Certificate Authorities), qui garantissent l'authenticité des clefs publiques et permettent une gestion hiérarchisée de celles ci

C - Echange de clefs et authentification

La première étape lors de l'établissement d'une communication sécurisée, est l'authentification des interlocuteurs. Ensuite, un échange de clef permet l'utilisation d'un mécanisme de sécurisation des échanges : l'authentification est ainsi étendue à la suite de la communication (L'échange de clef devant bien sur être authentifié).

1 - Les mécanismes de sécurisation des échanges

Le « *Perfect Forward Secrecy » (PFS)* est assurée par une renégociation régulière des clefs. Dans le cas ou un attaquant intercepterait et déchiffrerait une clef de session, celle ci serait probablement déjà « périmée » avant qu'il puisse l'utiliser.

L'Identity Protection, ou protection de l'identité, est respectée si un message intercepté ne permet pas de déterminer l'identité des tiers communiquant.

Le *Back Traffic Protection* consiste en une génération de nouvelles clefs de sessions sans utilisation de clefs maîtresses. Les nouvelles clefs étant indépendantes des clefs précédentes, la découverte d'une clef de session ne permet ni de retrouver les clefs de session passées ni d'en déduire les clefs à venir.

2 - Algorithme de Diffie-Hellman

Inventé en 1976 par Diffie et Hellman, ce protocole permet à deux tiers de générer un secret partagé sans avoir aucune information préalable l'un sur l'autre. Il est basé sur un mécanisme de cryptage à clef publique, et fait donc intervenir les valeurs publiques et privées des tiers. Le secret généré à l'aide de ce protocole peut ensuite être utilisé pour dériver une ou plusieurs clefs (clef secrète, clef de chiffrement de clefs...).

Cette algorithme est très simple pour l'échange des clefs :

Soient 2 personnes A et B désirant communiquer sans utiliser une clef secrète. Pour cela ils se mettent d'accord sur 2 nombres **g** et **n** tels que n soit supérieur à g et g supérieur à 1, et cela sur un canal non sécurisé (il faut que n soit grand: de l'ordre de 512 ou 1024 bits pour que l'échange des clefs soit sécurisé). Ils prennent chacun chez eux un nombre aléatoire :

- A choisit **x** ,calcul **X=g^x mod n** et l'envoie à B ;

- B choisit **y** ,calcul **Y=g^y mod n** et l'envoie à A.

Ainsi le pirate peut intercepter X, et Y mais il lui est très très difficile d'en déduire x et y (c'est sur ce principe que repose la sécurité de l'algorithme). Une fois dans son coin, A calcule **k=Y^x mod n** et B calcule **k'=X^y mod n**. En regardant de plus près, on constate que : **k=k'=g^xy mod n**. Ainsi, A et B ont réussi à créer un clef privée dont ils sont les seuls détenteurs

D - ISAKMP et IKE

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.

1 - ISAKMP

ISAKMP (Internet Security Association and Key Management Protocol) permet la négociation, l'établissement, et la suppression d'associations de sécurité (SA), permettant ainsi la sécurisation de paquets devant être acheminés.

Il s'agit d'un cadre générique permettant la négociation des associations de sécurité, mais il n'impose rien quant aux paramètres qui les composent. Cette négociation s'effectue en deux phases, permettant de séparer la négociation des SA pour la protection des données à transférer, de celle pour la protection du trafic propre à ISAKMP :

- Durant la première phase, un ensemble d'attributs relatifs à la sécurité est négocié, les identités des tiers sont authentifiées et des clefs sont générées. Ces éléments forment la SA/ISAKMP. Contrairement aux SA IPsec, la SA ISAKMP est bidirectionnelle. Elle srvira à sécuriser l'ensemble des échanges ISAKMP futurs.

- La seconde phase permet de négocier les paramètres de sécurité qui interviendront pour le transferts des données applicatives (le paquet IP qui devait être transmis, et qui est à l'origine de l'établissement d'une

SA). Les échanges de cette phase sont sécurisés grâce à la SA ISAKMP.

