Groupe de travail Réseau
Request for Comments : 5374
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

B. Weis, Cisco Systems
G. Gross, Secure Multicast Networks
D. Ignjatic, Polycom
novembre 2008

Extensions de diffusion groupée à l'architecture de sécurité du protocole Internet

Statut du présent mémoire

Le présent document spécifie un protocole de l'Internet sur la voie de la 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

L'architecture de sécurité pour le protocole Internet décrit les services de sécurité pour le trafic à la couche IP. Cette architecture définit principalement des services pour les paquets du protocole Internet (IP) en envoi individuel. Le présent document décrit comment les services IPsec de sécurité sont appliqués aux paquets de diffusion groupée IP. Ces extensions ne sont pertinentes que pour une mise en œuvre IPsec qui prend en charge la diffusion groupée.

Table des matières

1. Introduction

L'architecture de sécurité pour le protocole Internet [RFC4301] fournit des services de sécurité pour le trafic à la couche IP. Elle décrit une architecture pour les systèmes conformes à IPsec et un ensemble de services de sécurité pour la couche IP. Ces services de sécurité décrivent principalement les services et la sémantique des associations de sécurité (SA, *Security Association*) IPsec partagées entre deux appareils IPsec. Normalement, cela inclut des SA avec des sélecteurs de trafic qui incluent une adresse en envoi individuel dans le champ de destination IP, et résulte en un paquet IPsec avec une adresse en envoi individuel dans le champ de destination IP. Les services de sécurité définis dans la RFC 4301 peuvent aussi être utilisés pour tunneler des paquets de diffusion groupée IP, où le tunnel est une association appariée entre deux appareils IPsec. La RFC 4301 définit la prise en charge de SA IPsec en mode transport chiffrées manuellement pour les paquets IP avec une adresse de diffusion groupée dans le champ Adresse de destination IP. Cependant, la RFC 4301 ne définit pas l'interaction d'un sous système IPsec avec un protocole de gestion de clé de groupe (GKM, *Group Key Management*) ni la sémantique d'une SA IPsec en mode tunnel avec une adresse de diffusion groupée IP dans l'en-tête IP externe.

Le présent document décrit des extensions FACULTATIVES à la RFC 4301 qui définissent l'architecture de sécurité IPsec afin que les groupes d'appareils IPsec partagent des SA. En particulier, il prend en charge les SA avec des sélecteurs de trafic qui incluent une adresse de diffusion groupée dans le champ de destination IP et qui résultent en un paquet IPsec avec une adresse de diffusion groupée IP dans le champ de destination IP. Il décrit aussi des sémantiques supplémentaires pour les sous systèmes de gestion de clé de groupe IPsec. Noter que le présent document utilise le terme de "protocole GKM" de façon générique et ne suppose donc pas un protocole GKM particulier.

Une mise en œuvre de IPsec qui ne prend pas en charge la diffusion groupée n'est pas obligée de prendre en charge ces extensions.

Dans le présent document, la sémantique de la RFC 4301 reste inchangée en présence de ces extensions de diffusion groupée sauf mention contraire spécifique.

1.1 Domaine d'application

Les extensions IPsec décrites dans ce document prennent en charge les associations de sécurité IPsec qui résultent en paquets IPsec avec des adresses de groupe de diffusion groupée IPv4 ou IPv6 comme adresse de destination. Les deux adresses de groupe Toute source de diffusion groupée (ASM, *Any-Source Multicast*) et Diffusion groupée spécifique de source (SSM, *Source-Specific Multicast*) [RFC3569] sont prises en charge. Ces extensions sont utilisées quand la politique de gestion exige que les paquets de diffusion groupée IP protégés par IPsec restent des paquets de diffusion groupée IP. Quand la politique de gestion exige que les paquets de diffusion groupée IP soient encapsulés dans des paquets IP en envoi individuel (par exemple, parce que le réseau connecté à l'interface non protégée ne prend pas en charge la diffusion groupée IP) les extensions de ce document ne sont pas utilisées.

Ces extensions prennent aussi en charge les associations de sécurité avec des adresses de diffusion IPv4 qui résultent en un paquet de diffusion IPv4 de niveau liaison, et des adresses IPv6 d'envoi à la cantonade [RFC2526] qui résultent en un paquet IPv6 en envoi à la cantonade. Ces types d'adresse de destination partagent beaucoup des mêmes caractéristiques des adresses de diffusion groupée parce que il peut y avoir plusieurs candidats receveurs d'un paquet protégé par IPsec.

L'architecture IPsec n'a pas d'exigences sur les entités qui ne participent pas à IPsec (par exemple, les appareils réseau entre les points d'extrémité IPsec). À ce titre, ces extensions de diffusion groupée n'exigent pas que les systèmes intermédiaires dans un réseau à capacité de diffusion groupée participent à IPsec. En particulier, il n'y a pas d'exigence sur l'utilisation de protocole d'acheminement de diffusion groupée (par exemple, le protocole de diffusion groupée en mode épars (PIM-SM, *Protocol Independent Multicast -Sparse Mode*) [RFC4601]) ou les protocoles d'admission de diffusion groupée (par exemple, le protocole de gestion de groupe Internet (IGMP, *Internet Group Management Protocol*) [RFC3376]).

Tous les modèles de mise en œuvre de IPsec (par exemple, "pris dans la pile", "pris dans le réseau") sont supportés.

Cette version de la spécification de l'extension de IPsec en diffusion groupée exige que toux les appareils IPsec qui

participent à une association de sécurité soient homogènes. Ils DOIVENT partager un ensemble commun de transformations cryptographiques et de capacités de traitement de protocole. La sémantique d'un "groupe IPsec composite" [COMPGRP], un groupe cryptographique hétérogène IPsec formé de l'union de deux sous-groupes ou plus, fera l'objet d'une normalisation future.

1.2 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].

Les termes clés suivants sont utilisés dans le présent document.

ASM *(Any-Source Multicast)* : diffusion groupée toutes sources. Modèle de service de diffusion groupée du protocole Internet comme défini dans la [RFC1112]. Dans ce modèle, un ou plusieurs envoyeurs génèrent des paquets à une seule adresse de diffusion groupée IP. Quand des receveurs se joignent au groupe, ils reçoivent tous les paquets envoyés à cette adresse de diffusion groupée IP. Ceci est appelé un groupe (*,G).

Groupe : ensemble d'appareils qui travaillent ensemble pour protéger les communications de groupe.

GCKS *(Group Controller Key Server)* : serveur de clé de contrôleur de groupe. Serveur du protocole de gestion de clé de groupe (GKM, *Group Key Management*) qui gère l'état IPsec pour un groupe. Un GCKS authentifie et donne la politique IPsec de SA et le matériel de chiffrement aux membres du groupe GKM.

Protocole de gestion de clé de groupe : protocole de gestion de clé utilisé par un GCKS pour distribuer la politique d'associations de sécurité IPsec et le matériel de chiffrement. Un protocole GKM est utilisé quand un groupe d'appareils IPsec exige les mêmes SA. Par exemple, quand une SA IPsec décrit une destination de diffusion groupée IP, l'envoyeur et tous les receveurs ont besoin d'avoir la SA de groupe.

Sous système de gestion de clé de groupe : sous système dans un appareil IPsec qui met en œuvre un protocole de gestion de clé de groupe. Le sous système GKM fournit les SA IPsec au sous système IPsec sur l'appareil IPsec. Voir les [RFC3547] et [RFC4535] pour des informations supplémentaires.

Membre de groupe : appareil IPsec qui appartient à un groupe. Un membre du groupe est autorisé à être un envoyeur de groupe et/ou un receveur de groupe.

Propriétaire du groupe : entité administrative qui choisit la politique pour un groupe.

GSA *(Group Security Association)* : association de sécurité de groupe. Collection d'associations de sécurité IPsec et de SA de sous système GKM nécessaire pour qu'un membre de groupe reçoive les mises à jour de clés. Une GSA décrit la politique de travail pour un groupe. Voir la [RFC4046] pour des informations supplémentaires.

GSPD (*Group Security Policy Database*) base de données de politiques de sécurité de groupe : la GSPD est une base de données de politiques de sécurité de diffusion groupée, comme mentionné dans la RFC 3740 et au paragraphe 4.4.1.1 de la RFC 4301. Sa signification est un sur ensemble de la base de données de politiques de sécurité (SPD, *Security Policy Database*) en envoi individuel définie au paragraphe 4.4.1 de la RFC 4301. À la différence de la SPD-S en envoi individuel, dans laquelle les sélecteurs de trafic en point à point sont par nature des sélecteurs de trafic bidirectionnels, les sélecteurs de trafic de sécurité de diffusion groupée dans la GSPD-S incluent un attribut de direction "envoi seul", "receveur seul", ou "symétrique". Voir les détails au paragraphe 4.1.1.

GSPD-S, GSPD-I, GSPD-O : respectivement base de données de politique de sécurité de groupe (trafic sécurisé), (entrant), et (sortant). Voir le paragraphe 4.4.1 de la RFC 4301.

Receveur de groupe : membre de groupe autorisé à recevoir des paquets envoyés à un groupe par un envoyeur de groupe.

Envoyeur de groupe : membre de groupe autorisé à envoyer des paquets à un groupe.

SSM (*Source-Specific Multicast*) diffusion groupe spécifique de source : modèle de service de diffusion groupée du protocole Internet (IP) comme défini dans la [RFC3569]. Dans ce modèle, chaque combinaison d'un envoyeur et d'une adresse de diffusion groupée IP est considérée comme un groupe. Ceci est appelé un groupe (S,G).

Mode tunnel avec préservation de l'adresse : type de mode tunnel IPsec utilisé par les mises en œuvre de passerelle de sécurité lors de l'encapsulation de paquets de diffusion groupée IP de telle façon qu'ils restent des paquets de diffusion groupée IP. Ce mode est nécessaire pour que l'acheminement de diffusion groupée IP achemine correctement les paquets de diffusion groupée IP protégés par IPsec.

2. Vue d'ensemble du fonctionnement de la diffusion groupée IP

La diffusion groupée IP est un moyen d'envoyer un seul paquet à un "groupe d'hôtes", un ensemble de zéro, un ou plusieurs hôtes identifié par une seule adresse de destination IP. Les paquets de diffusion groupée IP sont livrés à tous les membres du groupe soit avec une fiabilité "au mieux" [RFC1112], soit au titre d'un flux fiable (par exemple, la diffusion groupée fiable s'appuyant sur l'accusé de réception négatif (NORM, *NACK-Oriented Reliable Multicast*) [RFC3940]).

Un envoyeur à un groupe de diffusion groupée IP règle la destination du paquet à une adresse IP qui a été allouée pour la diffusion groupée IP. Les adresses de diffusion groupée IP allouées sont définies dans les [RFC3171], [RFC3306], et [RFC3307]. Les receveurs potentiels du paquet "se joignent" au groupe de diffusion groupée IP en s'enregistrant auprès d'un appareil d'acheminement du réseau ([RFC3376], [RFC3810]) en signalant son intention de recevoir les paquets envoyés à un groupe de diffusion groupée IP particulier.

