Groupe de travail Réseau
Request for Comments : 4877
RFC mise à jour : 3776
Catégorie : Sur la voie de la normalisation

V. Devarapalli, Azaire Networks
F. Dupont, CELAR
avril 2007
Traduction Claude Brière de L'Isle

Fonctionnement de IPv6 mobile avec IKEv2 et l'architecture IPsec révisée

Résumé
Le présent document décrit le fonctionnement de IPv6 mobile avec l'architecture IPsec révisée et IKEv2.

Table des matières

1. Introduction

La RFC 3776 décrit comment IPsec, décrit dans la [RFC2401], est utilisé avec IPv6 mobile [RFC3775] pour protéger les messages de signalisation. Elle illustre aussi des exemples d'entrées de base de données de politique de sécurité et de base de données d'association de sécurité qui peuvent être utilisées pour protéger les messages de signalisation IPv6 mobile.

L'architecture IPsec a été révisée dans la [RFC4301]. Parmi de nombreux changements, la liste des sélecteurs a été étendue pour inclure le type de message En-tête de mobilité. Cela a un impact sur la façon dont les politiques de sécurité et les associations de sécurité sont configurées pour protéger les messages En-tête de mobilité. Il devient plus facile de différencier entre les divers messages En-tête de mobilité sur la base de la valeur de type au lieu de vérifier si un message En-tête de mobilité particulier est envoyé sur une interface de tunnel entre le nœud mobile et l'agent de rattachement, comme c'était le cas dans la RFC 3776. La spécification révisée de l'architecture IPsec inclut aussi le type et le code de message ICMP comme sélecteurs. Cela rend possible de protéger les messages de découverte de préfixe mobile sans appliquer la même association de sécurité à tous les messages ICMPv6.

Le présent document discute la nouvelle exigence pour l'agent de rattachement et le nœud mobile d'utiliser l'architecture IPsec révisée et IKEv2. La Section 4 fait la liste des exigences. Les Sections 6 et 7 décrivent les entrées exigées de base de données de politique de sécurité (SPD, *Security Policy Database*) et de base de données d'association de sécurité (SAD, *Security Association Database*).

Le protocole d'échange de clé Internet (IKE, *Internet Key Exchange*) a aussi été substantiellement révisé et simplifié [RFC4306]. Le paragraphe 7.3 de ce document décrit comment IKEv2 peut être utilisé pour établir des associations de sécurité pour IPv6 mobile.

L'utilisation de EAP dans IKEv2 est permise pour authentifier le nœud mobile auprès de l'agent de rattachement. Ceci est décrit dans la Section 8. Une méthode pour la configuration dynamique d'une adresse de rattachement provenant de l'agent de rattachement en utilisant la charge utile de configuration dans IKEv2 est décrite à la Section 9.

2. Terminologie

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

3. Formats de paquet

Le nœud mobile et l'agent de rattachement DOIVENT prendre en charge les formats de paquet définis à la Section 3 de la RFC 3776.

Dans le cas où le nœud mobile tunnelle à l'envers tout le trafic y compris les messages de signalisation IPv6 mobile échangés entre le nœud mobile et l'agent de rattachement, il n'est pas exigé que l'option Adresse de rattachement soit présente dans les messages envoyés à l'agent de rattachement. Le format de paquet pour la mise à jour de lien quand il est envoyé en mode tunnel est comme suit :

En-tête IPv6 (source = adresse d'entretien, destination = agent de rattachement)
En-tête ESP en mode tunnel
En-tête IPv6 (source = adresse d'entretien, destination = agent de rattachement)
En-tête de mobilité
Mise à jour de lien
Option adresse d'entretien de remplacement)

L'accusé de réception de lien envoyé au nœud mobile quand il est hors de la liaison de rattachement ressemble à .

En-tête (source = agent de rattachement, destination = adresse d'entretien)
En-tête ESP en mode tunnel
En-tête (source = agent de rattachement, destination = adresse de rattachement)
En-tête de mobilité
Accusé de réception de lien

Les formats de paquet pour les messages de découverte de préfixe mobile tunnelés sont trés similaires à la mise à jour de lien et l'accusé de réception de lien tunnelés avec l'adresse de rattachement comme adresse de source dans l'en-tête IP interne.

La prise en charge du format de paquet tunnelé ci-dessus est facultative pour le nœud mobile et l'agent de rattachement.

4. Exigences

Cette Section décrit les règles et exigences obligatoires pour tous les nœuds mobiles et agents de rattachement IPv6 mobile afin que IPsec, avec IKEv2 comme protocole de gestion de clés, puisse être utilisé pour protéger le trafic entre le nœud mobile et l'agent de rattachement. Beaucoup des exigences sont répétées de la RFC 3776 pour rendre le présent document autonome et complet.

4.1 Exigences générales

- La RFC 3775 déclare que la configuration manuelle des associations de sécurité IPsec DOIT être prise en charge, et que la gestion automatisée des clés PEUT être prise en charge. Le présent document ne fait aucune recommandation concernant la prise en charge de la configuration manuelle de IPsec et la configuration dynamique de IPsec. Le présent document décrit juste l'utilisation des associations de sécurité IPsec créées manuellement et l'utilisation de IKEv2 comme protocole IPsec de gestion de clés automatisée pour protéger les messages de signalisation IPv6 mobile.

- L'encapsulation ESP pour les mises à jour de lien et accusés de réception de lien DOIT être prise en charge et utilisée.

- L'encapsulation ESP en mode tunnel pour les messages Initiation d'essai de rattachement (HoTi, *Home Test Init*) et Essai de rattachement (HoT, *Home Test*) tunnelés entre le nœud mobile et l'agent de rattachement DOIT être prise en charge et DEVRAIT être utilisée.

- L'encapsulation ESP des messages ICMPv6 relatifs à la découverte de préfixe mobile DOIT être prise en charge et DEVRAIT être utilisée.

- L'encapsulation ESP des paquets de charge utile tunnelés entre le nœud mobile et l'agent de rattachement PEUT être prise en charge et utilisée.

- Si des protocoles de contrôle des membres de groupe de diffusion groupée ou des protocoles d'autoconfiguration d'adresse à états pleins sont pris en charge, la protection des données de charge utile DOIT être prise en charge pour ces protocoles.

- L'agent de rattachement et le nœud mobile PEUVENT prendre en charge l'authentification en utilisant EAP dans IKEv2 comme décrit à la Section 8.

- L'agent de rattachement et le nœud mobile PEUVENT prendre en charge la configuration à distance de l'adresse de rattachement comme décrit à la Section 9. Quand l'agent de rattachement reçoit une charge utile de configuration avec une CFG_REQUEST pour INTERNAL_IP6_ADDRESS, il doit répondre avec une adresse de rattachement valide pour le nœud mobile. L'agent de rattachement peut prendre une adresse de rattachement dans une base de données locale ou dans un serveur DHCPv6 sur la liaison de rattachement.

