Groupe de travail Réseau
Request for Comments : 4301
RFC rendue obsolète : 2401
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

S. Kent
K. Seo
BBN Technologies

décembre 2005
novembre 2007

Architecture de sécurité pour le protocole Internet

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

Résumé
Le présent document décrit une version mise à jour d'une "architecture de sécurité pour IP", qui est destinée à fournir des services de sécurité pour le trafic à la couche IP. Le présent document rend obsolète la RFC 2401 (novembre 1998).

Dédicace
Le présent document est dédié à la mémoire de Charlie Lynn, longtemps collaborateur de BBN Technologies, qui a fait des contributions très significatives aux documents IPsec.

Table des matières

1 Introduction

1.1 Résumé du contenu du document

Le présent document spécifie l'architecture de base des systèmes conformes à IPsec. Il décrit comment fournir un ensemble de services de sécurité pour le trafic à la couche IP, aussi bien pour les environnements IPv4 [RFC0791] que IPv6 [RFC2460]. Le présent document décrit les exigences pour les systèmes qui mettent en œuvre IPsec, les éléments fondamentaux de tels systèmes, et comment les éléments s'harmonisent ensemble et avec l'environnement IP. Il décrit aussi les services de sécurité offerts par les protocoles IPsec, et comment ces services peuvent être utilisés dans l'environnement IP. Le présent document ne vise pas tous les aspects de l'architecture IPsec.

D'autres documents visent des détails architecturaux supplémentaires dans des environnements spécialisés, par exemple, l'utilisation de IPsec dans les environnements de traducteur d'adresse réseau (NAT, *Network Address Translation*) et d'une prise en charge plus complète de la diffusion groupée IP. Les composants fondamentaux de l'architecture de sécurité IPsec sont exposés sous l'aspect de leur fonction nécessaire sous-jacente. D'autres RFC (voir au paragraphe 1.3 des références aux autres documents) définissent les protocoles en (a), (c), et (d).

a. Protocoles de sécurité – En-tête d'authentification (AH) et Encapsulement de charge utile de sécurité (ESP)
b. Associations de sécurité – ce qu'elles sont et comment elles fonctionnent, comment elles sont gérées, le traitement associé
c. Gestion des clés -- manuel et automatisé (l'échange de clés Internet (IKE))
d. Algorithmes cryptographiques pour l'authentification et le chiffrement

Le présent document n'est pas une architecture de sécurité pour l'Internet ; il ne vise la sécurité qu'à la couche IP, fournie par l'utilisation d'une combinaison de mécanismes de sécurité cryptographiques et de protocole.

La façon d'écrire "IPsec" est celle préférée et elle est utilisée dans la présente norme et celles qui se rapportent à IPsec. Toutes les autres manières d'écrire IPsec (par exemple, IPSEC, IPSec, ipsec) sont déconseillées. Cependant, toute forme d'écriture de la séquence des lettres "IPsec" devrait être comprise comme se référant aux protocoles IPsec.

Les mots clés DOIT, NE DOIT PAS, EXIGE, DEVRA, NE DEVRA PAS, DEVRAIT, NE DEVRAIT PAS, RECOMMANDE, PEUT, et FACULTATIF, lorsqu'ils apparaissent dans le présent document, sont à interpréter comme décrit dans la [RFC 2119].

1.2 Public visé

Le public visé par le présent document est principalement celui des individus qui mettent en œuvre la présente technologie de sécurité IP ou qui construisent des systèmes qui vont utiliser cette technologie. Les utilisateurs qui s'intéressent

techniquement à cette technologie (utilisateurs finaux ou administrateurs de système) font aussi partie du public visé. Un glossaire est fourni à l'Appendice A pour aider à retrouver le vocabulaire de base. Le présent document suppose que le lecteur est familiarisé avec le protocole Internet (IP), les technologies réseau qui s'y rapportent, et les termes et concepts généraux d'information des systèmes de sécurité.

1.3 Documents connexes

Comme mentionné ci-dessus, d'autres documents donnent des définitions détaillées de certains des composants d'IPsec et de leurs inter relations. Parmi eux sont des RFC sur les sujets suivants :

a. Protocoles de sécurité – RFC qui décrivent les protocoles d'en-tête d'authentification (AH) [RFC4302] et d'encapsulation de la charge utile de sécurité (ESP) [RFC4303].
b. Algorithmes cryptographiques pour l'intégrité et le chiffrement -- une RFC qui définit les algorithmes obligatoires par défaut à utiliser avec AH et ESP [RFC4305], une RFC semblable définit les algorithmes obligatoires avec IKEv2 [RFC4307] plus une autre RFC pour chaque algorithme cryptographique.
c. Gestion de clé automatique – des RFC sur le "protocole d'échange de clés sur Internet (IKEv2)" [RFC4306] et sur les "algorithmes cryptographiques à utiliser dans les échanges de clés sur Internet, version 2 (IKEv2)" [RFC4307].

2 Objectifs

2.1 Description des buts/objectifs/exigences/problèmes

IPsec a été conçu pour fournir une sécurité d'interopérabilité de haute qualité, fondée sur la cryptographie pour IPv4 et IPv6. L'ensemble des services de sécurité offerts inclut le contrôle d'accès, l'intégrité sans connexion, l'authentification de l'origine des données, la détection et le rejet des répétitions (une forme d'intégrité de séquence partielle), la confidentialité (via le chiffrement) et une confidentialité limitée des flux de trafic. Ces services sont fournis à la couche IP, offrant une protection standard pour tous les protocoles qui peuvent être portés sur IP (y compris IP lui-même).

IPsec inclut la spécification de la fonction pare-feu minimale, car c'est un aspect essentiel du contrôle d'accès à la couche IP. Les mises en œuvre sont libres de fournir des mécanismes de pare-feu plus sophistiqués, et de mettre en œuvre la fonction obligatoire selon IPsec à l'aide de mécanismes plus sophistiqués. (Noter que l'interopérabilité peut souffrir si des contraintes de pare-feu supplémentaires sont imposées aux flux de trafic par une mise en œuvre de IPsec mais ne peuvent être négociées sur la base des caractéristiques de choix du trafic définies dans le présent document et négociées via IKEv2.) La fonction pare-feu d'IPsec utilise l'authentification et l'intégrité mises en application par la cryptographie fournie pour tout le trafic IPsec afin d'offrir un meilleur contrôle d'accès que ce qui pourrait être obtenu à travers l'utilisation d'un pare-feu (un qui ne serait pas instruit des paramètres internes d'IPsec) plus une protection cryptographique séparée.