Les appareils d'acheminement du réseau configurés à passer les paquets de diffusion groupée IP participent aux protocoles d'acheminement de diffusion groupée (par exemple, PIM-SM) [RFC4601]. Les protocoles d'acheminement de diffusion groupée maintiennent l'état concernant quels appareils sont enregistrés pour recevoir les paquets pour un groupe de diffusion groupée IP particulier. Quand un routeur reçoit un paquet de diffusion groupée IP, il transmet une copie du paquet sur chaque interface pour laquelle il y a des receveurs connus.

3. Modes d'association de sécurité

IPsec prend en charge deux modes d'utilisation : le mode transport et le mode tunnel. En mode transport, l'en-tête d'authentification (AH, *Authentication Header*) IP [RFC4302] et la charge utile de sécurité encapsulante (ESP, *Encapsulating Security Payload*) IP [RFC4303] fournissent la protection principalement pour les protocoles de prochaine couche ; en mode tunnel, AH et ESP sont appliqués aux paquets IP tunnelés.

Une mise en œuvre d'hôte de IPsec qui utilise les extensions de diffusion groupée PEUT utiliser le mode transport ou le mode tunnel pour encapsuler un paquet de diffusion groupée IP. Ces règles de traitement sont identiques aux règles décrites au paragraphe 4.1 de la [RFC4301]. Cependant, l'adresse de destination pour le paquet IPsec est une adresse de diffusion groupée IP, plutôt que une adresse d'hôte en envoi individuel.

Une mise en œuvre de passerelle de sécurité de IPsec DOIT utiliser une SA en mode tunnel, pour les raisons décrites au paragraphe 4.1 de la [RFC4301]. En particulier, la passerelle de sécurité a besoin d'utiliser le mode tunnel pour encapsuler les fragments entrants, car IPsec ne peut pas directement opérer sur des fragments.

3.1 Mode tunnel avec préservation d'adresse

Une nouvelle sémantique de construction d'en-tête (tunnel) est nécessaire quand le mode tunnel est utilisé pour encapsuler des paquets de diffusion groupée IP qui doivent rester des paquets de diffusion groupée IP. Cette sémantique est due aux exigences uniques suivantes des protocoles d'acheminement de diffusion groupée IP (par exemple, PIM-SM [RFC4601]). Le présent document décrit cette nouvelle sémantique de construction d'en-tête comme le "mode tunnel avec préservation d'adresse", qui est décrit comme suit.

- Quand un paquet de diffusion groupée IP est reçu par un hôte ou routeur, l'adresse de destination du paquet est comparée à l'état de diffusion groupée IP local. Si l'adresse de destination IP (externe) d'un paquet de diffusion groupée IP est réglée à une autre adresse IP, l'hôte ou routeur qui reçoit le paquet de diffusion groupée IP ne va pas le traiter correctement. Donc, une passerelle de sécurité IPsec a besoin de remplir l'adresse de destination IP de diffusion groupée dans l'en-tête externe en utilisant l'adresse de destination provenant de l'en-tête interne après l'encapsulation de tunnel IPsec.

- Les protocoles d'acheminement de diffusion groupée IP créent normalement des arborescences de distribution de

diffusion groupée sur la base de l'adresse de source ainsi que de l'adresse de groupe. Si une passerelle de sécurité IPsec remplit l'adresse de source (externe) d'un paquet de diffusion groupée IP (avec sa propre adresse IP, comme demandé dans la RFC 4301) le paquet protégé par IPsec résultant peut échouer aux vérifications de transmission sur le chemin inverse (RPF, *Reverse Path Forwarding*) effectuées par les autres routeurs. Un échec de vérification de RDP peut résulter en l'élimination du paquet. Pour s'accommoder des vérifications de RPF de protocole d'acheminement, la passerelle de sécurité qui met en œuvre les extensions IPsec de diffusion groupée DEVRAIT remplir l'adresse IP externe provenant de l'adresse de source IP du paquet original. Cependant, on devrait noter qu'une passerelle de sécurité effectuant la préservation de l'adresse de source ne va pas recevoir la MTU de chemin (PMTU, *Path MTU*) ICMP ni les autres messages destinés à la passerelle de sécurité (déclenchés par les paquets qui ont eu l'adresse de source IP externe réglée à celle de l'en-tête interne). Les applications de passerelle de sécurité qui n'exigent pas la préservation de l'adresse de source vont être capables de recevoir les messages ICMP de PMTU et de les traiter comme décrit au paragraphe 6.1 de la RFC 4301.

Parce que certaines applications de préservation d'adresse peuvent exiger que seule l'adresse de destination soit préservée, la spécification de la préservation d'adresse de destination et la préservation de l'adresse de source sont séparées dans la description ci-dessus. Les attributs de préservation d'adresse de destination et de préservation d'adresse de source sont décrits dans la base de données de politiques de sécurité de groupe (GSPD) (définie plus loin dans ce document) et sont copiés dans les entrées correspondantes de base de données d'association de sécurité (SAD, *Security Association Database*).

La préservation de l'adresse est applicable seulement aux SA en mode tunnel IPsec qui spécifient la version IP de l'en-tête encapsulant comme étant de la même version que celle de l'en-tête interne. Quand les versions IP sont différentes, les paquets de diffusion groupée IP peuvent être encapsulés en utilisant une interface de tunnel, par exemple comme décrit dans la [RFC4891], où le tunnel est aussi traité comme une interface par les protocoles d'acheminement de diffusion groupée IP.

En résumé, la propagation des deux adresses IP de source et de destination de l'en-tête IP interne dans l'en-tête externe (tunnel) permet aux protocoles d'acheminement de diffusion groupée IP d'acheminer correctement un paquet quand le paquet est protégé par IPsec. Ce résultat est nécessaire afin que les extensions de diffusion groupée permettent à un hôte ou passerelle de sécurité de fournir des services IPsec pour les paquets de diffusion groupée IP. Cette méthode du mode tunnel de la RFC 4301 est appelé le "mode tunnel avec préservation d'adresse".

4. Association de sécurité

4.1 Bases de données IPsec majeures

Les paragraphes qui suivent décrivent le sous système GKM et les interactions d'extension IPsec avec les bases de données IPsec. Les bases de données IPsec majeures ont besoin d'une expansion de leur sémantique pour prendre pleinement en charge la diffusion groupée.

4.1.1 Base de données de politique de sécurité de groupe (GSPD)

La base de données de politique de sécurité de groupe (GSPD, *Group Security Policy Database*) est une base de données de politiques de sécurité capable de prendre en charge les deux associations de sécurité en envoi individuel définies par la RFC 4301 et les extensions de diffusion groupée définies par la présente spécification. La GSPD est considérée comme étant la SPD, avec l'ajout de la sémantique relative aux extensions de diffusion groupée décrites dans cette section. L'Appendice B donne un exemple de définition ASN.1 d'une entrée de GSPD.

Le présent document décrit un nouveau fanion "préservation d'adresse" (AP) indiquant que le mode tunnel avec préservation d'adresse est à appliquer à une entrée de GSPD. Le fanion AP a deux attributs : AP-L, utilisé dans le traitement de l'adresse locale de tunnel, et AP-R, utilisé dans le traitement du tunnel distant. Ce fanion est ajouté au champ GSPD "Informations de traitement" de la GSPD. Le texte suivant, reproduit du paragraphe 4.4.1.2 de la RFC 4301 est amendé pour inclure ce traitement supplémentaire. (Note : par souci de concision seul le texte de "Informations de traitement" relatif au traitement du tunnel a été reproduit.)

o Informations de traitement -- quelle action est requise -- PROTECT, BYPASS, ou DISCARD. Il y a juste une action qui va avec tous les ensembles de sélecteurs, et non une action séparée pour chaque ensemble. Si le traitement requis est PROTECT, l'entrée contient les informations suivantes. - mode IPsec -- tunnel ou transport – (si c'est le mode tunnel) adresse locale du tunnel -- Pour un hôte non mobile, si il y a juste une interface, c'est direct ; si il y a plusieurs

interfaces, cela doit être configuré de façon statique. Pour un hôte mobile, la spécification de l'adresse locale est traitée à l'extérieur de IPsec. Si le mode tunnel avec préservation d'adresse est spécifié pour l'adresse locale du tunnel, l'attribut AP-L est réglé à VRAI pour l'adresse locale du tunnel et l'adresse locale du tunnel est non spécifiée. La présence de l'attribut AP-L indique que l'adresse de source de l'en-tête IP interne va être copiée dans l'adresse de source de l'en-tête IP externe durant la construction de l'en-tête IP pour le mode tunnel. - (si c'est le mode tunnel) l'adresse distante du tunnel – Il n'y a pas de moyen standard de déterminer cela. Voir le paragraphe 4.5.3 de la RFC 4301, "Localisation d'une passerelle de sécurité". Si le mode tunnel avec préservation d'adresse est spécifié pour l'adresse distante du tunnel, l'attribut AP-R est réglé à VRAI pour l'adresse distante de tunnel et l'adresse distante du tunnel est non spécifiée. La présence de l'attribut AP-R indique que l'adresse de destination de l'en-tête IP interne va être copiée à l'adresse de destination de l'en-tête IP externe durant la construction de l'en-tête IP pour le mode tunnel.

Le présent document décrit un traitement unique de direction pour les entrées de GSPD avec une adresse de diffusion groupée IP distante. Comme une adresse de diffusion groupée IP ne doit pas être envoyée comme adresse de source pour un paquet IP [RFC1112], la direction des adresses locale et distante et des accès est maintenue durant les vérifications de SPD-S et SPD-I entrantes plutôt que de les échanger. Le paragraphe 4.4.1 de la RFC 4301 est amendé comme suit :

Représentation de la direction dans une entrée de SPD : pour le trafic protégé par IPsec, l'adresse et les accès locaux et distants dans une entrée de SPD sont échangées pour représenter la direction, en cohérence avec les conventions IKE. En général, les protocoles avec lesquels traite IPsec ont la propriété d'exiger des SA symétriques avec des adresses IP local/distante échangées. Cependant, les entrées de SPD avec une adresse de diffusion groupée IP distante n'ont pas leurs adresses et accès locaux/distants dans l'entrée de SPD échangés durant les vérifications de SPD-S et SPD-I entrantes.

Un nouvel attribut de base de données de politique de sécurité de groupe (GSPD) est introduit : Direction d'entrée de GSPD. Le texte suivant est ajouté à la liste des champs de SPD décrite au paragraphe 4.4.1.2 de la RFC 4301.

o Direction -- peut être d'un des trois types : "symétrique", "envoi seul", ou "receveur seul". "Symétrique" indique qu'une paire de SA sont à créer (une dans chaque direction, comme spécifié par la RFC 4301). Les entrées de GSPD marquées comme "envoi seul" indiquent qu'une SA est à créer dans la direction sortante. Les entrées de GSPD marquées comme "receveur seul" indiquent que une SA est à créer dans la direction entrante. Les entrées de GSPD marquées comme "envoi seul" ou "receveur seul" DEVRAIENT prendre en charge les adresses IP de diffusion groupée dans leurs sélecteurs d'adresse de destination. Si le traitement demandé est BYPASS ou DISCARD et si un type "envoi seul" est configuré, l'entrée DOIT être mise en GSPD-O seulement. Réciproquement, si le type est "receveur seul", l'entrée DOIT aller à GSPD-I seulement.