4.2 Exigences de politique

Les exigences suivantes sont relatives à la configuration de la base de données de politique de sécurité sur l'agent de rattachement et le nœud mobile.

- La RFC 3776 exigeait une configuration des politiques de sécurité par interface afin d'être capable de différencier entre les messages En-tête de mobilité envoyés à l'agent de rattachement et ceux tunnelés à travers l'agent de rattachement au nœud correspondant. Comme le type de message En-tête de mobilité est un sélecteur, il est maintenant facile de différencier entre messages HoTi et HoT et les autres messages En-tête de mobilité. Donc la configuration par interface des politiques de sécurité n'est pas requise pour protéger les messages En-tête de mobilité. Noter que sans des politiques de sécurité par interface, la protection des paquets de charge utile est limitée aux paquets originaires de, ou se terminant à, l'adresse de rattachement. Le trafic qui utilise une adresse de liaison locale dans le tunnel IP mobile ne peut pas être protégé par IPsec sans des politiques de sécurité par interface.

- L'agent de rattachement DOIT être capable d'empêcher un nœud mobile d'utiliser son association de sécurité pour

envoyer une mise à jour de lien au nom d'un autre nœud mobile. Avec la configuration IPsec manuelle, l'agent de rattachement DOIT être capable de vérifier qu'une association de sécurité a été créée pour une adresse de rattachement particulière. Avec le changement dynamique de clés, l'agent de rattachement DOIT être capable de vérifier que l'identité présentée dans l'échange IKE_AUTH a la permission de créer des associations de sécurité pour une adresse de rattachement particulière.

- L'agent de rattachement utilise la base de données d'autorisation des homologues (PAD, *Peer Authorization Database*) [RFC4301] pour mémoriser l'état par nœud mobile. Plus précisément, l'état par nœud mobile mémorise les informations qui sont utilisées pour authentifier le nœud mobile et les informations d'autorisation qui lient l'identité du nœud mobile à l'adresse de rattachement du nœud mobile. Cela va permettre à l'agent de rattachement d'empêcher un nœud mobile de créer des associations de sécurité IPsec pour l'adresse de rattachement d'un autre nœud mobile. En cas d'allocation dynamique d'adresse de rattachement, l'agent de rattachement crée une entrée temporaire de PAD liant l'identité de l'homologue authentifié et la nouvelle adresse de rattachement allouée.

- Comme exigé dans la spécification de base [RFC3775], quand un paquet destiné au nœud receveur est confronté à la politique de sécurité IPsec ou aux sélecteurs d'une association de sécurité, une adresse qui apparaît dans une option d'adresse de destination de rattachement est considérée comme l'adresse de source du paquet.

Noter que l'option Adresse de rattachement apparaît avant les en-têtes IPsec. Le paragraphe 11.3.2 de la spécification de base décrit une approche possible de mise en œuvre pour cela : les opérations de politique d'IPsec peuvent être effectuées au moment où le paquet n'a pas encore été modifié par les règles de IPv6 mobile, ou a été ramené à sa forme normale après le traitement IPv6 mobile. C'est-à-dire, le traitement de l'option Adresse de rattachement est vu comme une transformation fixe des paquets qui n'affecte pas le traitement IPsec.

- De façon similaire, une adresse de rattachement au sein d'un en-tête d'acheminement de type 2 destiné au nœud receveur est considérée comme l'adresse de destination du paquet, quand un paquet est confronté à la politique de sécurité IPsec ou aux sélecteurs d'une association de sécurité. Des considérations de mise en œuvre s'appliquent au traitement de l'en-tête Acheminement, similaires à celles décrites ci-dessus pour l'option Adresse de destination de rattachement.

- Quand le nœud mobile retourne chez lui et se désenregistre de l'agent de rattachement, le tunnel entre l'agent de rattachement et l'adresse d'entretien du nœud mobile est supprimé. Les entrées de politique de sécurité qui étaient utilisées pour protéger le trafic tunnelé entre le nœud mobile et l'agent de rattachement DEVRAIENT être désactivées (par exemple, en les retirant et les réinstallant plus tard par une API). Les associations de sécurité correspondantes pourraient être laissées comme elles sont, ou supprimées selon la façon dont elles ont été créées. Si les associations de sécurité ont été créées dynamiquement en utilisant IKE, elles sont automatiquement supprimées quand elles arrivent à expiration. Si les associations de sécurité ont été créées par configuration manuelle, elles DOIVENT être conservées et utilisées plus tard quand le nœud mobile quitte à nouveau son domaine de rattachement. Les associations de sécurité qui protègent les mises à jour de lien, les accusés de réception de lien et les messages de découverte de préfixe mobile NE DEVRAIENT PAS être supprimées car elles ne dépendent pas des adresses d'entretien et peuvent être réutilisées.

- Le nœud mobile DOIT utiliser l'option Adresse de destination de rattachement dans les mises à jour de lien et les sollicitations de préfixe mobile quand la protection IPsec de mode de transport est utilisée, afin que l'adresse de rattachement soit visible quand les vérifications de politique IPsec sont effectuées.

- L'agent de rattachement DOIT utiliser l'en-tête Acheminement de type 2 dans les accusés de réception de lien et les annonces de préfixe mobile envoyés au nœud mobile quand la protection IPsec de mode de transport est utilisée, là encore à cause du besoin d'avoir l'adresse de rattachement visible quand les vérifications de politique sont effectuées.

4.3 Exigences pour le traitement du protocole IPsec

Voici la liste des exigences pour le traitement de IPsec à l'agent de rattachement et au nœud mobile.

- L'agent de rattachement et le nœud mobile DEVRAIENT prendre en charge le type de message En-tête de mobilité comme sélecteur IPsec.

- L'agent de rattachement et le nœud mobile DEVRAIENT prendre en charge le type de message ICMPv6 comme sélecteur IPsec.

- L'agent de rattachement DOIT être capable de distinguer les messages HoTi envoyés à lui-même (quand il agit comme

nœud correspondant) et ceux envoyés aux nœuds correspondants (quand il agit comme agent de rattachement) sur la base de l'adresse de destination du paquet.

