Groupe de travail Réseau
Request for Comments : 5265
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

S. Vaarala, Codebay
E. Klovning, Birdstep

juin 2008

Traversée de IPv4 mobile à travers des routeurs de VPN fondés sur IPsec

Statut du présent mémoire

Résumé

Le présent document présente une solution pour le problème de la coexistence de IPv4 mobile (MIPv4) et de IPsec pour les utilisateurs professionnels. La solution consiste en une déclaration d'applicabilité pour l'utilisation de IPv4 mobile et d'IPsec pour la mobilité de session dans les scénarios d'accès professionnel distant, et en un mécanisme exigé pour détecter en toute sécurité le réseau interne de confiance.

Table des matières

1. Introduction

Le groupe de travail IP mobile a été établi pour explorer le problème et les espaces de solutions de la coexistence entre IPsec et IP mobile. La déclaration du problème et les exigences de solutions pour IPv4 mobile ont été documentées dans la [RFC4093]. Le présent document propose une solution pour IPv4.

Le document contient deux parties :

- une solution de base qui est une déclaration d'applicabilité de IPv4 mobile et d'IPsec traite de la mobilité de session entre intranets d'entreprise et réseaux externes, destinée aux utilisateurs de mobiles d'entreprise ;

- une spécification technique et un ensemble d'exigences pour la détection sécurisée des réseaux internes et externes, incluant une nouvelle extension qui doit être mise en œuvre par un nœud mobile et un agent de rattachement situés à l'intérieur du réseau d'entreprise.

Il y a de nombreuses façons utiles de combiner IPv4 mobile et IPsec. La solution spécifiée dans le présent document est surtout applicable quand les hypothèses documentées dans la déclaration de problème [RFC4093] sont valides ; entre autres, que la solution :
- doit minimiser les changements aux déploiements de pare-feu/VPN/DMZ existants ;
- doit assurer que le trafic n'est pas acheminé à travers la DMZ quand le nœud mobile est à l'intérieur (pour éviter les problèmes d'adaptabilité et de gestion) ;
- doit prendre en charge les réseaux étrangers avec seulement l'accès par l'agent étranger ;
- ne devrait pas exiger de changement aux protocoles existants IPsec ou d'échange de clés ;
- doit se conformer au protocole IPv4 mobile (mais peut exiger de nouvelles extensions ou plusieurs instances de IPv4 mobile) ; et
- doit proposer un mécanisme pour éviter ou minimiser la re-négociation IPsec quand le nœud mobile se déplace.

1.1 Généralités

Les réseaux d'entreprise normaux consistent en trois domaines différents : l'Internet (réseau externe non de confiance) l'intranet (réseau interne de confiance) et la DMZ, qui connecte les deux réseaux. L'accès au réseau interne est gardé à la fois par un pare-feu et un appareil VPN ; l'accès n'est permis que si les politiques de sécurité du pare-feu et du VPN sont respectées.

Les utilisateurs mobiles d'entreprise bénéficient d'une mobilité de session intégrale sans restriction entre les sous réseaux, sans considération de si les sous réseaux font partie du réseau interne ou externe. Malheureusement, les normes actuelles de IPv4 mobile et de IPsec seules ne fournissent pas un tel service [tessier].

La solution est d'utiliser l'IPv4 mobile standard (sauf pour une nouvelle extension utilisée par l'agent de rattachement dans le réseau interne pour aider à la détection de réseau) quand le nœud mobile est dans le réseau interne, et d'utiliser l'adresse de point d'extrémité de tunnel du VPN pour l'enregistrement IPv4 mobile quand il est en déplacement. Les tunnels VPN fondés sur IPsec exigent une renégociation après un mouvement. Pour surmonter cette limitation, une autre couche de IPv4 mobile est utilisée en dessous de IPsec, rendant en fait IPsec ignorant du mouvement. Donc, le nœud mobile peut se déplacer librement dans le réseau externe sans perturber la connexion de VPN.

En bref, quand il est à l'extérieur, le nœud mobile :
- détecte qu'il est à l'extérieur (Section 3) ;

- o enregistre son adresse d'entretien co-localisée ou d'agent étranger auprès de l'agent de rattachement externe ;
- o établit un VPN tunnel en utilisant, par exemple, le protocole d'échange de clés Internet (IKE, *Internet Key Exchange Protocol*) (ou IKEv2) si des associations de sécurité ne sont pas déjà disponibles ;
- o enregistre l'adresse du tunnel VPN comme son adresse d'entretien co-localisée auprès de l'agent de rattachement interne ; cette demande d'enregistrement est envoyée à l'intérieur du tunnel IPsec.

La solution exige le contrôle sur les couches de protocole dans le nœud mobile. Elle doit être capable de (1) détecter si il est à l'intérieur ou à l'extérieur de façon sûre, et (2) contrôler les couches de protocole en conséquence. Par exemple, si le nœud mobile est à l'intérieur, la couche IPsec doit devenir dormante.

Sauf la nouvelle extension IPv4 mobile pour améliorer la sécurité de la détection du réseau interne, les normes actuelles IPv4 mobile et IPsec, quand elles sont utilisées dans une combinaison appropriés, sont suffisantes pour mettre en œuvre la solution. Aucun changement n'est requis des appareils de VPN ou agents étrangers existants.

La solution décrite est compatible avec différentes sortes de VPN fondés sur IPsec, et aucune sorte particulière de VPN n'est requise. Parce que les entrées appropriées de base de données de politique de sécurité (SDP, *Security Policy Database*) et autres spécificités de IKE et IPsec diffèrent entre les produits de VPN fondé sur IPsec déployés, ces détails ne sont pas discutés dans le document.

1.2 Portée

Le présent document ne décrit une solution que pour IPv4. L'inconvénient de l'approche décrite est qu'un agent de rattachement externe est nécessaire et que les frais généraux par paquet (voir la Section 5) et la complexité globale augmentent. Des optimisations exigeraient des changements significatifs à IPv4 mobile et/ou IPsec, et sortent du domaine d'application du présent document.

VPN, dans ce document, se réfère à un VPN d'accès distant fondé sur IPsec. Les autres types de VPN sortent du domaine d'application.

1.3 Travaux connexes

Des travaux connexes ont été faits sur IPv6 mobile dans la [RFC3776], qui discutent de l'interaction de IPsec et de IPv6 mobile en protégeant la signalisation IPv6 mobile. Le document discute aussi de la mise à jour dynamique du point d'extrémité IPsec fondée sur les paquets de signalisation IP mobile.

L'attaque du "pseudo-NAT transitoire", décrite dans [pseudonat] et la [RFC3519], affecte toute approche qui tente de fournir la sécurité de la signalisation de la mobilité en conjonction avec des appareils de NAT. Dans de nombreux cas, on ne peut pas supposer de coopération de la part des appareils de NAT, qui doivent donc être traités comme toutes les autres entités de réseautage.

Le protocole de mobilité et multi rattachements IKEv2 (MOBIKE, *IKEv2 Mobility and Multihoming Protocol*) [RFC4555] fournit une meilleure mobilité pour IPsec. Cela permettrait à la couche externe IPv4 mobile décrite dans cette spécification d'être retirée. Cependant, déployer MOBIKE exige des changements aux appareils de VPN, et sort donc du domaine d'application de la présente spécification.

1.4 Termes et abréviations

Co-CoA *(co-located Care-of Address)* : adresse d'entretien co localisée

DMZ *(DeMilitarized Zone)* : zone démilitarisée, petit réseau inséré comme une "zone neutre" entre le réseau privé d'une entreprise et le réseau public extérieur pour empêcher les utilisateurs extérieurs d'obtenir un accès direct au réseau privé de l'entreprise.

FA *(Foreign Agent)* : agent étranger IPv4 mobile.

FA-CoA *(Foreign Agent Care-of Address)* : adresse d'entretien d'agent étranger.

FW *(FireWall)* : pare-feu.

I-FA *(IPv4 mobile Foreign Agent)* : agent étranger IPv4 mobile résidant dans le réseau interne.

I-HA *(IPv4 mobile Home Agent)* : agent de rattachement IPv4 mobile résidant dans le réseau interne ; il a normalement une adresse privée [RFC1918].

I-HoA : adresse de rattachement du nœud mobile dans l'agent de rattachement interne.

MN *(Mobile Node)* : nœud mobile.

NAI *(Network Access Identifier)* : identifiant d'accès réseau [RFC4282].

R : routeur.

réseau externe : réseau qui n'est pas de confiance (c'est-à-dire, Internet). Noter qu'un réseau privé (par exemple, un autre réseau d'entreprise) autre que le réseau interne du nœud mobile est considéré comme un réseau externe.

réseau interne : le réseau de confiance ; par exemple, un réseau d'entreprise sécurisé physiquement où est situé l'agent de rattachement IPv4 mobile.

SA *(Security Association)* : association de sécurité

tunnel VPN : tunnel fondé sur IPsec ; par exemple, une connexion IPsec en mode tunnel IPsec, ou du protocole de tunnelage de couche 2 (L2TP, *Layer 2 Tunneling Protocol*) combinée avec une connexion de transport IPsec.

VPN *(Virtual Private Network)* : réseau privé virtuel, fondé sur IPsec.

VPN-TIA *(VPN Tunnel Inner Address)* : adresse interne de tunnel VPN, la ou les adresses négociées durant IKE phase 2 (mode rapide) allouées manuellement, en utilisant IPsec-DHCP [RFC3456], en utilisant le mode de configuration standard "de facto" du protocole d'association de sécurité et de gestion de clés Internet (ISAKMP, *Internet Security Association and Key Management Protocol*) ou par d'autres moyens. Certains VPN clients utilisent leur adresse d'entretien actuelle comme adresse interne de tunnel (TIA, *Tunnel Inner Address*) pour des raisons d'architecture.

x-FA : agent étranger IPv4 résidant dans le réseau externe.

x-HA : agent de rattachement IPv4 mobile résidant dans le réseau externe.

x-HoA : adresse de rattachement du nœud mobile dans l'agent de rattachement externe.

1.5 Niveaux d'exigences

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDÉ", "PEUT", et "FACULTATIF" dans le présent document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

1.6 Hypothèses et justifications

La solution est une tentative de résolution du problème décrit dans la [RFC4093]. Les hypothèses majeures et leur raison sont résumées ci-dessous.