La plupart des services de sécurité sont fournis grâce à l'utilisation de deux protocoles de sécurité du trafic, l'en-tête d'authentification (AH, *Authentication Header*) et l'encapsulation de charge utile de sécurité (ESP, *Encapsulating Security Payload*) et par l'utilisation de procédures et protocoles de gestion de clés cryptographiques. L'ensemble des protocoles IPsec employés dans un contexte, et la façon dont ils sont employés, sera déterminé par les usagers/administrateurs dans ce contexte. Le but de l'architecture IPsec est d'assurer que les mises en œuvre conformes incluent les interfaces de services et de gestion nécessaires pour satisfaire aux exigences de sécurité d'une large population d'utilisateurs.

Lorsque IPsec est correctement mis en œuvre et développé, il ne devrait pas avoir d'effets contraires sur les usagers, hôtes, et autres composants de l'Internet qui n'utilisent pas IPsec pour la protection du trafic. Les protocoles de sécurité d'IPsec (AH et ESP, et à une moindre échelle, IKE) sont conçus comme des algorithmes cryptographiques indépendants. Cette modularité permet le choix de différents ensembles d'algorithmes cryptographiques en tant que de besoin, sans affecter les autres parties de la mise en œuvre. Par exemple, des communautés d'utilisateurs différentes peuvent utiliser, si besoin en est, des ensembles d'algorithmes cryptographiques différents (créant ainsi des groupes mis en œuvre par la cryptographie).

Pour faciliter l'interopérabilité dans l'Internet mondial, un ensemble d'algorithmes cryptographiques par défaut à utiliser avec AH et ESP est spécifié dans la [RFC4305] et un ensemble d'algorithmes de mise en œuvre obligatoire pour IKEv2 est spécifié dans a [RFC4307]. Les [RFC4305] et [RFC4307] seront périodiquement mis à jour pour rester dans le rythme des avancées du calcul et de la cryptologie. En spécifiant ces algorithmes dans des documents distincts des spécifications AH, ESP, et IKEv2, ces algorithmes peuvent être mis à jour ou remplacés sans affecter les progrès de la normalisation du reste de la série des documents IPsec. L'utilisation de ces algorithmes cryptographiques, en conjonction avec les protocoles IPsec de protection du trafic et de gestion des clés, est destinée à permettre aux développeurs de systèmes et d'applications de déployer des technologies de sécurité cryptographique de haute qualité à la couche Internet.

2.2 Avertissements et hypothèses

La série des protocoles IPsec et des algorithmes cryptographiques associés par défaut est conçue pour fournir une sécurité de grande qualité pour le trafic Internet. Cependant, la sécurité offerte par l'utilisation de ces protocoles dépend en fin de compte de la qualité de leur mise en œuvre, ce qui est en dehors du domaine d'application du présent ensemble de normes. De plus, la sécurité d'un système ou réseau informatique est fonction de nombreux facteurs, y compris personnels, physiques, de procédure, de relations compromettantes, et des pratiques de sécurité informatique. Et donc, IPsec est seulement une partie d'un système global d'architecture de sécurité.

Finalement, la sécurité apportée par l'utilisation d'IPsec est très dépendante de nombreux aspects de l'environnement opérationnel dans lequel s'exécute la mise en œuvre IPsec. Par exemple, des défauts dans la sécurité du système d'exploitation, une mauvaise qualité des sources de nombres aléatoires, des protocoles et pratiques de gestion de système négligents, etc., peuvent tous dégrader la sécurité fournie par IPsec. Comme indiqué ci-dessus, aucun de ces attributs environnementaux n'entre dans le domaine d'application de la présente norme ou des autres normes IPsec.

3 Vue générale du système

La présente section donne une description générale de la façon dont fonctionne IPsec, des composants du système, et de comment ils s'articulent pour fournir les services de sécurité notés ci-dessus. Le but de cette description est de permettre au lecteur de "visualiser" le processus/système global, de voir comment il s'articule dans l'environnement IP, et de fournir un contexte aux sections ultérieures du présent document, qui décrivent chacun des composants plus en détail.

Une mise en œuvre IPsec fonctionne dans un hôte, comme une passerelle de sécurité (SG, *passerelle de sécurité*), ou comme un appareil indépendant, apportant la protection au trafic IP. (Une passerelle de sécurité est un système intermédiaire qui met en œuvre IPsec, par exemple, un pare-feu ou un routeur qui possède la capacité IPsec.) Des détails sur ces classes de mises en œuvre sont fournis plus loin, au paragraphe 3.3. La protection offerte par IPsec se fonde sur des exigences définies par une base de données de politique de sécurité (SPD, *Security Policy Database*) établie et entretenue par un usager ou un administrateur de système, ou par une application fonctionnant sous des contraintes établies par l'un d'eux. En général, les paquets sont choisis pour une des trois actions de traitement fondées sur les informations d'en-tête IP et de la couche suivante ("Sélecteurs", paragraphe 4.4.1.1) comparées aux entrées de la SPD. Chaque paquet est soit PROTEGÉ en utilisant les services de sécurité IPsec, ÉLIMINÉ, soit autorisé à OUTREPASSER la protection IPsec, sur la base des politiques applicables de la SPD identifiées par les sélecteurs.

3.1 Ce que fait IPsec

IPsec crée une frontière entre les interfaces non protégées et protégées, pour un hôte ou un réseau (voir la Figure 1 ci-dessous). Le trafic traversant la frontière est soumis au contrôle d'accès spécifié par l'usager ou l'administrateur responsable de la configuration IPsec. Ces contrôles indiquent si les paquets traversent la frontière sans obstacle, sont présentés aux services de sécurité via AH ou ESP, ou sont éliminés.

Les services de sécurité IPsec sont présentés à la couche IP par la sélection des protocoles de sécurité appropriés, des algorithmes cryptographiques, et des clés cryptographiques. IPsec peut être utilisé pour protéger un ou plusieurs "chemins" (a) entre une paire d'hôtes, (b) entre une paire de passerelles de sécurité, ou (c) entre une passerelle de sécurité et un hôte. Une mise en œuvre d'hôte conforme DOIT prendre en charge (a) et (c) et une passerelle de sécurité conforme doit prendre en charge ces trois formes de connectivité, car dans certaines circonstances une passerelle de sécurité agit comme un hôte.

