IPSEC - ACCÈS DISTANT

Jean-Jacques Puig
Jean-Jacques.Puig@int-evry.fr
Doctorant
I.N.T

Maryline Laurent-Maknavicius
Maryline.Maknavicius@int-evry.fr
Maître de Conférence
I.N.T

- MAI 2002 -

Préambule

Dans le combat qui oppose les technologies économiques aux technologies de qualité, IP constitue le cheval de bataille des petits et moyens budgets. Dès lors, on essaie d'utiliser ce ``couteau suisse'' afin d'atteindre des objectifs - en apparence - dignes d'un gros-oeuvre, tels que la téléphonie, la diffusion vidéo ou radio, ou encore les réseaux privés étendus (de type WAN), etc, qui restaient les fiefs de technologies bien plus coûteuses, comme ATM, X25, le RTC, le RNIS, le réseau hertzien, les satellites... Le pari IP tient-il de l'audace ou de l'extravagance ?

Dans le cadre des réseaux privés, comme souvent sur Internet, de nombreuses solutions - incompatibles et non standardisées - ont été initialement développées (et continuent de l'être !) sans concertations mutuelles. Quelques directions sont désormais tracées dans cet espace ; PPTP, L2TP, TLS, SSL et SSH en font parties. Une autre de ces directions commence à acquérir de la valeur : IPsec.

Cette étude va se focaliser sur l'utilisation d'IPsec pour la constitution de réseaux privés virtuels impliquant des utilisateurs dotés d'une mobilité réduite - i.e. sans support du ``hand-over'' - et appelés ``télétravailleurs''. IPsec en mode tunnel est évidemment au premier plan, mais ses capacités sont trop limitées pour faire face à la complexité du problème : il est épaulé par d'autres protocoles spécialement conçus ou mis à niveau pour l'occasion, notamment PIC [6], DHCPv4 [5] et L2TP [9]. Interviennent aussi d'autres systèmes, comme des autorités de certifications ou des serveurs d'authentification.

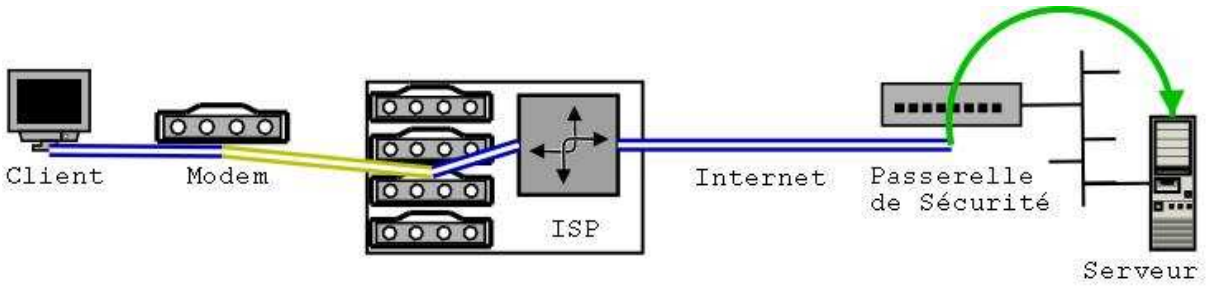
Tous ces points seront abordés ici mais, avant tout, il convient de préciser les sources d'informations qui ont été utilisées. De nombreux logiciels proposent déjà des implémentations d'IPsec pour le télétravail, mais leur compatibilité n'est pas assurée. Une information moins spécifique et moins propriétaire devait constituer la base de ce rapport. Pour cette raison, une attention particulière a été portée sur les travaux de standardisation du groupe IPSRA (IPsec Remote Access) de l'IETF. Ce groupe a produit trois drafts à ce jour, [2], [5] et [6], qui apportent de nombreuses précisions sur des points spécifiques. Les personnes les plus impliquées dans ces travaux sont Bernard Aboba (Microsoft) et Scott Kelly. Par ailleurs, le RFC 2401 [1], ``Architecture de Sécurité pour IP'' et les livres [3], [4] précisent comment est perçu l'accès distant d'un point de vue général, quels sont les besoins auxquels il doit répondre, et comment il doit s'intégrer à la stratégie de sécurité pré-existante de l'entreprise.

Les scénarios d'accès distant [2], les protocoles utilisés ([5] et [6]), les entités réseaux nécessaires ([2] et [6]), seront les objets successivement abordés dans cette analyse. Comme le processus de standardisation en est encore à ses balbutiements, nous étudierons la solution adoptée par Cisco et Microsoft dans leurs implémentations. En effet, cette solution bénéficiera d'une diffusion exceptionnelle auprès des entreprises et du public, et ne peut donc être ignorée.

I

Scénario 1

*Dans ce scénario, décrit dans [2], **les télétravailleurs utilisent un modem** (rtc, rnis, dsl, câble...) pour accéder à une ressource distante. **IPsec est intégré au poste de l'utilisateur**.*



Accès par Modem

Remarque : Au lieu d'intégrer IPsec dans le poste client, il est possible d'utiliser une passerelle de sécurité entre le poste client et le modem (cela est très fréquent pour les connexions dsl ou câble). Cela ne fait que déplacer le problème, car la passerelle de sécurité ainsi introduite se comporte à l'image d'un client vis à vis de la ressource distante à accéder. Cependant, cette passerelle se justifie dans un scénario 'agence satellite' (solution ``Satellite-Office - Home-Office" (SOHO)), ou lorsque les besoins de performances nécessitent l'utilisation d'un appareil spécialisé comportant une pile IPsec dite ``Bump In The Wire" (BITW).

Le télétravail nécessite de la part de l'utilisateur nomade de s'authentifier auprès de la passerelle de sécurité de son entreprise. La table suivante résume les besoins en terme d'authentification (quel que soit le protocole utilisé pour y parvenir) dans ce scénario (voir [2] pour plus de précisions) :

	Authentification Machine	**Authentification Utilisateur**	**Authentification Périodique**	**Mot de passe variable**
Serveur (@IP fixe, connexion persistante)	Obligatoire	-	-	-
Client rtc (@IP variable, connexion courte)	Facultative	Obligatoire	Facultative	Recommandé
Client dsl/câble (@IP fixe, connexion longue)	Facultative	Obligatoire	Recommandée	Recommandé
Client dsl/câble (@IP variable, connexion longue)	Facultative	Obligatoire	Recommandée	Recommandé

Modes d'Authentification Client - Passerelle de Sécurité

Considérations Politiques et Stratégiques :

- L'accès à Internet doit se faire via la connexion sécurisée, afin de bénéficier des systèmes (firewall, antivirus, proxy) du réseau mère. Alternativement, la politique de sécurité du réseau mère peut être répliquée sur la machine du télétravailleur pour lui permettre un accès direct à Internet. Enfin, il est aussi possible de bloquer l'accès à Internet quand une connexion sécurisée est établie.
- Une seule et unique connexion doit être autorisée pour un jeu de données d'accréditation (jeton, mot de passe, etc). PIC (voir plus loin) peut être utilisé pour l'obtention de ces données.
- Le réseau mère renvoie des paquets vers le client, et doit donc être sûr de la persistance de l'adresse IP de ce dernier. Le client peut disposer d'une adresse IP fixe allouée dans le domaine de l'ISP, mais le plus souvent, il se voit allouer une deuxième adresse IP (généralement privée) dans le réseau mère, qui lui permet ainsi d'avoir une présence ``virtuelle" dans ce réseau (réseau virtuel). Des paramètres complets sont alors nécessaires (masque de sous-réseau, routes, adresse de diffusion... voir DHCPv4 plus loin).