Les changements aux déploiements existants de pare-feu et de VPN devraient être minimisés :
- o les déploiement actuels de pare-feu et de VPN fondés sur IPsec sont beaucoup plus grands que les éléments IPv4 mobile correspondants. Donc, une solution devrait fonctionner dans l'infrastructure de VPN existante ;
- o les déploiements actuels de réseaux d'entreprise centralisent normalement la gestion de la sécurité et de l'accès au réseau dans une DMZ compacte.

Quand le nœud mobile est à l'intérieur, le trafic ne devrait pas passer à travers le réseau DMZ :
- o acheminer tout le trafic de nœud mobile à travers la DMZ est vu comme un problème de performances dans les déploiements de pare-feu existants. Plus la technologie de pare-feu est sophistiquée (par exemple, examen du contenu) plus le problème de performances est sérieux.

- o les déploiements actuels de pare-feu et de DMZ ont en général été optimisés pour le cas où seule une faible minorité du trafic total de l'entreprise passe à travers la DMZ. De plus, les utilisateurs des solutions courantes de VPN à accès distant n'acheminent pas leur trafic à travers la DMZ quand ils sont connectés à un réseau interne.

Un agent de rattachement à l'intérieur de l'entreprise ne peut pas être joint directement depuis l'extérieur, même si l'agent de rattachement contient la fonction IPsec :

- o les déploiements de solutions IPsec/MIPv4 combinées actuelles ne sont pas courantes dans les grandes installations ;
- o faire le déchiffrement dans les agents de rattachement "en profondeur " dans l'entreprise signifie effectivement d'avoir un périmètre de sécurité plus grand que la DMZ compacte utilisée normalement par la majorité des entreprises d'aujourd'hui ;
- o afin de maintenir un niveau de sécurité égal aux déploiements courants de pare-feu/DMZ, chaque agent de rattachement qui désencapsule IPsec va avoir besoin de faire le même travail de pare-feu que les pare-feu/DMZ courants (examen du contenu, suivi de la connexion, etc.).

Le trafic ne peut pas être chiffré quand le nœud mobile est à l'intérieur :

- o Il y a un impact considérable sur les performances des agents de rattachement (qui font actuellement un traitement assez léger) et des nœuds mobiles (en particulier les petits appareils). Noter que le débit du trafic à l'intérieur de l'entreprise est normalement d'un ordre de grandeur (ou plus) supérieur au trafic d'accès distant à travers un VPN.
- o Le chiffrement consomme de la puissance de traitement et a un impact significatif sur la durée de vie de la batterie.
- o Il y a aussi un problème d'utilisabilité ; l'utilisateur a besoin d'authentifier la connexion à la couche IPsec chez l'agent de rattachement pour obtenir l'accès. Pour les mécanismes d'authentification interactive (par exemple, SecurID) cela signifie toujours une interaction d'utilisateur.
- o De plus, si il y a dans la DMZ des appareils de VPN séparés pour l'accès à distance, l'utilisateur a besoin de s'authentifier aux deux appareils, et pourrait avoir besoin d'accréditifs distincts pour chacun.
- o Les agents de rattachement IPv4 mobile actuels n'incorporent pas normalement la fonction IPsec, qui est une solution pertinente quand on suppose zéro changement ou des changements minimaux aux nœuds IPv4 mobile existants.

Noter, cependant, que l'hypothèse (pas de chiffrement quand on est à l'intérieur) ne s'applique pas nécessairement à toutes les solutions de l'espace de solutions ; si les problèmes mentionnés ci-dessus sont résolus, il n'y a pas de raison fondamentale de ne pas appliquer le chiffrement quand on est à l'intérieur.

1.7 Pourquoi IPsec manque de mobilité

IPsec, comme spécifié actuellement [RFC4301], exige qu'une nouvelle négociation IKE soit faite chaque fois qu'un homologue IPsec bouge, c'est-à-dire, change d'adresse d'entretien. La principale raison en est qu'une association de sécurité est unidirectionnelle et identifiée par un triplet consistant en (1) l'adresse de destination (qui est l'adresse externe quand le mode tunnel est utilisé) (2) le protocole de sécurité (charge utile de sécurité encapsulante (ESP, *Encapsulating Security Payload*) ou en-tête d'authentification (AH, *Authentication Header*)) et (3) l'indice de paramètre de sécurité (SPI, *Security Parameter Index*) ([RFC4301], paragraphe 4.1). Bien qu'une mise en œuvre ne soit pas obligée de les utiliser tous pour ses propres associations de sécurité, une mise en œuvre ne peut pas supposer qu'un homologue ne le fait pas.

Quand un homologue mobile IPsec envoie des paquets à un homologue IPsec stationnaire, il n'y a pas de problème ; la SA est "la propriété" de l'homologue IPsec stationnaire, et donc, l'adresse de destination n'a pas besoin de changer. L'adresse de source (externe) devrait être ignorée par l'homologue stationnaire (bien que certaines mises en œuvre vérifient aussi l'adresse de source).

Le problème se pose quand les paquets sont envoyés de l'homologue stationnaire à l'homologue mobile. L'adresse de destination de cette SA (les SA sont unidirectionnelles) est établie durant la négociation IKE, et est effectivement l'adresse d'entretien de l'homologue mobile au moment de la négociation. Donc, les paquets vont être envoyés à l'adresse d'entretien d'origine, et non à une adresse d'entretien changée.

Le mécanisme IPsec de traversée de NAT peut aussi être utilisé pour une mobilité limitée, mais le tunnelage UDP doit être utilisé même quand il n'y a pas de NAT sur le chemin entre les homologues mobile et stationnaire. De plus, la prise en charge des changements dans la transposition de NAT actuelle n'est pas exigée par la spécification de traversée de NAT [RFC3947].

En résumé, bien que la norme IPsec n'empêche pas par elle-même la mobilité (au sens de la mise à jour au vol des associations de sécurité) la norme n'inclut pas de mécanisme incorporé (explicite ou implicite) pour le faire. Donc, on suppose dans ce document que tout changement des adresses comprenant l'identité d'une SA exige la renégociation de IKE, ce qui implique trop de calculs lourds et une trop grande latence pour une mobilité utile.

Le protocole de mobilité et multi rattachements IKEv2 (MOBIKE, *Mobility and Multihoming Protocol IKEv2*) [RFC4555] fournit une meilleure mobilité pour IPsec. Cela permettrait que la couche externe IPv4 mobile décrite dans cette spécification soit supprimée. Cependant, déployer MOBIKE exige des changements aux appareils de VPN, et sort donc du domaine d'application de cette spécification.

2. Environnement du réseau

Les utilisateurs professionnels vont accéder aux deux réseaux interne et externe en utilisant des technologies de réseautage différentes. Dans certains réseaux, le MN va utiliser des agents étrangers (FA) et dans d'autres il va s'ancrer à l'agent de rattachement (HA) en utilisant le mode co-localisé. La figure suivante décrit un exemple de topologie de réseau qui illustre les relations entre les réseaux interne et externe, et la localisation possible du nœud mobile (MN).

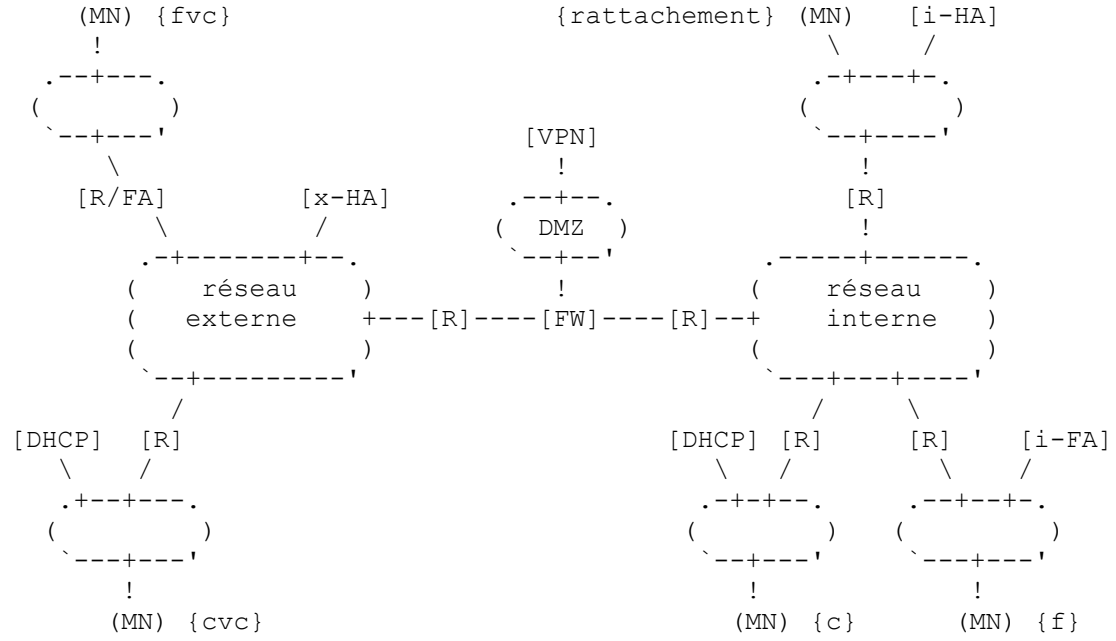


Figure 1 : Topologie de base, localisations possibles de MN, et modes d'accès

Dans chaque localisation possible décrite dans la figure, le nœud mobile peut établir une connexion aux HA correspondants en utilisant un "mode d'accès" convenable. Un mode d'accès est défini ici comme consistant en :

1. une composition de la pile de réseautage du nœud mobile (i-MIP ou x-MIP/VPN/i-MIP) ; et
2. un ou des modes d'enregistrement de i-MIP et x-MIP (si utilisé) ; c'est-à-dire, l'adresse d'entretien co-localisée ou l'adresse d'entretien de l'agent étranger.