2 - IKE

IKE utilise ISAKMP, pour construire un protocole pratique. Le protocole de gestion des clefs associé à ISAKMP dans ce but est inspiré à la fois d'Oakley et de SKEME. Plus exactement, IKE utilise certains des modes définis par Oakley et emprunte à SKEME son utilisation du chiffrement à clef publique pour l'authentification et sa méthode de changement de clef.

IKE comprend quatre modes : le mode principal (*Main Mode*), le mode agressif *(Aggressive Mode*), le mode rapide (*Quick Mode*) et le mode nouveau groupe (*New Group Mode*).

Main Mode et *Aggressive Mode* sont utilisés durant la phase 1, et sont détaillés ci dessous. Q*uick Mode, quand à lui,* est un échange de phase 2, détaillé en 4.4.2.2.

New Group Mode sert à se mettre d'accord sur un nouveau groupe pour de futurs échanges Diffie-Hellman.

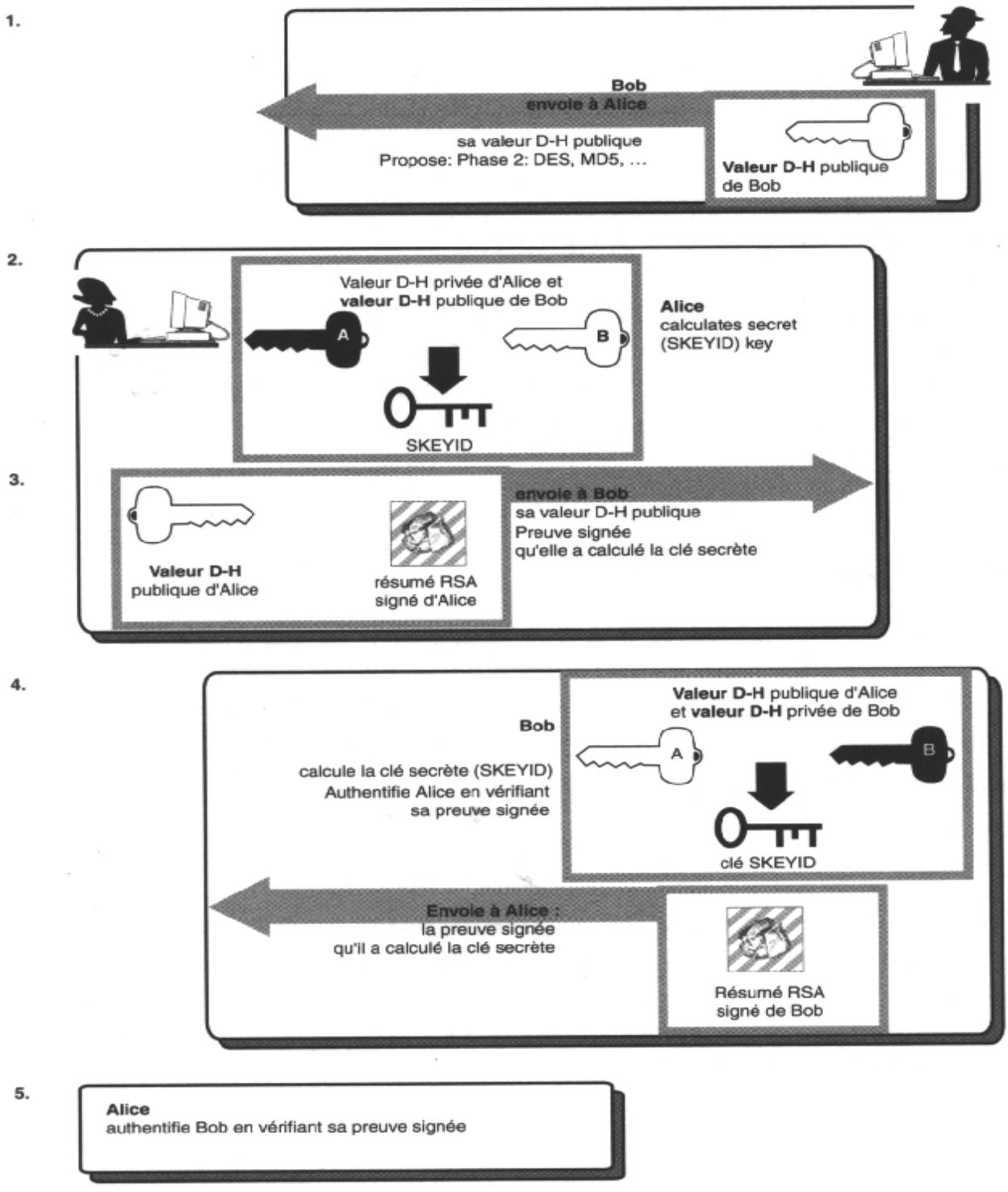
a) Phase 1

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.

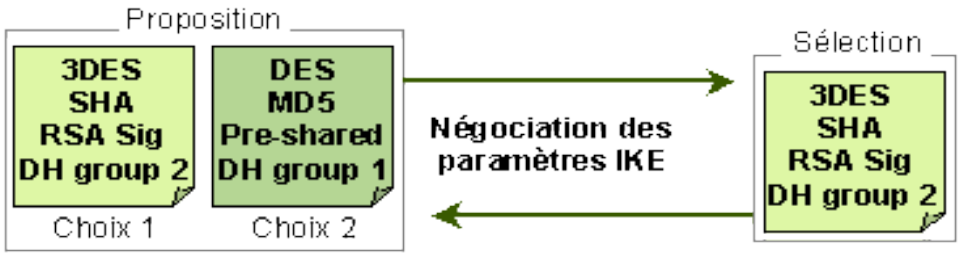
Trois clefs sont générées à l'issue de la phase 1 : une pour le chiffrement, une pour l'authentification et une pour la dérivation d'autres clefs. Ces clefs dépendent des cookies, des aléas échangés et des valeurs publiques Diffie-Hellman ou du secret partagé préalable. Leur calcul fait intervenir la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