Commentaires :

- L'authentification du serveur garantit au client que le serveur n'a pas été usurpé.
- Côté client, c'est l'utilisateur qui doit être authentifié. Ainsi, le portable ne peut pas être utilisé à mauvais es-

cient si l'utilisateur n'est pas connecté. Une combinaison des deux modes d'authentification (machine et utilisateur) est cependant possible. Par exemple, le mot de passe fourni par l'utilisateur peut permettre de déchiffrer une clef sur le disque.

- Quand la durée de la connexion est longue (dsl, câble), il convient de re-authentifier périodiquement l'utilisateur, afin de s'assurer qu'un intrus ne profite pas d'une connexion ouverte ; la durée de la période est un compromis difficile de sécurité et de harcèlement de l'utilisateur.
- Un mot de passe variable ou à usage unique garantit qu'une interception du mot de passe ne laissera pas une faille persistante. Un système de type ``SmartCard'' peut aussi être utilisé.

Les risques rencontrés :

Risque N°1 :

Un Cheval de Troie a pris le contrôle total du client ; **la sécurité est compromise et il n'y a pas de solution standard**. Il est important de noter que ce risque existe notamment par le fait que le poste client a accès à Internet, et peut donc télécharger des codes hostiles. Une disquette ou un cdrom peut aussi contenir un tel programmme. Le troyen peut alors accéder via la connexion sécurisée au réseau privé de l'entreprise, s'y propager, y récupérer des données qu'il renverra directement sur Internet depuis le client (en simultané si la connexion Internet n'est pas désactivée pendant la connexion sécurisée, sinon en différé), via la passerelle Internet de l'entreprise, ou au travers de canaux cachés (par exemple en envoyant un mail ou en effectuant des requêtes DNS fantaisistes).

Risque N°2 :

Un intrus utilise la connexion de l'utilisateur. La re-authentification périodique permet de rompre la connexion avec l'intrus.

Risque N°3 :

Les données d'accréditation de l'utilisateur (mot de passe, jeton d'accès...) peuvent être subtilisées par un intrus. L'emploi de mots de passe fréquemment renouvelés, de données d'accréditation avec des durées de vie faibles, limitent les conséquences d'une telle situation: le pirate n'obtiendra qu'un accès temporaire (cela peut cependant lui permettre d'ouvrir des brèches permanentes). Par ailleurs, soulignons que s'il est interdit d'établir deux connexions simultanées avec les mêmes données d'accréditation, alors soit l'utilisateur peut se connecter, et le pirate ne le peut, soit le pirate est connecté, ce qui empêche l'utilisateur de se connecter et permet donc de suspecter la présence d'un intrus.

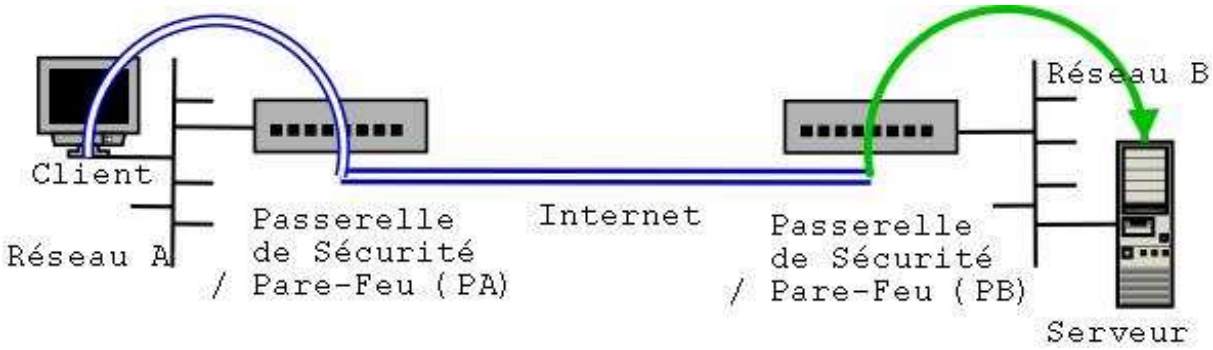
Risque N°4 :

Des mécanismes peuvent interagir avec IPsec (NAPT notamment). Il convient de s'assurer que ces mécanismes ne compromettent pas la connectivité. Ce risque ne relève pas de la sécurité du service, mais plutôt de sa disponibilité ou de sa sûreté.

II

Scénario 2

Dans ce scénario, ***le télétravailleur se connecte depuis un réseau A*** *pour accéder à une ressource distante située dans un réseau B. Pour plus de précisions, [2] décline ce scénario en trois versions dans ses sections 3.2, 3.3 et 3.4.*



Accès depuis un réseau

Les associations de sécurité se font, au choix :

i) Entre les extrémités (client <-> serveur) :

Les modes d'authentification sont dans ce cas similaires à ceux décrits dans le premier scénario.

ii) Entre le télétravailleur et la passerelle de sécurité du réseau distant (PB) :

Seul le trafic télétravailleur <-> serveur est alors autorisé par PB. Les modes d'authentification sont similaires à ceux décrits dans le premier scénario. Dans ce type de scénario, le réseau B est généralement supposé ``de confiance", alors que le réseau A, d'où se connecte le télétravailleur, n'est pas sûr. L'association de sécurité décrite ici assure, sous ces hypothèses, un niveau de sécurité suffisant.

iii) Entre les passerelles de sécurité des deux réseaux :

Seul le trafic télétravailleur <-> serveur est autorisé. Le niveau de sécurité réel dépend fortement de celui du réseau A. Notamment, il faut déterminer au niveau de quelle passerelle et via quel protocole se fait l'authentification de l'utilisateur, et il serait plus sûr de sécuriser le lien entre le télétravailleur et PA ; le réseau B doit donc avoir une certaine confiance dans les mécanismes de sécurité du réseau A, et plus particulièrement en PA ; en matière de sécurité, ce cas est déjà complexe et peut mener à des failles. En revanche, **une telle association de sécurité posera moins de problèmes d'incompatibilités avec le NAT que les deux solutions précédentes.**

Remarque : Dans ce scénario, il est possible de considérer une unité administrative du réseau A comme un ensemble de télétravailleurs autorisés, auquel cas une politique de sécurité peut être définie pour chaque machine et/ou utilisateur de l'unité administrative. Il est aussi possible d'isoler cette unité administrative (via une passerelle de sécurité, un VLAN...).