Chaque mode d'accès possible est codé comme "xyz", où :

- "x" indique si la couche x-MIP est utilisée, et si utilisée, le mode ("f" indique FA-CoA, "c" indique co-CoA, l'absence indique non utilisé) ;
- "y" indique si la couche VPN est utilisée ("v" indique VPN utilisé, l'absence indique non utilisé) ; et
- "z" indique le mode de couche i-MIP ("f" indique FA-CoA, "c" indique co-CoA).

Il en résulte quatre modes d'accès :

c : i-MIP avec co-CoA
f : i-MIP avec FA-CoA
cvc : x-MIP avec co-CoA, VPN-TIA comme co-CoA i-MIP
fvc : x-MIP avec FA-CoA, VPN-TIA comme co-CoA i-MIP

Cette notation est la plus utile quand on envisage des optimisations aux couches de protocole. La notation est préservée ici afin que le travail d'optimisation puisse se référer à une notation commune.

Le réseau interne est normalement un réseau multi sous réseaux qui utilise un adressage privé [RFC1918]. Les sous réseaux peuvent contenir un ou des agents de rattachement internes, des serveurs DHCP, et/ou un ou des agents étrangers. Les LAN sans fil IEEE 802.11 actuels sont normalement déployés dans le réseau externe ou la DMZ à cause des soucis de sécurité.

La figure laisse de côté quelques détails qu'il vaut la peine de remarquer :
o Il peut y avoir plusieurs appareils de NAT n'importe où dans le diagramme ;
  * quand le MN est en dehors, les appareils de NAT peuvent être placés entre le MN et le x-HA ou le x-HA et le VPN ;
  * il peut aussi y avoir un ou des NAT entre le VPN et le i-HA, ou un NAT intégré dans le VPN. Par nature, tout routeur dans la figure peut être considéré représenter zéro, un ou plusieurs routeurs, chacun effectuant éventuellement un NAT et/ou un filtrage d'entrée ;
  * quand le MN est à l'intérieur, il peut y avoir des appareils de NAT entre le MN et le i-HA.
o Les tunnels de VPN de site à site ne sont pas montrés. Bien que transparents pour la plupart, les points d'extrémité IPsec peuvent effectuer un filtrage d'entrée au titre de l'application de leur politique.
o La figure représente une topologie où chaque entité fonctionnelle est illustrée comme un appareil distinct. Cependant, il est possible que plusieurs fonctions de réseau soient co-localisées dans un seul appareil. En fait, les trois composants de serveur (x-HA, VPN, et i-HA) peuvent être colocalisés dans un seul appareil physique.

Les questions suivantes sont aussi importantes quand on considère des utilisateurs mobiles professionnels :
o Certains pare-feu sont configurés à bloquer les messages et/ou fragments ICMP. Ces pare-feu (routeurs) ne peuvent pas être détectés de façon fiable.
o Certains réseaux contiennent des mandataires d'application transparents, en particulier pour HTTP. Comme les pare-feu, de tels mandataires ne peuvent pas être en général détectés de façon fiable. IPsec et IPv4 mobile sont incompatibles avec de tels réseaux.

Chaque fois qu'un nœud mobile obtient une co-CoA ou une FA-CoA, les étapes conceptuelles suivantes ont lieu :
o Le nœud mobile détecte si le sous réseau où l'adresse d'entretien a été obtenue appartient au réseau interne ou externe en utilisant la méthode décrite à la Section 3 (ou un mécanisme spécifique du fabricant satisfaisant les exigences décrites).
o Le nœud mobile effectue les enregistrements nécessaires et autre signalisation d'établissement de connexion pour les couches de protocole (dans l'ordre suivant) :
  * x-MIP (si utilisé) ;
  * VPN (si utilisé) ;
  * i-MIP.

Noter que ces deux tâches sont entremêlées dans une certaine mesure : la détection du réseau interne résulte en un enregistrement réussi au i-HA en utilisant l'algorithme de détection de réseau proposé. Un mécanisme de détection de réseau amélioré non fondé sur les messages d'enregistrement IPv4 mobile pourrait n'avoir pas cet effet colatéral.

Les paragraphes qui suivent décrivent les différents modes d'accès et les exigences pour la phase d'enregistrement et d'établissement de connexion.

2.1 Mode d'accès : 'c'

Ce mode d'accès est l'IPv4 mobile standard [RFC3344] avec une adresse co-localisée, excepté que :
o le nœud mobile DOIT détecter qu'il est dans le réseau interne, et
o le nœud mobile DOIT se réenregistrer périodiquement (avec un intervalle configurable) pour s'assurer qu'il est encore à l'intérieur du réseau interne (voir la Section 4).

2.2 Mode d'accès : 'f'

Ce mode d'accès est l'IPv4 mobile standard [RFC3344] avec une adresse d'entretien d'agent étranger, excepté que :
o le nœud mobile DOIT détecter qu'il est dans le réseau interne, et
o le nœud mobile DOIT se réenregistrer périodiquement (avec un intervalle configurable) pour s'assurer qu'il est encore à l'intérieur du réseau interne (voir la Section 4).

2.3. Mode d'accès : 'cvc'

Étapes :
o Le nœud mobile obtient une adresse d'entretien.
o Le nœud mobile détecte qu'il n'est pas à l' intérieur et s'enregistre avec le x-HA, où

* le bit T PEUT être établi (tunnelage inverse) minimisant la probabilité de problème de connexité relatif au pare-feu.

- Si le nœud mobile n'a pas une association de sécurité IPsec existante, il utilise IKE pour établir une association de sécurité IPsec avec la passerelle de VPN, en utilisant la x-HoA comme adresse IP pour la communication IKE/IPsec. Comment la VPN-TIA est allouée sort du domaine d'application du présent document.
- Le nœud mobile envoie une demande d'enregistrement MIPv4 (RRQ, *Registration ReQuest*) au i-HA, enregistrant la VPN-TIA comme adresse d'entretien colocalisée, où
  * le bit T DEVRAIT être établi (tunnelage inverse) (voir la discussion ci-dessous).

Le tunnelage inverse dans la couche interne IPv4 mobile est souvent requis à cause des limitations de la politique de sécurité de IPsec. Les sélecteurs IPsec définissent les adresses IP permises pour les paquets envoyés à l'intérieur du tunnel IPsec. Les sélecteurs de VPN distant IPsec normaux restreignent l'adresse de client à être la VPN-TIA (l'adresse distante est souvent non restreinte). Si le tunnelage inverse n'est pas utilisé, l'adresse de source d'un paquet envoyé par le MN va être l'adresse de rattachement du MN (enregistrée avec i-HA) qui est différente de la VPN-TIA, violant donc la politique de sécurité IPsec. Par conséquent, le paquet va être éliminé, résultant en un trou noir de connexion.

Certains types de VPN fondés sur IPsec, en particulier les VPN L2TP/IPsec (PPP sur L2TP sur IPsec) n'ont pas ces limitations et peuvent utiliser un acheminement triangulaire.

Noter que bien que le MN puisse utiliser l'acheminement triangulaire, c'est-à-dire, sauter la couche MIPv4 interne, il NE DOIT PAS, pour des raisons de sécurité, sauter la couche de VPN.

2.4 Mode d'accès : 'fvc'

Étapes :

- Le nœud mobile obtient une annonce d'agent étranger de la part du réseau local.
- Le nœud mobile détecte qu'il est en dehors et s'enregistre auprès du x-HA, où
  * le bit T PEUT être établi (tunnelage inverse) minimisant la probabilité de problème de connexité relatif au pare-feu.
- Si nécessaire, le nœud mobile utilise IKE pour établir une connexion IPsec avec la passerelle de VPN, en utilisant la x-HoA comme adresse IP pour la communication IKE/IPsec. Comment la VPN-TIA est allouée sort du domaine d'application du présent document.
- Le nœud mobile envoie une RRQ MIPv4 au i-HA, enregistrant la VPN-TIA comme adresse d'entretien colocalisée, où
  * le bit T DEVRAIT être établi (tunnelage inverse) (voir la discussion au paragraphe 2.3).

Noter que bien que le MN puisse utiliser l'acheminement triangulaire, c'est-à-dire, sauter la couche MIPv4 interne, il NE DOIT PAS, pour des raisons de sécurité, sauter la couche de VPN.

2.5 Traversée de NAT

Les appareils de NAT peuvent affecter indépendamment chaque couche. La traversée de NAT IPv4 mobile [RFC3519] DEVRAIT être prise en charge pour les couches x-MIP et i-MIP, tandis que la traversée de NAT IPsec [RFC3947] [RFC3948] DEVRAIT être prise en charge pour la couche de VPN.

Noter que la traversée de NAT pour la couche MIPv4 interne peut être nécessaire même quand il n'y a pas d'appareil de NAT séparé entre la passerelle de VPN et le réseau interne. Certaines mises en œuvre de NAT de VPN tunnellent les adresses internes avant d'acheminer le trafic à l'intranet. Parfois, cela est fait pour faciliter un déploiement, mais dans certains cas, cette approche rend plus facile la mise en œuvre du client de VPN. La traversée de NAT IPv4 mobile est nécessaire pour établir une session MIPv4 dans ce cas.

3. Détection du réseau interne

La détection sûre du réseau interne est critique pour empêcher que le trafic en clair soit envoyé sur un réseau qui n'est pas de confiance. En d'autres termes, la sécurité globale (confidentialité et intégrité des données d'utilisateur) s'appuie sur la sécurité du mécanisme de détection du réseau interne en plus de IPsec. Pour cette raison, les exigences de sécurité sont décrites dans cette section.

En plus de détecter l'entrée dans le réseau interne, le nœud mobile doit aussi détecter quand il a quitté le réseau interne. L'entrée dans le réseau interne est plus facile du point de vue de la sécurité : le nœud mobile peut s'assurer qu'il est à

l'intérieur du réseau interne avant d'envoyer du trafic en clair. La sortie du réseau interne est plus difficile à détecter, et le MN peut accidentellement laisser fuir des paquets en clair si l'événement n'est pas détecté à temps.

Plusieurs événements peuvent causer le départ du nœud mobile du réseau interne, incluant :
o un changement d'acheminement en amont ;
o une réassociation de 802.11 sur la couche 2 que le logiciel de nœud mobile ne détecte pas ;
o une déconnexion du câble physique et une reconnexion que le logiciel du nœud mobile ne détecte pas.