Main mode

Composé de six messages, Main Mode est une instance de l'échange ISAKMP Identity Protection Exchange :

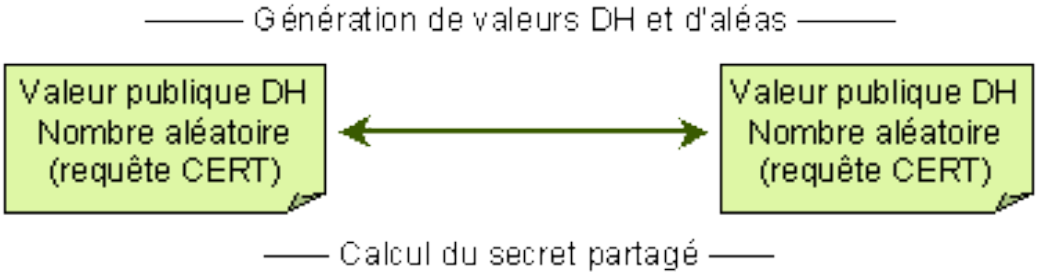

1.
Bob
envoie à Alice
sa valeur D-H publique
Propose: Phase 2: DES, MD5, ...
Valeur D-H publique
de Bob
2.
Valeur D-H privée d'Alice et
valeur D-H publique de Bob
A
B
SKEYID
Alice
calculates secret
(SKEYID) key
3.
Valeur D-H
publique d'Alice
résumé RSA
signé d'Alice
envoie à Bob
sa valeur D-H publique
Preuve signée
qu'elle a calculé la clé secrète
4.
Bob
calcule la clé secrète (SKEYID)
Authentifie Alice en vérifiant
sa preuve signée
Valeur D-H publique d'Alice
et valeur D-H privée de Bob
A
B
clé SKEYID
Envoie à Alice :
la preuve signée
qu'il a calculé la clé secrète
Résumé RSA
signé de Bob
5.
Alice
authentifie Bob en vérifiant sa preuve signée

- Les deux premiers messages servent à négocier les paramètres IKE : algorithme de chiffrement, fonction de hachage, méthode d'authentification des tiers et groupe pour Diffie-Hellman.