Considérations Politiques et Stratégiques :

- Quand le télétravailleur constitue une des extrémités de l'association de sécurité, il est possible de lui allouer une adresse IP dans le réseau B. Il a alors une présence ``virtuelle" dans ce réseau.
- Quand le télétravailleur constitue une des extrémités de l'association de sécurité, la connexion doit expirer automatiquement après un certain temps si le client n'en demande pas explicitement le maintien. Quand le tunnel concerne uniquement les deux passerelles de sécurité, l'absence de trafic pendant un certain temps permet de rompre l'association.
- Lorsque la connexion sécurisée est active, il convient de décider si l'utilisateur peut toujours accéder à Internet et via quel réseau. De plus, il faut aussi définir quelles sont les intéractions autorisées entre le client et le reste du réseau A (cela dépend en particulier de l'origine du client, des spécificités de son contrat, etc).
- Il convient d'archiver les dates de connexions et de déconnexions, et de rompre automatiquement au bout d'un certain temps d'inutilisation.

Risques :

Les risques majeurs rencontrés dans ce scénario sont de type opérationnels : suivant si les adresses des machines sont routables, suivant s'il existe des mécanismes de translation d'adresse, suivant si les protocoles d'IPsec sont

filtrés sur des noeuds intermédiaires, l'établissement des associations de sécurité pourra être difficile ou compromis.

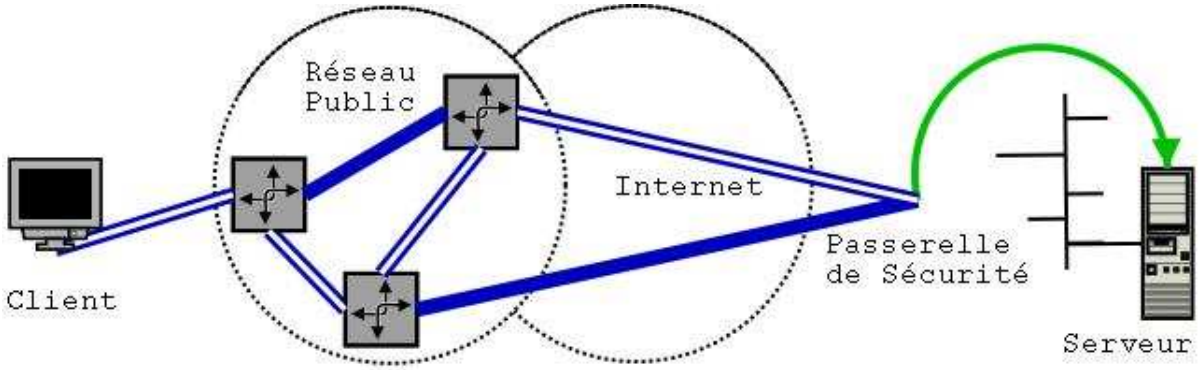
Remarque : Ce scénario englobe tout un ensemble de cas : coopération entre départements A et B d'entreprises, prestataire avec un ordinateur de bureau du site A, intervenant pourvu de son propre portable, etc (voir [2], sections 3.3 et 3.4). Quand la machine cliente est originellement issue du site B (cas d'un ordinateur portable), on pourrait se contenter d'effectuer une authentification de la machine et non de l'utilisateur. En réalité, il faut aussi considérer que le portable peut être utilisé à l'insu de son propriétaire ; l'authentification de l'utilisateur, si possible renouvelée périodiquement, est donc préférable.

III

Scénario 3

*Dans ce scénario, **le télétravailleur se connecte depuis un terminal d'un réseau public** pour accéder à une ressource distante située dans un réseau privé.*

Remarque : [2] présente ce scénario ainsi que le suivant dans une seule section (3.5). Or le présent rapport est plus concerné par la vision opérateur de l'accès distant, ce qui a nécessité une séparation plus explicite, en deux parties



Connexion depuis un terminal du réseau public

Dans ce scénario, on ne peut avoir confiance en la machine cliente. L'authentification ne se fera donc pas sur l'identité de la machine mais sur celle de l'utilisateur. Il convient de noter que la machine cliente peut **observer** les mots de passe, **modifier** les données saisies par l'utilisateur et **maintenir des connexions** ouvertes.

Par conséquent :

- Les informations nécessaires à l'accès doivent avoir une expression temporaire. Par exemple, les mots de passe à **usage unique** constituent l'expression temporaire d'un secret (la ``graine" du générateur de mots de passes); un dispositif de type ``SmartCard" (par exemple SecurID en version SmartCard) peut aussi remplir cette fonction, mais nécessite un périphérique approprié sur le client.
- Connexions à **durée limitée** uniquement, avec vérifications fréquentes de l'identité de l'utilisateur.
- Cette méthode ne peut être utilisée que pour accéder à des **données ayant une importance mineure**. On privilégiera notamment les accès en lecture uniquement.

Remarque : Concernant l'utilisation d'IPsec dans ce scénario, cela n'est possible que si celui-ci est disponible sur la machine cliente. Mais encore une fois, il n'y a aucune garantie quand au niveau de confiance que l'on peut avoir en cette machine. De plus, la configuration locale d'IPsec risque d'être contradictoire avec celle du réseau privé : si le réseau public utilise le NAT et propose le mode tunnel alors que le réseau privé n'accepte que le mode transport, la négociation de ISAKMP échouera.

Audit :

Comme pour le scénario précédent, il convient d'archiver les caractéristiques des connexions (dates de début et de fin, utilisateur, machines et données impliquées, etc). De plus, le client doit explicitement et périodiquement maintenir l'état de la connexion.

