Groupe de travail Réseau
Request for Comments : 3776
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

J. Arkko, Ericsson
V. Devarapalli, Nokia Research Center
F. Dupont, GET/ENST Bretagne
juin 2004

Utilisation d'IPsec pour protéger la signalisation IPv6 mobile entre nœuds mobiles et agents de rattachement

Statut du présent mémoire
Le présent document spécifie un protocole de l'Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. Prière de se référer à l'édition en cours des "Protocoles officiels de l'Internet" (STD 1) pour voir l'état de normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé
IPv6 mobile utilise IPsec pour protéger la signalisation entre l'agent de rattachement et le nœud mobile. Le document de base IPv6 mobile définit les principales exigences que doivent respecter ces nœuds. Le présent document expose ces exigences plus en profondeur, illustre les formats de paquet utilisés, décrit les procédures de configuration convenables, et montre comment les mises en œuvre peuvent traiter les paquets dans le bon ordre.

Table des Matières

1. Introduction

Le présent document illustre l'utilisation de IPsec pour sécuriser le trafic IPv6 mobile [RFC3775] entre les nœuds mobiles et les agents de rattachement. Dans IPv6 mobile, un nœud mobile est toujours supposé être adressable à son adresse de rattachement, qu'il soit actuellement rattaché à sa liaison de rattachement ou en itinérance. Une "adresse de rattachement" est une adresse IP allouée au nœud mobile au sein de son préfixe de sous réseau de rattachement sur sa liaison de rattachement. Lorsque un nœud mobile est à son point de rattachement, les paquets adressés à son adresse de rattachement sont acheminés à la liaison de rattachement du nœud mobile.

Lorsque un nœud mobile est rattaché à une liaison étrangère loin de son rattachement, il est aussi adressable à une adresse d'entretien. Une adresse d'entretien est une adresse IP associée à un nœud mobile qui a un préfixe de sous réseau d'une liaison étrangère particulière. L'association entre l'adresse de rattachement d'un nœud mobile et l'adresse d'entretien est connue comme un "lien" pour le nœud mobile. Lorsque il est en déplacement, un nœud mobile enregistre sa principale adresse d'entretien auprès d'un routeur sur sa liaison de rattachement, et demande à ce routeur de fonctionner comme "l'agent de rattachement" pour le nœud mobile. Le nœud mobile effectue cet enregistrement de lien par l'envoi d'un message "Mise à jour de lien" (BU, *Binding Update*) à l'agent de rattachement. L'agent de rattachement répond au nœud mobile en retournant un message "Accusé de réception de lien".

Tous les autres nœuds qui communiquent avec un nœud mobile sont appelés des "nœuds correspondants". Les nœuds mobiles peuvent fournir des informations sur leur localisation actuelle aux nœuds correspondants, là encore en utilisant les messages de mise à jour de lien et d'accusé de réception de lien. De plus, un essai sur l'acheminement de retour est effectué entre le nœud mobile, l'agent de rattachement, et le nœud correspondant afin d'autoriser l'établissement du lien. Les paquets entre le nœud mobile et le nœud correspondant sont soit tunnelés via l'agent de rattachement, soit envoyés directement si un lien existe dans le nœud correspondant pour la localisation actuelle du nœud mobile.

IPv6 mobile tunnelle les paquets de charge utile entre le nœud mobile et l'agent de rattachement dans les deux directions. Ce tunnelage utilise l'encapsulation IPv6 [RFC2473]. Lorsque il est nécessaire de sécuriser les tunnels, ils sont remplacés par des tunnels IPsec [RFC2401].

IPv6 mobile fournit aussi la prise en charge de la reconfiguration du réseau de rattachement. Ici, les préfixes de sous réseau de rattachement peuvent changer au fil du temps. Les nœuds mobiles peuvent apprendre de nouvelles informations sur les préfixes de sous réseau de rattachement par le mécanisme de "découverte de préfixe".

Le présent document discute des mécanismes de sécurité pour le trafic de contrôle entre le nœud mobile et l'agent de rattachement. Si ce trafic n'est pas protégé, les nœuds mobiles et les nœuds correspondants sont vulnérables aux attaques par interposition, de capture, d'espionnage passif, d'usurpation d'identité, et de déni de service. Tous les tiers sont aussi vulnérables aux attaques de déni de service, par exemple si l'attaquant peut diriger le trafic s'écoulant à travers l'agent de rattachement vers un tiers innocent. Ces attaques sont discutées plus en détail au paragraphe 15.1 de la spécification IPv6 mobile de base [RFC3775].

Pour éviter ces attaques, la spécification de base utilise la charge utile de sécurité encapsulée dans IPsec (ESP, *Encapsulating Security Payload*) de la [RFC2406] pour protéger le trafic de contrôle entre l'agent de rattachement et le nœud mobile. Ce trafic de contrôle consiste en divers messages portés par le protocole d'en-tête de mobilité dans IPv6 [RFC2460]. Le trafic prend les formes suivantes :

- Les messages Mise à jour de lien et Accusé de réception échangés entre le nœud mobile et l'agent de rattachement, comme décrit aux paragraphes 10.3.1, 10.3.2, 11.7.1, et 11.7.3 de la spécification de base [RFC3775].
- Les messages d'acheminement de retour Initiation d'essai de rattachement *(Home Test Init)* et Essai de rattachement *(Home*

Test) qui passent à travers l'agent de rattachement sur le chemin vers un nœud correspondant, comme décrit au paragraphe 10.4.6 de la spécification de base [RFC3775].

- Les messages ICMPv6 échangés entre le nœud mobile et l'agent de rattachement pour les besoins de la découverte de préfixe, comme décrit aux paragraphes 10.6 et 11.4 de la spécification de base [RFC3775].

Les nœuds peuvent aussi facultativement protéger le trafic de charge utile qui passe à travers l'agent de rattachement, comme décrit au paragraphe 5.5 de la spécification de base [RFC3775]. Si des protocoles de contrôle des membres de groupe de diffusion groupée ou d'autoconfiguration d'adresse à états pleins sont pris en charge, la prise en charge de la protection des données de charge utile est requise.

Le trafic de contrôle entre le nœud mobile et l'agent de rattachement exige l'authentification du message, la protection de l'intégrité, de l'ordre correct et de l'anti-répétition. Le nœud mobile et l'agent de rattachement doivent avoir une association de sécurité IPsec pour protéger ce trafic. IPsec ne vérifiant pas l'ordre correct des messages, celui du trafic de contrôle est assuré par un numéro de séquence dans les messages Mise à jour de lien et Accusé de réception de lien. Le numéro de séquence dans les mises à jour de lien fournit aussi dans une certaine mesure une protection. Elle échoue dans certains scénarios, par exemple, si l'agent de rattachement perd l'état de mise en antémémoire de lien. Une protection complète contre les attaques en répétition n'est possible que lorsque IKE est utilisé.

Un grand soin doit être apporté lors de l'utilisation de IKE [RFC2409] à l'établissement des associations de sécurité avec les agents de rattachement IPv6 mobile. Le bon type d'adresses doit être utilisé pour transporter IKE. C'est nécessaire pour éviter des dépendances circulaires dans lesquelles l'utilisation d'une mise à jour de lien déclanche le besoin d'un échange IKE qui ne peut pas se terminer avant l'achèvement de la mise à jour de lien.

Le document de base IPv6 mobile définit les principales exigences que les nœuds mobiles et les agents de rattachement doivent suivre pour sécuriser le trafic ci-dessus. Le présent document discute ces exigences plus en profondeur, illustre les formats de paquet utilises, décrit les procédures de configuration convenables, et montre comment les mises en œuvre peuvent traiter les paquets dans le bon ordre.

On commence notre description en montrant les formats de réseau requis pour les paquets protégés à la Section 3. La Section 4 décrit les règles que les mises en œuvre associées de IPv6 mobile, IPsec, et IKE doivent observer. La Section 5 expose comment configurer les associations de sécurité IPsec chiffrées manuellement ou comment configurer IKE pour les établir automatiquement. La Section 6 montre des exemples de la façon dont les paquets sont traités au sein des nœuds.

Toutes les mises en œuvre de nœud mobile et d'agent de rattachement IPv6 mobile DOIVENT prendre en charge au moins les formats décrits à la Section 3 et respecter les règles de la Section 4.

Les sections sur la configuration et le traitement sont pour information, et ne devraient être considérées que comme une des façons possibles de fournir la fonctionnalité demandée.

Noter que lorsque le présent document indique qu'une caractéristique DOIT être prise en charge et DEVRAIT être utilisée, cela implique que toutes les mises en œuvre doivent être capables d'utiliser la caractéristique spécifiée, mais il peut y avoir des cas où, par exemple, une option de configuration désactive l'utilisation de la caractéristique dans une situation particulière.

2. Terminologie

Dans le présent document, les mots clés "DOIT", "NE DOIT PAS", "EXIGÉ", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" sont à interpréter comme décrit dans le BCP 14, [RFC2119].

3. Formats de paquet

3.1 Mises à jour et accusés de réception de liens

Lorsque le nœud mobile est en déplacement, les mises à jour de lien envoyées à l'agent de rattachement DOIVENT accepter au moins les en-têtes suivants dans l'ordre suivant :

En-tête IPv6 (source = adresse d'entretien, destination = agent de rattachement)
En-tête d'option de destination : option adresse de rattachement (*Home Address)*
En-tête ESP en mode transport
En-tête Mobility : Mise à jour de lien *(Binding Update)*; Option adresse d'entretien *(Care-of Address)* de remplacement

Noter que l'option Adresse d'entretien de remplacement est destinée à assurer que l'adresse d'entretien est protégée par ESP. L'agent de rattachement considère l'adresse au sein de cette option comme l'adresse d'entretien en cours pour le nœud mobile. L'adresse de rattachement n'est pas protégée directement par ESP, mais l'utilisation d'une adresse de rattachement spécifique avec une association de sécurité spécifique est exigée par la politique.