- Quand ils sécurisent les mises à jour de lien, les accusés de réception de lien, et les messages de découverte de préfixe mobile, le nœud mobile et l'agent de rattachement DOIVENT tous deux prendre en charge l'utilisation de l'en-tête Encapsulation de charge utile de sécurité (ESP, *Encapsulating Security Payload*) [RFC4303] en mode transport et DOIVENT utiliser un algorithme non nul d'authentification de charge utile pour fournir l'authentification de l'origine des données, la protection de l'intégité sans connexion, et facultativement la protection contre la répétition. L'utilisation d'un numéro de séquence dans l'en-tête ESP pour fournir la protection contre la répétition est facultative parce que les numéros de séquence dans les mises à jour de lien fournissent la protection contre la répétition. Cependant, la protection contre la répétition échoue si l'agent de rattachement perd l'état d'antémémoire de lien, par exemple, à cause d'un réamorçage. Comme l'état de l'association de sécurité IPsec peut aussi être supposé perdu, ESP ne peut pas fournir de protection contre la répétition dans ce cas. Une protection complète contre la répétition peut seulement être fournie par l'utilisation d'un mécanisme dynamique de changement de clés, comme IKEv2. La prise en charge de la protection de ces messages en utilisant ESP en mode tunnel est facultative.

- IPsec ESP en mode tunnel DOIT être pris en charge et DEVRAIT être utilisé pour la protection des paquets qui relèvent de la procédure d'acheminement de retour. Une transformation de chiffrement non nulle et un algorithme d'authentification non nul DOIVENT être appliqués.

- Quand ESP est utilisé pour protéger les mises à jour de lien, il n'y a pas de protection pour l'adresse d'entretien qui apparaît dans l'en-tête IPv6 en dehors de la zone protégée par ESP. Il est important pour l'agent de rattachement de vérifier que l'adresse d'entretien n'a pas été altérée. Par suite, l'attaquant aurait redirigé le trafic du nœud mobile sur une autre adresse. Afin d'empêcher cela, les mises en œuvre de IPv6 mobile DOIVENT utiliser l'option de mobilité Autre adresse d'entretien dans les mises à jour de lien envoyées par les nœuds mobiles lorsque ils sont hors de leur domaine de rattachement. Une exception est quand le nœud mobile retourne dans son domaine de rattachement et envoie une mise à jour de lien à l'agent de rattachement afin de se désenregistrer. Quand IPsec est utilisé pour protéger la signalisation d'acheminement de retour ou des paquets de charge utile, le nœud mobile DOIT régler l'adresse de source qu'il utilise pour les paquets qui sortent du tunnel à l'adresse d'entretien principale actuelle.

- Quand IPsec est utilisé pour protéger la signalisation d'acheminement de retout ou des paquets de charge utile, des associations de sécurité IPsec sont nécessaires pour fournir cette protection. Quand l'adresse d'entretien pour le nœud mobile change par suite d'une mise à jour de lien acceptée, un traitement particulier est nécessaire pour les paquets suivants envoyés en utilisant ces associations de sécurité. L'agent de rattachement DOIT régler la nouvelle adresse d'entretien comme adresse de destination de ces paquets, comme si l'adresse de destination de l'en-tête externe dans l'association de sécurité avait changé. De même, l'agent de rattachement commence à attendre la nouvelle adresse de source dans les paquets de tunnel reçus du nœud mobile.

De tels changements d'adresses peut être mis en œuvre, par exemple, par une API de la mise en œuvre de IPv6 mobile à la mise en œuvre de IPsec. Une telle API est décrite dans [PF_KEY]. On devrait noter que l'utilisation d'une telle API et des changements d'adresses DOIVENT seulement être faits sur la base des mises à jour de lien reçues par l'agent de rattachement et protégées par IPsec. Les modifications d'adresses fondées sur d'autres sources, comme des mises à jour de lien aux nœuds correspondants protégées par l'acheminement de retour, ou l'accès ouvert à une API de toute application peut résulter en des faiblesses de la sécurité.

4.4 Exigences de changement de clés dynamique

Les exigences suivantes sont relatives à l'utilisation d'un protocole de gestion dynamique de clés par le nœud mobile et l'agent de rattachement. Le paragraphe 7.3 décrit l'utilisation de IKEv2 comme protocole de gestion dynamique de clés.

- Le nœud mobile DOIT utiliser son adresse d'entretien comme adresse de source dans les échanges de protocole, quand il utilise le changement dynamique de clés.

- Le nœud mobile et l'agent de rattachement DOIVENT créer des associations de sécurité sur la base de l'adresse de rattachement, afin que les associations de sécurité survivent aux changements de l'adresse d'entretien. Quand on utilise IKEv2 comme protocole d'échange de clés, l'adresse de rattachement devrait être portée comme l'adresse IP de l'initiateur dans la charge utile TSi durant l'échange CREATE_CHILD_SA [RFC4306].

- Si le nœud mobile a utilisé IKEv2 pour établir les associations de sécurité avec son agent de rattachement, il devrait suivre les procédures des paragraphes 11.7.1 et 11.7.3 de la spécification de base [RFC3775] pour déterminer si les

points d'extrémité IKE peuvent être déplacés ou si les SA, incluant la SA IKEv2, doivent être re-établies.

- Si l'agent de rattachement a utilisé IKEv2 pour établir les associations de sécurité avec le nœud mobile, il devrait suivre les procédures des paragraphes 10.3.1 et 10.3.2 de la spécification de base [RFC3775] pour déterminer si les points d'extrémité IKE peuvent être déplacés ou si les SA, incluant la SA IKEv2, doivent être re-établies.

5. Considérations de granularité du sélecteur

Les mises en œuvre de IPsec sont compatibles avec le présent document même si elles ne prennent pas en charge des sélecteurs de granularité fine comme le type de message En-tête de mobilité et le type de message ICMPv6. Noter que ces mises en œuvre de IPsec ne sont pas conformes à la [RFC4301]. Pour diverses raisons, certaines mises en œuvre peuvent choisir de prendre seulement en charge des sélecteurs à grosse granularité (c'est-à-dire, des adresses et dans certains cas, le champ Protocole) pour le trafic transmis. Comme les sélecteurs de granularité fine donnent un meilleur contrôle, c'est-à-dire que la protection est seulement appliquée quand elle est nécessaire, les exemples du présent document utilisent toujours la plus fine granularité.

On décrit ensuite les différentes façons d'établir les politiques IPsec pour protéger les messages IPv6 mobile :

1. Les mises en œuvre de IPsec sur le nœud mobile et l'agent de rattachement prennent en charge les sélecteurs à granularité fine, incluant le type de message En-tête de mobilité. C'est le cas supposé dans les exemples de SPD et SAD IPsec de ce document.

2. Les mises en œuvre de IPsec prennent seulement en charge les sélecteurs au niveau du protocole. Une telle mise en œuvre de IPsec peut seulement identifier le trafic d'en-têtes de mobilité et ne peut pas identifier les messages En-tête de mobilité individuels. Dans ce cas, la protection des messages Acheminement de retour utilise un établissement similaire à celui des paquets de charge utile réguliers envoyés au nœud correspondant avec le sélecteur de protocole réglé à En-tête de mobilité. Tous les messages En-tête de mobilité tunnelés vont être protégés.