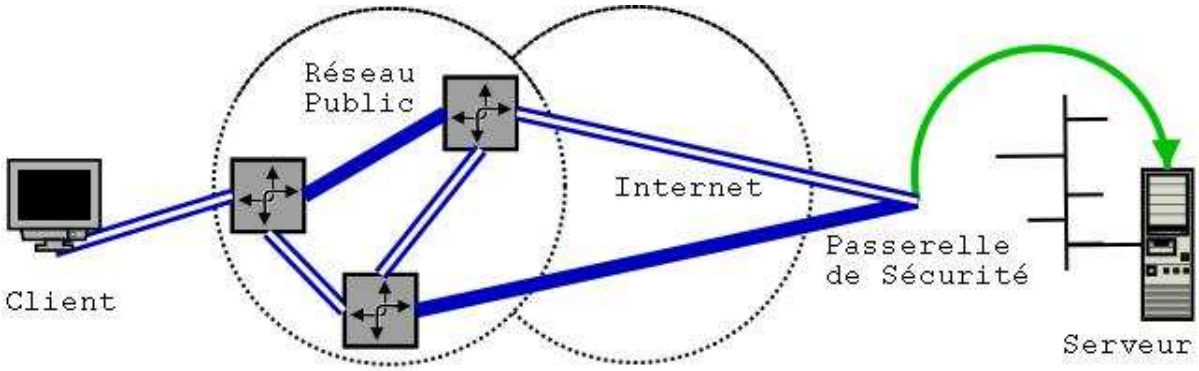
Les Problèmes Majeurs :

1. Dans le cas présent, une authentification par mot de passe est particulièrement vulnérable à une attaque ``Man in the middle". Ainsi, si le terminal client est malveillant, il peut intercepter lui-même le mot de passe (par exemple par le clavier) de l'utilisateur. Par ailleurs, le terminal client a pu être abusé: ``DNS poisoning", interception directe sur les câbles du terminal...
2. L'utilisateur n'est pas en mesure de vérifier l'identité du serveur, puisqu'il n'a pas nécessairement confiance en la machine cliente qui effectue les vérifications d'identités.

IV

Scénario 4

Comme dans le scénario précédent, dans ce scénario, ***le télétravailleur se connecte depuis un terminal d'un réseau public*** *pour accéder à une ressource distante située dans un réseau privé. La différence avec le scénario précédent est que l'****opérateur de réseau public est ici un partenaire de confiance*** *(un contrat lie les deux entités).*



Connexion depuis un opérateur public de confiance

Dans ce cas, la machine cliente est de confiance. On peut donc effectuer une authentification conjointe de la machine et du client. De plus, l'utilisation d'un mot de passe statique devient tolérable, par exemple en utilisant PIC (voir plus bas) pour construire un canal sécurisé entre le client et la passerelle de sécurité. En revanche, **limiter la durée de la connexion et effectuer des vérifications périodiques de l'identité de l'utilisateur restent indispensables**.

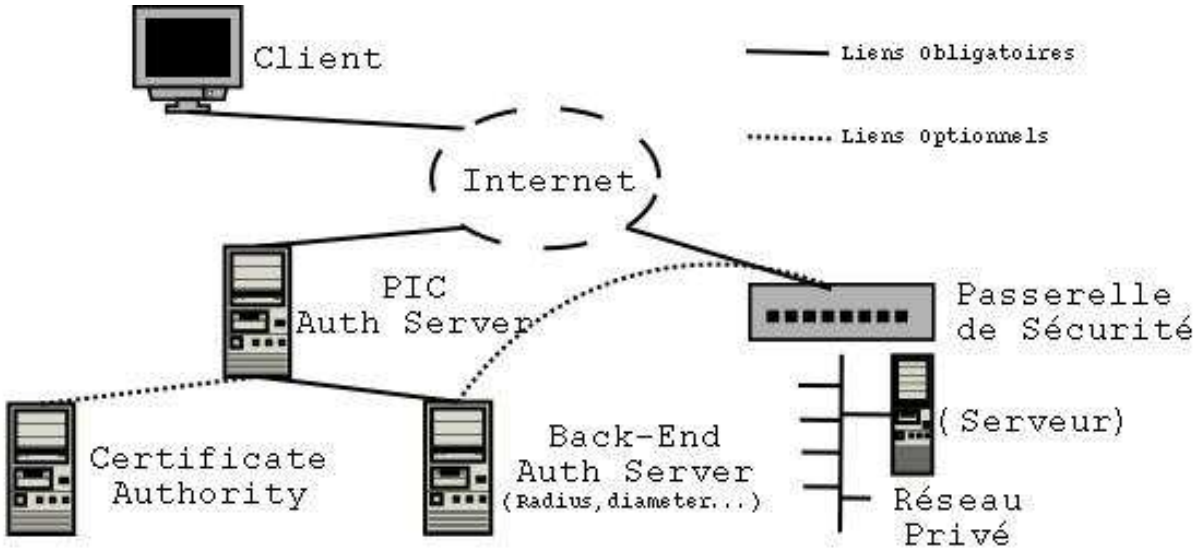
Audit :

Comme dans le scénario 3, il convient d'archiver les caractéristiques des connexions (dates de début et de fin, utilisateur, machines et données impliquées, etc). Le client doit explicitement et périodiquement maintenir l'état de la connexion.

V

Contrôle d'accès: PIC

PIC est l'acronyme de ``Pre-IKE Credential'' ; il est décrit dans le draft [6]. Grâce à ce protocole, le télétravailleur peut obtenir des jetons ou des certificats temporaires qui lui permettront de négocier une association de sécurité avec une passerelle de sécurité. PIC a été conçu pour s'intégrer au mieux dans le système de sécurité pré-existant de l'entreprise.