Les accusés de réception de lien renvoyés au nœud mobile lorsque il est en déplacement DOIVENT prendre en charge au moins les en-têtes qui suivent dans l'ordre suivant :

En-tête IPv6 (source = agent de rattachement, destination = adresse d'entretien)
En-tête Acheminement (type 2) : adresse de rattachement
En-tête ESP en mode transport
En-tête Mobility : Accusé de réception de lien

Lorsque le nœud mobile est chez lui, les règles ci-dessus sont différentes car le nœud mobile peut utiliser son adresse de rattachement comme adresse de source. Cela arrive normalement pour la mise à jour de lien de désenregistrement lorsque le mobile revient chez lui. Dans cette situation, les mises à jour de lien DOIVENT prendre en charge au moins les en-têtes qui suivent dans l'ordre suivant :

En-tête IPv6 (source = adresse de rattachement, destination = agent de rattachement)
En-tête ESP en mode transport
En-tête Mobility : Mise à jour de lien

Les messages Accusé de réception de lien envoyés à l'adresse de rattachement DOIVENT prendre en charge au moins les en-têtes qui suivent dans l'ordre suivant :

En-tête IPv6 (source = agent de rattachement, destination = adresse de rattachement)
En-tête ESP en mode transport
En-tête Mobility : Accusé de réception de lien

3.2 Signalisation de la possibilité d'acheminement de retour

Lorsque les messages Initialiser l'essai de rattachement *(Home Test Init)* tunnelés à l'agent de rattachement sont protégés par IPsec, ils DOIVENT prendre en charge au moins les en-têtes qui suivent dans l'ordre suivant :

En-tête IPv6 (source = adresse d'entretien, destination = agent de rattachement)
En-tête ESP en mode tunnel
En-tête IPv6 (source = adresse de rattachement, destination = nœud correspondant)
En-tête Mobility : Initialiser l'essai de rattachement

Ce format suppose que l'adresse d'entretien actuelle du nœud mobile est utilisée comme adresse de destination de l'en-tête externe dans l'association de sécurité. Comme exposé au paragraphe 4.3, cela exige que l'agent de rattachement mette à jour l'adresse de destination lorsque le nœud mobile se déplace. Les sélecteurs d'entrée de politique et d'association de sécurité restent cependant les mêmes, car les paquets internes ne changent pas lors des mouvements.

Noter qu'il y a des compromis à faire entre l'utilisation des adresses d'entretien comme des adresses de destination et l'utilisation de l'adresse de rattachement et attacher un en-tête d'option supplémentaire Adresse de rattachement de destination et/ou Acheminement aux paquets. Les bases pour demander la prise en charge d'au moins le cas de l'adresse d'entretien ont été exposées à la Section 7.

De façon similaire, lorsque les messages Essai de rattachement *(Home Test)* tunnelés depuis l'agent de rattachement sont protégés par IPsec, ils DOIVENT prendre en charge au moins les en-têtes qui suivent dans l'ordre suivant :

En-tête IPv6 (source = agent de rattachement, destination = adresse d'entretien)
En-tête ESP en mode tunnel
En-tête IPv6 (source = nœud correspondant, destination = adresse de rattachement)
En-tête Mobility : Essai de rattachement

Le format utilisé pour protéger l'acheminement en retour des paquets s'appuie sur la destination des paquets tunnelés qui change pour le nœud mobile lorsque il se déplace. L'adresse de l'agent de rattachement reste la même, mais l'adresse du nœud mobile change avec les mouvements, comme si l'adresse de destination de l'en-tête externe de l'association de sécurité avait changé. Lorsque le nœud mobile adopte une nouvelle adresse d'entretien, il adopte aussi une nouvelle adresse de source pour

les paquets tunnelés sortants. L'agent de rattachement accepte les paquets envoyés comme cela, car l'adresse de source externe dans les paquets tunnelés n'est pas vérifiée selon les règles de la RFC 2401. (On note cependant que certaines mises en œuvre sont connues pour faire des vérifications d'adresse de source.) Pour une discussion du rôle des adresses de source dans les en-têtes de tunnel externes, voir le paragraphe 5.1.2.1 de la [RFC2401]. Noter aussi que l'agent de rattachement exige que les paquets soient authentifiés sans considération des changements de l'adresse de source, donc le "nouvel" envoyeur doit posséder les mêmes clés pour l'association de sécurité qu'il avait dans la localisation précédente. Cela prouve que l'envoyeur est la même entité, sans considération des changements des adresses.

Le processus est plus compliqué du côté de l'agent de rattachement, car celui-ci a mémorisé l'adresse d'entretien précédente dans sa base de données des associations de sécurité comme l'adresse de destination de l'en-tête externe. Lorsque IKE est utilisé, le nœud mobile le fait fonctionner par dessus son adresse d'entretien en cours, et les associations de sécurité en mode tunnel résultantes vont utiliser les mêmes adresses que celles sur lesquelles fonctionne IKE. Pour que l'agent de rattachement soit capable de tunneler un message Essai de rattachement *(Home Test)* au nœud mobile, il utilise l'adresse d'entretien courante comme destination des paquets tunnelés, comme si l'agent de rattachement avait modifié l'adresse de destination de l'en-tête externe dans l'association de sécurité utilisée pour cette protection. Cela implique que la même association de sécurité peut être utilisée dans plusieurs localisations, et aucune nouvelle configuration ou aucun rétablissement des phases IKE n'est nécessaire pour un mouvement. Le paragraphe 5.2.2 exposé les entrées de la base de données de politique de sécurité et des associations de sécurité qui sont nécessaires pour réaliser cela.

3.3 Découverte du préfixe

Si IPsec est utilisé pour protéger la découverte de préfixe, les demandes de préfixes provenant du nœud mobile à l'agent de rattachement DOIVENT prendre en charge au moins les en-têtes qui suivent dans l'ordre suivant :

En-tête IPv6 (source = adresse d'entretien, destination = agent de rattachement)
En-tête Options de destination : Option Adresse de rattachement (adresse de rattachement)
En-tête ESP en mode transport
ICMPv6 : Sollicitation de préfixe mobile

Là encore, si IPsec est utilisé, les annonces d'informations de préfixe sollicitées et non sollicitées provenant de l'agent de rattachement au nœud mobile DOIVENT prendre en charge au moins les en-têtes qui suivent dans l'ordre suivant :

En-tête IPv6 (source = agent de rattachement, destination = adresse d'entretien)
En-tête Routing (type 2) : adresse de rattachement
En-tête ESP en mode transport
ICMPv6 : Annonce de préfixe mobile

3.4 Paquets de charge utile

Si IPsec est utilisé pour protéger les paquets de charge utile tunnelés à l'agent de rattachement depuis le nœud mobile, on utilise un format similaire à celui du paragraphe 3.2. Cependant, au lieu de l'en-tête Mobility, ces paquets peuvent contenir tous protocoles légaux IPv6 :

En-tête IPv6 (source = adresse d'entretien, destination = agent de rattachement)
En-tête ESP en mode tunnel
En-tête IPv6 (source = adresse de rattachement, destination = nœud correspondant)
Tout protocole

De façon similaire, lorsque les paquets de charge utile sont tunnelés de l'agent de rattachement au nœud mobile avec encapsulation ESP, ils DOIVENT prendre en charge au moins les en-têtes qui suivent dans l'ordre suivant :

En-tête IPv6 (source = agent de rattachement, destination = adresse d'entretien)
En-tête ESP en mode tunnel
En-tête IPv6 (source = nœud correspondant, destination = adresse de rattachement)
Tout protocole

4. Exigences

La présente section décrit les règles obligatoires pour tous les nœuds mobiles et agents de rattachement IPv6 mobile. Ces règles sont nécessaires pour qu'il soit possible de permettre les communications IPsec en dépit des mouvements, de garantir

une sécurité suffisante, et d'assurer un traitement correct de l'ordre des paquets.

Les règles des paragraphes qui suivent ne s'appliquent qu'aux communications entre agents de rattachement et nœuds mobiles. Elles ne devraient pas être prises comme des exigences sur la façon dont IPsec en général est utilisé par les nœuds mobiles.

4.1 Prise en charge obligatoire

Les exigences suivantes s'appliquent aux agents de rattachement et aux nœuds mobiles :

- La configuration manuelle des associations de sécurité IPsec DOIT être supportée. La configuration des clés est supposée avoir lieu hors bande, par exemple au moment où le nœud mobile est configuré à utilises son agent de rattachement.

- La gestion automatique de clés avec IKE [RFC2409] PEUT être supportée. Seul IKEv1 est discuté dans le présent document. D'autres mécanismes de gestion automatique de clé existent et vont apparaître au delà de IKEv1, mais le présent document ne traite pas des questions qui s'y rapportent.

- L'encapsulation ESP des mises à jour de lien et des accusés de réception de lien entre le nœud mobile et l'agent de rattachement DOIT être supportée et DOIT être utilisée.

- L'encapsulation ESP des messages Initialisation d'essai de rattachement et Essai de rattachement tunnelés entre le nœud mobile et l'agent de rattachement DOIT être supportée et DEVRAIT être utilisée.

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

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

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

4.2 Exigences de politique

Les exigences suivantes s'appliquent aux agents de rattachement et aux nœuds mobiles :

- Comme exigé dans la spécification de base [RFC3775], lorsque 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 Adresse de rattachement de destination 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 de mise en œuvre possible pour cela : les opérations de politique IPsec peuvent être effectuées au moment où le paquet n'a pas encore été modifié selon les règles de IPv6 mobile, ou a été ramené à sa forme normale après le traitement IPv6 mobile. C'est-à-dire que le traitement de l'option Adresse de rattachement est vu comme une transformation fixe des paquets qui n'affecte pas le traitement IPsec.