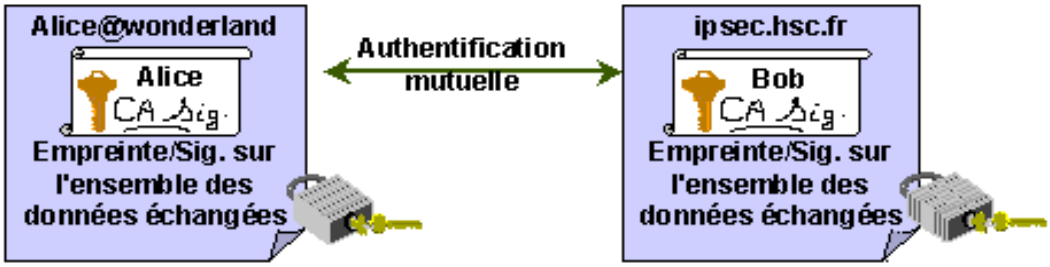
Les quatre méthodes d'authentification possibles sont la signature numérique, deux formes d'authentification par chiffrement à clef publique et l'utilisation d'un secret partagé préalable.

- Les deux seconds messages permettent l'établissement d'un secret partagé via l'utilisation du protocole Diffie-Hellman.



Le secret partagé sert à dériver des clefs de session, deux d'entre elles étant utilisées pour protéger la suite des échanges avec les algorithmes de chiffrement et de hachage négociés précédemment.

Les deux derniers messages servent à l'authentification des échanges et notamment des valeurs publiques.