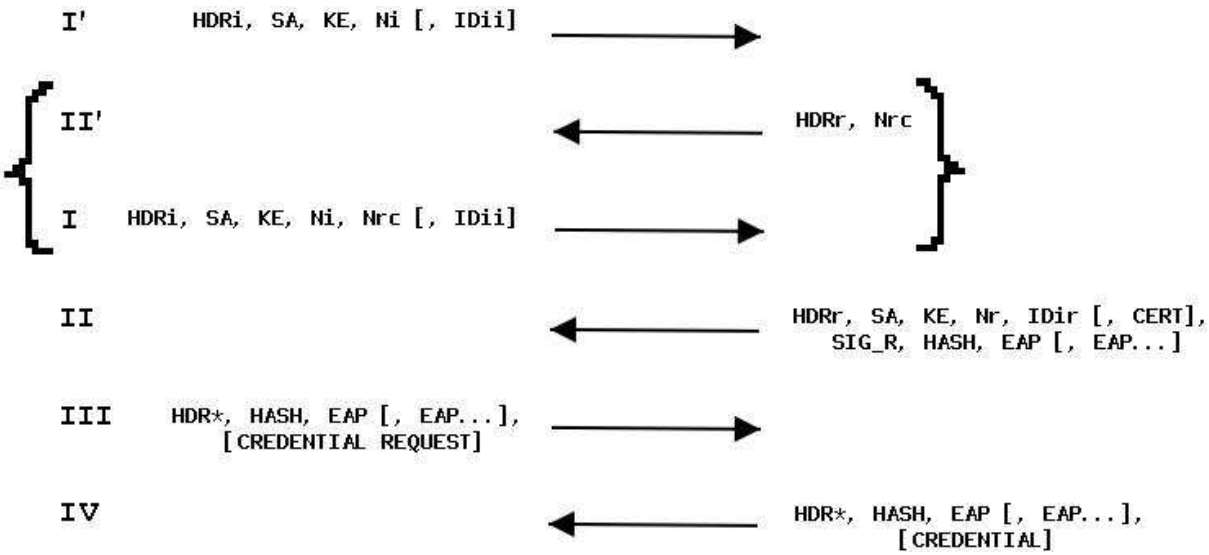
Architecture d'exploitation de PIC

Le schéma ci-dessus décrit dans quel existant PIC s'intègre. Une entreprise désire fournir un service d'accès distant sécurisé avec IPsec, et dispose donc d'une passerelle de sécurité (à droite sur le schéma) donnant accès aux services de son réseau privé. Cette passerelle est en mesure d'établir des associations de sécurité en utilisant IKE. Aucune hypothèse n'est faite sur la machine cliente (sauf, bien sûr, la présence des protocoles indispensables !), et c'est donc l'utilisateur qui sera authentifié. Malheureusement, IKE ne permet pas l'authentification d'une extrémité par un simple mot de passe. C'est à ce niveau que PIC intervient. PIC est en réalité une version allégée du couple ISAKMP/IKE, et augmentée de quelques caractéristiques, plus précisément de ``payloads'' EAP (Extended Authentication Protocol). Par l'entremise de PIC, l'utilisateur va obtenir un certificat qui lui permettra de négocier par IKE une association de sécurité avec la passerelle de sécurité. Pour cela, dans un premier temps, l'utilisateur se connecte à un serveur PIC. Ce dernier achemine les données d'authentification de l'utilisateur auprès d'un serveur d'authentification (de type Radius ou Diameter, qui garde notamment une trace de la transaction). Si l'authentification réussit, le serveur PIC renvoie un jeton/certificat à l'utilisateur, qui lui permettra d'entamer une négociation via IKE avec la passerelle de sécurité, en utilisant son adresse IP actuelle comme identité.

Remarque : Le scénario précédent peut être enrichi en fonction des éléments pré-existants du réseau ; notamment, le serveur PIC peut être connecté à un serveur spécialisé en tant qu'autorité de certification et l'utiliser, après une authentification réussie de l'utilisateur, pour générer un certificat temporaire.

Les échanges du protocole :

Le schéma suivant présente les échanges du protocole. Ils ressemblent fortement à la mise en oeuvre d'un mode agressif avec ISAKMP/IKE. Comme souvent dans ce type d'échange, deux messages (II' et I) sont introduits pour prévenir un déni de service et/ou pour protéger les identités des acteurs. Le champ Nrc créé par le récepteur dans le message II' s'appelle ``Routability Cookie'' et a pour but de vérifier que l'initiateur est bien joignable sur Internet. Pour cette raison, ce cookie est renvoyé en confirmation dans le message I (ce qui n'est pas le cas pour les ``Nonces'' Ni et Nr). Le serveur peut décider d'utiliser ou non ce système de cookies, et donc choisir entre un échange à six ou à quatre messages, en fonction de sa charge.



Les échanges de PIC (client - serveur PIC)

Concernant les payloads transportés dans l'échange, quelques précisions complémentaires s'imposent ; certains payloads sont en effet définis pour la première fois dans le draft de PIC [6] :

- Le payload ``SA'' des messages I', II', I, II comporte la description d'une association de sécurité particulière, pour laquelle la transformation n'est autre que celle de PIC : ``#PIC_TRANSF'' (nécessite l'enregistrement d'un numéro de transformation auprès de IANA).
- Les payloads EAP se comportent à la manière d'un tunnel pour acheminer des messages EAP classiques jusqu'à un serveur AAA.
- Les payloads CREDENTIAL_REQUEST et CREDENTIAL sont chargés, respectivement, de la demande explicite d'émission d'un jeton/certificat et de l'acheminement du jeton/certificat.

En conclusion, PIC répond a un besoin précis et a été conçu de façon à s'intégrer en souplesse avec les solutions de sécurité existantes. En revanche, la relative maturité du draft (cinquième version) peut être menacée par l'émergence prochaine d'une nouvelle version de IKE (laquelle risque de s'accompagner de modifications majeures de ISAKMP).

VI

Configuration distante: DHCPv4

Le groupe IPSRA a émis un draft [5] concernant les mises à jour à effectuer sur DHCPv4 pour une utilisation en mode tunnel dans le cadre de l'accès distant. En effet, les scénarios présentés précédemment (issus de [2]), nécessitent un tel protocole pour la configuration de la machine cliente.

Ce draft, qui en est tout de même à sa treizième version, se réfère aux besoins des scénarios d'accès distants pour la configuration à distance, plus précisément :

Paramètres de configuration distante :

- Adresses IP
- Masques de sous-réseaux
- Adresses de diffusion
- Noms des machines
- Noms des domaines
- Temps
- Serveurs (SMTP, POP, WWW, DNS/NIS, LPR, Syslog, WINS, NTP...)
- Routeurs (passerelles)
- Options de découverte des routeurs
- Routes statiques
- Unité maximale de transport (MTU)
- Durée de vie par défaut des paquets (TTL)
- Options de routage de source
- Activation/Désactivation de l'acheminement des paquets
- Options MTU du chemin (PMTU)
- Durée de vie du cache ARP
- Options de X-Windows
- Options du NIS
- Options de NetBIOS
- Options spécifiques au revendeur
- Autres options

Tous ces pré-requis, qualifiés de ``basiques" dans le draft, sont déjà pris en charges par DHCPv4, au contraire d'autres solutions, comme IKECFG (dont le draft a expiré). En revanche, pour une utilisation plus ``avancée", DHCPv4 doit être mis à niveau :

- Afin de supporter les reconfigurations ou des profils de configuration multiples.
- Afin de supporter les pools d'adresses.
- Afin d'assurer des reprises sur échec (``fail-over"). Le draft démontre à ce sujet la justesse du comportement de DHCPv4 vis à vis de IKE, qui peut faciliter ces reprises.

L'objet de [5] est surtout de définir un processus d'utilisation des différents protocoles impliqués dans le scénario d'accès distant : IKE, ISAKMP, IPsec, DHCPv4, etc.