3. Le troisième cas est lorsque le sélecteur de protocole n'est pas disponible dans la mise en œuvre de IPsec. Dans ce cas, tout le trafic envoyé par le nœud mobile qui est tunnelé à l'envers à travers l'agent de rattachement est protégé en utilisant ESP en mode tunnel. Ce cas est aussi applicable quand le nœud mobile, à cause de considérations de confidentialité, tunnelle tout le trafic à l'agent de rattachement. Cela inclut les messages de signalisation IPv6 mobile échangés entre le nœud mobile et l'agent de rattachement et tout le trafic échangé entre le nœud mobile et le nœud correspondant. Ce cas utilise des SA IPsec en mode tunnel avec le sélecteur de protocole réglé à 'any'.

Le troisième cas où tout le trafic tunnelé est protégé introduit des considérations supplémentaires :

- Si il y a juste une SA IPsec qui fournit la protection pour tout le trafic, alors la SA DOIT satisfaire aux exigences de protection des messages Acheminement de retour qui exigent la protection de la confidentialité. Si le troisième cas est utilisé pour des considérations de confidentialité, alors il peut aussi y avoir des entrées de SPD séparées de mode tunnel pour protéger les messages Acheminement de retour avec une priorité supérieure dans la SPD afin que l'entrée de SPD avec la plus haute priorité soit appliquée en premier.

- La réception d'une mise à jour de lien provenant de la nouvelle adresse d'entretien met à jour le point d'extrémité de tunnel de la SA IPsec comme décrit au paragraphe 4.3. Comme la mise à jour de lien qui met à jour le point d'extrémité de tunnel est reçue à travers la même interface de tunnel qui doit être mise à jour, une attention particulière devrait être apportée par l'agent de rattachement à s'assurer que la mise à jour de lien n'est pas éliminée. Ceci peut être réalisé soit en effectuant la vérification de l'adresse de source sur l'en-tête IPv6 externe après le traitement de la mise à jour de lien, soit en ayant un traitement exceptionnel pour vérifier le paquet interne pour une mise à jour de lien quand la confrontation de l'adresse de source à l'adresse de source externe échoue. Le traitement normal de IPsec ne vérifie pas l'adresse de source externe quand l'origine du paquet a déjà été authentifiée.

6. Configuration manuelle

Cette Section décrit les entrées de SPD et de SAD qui peuvent être utilisées pour protéger les messages de signalisation IPv6 mobile. Les entrées de SPD et de SAD sont seulement un exemple de configurations. Une mise en œuvre particulière de nœud mobile et une mise en œuvre d'agent de rattachement pourraient configurer des entrées différentes de SPD et de

SAD pour autant qu'elles fournissent la sécurité requise des messages de signalisation IPv6 mobile.

Pour les exemples décrits dans ce document, on suppose un nœud mobile avec l'adresse de rattachement, "home_address_1", l'adresse d'entretien principale, "care_of_address_1", un agent de rattachement avec l'adresse, "home_agent_1" et un utilisateur du nœud mobile avec l'identité "user_1". Si l'adresse de rattachement du nœud mobile change, les entrées de SPD et de SAD doivent être re-créées ou mises à jour pour la nouvelle adresse de rattachement.

La base de données d'autorisation des homologues n'est pas utilisée quand la configuration manuelle IPsec est utilisée pour établir les associations de sécurité pour protéger les messages de signalisation IPv6 mobile.

6.1 Mises à jour et accusés de réception de liens

Les entrées de SPD et de SAD suivantes sont sur le nœud mobile et l'agent de rattachement pour protéger les mises à jour de lien et les accusés de réception.

SPD-S de nœud mobile :
- Si adresse locale = home_address_1 & adresse distante = home_agent_1 & proto = MH &
  local_mh_type = BU & remote_mh_type = BAck
Alors utiliser la SA SA1 (OUT) et la SA2 (IN)

SAD de nœud mobile :
- SA1(OUT, spi_a, home_agent_1, ESP, TRANSPORT):
adresse locale = home_address_1 & adresse distante = home_agent_1 & proto = MH & mh_type = BU
- SA2(IN, spi_b, home_address_1, ESP, TRANSPORT):
adresse locale = home_agent_1 & adresse distante = home_address_1 & proto = MH & mh_type = BAck

SPD-S d'agent de rattachement :
- Si adresse locale = home_agent_1 & adresse distante = home_address_1 & proto = MH &
  local_mh_type = BAck & remote_mh_type = BU
Alors utiliser la SA SA2 (OUT) et SA1 (IN)

SAD d'agent de rattachement :
- SA2(OUT, spi_b, home_address_1, ESP, TRANSPORT) :
adresse locale = home_agent_1 & adresse distante = home_address_1 & proto = MH & mh_type = BAck
- SA1(IN, spi_a, home_agent_1, ESP, TRANSPORT) :
adresse locale = home_address_1 & adresse distante = home_agent_1 & proto = MH & mh_type = BU

6.2 Messages d'acheminement de retour

Les entrées de SPD et de SAD suivantes sont utilisées sur le nœud mobile et l'agent de rattachement pour protéger les messages Acheminement de retour.

SPD-S de nœud mobile :
- Si adresse locale = home_address_1 & adresse distante = any &
  proto = MH & local_mh_type = HoTi & remote_mh_type = HoT
Alors utiliser la SA SA3 (OUT) et SA4 (IN)

SAD de nœud mobile :
- SA3(OUT, spi_c, home_agent_1, ESP, TUNNEL) :
adresse locale = home_address_1 & adresse distante = any & proto = MH & mh_type = HoTi
- SA4(IN, spi_d, care_of_address_1, ESP, TUNNEL):
adresse locale = any & adresse distante = home_address_1 & proto = MH & mh_type = HoT

SPD-S d'agent de rattachement :
- Si adresse distante = home_address_1 & adresse locale = any &
  proto = MH & local_mh_type = HoT & remote_mh_type = HoTi
Alors utiliser la SA SA4 (OUT) et SA3 (IN)

SAD d'agent de rattachement :

- SA4(OUT, spi_d, care_of_address_1, ESP, TUNNEL) :
adresse locale = any & adresse distante = home_address_1 & proto = MH & mh_type = HoT
- SA3(IN, spi_c, home_agent_1, ESP, TUNNEL) :
adresse locale = home_address_1 & adresse distante = any & proto = MH & mh_type = HoTi

6.3 Messages de découverte de préfixe mobile

Les entrées de SPD et de SAD suivantes sont utilisées pour protégeer les messages de découverte de préfixe mobile.