- De même, une adresse de rattachement au sein d'un en-tête Acheminement de type 2 destinée au nœud receveur est considérée comme l'adresse de destination du paquet, lorsque un paquet est confronté à une politique de sécurité IPsec ou aux sélecteurs d'une association de sécurité. Des considérations de mise en œuvre similaires s'appliquent au traitement de l'en-tête Acheminement comme décrit ci-dessus pour l'option d'adresse de rattachement de destination.

- Lorsque IPsec est utilisé pour protéger la signalisation d'acheminement de retour ou des paquets de charge utile, cette protection DOIT être appliquée seulement aux paquets d'acheminement de retour qui entrent dans l'interface de tunnel IPv6 encapsulé entre le nœud mobile et l'agent de rattachement. Ceci peut être réalisé, par exemple, en définissant les entrées de la base de données de politique de sécurité spécifiques de l'interface du tunnel. C'est-à-dire que les entrées de politique ne sont généralement pas appliquées sur tout le trafic de la ou des interfaces physiques des nœuds, mais plutôt seulement au trafic qui entre dans ce tunnel.

- L'authentification des nœuds mobiles PEUT se fonder sur des accréditifs de machine ou d'usager. Noter que les systèmes d'exploitation multi usagers permettent normalement à tous les utilisateurs d'un nœud d'utiliser toutes les adresses IP allouées au nœud. Cela limite la capacité de l'agent de rattachement à restreindre l'utilisation d'une adresse de rattachement à un usager particulier dans un tel environnement. Lorsque des accréditifs d'usager sont appliqués à un environnement multi utilisateurs, la configuration devrait autoriser tous les usagers du nœud à contrôler toutes les adresses de rattachement allouées au nœud.

- Lorsque le nœud mobile retourne chez lui et se désenregistre auprès de l'agent de rattachement, le tunnel entre l'agent de rattachement et l'adresse d'entretien du nœud mobile est supprimée. Les entrées de politique de sécurité, qui étaient utilisées pour protéger le trafic tunnelé entre le nœud mobile et l'agent de rattachement DOIVENT être désactivées (par exemple, en les retirant et en les réinstallant plus tard à travers une API). Les associations de sécurité correspondantes pourraient être conservées comme elles sont ou supprimées selon la façon dont elles ont été crées. Si les associations de sécurité avaient été créées de façon dynamique en utilisant IKE, elles sont automatiquement supprimées lorsque 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 et les accusés de réception de liens, et la découverte de préfixe, NE DEVRAIENT PAS être supprimées car elles ne dépendent pas des adresses d'entretien et peuvent être réutilisées.

Les règles suivantes s'appliquent aux nœuds mobiles :

- Le nœud mobile DOIT utiliser l'option Destination d'adresse de rattachement dans les sollicitations de préfixe mobile et les mises à jour de lien envoyées à l'agent de rattachement à partir d'une adresse d'entretien.

- Lorsque le nœud mobile reçoit un ensemble changé de préfixes de l'agent de rattachement durant une découverte de préfixe, il est nécessaire de configurer de nouvelles entrées de politique de sécurité, et il peut être nécessaire de configurer de nouvelles associations de sécurité. Il sort du domaine d'application de cette spécification de discuter des méthodes automatiques pour le faire.

Les règles suivantes s'appliquent aux agents de rattachement :

- L'agent de rattachement DOIT utiliser l'en-tête Acheminement de type 2 dans les accusés de réception de liens et les annonces de préfixe mobile envoyés au nœud mobile, là encore à cause du besoin d'avoir l'adresse de rattachement visible lorsque les vérifications de politique sont faites.

- Il est nécessaire d'éviter la possibilité qu'un nœud mobile puisse utiliser son association de sécurité pour envoyer une mise à jour de lien au nom d'un autre nœud mobile utilisant le même agent de rattachement. Pour faire cela, les entrées de la base de données de sécurité DOIVENT identifier sans équivoque une seule association de sécurité pour protéger les mises à jour de lien entre une certaine adresse de rattachement et l'agent de rattachement lorsque on utilise des associations de sécurité IPsec configurées manuellement. Lorsque la configuration dynamique est utilisée, les entrées de la base de données de politique de sécurité DOIVENT identifier sans équivoque les accréditifs IKE phase 1 qui peuvent être utilisés pour autoriser la création des associations de sécurité pour protéger les mises à jour de liens pour une adresse de rattachement particulière. Comment ces transpositions sont effectuées sort du domaine d'application de la présente spécification, mais elles peuvent être effectuées, par exemple, par un tableau administré localement chez l'agent de rattachement. Si l'identité de phase 1 est un nom de domaine pleinement qualifié (FQDN), des formes sûres du DNS peuvent aussi être utilisées.

- Lorsque l'ensemble de préfixes annoncés par l'agent de rattachement change, il est nécessaire de configurer de nouvelles entrées de politique de sécurité, et il peut être nécessaire de configurer de nouvelles associations de sécurité. Il sort du domaine d'application de la présente spécification de discuter des méthodes automatiques de le faire, si de nouvelles adresses de rattachement sont nécessaires.

4.3 Traitement du protocole IPsec

Les exigences suivantes s'appliquent aux agents de rattachement et aux nœuds mobiles :

- Lors de la sécurisation des mises à jour de liens, des accusés de réception de lien, et de la découverte de préfixe, les nœuds mobiles et les agents de rattachement DOIVENT tous prendre en charge et DEVRAIENT utiliser l'en-tête d'encapsulation de charge utile de sécurité (ESP) [RFC2406] en mode transport et DOIVENT utiliser un algorithme d'authentification de charge utile non nul pour fournir l'authentification de l'origine des données, la protection de l'intégrité sans connexion et la protection facultative contre la répétition. La prise en charge obligatoire des algorithmes de chiffrement et de protection de l'intégrité est définie dans la [RFC2401], la [RFC2402], et la [RFC2406]. Il faut cependant faire attention lors du choix des algorithmes de chiffrement convenables pour ESP. Les algorithmes de protection de l'intégrité actuellement disponibles sont en général considérés comme sûrs. L'algorithme de chiffrement DES, rendu obligatoire par les normes IPsec actuelles ne l'est cependant pas. Ceci est particulièrement problématique lorsque des associations de sécurité IPsec sont configurées manuellement, car la même clé est utilisée pendant longtemps.

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

Noter que la procédure d'acheminement de retour implique deux échanges de messages du nœud mobile au nœud correspondant. L'objet de ces échanges est d'assurer que le nœud mobile est vivant aux adresses de rattachement et d'entretien prétendues. Un des échanges est envoyé directement au et du nœud correspondant, tandis que l'autre est tunnelé à travers l'agent de rattachement. Si un attaquant est sur la liaison du nœud mobile et si la liaison actuelle du nœud mobile est une liaison sans fil non protégée, l'attaquant serait capable de voir les deux ensembles de messages, et de lancer des attaques sur ces bases (ces attaques sont discutées plus avant au paragraphe 15.4 de la spécification de base [RFC3775].) On peut empêcher l'attaque en s'assurant que les paquets tunnelés à travers l'agent de rattachement sont chiffrés.

Noter que la présente spécification ne concerne que les formats sans fil, et ne dicte aucun mécanisme spécifique de mise en œuvre. Dans le cas du mode tunnel IPsec, l'utilisation de l'encapsulation IP dans IP suivie par l'encapsulation IPsec en mode transport est aussi possible.

Les règles suivantes s'appliquent aux nœuds mobiles :

- Lorsque ESP est utilisé pour protéger les mises à jour de liens, 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 liens envoyées par les nœuds mobiles lorsque ils sont en dehors de chez eux. Une exception est lorsque le nœud mobile retourne chez lui et envoie une mise à jour de lien à l'agent de rattachement afin de se désenregistrer. Dans ce cas, aucune option Autre adresse d'entretien n'est nécessaire, comme décrit au paragraphe 3.1.

- Lorsque 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 de tunnel sortant à l'adresse d'entretien principale actuelle. Le nœud mobile commence à utiliser une nouvelle adresse d'entretien principale immédiatement après l'envoi d'une mise à jour de lien à l'agent de rattachement pour enregistrer cette nouvelle adresse. De même, il commence à utiliser la nouvelle adresse comme adresse de destination exigée des paquets tunnelés reçus de l'agent de rattachement.

Les règles suivantes s'appliquent aux agents de rattachement :

- Lorsque IPsec est utilisé pour protéger la signalisation d'acheminement de retour ou des paquets de charge utile, des associations de sécurité IPsec sont nécessaires pour assurer cette protection. Lorsque l'adresse d'entretien pour le nœud mobile change par suite d'une mise à jour de lien acceptée, un traitement spécial est nécessaire pour les prochains paquets 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 tunnelés reçus du nœud mobile.

De tels changements d'adresse peuvent être mis en œuvre, par exemple, par une API à partir de la mise en œuvre de IPv6 mobile vers la mise en œuvre IPsec. On notera que l'utilisation d'une telle API et de changements d'adresse DOIVENT être seulement faits sur la base des mises à jour de liens reçues par l'agent de rattachement et protégées par l'utilisation de IPsec. Les modifications d'adresse fondées sur d'autres sources, comme des mises à jour de liens aux nœuds correspondants protégés par l'acheminement de retour, ou l'accès ouvert à une API à partir d'une application peuvent résulter en des faiblesses de sécurité.

4.4 Chiffrement dynamique

Les exigences suivantes s'appliquent aux agents de rattachement et aux nœuds mobiles :

- Si la protection contre la répétition est exigée, le chiffrement dynamique DOIT être utilisé. IPsec ne peut fournir de protection contre la répétition que si le chiffrement dynamique est utilisé (ce qui peut n'être pas toujours le cas). IPsec ne garantit pas non plus l'ordre correct des paquets, mais seulement qu'ils n'ont pas été répétés. À cause de cela, les numéros de séquence au sein des messages IPv6 mobile sont utilisés pour s'assurer de l'ordre correct. Cependant, si l'espace de numéro de séquence de 16 bits de IPv6 mobile est entièrement parcouru, ou si l'agent de rattachement réamorce et perd son état concernant les numéros de séquence, des attaques en répétition et en réarrangement deviennent possibles. L'utilisation du chiffrement dynamique, de la protection IPsec anti-répétition, et les numéros de séquence IPv6 mobile peuvent ensemble empêcher de telles attaques.