Agressive mode

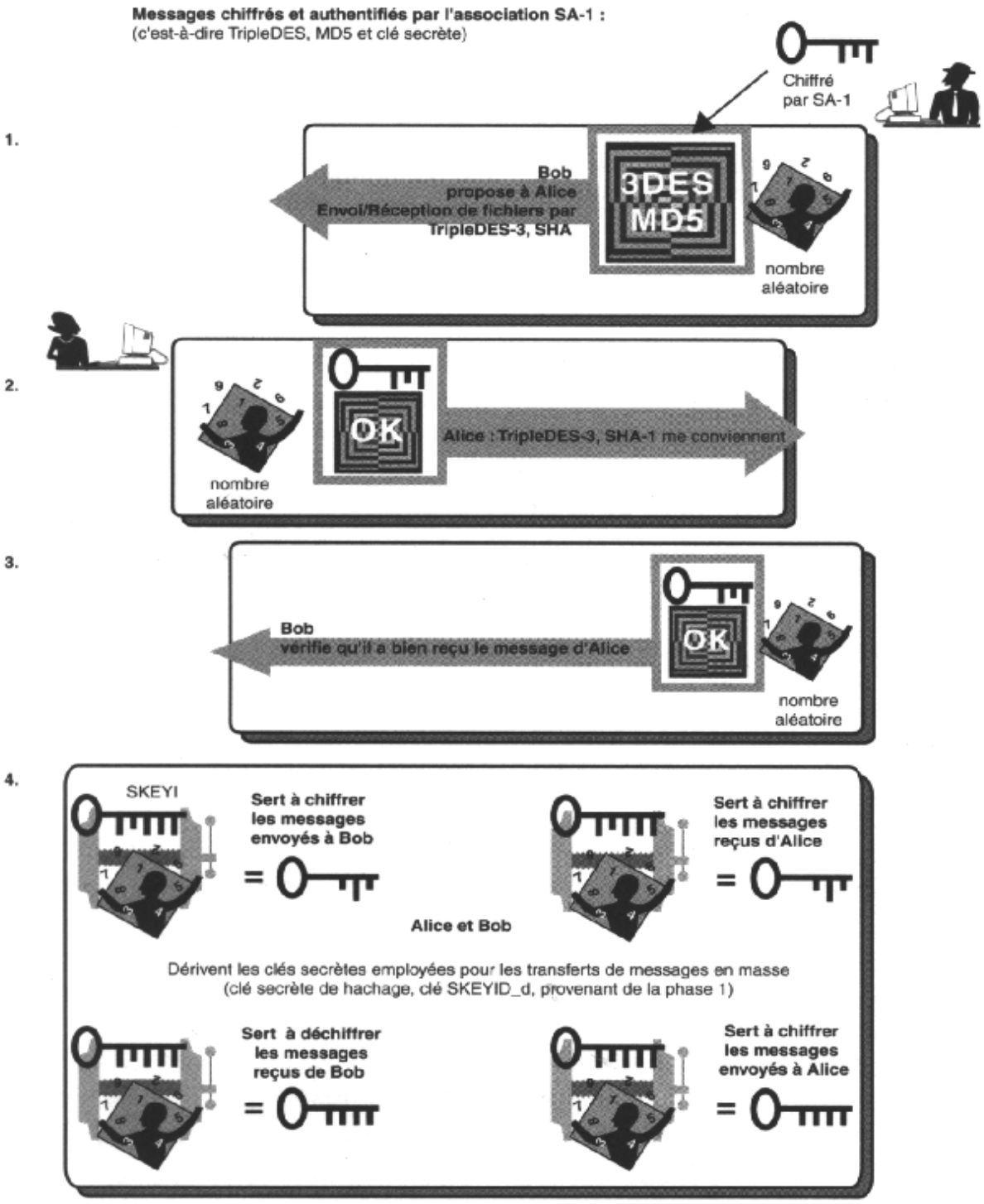
Aggressive Mode est une instance de l'échange ISAKMP Aggressive Exchange : il combine les échanges décrits ci-dessus pour Main Mode de façon à ramener le nombre total de messages à trois.

Dans les deux cas, la méthode choisie pour l'authentification influence le contenu des messages et la méthode de génération de la clef de session. Les quatre méthodes d'authentification possibles sont la signature numérique, deux formes d'authentification par chiffrement à clef publique et l'utilisation d'un secret partagé préalable.

b) Phase 2 : Quick Mode

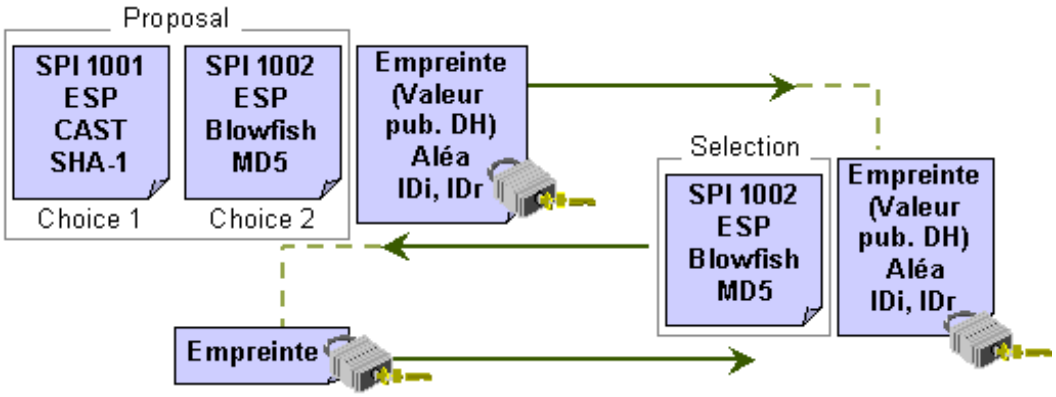
Les messages échangés durant la phase 2 sont protégés en authenticité et en confidentialité grâce aux éléments négociés durant la phase 1. L'authenticité des messages est assurée par l'ajout d'un bloc HASH après l'en-tête ISAKMP, et la confidentialité est assurée par le chiffrement de l'ensemble des 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.