Le scénario standard décrit dans le draft se décompose en trois étapes :

1. Etablissement entre le client et la passerelle d'une association de sécurité pour ISAKMP (phase 1).
2. Etablissement entre le client et la passerelle d'une association de sécurité pour IPsec en mode tunnel (phase 2 - ``quick mode") ; cette association est appelée ``DHCP AS" (Association de Sécurité pour DHCPv4) et sert à acheminer les messages de DHCP.
3. Enfin, soit l'association DHCP AS est abandonnée et une nouvelle association d'IPsec en mode tunnel est établie pour le transfert de données, soit l'association DHCP AS est recyclée pour remplir ce nouvel objectif.

A l'issue de ces étapes, le client est configuré et accède de façon sécurisée et transparente à son réseau.

En conclusion, DHCPv4 est la solution la plus cohérente, et la plus transparente pour l'existant de l'entreprise si ce protocole est déjà utilisé localement pour la configuration des machines. L'administration aussi s'en voit simplifiée (administration commune du serveur DHCP pour les deux contextes local et distant).

VII

Remarques Diverses

Nous avons pu remarquer un certain nombre de points communs dans les scénarios présentés ; notamment :

1 L'authentification de l'utilisateur est un leitmotiv.
2 L'authentification de la machine cliente vient en complément de l'authentification de l'utilisateur.
3 Le serveur doit aussi s'authentifier (authentification machine).
4 Un système d'audit doit être systématiquement mis en place.
5 On doit pouvoir configurer depuis le réseau mère les paramètres IP et politiques de sécurité du client.

Il faut aussi souligner **les absences ou les manques des solutions présentées** :

- La gestion des politiques de sécurité **n'est pas assez précise**: la réplication, la configuration distante et dynamique, la reprise ou le durcissement de la sécurité sur ``fail-over'' (i.e. lorsque le mécanisme principal n'est plus disponible et qu'un mécanisme de secours doit prendre le relais) n'ont pas fait l'objet de recommandations explicites ou n'ont pas été évoqués.
- L'accent est souvent mis sur les durées de vie des connexions, les périodes de re-authentification, mais **aucune valeur quantitative n'est donnée**.
- Dans tous les cas, il convient de déterminer si des mécanismes tels que le NAT ou un firewall peuvent compromettre une mise en oeuvre correcte d'IPsec, et si la passerelle de sécurité est connue a-priori. Cela peut nécessiter un processus de découverte et d'analyse des chemins impliqués dans la communication.
- Bien que le ``fail-over'' soit évoqué dans [5], **aucunes précisions ou recommandations n'ont été émises à ce sujet.** De plus, un tel mécanisme doit partager, dans certains cas, les secrets que le système principal, habituellement disponible, utilise avec les clients: pour le maintien des associations de sécurité en cours, pour en créer de nouvelles, etc.
- Ces scénarios semblent **incompatibles avec les solutions envisagées actuellement pour la mobilité forte** (``Hand-Over''). Par exemple, aucun processus standardisé n'explique comment une association de sécurité client - passerelle de sécurité peut être mise à jour lorsque l'adresse IP change. IKEv2 adresse des problématiques qui peuvent faciliter la construction d'une solution à ce niveau, par exemple la possibilité de détruire une association de sécurité (avant le ``Hand-Over'').
- Les scénarios présentés dans [2] font un grand cas de l'authentification, mais parce que ce draft a pour but de définir tout un ensemble de besoins, aucune solution, aucun protocole d'authentification n'y est présenté, ni à titre de solution, ni même à titre d'exemple. **La seule réponse du groupe IPSRA aux besoins d'authentification est ``EAP'', encapsulé dans PIC**.

La place de l'opérateur :

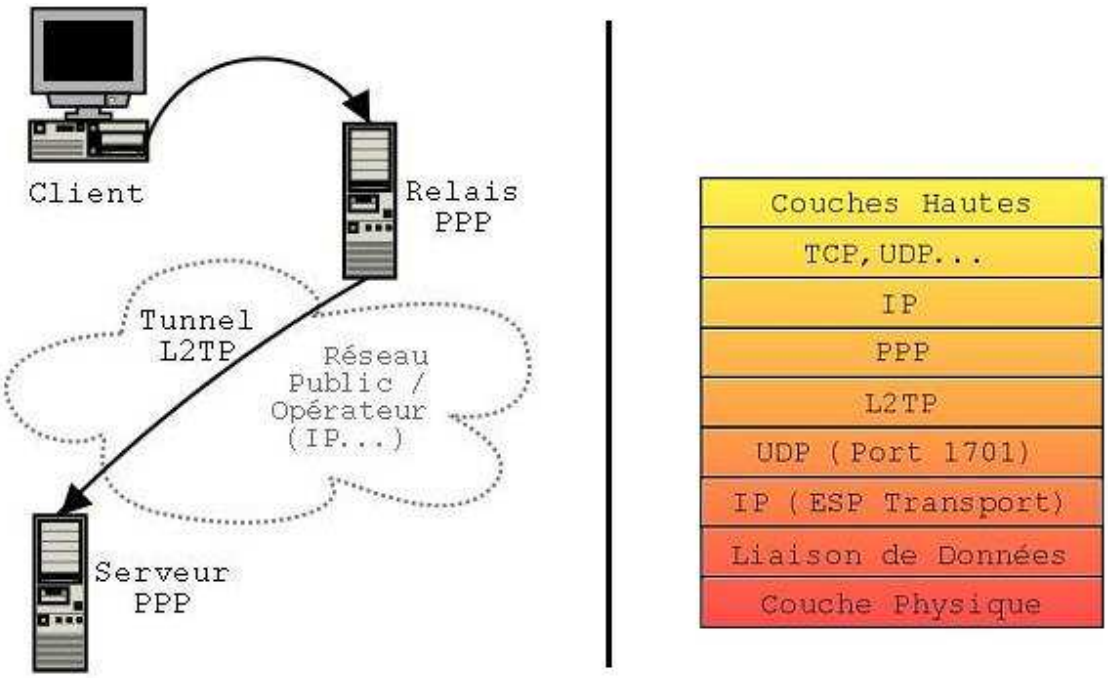
Cette étude a permis d'établir quelques scénarios dans lesquels un opérateur peut s'intercaler pour fournir un service à valeur ajoutée :