Les entrées de GSPD créées par un GCKS peuvent recevoir des indices de paramètre de sécurité (SPI, *Security Parameter Index*) identiques aux entrées de SAD créées par IKEv2 [RFC4306]. Ce n'est pas un problème pour le trafic entrant car les SA appropriées peuvent être confrontées en utilisant l'algorithme décrit au paragraphe 4.1 de la RFC 4301. Cependant, le trafic sortant doit être confronté aux sélecteurs de la GSPD afin que la SA appropriée puisse être créée.

Pour faciliter le chiffrement dynamique de groupe, la GSPD sortante DOIT mettre en œuvre une capacité d'action de politique qui déclenche un échange d'enregistrement de protocole GKM (conformément au paragraphe 5.1 de la [RFC4301]). Par exemple, l'envoyeur de la GSPD de politique de groupe pourrait déclencher une correspondance avec un paquet d'application de diffusion groupée spécifiée qui entre dans la mise en œuvre via l'interface protégée ou qui est émis par la mise en œuvre sur le côté protégé de la frontière et dirigé vers l'interface non protégée. L'échange d'enregistrement d'envoyeur de groupe qui s'ensuit va établir l'entrée de SAD sortante de l'envoyeur de groupe qui chiffre le flux de données de l'application de diffusion groupée. Dans la direction inverse, la politique de groupe peut aussi établir une SA IPsec entrante.

Aux points d'extrémité de receveur de groupe, le sous système IPsec PEUT utiliser les mécanismes de politique de GSPD qui initient un échange d'enregistrement de protocole GKM. Un de ces mécanismes de politique pourrait être la détection d'un appareil dans le réseau protégé qui se joint à une politique de GSPD correspondant à un groupe de diffusion groupée (par exemple, en recevant un message IGMP/MLD (Multicast Listener Discovery, *découverte d'écoutant de diffusion groupée*) pour se joindre au groupe sur une interface protégée). L'échange d'enregistrement de receveur de groupe qui s'ensuit va établir l'entrée de SAD entrante du receveur de groupe qui déchiffre le flux de données de l'application de diffusion groupée. Dans la direction inverse, la politique de groupe peut aussi établir une SA IPsec sortante (par exemple, quand elle prend en charge un modèle de service ASM).

Note : une passerelle de sécurité qui se déclenche à réception de messages non authentifiés qui arrivent sur une interface protégée peut résulter en un enregistrement précoce du receveur de groupe si le message ne résulte pas d'un appareil sur le réseau protégé qui souhaite en fait se joindre à un groupe de diffusion groupée. Les messages non authentifiés vont seulement causer une fois l'enregistrement du receveur de groupe ; les messages suivants n'auront pas d'effet

sur le receveur de groupe.

Le sous système IPsec PEUT fournir des mécanismes de politique de GSPD qui initient automatiquement un échange de désenregistrement de protocole GKM. Le désenregistrement permet à un GCKS de minimiser l'exposition de la clé secrète du groupe en changeant la clé d'un groupe lors d'un événement de changement de l'appartenance au groupe. Il minimise aussi le coût sur un GCKS pour les groupes dont il conserve l'état des membres. Un de ces mécanismes de politique pourrait être la détection des échanges IGMP/MLD pour quitter le groupe. Cependant, une passerelle de sécurité membre de groupe ne va pas initier un échange de désenregistrement de protocole GKM tant qu'elle ne détecte pas qu'il n'y a plus de receveur derrière une interface protégée.

De plus, le sous système GKM PEUT établir les informations d'état de GSPD/SAD indépendamment de l'état de l'application de diffusion groupée. Dans ce scénario, le propriétaire de groupe produit des directives de gestion qui disent au sous système GKM quand il devrait commencer les échanges de protocole d'enregistrement et de désenregistrement GKM. Normalement, la politique d'enregistrement s'efforce de s'assurer que l'état du sous système IPsec du groupe est "toujours prêt" en anticipation du début de l'exécution de l'application de diffusion groupée.

4.1.2 Base de données d'association de sécurité (SAD)

La SAD contient un élément qui décrit si le mode tunnel ou transport est appliqué au trafic sur cette SA. Le texte du paragraphe 4.4.2.1 de la RFC 4301 est amendé pour décrire la préservation d'adresse.

- Mode de protocole IPsec : tunnel ou transport. Indique quel mode de AH ou ESP est appliqué au trafic sur cette SA. Quand le mode tunnel est spécifié, l'élément de données indique aussi si la préservation d'adresse est ou non appliquée à l'en-tête IP externe. La préservation de l'adresse NE DOIT PAS être spécifiée quand la version IP de l'en-tête encapsulant et la version IP de l'en-tête interne ne correspondent pas. L'adresse locale, l'adresse distante, ou les deux adresses PEUVENT être marquées comme étant préservées durant l'encapsulation de tunnel.

4.1.3 Base de données d'autorisation de groupe homologue (GPAD)

Les extensions IPsec de diffusion groupée introduisent une nouvelle structure de données appelée la base de données d'autorisation d'homologue de groupe (GPAD, *Group Peer Authorization Database*). La GPAD est analogue à la PAD définie dans la RFC 4301. Elle fournit un lien entre la GSPD et un sous système de gestion de clé de groupe (GKM). La GPAD incorpore les fonctions critiques suivantes :

- identifie un GCKS (ou un groupe d'appareils GCKS) qui est autorisé à communiquer avec cette entité IPsec,
- spécifie le protocole et la méthode utilisés pour authentifier chaque GCKS,
- fournit les données d'authentification pour chaque GKCS,
- contraint les sélecteurs de trafic qui peuvent être certifiés par un GCKS à l'égard de la création de SA,
- contraint les types et valeurs d'identifiants de groupe pour lesquels un GCKS est autorisé à fournir une politique de groupe.

La GPAD fournit ces fonctions pour un sous système de gestion de clé de groupe. La GPAD n'est pas consultée par IKE ou autre protocole d'authentification qui n'agit pas comme protocole de GKM.

Pour fournir ces fonctions, la GPAD contient une entrée pour chaque GCKS que l'entité IPsec est configurée à contacter. Une entrée contient un ou plusieurs identifiants de GCKS, le protocole d'authentification (par exemple, interprétation du domaine de groupe (GDOI, *Group Domain of Interpretation*) ou protocole de gestion de clé d'association de sécurité de groupe (GSAKMP, *Group Secure Association Key Management Protocol*)) la méthode d'authentification utilisée (par exemple, des certificats ou secrets pré-partagés) et les données d'authentification (par exemple, le secret pré-partagé ou l'ancre de confiance à l'égard de laquelle le certificat de l'homologue va être validé). Pour l'authentification fondée sur le certificat, l'entrée peut aussi fournir des informations pour aider à vérifier l'état de révocation de l'homologue, par exemple, un pointeur sur un répertoire de listes de révocation de certificats (CRL, *Certificate Revocation List*) ou le nom d'un serveur du protocole d'état de certificat en ligne (OCSP, *Online Certificate Status Protocol*) associé à l'homologue ou l'ancre de confiance associée à l'homologue. L'entrée contient aussi les contraintes qu'un membre du groupe applique à la politique reçue du GKCS.

4.1.3.1 Identifiants GCKS

Les identifiants de GCKS sont utilisés pour identifier un ou plusieurs appareils qui sont autorisés à agir comme GCKS pour ce groupe. Les identifiants de GCKS sont spécifiés comme des identifiants d'entrée de PAD au paragraphe 4.4.3.1 de la RFC 4301 et suivent les règles de confrontation qui y sont décrites.

4.1.3.2 Données d'authentification d'homologue GCKS

Une fois qu'une entrée de GPAD est localisée, il est nécessaire de vérifier l'identité affirmée, c'est-à-dire, d'authentifier l'identifiant de GCKS affirmé. Les types de données d'authentification de PAD et la sémantique spécifiés au paragraphe 4.4.3.2 de la RFC 4301 sont utilisés pour authentifier un GCKS.

Voir GDOI [RFC3547] et GSAKMP [RFC4535] pour les détails de comment un protocole GKM effectue l'authentification d'homologue en utilisant des certificats et des secrets pré-partagés.

4.1.3.3 Données d'autorisation d'identifiant de groupe

Un identifiant de groupe est utilisé par un protocole GKM pour identifier un groupe particulier à un GCKS. Une entrée de GPAD inclut un identifiant de groupe pour indiquer que les identifiants de GKCS dans l'entrée de GPAD sont autorisés à agir comme un GCKS pour le groupe.

L'identifiant de groupe est une chaîne opaque d'octets du type identifiant de clé IKE qui identifie un groupe de diffusion groupée sûr. La chaîne d'octets de l'identifiant de groupe DOIT être d'au moins quatre octets et de moins de 256 octets.

Les types d'identifiant IKE autres que Identifiant de clé PEUVENT être acceptés.

4.1.3.4 Données d'autorisation de sélecteur de tazfic de SA IPsec

Une fois qu'un GCKS est authentifié, le GCKS livre la politique de SA IPsec au membre du groupe. Avant que le membre du groupe accepte la politique de SA IPsec, les sélecteurs de trafic de source et destination de la SA sont comparés à un ensemble de flux de données autorisés. Chaque flux de données inclut un ensemble de sélecteurs de trafic de source autorisé et un ensemble de sélecteurs de trafic de destination autorisé. Les sélecteurs de trafic sont représentés comme un ensemble de gammes d'adresses IPv4 et/ou IPv6. (Un homologue peut être autorisé pour les deux types d'adresses, de sorte qu'il DOIT y avoir des dispositions pour les deux gammes d'adresse v4 et v6.)

4.1.3.5 Utilisation de la GPAD

Quand un échange d'enregistrement de protocole GKM est déclenché, le membre du groupe et le GCKS affirment chacun leur identité au titre de l'échange. Chaque échange d'enregistrement de protocole GKM DOIT utiliser l'identifiant affirmé pour localiser une identité dans la GPAD. L'entrée de GPAD spécifie la méthode d'authentification à employer pour le GCKS identifié. L'entrée spécifie aussi les données d'authentification qui vont être utilisées pour vérifier l'identité affirmée. Ces données sont employées conjointement avec la méthode spécifiée pour authentifier le GCKS avant d'accepter une politique de groupe du GCKS.