- Si IKE version 1 est utilisé avec le secret pré partagés en mode principal, il détermine le secret partagé à utiliser à partir de l'adresse IP de l'homologue. Avec IPv6 mobile, cependant, cela peut être une adresse d'entretien et n'indique pas quel nœud mobile tente de contacter l'agent de rattachement. Donc, si l'authentification par secret pré partagé est utilisée dans IKEv1

entre le nœud mobile et l'agent de rattachement, le mode agressif DOIT alors être utilisé. Noter aussi qu'il faut apporter le plus grand soin au choix de l'identité dans la phase 1. Lorsque les charges utiles d'identité ID_IPV6_ADDR sont utilisées, une transposition non ambiguë des identités en clés n'est pas possible. (La prochaine version de IKE peut n'avoir pas ces limitations.)

Noter que les difficultés avec le mode principal et le secret pré partagés dans IKE version 1 sont bien connues pour les adresses dynamiques. Avec les adresses statiques, cela n'a pas posé de problème. Cependant, avec IPv6 mobile, l'utilisation des adresses d'entretien pour faire fonctionner IKE chez l'agent de rattachement présente un problème même lorsque l'adresse de rattachement reste stable. Des précisions sur l'utilisation de cette façon des adresses d'entretien sont données à la Section 7.

Les règles suivantes s'appliquent aux nœuds mobiles :

- En plus des règles ci-dessus, si le chiffrement dynamique est utilisé, le protocole de gestion de clés DOIT utiliser l'adresse d'entretien comme adresse de source dans les échanges de protocole avec l'agent de rattachement du nœud mobile.

- Cependant, les associations de sécurité IPsec avec l'agent de rattachement du nœud mobile utilisent les adresses de rattachement. C'est-à-dire que les associations de sécurité IPsec DOIVENT être demandées au protocole de gestion de clés en utilisant l'adresse de rattachement du nœud mobile comme identité du client. Les associations de sécurité pour protéger les mises à jour et les accusés de réception de liens sont demandées pour le protocole d'en-tête de mobilité en mode transport et pour les adresses IP spécifiques comme points d'extrémité. Aucun autre sélecteur n'est utilisé. De même, les associations de sécurité pour protéger la découverte de préfixe sont demandées pour le protocole ICMPv6 et les adresses IP spécifiques, là encore sans autre sélecteur. Les associations de sécurité pour la protection de la charge utile et l'acheminement de retour sont demandées pour une interface tunnel spécifique et soit le protocole de charge utile, soit le protocole d'en-tête de mobilité, en mode tunnel. Dans ce cas, un point d'extrémité demandé est une adresse IP et l'autre est un caractère générique, et il n'y a pas d'autre sélecteur.

- Si le nœud mobile a utilisé IKE version 1 pour établir les associations de sécurité avec son agent de rattachement, il devrait suivre les procédures discutées aux 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 IKE phase 1 doit être rétabli.

Les règles suivantes s'appliquent aux agents de rattachement :

- Si l'agent de rattachement a utilisé IKE version 1 pour établir des associations de sécurité avec le nœud mobile, il devrait suivre les procédures discutées aux 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 IKE phase 1 doit être rétabli.

5. Exemples de configurations

Dans ce qui suit, on décrit les entrées de base de données de politique de sécurité (SPD, *Security Policy Database*) et de base de données d'associations de sécurité (SAD, *Security Association Database*) nécessaires pour protéger les mises à jour de liens et des accusés de réception de lien échangés entre le nœud mobile et l'agent de rattachement.

Le paragraphe 5.1 introduit le format qu'on utilise pour décrire la SPD et la SAD. Le paragraphe 5.2 décrit comment configurer manuellement les associations de sécurité IPsec chiffrées sans chiffrement dynamique, et le paragraphe 5.3 décrit comment utiliser le chiffrement dynamique.

5.1 Format

Le format utilisé dans les exemples est le suivant. La description SPD a le format

```
<nœud> "SPD OUT:"
  "-" <spdentrée>
  "-" <spdentrée>
  ...
  "-" <spdentrée>

<nœud> "SPD IN:"
  "-" <spdentrée>
  "-" <spdentrée>
  ...
  "-" <spdentrée>
```

où <nœud> représente le nom du nœud, et <spdentrée> a le format suivant :

```
 "SI" <condition> "ALORS UTILISER SA " <sa> |
 "SI" <condition> "ALORS UTILISER SA " <pattern> |
```

où <condition> est une expression booléenne sur les champs du paquet IPv6, <sa> est le nom d'une association de sécurité spécifique, et <pattern> est une spécification pour une association de sécurité à négocier via IKE [RFC2409]. La description de SAD a le format

```
 <nœud> "SAD:"
  "-" <sadentrée>
  "-" <sadentrée>
  ...
  "-" <sadentrée>
```

où <nœud> représente le nom du nœud, et <sadentrée> a le format suivant :

```
 <sa> "(" <dir> ","
        <spi> ","
        <destination> ","
        <ipsec-proto> ","
        <mode> ")" ":"
     <règle>
```

où <dir> est "IN" ou "OUT", <spi> est le SPI de l'association de sécurité, <destination> est sa destination, <ipsec-proto> est dans notre cas "ESP", <mode> est soit "TUNNEL" soit "TRANSPORT", et <règle> est une expression qui décrit les sélecteurs IPsec, c'est-à-dire, quels champs du paquet IPv6 doivent avoir quelles valeurs.

On va dans cette section utiliser un exemple de nœud mobile qui a une adresse de rattachement "adresse_rattach_1". L'identité de l'usager dans ce nœud mobile est "usager_1". L'adresse de l'agent de rattachement est "agent_rattach_1".

5.2. Configuration manuelle

5.2.1 Mises à jour et accusés de réception de lien

Voici les contenus de la SPD et de la SAD pour protéger les mises à jour de liens et les accusés de réception :

nœud mobile SPD OUT :
- SI source = adresse_rattach_1 & destination = agent_rattach_1 & proto = En-tête Mobility (MH, *Mobility Header*)
  ALORS UTILISER SA SA1

nœud mobile SPD IN :
- SI source = agent_rattach_1 & destination = adresse_rattach_1 & proto = MH
  ALORS UTILISER SA SA2

nœud mobile SAD :
- SA1(OUT, spi_a, agent_rattach_1, ESP, TRANSPORT) :
  source = adresse_rattach_1 & destination = agent_rattach_1 & proto = MH
- SA2(IN, spi_b, adresse_rattach_1, ESP, TRANSPORT) :
  source = agent_rattach_1 & destination = adresse_rattach_1 & proto = MH

agent de rattachement SPD OUT :
- SI source = agent_rattach_1 & destination = adresse_rattach_1 & proto = MH
  ALORS UTILISER SA SA2

agent de rattachement SPD IN :
- SI source = adresse_rattach_1 & destination = agent_rattach_1 & proto = MH
  ALORS UTILISER SA SA1

agent de rattachement SAD :
- SA2(OUT, spi_b, adresse_rattach_1, ESP, TRANSPORT) :
  source = agent_rattach_1 & destination = adresse_rattach_1 & proto = MH

- SA1(IN, spi_a, agent_rattach_1, ESP, TRANSPORT) :
  source = adresse_rattach_1 & destination = agent_rattach_1 & proto = MH

Dans ce qui précède, "MH" se réfère au numéro de protocole d'en-tête de mobilité [RFC3775].

5.2.2 Signalisation de possibilité d'acheminement en retour

Dans ce qui suit, on décrit les entrées nécessaires de SPD et SAD pour protéger la signalisation d'acheminement de retour entre le nœud mobile et l'agent de rattachement. Noter que les règles dans la SPD sont ordonnées, et que celles du paragraphe précédent doivent avoir la préséance sur celles-ci. En d'autres termes, les entrées de plus forte préséance doivent se présenter en premier dans la liste ordonnée d'entrées de SPD de la [RFC2401].

nœud mobile SPD OUT :
- SI interface = tunnel IPv6 avec agent_rattach_1 &
  source = adresse_rattach_1 & destination = toute & proto = MH
  ALORS UTILISER SA SA3

nœud mobile SPD IN :
- SI interface = tunnel IPv6 provenant de agent_rattach_1 & source = toute & destination = adresse_rattach_1 & proto = MH
  ALORS UTILISER SA SA4

nœud mobile SAD :
- SA3(OUT, spi_c, agent_rattach_1, ESP, TUNNEL) :
  source = adresse_rattach_1 & destination = toute & proto = MH
- SA4(IN, spi_d, care_of_address_1, ESP, TUNNEL) :
  source = toute & destination = adresse_rattach_1 & proto = MH

agent de rattachement SPD OUT :
- SI interface = tunnel IPv6 vers adresse_rattach_1 & source = toute & destination = adresse_rattach_1 & proto = MH
  ALORS UTILISER SA SA4

agent de rattachement SPD IN :
- SI interface = tunnel IPv6 provenant de adresse_rattach_1 & source = adresse_rattach_1 & destination = toute & proto = MH
  ALORS UTILISER SA SA3

agent de rattachement SAD :
- SA4(OUT, spi_d, care_of_address_1, ESP, TUNNEL) :
  source = toute & destination = adresse_rattach_1 & proto = MH
- SA3(IN, spi_c, agent_rattach_1, ESP, TUNNEL) :
  source = adresse_rattach_1 & destination = toute & proto = MH

L'association de sécurité provenant de l'agent de rattachement avec le nœud mobile utilise l'adresse d'entretien courante comme destination. Comme indiqué précédemment, cette adresse est mise à jour dans la SAD lorsque le nœud mobile se déplace. Il peut être initialisé à l'adresse de rattachement avant que le nœud mobile se soit enregistré.