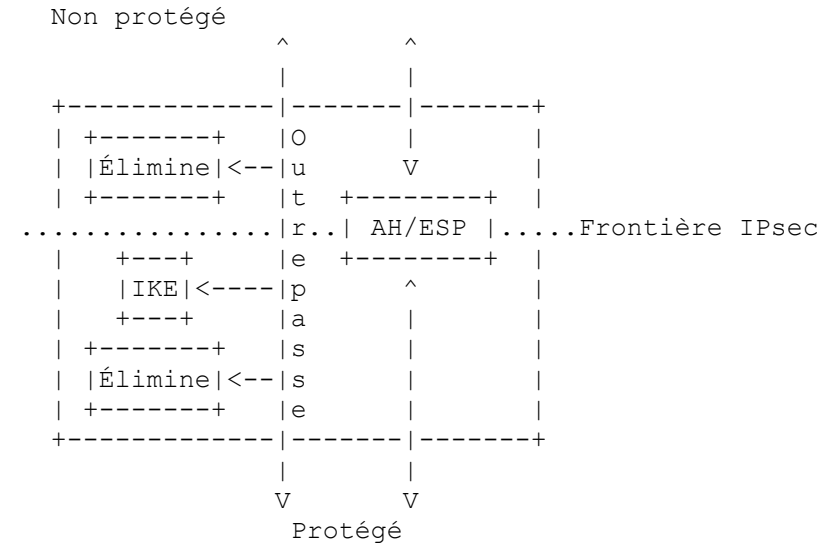


Figure 1 : Modèle général de traitement IPsec

Dans ce diagramme, "non protégé" se réfère à une interface qui pourrait aussi être décrite comme "boîte noire" ou "texte chiffré". Ici, "protégé" se réfère à une interface qui pourrait aussi être décrite comme "rouge" ou "texte en clair". L'interface protégée notée ci-dessus peut être interne, par exemple, dans une mise en œuvre d'hôte de IPsec, l'interface protégée peut relier à une interface de couche de connexion présentée par le système d'exploitation. Dans le présent document, le terme "entrant" se réfère au trafic entrant dans une mise en œuvre IPsec via l'interface non protégée ou émis par la mise en œuvre du côté non protégé de la frontière et dirigé vers l'interface protégée. Le terme "sortant" se réfère au trafic entrant dans la mise en œuvre via l'interface protégée, ou émis par la mise en œuvre sur le côté protégé de la frontière et dirigé vers l'interface non protégée. Une mise en œuvre IPsec peut prendre en charge plus d'une interface sur l'un ou l'autre ou sur les deux côtés de la frontière.

Noter les facilités pour éliminer du trafic sur l'un ou l'autre côté de la frontière IPsec : la facilité BYPASS *(outrepasser)* qui permet au trafic de traverser la frontière sans protection cryptographique, et la référence à IKE comme à une clé du côté protégé et une fonction de gestion de la sécurité.

IPsec prend facultativement en charge la négociation de la compression IP [RFC3173], motivée en partie par l'observation que lorsque le chiffrement est employé au sein d'IPsec, il empêche une compression effective par les couches de protocole inférieures.

3.2 Comment fonctionne IPsec

IPsec utilise deux protocoles pour fournir des services de sécurité du trafic -- en-tête d'authentification (AH) et encapsulation de charge utile de sécurité (ESP). Ces deux protocoles sont décrits en détail dans leurs RFC respectives [RFC4302], [RFC4303]. Les mises en œuvre IPsec DOIVENT prendre en charge ESP et PEUVENT prendre en charge AH. (La prise en charge de AH a été dégradée en PEUT parce que l'expérience a montré qu'il y a très peu de contextes dans lesquels ESP ne peut pas fournir les services de sécurité requis. Noter qu'ESP peut être utilisé pour ne fournir que l'intégrité, sans la confidentialité, le rendant comparable à AH dans la plupart des contextes.)

- L'en-tête d'authentification IP (AH) [RFC4302] offre l'intégrité et l'authentification de l'origine des données, avec un dispositif anti-répétition facultatif (à la discrétion du receveur).

- Le protocole d'encapsulation de charge utile de sécurité (ESP) [RFC4303] offre le même ensemble de services, et offre aussi la confidentialité. L'utilisation de ESP pour fournir la confidentialité sans l'intégrité N'EST PAS RECOMMANDÉE. Lorsque ESP est utilisé avec la confidentialité activée, il y a des dispositions pour la confidentialité de flux de trafic limités, c'est-à-dire, des dispositions pour cacher la longueur du paquet, et pour faciliter une génération efficace et éliminer les mauvais paquets. Cette capacité sera vraisemblablement efficace principalement dans un réseau virtuel privé (VPN) et des contextes de recouvrement de réseau.

- AH et ESP offrent tous deux le contrôle d'accès, mis en application au moyen de la distribution de clés de chiffrement et de la gestion des flux de trafic selon la base de données de politique de sécurité (SPD, § 4.4.1).

Ces protocoles peuvent s'appliquer individuellement ou en combinaison les uns avec les autres pour fournir des services de sécurité IPv4 et IPv6. Cependant, la plupart des exigences de sécurité peuvent être satisfaites par l'utilisation d'ESP seul. Chaque protocole prend en charge deux modes d'utilisation : le mode transport et le mode tunnel. Dans le mode transport, AH et ESP fournissent la protection principalement pour les protocoles de la couche suivante ; dans le mode tunnel, AH et ESP sont appliqués aux paquets IP tunnelés. Les différences entre les deux modes sont exposées au paragraphe 4.1.

IPsec permet à l'usager (ou administrateur de système) de contrôler la granularité qu'offre un service de sécurité. Par exemple, on peut créer un seul tunnel chiffré pour porter tout le trafic entre deux passerelles de sécurité, ou un tunnel chiffré séparé peut être créé pour chaque connexion TCP entre chaque paire d'hôtes communiquant à travers ces passerelles. IPsec, grâce au paradigme de gestion SPD, incorpore des dispositifs pour spécifier :
- quel protocole de sécurité (AH ou ESP) employer, le mode (transport ou tunnel), les options de service de sécurité, quels algorithmes cryptographiques utiliser, et dans quelles combinaisons utiliser les protocoles et services spécifiés, et
- la granularité à laquelle la protection devrait être appliquée.