Si le nœud mobile peut détecter de façon fiable de tels changements dans la connexion actuelle dépend de la mise en œuvre et de la technologie de réseautage. Par exemple, certains nœuds mobiles peuvent être mis en œuvre comme de pures entités de couche 3. Même si le logiciel du nœud mobile a accès aux informations de couche 2, ces informations ne sont pas fiables du point de vue de la sécurité, et dépendent du pilote de l'interface réseau.

Si le nœud mobile ne détecte pas correctement ces événements, il peut laisser fuir du trafic en clair dans un réseau qui n'est pas de confiance. Un certain nombre d'approches peuvent être utilisées pour détecter la sortie du réseau interne, allant du réenregistrement fréquent à l'utilisation d'informations de couche 2.

Un nœud mobile DOIT mettre en œuvre un mécanisme de détection satisfaisant les exigences décrites au paragraphe 3.2 ; cela assure que les exigences de base de la sécurité sont satisfaites. L'algorithme de base décrit au paragraphe 3.3 est une façon de faire cela, mais d'autres méthodes peuvent être utilisées à la place ou conjointement. Les hypothèses sur lesquelles les exigences et le mécanisme proposé s'appuient sont décrites au paragraphe 3.1.

3.1 Hypothèses

Le pare-feu d'entreprise DOIT être configuré à bloquer le trafic originaire de réseaux externes allant au i-HA. En d'autres termes, le nœud mobile NE DOIT PAS être capable d'effectuer un échange réussi de demande d'enregistrement/réponse d'enregistrement (RRQ/RRP) (sans utiliser IPsec) sauf si il est connecté au réseau interne de confiance ; le nœud mobile peut alors arrêter d'utiliser IPsec sans compromettre la confidentialité des données.

Si cette hypothèse ne tient pas, la confidentialité des données est compromise d'une manière potentiellement silencieuse et donc dangereuse. Pour minimiser l'impact de ce scénario, le i-HA doit aussi vérifier l'adresse de source de toute RRQ pour déterminer si elle vient d'une adresse de confiance (réseau interne). Le i-HA a beoin d'indiquer au MN qu'il prend en charge la vérification des adresses de source de confiance en incluant une extension Réseaux de confiance configurés dans sa réponse d'enregistrement. Cette nouvelle extension, qui doit être mise en œuvre par l'i-HA et le MN, est décrite au paragraphe 3.4.

Le pare-feu PEUT être configuré à bloquer le trafic d'enregistrement au x-HA d'origine de l'intérieur du réseau interne, ce qui rend l'algorithme de détection de réseau plus simple et plus robuste. Cependant, comme la demande d'enregistrement est essentiellement du trafic UDP, un pare-feu ordinaire (même à états pleins) va normalement permettre que la demande d'enregistrement soit envoyée et qu'une réponse d'enregistrement soit reçue à travers le pare-feu.

3.2 Exigences de mise en œuvre

Tout mécanisme utilisé pour détecter le réseau interne DOIT satisfaire les exigences décrites dans cette section. Un exemple de mécanisme de détection de réseau satisfaisant ces exigences est donné au paragraphe 3.3.

3.2.1 Suivi séparé des interfaces réseau

La mise en œuvre de nœud mobile DOIT tracer séparément chaque interface réseau. L'enregistrement réussi avec le i-HA à travers l'interface X n'implique rien sur l'état de l'interface Y.

3.2.2 Changement d'état de connexion

Quand le nœud mobile détecte un changement de son état de connexion sur une certaine interface de réseau, il DOIT :
- o arrêter immédiatement de relayer les paquets de données d'utilisateur ;
- o détecter si cette interface est connectée au réseau interne ou externe, et
- o ne reprendre le trafic de données qu'après la détection du réseau interne et que les enregistrements nécessaires et l'établissement du tunnel de VPN ont été terminés.

Les mécanismes utilisés pour détecter un changement de l'état d'une connexion dépendent de la mise en œuvre de nœud mobile, de la technologie de réseautage, et du mode d'accès.

3.2.3 Détection du réseau interne fondée sur l'enregistrement

Le nœud mobile NE DOIT PAS déduire qu'une interface est connectée au réseau interne à moins qu'un enregistrement réussi ait été réalisé à travers cette interface particulière à l'i-HA, que la réponse d'enregistrement de l'i-HA contienne une extension Réseaux de confiance configurés (paragrapghe 3.4) et que l'état de connexion de l'interface n'ait pas changé depuis.

3.2.4 Surveillance du réseau interne fondée sur l'enregistrement

Certaines fuites de paquets en clair sur un réseau qui n'est (potentiellement) pas de confiance ne peuvent pas toujours être complètement évitées ; cela dépend fortement de la mise en œuvre de client. Dans certains cas, le client ne peut pas détecter ce changement, par exemple, si l'acheminement vers l'amont est changé.

Des réenregistrements plus fréquents quand le MN est à l'intérieur sont une façon simple de s'assurer que le MN est encore à l'intérieur. Le MN DEVRAIT commencer le réenregistrement toutes les (T_MONITOR - N) secondes quand il est à l'intérieur, où N est une période de grâce qui assure que le réenregistrement est achevé avant que T_MONITOR secondes soient écoulées. Pour donner une limite supérieure à la durée pendant laquelle peut persister une fuite de texte en clair, le nœud mobile doit satisfaire les exigences de sécurité suivantes quand il est à l'intérieur :

- Le nœud mobile NE DOIT PAS envoyer ou recevoir de paquet de données d'utilisateur si plus de T_MONITOR secondes se sont écoulées depuis le dernier réenregistrement réussi avec l'i-HA.

- Si plus de T_MONITOR secondes se sont écoulées, les paquets de données DOIVENT être éliminés ou mis en file d'attente. Si les paquets sont mis en file d'attente, les files d'attente NE DOIVENT PAS être traitées tant que le réenregistrement n'est pas achevé avec succès sans changement de l'état de connexion.

- Le paramètre T_MONITOR DOIT être configurable, et avoir la valeur par défaut de 60 secondes. Cette valeur par défaut est un compromis entre la surcharge de trafic et une limite raisonnable à l'exposition.

Cette approche est raisonnable pour une large gamme de nœuds mobiles (par exemple, les ordinateurs portables) mais a des frais généraux inutiles quand le nœud mobile est inactif (n'envoie ni ne reçoit de paquets). Si le réenregistrement ne s'achève pas avant T_MONITOR secondes, les paquets de données doivent être mis en file d'attente ou éliminés comme spécifié ci-dessus. Noter que les paquets de réenregistrement DOIVENT être envoyés même si du trafic bidirectionnel de données d'utilisateur est relayé : les paquets de données ne sont pas un substitut d'un réenregistrement authentifié.

Pour minimiser les frais généraux du trafic quand le nœud mobile est inactif, les réenregistrements peuvent être arrêtés quand aucun trafic n'est envoyé ni reçu. Si le nœud mobile reçoit ou a besoin ensuite d'envoyer un paquet, le paquet doit être éliminé ou mis en file d'attente (comme spécifié ci-dessus) jusqu'à ce qu'un réenregistrement avec le i-HA ait été réalisé avec succès. Bien que cette approche ajoute de la complexité au traitement de paquet, elle peut être appropriée pour les petits appareils, alimentés avec des piles, qui peuvent être inactifs la plupart du temps. (Noter que le réenregistrement ordinaire avant l'expiration de la durée de vie du lien de mobilité devrait quand même être fait pour que le MN reste joignable.)

Il est exigé que T_MONITOR soit configurable afin qu'un administrateur puisse déterminer le niveau de sécurité requis pour le déploiement particulier. Il n'est pas pratique de configurer T_MONITOR à quelques secondes ; des mécanismes de remplacement doivent être envisagés si un tel niveau de confiance est désiré.

Le mécanisme de réenregistrement est un mécanisme de repli au pire. Si des informations supplémentaires (comme des déclenchements de couche deux) sont disponibles au nœud mobile, il DEVRAIT utiliser les déclencheurs pour détecter le mouvement du MN et redémarrer le processus de détection pour minimiser l'exposition.

Noter que le réenregistrement est exigé par défaut par IPv4 mobile (sauf pour le cas atypique d'une durée de vie de lien infinie) ; cependant, l'intervalle de réenregistrement peut être bien plus grand quand on utilise un client IPv4 mobile ordinaire. Un intervalle de réenregistrement plus court n'est généralement pas un problème, parce que le réseau interne est normalement un réseau filaire rapide, et l'intervalle de réenregistrement raccourci s'applique seulement quand le nœud mobile est à l'intérieur du réseau interne. Quand il est à l'extérieur, le processus ordinaire de réenregistrement IPv4 mobile (fondé sur la limitation de la durée de vie) est utilisé.

3.3 Algorithme proposé

Quand le MN détecte qu'il a changé son point de rattachement au réseau sur une certaine interface, il produit deux demandes simultanées d'enregistrement, une au i-HA et l'autre au x-HA. Ces demandes d'enregistrement sont périodiquement retransmises si des messages de réponse ne sont pas reçus.

Les réponses d'enregistrement sont traitées comme suit :

- Si une réponse est reçue du x-HA, le MN arrête de retransmettre sa demande d'enregistrement au x-HA et tente de déterminer si il est dehors. Cependant, le MN DOIT continuer de retransmettre son enregistrement au i-HA pendant un certain temps. Le MN PEUT retarder l'établissement de connexion IPsec pendant un certain temps alors qu'il attend une (éventuelle) réponse du i-HA.
- Si une réponse est reçue du i-HA et si la réponse contient l'extension Réseaux de confiance configurés (paragraphe 3.4) le MN DEVRAIT déterminer qu'il est à l'intérieur. Dans tous les cas, le MN DOIT arrêter de retransmettre ses demandes d'enregistrement au i-HA et au x-HA.
- Quand il a réussi à s'enregistrer directement auprès du i-HA, le MN DEVRAIT se désenregistrer du x-HA.

Si le MN finit par détecter qu'il est à l'intérieur, il DOIT se réenregistrer périodiquement (sans considération de la durée de vie du lien) ; voir le paragraphe 3.2.4. Si le réenregistrement échoue, le MN DOIT arrêter d'envoyer et recevoir du trafic en clair, et DOIT redémarrer l'algorithme de détection.