SPD-S de nœud mobile :
- Si adresse locale = home_address_1 & adresse distante = home_agent_1 & proto = ICMPv6 &
local_icmp6_type = MPS & remote_icmp6_type = MPA
Alors utiliser la SA SA5 (OUT) et SA6 (IN)

SAD de nœud mobile :
- SA5(OUT, spi_e, home_agent_1, ESP, TRANSPORT) :
adresse locale = home_address_1 & adresse distante = home_agent_1 & proto = ICMPv6 & icmp6_type = MPS
- SA6(IN, spi_f, home_address_1, ESP, TRANSPORT) :
adresse locale = home_agent_1 & adresse distante = home_address_1 & proto = ICMPv6 & icmp6_type = MPA

SPD-S d'agent de rattachement :
- Si adresse locale = home_agent_1 & adresse distante = home_address_1 & proto = ICMPv6 &
local_icmp6_type = MPA & remote_icmp6_type = MPS
Alors utiliser la SA SA6 (OUT) et SA5 (IN)

SAD d'agent de rattachement :
- SA6(OUT, spi_f, home_address_1, ESP, TRANSPORT) :
adresse locale = home_agent_1 & adresse distante = home_address_1 & proto = ICMPv6 & icmp6_type = MPA
- SA5(IN, spi_e, home_agent_1, ESP, TRANSPORT) :
adresse locale = home_address_1 & adresse distante = home_agent_1 & proto = ICMPv6 & icmp6_type = MPS

6.4 Paquets de charge utile

Le trafic régulier de charge utile entre le nœud mobile et le nœud correspondant tunnelé à travers l'agent de rattachement peut être protégé par IPsec, si nécessaire. Le nœud mobile et l'agent de rattachement utilisent ESP en mode tunnel pour protéger le trafic tunnelé. Les entrées de SPD et de SAD montrées au paragraphe 5.2.4 de la [RFC3776] sont applicables ici.

7. Configuration dynamique

Cette Section décrit l'utilisation de IKEv2 pour établir les associations de sécurité requises.

7.1 Entrées de base de données d'autorisation d'homologue

On décrit ensuite les entrées de PAD sur le nœud mobile et l'agent de rattachement. Les entrées de PAD sont seulement des exemples de configurations. Noter que la PAD est un concept logique ; un nœud mobile et un agent de rattachement particuliers peuvent mettre en œuvre la PAD d'une manière spécifique. L'état de la PAD peut aussi être réparti à travers diverses bases de données dans une mise en œuvre spécifique.

PAD de nœud mobile :
- Si identité distante = home_agent_identity_1
Alors authentifier (secret partagé/certificat/EAP) et autoriser la CHILD_SA pour l'adresse distante de home_agent_1

PAD d'agent de rattachement :
- Si identité distante = user_1
Alors authentifier (secret partagé/certificat/EAP) et autoriser les CHILD_SA pour l'adresse distante de home_address_1

La liste des mécanismes d'authentification dans les exemples ci-dessus n'est pas exhaustive. Il pourrait y avoir d'autres accréditifs utilisés pour l'authentification mémorisés dans le PAD.

En cas d'allocation dynamique d'adresse de rattachement, l'agent de rattachement crée une entrée temporaire de PAD liant l'identité authentifiée de l'homologue et la nouvelle adresse de rattachement allouée.

7.2 Entrées de base de données de politique de sécurité

Les paragrphes qui suivent décrivent les entrées de politique de sécurité sur le nœud mobile et l'agent de rattachement. Les entrées de SPD sont seulement des exemples de configurations. Une mise en œuvre particulière de nœud mobile et d'agent de rattachement pourrait configurer des entrées de SPD différentes pour autant qu'elles fournissent la sécurité requise aux messages de signalisation IPv6 mobile.

Dans les exemples ci-dessous, l'identité de l'utilisateur du nœud mobile est supposée être user_1, l'adresse de rattachement du nœud mobile est supposée être home_address_1, l'adresse d'entretien principale du nœud mobile est supposée être care_of_address_1, et l'adresse IPv6 de l'agent de rattachement est supposée être home_agent_1.

7.2.1 Mises à jour et accusés de réception de liens

Les entrées de SPD suivantes sont sur le nœud mobile et l'agent de rattachement pour protéger les mises à jour de lien et les accusés de réception.

SPD-S de nœud mobile :
- Si adresse locale = home_address_1 & adresse distante = home_agent_1 &
  proto = MH & local_mh_type = BU & remote_mh_type = BAck
Alors utiliser une SA ESP en mode transport.
  Initier en utilisant IDi = user_1 à l'adresse home_agent_1

SPD-S d'agent de rattachement :
- Si adresse locale = home_agent_1 & adresse distante = home_address_1 &
  proto = MH & local_mh_type = BAck & remote_mh_type = BU
Alors utiliser une SA ESP en mode transport.

Dans les exemples ci-dessus, l'adresse de rattachement du nœud mobile pourrait n'être pas disponlble tout le temps. Par exemple, le nœud mobile pourrait n'avoir pas encore configuré d'adresse de rattachement. Quand le nœud mobile acquiert une nouvelle adresse de rattachement, il doit soit ajouter l'adresse aux entrées de SPD correspondantes, soit créer les entrées de SPD pour l'adresse de rattachement.

L'agent de rattachement devrait avoir des entrées de SPD nommées par nœud mobile, sur la base de l'identité du nœud mobile. L'identité du nœud mobile est mémorisée dans le sélecteur "Nom" dans la SPD [RFC4301]. L'adresse de rattachement présentée par le nœud mobile durant la négociation IKE est mémorisée comme adresse IP distante dans les associations de sécurité IPsec résultantes. Si le nœud mobile configure dynamiquement un agent de rattachement et l'adresse de rattachement, l'agent de rattachement peut ne pas savoir quels nœuds mobiles il est supposé desservir. Donc, l'agent de rattachement ne peut pas avoir des entrées de SPD configurées par nœud mobile. L'agent de rattachement devrait plutôt avoir des entrées de SPD génériques pour empêcher le trafic d'en-têtes de mobilité qui exige une protection par IPsec d'outrepasser les filtres IPsec. Une fois qu'un nœud mobile s'authentifie auprès de l'agent de rattachement et configure une adresse de rattachement, les entrées de SPD appropriées sont créées pour le nœud mobile.

Le type de message En-tête de mobilité est négocié en le plaçant dans les huit bits de poids fort des 16 bits du sélecteur d'accès local durant l'échange IKEv2. Pour les détails, se reporter à la [RFC4301]. Les charges utiles TSi et TSr dans les exemples ci-dessus vont contenir de nombreux autres sélecteurs en plus de home_address_1. Pour faire bref, on montre seulement les valeurs pertinentes pour IPv6 mobile.