Durant l'enregistrement de protocole GKM, un membre du groupe inclut un identifiant de groupe. Avant de présenter cet identifiant de groupe au GCKS, un membre de groupe vérifie que l'entrée de GPAD pour l'entrée de GPAD du GCKS authentifié inclut l'identifiant de groupe. Cela assure que le GCKS est autorisé à fournir la politique pour le groupe.

Quand la politique de SA IPsec est reçue, chaque flux de données est comparé au flux de données dans l'entrée de GPAD. Le membre du groupe accepte la politique qui correspond à un flux de données. Une politique qui ne correspond pas à un flux de données est éliminée, et la raison DEVRAIT être enregistrée dans le journal d'audit.

Un protocole GKM peut distribuer la politique de SA IPsec aux appareils IPsec qui se sont préalablement enregistrés auprès de lui. La méthode de distribution fait partie du protocole GKM et sort du domaine d'application du présent mémoire. Quand l'appareil IPsec reçoit cette nouvelle politique, il la compare au flux de données dans l'entrée de GPAD comme décrit ci-dessus.

4.2 Association de sécurité de groupe (GSA)

Une mise en œuvre de IPsec prenant en charge ces extensions va accepter un certain nombre d'associations de sécurité : une ou plusieurs SA IPsec plus une ou plusieurs SA GKM utilisées pour télécharger les paramètres qui sont utilisés pour créer les SA IPsec. Ces SA sont collectivement appelées une association de sécurité de groupe (GSA) [RFC3740].

4.2.1 Durée de vie de SA IPsec concurrentes et débordement de changement de clé

Durant la vie d'un groupe de diffusion groupée sûr, plusieurs associations de sécurité IPsec de groupe peuvent exister concurremment. Cela arrive principalement pour deux raisons :

- Il y a plusieurs envoyeurs de groupe autorisés dans le groupe, chacun avec sa propre SA IPsec, qui maintient l'état anti-répétition. Un groupe qui ne s'appuie pas sur des services IP de sécurité anti-répétition peut partager une SA IPsec pour tous ses envoyeurs de groupe.

- La durée de vie de deux (ou plus) SA IPsec d'un envoyeur de groupe peut se chevaucher afin qu'il y ait une continuité dans le flux de données de diffusion groupée à travers les événements de changement de clés du groupe. Cette capacité est appelée la "continuité de changement de clé".

L'algorithme de continuité de changement de clé dépend d'une interface de gestion de SA IPsec entre le sous système GKM et le sous système IPsec. Le sous système IPsec DOIT fournir les mécanismes d'interface de gestion au sous système GKM pour ajouter des SA IPsec et pour supprimer des SA IPsec. Pour illustrer cela, on définit l'algorithme de continuité de changement de clé dans les termes de deux paramètres de temporisation qui gouvernent la durée de vie des SA IPsec par rapport au début d'un événement de changement de clé de groupe. Cependant, il devrait être souligné que le sous système GKM interprète la politique de sécurité du groupe pour régler le moment correct d'activation et désactivation des SA IPsec. Une politique de groupe donnée peut choisir des valeurs de temporisateur qui diffèrent de celles recommandées par ce texte. Les deux paramètres de temporisateur de continuité de changement de clés sont :

1. ATD (Activation Time Delay) délai de temps d'activation : l'ATD définit le temps qu'il faut attendre après le début d'un événement de changement de clé pour activer de nouvelles SA IPsec. Le paramètre ATD est exprimé en unités de secondes. Normalement, le paramètre ATD est réglé au temps maximum qu'il faut pour livrer un message de diffusion groupée du GCKS à tous les membres du groupe. Pour un GCKS qui s'appuie sur un protocole fiable de transport de diffusion groupée (RMTP, *Reliable Multicast Transport Protocol*) le paramètre ATD pourrait être réglé égal au temps maximum de récupération d'erreur du RTMP. Quand un RMTP n'est pas présent, le paramètre ATD pourrait être réglé égal à la latence maximum de livraison d'un message de diffusion groupée sur le réseau à travers tous les points d'extrémité du groupe. L'ATD est un paramètre de la GKM de la politique de groupe. Cette valeur DEVRAIT être configurable à l'interface de gestion du propriétaire du groupe pour chaque groupe.

2. DTD (Deactivation Time Delay) délai de temps de désactivation : le DTD définit le délai après le début d'un événement de changement de clé pour désactiver les SA IPsec qui sont détruites par l'événement de changement de clé. L'objet du paramètre DTD est de minimiser l'exposition résiduelle du matériel de chiffrement d'un groupe après qu'un événement de changement de clé a retiré ce matériel de chiffrement. Le DTD est indépendant, et ne devrait pas être confondu avec l'attribut de durée de vie de la SA IPsec. Le paramètre DTD est exprimé en unités de secondes. Normalement, le paramètre DTD va être réglé à l'ADT plus le temps maximum que prend la livraison d'un message de diffusion groupée de l'envoyeur de groupe à tous les membres du groupe. Pour un envoyeur de groupe qui s'appuie sur un RMTP, le paramètre DTD pourrait être réglé égal à l'ADT plus le temps maximum de récupération d'erreur du RMTP. Quand un RMTP n'est pas présent, le paramètre DTD pourrait être réglé égal à l'ADT plus la latence maximum de livraison d'un message de diffusion groupée du réseau à travers tous les points d'extrémité du groupe. Un sous système GKM PEUT mettre en œuvre le DTD comme paramètre de politique de sécurité de groupe. Si un sous système GKM ne met pas en œuvre le paramètre DTD, d'autres mécanismes de politique de sécurité de groupe DOIVENT déterminer quand désactiver une SA IPsec.

Chaque message de diffusion groupée de changement de clé de groupe envoyé par un GCKS signale le début d'une nouvelle époque de SA IPsec d'envoyeur de groupe, avec chacune de ces époques ayant un ensemble associé de deux SA IPsec. Noter que le présent document se réfère aux mécanismes de changement de clé comme étant en diffusion groupée à cause de l'adaptabilité inhérente à la distribution de diffusion groupée IP. Cependant, il n'y a pas de raison particulière pour que les mécanismes de changement de clé soient en diffusion groupée. Par exemple, [ZLLY03] décrit une méthode de changement de clé employant les deux messages en envoi individuel et en diffusion groupée.

La composition du groupe interagit avec ces SA IPsec comme suit :

- Comme précurseur de l'envoyeur de groupe commençant son traitement de continuité de changement de clé, le GCKS envoie périodiquement en diffusion groupé un message Événement de changement de clé (RKE, *Re-Key Event*) au groupe. Le RKE en diffusion groupée PEUT contenir des directives de politique de groupe, une nouvelle politique de SA IPsec, et du matériel de chiffrement de groupe. En l'absence d'un RMTP, le GCKS peut retransmettre le RKE un nombre de fois défini par la politique pour améliorer la disponibilité des informations de changement de clé. Le sous système GKM lance les temporisateurs ATD et DTD après avoir reçu la dernière retransmission de RKE.

- Le sous système GKM interprète la diffusion groupée de RKE pour configurer la GSPD/SAD du groupe avec la nouvelle SA IPsec. Chaque SA IPsec qui remplace une SA existante est appelée une SA IPsec de "bord d'attaque". La SA IPsec de bord d'attaque a un nouvel indice de paramètre de sécurité (SPI, *Security Parameter Index*) et son matériel de chiffrement associé, qui le chiffre. Pour une durée de ATD secondes après l'envoi en diffusion groupée du RKE par le GCKS, un envoyeur de groupe ne transmet pas encore les données en utilisant la SA IPsec de bord d'attaque. Pendant ce temps là, les autres membres du groupe se préparent à utiliser cette SA IPsec en installant la SA IPsec de bord d'attaque dans leurs GSPD/SAD respectives.

- Après avoir attendu la période ATD, afin que tous les membres du groupe aient reçu et traité le message RKE, le sous système GKM ordonne à l'envoyeur de groupe de commencer à transmettre en utilisant la SA IPsec de bord d'attaque avec ses données chiffrées par le nouveau matériel de chiffrement. Seuls les membres du groupe autorisés peuvent déchiffrer ces transmissions en diffusion groupée de SA IPsec.

- La SA de "bord de queue" de l'envoyeur de groupe est la plus ancienne association de sécurité en usage par le groupe pour cet envoyeur. Tous les membres autorisés du groupe peuvent recevoir et déchiffrer les données pour cette SA, mais l'envoyeur de groupe ne transmet pas de nouvelles données en utilisant la SA IPsec de bord de queue après qu'il est passé à la SA IPsec de bord d'attaque. La SA IPsec de bord de queue est supprimée par les sous systèmes GKM de groupe après l'écoulement du délai de DTD depuis la transmission de RKE.

Cette stratégie de changement de clé permet au groupe d'évacuer ses datagrammes en transit dans le réseau tout en effectuant la transition à la SA IPsec de bord d'attaque. Étaler les rôles de chaque SA IPsec respective comme décrit ci-dessus améliore la synchronisation du groupe même quand il y a de forts délais de propagation du réseau. Noter que du fait des mouvements d'adjonction et de suppression de membres, chaque époque de SA IPsec d'envoyeur de groupe peut avoir un ensemble différent de membres du groupe.

C'est une décision de la politique de groupe de dire si la transition d'événement de changement de clé entre les époques fournit le secret vers l'avant et vers l'arrière. Le matériel et l'algorithme de chiffrement du protocole de changement de clés du groupe (par exemple, la hiérarchie de clés logiques ; voir la [RFC2627] et l'Appendice A de la [RFC4535]) appliquent cette politique. Les mises en œuvre PEUVENT offrir une option d'interface de gestion de propriétaire de groupe pour activer/désactiver la continuité du changement de clé pour un groupe particulier. La présente spécification exige qu'une mise en œuvre de GKM/IPsec DOIT prendre en charge au moins ces deux SA IPsec concurrentes par envoyeur de groupe ainsi que cet algorithme de continuité de changement de clé.

4.3 Authentification de l'origine des données

Comme défini dans la [RFC4301], l'authentification de l'origine des données est un service de sécurité qui vérifie l'identité de la source prétendue des données. Un code d'authentification de message (MAC, *Message Authentication Code*) est souvent utilisé pour réaliser l'authentification de l'origine des données pour les connexions partagées entre deux parties. Cependant, les méthodes normales d'authentification par MAC en utilisant un seul secret partagé ne sont pas suffisantes pour assurer l'authentification de l'origine des données pour des groupes de plus de deux parties. Avec un algorithme de MAC, chaque membre de groupe peut utiliser la clé de MAC pour créer une étiquette de MAC valide, qu'il soit ou non l'origine authentique des données de l'application de groupe.

Quand la propriété de l'authentification de l'origine des données est exigée pour une SA IPsec partagée par plus de deux parties, une transformation d'authentification où le receveur est assuré que l'envoyeur a généré ce message devrait être utilisée. Deux algorithmes possibles sont l'authentification tolérante aux pertes de flux à synchronisation efficace (TESLA, *Timed Efficient Stream Loss-Tolerant Authentication*) [RFC4082] ou la signature numérique RSA [RFC4359].