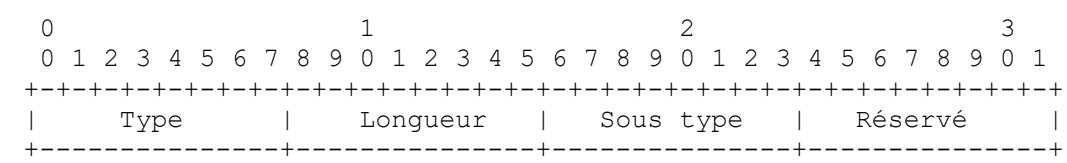
Les messages de réenregistrement en clair sont toujours adressés soit au x-HA, soit au i-HA, pas aux deux. C'est parce que le MN sait, après l'enregistrement initial, si il est à l'intérieur ou à l'extérieur. (Cependant, quand le nœud mobile est à l'extérieur, il se réenregistre indépendamment avec le x-HA en utilisant du texte en clair, et avec le i-HA à travers le tunnel VPN.)

Retarder l'établissement de connexion IPsec pourrait empêcher l'interruption des sessions IKE. Interrompre une session IKE peut être un problème dans certains cas parce que IKE ne fournit pas de mécanisme fiable, normalisé, et de mise en œuvre obligatoire pour terminer proprement une session.

Si le x-HA n'est pas joignable de l'intérieur (c'est-à-dire, la configuration de pare-feu est connue) une période de détection de zéro est préférée, car elle minimise les frais généraux d'établissement de connexion et ne cause pas de problème de temps. Si cette hypothèse n'était pas vérifiée et si une réponse du i-HA était reçue après une réponse du x-HA, le MN DEVRAIT se réenregistrer directement auprès du i-HA.

3.4 Extension Réseaux de confiance configurés

L'extension Réseaux de confiance configurés (TNC, *Trusted Networks Configured*) est une extension qui peut être sautée. Un i-HA qui envoie l'extension doit satisfaire les exigences décrites au paragraphe 4.3, tandis qu'un MN qui traite l'extension doit satisfaire les exigences décrites au paragraphe 4.1. Le format de l'extension est décrit ci-après. Il respecte le format court d'extension décrit dans la [RFC3344] :



Type : 149

Longueur : 2

Sous type : 0

Réservé : réglé à 0 à l'envoi, ignoré en réception.

3.5 Questions de mise en œuvre

Quand le MN utilise un algorithme parallèle de détection et un agent étranger (FA) le MN envoie deux demandes d'enregistrement à travers le même FA avec la même adresse de contrôle d'accès au support (MAC, *Media Acces Control*)

(ou équivalente) et éventuellement la même adresse de rattachement. Bien que ceci ne soit pas en conflit avec les spécifications existantes, c'est un scénario inhabituel ; donc certaines mises en œuvre de FA peuvent ne pas fonctionner correctement dans une telle situation. Cependant, des essais sur les agents étrangers déployés semblent indiquer qu'une majorité des agents étrangers disponibles maîtrisent cette situation.

Quand les adresses du x-HA et du i-HA sont la même, le scénario est encore plus difficile pour le FA, et il est presque certain que les FA existants ne traitent pas correctement cette situation. Donc, les adresses de x-HA et de i-HA DOIVENT être différentes.

Ceci étant, si le MN détecte que son i-HA et son x-HA ont la même adresse, il DOIT supposer qu'il est dans le réseau externe et sauter la détection de réseau pour éviter de troubler le FA. Parce que les adresses d'agent de rattachement sont utilisées à des couches différentes, réaliser la connexité est possible sans confusion d'adresse.

Le nœud mobile PEUT utiliser les conseils suivants pour déterminer qu'il est à l'intérieur, mais DOIT vérifier l'accessibilité du i-HA de toutes façons :
- o un nom de domaine dans un message DHCPDISCOVER / DHCPOFFER
- o un NAI dans une annonce d'agent étranger
- o une liste d'adresses MAC de passerelles par défaut qui sont connues pour résider dans le réseau interne (c'est-à-dire, configurées comme telles, ou dont il a été vérifié précédemment qu'elles sont à l'intérieur).

Par exemple, si le MN a des raisons de croire qu'il est à l'intérieur, il PEUT retarder pendant un certain temps l'envoi d'une demande d'enregistrement au x-HA. De même, si le MN a des raisons de croire qu'il est à l'extérieur, il peut commencer l'établissement de connexion IPsec immédiatement après la réception d'une réponse d'enregistrement du x-HA. Cependant, si le MN devait recevoir une réponse d'enregistrement du i-HA après que l'établissement de connexion IPsec a commencé, le MN DEVRAIT quand même passer à l'utilisation directe du i-HA.

3.6 Raison des choix de conception

3.6.1 Exigences pour la configuration de pare-feu

L'exigence que le i-HA ne puisse pas être joint à partir du réseau externe est nécessaire. Sinon, un enregistrement réussi avec le i-HA (sans IPsec) ne peut pas être utilisé comme indication sûre que le nœud mobile est à l'intérieur. Une solution possible au problème évident de sécurité serait de définir et déployer un mécanisme sûr de détection du réseau interne fondé, par exemple, sur une annonce de FA signée ou de messages DHCP signés.

Cependant, sauf si le mécanisme est défini pour les deux FA et messages DHCP et est déployé dans chaque réseau interne, il a une applicabilité limitée. En d'autres termes, le nœud mobile NE DOIT PAS supposer qu'il est dans le réseau interne sauf si il reçoit un message du FA ou DHCP signé (sans considérer si il peut ou non s'enregistrer directement avec le i-HA). Si il reçoit un message non signé du FA ou DHCP, il DOIT utiliser IPsec ; autrement, le nœud mobile peut être facilement amené à utiliser du texte en clair.

Supposer que tous les FA et serveurs DHCP dans le réseau interne sont mis à niveau pour prendre en charge une telle caractéristique ne semble pas réaliste ; il est très souhaitable d'être capable de tirer parti des déploiements existants de DHCP et de FA. Une analyse similaire semble s'appliquer sans considération de la sorte de mécanisme de sécurité supplémentaire qui est défini.

Parce qu'une erreur de configuration de pare-feu peut avoir des conséquences catastrophiques sur la sécurité des données (l'exposition silencieuse des données d'utilisateur à des attaquants externes) un mécanisme de protection séparé est fourni par le i-HA. Le i-HA doit être configuré, par l'administrateur, avec une liste de réseaux de confiance. Le i-HA annonce qu'il sait quelles adresses de source de demande d'enregistrement sont de confiance, en utilisant une extension de demande d'enregistrement (extension Réseaux de confiance configurés, paragraphe 3.4). Sans cette extension, un MN ne peut pas s'appuyer sur la réussite d'un enregistrement pour indiquer qu'il est connecté au réseau interne. Cela assure que la compromission des données d'utilisateur ne se produit que si le pare-feu et le i-HA sont tous deux incorrectement configurés. De plus, les occurrences de demandes d'enregistrement provenant d'adresses qui ne sont pas de confiance devraient être enregistrées par l'i-HA, les exposant à l'examen de l'administrateur.

3.6.2 Surveillance du réseau interne fondée sur l'enregistrement

Ce problème affecte aussi la sécurité du client IPsec. Cependant, comme les spécifications IPsec ne déclarent pas comment et quand les politiques de client IPsec sont configurées ou changées (par exemple, en réponse à un changement de la

connexité du réseau) la question sort du domaine de IPsec. Comme le présent document décrit un algorithme et les exigences pour la détection (sûre) du réseau interne, la question relève du présent document.

L'exigence actuelle de surveillance du réseau interne a été ajoutée comme mécanisme de repli.

3.6.3 Pas de chiffrement à l'intérieur

Si un chiffrement était appliqué aussi quand le MN était à l'intérieur, il n'y aurait pas de raison de sécurité pour surveiller périodiquement le réseau interne.

La principale raison pour laquelle le chiffrement ne peut pas être appliqué quand le MN est à l'intérieur a été donnée au paragraphe 1.6. En bref, les questions principales sont (1) la consommation d'énergie ; (2) la charge supplémentaire de CPU, en particulier parce que les réseaux internes sont normalement des réseaux commutés et qu'une grande quantité de données peut être transférées de façon habituelle ; (3) les appareils existants de HA n'intègrent normalement pas la fonction IPsec ; (4) le chiffrement (IPsec) exige l'authentification de l'utilisateur, qui peut être interactive dans certains cas (par exemple, SecurID) et donc pose un problème d'utilisabilité ; et (5) l'utilisateur peut avoir besoin d'accréditifs séparés pour les appareils de VPN dans la DMZ et le HA.

3.7 Améliorations

Le processus d'enregistrement peut être amélioré de nombreuses façons. Une façon simple est de faire détecter au x-HA si une demande d'enregistrement vient de l'intérieur ou de l'extérieur du réseau de l'entreprise. Si elle vient de l'intérieur du réseau de l'entreprise, le x-HA peut simplement éliminer la demande d'enregistrement.

Cette approche est faisable sans changement du protocole dans les scénarios où une entreprise possède à la fois le VPN et le x-HA. Le x-HA peut simplement déterminer sur la base de l'identifiant d'interface entrante (ou du routeur qui relaye le paquet) si la demande d'enregistrement vient ou non de l'intérieur.

Dans d'autres scénarios, des changements du protocole peuvent être nécessaires. De tels changements sortent du domaine d'application du présent document.

4. Exigences

4.1 Exigences pour le nœud mobile

Le nœud mobile DOIT mettre en œuvre un algorithme de détection du réseau interne satisfaisant les exigences mentionnées au paragraphe 3.2. Un nouveau paramètre configurable de MN, T_MONITOR, est requis. La valeur de ce paramètre reflète un équilibre entre sécurité et quantité de frais généraux de signalisation, et donc doit être configurable. De plus, quand il fait la détection du réseau interne, le MN NE DOIT PAS désactiver la protection IPsec sauf si la réponse d'enregistrement du i-HA contient une extension Réseaux de confiance configurés (paragraphe 3.4).

Le nœud mobile DOIT prendre en charge les modes d'accès c, f, cvc, fvc (Section 2).