7.2.2 Messages d'acheminement de retour

Les entrées de SPD suivantes sur le nœud mobile et l'agent de rattachement sont pour protéger les messages Acheminement de retour.

SPD-S de nœud mobile :

- Si adresse locale = home_address_1 & adresse distante = any &
proto = MH & local_mh_type = HoTi & remote_mh_type = HoT
Alors utiliser une SA ESP en mode tunnel.
Initier en utilisant IDi = user_1 à l'adresse home_agent_1

SPD-S d'agent de rattachement :
- Si adresse locale = any & adresse distante = home_address_1 &
proto = MH & local_mh_type = HoT & remote_mh_type = HoTi
Alors utiliser une SA ESP en mode tunnel.

Quand l'adresse d'entretien du nœud mobile change, les entrées de SPD sur le nœud mobile et l'agent de rattachement doivent être mises à jour. L'agent de rattachement connaît le changement d'adresse d'entretien du nœud mobile quand il reçoit une mise à jour de lien de la part du nœud mobile.

7.2.3 Messages de découverte de préfixe mobile

Les entrées de SPD suivantes sont sur le nœud mobile et l'agent de rattachement pour protéger les messages Découverte de préfixe mobile.

SPD-S de nœud mobile :
- Si adresse locale = home_address_1 & adresse distante = home_agent_1 &
proto = ICMPv6 & local_icmp6_type = MPS & remote_icmp6_type = MPA
Alors utiliser une SA ESP en mode transport.
Initier en utilisant IDi = user_1 à l'adresse home_agent_1

SPD-S d'agent de rattachement :
- Si adresse locale = home_agent_1 & adresse distante = home_address_1 &
proto = ICMPv6 & local_icmp6_type = MPA & remote_icmp6_type = MPS
Alors utiliser une SA ESP en mode transport.

Dans les exemples ci-dessus, l'adresse de rattachement du nœud mobile pourrait n'être pas disponlble tout le temps. Quand le nœud mobile acquiert une nouvelle adresse de rattachement, il doit ajouter l'adresse aux entrées de SPD correspondantes.

Les charges utiles TSi et TSr dans les exemples ci-dessus vont contenir de nombreux autres sélecteurs en plus de home_address_1. Ils ne sont pas montrés ici dans un souci de concision.

7.2.4 Paquets de charge utile

Les entrées de SPD suivantes sur le nœud mobile et l'agent de rattachement ont lieu si le trafic de charge utile échangé entre le nœud mobile et son nœud correspondant ont besoin d'être protégés. Les entrées de SPD sont similaires aux entrées pour protéger les messages Acheminement de retour et ont une priorité inférieure à celle des entrées de SPD ci-dessus.

SPD-S de nœud mobile :
- Si interface = tunnel IPv6 à home_agent_1 & source = home_address_1 & destination = any & proto = X
Alors utiliser une SA ESP en mode tunnel.
Initier en utilisant IDi = user_1 à l'adresse home_agent_1

SPD-S d'agent de rattachement :
- Si interface = tunnel IPv6 à home_address_1 & source = any & destination = home_address_1 & proto = X
Alors utiliser une SA ESP en mode tunnel.

7.3 Négociation d'association de sécurité en utilisant IKEv2

Les messages de signalisation IPv6 mobile sont normalement initiés par le nœud mobile. Le nœud mobile envoie une mise à jour de lien à l'agent de rattachement chaque fois qu'il bouge et acquiert une nouvelle adresse d'entretien.

Le nœud mobile initie un échange de protocole IKEv2 si les associations de sécurité requises ne sont pas présentes. Un mécanisme possible utilisé pour l'authentification mutuelle est un secret partagé entre le nœud mobile et l'agent de rattachement. L'agent de rattachement utilise l'identité du nœud mobile pour identifier le secret partagé correspondant.

Quand un mécanisme fondé sur la clé publique est disponible, il devrait être préféré pour l'authentification mutuelle.

Si un secret partagé est utilisé, le nœud mobile utilise le secret partagé pour générer la charge utile AUTH dans l'échange IKE_AUTH. Si le nœud mobile utilise un mécanisme fondé sur la clé publique, il utilise alors sa clé privée pour générer la charge utile AUTH dans l'échange IKE_AUTH.

Nœud mobile **Agent de rattachement**

HDR, SAi1, KEi, Ni -->

<-- HDR, SAr1, KEr, Nr, [CERTREQ]

HDR, SK {IDi, [CERT,] [CERTREQ,] [IDr,] AUTH, SAi2, TSi, TSr} -->

<-- HDR, SK {IDr, [CERT,] AUTH, SAr2, TSi, TSr}

Le nœud mobile inclut toujours son identité dans la charge utile IDi dans l'échange IKE_AUTH. Le nœud mobile pourrait utiliser les différents types d'identités suivants pour s'identifier auprès de l'agent de rattachement.

- o Adresse de rattachement - le nœud mobile pourrait utiliser son adresse de rattachement configurée statiquement comme son identité. Dans ce cas, le champ Type d'identité est réglé à ID_IPV6_ADDR.
- o FQDN - le nœud mobile peut utiliser un nom de domaine pleinement qualifié comme identifiant et régler le champ Type d'identifiant à ID_FQDN.
- o Identifiant de la RFC 822 - si le nœud mobile utilise un identifiant de la [RFC0822], il règle le champ Type d'identifiant à ID_RFC822_ADDR.

La liste d'identités ci-dessus n'est pas exhaustive.

Dans l'échange IKE_AUTH, le nœud mobile inclut l'adresse de rattachement et les sélecteurs appropriés dans la charge utile TSi (initiateur de sélecteur de trafic) pour négocier les associations de sécurité IPsec pour protéger les messages de mise à jour de lien et d'accusé de réception de lien. Le nœud mobile PEUT utiliser une gamme de sélecteurs qui inclut les types de message de mobilité pour la mise à jour de lien et l'accusé de réception de lien pour utiliser la même paire d'associations de sécurité IPsec pour les deux messages.

Après l'achèvement de l'échange IKE_AUTH, le nœud mobile initie l'échange CREATE_CHILD_SA pour négocier des associations de sécurité supplémentaires pour protéger la signalisation d'acheminement de retour, la découverte de préfixe mobile, et (facultativement) le trafic de charges utiles. Les échanges CREATE_CHILD_SA sont protégés par les associations de sécurité IKEv2 créées durant l'échange IKE_SA_INIT. Si un nœud correspondant, qui est aussi un nœud mobile, initie l'échange d'acheminement de retour, alors l'agent de rattachement initie l'échange CREATE_CHILD_SA pour négocier les associations de sécurité pour protéger les messages d'acheminement de retour.