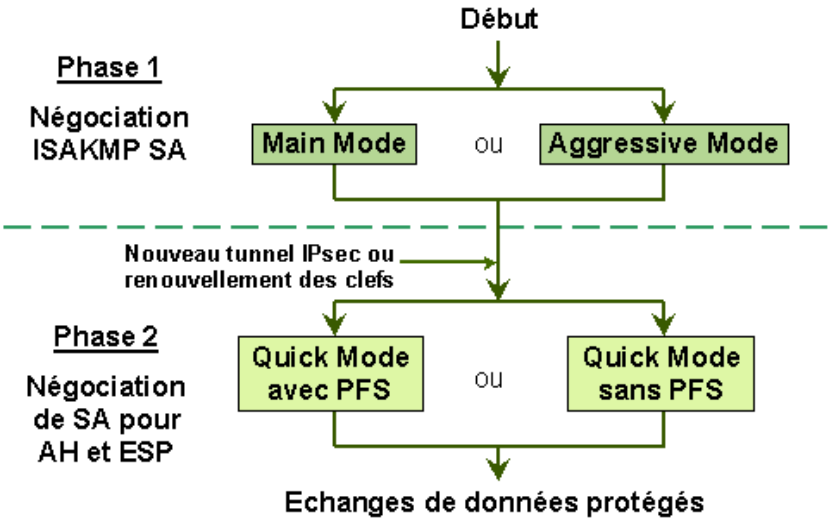

Messages chiffrés et authentifiés par l'association SA-1 :
(c'est-à-dire TripleDES, MD5 et clé secrète)
1.
Chiffré par SA-1
Bob propose à Alice Envoi/Réception de fichiers par TripleDES-3, SHA
3DES
MD5
nombre aléatoire
2.
OK
Alice : TripleDES-3, SHA-1 me conviennent
nombre aléatoire
3.
Bob vérifie qu'il a bien reçu le message d'Alice
OK
nombre aléatoire
4.
SKEYI
Sert à chiffrer les messages envoyés à Bob
Sert à chiffrer les messages reçus d'Alice
Alice et Bob
Dérivent les clés secrètes employées pour les transferts de messages en masse
(clé secrète de hachage, clé SKEYID_d, provenant de la phase 1)
Sert à déchiffrer les messages reçus de Bob
Sert à chiffrer les messages envoyés à Alice

Durant cette phase, il s'agit de :

- Négocier les paramètres IPSec ;
- Générer une nouvelle clef dérivée de celle négociée en phase 1 grace au protocole Diffie-Hellman. (si on prend on compte les mécanismes de sécurisation des échanges tels que PFS Perfect Forward Secrecy, ou le Back trafic Protection cus plus hauts, il peut y avoir d'autres échanges tels qu'une nouvelle négociation Diffie-Hellman..) ;
- Identifier le trafic que les SA négociées protégeront.



c) Synthèse de la négociation IKE



V - Démonstration

Ce dossier n'étant pas porté sur la configuration fine et l'explication de celles-ci, nous ne nous contenterons que de mettre à disposition nos configuration avec un minimum d'information.

A - Configuration du kernel

Pour base de nos maquette, nous avons configuré un noyau Linux 2.6.1 avec le support IPSec. Pour pouvoir utiliser IPSec avec ce noyau, il vous faudra compilé votre noyau avec les options suivante :

Dans "Networking options" :

- IP : AH transformation (CONFIG_INET_AH) ;
- IP : ESP transformation (CONFIG_INET_ESP) ;
- IPSec user configuration interface (CONFIG_XFRM_USER) ;

La dernière option nous permettra de pouvoir configurer IPSec depuis une interface utilisateur grâce à des outils Linux natif.