5.2.3 Découverte du préfixe

Dans ce qui suit, on décrit des entrées supplémentaires de SPD et de SAD pour protéger la découverte de préfixe. Noter que les SPD décrites ci-dessus protègent tout le trafic ICMPv6 entre le nœud mobile et l'agent de rattachement, car IPsec peut n'avoir pas la capacité de distinguer entre les différents types ICMPv6.

nœud mobile SPD OUT :
- SI source = adresse_rattach_1 & destination = agent_rattach_1 & proto = ICMPv6
  ALORS UTILISER SA SA5.

nœud mobile SPD IN :
- SI source = agent_rattach_1 & destination = adresse_rattach_1 & proto = ICMPv6
  ALORS UTILISER SA SA6

nœud mobile SAD :
- SA5(OUT, spi_e, agent_rattach_1, ESP, TRANSPORT) :
  source = adresse_rattach_1 & destination = agent_rattach_1 & proto = ICMPv6

- SA6(IN, spi_f, adresse_rattach_1, ESP, TRANSPORT) :
  source = agent_rattach_1 & destination = adresse_rattach_1 & proto = ICMPv6

agent de rattachement SPD OUT :
- SI source = agent_rattach_1 & destination = adresse_rattach_1 & proto = ICMPv6
  ALORS UTILISER SA SA6

agent de rattachement SPD IN :
- SI source = adresse_rattach_1 & destination = agent_rattach_1 & proto = ICMPv6
  ALORS UTILISER SA SA5

agent de rattachement SAD :
- SA6(OUT, spi_f, adresse_rattach_1, ESP, TRANSPORT) :
  source = agent_rattach_1 & destination = adresse_rattach_1 & proto = ICMPv6
- SA5(IN, spi_e, agent_rattach_1, ESP, TRANSPORT) :
  source = adresse_rattach_1 & destination = agent_rattach_1 & proto = ICMPv6

5.2.4 Paquets de charge utile

Il est aussi possible d'effectuer une protection supplémentaire facultative des paquets de charge utile tunnelés. Cette protection a lieu d'une façon similaire à la protection d'acheminement de retour décrite ci-dessus, mais exige une valeur différente pour le champ Protocole. Les entrées de SPD et SAD nécessaires sont montrées ci-dessous. On suppose que les entrées pour protéger les mises à jour de liens et les accusés de réception, et les entrées pour protéger les messages Initialisation d'essai de rattachement et Essai de rattachement ont la préséance sur ces entrées.

nœud mobile SPD OUT :
- SI interface = tunnel IPv6 vers agent_rattach_1 & source = adresse_rattach_1 & destination = toute & proto = X
  ALORS UTILISER SA SA7

nœud mobile SPD IN :
- SI interface = tunnel IPv6 provenant de agent_rattach_1 & source = toute & destination = adresse_rattach_1 & proto = X
  ALORS UTILISER SA SA8

nœud mobile SAD:
- SA7(OUT, spi_g, agent_rattach_1, ESP, TUNNEL) :
  source = adresse_rattach_1 & destination = toute & proto = X
- SA8(IN, spi_h, care_of_address_1, ESP, TUNNEL) :
  source = toute & destination = adresse_rattach_1 & proto = X

agent de rattachement SPD OUT :
- SI interface = tunnel IPv6 vers adresse_rattach_1 & source = toute & destination = adresse_rattach_1 & proto = X
  ALORS UTILISER SA SA8

agent de rattachement SPD IN :
- SI interface = tunnel IPv6 provenant de adresse_rattach_1 & source = adresse_rattach_1 & destination = toute & proto = X
  ALORS UTILISER SA SA7

agent de rattachement SAD :
- SA8(OUT, spi_h, care_of_address_1, ESP, TUNNEL) :
  source = toute & destination = adresse_rattach_1 & proto = X
- SA7(IN, spi_g, agent_rattach_1, ESP, TUNNEL) :
  source = adresse_rattach_1 & destination = toute & proto = X

Si des protocoles de contrôle de l'adhésion à des groupes de diffusion groupée comme MLDv1 [RFC2710] ou MLDv2 [RFC3810] ont besoin d'être protégés, ces paquets peuvent utiliser une adresse de liaison locale plutôt que l'adresse de rattachement du nœud mobile. Dans ce cas, la source et la destination peuvent être laissées comme des caractères génériques et les entrées de la SPD vont fonctionner sur la seule base de l'interface utilisée et du protocole, qui est ICMPv6 pour MLDv1 et MLDv2.

Des problèmes similaires se rencontrent lorsque des protocoles d'autoconfiguration d'adresse à états pleins tels que DHCPv6 [RFC3315] sont utilisés. La même approche est applicable aussi pour DHCPv6. DHCPv6 utilise le protocole UDP.

La prise en charge de plusieurs couches d'encapsulation (comme ESP encapsulé dans ESP) n'est pas exigée par la [RFC2401] et est aussi souvent problématique par ailleurs. Il est donc utile d'éviter de régler le protocole X dans les entrées ci-dessus à AH

ou ESP.

5.3 Chiffrement dynamique

Dans ce paragraphe, on montre un exemple de configuration qui utilise IKE pour négocier les associations de sécurité.

5.3.1 Mises à jour et accusés de réception de liens

Voici les contenus de la SPD pour protéger les mises à jour de liens et les accusés de réception :

nœud mobile SPD OUT :
- SI source = adresse_rattach_1 & destination = agent_rattach_1 & proto = MH
  ALORS UTILISER SA ESP TRANSPORT: identité locale de phase 1 = usager_1

nœud mobile SPD IN :
- SI source = agent_rattach_1 & destination = adresse_rattach_1 & proto = MH
  ALORS UTILISER SA ESP TRANSPORT : identité locale de phase 1 = usager_1

agent de rattachement SPD OUT :
- SI source = agent_rattach_1 & destination = adresse_rattach_1 & proto = MH
  ALORS UTILISER SA ESP TRANSPORT : identité d'homologue de phase 1 = usager_1

agent de rattachement SPD IN :
- SI source = adresse_rattach_1 & destination = agent_rattach_1 & proto = MH
  ALORS UTILISER SA ESP TRANSPORT : identité d'homologue de phase 1 = usager_1

On a omis les détails des transformations proposées ci-dessus, et tous les détails relatifs à la méthode d'authentification particulière comme les certificats allant au delà de la liste d'identités spécifiques qui doit être utilisée.

Il est exigé que IKE version 1 soit utilisé avec les adresses d'entretien mais on négocie quand même les SA IPsec qui utilisent les adresses de rattachement. Les conditions supplémentaires établies par la SDP de l'agent de rattachement pour que l'identité de l'homologue de phase 1 soit "usager_1" doivent être vérifiées par l'agent de rattachement. L'objet de la condition est de s'assurer que la négociation IKE phase 2 pour l'adresse de rattachement d'un certain usager ne soit pas demandée par un autre usager. Dans le nœud mobile, on règle simplement notre identité locale comme étant "usager_1".

Ces vérifications impliquent aussi que la configuration de l'agent de rattachement soit spécifique de l'usager : tout usager ou adresse de rattachement exige une entrée de configuration spécifique. Il serait possible d'alléger les tâches de configuration en utilisant des certificats qui aient des adresses de rattachement dans le champ Subject AltName. Cependant, il n'est pas clair que toutes les mises en œuvre IKE permettent qu'une adresse soit utilisée pour porter les négociations IKE alors qu'une autre adresse est mentionnée dans les certificats utilisés. Dans tous les cas, même cette approche aurait exigé des tâches spécifiques de l'usager dans l'autorité de certification.

5.3.2 Signalisation de possibilité d'acheminement en retour

La protection de la signalisation de l'acheminement de retour peut être configurée d'une façon similaire à celle ci-dessus.

nœud mobile SPD OUT :
- SI interface = tunnel IPv6 vers agent_rattach_1 & source = adresse_rattach_1 & destination = toute & proto = MH
  ALORS UTILISER SA ESP TUNNEL : destination externe = agent_rattach_1 & identité locale de phase 1 = usager_1

nœud mobile SPD IN :
- SI interface = tunnel IPv6 provenant de agent_rattach_1 & source = toute & destination = adresse_rattach_1 & proto = MH
  ALORS UTILISER SA ESP TUNNEL : destination externe = agent_rattach_1 & identité locale de phase 1 = usager_1

agent de rattachement SPD OUT :
- SI interface = tunnel IPv6 vers adresse_rattach_1 & source = toute & destination = adresse_rattach_1 & proto = MH
ALORS UTILISER SA ESP TUNNEL : destination externe = adresse_rattach_1 & identité d'homologue phase 1 = usager_1

agent de rattachement SPD IN :
- SI interface = tunnel IPv6 venant de adresse_rattach_1 & source = adresse_rattach_1 & destination = toute & proto = MH
  ALORS UTILISER SA ESP TUNNEL : destination externe = adresse_rattach_1 & identité d'homologue phase 1 = usager_1

L'association de sécurité venant de l'agent de rattachement avec le nœud mobile utilise l'adresse d'entretien courante comme destination. Comme mentionné précédemment, cette adresse est mise à jour dans la SAD lorsque le nœud mobile bouge.
Les entrées de SPD peuvent être écrites en utilisant l'adresse de rattachement (comme ci-dessus) si la mise à jour de l'adresse d'entretien dans la SAD est aussi faite à la création des associations de sécurité.