Il est important que les associations de sécurité soient créées sur la base de l'adresse de rattachement du nœud mobile, afin que les associations de sécurité survivent au changement d'adresse d'entretien. Le nœud mobile DOIT utiliser son adresse de rattachement comme adresse IP d'initiateur dans la charge utile TSi de l'échange CREATE_CHILD_SA afin de créer les associations de sécurité IPsec pour l'adresse de rattachement.

Nœud mobile **Agent de rattachement**

HDR, SK {[N], SA, Ni, [KEi], [TSi, TSr]} ------->

<---------- HDR, SK {SA, Nr, [KEr], [TSi, TSr]}

Quand l'authentification fondée sur PKI est utilisée entre le nœud mobile et l'agent de rattachement, l'identité présentée par le nœud mobile dans la charge utile IDi DOIT correspondre à l'identité dans le certificat obtenu par l'agent de rattachement. L'agent de rattachement utilise l'identité présentée dans la charge utile IDi pour chercher la politique et le certificat qui correspondent au nœud mobile. Si le nœud mobile présente son adresse de rattachement dans la charge utile IDi, alors l'agent de rattachement DOIT vérifier que l'adresse de rattachement correspond à l'adresse dans un champ Adresse IP dans l'extension SubjectAltName [RFC4945].

Quand le nœud mobile utilise son adresse de rattachement dans le champ IDi, les mises en œuvre ne sont pas obligées de faire correspondre l'adresse de source dans l'en-tête IP externe avec l'adresse IP dans le champ IDi. Selon la [RFC4306], les champs d'en-tête IP dans les messages IKEv2 sont ignorés et utilisés seulement dans les en-têtes IP pour les messages IKEv2 envoyés en réponse.

7.4 Mouvements et changement dynamique de clés

Si le nœud mobile se déplace et que son adresse d'entretien change, la SA IKEv2 SA pourrait n'être plus valide. La RFC 3775 définit un mécanisme fondé sur la réussite de l'échange des messages de mise à jour de lien et d'accusé de

réception de lien. Le nœud mobile établit la SA IKE avec l'agent de rattachement en utilisant son adresse d'entretien principale. Les points d'extrémité de la SA IKE sont mis à jour chez l'agent de rattachement quand il reçoit la mise à jour de lien provenant de la nouvelle adresse d'entretien du nœud mobile et chez le nœud mobile quand il envoie la mise à jour de lien à l'agent de rattachement ou quand il reçoit l'accusé de réception de lien envoyé par l'agent de rattachement. Cette capacité de changer les points d'extrémité IKE est indiquée en établissent le fanion Capacité de gestion de clé (K) [RFC3775] dans les messages de mise à jour de lien et d'accusé de réception de lien. Si le nœud mobile ou l'agent de rattachement ne prend pas en charge cette capacité, et n'a pas d'autre moyen pour mettre à jour les adresses, un échange IKEv2 DOIT alors être initié pour établir une nouvelle SA IKE.

8. Utilisation de l'authentification EAP

En plus de l'utilisation de signatures à clé publique et secrets partagés, EAP [RFC3748] peut être utilisé avec IKEv2 pour authentifier le nœud mobile auprès de l'agent de rattachement.

Le nœud mobile indique qu'il veut utiliser EAP en incluant la charge utile IDi mais sans inclure la charge utile AUTH dans le premier message durant l'échange IKE_AUTH. L'agent de rattachement inclut alors une charge utile EAP si il veut utiliser une méthode d'authentification extensible. Les associations de sécurité ne sont pas créées avant l'échange IKE_AUTH suivant après la réussite de l'authentification EAP. L'utilisation de EAP ajoute au moins deux allers-retours à la négociation IKE. Le nombre d'allers-retours dépend de la méthode EAP utilisée.

```
Nœud mobile                              Agent de rattachement
HDR, SAi1, KEi, Ni     -->
                                <--   HDR, SAr1, KEr, Nr, [CERTREQ]
HDR, SK {IDi, [CERTREQ,] [IDr,] SAi2, TSi, TSr}-->
                                <--   HDR, SK {IDr, [CERT,] AUTH, EAP }
                                .
                                .
                                .
HDR, SK {EAP}          -->
                                <--   HDR, SK {EAP (succès)}
HDR, SK {AUTH}         -->
                                <--   HDR, SK {AUTH, SAr2, TSi, TSr}
```

Quand EAP est utilisé, l'identité présentée par le nœud mobile dans le champ IDi peut n'être pas l'identité réelle du nœud mobile. Elle pourrait être réglée à une identité qui est utilisée seulement pour les besoins de l'acheminement de l'authentification, l'autorisation, et la comptabilité (AAA) et choisir la bonne méthode EAP. Il est possible que l'identité réelle soit portée dans EAP, invisible à l'agent de rattachement. Alors que IKEv2 ne permet pas un échange de message demande/réponse d'identité EAP, les méthodes EAP peuvent échanger des identités au sein d'elles-mêmes. Dans ce cas, l'agent de rattachement DOIT acquérir l'identité du nœud mobile à partir du serveur AAA correspondant. Comment l'agent de rattachement acquiert l'identité du nœud mobile sort du domaine d'application de ce document.

Certaines méthodes EAP, quand elles sont utilisées avec IKEv2, génèrent une clé partagée sur le nœud mobile et l'agent de rattachement une fois que l'authentification EAP a réussi. Cette clé partagée est utilisée pour générer les charges utiles AUTH dans les messages IKEv2 suivants. La clé partagée, si elle est utilisée pour générer les charges utiles AUTH, NE DOIT PAS être utilisée pour autre chose. Pour les détails, voir la [RFC4306].

L'utilisation de EAP entre le nœud mobile et l'agent de rattachement pourrait exiger que l'agent de rattachement contacte un serveur d'autorisation comme le serveur de rattachement AAA, sur la liaison de rattachement, pour authentifier le nœud mobile. Voir les détails dans la [RFC5637].

9. Configuration dynamique d'adresse de rattachement

Le nœud mobile peut configurer dynamiquement une adresse de rattachement en incluant une charge utile Configuration dans l'échange IKE_AUTH, avec une demande d'adresse à la liaison de rattachement. Le nœud mobile devrait inclure un attribut INTERNAL_IP6_ADDRESS de longueur zéro dans la charge utile CFG_REQUEST. Le nœud mobile PEUT inclure plusieurs instances de INTERNAL_IP6_ADDRESS pour demander plusieurs adresses de rattachement à allouer par l'agent de rattachement.