Dans certains cas (par exemple, les transformations d'authentification de signature numérique) le coût de traitement de l'algorithme est significativement supérieur à celui de la méthode d'authentification par code d'authentification de message haché (HMAC, *Hashed Message Authentication Code*). Pour protéger contre les attaques de déni de service provenant d'un appareil qui n'est pas autorisé à se joindre au groupe, la SA IPsec qui utilise cet algorithme peut être encapsulée dans une SA IPsec en utilisant un algorithme d'authentification par MAC. Cependant, faire ainsi exige que le paquet soit envoyé à travers la frontière IPsec une deuxième fois pour un traitement sortant supplémentaire sur l'envoyeur de groupe (voir le paragraphe 5.1 de la [RFC4301]) et une deuxième fois pour le traitement entrant sur les receveurs de groupe (voir le paragraphe 5.2 de la [RFC4301]). Cette utilisation de AH ou ESP encapsulé au sein de AH ou ESP s'accommode de la contrainte que AH et ESP définisse une valeur de vérification d'intégrité (ICV, *Integrity Check Value*) pour seulement une seule transformation d'authentificateur.

4.4 SA de groupe et gestion de clés

4.4.1 Coexistence de plusieurs protocoles de gestion de clés

Souvent, le sous système GKM va être introduit dans un sous système IPsec existant comme protocole de gestion de clé d'accompagnement de IKEv2 [RFC4306]. Une exigence fondamentale du sous système de sécurité du protocole GKM IP est que les deux protocoles GKM et IKEv2 puissent simultanément partager l'accès à une base de données commune de politique de sécurité de groupe et d'associations de sécurité. Les mécanismes qui fournissent un accès mutuellement exclusif aux structures communes de données de GSPD/SAD sont une affaire locale. Cela inclut l'antémémoire de GSPD-O et de GSPD-I. Cependant, les mises en œuvre devraient noter que l'allocation de SPI IKEv2 est entièrement indépendante de l'allocation de SPI GKM parce que les associations de sécurité de groupe sont qualifiées par une adresse de destination de diffusion groupée IP et peuvent facultativement avoir un qualificatif d'adresse de source IP. Voir le paragraphe 2.1 def [RFC4303] pour plus d'explications.

La base de données d'autorisation d'homologues exige une coordination explicite entre le protocole GKM et IKEv2. Le paragraphe 4.1.3 décrit ces interactions.

5. Traitement du trafic IP

Le traitement du trafic suit la Section 5 de la [RFC4301], avec les ajouts décrits ci-dessous quand ces extensions de diffusion groupée IP sont prises en charge.

5.1 Traitement du trafic IP sortant

Si une SA IPsec est marquée comme prenant en charge le mode tunnel avec préservation d'adresse (comme décrit au paragraphe 3.1) une ou les deux adresses de source et de destination de l'en-tête externe sont marquées comme étant préservées.

La construction de l'en-tête pour le mode tunnel est décrite au paragraphe 5.1.2 de la RFC 4301. Le premier tiret de ce paragraphe est amendé comme suit :

- Si la préservation d'adresse n'est pas marquée dans l'entrée de SAD pour l'adresse de source ou l'adresse de destination de l'en-tête IP externe, l'adresse de source et l'adresse de destination de l'en-tête IP externe identifient les "points d'extrémité" du tunnel (l'encapsuleur et le désencapsuleur). Si la préservation d'adresse est marquée pour l'adresse de source de l'en-tête IP, elle est copiée de l'adresse de source de l'en-tête IP interne. Si la préservation d'adresse est marquée pour l'adresse de destination de l'en-tête IP, elle est copiée de l'adresse de destination de l'en-tête IP interne. L'adresse de source et l'adresse de destination de l'en-tête IP interne identifient respectivement l'envoyeur et le receveur original du datagramme (du point de vue de ce tunnel). La préservation de l'adresse NE DOIT PAS être marquée quand la version IP de l'en-tête encapsulant et la version IP de l'en-tête interne ne correspondent pas.

Note (3), concernant la construction des adresses de tunnel au paragraphe 5.1.2.1 de la RFC 4301, il est amendé comme suit. (Note : pour abréger, la note (3) de la RFC 4301 n'est pas reproduite en entier.)

(3) Sauf si elles sont marquées pour la préservation d'adresse, les adresses locale et distante dépendent de la SA, qui est utilisée pour déterminer l'adresse distante, qui à son tour détermine quelle adresse locale (interface réseau) est utilisée pour transmettre le paquet. Si la préservation d'adresse est marquée pour l'adresse locale, elle est copiée de l'en-tête IP interne. Si la préservation d'adresse est marquée pour l'adresse distante, cette adresse est copiée de l'en-tête IP interne.

5.2 Traitement du trafic IP entrant

Les paquets protégés par IPsec générés par un appareil IPsec prenant en charge ces extensions de diffusion groupée peuvent (selon sa politique de GSPD) remplir un en-tête externe de tunnel avec une adresse de destination de sorte qu'ils ne sont pas adressés à un appareil IPsec. Cela exige qu'un appareil IPsec prenant en charge ces extensions de diffusion groupée accepte et traite le trafic IP qui n'est pas adressé à l'appareil IPsec lui-même. Les ajouts suivants au traitement IPsec du trafic IP entrant sont nécessaires.

Pour la compatibilité avec la RFC 4301, la phrase "adressé à cet appareil" est prise pour signifier les paquets avec une adresse de destination en envoi individuel appartenant au système lui-même, et aussi les paquets de diffusion groupée qui

sont reçus par le système lui-même. Cependant, les paquets de diffusion groupée non reçus par l'appareil IPsec ne sont pas considérés comme adressés à cet appareil.

La discussion du traitement du trafic IP entrant décrite au paragraphe 5.2 de la RFC 4301 est amendée comme suit :

Le premier tiret de l'élément 2 est amendé comme suit :

- Si le paquet apparaît comme étant protégé par IPsec et si il est adressé à cet appareil, ou apparaît être protégé par IPsec et est adressé à un groupe de diffusion groupée, on tente de le transposer en une SA active via la SAD. Noter que l'appareil peut avoir plusieurs adresses IP qui peuvent être utilisées dans la recherche de la SAD, par exemple, dans le cas de protocoles comme SCTP.

Un nouvel élément est ajouté à la liste entre les éléments 3a et 3b pour décrire le traitement des paquets IPsec avec application de la préservation de l'adresse de destination :

3aa. Si le paquet est adressé à un groupe de diffusion groupée et si AH ou ESP est spécifié comme protocole, le paquet est cherché dans la SAD. On utilise le SPI plus l'adresse de destination ou le SPI plus les adresses de destination et de source, comme spécifié au paragraphe 4.1. Si il n'y a pas de correspondance, le paquet est dirigé sur une recherche de SPD-I. Noter que si l'appareil IPsec est une passerelle de sécurité, et si la politique de SPD-I est de BYPASS *(outrepasser)* le paquet, une passerelle de sécurité suivante le long du chemin du paquet en diffusion groupée peut déchiffrer le paquet.

La Figure 3 de la RFC 4301 est mise à jour pour montrer le nouveau chemin de traitement défini dans le point 3aa.

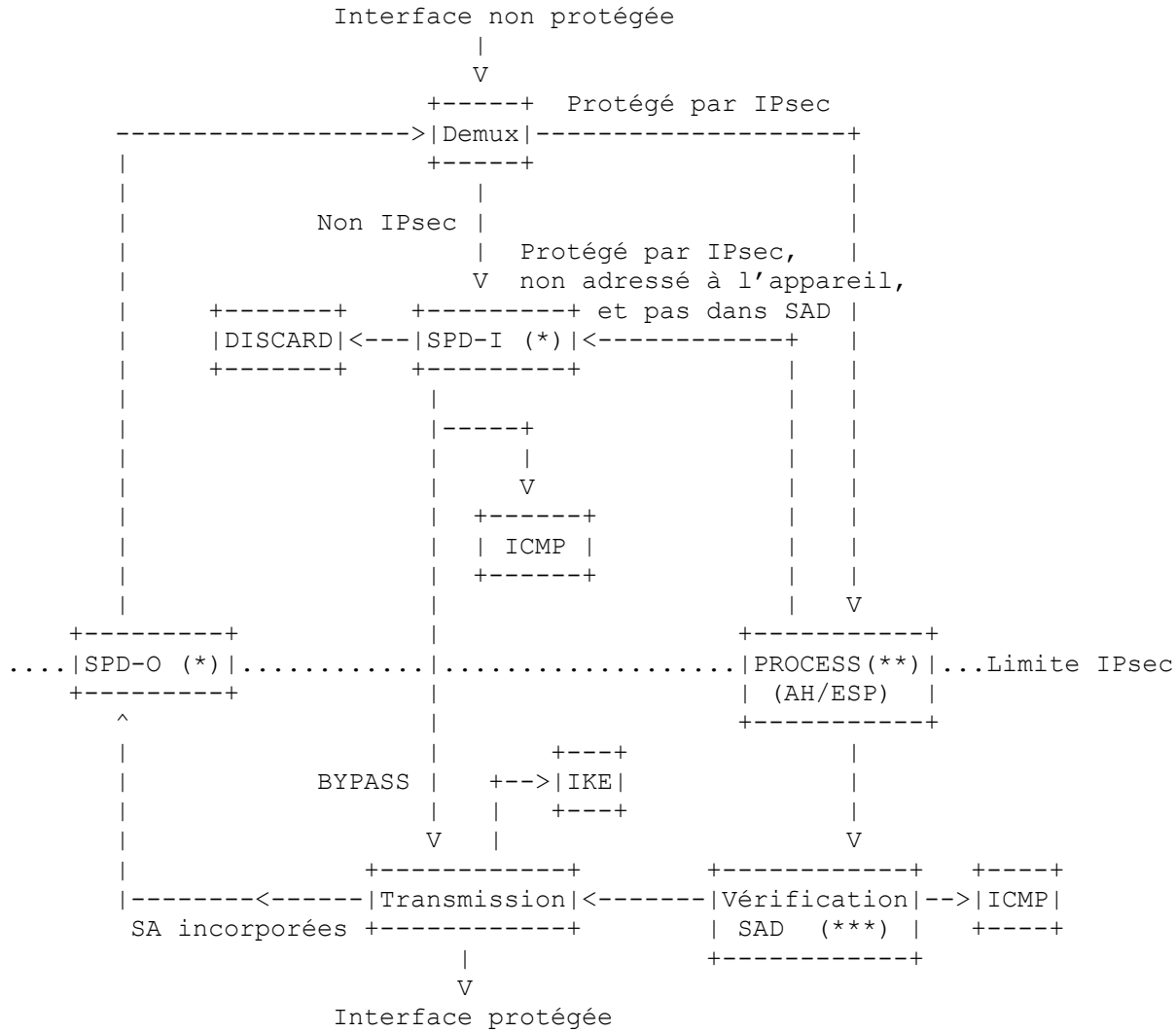

Figure 1 : Modèle de traitement pour le trafic entrant (amende la Figure 3 de la RFC 4301)

La discussion du traitement du trafic IP entrant du paragraphe 5.2 de la RFC 4301 est amendée pour insérer un nouvel élément 6 comme suit :

6. Si une SA IPsec est marquée comme prenant en charge le mode tunnel avec préservation d'adresse (comme décrit au paragraphe 3.1) la ou les adresses marquées (c'est-à-dire, la ou les adresses de source et/ou de destination dans l'en-tête IP externe DOIVENT être vérifiées comme ayant la même valeur que dans l'en-tête IP interne. Si les adresses ne sont pas cohérentes, le système IPsec DOIT éliminer le paquet et traiter l'incohérence comme un événement à examiner.