Parce que la plupart des services de sécurité fournis par IPsec exigent l'utilisation de clés de chiffrement, IPsec s'appuie sur un ensemble séparé de mécanismes pour mettre ces clés en place. Le présent document exige la prise en charge de la distribution de clés à la fois manuelle et automatique. Il spécifie une approche spécifique fondée sur les clés publiques (IKEv2 [RFC4306]) pour la gestion de clés automatique, mais d'autres techniques automatiques de distribution de clés PEUVENT être utilisées.

Note : Le présent document rend obligatoire la prise en charge de plusieurs dispositifs pour lesquels la prise en charge est

disponible dans IKEv2 mais pas dans IKEv1, par exemple, la négociation d'une SA représentant des gammes de ports locaux et distants, ou la négociation de plusieurs SA avec les mêmes sélecteurs. Donc, le présent document suppose l'utilisation de IKEv2 ou d'une clé et système de gestion d'association de sécurité avec des dispositifs comparables.

3.3 Où IPsec peut être mis en œuvre

IPsec peut être mis en œuvre dans un hôte de nombreuses façons, ou en conjonction avec un routeur ou pare-feu pour créer une passerelle de sécurité, ou comme un appareil de sécurité indépendant.

a. IPsec peut être intégré dans la pile IP native. Cela exige l'accès au code source IP et est applicable à la fois aux hôtes et aux passerelle de sécurités, bien que les mises en œuvre d'hôte natives bénéficient le plus de cette stratégie, comme il sera expliqué plus loin (paragraphe 4.4.1, alinéa 6 ; paragraphe 4.4.1.1, dernier alinéa).

b. Dans une mise en œuvre "prise dans la pile" (BITS, *bump-in-the-stack*), IPsec est mis en œuvre "en dessous" d'une mise en œuvre existante d'une pile de protocoles IP, entre le IP natif et les pilotes de réseau locaux. L'accès au code source pour la pile IP n'est pas exigé dans ce contexte, rendant cette approche de mise en œuvre appropriée pour une utilisation avec les systèmes traditionnels. Cette approche, quant elle est adoptée, est habituellement utilisée dans les hôtes.

c. L'utilisation d'un processeur dédié de protocole de sécurité en ligne est un dispositif de conception courante pour les systèmes utilisés par les militaires, et aussi quelques systèmes commerciaux. On l'appelle parfois une mise en œuvre "prise sur le fil" (BITW, *bump-in-the-wire*). De telles mises en œuvre peuvent être conçues pour servir soit à un hôte soit à une passerelle. Habituellement, l'appareil BITW est lui-même adressable sur IP. Lorsqu'il ne prend en charge qu'un seul hôte, il peut être assez analogue à une mise en œuvre BITS, mais en prenant en charge un routeur ou un pare-feu, il doit fonctionner comme une passerelle de sécurité.

Le présent document parle souvent d'utilisation d'IPsec par un hôte ou une passerelle de sécurité, sans égard au fait que la mise en œuvre est native, BITS, ou BITW. Lorsque la distinction entre ces options de mise en œuvre est significative, le document fait référence à l'approche spécifique de mise en œuvre.

Une mise en œuvre d'hôte IPsec peut apparaître dans des appareils qu'on ne percevrait pas comme "hôtes". Par exemple, un routeur peut employer IPsec pour protéger des protocoles d'acheminement (par exemple, BGP) et des fonctions de gestion (par exemple, Telnet), sans affecter le trafic d'abonnés qui traverse le routeur. Une passerelle de sécurité peut employer des mises en œuvre IPsec séparées pour protéger son trafic de gestion et le trafic d'abonné. L'architecture décrite dans le présent document est très souple. Par exemple, un ordinateur avec une mise en œuvre d'origine de son système d'exploitation complètement conforme à IPsec devrait être capable d'être configuré pour protéger les applications résidentes (l'hôte) et pour fournir une protection de passerelle de sécurité pour le trafic traversant l'ordinateur. Une telle configuration utiliserait les tableaux de transmission et la fonction de sélection SPD décrite aux paragraphes 5.1 et 5.2.

4 Associations de sécurité

La présente section définit les exigences de gestion des associations de sécurité pour toutes les mises en œuvre IPv6 et pour celles des mises en œuvre IPv4 qui utilisent AH ou ESP, ou à la fois AH et ESP. Le concept d'une "association de sécurité" (SA) est fondamental pour IPsec. AH et ESP utilisent tous deux les SA, et une fonction majeure de IKE est l'établissement et la maintenance des SA. Toutes les mises en œuvre de AH ou ESP DOIVENT prendre en charge le concept de SA tel que décrit ci-dessous. Le reste de la présente section décrit divers aspects de la gestion de SA, définit les caractéristiques requises pour une gestion de la politique de SA et les techniques de gestion de SA.

4.1 Définition et domaine d'application

Une SA est une "connexion" simplex qui offre des services de sécurité au trafic qu'elle porte. Les services de sécurité sont offerts à une SA par l'utilisation de AH, ou ESP, mais pas les deux. Si les protections AH et ESP sont toutes deux appliquées à un flux de trafic, deux SA doivent être créées et coordonnées pour effectuer la protection par une application itérative des protocoles de sécurité. Pour sécuriser normalement une communication bidirectionnelle entre deux systèmes IPsec, une paire de SA (une dans chaque direction) est nécessaire. IKE crée explicitement des paires de SA en application de cette exigence d'usage courante.

Pour une SA utilisée pour porter du trafic en envoi individuel, l'index des paramètres de sécurité (SPI, *Security Parameters Index*) suffit par lui-même à spécifier une SA. (Pour des informations sur le SPI, voir l'Appendice A et les spécifications de AH et ESP [RFC4302], [RFC4303].) Cependant, en tant qu'affaire locale, une mise en œuvre peut choisir d'utiliser le SPI

en conjonction avec le type de protocole IPsec (AH ou ESP) pour l'identification de la SA. Si une mise en œuvre IPsec prend en charge la diffusion groupée, elle DOIT alors prendre en charge les SA de diffusion groupée en utilisant l'algorithme ci-dessous pour transposer les datagrammes IPsec entrant en SA. Les mises en œuvre qui n'acceptent que le trafic en envoi individuel n'ont pas besoin de mettre en œuvre cet algorithme de démultiplexage.