Quand l'agent de rattachement reçoit une charge utile de configuration avec une CFG_REQUEST pour INTERNAL_IP6_ADDRESS, il répond avec une adresse de rattachement valide pour le nœud mobile. L'attribut INTERNAL_IP6_ADDRESS dans la CFG_REPLY contient la longueur du préfixe du préfixe de rattachement en plus des 128 bits de l'adresse de rattachement. L'agent de rattachement pourrait utiliser une base de données locale ou contacter un serveur DHCPv6 sur la liaison de rattachement pour allouer une adresse de rattachement. La durée de l'allocation de l'adresse de rattachement au nœud mobile est la même que la durée d'existence d'une association de sécurité IKEv2 entre le nœud mobile et l'agent de rattachement. Si l'association de sécurité IKEv2 change de clés, la durée de vie de l'adresse de rattachement est aussi étendue.

Nœud mobile **Agent de rattachement**

HDR, SK {IDi, [CERT,] [CERTREQ,] [IDr,] AUTH, CP(CFG_REQUEST),
SAi2, TSi, TSr} ---------->
<---------- HDR, SK {IDr, [CERT,] AUTH, CP(CFG_REPLY), SAr2, TSi, TSr}

Le nœud mobile pourrait suggérer une adresse de rattachement qu'il veut utiliser dans la CFG_REQUEST. Par exemple, ce pourrait être une adresse de rattachement qui a été allouée au nœud mobile auparavant ou une adresse que le nœud mobile a autoconfigurée à partir du préfixe IPv6 sur la liaison de rattachement. L'agent de rattachement pourrait laisser le nœud mobile utiliser la même adresse de rattachement en réglant l'attribut INTERNAL_IP6_ADDRESS dans la charge utile CFG_REPLY à la même adresse de rattachement. Si l'agent de rattachement veut que le nœud mobile utilise une adresse de rattachement différente, il envoie une nouvelle adresse de rattachement dans l'attribut INTERNAL_IP6_ADDRESS dans la charge utile CFG_REPLY. Le nœud mobile DOIT arrêter d'utiliser sa vieille adresse de rattachement et commencer d'utiliser la nouvelle adresse de rattachement allouée.

Dans le cas où l'agent de rattachement est incapable d'allouer une adresse de rattachement au nœud mobile durant l'échange IKE_AUTH, il DOIT envoyer une charge utile Notify avec un message INTERNAL_ADDRESS_FAILURE. Quand le nœud mobile reçoit une charge utile Notify avec un message INTERNAL_ADDRESS_FAILURE, il DEVRAIT terminer l'échange IKE_AUTH. Le nœud mobile devrait alors initier un nouvel échange IKE_SA_INIT et IKE_AUTH et essayer d'autoconfigurer une adresse de rattachement comme décrit dans la [RFC5026]. Le nœud mobile PEUT aussi passer à un autre agent de rattachement. L'adresse du nouvel agent de rattachement peut être obtenue en consultant une liste des agents de rattachement reçue durant une précédente phase de découverte d'agent de rattachement ou, si cette liste est vide ou non disponible, en tentant une nouvelle découverte d'agent de rattachement.

Si le nœud mobile veut configurer un serveur DNS à partir de la liaison de rattachement, il peut demander des informations de serveur DNS en incluant un attribut INTERNAL_IP6_DNS dans la charge utile CFG_REQUEST.

10. Considérations sur la sécurité

Le présent document décrit comment IPsec peut être utilisé pour sécuriser les messages de signalisation IPv6 mobile. Prière de se référer à la [RFC3775] pour les considérations sur la sécurité relatives à l'utilisation de IPsec avec IPv6 mobile.

Un nœud mobile qui se comporte mal pourrait créer des associations de sécurité IPsec pour une adresse de rattachement qui appartient à une autre nœud mobile. Donc, l'agent de rattachement devrait vérifier si un nœud mobile particulier est autorisé à utiliser une adresse de rattachement avant de créer des associations de sécurité IPsec pour l'adresse de rattachement. Si l'adresse de rattachement est allouée comme décrit à la Section 9, l'agent de rattachement DOIT associer l'adresse de rattachement à l'identité utilisée dans la négociation IKE. L'agent de rattachement PEUT mémoriser l'adresse de rattachement allouée dans les entrées de SPD créées pour le nœud mobile.

L'utilisation de EAP pour authentifier le nœud mobile auprès de l'agent de rattachement est décrite à la Section 8. Les considérations sur la sécurité relatives à l'utilisation de EAP avec IKEv2 sont décrites dans la [RFC4306].

11. Remerciements

Les auteurs souhaitent remercier Mika Joutsenvirta, Pasi Eronen, Jari Arkko, Gerardo Giaretta, Shinta Sugimoto, Tero Kivinen, Steve Bellovin, Kilian Weniger, et Vijay Gurbani de leur relecture du document.

Beaucoup des exigences mentionnées à la Section 4 sont copiées de la RFC 3776. Donc, les auteurs de la RFC 3776 sont

remerciés.

12. Références

12.1 Références normatives

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

[RFC3775] D. Johnson, C. Perkins, J. Arkko, "Prise en charge de la mobilité dans IPv6", juin 2004. *(P.S.) (Obs., voir* RFC6275)

[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.)*

[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.)*

[RFC4306] C. Kaufman, "Protocole d'échange de clés sur Internet (IKEv2)", décembre 2005. *(Obsolète, voir la* RFC5996)

12.2 Références pour information

[PF_KEY] Sugimoto, S., "Extension PF_KEY comme interface entre IPv6 mobile et IPsec/IKE", Travail en cours, septembre 2006.

[RFC0822] D. Crocker, "Norme pour le format des messages de texte de l'ARPA-Internet", STD 11, août 1982. (*Obsolète, voir RFC*5322)

[RFC2401] S. Kent et R. Atkinson, "Architecture de sécurité pour le protocole Internet", novembre 1998. (*Obsolète, voir* RFC4301)

[RFC3748] B. Aboba et autres, "Protocole extensible d'authentification (EAP)", juin 2004. *(P.S., MàJ par* RFC5247)

[RFC4945] B. Korver, "Profil Internet de PKI de sécurité IP de IKEv1/ISAKMP, IKEv2, et PKIX", août 2007. *(P.S.)*

[RFC5026] G. Giaretta et autres, "Amorçage IPv6 mobile dans un scénario de partage", octobre 2007. *(P.S.)*

[RFC5637] G. Giaretta, I. Guardini, E. Demaria, J. Bournelle, R. Lopez, "Objectifs d'authentification, d'autorisation et de comptabilité (AAA) pour IPv6 Mobile" septembre 2009. *(Information)*

Adresse des auteurs

Vijay Devarapalli
Azaire Networks
3121 Jay Street
Santa Clara, CA 95054
USA
mél : vijay.devarapalli@azairenet.com

Francis Dupont
CELAR
mél : Francis.Dupont@fdupont.fr

Remerciement

Le financement de la fonction d'édition des RFC est actuellement fourni par la Internet Society.