- Si les télétravailleurs ne doivent se connecter que depuis des terminaux (ordinateurs portables) de l'entreprise, la pile IPsec et des politiques de sécurité statiques peuvent être embarquées dans l'ordinateur. Une authentification conjointe (machine, utilisateur) est alors mise en oeuvre. Dans ce cas, l'opérateur peut vendre des adresses IP fixes de son domaine pour faciliter la constitution des politiques de sécurité et l'établissement des associations de sécurité. Si le réseau de l'opérateur comporte de nombreux routeurs, la mise à jour dynamique des tables de routage à la connexion d'un client peut devenir complexe. Il convient alors de réduire la disponibilité du service à certains points d'accès (POP).
- Si les télétravailleurs peuvent se connecter depuis n'importe quel terminal, l'opérateur peut assurer lui-même la sécurité par un tunnel IPsec avec la passerelle de sécurité de l'entreprise. Cela nécessite d'avoir des connexions sûres (sécurisées ou directes) entre les points d'accès POP de l'opérateur (serveurs PPP, DSLAM...) et les passerelles de sécurité du même opérateur. Ainsi, une fois le client authentifié auprès de son FAI par PPP (PAP, CHAP...), il est possible d'établir un tunnel IPsec entre une passerelle de sécurité de l'opérateur et celle de l'entreprise, et de garantir que le client ne sera pas en mesure de passer outre les politiques de sécurité (lesquelles auront été définies sur les passerelles de sécurité de l'opérateur). A grande échelle, ce système nécessite des serveurs de politiques de sécurité, afin de télécharger des politiques à la demande des passerelles de sécurité, ce qui induit une certaine inertie et une lourdeur d'administration. Par ailleurs, l'opérateur peut aussi prendre en charge la passerelle de sécurité du réseau d'entreprise et assurer ainsi un service ``VPN'' clefs-en-mains (Il ne reste alors plus au client qu'à définir ses besoins de politiques).

VIII

L'utilisation de L2TP au-dessus d'IPsec

En Novembre 2001, un document écrit conjointement par des équipes de Microsoft et de Cisco a acquis le statut de RFC 3193 [7]; Ce RFC décrit l'utilisation de L2TP au-dessus d'IPsec et constitue la fondation de la solution d'accès distant de ces deux entreprises [8].



L2TP: Utilisation et Encapsulation

Le document [7] est particulièrement obscur en ce qui concerne le contexte d'utilisation de L2TP sur IP. C'est en réalité parfaitement normal: les RFCs 2661 [9] et 2888 [10] traitent déjà de ces sujets. Le cas le plus général est présenté sur le schéma ci-dessus: le couple (L2TP,IPsec) y est utilisé pour acheminer un trafic PPP entre un relais, aussi appelé ``LAC'' (L2TP Access Concentrator), auquel est connecté un client, et un serveur PPP. Dans le cas qui nous intéresse, la connexion entre le relais et le serveur se fait sur Internet, d'où l'intérêt d'utiliser IPsec pour procéder à une authentification par paquet et à une vérification d'intégrité. En effet, la couche de sécurité de PPP ne fournit qu'une authentification initiale (à la connexion), et du chiffrement (en utilisant l'extension ``PPP Encryption Control Protocol (ECP)''); les caractéristiques de sécurité des deux protocoles se complètent donc bien. En revanche le trafic Client - Relais est faiblement sécurisé.

Dans le cadre de la solution d'accès distant fournie par Microsoft et Cisco, le Client et le Relais sont une seule et même machine. Voyons en quoi cela permet de construire un réseau privé virtuel:

- L'encapsulation du trafic se fait dans IPsec-ESP en mode transport ([7] propose aussi l'utilisation du mode tunnel, mais l'implémentation de Microsoft ne le supporte pas [8]). Cela assure la propriété ``privée'' de la communication.
- L'encapsulation de PPP par L2TP, puis par IPsec, permet d'allouer au client, via les mécanismes classiques de PPP, une adresse IP de l'entreprise. Cela assure la propriété "réseau virtuel", et s'inscrit donc en concurrence de DHCPv4 (voir plus haut).

En réalité, cette méthode d'accès distant sécurisé **s'inscrit dans une forme de tradition** : L'accès distant se faisait avant par modem sur un RAS (``Remote Access Server'', aussi appelé ``L2TP Network Server (LNS)'' dans le contexte L2TP) de l'entreprise, qui allouait au client une adresse IP du domaine privé via PPP. La couche de sécurité était alors liée à l'utilisation du réseau téléphonique, jugé sûr.

Cet aspect ``traditionnel'' de cette solution pourrait jouer en sa faveur. Malheureusement, elle introduit des effets de bords néfastes, conséquences inévitables d'un processus d'encapsulation lourd (voir pile de protocoles ci-dessus) : pour un client classique (modem RTC), l'encapsulation, pour du trafic http, sera: "données" -> http -> tcp -> IP -> PPP -> L2TP -> UDP -> IPsec -> PPP -> RTC.

- Chacune des couches citées précédemment a ses propres contraintes concernant les tailles des en-têtes, le padding, la taille des paquets d'informations (notamment, cette taille peut être variable ou non, comprise entre deux valeurs précises...). Les deux intéractions IP-PPP et PPP-IPsec sont notamment problématiques, d'autant plus que les MTU peuvent varier sur Internet et intéressent particulièrement le fonctionnement d'IPsec. Le RFC 3193 (section 3.2) propose donc de coupler l'information du PMTU obtenue par ICMP avec l'utilisation de PPP. Pour cela, IPsec doit remonter cette donnée à L2TP, qui redimensionne ses interfaces PPP. Il en résulte un mécanisme complexe dont le flux a sans doute une élasticité intéressante à étudier (d'autant plus si TCP est utilisé) et identifiable sur le réseau; il serait cependant étonnant que l'ensemble soit ``TCP-Friendly". De plus, on peut se poser des questions sur la performance d'un tel système, et l' ``overhead" dû à la traversé de la pile réduit nécessairement le débit d'informations utiles.
- D'autres intéractions peuvent advenir entre différentes couches de la pile. En particulier, **la compression et le chiffrement PPP peuvent augmenter les pertes de paquets** et ne s'accomodent pas nécessairement bien d'une arrivée désordonnée des paquets. Le RFC 3193, section 2.2 précise comment une implémentation peut éviter cela (au détriment de ses performances cependant).
- Les déconnexions, volontaires ou involontaires, peuvent se produire au niveau de PPP ou de la SA d'IPsec. Evidemment, une déconnexion au niveau d'une couche nécessite d'en informer l'autre et d'effectuer les traitements adéquats.
- L2TP est encapsulé dans UDP avant d'être encapsulé dans IPsec. Un port UDP est donc recommandé précisément pour cet usage: le port 1701. Bien sûr, le serveur PPP/L2TP peut avoir besoin de changer ce port, de façon à accepter les connexions issues de plusieurs clients (UDP ne différencie pas les clients communiquant sur le même port, au contraire de TCP). Des messages de L2TP permettent de le faire, et autorisent même le changement d'adresse IP (pour des raisons qui ne sont pas mentionnées dans le RFC). Le client n'en est pas capable, ce qui peut être un inconvénient dans le cas général où Client et Relais sont séparés. Le support technique de Microsoft précise, au sujet de l'implémentation: ``UDP port 1701 is used for both source and destination ports. This is non-negotiable" [8], et aucune information supplémentaire sur les ports n'est donnée. Il serait étonnant que les ports du serveur ne puissent changer, conformément à [7], même si le RFC est postérieur: il y aurait un problème évident de passage à l'échelle (un seul client pris en charge). Cependant, les administrateurs lisant le document [8] peuvent être amenés à définir des politiques de filtrage spécifiques pour le port 1701 en n'ayant pas conscience du fait que les ports peuvent évoluer en cours de communication. De la même manière, un port fixe au début de la négociation, mais évoluant par la suite, et la possibilité de changer d'adresse IP peuvent compromettre les définitions de politiques de sécurité pour IPsec, et détruire les associations de sécurité en cours.