Le nœud mobile DEVRAIT prendre en charge la traversée de NAT IPv4 mobile [RFC3519] pour IP mobile interne et externe.

Le nœud mobile DEVRAIT prendre en charge la traversée de NAT IPsec [RFC3947], [RFC3948].

Quand le nœud mobile a un accès direct au i-HA, il DEVRAIT utiliser seulement la couche IPv4 mobile interne pour minimiser l'impact du pare-feu et du VPN.

Quand le nœud mobile est à l'extérieur et utilise la connexion de VPN, les politiques IPsec DOIVENT être configurées à chiffrer tout le trafic envoyé de et vers le réseau d'entreprise. Les entrées particulières de base de données de politique (SPD, *Security Policy Database*) dépendent du type et de la configuration du VPN particulier (par exemple, IPsec complet ou L2TP/IPsec, tunnelage complet ou tunnelage partagé).

4.2 Exigences pour l'appareil de VPN

La politique de sécurité du VPN DOIT permettre la communication en utilisant UDP aux agents de rattachement internes, avec l'accès d'agent de rattachement 434 et tout accès distant. La politique de sécurité DEVRAIT permettre IP-IP aux agents de rattachement internes en plus de l'accès UDP 434.

L'appareil de VPN DEVRAIT mettre en œuvre le mécanisme de traversée de NAT IPsec décrit dans les [RFC3947] et [RFC3948].

4.3 Exigences pour l'agent de rattachement

L'agent de rattachement DEVRAIT mettre en œuvre le mécanisme de traversée de NAT IPv4 mobile décrit dans la [RFC3519]. (Cela se réfère aussi au i-HA : la traversée de NAT est exigée pour la prise en charge des VPN auxquels le tunnel de VPN de NAT adresse ou bloque du trafic IP-IP.)

Pour protéger la confidentialité des données d'utilisateur contre les erreurs de configuration du pare-feu, le i-HA :
- o DOIT être configuré avec une liste des sous réseaux IP de confiance (contenant seulement des adresses du réseau interne) sans sous réseau de confiance par défaut.
- o DOIT rejeter (éliminer en silence) toute demande d'enregistrement venant d'une adresse de source qui n'est pas dans un des sous réseaux de confiance configurés. Ces demandes d'enregistrement éliminées DEVRAIENT être enregistrées.
- o DOIT inclure une extension Réseaux de confiance configurés (paragraphe 3.4) dans une réponse d'enregistrement envoyée en réponse à une demande d'enregistrement venant d'une adresse de confiance.

5. Analyse

Cette Section fournit une comparaison avec les lignes directrices décrites à la Section 6 de la déclaration de problème [RFC4093] et une analyse supplémentaire des frais généraux par paquet avec et sans les mécanismes facultatifs.

5.1 Comparaison aux lignes directrices

Préservation de l'infrastructure de VPN existante :
- o La solution n'oblige à aucun changement de l'infrastructure de VPN existante, autre que d'éventuels changements de configuration pour éviter un filtrage à états pleins du trafic.

Mise à niveau de logiciel aux clients et passerelles de VPN existants :
- o La solution décrite n'oblige à aucun changement des passerelles de VPN ou des agents étrangers IPv4 mobile.

Protocole IPsec :
- o La solution n'exige aucun changement des protocoles IPsec ou d'échange de clé standard existants, et n'exige pas la mise en œuvre de nouveaux protocoles dans l'appareil de VPN.

Interopérabilité multi-fabricants :
- o La solution fournit une interopérabilité multi fabricants facile entre les composants de serveur (appareil de VPN, agents étrangers, et agents de rattachement). Bien sûr, ces composants n'ont pas besoin de se connaître les uns les autres.
- o La pile de réseautage de nœud mobile est un peu complexe à mettre en œuvre, ce qui peut être un problème pour l'interopérabilité multi fabricants. Cependant, c'est un problème de pure architecture de logiciel, et il n'y a pas de limitation de protocole connue pour l'interopérabilité multi fabricants.

Protocole MIPv4 :
- o La solution respecte le protocole MIPv4, mais exige que la nouvelle extension Réseaux de confiance configurés améliore la fiabilité de la détection du réseau interne.
- o La solution exige l'utilisation de deux couches MIPv4 parallèles.

Frais généraux de transfert :
- o La solution fournit un mécanisme pour éviter la renégociation de SA de tunnel de VPN sur un mouvement en utilisant la couche MIPv4 externe.

Adaptabilité, disponibilité, fiabilité, et performances :

- La complexité de la solution est linéaire avec le nombre de MN enregistrés et accédants aux ressources à l'intérieur de l'intranet.
- Des frais généraux supplémentaires sont imposés par la solution.

Entités fonctionnelles :
- La solution n'impose aucun nouveau type d'entité fonctionnelle ni de changement aux entités existantes. Cependant, un appareil de HA externe est requis.

Implications des passerelles de NAT intervenantes :
- La solution renforce les solutions de traversée de NAT MIPv4 [RFC3519] et de traversée de NAT IPsec [RFC3947] [RFC3948] existantes et n'exige aucune nouvelle fonctionnalité pour traiter avec les NAT.

Implications de sécurité :
- La solution exige un nouveau mécanisme pour détecter si le nœud mobile est dans le réseau interne ou externe. La sécurité de ce mécanisme est critique pour s'assurer que le niveau de sécurité fourni par IPsec n'est pas compromis par un mécanisme fautif de détection.
- Quand le nœud mobile est à l'extérieur, la couche externe IPv4 mobile peut permettre des attaques de redirection du trafic que IPsec complet ne permet pas. À part cela, la sécurité IPsec est inchangée.
- Plus de considérations sur la sécurité sont décrites à la Section 6.

5.2 Frais généraux de paquet

Le maximum des frais généraux de paquet dépend du mode d'accès comme suit :
- f : 0 octets
- c : 20 octets
- fvc : 77 octets
- cvc : 97 octets

Le maximum de frais généraux de 97 octets dans le mode d'accès 'cvc' consiste en :
- IP-IP pour i-MIPv4 : 20 octets
- IPsec ESP : 57 octets au total, consistant en 20 (nouvel en-tête IP) 4+4+8 = 16 (SPI, numéro de séquence, valeur d'initialisation de chiffrement) 7+2 = 9 (bourrage, champ Longueur de bourrage, prochain champ d'en-tête) 12 (en-queue d'authentification ESP)
- IP-IP pour x-MIPv4 : 20 octets

Quand IPsec est utilisé, une quantité variable de bourrage est présente dans chaque paquet ESP. Les données ont été calculées pour une taille de bloc de chiffrement de 64 bits, des frais généraux de bourrage de 9 octets (prochain champ d'en-tête, champ Longueur de bourrage, et 7 octets de bourrage ; voir le paragraphe 2.4 de la [RFC4303]) et le champ Authentification ESP de 12 octets (HMAC-SHA1-96 ou HMAC-MD5-96). Noter qu'une mise en œuvre de IPsec PEUT bourrer avec plus que la quantité minimum d'octets.

Les frais généraux de la traversée de NAT ne sont pas inclus, et ajoutent 8 octets quand la traversée de NAT IPsec [RFC3947] [RFC3948] est utilisée et 12 octets quand la traversée de NAT MIP [RFC3519] est utilisée. Par exemple, quand on utilise le mode d'accès cvc, les frais généraux maximum de la traversée de NAT sont de 12+8+12 = 32 octets. Donc, le plus mauvais cas de scénario (avec les hypothèses ESP susmentionnées) est de 129 octets pour cvc.

5.3 Considérations de latence

Quand le MN est à l'intérieur, la latence d'établissement de connexion n'augmente pas comparée au MIPv4 standard si le MN met en œuvre la séquence d'enregistrement parallèle suggérée (voir le paragraphe 3.3). L'échange de messages RRQ/RRP avec le i-HA confirme que le MN est à l'intérieur, et le MN peut commencer à envoyer et recevoir immédiatement le trafic d'utilisateur. Pour la même raison, les transferts dans le réseau interne n'ont pas de frais généraux par rapport au MIPv4 standard.

Quand le MN est à l'extérieur, la situation est légèrement différente. La latence de l'établissement initial de connexion consiste essentiellement en (1) l'enregistrement auprès du x-HA, (2) le délai facultatif de détection (attente de la réponse de i-HA) (3) l'établissement de connexion IPsec (IKE) et (4) l'enregistrement auprès de i-HA. Tous sauf (4) sont en plus du MIPv4 standard.

Cependant, les transferts dans le réseau externe ont des performances comparables au MIPv4 standard. Le MN se réenregistre simplement auprès du x-HA et commence à envoyer du trafic IPsec à la passerelle de VPN à partir de la nouvelle adresse.

Le MN peut minimiser la latence en (1) n'attendant pas une réponse du i-HA avant de déclencher IKE si l'enregistrement auprès de x-HA réussit et (2) envoyant d'abord la RRQ qui a le plus de chances de réussir (par exemple, si le MN est très probablement en dehors). Cela peut être fait sur la base d'une heuristique sur le réseau, par exemple, des adresses, l'adresse MAC de la passerelle par défaut (dont le nœud mobile peut se souvenir d'un accès précédent) ; sur la base du réseau d'accès précédent (c'est-à-dire, optimiser pour un mouvement intérieur-intérieur et extérieur-extérieur) ; etc.

5.4 Considérations d'état de pare-feu

Un appareil de pare-feu séparé ou un pare-feu intégré dans la passerelle de VPN effectue normalement une inspection à états pleins du trafic d'utilisateur. Le pare-feu peut, par exemple, tracer l'état de la session TCP et bloquer les segments TCP sans rapport avec les connexions ouvertes. D'autres mécanismes d'inspection à état pleins existent aussi.

L'état du pare-feu pose un problème quand le nœud mobile se déplace entre les réseaux interne et externe. Le nœud mobile peut, par exemple, initier une connexion TCP quand il est à l'intérieur, et plus tard sortir tout en s'attendant à garder la connexion active. Du point de vue du pare-feu, la connexion TCP n'a pas été initiée, car il n'a pas été témoin de paquets d'établissement de connexion TCP, résultant donc potentiellement en problèmes de connexité.