Vous pourrez aussi ajouter "IPComp transformation" (CONFIG_INET_IPCOMP) si vous voulez que votre noyau soit capable d'effectuer de la compression sur les données émise.

Dans "Cryptographic options", vous aurez la possibilité de sélectionner les différents algorithme que vous voudrez utiliser pour votre VPN, certains son coché d'office. Voici les options généralement voulues :

- Null algorithm ;
- MD5 digest algorithm ;
- SHA1 digest algorithm ;
- DES and Triple DES EDE cipher algorithms ;
- AES cipher algorithms.

B - Pré-requis de la maquette

1 - Configuration d'IPSec

Pour pouvoir utiliser et configurer correctement IPSec il nous faudra utiliser un outil spécifique qui aura pour rôle l'interface entre l'administration et le noyau.

Cet outil s'appelle "ipsec-tools" et est un portage de "KAME IPSec utilities" pour linux (http://ipsec-tools.sourceforge.net/).

Utilisant un système Debian pour la maquette j'ai pu installer cet outil avec la commande suivante :

```
# apt-get install ipsec-tools
```

Mais cet outil est aussi disponnible en paquage rpm.

2 - Configuration d'IKE

Pour pouvoir utiliser IPSec avec une gestion d'échange dynamique des clé, nous devons installer un serveur qui tiendra ce rôle. Le serveur que nous allons utiliser s'appelle "racoon" et est directement intégré dans ipsec-tools.

3 - Configuration réseau

Pour notre maquette nous avons dû simuler des réseaux locaux (172.16.0.0/16 et 172.15.0.0/16) utilisant les interfaces réelles de nos machines comme des passerelles de communication pour leurs échange. Ces deux interfaces (eth0) seront donc les points d'entrés dans notre tunnels IPSec.

Pour cela, nous avons donc configuré des interfaces virtuelles sur chaque machine avec la commande suivante :

Sur la première machine :

```
# ifconfig eth0:1 172.16.0.0 netmask 255.255.0.0
route add -net 172.15.0.0 netmask 255.255.0.0 gw 192.168.0.2
```

Sur la seconde :

```
# ifconfig eth0:1 172.15.0.0 netmask 255.255.0.0
route add -net 172.16.0.0 netmask 255.255.0.0 gw 192.168.0.10
```

C - Gestion des clés Manuelle

Ce mode permet de créer des VPN IPSec en utilisant toujours les même clés de chiffrage. Les deux hôte concerné par la communication doivent alors posséder ces même clés. Voici un la configuration que nous avons utilisé pour une maquette de ce type (fichier /etc/ipsec.conf) :

```
#!/sbin/setkey -f
flush;
spdflush;

# AH
#---
add 192.168.0.2 192.168.0.10 ah 15700 -A hmac-md5 "1234567890129999";
add 192.168.0.10 192.168.0.2 ah 24500 -A hmac-md5 "1234567890120000";

add 172.16.0.10 172.15.0.10 ah 15701 -A hmac-md5 "1234567890123499";
add 172.15.0.10 172.16.0.10 ah 24501 -A hmac-md5 "1234567890123400";

# ESP
#----
add 192.168.0.2 192.168.0.10 esp 15702 -E 3des-cbc "123456789012123456789999";
add 192.168.0.10 192.168.0.2 esp 24502 -E 3des-cbc "123456789012123456780000";

add 172.16.0.10 172.15.0.10 esp 15703 -E 3des-cbc "123456789012123456789099";
add 172.15.0.10 172.16.0.10 esp 24503 -E 3des-cbc "123456789012123456789000";



# Polices de Sécurité...
#-----------------------
spdadd 192.168.0.2 192.168.0.10 any -P in ipsec
        esp/transport//require
```

```
        ah/transport//require;

spdadd 192.168.0.10 192.168.0.2 any -P out ipsec
        esp/transport//require
        ah/transport//require;


spdadd 172.16.0.10 172.15.0.10 any -P in ipsec
        esp/transport//require
        ah/transport//require;

spdadd 172.15.0.10 172.16.0.10 any -P out ipsec
        esp/transport//require
        ah/transport//require;
```

Sur la seconde le machine, le fichier de configuration sera identique mis à part les "in" et les "out" qui devront être échangé.