Il est intéressant d'observer comment Microsoft et Cisco mènent la standardisation de cette solution en parallèle avec son implémentation et son déploiement. L2TP [9] est devenu un RFC en août 1999, et il s'agissait déjà d'une publication conjointe Cisco-Microsoft. Un an plus tard, la solution d'accès distant était disponible dans Windows 2000 (ce qui implique que l'implémentation était déjà en cours en 1999) et en même temps sortait le RFC 2888 -"Secure Remote Access with L2TP" [10]- qui, curieusement, n'a pas été produit par Microsoft ou Cisco. Enfin, le dernier pas a été franchi en novembre 2001 avec le RFC 3193 [7].

Quelle que soit la qualité de cette solution, le poids des acteurs fait qu'elle sera omniprésente. Cela ne signifie pas qu'il n'y en aura pas d'autres, ni même que ce sera la meilleure. Personnellement, j'y vois deux intérêts majeurs: sa disponibilité justement, et l'utilisation de PPP, qui s'inscrit dans la tradition de l'accès distant, et permet donc de maintenir des structures uniques (serveurs PPP) pour les clients qui se connectent via Internet et pour ceux qui se connectent directement via le RTC. J'y vois aussi un inconvénient majeur: cette solution dessine un fossé entre l'accès distant et Internet, qui sert en fait de medium. En ignorant les caractéristiques de IP, elle provoque un empilage conséquent de couches de protocoles. Une solution plus légère et plus cohérente avec l'usage d'IP peut être construite, en faisant fi de l'héritage de PPP. Le groupe IPSRA se tourne aujourd'hui vers ce dernier type de solutions. Microsoft est d'ailleurs aussi au premier plan, notamment au travers de ses contributeurs (les mêmes qui ont standardisé L2TP et son utilisation avec IPsec).

Conclusion

IP a des avantages indéniables dans un contexte d'accès distant :

- Les accès à Internet sont **largement disponibles**.
- Les accès à Internet sont **relativement économiques**.

En revanche, on ne peut nier l'aspect quelque peu ``bricolage'' des solutions de sécurité présentées. Si certains protocoles sont tout à fait matures (ESP surtout), d'autres sont difficiles à mettre en oeuvre (IKE et PIC). Dans le contexte de la mobilité réduite, le nombre important d'éléments nécessaires (serveurs, passerelles, configuration des clients) constituent un frein pour le déploiement et tendent à rendre difficile le passage à l'échelle.

L'intégration d'IPsec dans IPv6, soutenue par l'apparition de protocoles plus matures (IKEv2) et renforcée par la disparition de mécanismes tels que le NAT, pourrait constituer une bel avenir pour le support de la mobilité réduite sécurisée (et un bon tremplin pour celui de la mobilité forte sécurisée).

RÉFÉRENCES

[1] SECURITY ARCHITECTURE FOR THE INTERNET PROTOCOL
Date: Novembre 1998
Status: RFC 2401
Auteur: S. Kent, R.Atkinson
(Source: http://www.ietf.org/rfc/rfc2401.txt)

[2] REQUIREMENTS FOR IPSEC REMOTE ACCESS SCENARIOS
Date: Mars 2002
Status: draft-ietf-ipsra-reqmts-05
Auteur: S. Kelly, S.Ramamoorthi
(Source: http://www.ietf.org/internet-drafts/draft-ietf-ipsra-reqmts-05.txt)

[3] DEMYSTIFYING THE IPSEC PUZZLE
Date: 2001
Auteur: S. Frankel
Editeur: Artech House
(Source: ISBN: 1-58053-079-6)

[4] IPSEC SECURING VPNS
Date: 2001
Auteur: C.R. Davis
Editeur: RSA Press
(Source: ISBN: 0-07-212757-0)

[5] DHCPV4 CONFIGURATION OF IPSEC TUNNEL MODE
Date: Juillet 2001
Status: draft-ietf-ipsec-dhcp-13
Auteur: B. Patel, B. Aboba, S. Kelly, V. Gupta
(Source: http://www.ietf.org/internet-drafts/draft-ietf-ipsec-dhcp-13.txt)

[6] PIC, A PRE-IKE CREDENTIAL PROVISIONING PROTOCOL
Date: Février 2002
Status: draft-ietf-ipsra-pic-05
Auteur: Y. Sheffer, H. Krawczyk, B. Aboba
(Source: http://www.ietf.org/internet-drafts/draft-ietf-ipsra-pic-05.txt)

[7] SECURING L2TP USING IPSEC
Date: Novembre 2001
Status: RFC 3193
Auteur: B.Patel, B. Aboba, W.Dixon, G.Zorn, S.Booth
(Source: http://www.ietf.org/rfc/rfc3193.txt)

[8] IPSEC AND L2TP IMPLEMENTATION IN WINDOWS 2000
Date: 3 Août 2000
Status: Support Technique Microsoft (Q265112)
(Source: http://http://support.microsoft.com/default.aspx?scid=kb;EN-US;q265112)

[9] LAYER TWO TUNNELING PROTOCOL "L2TP"
Date: Août 1999
Status: RFC 2661
Auteur: W. Townsley, A. Valencia, A. Rubens, G. Pall, G. Zorn, B. Palter
(Source: http://www.ietf.org/rfc/rfc2661.txt)

[10] SECURE REMOTE ACCESS WITH L2TP
Date: Août 2000
Status: RFC 2888
Auteur: P. Srisuresh
(Source: http://www.ietf.org/rfc/rfc2888.txt)