Quand la VPN-TIA est enregistrée comme adresse d'entretien co-localisée auprès du i-HA, tout le trafic du nœud mobile apparaît comme IP-IP au pare-feu.

Normalement, les pare-feu ne continuent pas l'inspection au delà du tunnel IP-IP, mais la prise en charge d'une inspection plus approfondie est disponible dans de nombreux produits. En particulier, un administrateur peut configurer des politiques de trafic dans de nombreux produits de pare-feu même pour du trafic IP-IP encapsulé. Si cela est fait, des problèmes similaires d'état plein peuvent survenir.

En résumé, le pare-feu doit permettre que le trafic venant de et allant à la connexion IPsec soit acheminé, même si il peut n'avoir pas réussi à tracer l'état de connexion. Comment cela est fait sort du domaine d'application de ce document.

5.5 Systèmes de détection d'intrusion

De nombreux pare-feu incorporent des systèmes de détection d'intrusion (IDS, *Intrusion Detection System*) qui surveillent le trafic du réseau à la recherche de schémas inhabituels et de clairs signes d'attaque. Comme le trafic provenant d'un nœud mobile qui met en œuvre la présente spécification est d'UDP au i-HA à l'accès 434, et éventuellement du trafic IP-IP à l'adresse du i-HA, les IDS existants peuvent traiter le trafic différemment du trafic d'accès distant de VPN ordinaire. Comme les pare-feu, les IDS ne sont pas normalisés, donc il est impossible de garantir l'interopérabilité avec un système d'IDS particulier.

5.6 Mise en œuvre du nœud mobile

La mise en œuvre du nœud mobile exige l'utilisation de trois couches de tunnelage, qui peuvent être utilisées dans diverses configurations selon que cette interface particulière est à l'intérieur ou à l'extérieur. Noter qu'il est possible qu'une interface soit à l'intérieur et qu'une autre interface soit à l'extérieur, ce qui exige une mise en couches différente pour chaque interface au même moment.

Pour une mise en œuvre multi fabricants, les couches IPsec et MIPv4 doivent interopérer dans le même nœud mobile. Cela implique qu'un cadre souple est exigé pour la mise en couches du protocole (ou des API spécifiques du protocole).

5.7 Protocoles de VPN non IPsec

La solution fonctionne aussi pour les protocoles de tunnelage de VPN qui ne sont pas fondés sur IPsec, pourvu que le nœud mobile ait la connexité IPv4 avec une adresse convenable pour l'enregistrement. Cependant, de tels protocoles de VPN ne sont pas explicitement considérés.

6. Considérations pour la sécurité

6.1 Détection du réseau interne

Si le nœud mobile croit par erreur qu'il est dans le réseau interne et envoie des paquets en clair, il compromet la sécurité IPsec. Pour cette raison, la sécurité globale (confidentialité et intégrité) des données d'utilisateur est le minimum de (1) la sécurité IPsec et (2) la sécurité du mécanisme de détection du réseau interne.

La sécurité de la détection du réseau interne s'appuie sur la réussite de l'enregistrement avec le i-HA. Pour IPv4 mobile standard [RFC3344], cela signifie HMAC-MD5 et la protection de IPv4 mobile contre la répétition. La solution suppose aussi que le i-HA n'est pas directement accessible du réseau externe, exigeant une configuration soigneuse du pare-feu d'entreprise. Pour minimiser l'impact d'un problème de configuration de pare-feu, le i-HA est de son côté obligé d'être configuré avec des adresses de source de confiance (c'est-à-dire, des adresses appartenant au réseau interne) et d'inclure une indication de cela dans une nouvelle extension Réseaux de confiance configurés. Il est exigé du MN qu'il ne fasse pas confiance à un enregistrement comme l'indication qu'il est connecté au réseau interne, sauf si cette extension est présente dans la réponse à l'enregistrement. Donc, pour réellement compromettre la confidentialité des données d'utilisateur, le pare-feu d'entreprise et le i-HA doivent tous deux être mal configurés, ce qui réduit la probabilité du scénario.

Quand le nœud mobile envoie une demande d'enregistrement au i-HA à partir d'un réseau qui n'est pas de confiance et qui ne passe pas par le tunnel IPsec, il va révéler l'adresse de l'i-HA, sa propre identité incluant le NAI et l'adresse de rattachement, et la valeur de l'authentifiant dans les extensions d'authentification au réseau qui n'est pas de confiance. Cela peut poser un problème dans certains déploiements.

Quand l'état de connexion d'une interface change, une interface précédemment connectée au réseau interne de confiance peut soudainement être connectée à un réseau qui n'est pas de confiance. Bien que le même problème soit aussi pertinent pour les mises en œuvre de VPN fondées sur IPsec, le problème est particulièrement pertinent dans le cadre de cette spécification.

Dans la plupart des cas, les mises en œuvre de nœud mobile sont supposées avoir des informations de couche 2 disponibles, rendant la détection du changement de connexion à la fois rapide et robuste. Pour couvrir les cas où de telles informations ne sont pas disponibles (ou échouent pour une raison quelconque) le nœud mobile est obligé de se réenregistrer périodiquement auprès de l'agent de rattachement interne pour vérifier qu'il est toujours connecté au réseau de confiance. Il est aussi exigé que cet intervalle de réenregistrement soit configurable, donnant donc à l'administrateur un paramètre permettant de contrôler l'exposition potentielle.

6.2 IPv4 mobile contre IPsec

MIPv4 et IPsec ont des buts et approches différents pour fournir des services de sécurité. MIPv4 utilise normalement un secret partagé pour l'authentification du trafic de signalisation, tandis que IPsec utilise normalement IKE (un échange Diffie-Hellman authentifié) pour établir les clés de session. Donc, les propriétés de sécurité globales d'un système combiné MIPv4 et IPsec dépendent des deux mécanismes.

Dans la solution proposée par ce document, la couche MIPv4 externe fournit la mobilité pour le trafic IPsec. Si la sécurité de MIPv4 est rompue dans ce contexte, des attaques de redirection de trafic contre le trafic IPsec sont possibles. Cependant, de telles attaques d'acheminement n'affectent pas les autres propriétés d'IPsec (protection de la confidentialité, de l'intégrité, et de la répétition, etc.) parce que IPsec ne considère pas le réseau entre deux points d'extrémité IPsec comme étant sûr.

Parce que les secrets partagés MIPv4 sont généralement configurés manuellement, ils peuvent être faibles si des secrets facilement mémorisables sont choisis, ouvrant donc la porte aux attaques de redirection décrites plus haut. Noter en particulier qu'un secret faible dans le i-HA est fatal pour la sécurité, car le nœud mobile peut être conduit à abandonner le chiffrement si le secret du i-HA est découvert.

En supposant que les secrets partagés de MIPv4 ont une entropie suffisante, il y a encore au moins les différences et similarités suivantes entre MIPv4 et IPsec qu'il faut examiner :

- IPsec et MIPv4 sont tous deux susceptibles de l'attaque du "pseudo NAT transitoire" décrite dans [pseudonat] et la [RFC3519] en supposant que la traversée de NAT est activée (ce qui est normalement le cas). Les attaques de "pseudo NAT" permettent à un attaquant de rediriger les flux de trafic, résultant en la consommation de ressources, l'absence de connexité, et déni de service. Cependant, ces attaques ne peuvent pas compromettre la confidentialité des données d'utilisateur protégées en utilisant IPsec.

- Quand on considère une attaque de "pseudo NAT" contre IPsec standard et MIP standard (avec traversée de NAT) les attaques de redirection contre MIP peuvent être plus faciles parce que :
  * les réenregistrements MIPv4 se produisent normalement plus fréquemment que les établissement de SA IPsec (bien que cela puisse n'être pas le cas pour les hôtes mobiles) ;
  * il suffit de capturer et modifier une seule demande d'enregistrement, tandis que attaquer IKE exige que plusieurs paquets IKE soient capturés et modifiés.

- Il peut y avoir des soucis sur le mélange d'algorithmes. Par exemple, IPsec peut utiliser HMAC-SHA1-96, tandis que MIP utilise toujours HMAC-MD5 (RFC 3344) ou préfixe+suffixe MD5 (RFC 2002). De plus, alors que les algorithmes IPsec sont normalement configurables, les clients MIPv4 utilisent normalement seulement HMAC-MD5 ou préfixe+suffixe MD5. Bien que cela ne soit probablement pas un problème de sécurité en soi, il est plus difficile de communiquer avec les utilisateurs.

- Quand IPsec est utilisé avec une infrastructure de clé publique (PKI, *Public Key Infrastructure*) les propriétés de gestion de clé sont supérieures à celles du MIPv4 de base. Donc, ajouter MIPv4 au système rend la gestion de clé plus complexe.

- En général, l'ajout de nouveaux mécanismes de sécurité augmente la complexité globale et rend le système plus difficile à comprendre.

7. Considérations relatives à l'IANA

Le présent document spécifie une nouvelle extension sautable (en format court) au paragraphe 3.4, dont les valeurs de type et sous type ont été allouées.

L'allocation de valeurs de nouveaux sous types peut être faite via revue d'expert et spécification exigée [RFC5226].

8. Remerciements

Le présent document est un travail conjoint des auteurs contributeurs (par ordre alphabétique) : Farid Adrangi (Intel Corporation) Nitsan Baider (Check Point Software Technologies, Inc.) Gopal Dommety (Cisco Systems) Eli Gelasco (Cisco Systems) Dorothy Gellert (Nokia Corporation) Espen Klovning (Birdstep) Milind Kulkarni (Cisco Systems) Henrik Levkowetz (ipUnplugged AB) Frode Nielsen (Birdstep) Sami Vaarala (Codebay) Qiang Zhang (Liqwid Networks, Inc.).

Les auteurs tiennent à remercier l'équipe de conception MIP/VPN, en particulier Mike Andrews, Gaetan Feige, Prakash Iyer, Brijesh Kumar, Joe Lau, Kent Leung, Gabriel Montenegro, Ranjit Narjala, Antti Nuopponen, Alan O'Neill, Alpesh Patel, Ilkka Pietikainen, Phil Roberts, Hans Sjostrand, et Serge Tessier de leurs retours continus et de leur aide pour améliorer ce document. Des remerciements particuliers à Radia Perlman pour sa relecture attentive des questions de sécurité. Tom Hiller a soulevé des problèmes avec les appareils alimentés par batterie. Nous tenons aussi à remercier les précédents présidents du groupe de travail IP Mobile (Gabriel Montenegro, Basavaraj Patil, et Phil Roberts) pour leurs importants retours et leurs conseils.