6. Considérations sur la sécurité

Les extensions de diffusion groupée à la sécurité IP définies par la présente spécification s'appuient sur l'architecture de sécurité en envoi individuel IP [RFC4301]. Par conséquent, cette spécification hérite de beaucoup des considérations sur la sécurité de la RFC 4301, et il est conseillé au lecteur de s'y reporter pour les directives d'accompagnement.

6.1 Questions de sécurité résolues par les extensions de diffusion groupée IPsec

Le service d'extension de sécurité de diffusion groupée IP fournit les mécanismes de couche réseau suivants pour des communications de groupe sûres :
- Confidentialité en utilisant une clé de chiffrement partagée par le groupe.
- Authentification de source et protection de l'intégrité de groupe en utilisant une clé d'authentification de groupe partagée.
- Authentification de l'origine des données de l'envoyeur de groupe en utilisant une signature numérique, TESLA, ou un autre mécanisme.
- Protection anti-répétition pour un nombre limité d'envoyeurs de groupe en utilisant la facilité de numéro de séquence ESP (ou AH).
- Filtrage des transmissions de diffusion groupée identifiées avec une adresse de source des systèmes qui ne sont pas autorisés par la politique de groupe à être envoyeurs de groupe. Cette caractéristique renforce le service IPsec de pare-feu sans état (c'est-à-dire, les entrées de SPD-I et/ou SDP-O avec une disposition de paquet spécifiée comme DISCARD).

À l'appui des services ci-dessus, la présente spécification améliore la définition des bases de données SPD, PAD, et SAD pour faciliter la gestion automatisée de clé de groupe de groupes cryptographiques de grande taille.

6.2 Questions de sécurité non résolues par les extensions de diffusion groupée IPsec

Comme noté au paragraphe 2.2. de la RFC 4301, il sort du domaine d'application de cette architecture de défendre les clés de groupe ou ses données d'application contre les attaques visant des faiblesses de l'environnement de fonctionnement dans lequel la mise en œuvre de IPsec s'exécute. Cependant, on devrait noter que le risque d'attaques ayant pour origine un adversaire dans le réseau est amplifié dans la mesure où les clés de groupe sont partagées entre un grand nombre de systèmes.

Les problèmes de sécurité qui restent non résolus par le service d'extension de diffusion groupée IPsec se divisent en deux grandes catégories : les attaques de l'extérieur et les attaques de l'intérieur.

6.2.1 Attaques de l'extérieur

Le service d'extension de diffusion groupée IPsec ne défend pas contre un adversaire en dehors du groupe qui a :
- la capacité de lancer une attaque en diffusion groupée de déni de service par arrosage contre le groupe, générée à partir d'un système dont le sous système IPsec ne filtre pas les transmissions de diffusion groupée non autorisées ;
- un routeur de diffusion groupée compromis, permettant à l'adversaire de corrompre ou supprimer tous les paquets de diffusion groupée destinés aux points d'extrémité du groupe en aval de ce routeur ;
- capturé une copie d'une transmission antérieure de paquet en diffusion groupée et la réexécute à un groupe qui n'a pas de service d'anti-répétition activé. Noter que pour un grand groupe de diffusion groupe toutes sources, il est impossible aux receveurs de groupe de conserver un état d'anti-répétition pour chaque envoyeur de groupe potentiel. Les politiques de groupe qui exigent une protection anti répétition pour un groupe de diffusion groupée toutes sources de grande taille devraient envisager un protocole de couche d'application de diffusion groupée qui puisse détecter et rejeter les

répétitions.

6.2.2 Attaques de l'intérieur

Pour les groupes à grande échelle, les extensions de diffusion groupée à la sécurité IP dépendent d'un protocole automatique de gestion de clé de groupe pour authentifier et autoriser correctement les membres de confiance en accord avec les politiques du groupe. Un ensemble d'un ou plusieurs secrets partagés de confiance pour tous les membres du groupe est inhérent au concept de groupe cryptographique. Par conséquent, les garanties de la sécurité du service ne sont pas plus fortes que le plus faible membre admis dans le groupe par le système GKM. Le système GKM est chargé de répondre de la détection de la compromission de membres du groupe en exécutant une procédure de changement de clés. Le protocole de changement de clé GKM va expulser les membres compromis du groupe et distribuer un nouveau matériel de chiffrement de groupe aux membres de confiance. Autrement, la politique de groupe peut exiger du système GKM qu'il termine le groupe.

Dans le cas où un adversaire a été admis dans le groupe par le système GKM, les attaques suivantes sont possibles et ne peuvent pas être résolues par le service d'extension de diffusion groupée IPsec :

- L'adversaire peut divulguer la clé secrète du groupe ou les données du groupe à un tiers non autorisé en dehors du groupe. Après la compromission de la clé ou des données du groupe, des méthodes cryptographiques telles que le traçage du traître ou le marquage peuvent aider au processus criminalistique. Cependant, ces méthodes sortent du domaine d'application de la présente spécification.
- L'adversaire infiltré peut falsifier les transmissions de paquets qui paraissent provenir d'un membre du groupe. Pour se défendre contre cette attaque, pour les transmissions de l'envoyeur de groupe qui méritent la surcharge, la politique de groupe peut exiger que l'envoyeur de groupe diffuse les paquets de diffusion groupée en utilisant le service d'authentification de l'origine des données.
- Si le service d'authentification de l'origine des données du groupe utilise des signatures numériques, alors l'adversaire infiltré peut lancer une attaque de déni de service sur les ressource de calcul en diffusant des paquets signés bogués.

6.3 Questions demise en œuvre ou de déploiement qui impactent la sécurité

6.3.1 Capacités d'algorithme cryptographique de groupe homogène

Le service d'extensions de diffusion groupée à la sécurité IP ne peut pas défendre contre une politique de sécurité de groupe mal construite qui permet un algorithme de chiffrement plus faible simplement parce que tous les points d'extrémité du groupe sont connus pour le prendre en charge. Malheureusement, les groupes de grande taille peuvent être difficiles à mettre à niveau aux meilleurs algorithmes de chiffrement disponibles. Une approche possible pour résoudre beaucoup de ces problèmes est le déploiement de groupes composites qui peuvent être à cheval sur des groupes hétérogènes [COMPGRP]. Une solution standard pour les groupes hétérogènes sera l'objet d'une activité de normalisation future. En attendant, la synchronisation des capacités cryptographiques d'un groupe pourrait être réalisée en utilisant un outil sûr et adaptable de gestion de distribution de logiciel.

6.3.2 Groupes qui s'étendent sur deux domaines de politique de sécurité o uplus

Les groupes à grande échelle peuvent s'étendre sur plusieurs juridictions légales (par exemple, des pays) qui appliquent des limites aux algorithmes de chiffrement ou à la force des clés. Comme défini actuellement, le service d'extension de diffusion groupée IPsec exige une seule politique de groupe par groupe. Comme noté plus haut, ce problème reste un domaine de normalisation future.

6.3.3 Localisateurs transitoires d'envoyeur de groupe de diffusion groupe spécifique de la source

Une adresse IP de source d'un envoyeur de groupe de diffusion groupée spécifique de source (SSM, *Source Specific Multicast*) peut changer de façon dynamique durant la vie d'un groupe de diffusion groupée sûre. Des exemples d'événements qui peuvent causer le changement de l'adresse de source de l'envoyeur de groupe incluent mais ne se limitent pas à un NAT, un changement induit par la mobilité à l'adresse d'entretien, et un hôte multi rattachements utilisant une nouvelle interface IP. Le changement de l'adresse IP de source de l'envoyeur de groupe va causer la péremption des entrées de GSPD relatives au groupe de diffusion groupé par rapport à l'état d'acheminement de diffusion groupée du groupe. Dans le pire des cas, il y a un risque que les données de l'envoyeur de groupe originaires d'une nouvelle adresse de source soient traitées comme outrepassées *(BYPASS)* par une passerelle de sécurité. Si ce scénario n'a pas été anticipé, alors cela pourrait laisser fuir les données du groupe. Par conséquent, il est recommandé que la SSM de groupe de diffusion

groupé sûre ait une politique DISCARD *(élimination)* par défaut pour toutes les adresses IP de source d'envoyeur de groupe non autorisés pour les adresses de destination IP de groupe SSM.

7. Remerciements

Les auteurs souhaitent remercier Steven Kent, Russ Housley, Pasi Eronen, et Tero Kivinen de leurs utiles commentaires.

La [RFC3552] "Lignes directrices sur la rédaction d'un texte sur les considérations sur la sécurité dans les RFC" a été consultée pour développer la section de considérations sur la sécurité du présent mémoire.

8. Références

8.1 Références normatives

[RFC1112] S. Deering, "Extensions d'hôte pour diffusion groupée sur IP", STD 5, août 1989. *(Mise à jour par la* RFC2236*)*

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

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

[RFC4302] S. Kent, "En-tête d'authentification IP", décembre 2005. *(P.S.)*

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

8.2 Références pour information

[COMPGRP] Gross G. et H. Cruickshank, "Multicast IP Security Composite Cryptographic Groups", Travail en cours, février 2007.

[RFC2526] D. Johnson, S. Deering, "Adresses réservées d'envoi à la cantonade de sous-réseau IPv6", mars 1999. *(P.S.)*

[RFC2627] D. Wallner, E. Harder, R. Agee,"Gestion de clés en diffusion groupée : problèmes et architectures", juin 1999. *(Info.)*

[RFC2914] S. Floyd, "Principes du contrôle d'encombrement", BCP 41, septembre 2000.