Dans de nombreuses architectures de diffusion groupée sécurisées, par exemple, [RFC3740], un contrôleur de groupe/serveur de clé central alloue de façon unilatérale le SPI de l'association de sécurité de groupe GSA, *Group Security Association*). Cette allocation de SPI n'est pas négociée ou coordonnée avec les sous-systèmes de gestion de clés (par exemple, IKE) qui résident dans les systèmes d'extrémité individuels qui constituent le groupe. Par conséquent, il est possible qu'une GSA et une SA d'envoi individuel puissent simultanément utiliser le même SPI. Une mise en œuvre IPsec à capacité de diffusion groupée DOIT correctement démultiplexer le trafic entrant même dans le contexte de collisions de SPI.

Chaque entrée de la base de données de SA (SAD, *SA Database*) (paragraphe 4.4.2) doit indiquer si la recherche de SA utilise l'adresse IP de destination, ou les adresses IP de destination et de source, en plus du SPI. Pour les SA de diffusion groupée, le champ protocole n'est pas employé pour les recherches de SA. Pour chaque paquet entrant, protégé par IPsec, une mise en œuvre doit conduire sa recherche dans la SAD de telle sorte qu'elle trouve l'entrée qui correspond au plus "long" identifiant de SA. Dans ce contexte, si deux entrées de SAD ou plus correspondent sur la base de la valeur du SPI, l'entrée qui correspond alors aussi sur la base de l'adresse de destination, ou des adresses de destination et de source (comme indiqué dans l'entrée de la SAD) est celle de la plus "longue" correspondance. Ceci implique un ordre logique de la recherche dans la SAD comme suit :

1. Recherche dans la SAD pour une correspondance de la combinaison de SPI, adresse de destination, et adresse de source. Si une entrée de SAD correspond, traiter alors le paquet entrant avec cette entrée de SAD correspondante. Autrement, passer à l'étape 2.
2. Recherche dans la SAD pour une correspondance à la fois sur SPI et adresse de destination. Si l'entrée de SAD correspond, traiter alors le paquet entrant avec cette entrée de SAD correspondante. Autrement, passer à l'étape 3.
3. Recherche dans la SAD pour une correspondance seulement sur SPI si le receveur a choisi d'entretenir un seul espace de SPI pour AH et ESP, et autrement, à la fois sur SPI et protocole. Si une entrée de SAD correspond, traiter alors le paquet entrant avec cette entrée de SAD correspondante. Autrement, éliminer le paquet et enregistrer un événement à étudier.

En pratique, une mise en œuvre peut choisir toute méthode (ou aucune) pour accélérer cette recherche, bien que son comportement apparent DOIVE être fonctionnellement équivalent à avoir recherché dans la SAD dans l'ordre ci-dessus. Par exemple, une mise en œuvre fondée sur un logiciel pourrait indexer avec le SPI dans un tableau de hachage. Les entrées de SAD dans les compartiments de chaque liste liée du tableau de hachage pourraient être triées de façon à avoir d'abord dans cette liste liée les entrées de SAD qui ont les plus longs identifiants de SA. Les entrées de SAD ayant les plus courts identifiants de SA pourraient être triés de façon à ce qu'elles soient les dernières entrées dans la liste liée. Une mise en œuvre fondée sur un matériel spécifique peut être capable d'effectuer intrinsèquement la recherche de la plus longue correspondance, en utilisant des dispositifs couramment disponibles de mémoire ternaire à contenu adressable (TCAM, *Ternary Content-Addressable Memory*).

L'indication que c'est l'adresse de source ou de destination qui correspond est exigée pour faire correspondre le trafic IPsec entrant aux SA DOIT être réglée soit comme un effet secondaire d'une configuration manuelle de SA soit via négociation en utilisant un protocole de gestion de SA, par exemple, IKE ou domaine de groupe d'interprétation (GDOI, *Group Domain of Interpretation*) [RFC 3547]. Normalement, les groupes de diffusion groupée spécifiques de source (SSM, *Source-Specific Multicast*) [RFC4607] utilisent un triplet d'identifiant de SA composé d'un SPI, d'une adresse de destination de diffusion groupée et d'une adresse de source. Une association de sécurité de groupe de diffusion groupée toutes sources n'exige qu'un SPI et une adresse de destination de diffusion groupée comme identifiant.

Si différentes classes de trafic (distinguées par des bits de codets de services différenciés (DSCP, *Differentiated Services Code Point*) [RFC2474], [RFC3260]) sont envoyées sur la même SA, et si le receveur emploie le dispositif facultatif anti-répétition disponible dans AH et ESP, il peut en résulter une élimination intempestive des paquets de plus faible priorité du fait du mécanisme de fenêtre utilisé par ce dispositif. Donc, un envoyeur DEVRAIT mettre le trafic de différentes classes, mais avec les mêmes valeurs de sélecteur, sur des SA différentes pour prendre en charge correctement la qualité de service (QS). Pour le permettre, la mise en œuvre IPsec DOIT permettre l'établissement et la maintenance de plusieurs SA entre un envoyeur et un receveur donnés, avec les mêmes sélecteurs. La distribution du trafic parmi ces SA parallèles pour prendre en charge la qualité de service est déterminée localement par l'envoyeur et n'est pas négociée par IKE. Le receveur DOIT traiter les paquets provenant des différentes SA sans discrimination. Ces exigences s'appliquent aux associations de sécurité aussi bien en mode transport qu'en mode tunnel. Dans le cas de SA en mode tunnel, les valeurs de DSCP en question apparaissent dans l'en-tête IP interne. En mode transport, la valeur de DSCP peut changer en route, mais cela ne devrait pas causer de problème par rapport au traitement IPsec car cette valeur n'est pas employée pour la sélection de SA et NE DOIT PAS être vérifiée au titre de la validation de SA/paquet. Cependant, si un réordonnancement significatif des paquets

survient dans une SA, par exemple, résultant de changements de valeurs de DSCP en route, cela peut déclencher l'élimination du paquet par le receveur par l'application du mécanisme anti-répétition.

DISCUSSION : Bien que les champs DSCP [NiBlBaBL98, Gro02] et Notification d'encombrement explicite (ECN) [RFC3168] ne soient pas "sélecteurs", au sens où ce terme est utilisé dans cette architecture, l'envoyeur aura besoin d'un mécanisme pour diriger les paquets avec des (un ensemble de) valeurs DSCP sur l'association de sécurité appropriée. Ce mécanisme peut être dénommé un "classeur".

Comme noté ci-dessus, deux types d'associations de sécurité sont définis : mode transport et mode tunnel. IKE crée des paires de SA, et par souci de simplicité, nous choisissons d'exiger que les deux SA d'une paire soient du même mode, transport ou tunnel.