9. Références

9.1 Références normatives

[RFC1918] Y. Rekhter et autres, "Allocation d'adresse pour les internets privés", BCP 5, février 1996.

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. *(MàJ par* RFC8174)

[RFC3344] C. Perkins, éd., "Prise en charge de la mobilité IP pour IPv4", août 2002. (*Obsolète, voir* RFC5944) *(P.S.)*

[RFC3519] H. Levkowetz, S. Vaarala, "Traversée des appareils de traduction d'adresse réseau (NAT) par IP mobile", avril 2003. *(P.S.)*

[RFC3947] T. Kivinen et autres, "Négociation de traversée de NAT dans IKE", janvier 2005. *(P.S.)*

[RFC3948] A. Huttunen et autres, "Encapsulation UDP de paquets ESP d'IPsec", janvier 2005. *(P.S.)*

[RFC4301] S. Kent et K. Seo, "Architecture de sécurité pour le protocole Internet", décembre 2005. *(P.S.) (Remplace la* RFC2401)

[RFC4303] S. Kent, "Encapsulation de charge utile de sécurité dans IP (ESP)", décembre 2005. (*Remplace* RFC2406) *(P.S.)*

[RFC5226] T. Narten et H. Alvestrand, "Lignes directrices pour la rédaction d'une section Considérations relatives à l'IANA dans les RFC", BCP 26, mai 2008. (*Remplace* RFC2434 *; remplacée par* RFC8126)

9.2 Références pour information

[pseudonat] F. Dupont, et J. Bernard, "Attaques de pseudo-NAT transitoires ou comment les NAT sont encore plus dangereux qu'on ne le croit", Travail en cours, juin 2004.

[RFC2002] C. Perkins, éd., "Prise en charge de la mobilité sur IP", octobre 1996. (*Obsolète, voir* RFC5944) *(P.S.)*

[RFC3456] B. Patel et autres, "Protocole de configuration dynamique des hôtes (DHCPv4) Configuration du mode tunnel IPsec", janvier 2003. *(P.S.)*

[RFC3776] J. Arkko, V. Devarapalli, F. Dupont, "Utilisation de IPsec pour la protection de la signalisation IPv6 mobile entre nœuds mobiles et agents nominaux", juin 2004. (*MàJ par* RFC4877) *(P.S.)*

[RFC4093] F. Adrangi et autres, "Déclaration de problème : Traversée en IPv4 Mobile de passerelles de réseau privé virtuel (VPN)", août 2005. *(Information)*

[RFC4282] B. Aboba et autres, "L'identifiant d'accès réseau", décembre 2005. *(P.S., Remplacée par* RFC7542)

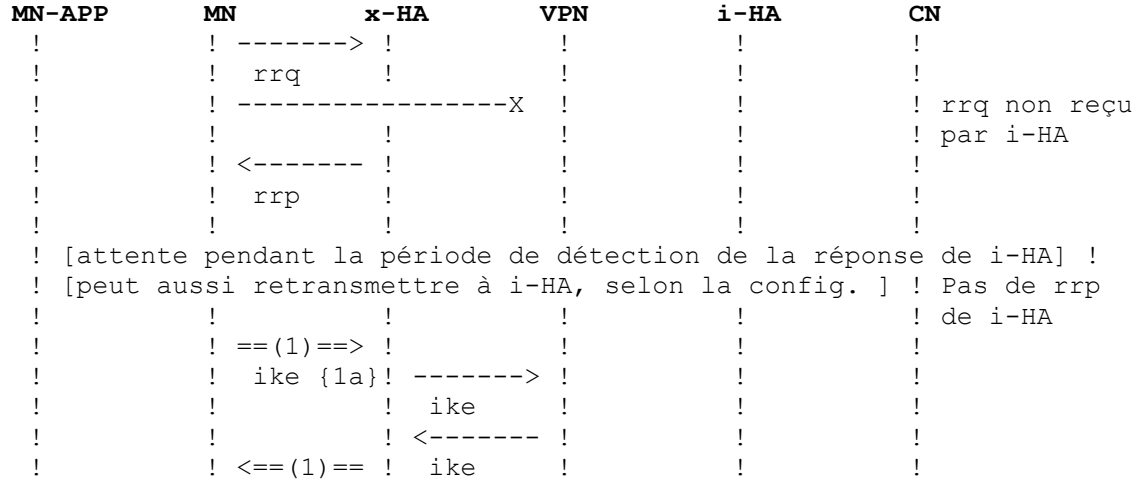
[RFC4555] P. Eronen, "Protocole IKEv2 de mobilité et de rattachement multiple (MOBIKE)", juin 2006. *(P.S.)*

[tessier] Tessier, S., "Guidelines for Mobile IP and IPsec VPN Usage", Travail en cours, décembre 2002.

Appendice A. Exemples de flux de paquets

A.1 Établissement de connexion pour le mode d'accès 'cvc'

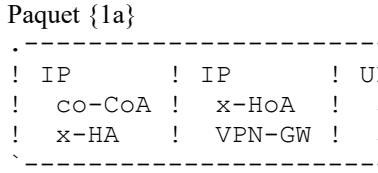
La figure suivante illustre l'établissement de connexion quand le nœud mobile est sorti et utilise une adresse d'entretien co-localisée. L'établissement de connexion IKE n'est pas montré en entier, et implique plusieurs allers-retours (4,5 allers-retours quand on utilise le mode principal suivi par le mode rapide).



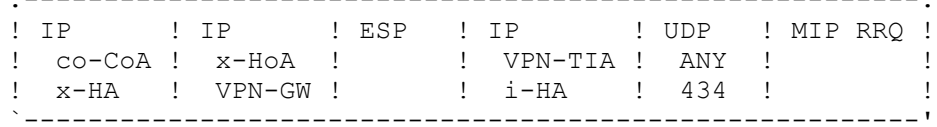
La notation "==(N)==>" ou "<==(N)==" indique que le paquet le plus interne a été encapsulé N fois, en utilisant IP-IP, ESP, ou la traversée de NAT MIP.

Les paquets marqués avec {xx} sont montrés plus en détails ci-dessous. Chaque zone représente un en-tête de protocole (étiqueté). Les adresses ou accès de source et destination sont montrés en dessous du nom du protocole quand c'est applicable. Noter qu'il n'y a pas d'en-tête de traversée de NAT dans les exemples de paquets.

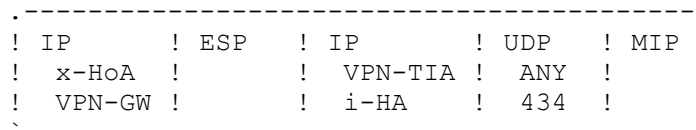
Paquet {1a}



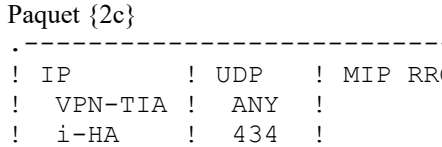
Paquet {2a}



Paquet {2b}



Paquet {2c}



```
`---------------------------'
```

Paquet {3a}

```
.----------------------.
! IP     ! Protocole   !
!  i-HoA ! utilisateur !
!  CN    !             !
`----------------------'
```

Paquet {3b}

```
.-------------------------------------------------------------------------
! IP      ! IP      ! ESP ! IP       ! IP     ! Protocole   ! en-queue !
!  co-CoA !  x-HoA  !     !  VPN-TIA !  i-HoA ! utilisateur ! ESP      !
!  x-HA   !  VPN-GW !     !  i-HA    !  CN    !             !          !
`-------------------------------------------------------------------------
```

Paquet {3c}

```
.-------------------------------------------------------------.
! IP      ! ESP ! IP       ! IP     ! Protocole   ! en-queue !
!  x-HoA  !     !  VPN-TIA !  i-HoA ! utilisateur ! ESP      !
!  VPN-GW !     !  i-HA    !  CN    !             !          !
`-------------------------------------------------------------'
```

Paquet {3d}

```
.---------------------------------.
! IP       ! IP     ! Protocole   !
!  VPN-TIA !  i-HoA ! utilisateur !
!  i-HA    !  CN    !             !
`---------------------------------'
```

Paquet {3e}

```
.----------------------.
! IP     ! Protocole   !
!  i-HoA ! utilisateur !
!  CN    !             !
`----------------------'
```

Le paquet {3b} avec tous les en-têtes de traversée de NAT (x-MIP, ESP, et i-MIP) est montré ci-dessous pour comparaison.

Paquet {3b} (avec en-têtes de traversée de NAT)

```
.------------------------------------------------ -
! IP      ! UDP  ! Données! IP      ! UDP   ! ESP.. \
!  co-CoA !  ANY ! tunnel !  x-HoA  !  4500 !       /
!  x-HA   !  434 ! MIP    !  VPN-GW !  4500 !       \
`------------------------------------------------ -
<==== MIPv4 externe =====> <=== IPsec ESP ======== = =

- - ------------------------------------------------------ -
\..ESP ! IP       ! UDP  ! Données! IP     ! Protocole    \
/      !  VPN-TIA !  ANY ! tunnel !  i-HoA ! utilisateur../
\      !  i-HA    !  434 ! MIP    !  CN    !              \
- - ------------------------------------------------------ -
= = ==> <===== MIPv4 interne ====> <== paquet d'utilisateur == =

- ------------------------.
\..Protocole   ! en-queue !
/  utilisateur ! ESP      !
\              !          !
- ------------------------'
= ============> <= ESP =>
```

Adresse des auteurs

Espen Klovning
Birdstep
Bryggegata 7
Oslo 0250
NORWAY
téléphone : +47 95 20 26 29
mél : espen@birdstep.com

Sami Vaarala
Codebay
P.O. Box 63
Espoo 02601
Finland
téléphone : +358 (0)50 5733 862
mél : sami.vaarala@iki.fi

Déclaration complète de droits de reproduction

Propriété intellectuelle