Pour mettre en place la configuration décrite dans ces fichiers, nous devrons lancer la commande suivante sur les deux machines :

```
# setkey -f /etc/ipsec.conf
```

D - Gestion des clés dynamique

Nous allons continuer à utiliser un fichier de configuration /etc/ipsec.conf, mais cette fois-ci, nous n'y configurerons que la partie sur les polices de sécurité. Effectivement, ici les clés ainsi que les protocoles à utiliser seront négociés par racoon.

Nous allons donc créer un second fichier de configuration pour racoon qui aura la forme suivante (/etc/racoon.conf) :

```
path certificate "/etc/certs";
```

```
remote 192.168.0.2
{
	exchange_mode aggressive,main;
	my_identifier asn1dn;
	peers_identifier asn1dn;

	certificate_type x509 "iG4x.public" "iG4x.private";

	peers_certfile "denix.public";
	proposal {
		encryption_algorithm 3des;
		hash_algorithm sha1;
		authentication_method rsasig;
		dh_group 2;
	}
}

sainfo anonymous
{
	pfs_group 1;
	encryption_algorithm 3des ;
	authentication_algorithm hmac_sha1;
	compression_algorithm deflate ;
}
```

Ce fichier de configuration permet de définir des information tels que le répertoire contenant les certificats, les protocoles à utiliser, les mode d'échange, etc.

VI - Conclusion

A travers ce dossier, nous avons vu un aperçu des différentes possibilités afin de déployer un VPN, et particulièrement la solution que représente IPSec. Nous avions en effet pour objectif de vous donner les concepts qui tournes autour de cette solution et de vous montrer un exemple de déploiement. Mais également que le terme de VPN ne se référençait pas qu'a la solution IPSec. Certes cette solution est la plus utilisée et est une référence. Mais le VPN est avant tout un concept et ne précise rien concernant ses moyens.

Ainsi s'achève notre étude sur les VPNs. On se rend compte que derrière ce concept, une multitude de protocoles, techniques et architectures existent pour leur déploiement. Néanmoins, le choix d'une solution pour votre VPN dépendra évidement de l'utilisation que vous en ferez et de l'investissement financier que vous y mettrez.

Le VPN à pris une dimension proportionnelle au développement d'internet. A l'origine pour déployer les réseaux privés, une nouvelle utilisation voit le jour aujourd'hui avec l'arrivée des technologies sans file. En effet, dès les premières mise en place du 802.11 (WIFI), on nous à démontré ses failles en matière de confidentialité et de sécurité. Un risque parmi d'autres, est de voir ses données transitant dans le réseau être lues par un « homme du milieu ». Ses problèmes de sécurité sont une grande problématique quand des données sensibles sont communiquées. Les solutions VPN offre une possibilité de garantir cette sécurité et on peut alors penser à la possibilité d'allier le confort d'utilisation d'un réseau sans file à la sécurité des données qu'on transmet.

Nous tenons à remercier les rédacteurs du magazine MISC ainsi des différents articles sur Internet, qui nous ont permis de mettre en oeuvre et d'approfondir notre étude sur les VPN. Nous espérons que ce dossier vous aura permis d'acquérir de bonnes bases et une bonne culture pour aller plus loin avec les VPN.

Ressources et documentation

Liens / Documentation :

- Magasine MISC. N°10 Novembre-Décembre 2003
- http://ipsec-tools.sourceforge.net/
- http://lartc.org/howto/lartc.ipsec.html
- http://www.ipsec-howto.org/x242.html

RFC :

- 2407 : IP Security Domain.
- 2402 : AH.
- 2406 : ESP.
- 2409 : IKE.

Autre projet d'implémentation d'IPSec :

- http://ipsec-tools.sourceforge.net/.