Une SA en mode transport est normalement employée entre une paire d'hôtes pour fournir des services de sécurité de bout en bout. Lorsque la sécurité est désirée entre deux systèmes intermédiaires le long d'un chemin (par opposition à une utilisation d'IPsec de bout en bout), le mode transport PEUT être utilisé entre passerelles de sécurité ou entre une passerelle de sécurité et un hôte. Dans le cas où le mode transport est nécessaire entre passerelles de sécurité ou entre une passerelle de sécurité et un hôte, le mode transport peut être utilisé pour prendre en charge le tunnelage à l'intérieur de IP (par exemple, IP à IP [RFC2003] ou le tunnelage par encapsulation général du routage (GRE, *Generic Routing Encapsulation*) [RFC2784] ou le routage dynamique [RFC3884]) sur des SA en mode transport. Pour préciser, l'utilisation du mode transport par un système intermédiaire (par exemple, une passerelle de sécurité) n'est permise qu'appliquée aux paquets dont l'adresse de source (pour les paquets sortants) ou l'adresse de destination (pour les paquets entrants) est une adresse appartenant au système intermédiaire lui-même. Les fonctions de contrôle d'accès qui sont une part importante d'IPsec sont significativement limitées dans ce contexte, car elles ne peuvent pas s'appliquer aux en-têtes de bout en bout des paquets qui traversent une SA en mode transport utilisée de cette façon. Et donc, cette utilisation du mode transport devrait être soigneusement soupesée avant de l'employer dans un contexte spécifique.

Dans IPv4, un en-tête de protocole de sécurité de mode transport apparaît immédiatement après l'en-tête IP et toute option, et avant tout protocole de la couche suivante (par exemple, TCP ou UDP). Dans IPv6, l'en-tête de protocole de sécurité apparaît après l'en-tête IP de base et les en-têtes des extensions choisies, mais peut apparaître avant ou après les options de destination ; il DOIT apparaître avant les protocoles de couche suivante (par exemple, TCP, UDP, protocole de transport des commandes de flux (SCTP, *Stream Control Transmission Protocol*)). Dans le cas de ESP, une SA en mode transport ne fournit des services de sécurité que pour ces protocoles de couche suivante, et non pour l'en-tête IP ou tout en-tête d'extension précédant l'en-tête ESP. Dans le cas de AH, la protection est aussi étendue aux portions sélectionnées de l'en-tête IP qui le précèdent, aux portions choisies des en-têtes d'extension, et aux options choisies (contenues dans l'en-tête IPv4, dans l'en-tête d'extension bond par bond IPv6, ou dans les en-têtes IPv6 d'extension de destination). Pour des compléments d'information sur la couverture offerte par AH, voir la spécification AH [RFC4302].

Une SA en mode tunnel est essentiellement une SA qui s'applique à un tunnel IP, avec le contrôle d'accès appliqué aux en-têtes du trafic à l'intérieur du tunnel. Deux hôtes PEUVENT établir une SA en mode tunnel entre elles-mêmes. À part les deux exceptions ci-dessus, chaque fois qu'une des extrémités d'une association de sécurité est une passerelle de sécurité, la SA DOIT être en mode tunnel. Et donc, une SA entre deux passerelles de sécurité est normalement une SA en mode tunnel, comme l'est une SA entre un hôte et une passerelle de sécurité. Les deux exceptions sont les suivantes :

- Lorsque le trafic est destiné à une passerelle de sécurité, par exemple, des commandes du protocole simple de gestion de réseau (SNMP, *Simple Network Management Protocol*) la passerelle de sécurité agit comme un hôte et le mode transport est permis. Dans ce cas, la SA se termine à une fonction hôte (gestion) au sein d'une passerelle de sécurité et donc mérite un traitement différent.
- Comme noté ci-dessus, les passerelles de sécurité PEUVENT prendre en charge une SA en mode transport pour fournir la sécurité au trafic IP entre deux systèmes intermédiaires le long d'un chemin, par exemple, entre un hôte et une passerelle de sécurité ou entre deux passerelles de sécurité.

Plusieurs problèmes motivent l'utilisation du mode tunnel pour une SA impliquant une passerelle de sécurité. Par exemple, si il y a plusieurs chemins (par exemple, via différentes passerelles de sécurité) pour la même destination derrière une passerelle de sécurité, il est important qu'un paquet IPsec soit envoyé à la passerelle de sécurité avec laquelle la SA a été négociée. De même, un paquet qui pourrait être fragmenté en route doit avoir tous ses fragments délivrés à la même instance IPsec pour réassemblage avant le traitement cryptographique. Aussi, quand un fragment est traité par IPsec et transmis, puis fragmenté en route, il est vital qu'il y ait des en-têtes internes et externes pour conserver les données d'état de fragmentation pour les formats de paquets pré- et post-IPsec. Et donc il y a plusieurs raisons pour utiliser le mode tunnel quand l'une ou l'autre extrémité d'une SA est une passerelle de sécurité. (L'utilisation d'un tunnel IP dans IP en conjonction avec le mode transport peut aussi viser ces problèmes de fragmentation. Cependant, cette configuration limite la capacité d'IPsec de mettre en application les politiques de contrôle d'accès sur le trafic.)

Note : AH et ESP ne peuvent pas être appliqués en utilisant le mode transport pour les paquets IPv4 qui sont fragmentés. Seul le mode tunnel peut être employé dans de tels cas. Pour IPv6, il serait faisable de porter un fragment de texte

en clair sur une SA en mode transport ; cependant, par simplicité, cette restriction s'applique aussi aux paquets IPv6. Voir à la section 7 des précisions sur le traitement des fragments de texte en clair sur le côté protégé de la barrière IPsec.

Pour une SA en mode tunnel, il y a un en-tête IP "extérieur" qui spécifie la source et la destination du traitement IPsec, plus un en-tête IP "interne" qui spécifie la source et destination ultime (apparente) pour le paquet. L'en-tête de protocole de sécurité apparaît après l'en-tête IP extérieur, et avant l'en-tête IP intérieur. Si AH est employé en mode tunnel, des portions de l'en-tête IP extérieur apportent leur protection (comme ci-dessus), ainsi qu'à tout le paquet IP tunnelé (c'est-à-dire, tout l'en-tête IP interne est protégé, ainsi que les protocoles de la couche suivante). Si ESP est employé, la protection ne vaut que pour le paquet tunnelé, et pas pour l'en-tête externe.