5.3.3 Découverte de préfixe

Dans ce qui suit, on décrit des entrées supplémentaires de SPD pour protéger la découverte de préfixe avec IKE. (Noter que lorsque de nouveaux préfixes réels sont découverts, il peut être nécessaire d'entrer de nouvelles entrées de SPD configurées manuellement pour spécifier la politique d'autorisation pour les nouvelles adresses de rattachement résultantes.)

nœud mobile SPD OUT :
- SI source = adresse_rattach_1 & destination = agent_rattach_1 & proto = ICMPv6
  ALORS UTILISER SA ESP TRANSPORT : identité locale de phase 1 = usager_1

nœud mobile SPD IN :
- SI source = agent_rattach_1 & destination = adresse_rattach_1 &proto = ICMPv6
  ALORS UTILISER SA ESP TRANSPORT : identité locale de phase 1 = usager_1

agent de rattachement SPD OUT :
- SI source = agent_rattach_1 & destination = adresse_rattach_1 & proto = ICMPv6
  ALORS UTILISER SA ESP TRANSPORT : identité d'homologue de phase 1 = usager_1

agent de rattachement SPD IN :
- SI source = adresse_rattach_1 & destination = agent_rattach_1 & proto = ICMPv6
  ALORS UTILISER SA ESP TRANSPORT : identité d'homologue de phase 1 = usager_1

5.3.4 Paquets de charge utile

La protection pour les paquets de charge utile se fait de façon similaire à celle de la signalisation d'acheminement de retour. Comme dans le cas du chiffrement manuel, ces entrées de SPD ont une priorité inférieure à celles de ci-dessus.

nœud mobile SPD OUT :
- SI interface = tunnel IPv6 vers agent_rattach_1 & source = adresse_rattach_1 & destination = toute & proto = X
  ALORS UTILISER SA ESP TUNNEL : destination externe = agent_rattach_1 & identité locale de phase 1 = usager_1

nœud mobile SPD IN :
- SI interface = tunnel IPv6 provenant de agent_rattach_1 & source = toute & destination = adresse_rattach_1 & proto = X
  ALORS UTILISER SA ESP TUNNEL : destination externe = agent_rattach_1 & identité locale de phase 1 = usager_1

agent de rattachement SPD OUT :
- SI interface = tunnel IPv6 vers adresse_rattach_1 & source = toute, destination = adresse_rattach_1 & proto = X
  ALORS UTILISER SA ESP TUNNEL : destination externe = adresse_rattach_1 &identité d'homologue phase 1 = usager_1

agent de rattachement SPD IN :
- SI interface = tunnel IPv6 venant de adresse_rattach_1 & source = adresse_rattach_1 & destination = toute & proto = X
  ALORS UTILISER SA ESP TUNNEL : destination externe = adresse_rattach_1 & identité d'homologue phase 1 = usager_1

6. Étapes du traitement au sein d'un nœud

6.1 Mise à jour du lien avec l'agent de rattachement

Étape 1. Au nœud mobile, le module IPv6 mobile produit d'abord le paquet suivant :

En-tête IPv6 (source = adresse de rattachement, destination = agent de rattachement)
En-tête Mobility Mise à jour de lien

Étape 2. Ce paquet est confronté à la SPD IPsec sur le nœud mobile et on note que IPsec doit être appliqué.

Étape 3. Puis, on ajoute les options IPv6 mobile nécessaires mais on ne change pas encore les adresses, comme décrit au paragraphe 11.3.2 de la spécification de base [RFC3775]. Il en résulte :

En-tête IPv6 (source = adresse de rattachement, destination = agent de rattachement)
En-tête Options de destination : Options d'adresse de rattachement (adresse d'entretien)
En-tête Mobility : Mise à jour de lien

Étape 4. Finalement, les en-têtes IPsec sont ajoutés et les valeurs d'authentifiant nécessaires sont calculées :

En-tête IPv6 (source = adresse de rattachement, destination = agent de rattachement)
En-tête Options de destination : Options d'adresse de rattachement (adresse d'entretien)
En-tête ESP (SPI = spi_a)
En-tête Mobility : Mise à jour de lien

Ici, spi_a est la valeur de SPI qui a été soit configurée manuellement, soit acceptée dans une négociation IKE antérieure.

Étape 5. Avant d'envoyer le paquet, les adresses dans l'en-tête IPv6 et dans l'en-tête Options de Destination sont changées :

En-tête IPv6 (source = adresse d'entretien, destination = agent de rattachement)
En-tête Options de destination : Options d'adresse de rattachement (adresse de rattachement)
En-tête ESP (SPI = spi_a)
En-tête Mobility : Mise à jour de lien

6.2 Mise à jour du lien provenant du nœud mobile

Étape 1. Le paquet suivant est reçu à l'agent de rattachement :

En-tête IPv6 (source = adresse d'entretien, destination = agent de rattachement)
En-tête Options de destination : Options d'adresse de rattachement (adresse de rattachement)
En-tête ESP (SPI = spi_a)
En-tête Mobility : Mise à jour de lien

Étape 2. L'option d'adresse de rattachement est traitée en premier, d'où il résulte

En-tête IPv6 (source = adresse de rattachement, destination = agent de rattachement)
En-tête Options de destination : Options d'adresse de rattachement (adresse d'entretien)
En-tête ESP (SPI = spi_a)
En-tête Mobility : Mise à jour de lien

Étape 3. L'en-tête ESP est traité ensuite, d'où il résulte :

En-tête IPv6 (source = adresse de rattachement, destination = agent de rattachement)
En-tête Options de destination : Options d'adresse de rattachement (adresse d'entretien)
En-tête Mobility : Mise à jour de lien

Étape 4. Ce paquet correspond à la politique exigée pour cette association de sécurité (source = adresse de rattachement, destination = agent de rattachement, proto = MH).

Étape 5. IPv6 mobile traite la mise à jour de lien. La mise à jour de lien est livrée au module IPv6 mobile.

Étape 6. Si il y a des associations de sécurité dans la base de données des associations de sécurité pour la protection de l'acheminement de retour ou des paquets de charge utile pour ce nœud mobile, ces associations de sécurité sont mises à jour avec la nouvelle adresse d'entretien.

6.3 Accusé de réception du lien vers le nœud mobile

Étape 1. IPv6 mobile produit le paquet: suivant :

En-tête IPv6 (source = agent de rattachement, destination = adresse de rattachement)
En-tête Mobility : Accusé de réception de lien

Étape 2. Ce paquet correspond aux entrées de politique IPsec, et on se souvient qu'IPsec doit être appliqué.

Étape 3. Puis on ajoute les en-têtes Route nécessaires mais on ne change pas encore les adresses, comme décrit au

paragraphe 9.5.4 de la spécification de base [RFC3775]. Il en résulte :

En-tête IPv6 (source = agent de rattachement, destination = adresse de rattachement)
En-tête Routing (type 2) : Adresse d'entretien
En-tête Mobility : Accusé de réception de lien

Étape 4. On applique IPsec :

En-tête IPv6 (source = agent de rattachement, destination = adresse de rattachement)
En-tête Routing(type 2) : Adresse d'entretien
En-tête ESP (SPI = spi_b)
En-tête Mobility : Accusé de réception de lien

Étape 5. Finalement, avant d'envoyer le paquet, on change les adresses dans l'en-tête IPv6 et l'en-tête Route :

En-tête IPv6 (source = agent de rattachement, destination = adresse d'entretien)
En-tête Routing (type 2) : Adresse de rattachement
En-tête ESP (SPI = spi_b)
En-tête Mobility : Accusé de réception de lien

6.4 Accusé de réception du lien provenant de l'agent de rattachement

Étape 1. Le paquet suivant est reçu au nœud mobile

En-tête IPv6 (source = agent de rattachement, destination = adresse d'entretien)
En-tête Routing (type 2) : Adresse de rattachement
En-tête ESP (SPI = spi_b)
En-tête Mobility : Accusé de réception de lien

Étape 2. Après le traitement de l'en-tête d'acheminement, le paquet devient :

En-tête IPv6 (source = agent de rattachement, destination = adresse de rattachement)
En-tête Routing (type 2) : Adresse d'entretien
En-tête ESP (SPI = spi_b)
En-tête Mobility : Accusé de réception de lien

Étape 3. L'en-tête ESP est traité ensuite, ce qui donne :

En-tête IPv6 (source = agent de rattachement, destination = adresse de rattachement)
En-tête Routing (type 2) : Adresse d'entretien
En-tête Mobility : Accusé de réception de lien

Étape 4. Ce paquet correspond à la politique exigée pour cette association de sécurité (source = agent de rattachement, destination = adresse de rattachement, proto = MH).

Étape 5. L'accusé de réception de lien est livré au module IPv6 mobile.

6.5 Initialisation de l'essai de rattachement à l'agent de rattachement

Étape 1. Le nœud mobile construit un message Initialisation d'essai de rattachement :

En-tête IPv6 (source = adresse de rattachement, destination = nœud correspondant)
En-tête Mobility : Initialisation d'essai de rattachement

Étape 2. IPv6 mobile détermine que ce paquet devrait aller au tunnel pour l'agent de rattachement.

Étape 3. Le paquet est confronté aux entrées de politique IPsec pour l'interface, et on trouve que IPsec doit être appliqué.

Étape 4. On ajoute les en-têtes IPsec mode tunnel. Noter qu'on utilise une adresse d'entretien comme adresse de source pour le paquet tunnelé.

En-tête IPv6 (source = adresse d'entretien, destination = agent de rattachement)

En-tête ESP (SPI = spi_c)
En-tête IPv6 (source = adresse de rattachement, destination = nœud correspondant)
En-tête Mobility : Initialisation d'essai de rattachement

Étape 5. Le paquet est envoyé directement à l'agent de rattachement en utilisant l'encapsulation IPsec.

6.6 Initialisation de l'essai de rattachement en provenance du nœud mobile

Étape 1. L'agent de rattachement reçoit le paquet suivant :

En-tête IPv6 (source = adresse d'entretien, destination = agent de rattachement)
En-tête ESP (SPI = spi_c)
En-tête IPv6 (source = adresse de rattachement, destination = nœud correspondant)
En-tête Mobility : Initialisation d'essai de rattachement

Étape 2. Le traitement IPsec est effectué, ce qui donne :

En-tête IPv6 (source = adresse de rattachement, destination = nœud correspondant)
En-tête Mobility : Initialisation d'essai de rattachement

Étape 3. Le paquet résultant correspond à la politique requise pour cette association de sécurité et le traitement du paquet peut continuer.