[RFC3171] Z. Albanna et autres, "Lignes directrices pour l'IANA sur l'allocation d'adresses de diffusion groupées IPv4", août 2001. (BCP0051) *(Remplacée par* RFC5771)

[RFC3306] B. Haberman, D. Thaler, "Adresses de diffusion groupée IPv6 fondées sur des préfixes d'envoi individuel", août 2002. (*MàJ par* RFC3956, RFC4489 et RFC7371) *(P.S.)*

[RFC3307] B. Haberman, "Lignes directrices pour l'allocation des adresses de diffusion groupée IPv6", août 2002. *(P.S.)*

[RFC3376] B. Cain et autres, "Protocole Internet de gestion de groupe, IGMP version 3", octobre 2002. *(P.S.)*

[RFC3547] M. Baugher, B. Weis, T. Hardjono et H. Harney, "Le domaine d'interprétation de groupe", juillet 2003. *(Obsolète, voir la* RFC6407)

[RFC3552] E. Rescorla, B. Korver, "Lignes directrices pour la rédaction d'une section de considérations sur la sécurité dans les RFC", juillet 2003. (BCP0072)

[RFC3569] S. Bhattacharyya et autres, "Généralités sur la diffusion groupée de source spécifique (SSM)", juillet 2003. *(Info.)*

[RFC3740] T. Hardjono et B. Weis, "Architecture de sécurité de groupe de diffusion groupée", mars 2004. *(Information)*

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

[RFC3940] B. Adamson et autres, "Protocole de diffusion groupée fiable s'appuyant sur l'accusé de réception négatif (NORM)", novembre 2004. *(Expérimentale ; Remplacée par* RFC5740)

[RFC4046] M. Baugher et autres, "Architecture de gestion de clé de groupe de diffusion groupée sécurisée (MSEC)", avril 2005. *(Info.)*

[RFC4082] A. Perrig et autres, "Authentification de flux tolérante aux pertes en temps efficace (TESLA) : Introduction à la transformation d'authentification de source de diffusion groupée", juin 2005. *(Information)*

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

[RFC4359] B. Weis, "Utilisation des signatures RSA/SHA-1 au sein d'une charge utile de sécurité par encapsulation (ESP) et d'un en-tête d'authentification (AH)", janvier 2006. *(P.S.)*

[RFC4535] H. Harney et autres, "GSAKMP : protocole de gestion de clés d'association de groupe sécurisé", juin 2006. *(P.S.)*

[RFC4601] B. Fenner et autres, "Diffusion groupée indépendante du protocole - Mode épars (PIM-SM) : spécification du protocole (révisée)", août 2006. (*Remplace* RFC2362 ; *MàJ par* RFC5059 ; *Rempl. par* RFC7761, STD83)

[RFC4891] R. Graveman et autres, "Utilisation d'IPsec pour sécuriser les tunnels IPv6 dans IPv4" mai 2007. *(Information)*

[ZLLY03] Zhang, X., and al., "Protocol Design for Scalable and Reliable Group Rekeying", IEEE/ACM Transactions on Networking (TON), Volume 11, Issue 6, décembre 2003.

Appendice A. Multicast Application Service Models

La grande majorité des applications de diffusion groupée sûre peuvent être cataloguées par leur modèle de service et le schéma d'accompagnement de communication intra groupe. Le sous système de gestion de clé de groupe (GKM) et le sous système IPsec DOIVENT tous deux être capables de configurer les politiques de sécurité de GSPD/SAD à correspondre à ces scénarios d'usage dominants. Les politiques de GSPD/SAD DOIVENT inclure la capacité de configurer les deux groupes de diffusion groupée Toute source et Spécifique de source pour chacun de ces modèles de service. L'interface de gestion de sous système GKM PEUT inclure des mécanismes pour configurer les politiques de sécurité pour des modèles de service non identifiés par cette norme.

A.1 Applications de diffusion groupée unidirectionnelle

Les applications de diffusion groupée de livraison de contenu multimédia qui n'ont pas de mécanisme de notification d'encombrement ou de retransmission de récupération d'erreur sont par nature unidirectionnelles. La RFC 4301 définit seulement des sélecteurs de trafic bidirectionnels en envoi individuel (selon les paragraphes 4.4.1 et 5.1 de la RFC 4301, sur la direction du sélecteur de trafic). Le sous système GKM exige que le sous système IPsec DOIT prendre en charge les entrées de SPD unidirectionnelles, ce qui cause l'installation d'une association de sécurité de groupe (GSA) dans seulement une direction. Les applications de diffusion groupée qui ont seulement un membre de groupe autorisé à transmettre peuvent utiliser ce type d'association de sécurité de groupe pour appliquer cette politique de groupe. Dans la direction inverse, la GSA n'a pas d'entrée de SAD, et la configuration de GSPD est établie facultativement pour éliminer les tentatives non autorisées de transmettre des paquets en envoi individuel ou de diffusion groupée au groupe.

L'interface de gestion du sous système GKM DOIT avoir la capacité d'établir un sous système de groupe GKM qui a une politique de sécurité de GSA unidirectionnelle.

A.2 Applications de diffusion groupée fiable bidirectionnelle

Certaines applications de diffusion groupée sûre sont caractérisées comme un envoyeur de groupe avec de nombreux receveurs mais avec un flux de données inverse exigé par un protocole fiable de transport de diffusion groupée (par exemple, NORM). Dans de telles applications, le flux de données de l'envoyeur est en diffusion groupée et le flux inverse provenant des receveurs du groupe est en envoi individuel à l'envoyeur. Normalement, le flux inverse de données porte des demandes de réparation d'erreur et d'état de contrôle d'encombrement.

Pour de telles applications, il est avantageux d'utiliser la même SA IPsec pour la protection des deux flux de données en envoi individuel et en diffusion groupée. Cela introduit un risque : l'application IKEv2 peut choisir le même SPI pour le trafic de réception en envoi individuel que celui que le GCKS choisit pour un groupe de SA IPsec couvrant le trafic en envoi individuel. Si les deux SA sont installées dans la SAD, la recherche de SA peut retourner la mauvaise SPI par suite d'une recherche de SA. Pour éviter ce problème, la SA IPsec installée par la GKM DEVRAIT utiliser le couple {adresse de destination IP, SPI} pour identifier chaque SA IPsec. De plus, la GKM DEVRAIT utiliser une adresse de destination IP d'envoi individuel qui ne corresponde à aucune adresse de destination IP utilisée par une SA IPsec IKEv2 en envoi individuel. Par exemple, supposons un membre de groupe utilisant les deux protocoles IKEv2 et GKM, et que la politique de sécurité de groupe exige de protéger le flux de données NORM inverse comme décrit ci-dessus. Dans ce cas, la politique de groupe DEVRAIT allouer et utiliser une unique adresse de destination IP en envoi individuel représentant l'envoyeur de groupe NORM. Cette adresse serait configurée en parallèle aux adresses IP existantes de l'envoyeur de groupe. Les sous systèmes GKM chez les deux points d'extrémité d'envoyeurs de groupe et de receveurs de groupe NORM vont installer la SA IPsec, protégeant les messages NORM en envoi individuel de façon que la recherche de SA utilise l'adresse de destination en envoi individuel ainsi que le SPI.

La GSA DEVRAIT utiliser le service de protection IPsec contre la répétition pour le flux de données de diffusion groupée de l'envoyeur au groupe de receveurs. À cause du problème de l'adaptabilité décrit dans le paragraphe suivant, il n'est pas pratique d'utiliser le service d'anti répétition IPsec pour les flux inverses en envoi individuel. Par conséquent, dans la direction inverse, la protection IPsec contre la répétition DOIT être désactivée. Cependant, les flux inverses en envoi individuel peuvent utiliser le mécanisme d'authentification de groupe IPsec du groupe. L'entrée de GSPD du receveur de groupe pour cette GSA DEVRAIT être configurée à permettre seulement une transmission en envoi individuel au nœud envoyeur plutôt qu'une transmission en diffusion groupée à tout le groupe.

Si une authentification ESP de signature numérique est disponible (par exemple, selon la RFC 4359) l'authentification de source PEUT être utilisée pour authentifier la transmission à l'envoyeur d'un nœud receveur. Le protocole GKM DOIT définir un mécanisme de gestion de clé pour que l'envoyeur de groupe valide la clé publique de signature certifiée de tout nœud receveur sans exiger que l'envoyeur conserve l'état sur chaque receveur de groupe.

Ce modèle de service d'application de diffusion groupée est RECOMMANDÉ parce que il inclut les capacités de retours de contrôle d'encombrement. Voir dans la [RFC2914] des informations de fond supplémentaires.

L'interface de gestion du propriétaire de groupe du sous système GKM DOIT avoir la capacité d'établir une entrée symétrique de GSPD et d'envoyeur de groupe. L'interface de gestion DEVRAIT être capable de configurer un groupe à avoir au moins 16 envoyeurs autorisés concurrents, chacun avec son propre état de GSA anti-répétition.

A.3 Applications de diffusion groupée Any-To-Many

Une autre famille d'applications de diffusion groupée sûre exhibe un schéma de communications de "un à plusieurs". Un exemple représentatif d'une telle application est une visioconférence combinée avec un tableau électronique.

Pour de telles applications, tous les membres (ou un large sous ensemble) du groupe sont des envoyeurs autorisés de diffusion groupée. Dans ces modèles de service, créer une SA IPsec distincte avec un état anti-répétition pour chaque envoyeur potentiel ne convient pas pour de larges groupes. Le groupe DEVRAIT partager une SA IPsec pour tous les envoyeurs. La SA IPsec NE DEVRAIT PAS utiliser le service de protection IPsec contre la répétition pour le flux de données de diffusion groupée de l'envoyeur aux receveurs du groupe.

L'interface de gestion du sous système GKM DOIT avoir la capacité d'établir un groupe ayant la politique de sécurité de GSA de diffusion groupée de un à plusieurs.

Appendice B. ASN.1 pour entrée de GSPD

Cet appendice montre une façon supplémentaire de décrire les entrées de GSPD, comme défini au paragraphe 4.1.1. Il utilise la syntaxe ASN.1 qui a été compilée. Cette syntaxe est simplement pour illustration et n'a pas besoin d'être employée dans une mise en œuvre pour réaliser la conformité. La description de GSPD du paragraphe 4.1.1 est normative. Comme montré au paragraphe 4.1.1, la GSPD met à jour la SPD et donc cet appendice met à jour l'identifiant d'objet SPD.