En résumé,

a) Une mise en œuvre d'hôte de IPsec DOIT prendre en charge les deux modes transport et tunnel. Ceci est vrai pour les mises en œuvre pour hôtes natives, BITS, et BITW.
b) Une passerelle de sécurité DOIT prendre en charge le mode tunnel et PEUT prendre en charge le mode transport. Si elle accepte le mode transport, il ne devrait être utilisé que lorsque la passerelle de sécurité agit comme un hôte, par exemple, pour la gestion du réseau, ou pour assurer la sécurité entre deux systèmes intermédiaires le long d'un chemin.

4.2 Fonction de la SA

L'ensemble des services de sécurité offerts par une SA dépend du protocole de sécurité choisi, du mode de SA, des points d'extrémité de la SA, et du choix des services facultatifs au sein du protocole.

Par exemple, AH et ESP offrent tous deux des services d'intégrité et d'authentification, mais la couverture diffère pour chaque protocole et ainsi que selon le mode, transport ou tunnel. Si l'intégrité d'un en-tête d'option IPv4 ou d'extension IPv6 doit être protégée en route entre envoyeur et receveur, AH peut fournir ce service, sauf pour les en-têtes IP ou d'extension qui peuvent changer d'une façon non prévisible par l'envoyeur.

Cependant, la même sécurité peut être obtenue dans certains contextes par l'application d'ESP à un tunnel qui porte un paquet.

La granularité du contrôle d'accès fourni est déterminée par le choix des sélecteurs qui définissent chaque SA. De plus, les moyens d'authentification employés par les homologues IPsec, par exemple, durant la création d'une SA IKE (opposée à fils) affectent aussi la granularité du contrôle d'accès fourni.

Si on choisit la confidentialité, une SA en ESP (mode tunnel) entre deux passerelles de sécurité peut offrir une confidentialité partielle du flux de trafic. L'utilisation du mode tunnel permet de chiffrer les en-têtes IP internes, dissimulant les identités de source et destination (ultimes) du trafic. De plus, des bourrages de charge utile ESP peuvent aussi être invoqués pour cacher la taille des paquets, dissimulant un peu plus les caractéristiques externes du trafic. Des services similaires de confidentialité des flux de trafic peuvent être offerts lorsqu'un usager mobile se voit allouer une adresse IP dynamique dans un contexte de téléphonie, et établit une association de sécurité ESP (mode tunnel) avec un pare-feu d'entreprise (jouant le rôle d'une passerelle de sécurité). Noter que les SA à granularité fine sont généralement plus vulnérables à l'analyse de trafic que celles à grosse granularité qui portent du trafic provenant de nombreux abonnés.

Note : Une mise en œuvre conforme NE DOIT PAS permettre l'instanciation d'une SA ESP qui emploie à la fois le chiffrement NULL et pas d'algorithme d'intégrité. Toute tentative de négocier une telle SA est un événement qui doit faire l'objet d'un audit, à la fois par le générateur et par celui qui répond. L'entrée d'enregistrement d'audit pour cet événement DEVRAIT inclure la date/heure en cours, l'adresse IP IKE locale, et l'adresse IP IKE distante. Le générateur DEVRAIT enregistrer l'entrée SPD en cause.

4.3 Combinaisons de SA

Le présent document n'exige pas la prise en charge d'associations de sécurité entrelacées ou de ce que la [RFC2401] appelle "faisceau de SA". Ces dispositifs peuvent toujours être réalisés par des configurations appropriées de la SPD et des fonctions locales de transmission (pour le trafic entrant et sortant), mais cette capacité est en dehors du module IPsec et donc du domaine d'application de la présente spécification. Il en résulte que la gestion des SA incorporées ou en faisceau est potentiellement plus complexe et moins assurée que dans le modèle impliqué par la [RFC2401]. Une mise en œuvre prenant en charge les SA incorporées DEVRAIT fournir une interface de gestion qui permette à un usager ou un administrateur d'exprimer les exigences d'incorporation, et ensuite de créer les entrées de SPD et de tableau de transmission appropriées pour effectuer le traitement requis. (Voir à l'Appendice E un exemple de la façon de configurer des SA incorporées.)

4.4 Bases de données IPsec majeures

Beaucoup des détails associés au traitement du trafic IP dans une mise en œuvre IPsec sont largement une affaire locale, non soumise à normalisation. Cependant, certains aspects externes du traitement doivent être normalisés pour assurer l'interopérabilité et fournir un minimum de capacité de gestion essentiel pour la productivité de l'utilisation d'IPsec. La présente section décrit un modèle général du traitement du trafic IP par rapport aux fonctionnalités d'IPsec, à l'appui de ces objectifs d'interopérabilité et de ces fonctionnalités. Le modèle décrit ci-dessous est nominal ; les mises en œuvre n'ont pas besoin de respecter les détails du modèle tel qu'il est présenté, mais le comportement externe des mises en œuvre DOIT correspondre aux caractéristiques externes observables de ce modèle pour y être conformes.

Il y a trois bases de données nominales dans ce modèle : la base de données de politique de sécurité (SPD, *Security Policy Database*), la base de données d'associations de sécurité (SAD, *Security Association Database*), et la base de données d'autorisation des homologues (PAD, *Peer Authorization Database*). La première spécifie les politiques qui déterminent la disposition de tout le trafic IP entrant ou sortant provenant d'un hôte ou passerelle de sécurité (paragraphe 4.4.1). La seconde base de données contient des paramètres associés à chaque SA établie (verrouillée) (paragraphe 4.4.2). La troisième base de données, PAD, fournit un lien entre un protocole de gestion de SA (comme IKE) et la SPD (paragraphe 4.4.3).

Plusieurs contextes IPsec séparés
Si une mise en œuvre IPsec agit comme passerelle de sécurité pour plusieurs abonnés, elle PEUT mettre en œuvre plusieurs contextes IPsec séparés. Chaque contexte PEUT avoir et PEUT utiliser des identités, politiques, SA de gestion de clés et/ou SA IPsec complètement indépendantes. Ceci est pour une large part une affaire de mise en œuvre locale. Cependant, il est nécessaire d'avoir un moyen d'associer les propositions de SA entrantes avec les contextes locaux. À cette fin, s'ils sont acceptés par le protocole de gestion de clés utilisé, des identifiants de contexte PEUVENT être portés du générateur au répondant dans les messages de signalisation, d'où il résultera que les SA IPsec seront créées avec une liaison avec un contexte particulier. Par exemple, une passerelle de sécurité qui fournit un service de VPN à plusieurs utilisateurs sera capable d'associer le trafic de chaque utilisateur au bon VPN.