Étape 4. Le paquet est alors transmis au nœud correspondant.

6.7 Essai de rattachement avec le nœud mobile

Étape 1. L'agent de rattachement reçoit un paquet Essai de rattachement provenant du nœud correspondant :

En-tête IPv6 (source = nœud correspondant, destination = adresse de rattachement)
En-tête Mobility : Initialisation d'essai de rattachement

Étape 2. L'agent de rattachement détermine que ce paquet est destiné à un nœud mobile qui est en déplacement, et décide de le tunneler.

Étape 3. Le paquet correspond aux entrées de politique pour l'interface de tunnel, et on note que IPsec doit être appliqué.

Étape 4. IPsec est appliqué, ce qui résulte en un nouveau paquet. Noter que l'agent de rattachement doit garder trace de la localisation du nœud mobile, et mettre à jour en conséquence l'adresse du point d'extrémité du tunnel dans la ou les associations de sécurité.

En-tête IPv6 (source = agent de rattachement, destination = adresse d'entretien)
En-tête ESP (SPI = spi_d)
En-tête IPv6 (source = nœud correspondant, destination = adresse de rattachement)
En-tête Mobility : Initialisation d'essai de rattachement

Étape 5. Le paquet est envoyé directement à l'adresse d'entretien en utilisant l'encapsulation IPsec.

6.8 Essai de rattachement depuis l'agent de rattachement

Étape 1. Le nœud mobile reçoit le paquet suivant :

En-tête IPv6 (source = agent de rattachement, destination = adresse d'entretien)
En-tête ESP (SPI = spi_d)
En-tête IPv6 (source = nœud correspondant, destination = adresse de rattachement)
En-tête Mobility : Initialisation d'essai de rattachement

Étape 2. IPsec est traité, ce qui donne :

En-tête IPv6 (source = nœud correspondant, destination = adresse de rattachement)
En-tête Mobility : Initialisation d'essai de rattachement

Étape 3. Cela correspond à la politique requise pour cette association de sécurité (source = toute, destination = adresse de rattachement).

Étape 4. Le paquet est passé au traitement IPv6 mobile.

6.9 Message de sollicitation de préfixe à l'agent de rattachement

Cette procédure est similaire à celle présentée au paragraphe 6.1.

6.10 Message de sollicitation de préfixe de la part du nœud mobile

Cette procédure est similaire à celle présentée au paragraphe 6.2.

6.11 Message d'annonce de préfixe au nœud mobile

Cette procédure est similaire à celle présentée au paragraphe 6.3.

6.12 Message d'annonce de préfixe provenant de l'agent de rattachement

Cette procédure est similaire à celle présentée au paragraphe 6.4.

6.13 Paquet de charge utile à l'agent de rattachement

Cette procédure est similaire à celle présentée au paragraphe 6.5.

6.14 Paquet de charge utile provenant de l'agent mobile

Cette procédure est similaire à celle présentée au paragraphe 6.6.

6.15 Paquet de charge utile au nœud mobile

Cette procédure est similaire à celle présentée au paragraphe 6.7.

6.16 Paquet de charge utile provenant de l'agent de rattachement

Cette procédure est similaire à celle présentée au paragraphe 6.8.

6.17 Établissement de nouvelles associations de sécurité

Étape 1. Le nœud mobile souhaite envoyer une Mise à jour de lien à l'agent de rattachement.

En-tête IPv6 (source = adresse de rattachement, destination = agent de rattachement)
En-tête Mobility : Mise à jour de lien

Étape 2. Il n'existe pas d'association de sécurité pour protéger la mise à jour de lien, de sorte que le nœud mobile initie IKE. Les paquets IKE sont envoyés comme montré dans les exemples suivants. Le premier paquet est un exemple de paquet IKE envoyé du nœud mobile, et le second est envoyé de l'agent de rattachement. Les exemples montrent aussi que l'identité de phase 1 utilisée pour le nœud mobile est un FQDN.

En-tête IPv6 (source = adresse d'entretien, destination = agent de rattachement)
    UDP
    IKE
      ... IDii = ID_FQDN mn123.ha.net ...

En-tête IPv6 (source = agent de rattachement, destination = adresse d'entretien)
    UDP
    IKE
      ... IDir = ID_FQDN ha.net ...

Étape 3. IKE phase 1 s'achève, et la phase 2 est initiée pour demander des associations de sécurité pour protéger le trafic entre

l'adresse de rattachement du nœud mobile et l'agent de rattachement. Ces adresses seront utilisées comme sélecteurs. Cela implique d'envoyer et recevoir des paquets IKE supplémentaires. L'exemple ci-dessous montre encore un paquet envoyé par le nœud mobile et un autre envoyé par l'agent de rattachement. L'exemple montre aussi que l'identité de phase 2 utilisée pour le nœud mobile est l'adresse de rattachement du nœud mobile.

En-tête IPv6 (source = adresse d'entretien, destination = agent de rattachement)
UDP
IKE
... IDci = ID_IPV6_ADDR adresse de rattachement ...

En-tête IPv6 (source = agent de rattachement, destination = adresse d'entretien)
UDP
IKE
... IDcr = ID_IPV6_ADDR agent de rattachement ...

Étape 4. Les étapes suivantes sont identiques à celles montrées au paragraphe 6.1.

6.18 Changement de clé des associations de sécurité

Étape 1. Le nœud mobile et l'agent de rattachement ont des associations de sécurité existantes. L'un ou l'autre côté peut décider à tout moment que les clés des associations de sécurité doivent être changées, par exemple, parce que la durée de vie spécifiée approche de sa fin.

Étape 2. Les paquets d'en-tête de mobilité envoyés durant le changement de clé peuvent être protégés par les associations de sécurité existantes.

Étape 3. Lorsque le changement de clés est fini, de nouvelles associations de sécurité sont établies. En pratique, il y a un intervalle de temps durant lequel une ancienne association de sécurité sur le point de se terminer et une association de sécurité nouvellement établie vont toutes deux exister. La nouvelle devrait être utilisée aussitôt qu'elle devient disponible.

Étape 4. Une notification de la suppression des vieilles associations de sécurité est reçue. Après cela, seules les nouvelles associations de sécurité peuvent être utilisées.

Noter qu'il n'est pas exigé que l'existence des associations de sécurité IPsec et IKE soit liée à l'existence des liens. Il n'est pas nécessaire de supprimer une association de sécurité si un lien est supprimé, car un nouveau lien peut être établi peu après cela.

Comme les matériels d'accélération cryptographique peuvent être seulement capables de traiter un nombre limité d'associations de sécurité actives, des associations de sécurité peuvent être supprimées via IKE afin de réduire à un minimum le nombre de contextes de chiffrement actifs. De telles suppressions ne devraient pas être interprétées comme le signe d'une perte de contact avec l'homologue ou comme une raison de supprimer un lien. Si du trafic supplémentaire doit être envoyé, il est plutôt préférable d'amener une autre association de sécurité pour le protéger.

6.19 Mouvements et changement de clés dynamique

On décrit dans ce paragraphe une séquence d'événements qui se rapportent au mouvement avec des associations de sécurité fondées sur IKE. Dans l'état initial, le nœud mobile n'est pas enregistré dans un site et n'a pas d'association de sécurité avec l'agent de rattachement. Selon que les homologues seront capables de déplacer les points d'extrémité IKE aux nouvelles adresses d'entretien, les actions prises dans les étapes 9 et 10 sont différentes.

Étape 1. Le nœud mobile avec l'adresse de rattachement A se déplace à l'adresse d'entretien B.

Étape 2. Le nœud mobile lance IKE à partir de l'adresse d'entretien B avec l'agent de rattachement, établissant une phase 1. L'agent de rattachement peut seulement agir comme répondant avant de savoir la localisation actuelle du nœud mobile.

Étape 3. Protégé par cette phase 1, le nœud mobile établit une paire d'associations de sécurité pour protéger le trafic d'en-tête de mobilité de et vers l'adresse de rattachement A.

Étape 4. Le nœud mobile envoie une mise à jour de lien et reçoit un accusé de réception de lien en utilisant les associations de sécurité créées à l'étape 3.

Étape 5. Le nœud mobile établit une paire d'associations de sécurité pour protéger les paquets d'acheminement de retour. Ces associations de sécurité sont en mode tunnel et leur point d'extrémité du côté du nœud mobile est l'adresse d'entretien B. Pour les besoins de notre exemple, cette étape utilise la connexion de phase 1 établie à l'étape 2. Plusieurs connexions de phase 1

sont aussi possibles.

Étape 6. Le nœud mobile utilise les associations de sécurité créées dans l'étape 5 pour faire fonctionner l'acheminement de retour.

Étape 7. Le nœud mobile passe à une nouvelle localisation et adopte une nouvelle adresse d'entretien C.

Étape 8. Le nœud mobile envoie une mise à jour de lien et reçoit un accusé de réception de lien en utilisant les associations de sécurité créées à l'étape 3. L'agent de rattachement s'assure que les prochains paquets envoyés en utilisant les associations de sécurité créées à l'étape 5 vont avoir la nouvelle adresse d'entretien comme adresse de destination, comme si l'adresse de destination de l'en-tête externe dans l'association de sécurité avait changé.

Étape 9. Si le nœud mobile et l'agent de rattachement avaient la capacité de changer les points d'extrémité IKE, ils changent l'adresse en C. Si ils n'ont pas cette capacité, les deux nœuds suppriment leurs connexions de phase 1 créées par dessus l'adresse d'entretien B et vont établir une nouvelle phase 1 IKE par dessus l'adresse d'entretien C. Cette capacité de changer les points d'extrémité IKE phase 1 est indiquée par l'établissement du fanion Capacité de gestion de clé de mobilité (K) [RFC3775] dans les messages Mise à jour de lien et accusé de réception de lien.