B.1 Champs spécifiques d'entrée de GSPD

Les champs suivants résument les champs de la GSPD qui ne sont pas présents dans la SPD.
- direction (dans une IPsecEntry)
- DirectionFlags
- noswap (dans une SelectorList)
- ap-l, ap-r (dans des TunnelOptions)

B.2 Module SPD

```
SPDModule

iso(1) org (3) dod (6) internet (1) security (5) mechanisms (5) ipsec (8) asn1-modules (3) spd-module (1) }

ÉTIQUETTES DE DÉFINITIONS IMPLICITES ::=

DÉBUT

IMPORTE
  RDNSequence DE PKIX1Explicit88
   { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) id-mod(0) id-pkix1-
explicit(18) } ;

-- Un SPD est une liste de politiques en ordre décroissant de préférence
   SPD ::= SEQUENCE DE SPDEntry

   SPDEntry ::= CHOIX {
      iPsecEntry       IPsecEntry,                          -- trafic PROTECT
      bypassOrDiscard  [0] BypassOrDiscardEntry }           -- DISCARD/BYPASS

   IPsecEntry ::= SEQUENCE {                               -- chaque entrée consiste en
      name        NameSets FACULTATIF,
      pFPs        PacketFlags,                             -- rempli à partir des fanions de paquet
                                  -- s'applique à tous les sélecteur de trafic correspondants dans la SelectorLists
      direction   DirectionFlags,                          -- direction de la SA
      condition   SelectorLists,                           -- "condition" de politique
      processing  Processing                               -- "action" de politique
      }

    BypassOrDiscardEntry ::= SEQUENCE {
       bypass      BOOLÉEN,                                -- VRAI, BYPASS, FAUX, DISCARD
       condition   InOutBound }

    InOutBound ::= CHOIX {
       outbound    [0] SelectorLists,
       inbound     [1] SelectorLists,
       bothways    [2] BothWays }

    BothWays ::= SEQUENCE {
       inbound     SelectorLists,
```

```
   outbound    SelectorLists }

NameSets ::= SEQUENCE {
   passed    ENSEMBLE DE Names-R,          -- confronté à l'identifiant IKE par le répondeur
   local     ENSEMBLE DE Names-I }         -- utilisé en interne par l'initiateur IKE

Names-R ::= CHOIX {                       -- identifiants IKEv2
   dName      RDNSequence,                -- ID_DER_ASN1_DN
   fqdn       FQDN,                       -- ID_FQDN
   rfc822     [0] RFC822Name,             -- ID_RFC822_ADDR
   keyID      CHAINE D'OCTETS }           -- KEY_ID

Names-I ::= CHAINE D'OCTETS               -- utilisé en interne par l'initiateur IKE

FQDN ::= IA5String

RFC822Name ::= IA5String

PacketFlags ::= CHAINE DE BITS {
-- si établi, prend la valeur du sélecteur dans le paquet établissant la SA, autrement, utilise la valeur en entrée de SPD
   localAddr    (0),
   remoteAddr   (1),
   protocol     (2),
   localPort    (3),
   remotePort   (4) }

DirectionFlags ::= CHAINE DE BITS {
-- si établi, installer la SA dans la direction spécifiée. Une politique symétrique est représentée en établissant les deux bits
   inbound   (0),
   outbound  (1)  }

SelectorLists ::= ENSEMBLE DE SelectorList

SelectorList ::= SEQUENCE {
   localAddr    AddrList,
   remoteAddr   AddrList,
   protocol     ProtocolChoice,
   noswap     BOOLÉEN }  -- ne pas échanger les adresses et accès local et distant sur les vérifications de SPD-S et
                            SPD-I entrants

Processing ::= SEQUENCE {
   extSeqNum   BOOLÉEN,                  -- VRAI, compteur de 64 bits, FAUX, de 32 bits
   seqOverflow BOOLÉEN,                  -- VRAI changement de clé, FAUX terminer & audit
   fragCheck   BOOLÉEN,                  -- VRAI vérification de fragment à états pleins
                                         -- FAUX, pas de vérification de fragment à états pleins
   lifetime    SALifetime,
   spi         ManualSPI,
   algorithms  ProcessingAlgs,
   tunnel      TunnelOptions FACULTATIF }    -- si absent, utiliser le mode transport

SALifetime ::= SEQUENCE {
   seconds   [0] ENTIER FACULTATIF,
   bytes     [1] ENTIER FACULTATIF }

ManualSPI ::= SEQUENCE {
   spi     ENTIER,
   keys    KeyIDs }

KeyIDs ::= SEQUENCE DE CHAINE D'OCTETS

ProcessingAlgs ::= CHOIX {
```

```
      ah        [0] IntegrityAlgs,                    -- AH
      esp       [1] ESPAlgs}                          -- ESP

   ESPAlgs ::= CHOIX {
      integrity         [0] IntegrityAlgs,            -- intégrité seulement
      confidentiality [1] ConfidentialityAlgs,        -- confidentialité seulement
      les deux          [2] IntegrityConfidentialityAlgs,
      combined          [3] CombinedModeAlgs }

   IntegrityConfidentialityAlgs ::= SEQUENCE {
      integrity         IntegrityAlgs,
      confidentiality ConfidentialityAlgs }

-- Algorithmes d'intégrité, rangés par préférence décroissante
   IntegrityAlgs ::= SEQUENCE DE IntegrityAlg

-- Algorithmes de confidentialité, rangés par préférence décroissante
   ConfidentialityAlgs ::= SEQUENCE DE ConfidentialityAlg

--  Algorithmes d'intégrité
   IntegrityAlg ::= SEQUENCE {
      algorithm   IntegrityAlgType,
      parameters  ANY – DÉFINI PAR l'algorithme -- FACULTATIF }

   IntegrityAlgType ::= ENTIER {
      none                    (0),
      auth-HMAC-MD5-96   (1),
      auth-HMAC-SHA1-96  (2),
      auth-DES-MAC            (3),
      auth-KPDK-MD5           (4),
      auth-AES-XCBC-96        (5)
-- à définir                  (6 à 65535)
      }

-- Algorithmes de confidentialité
   ConfidentialityAlg ::= SEQUENCE {
      algorithm   ConfidentialityAlgType,
      parameters  ANY                               -- DÉFINI PAR l'algorithme -- FACULTATIF }

   ConfidentialityAlgType ::= ENTIER {
      encr-DES-IV64    (1),
      encr-DES         (2),
      encr-3DES        (3),
      encr-RC5         (4),
      encr-IDEA        (5),
      encr-CAST        (6),
      encr-BLOWFISH    (7),
      encr-3IDEA       (8),
      encr-DES-IV32    (9),
      encr-RC4        (10),
      encr-NULL       (11),
      encr-AES-CBC    (12),
      encr-AES-CTR    (13)
-- à définir        (14 à 65535)
      }

   CombinedModeAlgs ::= SEQUENCE DE CombinedModeAlg

   CombinedModeAlg ::= SEQUENCE {
      algorithm   CombinedModeType,
      parameters  ANY                               -- DÉFINI PAR l'algorithme -- }
```

```
                                                -- défini en dehors de de document pour les modes AES.

    CombinedModeType ::= ENTIER {
       comb-AES-CCM    (1),
       comb-AES-GCM    (2)
--  à définir               (3 à 65535)
       }

    TunnelOptions ::= SEQUENCE {
       dscp       DSCP,
       ecn        BOOLÉEN,                    -- VRAI Copie CE à l'en-tête interne
       ap-l       BOOLÉEN,                    -- VRAI Copie l'en-tête IP interne
                                              -- adresse de source à l'adresse de source d'en-tête IP externe
       ap-r       BOOLÉEN,                    -- VRAI Copy en-tête IP interne
                                              -- adresse de destination à l'adresse de destination d'en-tête IP externe
       df         DF,
       addresses   TunnelAddresses }

    TunnelAddresses ::= CHOIX {
       ipv4       IPv4Pair,
       ipv6       [0] IPv6Pair }

    IPv4Pair ::= SEQUENCE {
       local       CHAINE D'OCTETS (TAILLE(4)),
       remote     CHAINE D'OCTETS (TAILLE(4)) }

    IPv6Pair ::= SEQUENCE {
       local        CHAINE D'OCTETS (TAILLE(16)),
       remote      CHAINE D'OCTETS (TAILLE(16)) }

    DSCP ::= SEQUENCE {
       copy      BOOLÉEN,                          -- VRAI, copié de l'en-tête interne
                                                   -- FAUX, ne pas copier
       mapping   CHAINE D'OCTETS FACULTATIF}       -- pointe sur le table siil n'y a pas de copie

    DF ::= ENTIER {
       clear    (0),
       set      (1),
       copy     (2) }

    ProtocolChoice::= CHOIX {
       anyProt  AnyProtocol,                       -- pour TOUT protocole
       noNext   [0] NoNextLayerProtocol,           -- n'a pas d'élément prochaine couche
       oneNext  [1] OneNextLayerProtocol,          -- a un élément prochaine couche
       twoNext  [2] TwoNextLayerProtocol,          -- a deux éléments prochaine couche
       fragment FragmentNoNext }                   -- n'a pas d'information de prochaine couche

    AnyProtocol ::= SEQUENCE {
       id              ENTIER (0),                 -- TOUT protocole
       nextLayer   AnyNextLayers }

    AnyNextLayers ::= SEQUENCE {                   -- avec soit
       first          AnyNextLayer,               -- TOUT sélecteur de prochaine couche
       second        AnyNextLayer }               -- TOUT sélecteur de prochaine couche

    NoNextLayerProtocol ::= ENTIER (2..254)

    FragmentNoNext ::= ENTIER (44)                 -- identifiant de fragment

    OneNextLayerProtocol ::= SEQUENCE {
       id         ENTIER (1..254),                 -- ICMP, MH, ICMPv6
```

```
      nextLayer   NextLayerChoice }                    -- ICMP Type*256+Code MH Type*256

   TwoNextLayerProtocol ::= SEQUENCE {
      id          ENTIER (2..254),                     -- Protocole
      local       NextLayerChoice,                     -- accès local et distant
      remote      NextLayerChoice }

   NextLayerChoice ::= CHOIX {
      any         AnyNextLayer,
      opaque      [0] OpaqueNextLayer,
      range       [1] NextLayerRange }

-- Représentation de ANY dans le champ prochaine couche
   AnyNextLayer ::= SEQUENCE {
      start       ENTIER (0),
      end         ENTIER (65535) }

-- Représentation de OPAQUE dans le champ prochaine couche.
-- Conforme à la convention IKE
   OpaqueNextLayer ::= SEQUENCE {
      start       ENTIER (65535),
      end         ENTIER (0) }

-- Gamme pour un champ prochaine couche
   NextLayerRange ::= SEQUENCE {
      start       ENTIER (0 à 65535),
      end         ENTIER (0 à 65535) }

-- Liste des adresses IP
   AddrList ::= SEQUENCE {
      v4List      IPv4List       FACULTATIF,
      v6List      [0] IPv6List   FACULTATIF }

-- Représentations d'adresse IPv4
   IPv4List ::= SEQUENCE DE IPv4Range
   IPv4Range ::= SEQUENCE {                         -- proche, mais pas tout à fait  ...
      ipv4Start    CHAINE D'OCTETS (TAILLE (4)),
      ipv4End      CHAINE D'OCTETS (TAILLE (4)) }

-- Représentations d'adresse IPv6
   IPv6List ::= SEQUENCE DE IPv6Range
   IPv6Range ::= SEQUENCE {                         -- proche, mais pas tout à fait ...
      ipv6Start    CHAINE D'OCTETS (TAILLE (16)),
      ipv6End      CHAINE D'OCTETS (TAILLE (16)) }

FIN
```

Adresse des auteurs

Brian Weis
Cisco Systems
170 W. Tasman Drive,
San Jose, CA 95134-1706
USA
mél : bew@cisco.com

George Gross
Secure Multicast Networks LLC
977 Bates Road
Shoreham, VT 05770
USA
mél : gmgross@securemulticast.net

Dragan Ignjatic
Polycom
Suite 200, 3605 Gilmore Way
Burnaby, BC V5G 4X5
Canada
mél : dignjatic@polycom.com