Étape 10. Si une nouvelle connexion IKE phase 1 a été établie après le mouvement, le nœud mobile ne sera pas capable de recevoir de notifications livrées par dessus l'ancienne association de sécurité IKE phase 1. Les notifications livrées par dessus la nouvelle association de sécurité sont reçues et traitées normalement. Si le nœud mobile et l'agent de rattachement étaient capables de mettre à jour les points d'extrémité IKE, ils peuvent continuer en utilisant la même connexion IKE phase 1.

7. Considérations de mise en œuvre

7.1 IPsec

Noter que les formats de paquet et l'ordre des en-têtes discutés à la Section 3 doivent être pris en charge, mais les mises en œuvre peuvent aussi accepter d'autres formats. En général, l'utilisation de formats non exigés ici peut conduire à un traitement incorrect des paquets par l'homologue (comme leur élimination en silence) sauf si la prise en charge de ces formats a été vérifiée hors ligne. Une telle vérification peut avoir lieu en même temps que l'accord sur les paramètres des associations de sécurité. Dans certains cas, cependant, les spécifications de base de IPv6 appellent à la prise en charge d'options qui ne sont pas discutées ici. Dans ces cas, une telle étape de vérification peut être inutile tant que l'homologue prend pleinement en charge les spécifications IPv6 pertinentes. Cependant, le présent document ne fait aucune hypothèse sur la validité de ces autres formats dans le contexte de IPv6 mobile. Il est aussi vraisemblable que les systèmes qui prennent en charge IPv6 mobile ont été abondamment vérifiés avec les formats exigés.

On a choisi d'exiger un format d'encapsulation pour la protection des paquets d'acheminement de retour et des paquets de charge utile qui ne peut être réalisé que si la destination des paquets IPsec envoyés depuis l'agent de rattachement peut être changée lorsque le nœud mobile bouge. Une des principales raisons du choix d'un tel format est qu'il supprime la redondance de vingt quatre octets lorsque une option d'adresse de rattachement ou un en-tête d'acheminement est ajouté au paquet tunnelé. Une telle redondance ne serait pas significative pour la protection des paquets d'acheminement de retour, mais créerait une redondance supplémentaire si IPsec est utilisé pour protéger le tunnelage des paquets de charge utile à l'agent de rattachement. Cette redondance peut être significative pour le trafic en temps réel. Étant donné que l'utilisation de formats de paquet plus courts pour tout trafic exige l'existence d'API convenables, on a choisi d'exiger la prise en charge des plus courts formats de paquet pour les deux paquets de charge utile et d'acheminement de retour.

Pour prendre en charge l'adresse d'entretien comme adresse de destination sur le côté nœud mobile, l'agent de rattachement doit agir comme si l'adresse de destination de l'en-tête externe dans l'association de sécurité avec le nœud mobile avait changé lors des mouvements. Les mises en œuvre sont libres de choisir une méthode particulière pour faire ce changement, comme d'utiliser une API pour que la mise en œuvre de IPsec change les paramètres de l'association de sécurité, supprime l'association de sécurité et en installe une nouvelle, ou pour modifier le paquet après qu'il soit parti à travers le traitement IPsec. La seule exigence est qu'après l'enregistrement d'un nouveau lien chez l'agent de rattachement, les prochains paquets IPsec envoyés sur cette association de sécurité seront adressés à la nouvelle adresse d'entretien.

On a choisi d'exiger des entrées de politique qui sont spécifiques d'une interface de tunnel. Cela signifie que les mises en œuvre doivent considérer le tunnel entre l'agent de rattachement et le nœud mobile comme une interface séparée sur laquelle les SPD IPsec peuvent se fonder. Une autre complication du traitement IPsec sur une interface de tunnel est que cela exige un accès à la mise en œuvre de BITS avant que le paquet ne soit réellement transmis.

7.2 IKE

On a choisi d'exiger qu'un protocole de gestion dynamique de clés soit capable de prendre une décision d'autorisation pour la création d'une association de sécurité IPsec avec des adresses différentes de celles sur lesquelles fonctionne le protocole de gestion de clés. On s'attend à ce que ceci soit normalement fait en configurant les combinaisons permises d'identités d'utilisateur de phase 1 et d'adresses de rattachement.

Lorsque l'authentification par certificat est utilisée, on peut rencontrer la fragmentation IKE. Cela peut se produire lorsque des chaînes de certificats sont utilisées, ou même avec un seul certificat si il est long. De nombreux pare-feu ne traitent pas les fragments de façon appropriée, et peuvent les éliminer. Les routeurs sur le chemin peuvent aussi éliminer les fragments qui suivent le premier, car ils ne vont normalement pas contenir tous les en-têtes IP qui peuvent être comparés à une liste d'accès. Lorsque une fragmentation survient, les points d'extrémité ne vont pas toujours être capables d'établir une association de sécurité.

Heureusement, les déploiements typique de IPv6 mobile utilisent des chaînes courtes de certificats, car le nœud mobile communique directement avec son réseau de rattachement. Lorsque le problème apparaît, il peut être difficile (au moins en itinérance) de remplacer les pare-feu ou les routeurs par des équipements qui puissent correctement prendre en charge les fragments. Cela peut aider de mémoriser localement les certificats de l'homologue, ou de les obtenir par d'autres moyens.

7.3 Pris dans la pile

IPv6 mobile met des exigences fortes pour la mise en œuvre du modèle d'IPsec appelé pris dans la pile (BITS, *Bump-In-The-Stack*). Comme des modifications des paquets spécifiques de IPv6 mobile sont exigées avant ou après le traitement IPsec, la mise en œuvre de BITS doit effectuer aussi certaines tâches relatives à la mobilité. Cela peut accroître la complexité de la mise en œuvre, même si elle effectue déjà certaines tâches de la couche IP (comme la fragmentation).

Spécifiquement, les mises en œuvre de BITS peuvent devoir traiter les problèmes suivants :

- Traitement de l'option de destination Adresse de rattachement et de l'en-tête Acheminement de type 2 pour les mettre dans une forme convenable pour que le traitement IPsec ait lieu. Ceci est nécessaire, entre autres choses, pour les recherches d'association de sécurité et de politique. Bien que relativement direct, le traitement exigé peut avoir un effet sur le matériel dans les mises en œuvre de BITS, si elles utilisent un support matériel qui va au delà des opérations cryptographiques.

- Détecter les paquets envoyés entre le nœud mobile et son agent de rattachement en utilisant l'encapsulation IPv6.

- Offrir les API nécessaires pour mettre à jour les points d'extrémité d'association de sécurité IPsec et IKE.

8. Considérations relatives à l'IANA

Aucune action de l'IANA n'est nécessaire sur la base du présent document. Les actions de l'IANA pour le protocole IPv6 mobile lui-même sont couvertes dans la [RFC3775].

9. Considérations sur la sécurité

La spécification de base IPv6 mobile [RFC3775] exige une forte sécurité entre le nœud mobile et l'agent de rattachement. Le présent mémoire discute de la façon dont cette sécurité peut être arrangée en pratique, en utilisant IPsec. Les considérations de sécurité qui se rapportent à cela sont documentées dans la spécification de base, incluant une discussion des implications de l'utilisation du chiffrement manuel ou dynamique.

10. Références

10.1 Références normatives

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

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

[RFC2406] S. Kent et R. Atkinson, "Encapsulation de charge utile de sécurité IP (ESP)", novembre 1998. *(Obsolète, voir*

RFC4303)

[RFC2409] D. Harkins et D. Carrel, "L'échange de clés Internet (IKE)", novembre 1998. *(Obsolète, voir la* RFC4306)

[RFC2460] S. Deering et R. Hinden, "Spécification du protocole Internet, version 6 (IPv6) ", décembre 1998. *(MàJ par* 5095, 6564 *; D.S)*

[RFC2473] A. Conta, S. Deering, "Spécification du tunnelage générique de paquet dans IPv6", décembre 1998. *(P.S.)*

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

10.2 Références pour information

[RFC2402] S. Kent et R. Atkinson, "En-tête d'authentification IP", novembre 1998. (*Obsolète, voir* RFC4302, 4305)

[RFC2710] S. Deering, W. Fenner et B. Haberman, "Découverte d'écouteur de diffusion groupée (MLD) pour IPv6", octobre 1999.

[RFC3315] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins et M. Carney, "Protocole de configuration dynamique d'hôte pour IPv6 (DHCPv6)", juillet 2003. (*MàJ par* RFC6422 et RFC6644, RFC7227)

[RFC3810] R. Vida, L. Costa, éditeurs, "Découverte d'écouteur de diffusion groupée version 2 (MLDv2) pour IPv6", juin 2004.

11. Remerciements

Les auteurs tiennent à remercier Greg O'Shea, Michael Thomas, Kevin Miles, Cheryl Madson, Bernard Aboba, Erik Nordmark, Gabriel Montenegro, Steven Kent, et Santeri Paavolainen des intéressantes discussions qu'ils ont eues sur ces problèmes.

12. Adresse des auteurs

Jari Arkko
Ericsson
02420 Jorvas
Finland
mél : jari.arkko@ericsson.com

Vijay Devarapalli
Nokia Research Center
313 Fairchild Drive
Mountain View CA 94043
USA
mél : vijayd@iprg.nokia.com

Francis Dupont
ENST Bretagne
2, rue de la Chataigneraie
CS 17607
35576 Cesson-Sevigne Cedex
France
mél : Francis.Dupont@enst-bretagne.fr

13. Déclaration complète de droits de reproduction

documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur répertoire en ligne des IPR de l'IETF à http://www.ietf.org/ipr.

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf-ipr@ietf.org.

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