Transmission contre décisions de sécurité
Le modèle IPsec décrit ici comporte une claire séparation entre décision de transmission (routage) et décisions de sécurité, pour s'accommoder d'une large gamme de contextes où IPsec peut être employé. La transmission peut être triviale, dans le cas où il n'y a que deux interfaces, ou elle peut être complexe, par exemple, si le contexte dans lequel IPsec est mis en œuvre emploie une fonction de transmission sophistiquée. IPsec suppose seulement que le trafic entrant et sortant qui est passé à travers le traitement IPsec est transmis d'une façon cohérente avec le contexte dans lequel IPsec est mis en œuvre. La prise en charge de SA incorporées es facultatif ; s'il est exigé, cela suppose une coordination entre tableaux de transmission et entrées de SPD pour faire qu'un paquet traverse plus d'une fois la frontière IPsec.

"Local" contre "distant"
Dans le présent document, par rapport aux adresses et ports IP, les termes "local" et "distant" sont utilisés pour les règles de politique. "Local" se réfère à l'entité protégée par une mise en œuvre IPsec, c'est-à-dire, l'adresse/accès de "source" des paquets sortants ou l'adresse/accès de "destination" des paquets entrants. "Distant" se réfère à une ou des entités homologues. Les termes de "source" et "destination" sont utilisés pour les champs d'en-tête de paquet.

Fragment "non-initial" contre "initial"
Tout au long du présent document, la proposition "fragment non initial" est utilisée pour désigner des fragments qui ne contiennent pas toutes les valeurs du sélecteur qui peuvent être nécessaires pour le contrôle d'accès (par exemple, elles pourraient ne pas contenir le protocole de couche suivante, les accès de source et destination, le type/code de message ICMP, le type d'en-tête de mobilité). Et la proposition "fragment initial" est utilisée pour désigner un fragment qui contient toutes les valeurs de sélecteur nécessaires pour le contrôle d'accès. Cependant, il vaut de noter que pour IPv6, le fragment qui va contenir le protocole de couche suivante et les accès (ou le type/code de message ICMP ou le type d'en-tête de mobilité [RFC3775]) dépendra de la sorte et du nombre des en-têtes d'extension présents. Le fragment "initial" pourrait dans ce contexte n'être pas le premier fragment.

4.4.1 La base de données de politique de sécurité (SPD)

Une SA est une construction de gestion utilisée pour mettre en application la politique de sécurité pour le trafic qui franchit la frontière IPsec. Et donc, un élément essentiel du traitement de SA est une base de données de politique de sécurité (SPD) sous-jacente qui spécifie quels services sont à offrir aux datagrammes IP et de quelle façon. La forme de la base de données et son interface sont en dehors du domaine d'application de la présente spécification. Cependant, ce paragraphe spécifie les fonctionnalités de gestion minimales qui doivent être fournies, pour permettre à un usager ou administrateur de système de contrôler si et comment IPsec est appliqué au trafic transmis ou reçu par un hôte ou qui transite par une passerelle de sécurité. La SPD, ou les antémémoires pertinentes, doivent être consultées durant le traitement de tout le trafic (entrant et sortant), y compris le trafic non protégé par IPsec, qui traverse la frontière IPsec. Cela inclut le trafic de gestion IPsec tel

que IKE. Une mise en œuvre IPsec DOIT avoir au moins une SPD, et elle PEUT prendre en charge plusieurs SPD, si c'est approprié pour le contexte dans lequel fonctionne la mise en œuvre IPsec. Il n'est pas exigé que les SPD soient entretenues interface par interface, comme le spécifiait la [RFC2401]. Cependant, si une mise en œuvre prend en charge plusieurs SPD, elle DOIT alors inclure une fonction explicite de sélection de SPD qui sera invoquée pour choisir la SPD appropriée pour le traitement du trafic sortant. Les entrées à cette fonction sont le paquet sortant et toutes métadonnées locales (par exemple, l'interface par laquelle le paquet est arrivé) nécessaires pour effectuer la fonction de sélection de SPD. La sortie de la fonction est un identifiant de SPD (SPD-ID).

La SPD est une base de données ordonnée, cohérente avec l'utilisation des listes de contrôle d'accès (ACL, *Access Control List*) ou des filtres de paquets dans les pare-feu, les routeurs, etc. L'exigence d'ordonnancement vient de ce que les entrées vont souvent se chevaucher du fait de la présence de gammes (non triviales) comme valeurs des sélecteurs. Et donc, un usager ou administrateur DOIT être capable d'ordonner les entrées pour exprimer le désir d'une politique de contrôle d'accès. Il n'est pas question d'imposer un ordre canonique général aux entrées de SPD, à cause de l'autorisation d'utiliser des caractères génériques *(wildcards)* comme valeurs de sélecteur et parce que les différents types de sélecteurs n'ont pas de relation hiérarchisée.

Choix de traitement : DISCARD, BYPASS, PROTECT
Une SPD doit faire une discrimination entre le trafic auquel elle offre la protection IPsec et le trafic qui est admis à outrepasser IPsec. Ceci s'applique à la protection IPsec à appliquer par un envoyeur et à la protection IPsec qui doit être présente chez le receveur. Pour tout datagramme entrant ou sortant, trois choix de traitement sont possibles : DISCARD *(éliminer)*, BYPASS *(outrepasser)* IPsec, ou PROTECT *(protéger)* en utilisant IPsec. Le premier choix se réfère au trafic dont il n'est pas admis qu'il traverse la frontière IPsec (dans la direction spécifiée). Le second choix se réfère au trafic qui est admis à traverser la frontière IPsec sans protection IPsec. Le troisième choix se réfère au trafic auquel la protection IPsec est accordée, et pour un tel trafic, la SPD doit spécifier les protocoles de sécurité à employer, leur mode, les options de service de sécurité, et les algorithmes cryptographiques à utiliser.

SPD-S, SPD-I, SPD-O
Une SPD est logiquement divisée en trois parties. La SPD-S (trafic sécurisé) contient les entrées pour tout trafic soumis à la protection IPsec. SPD-O (sortant) contient les entrées pour tout le trafic sortant qui va outrepasser ou être éliminé. SPD-I (entrant) est appliquée au trafic entrant qui outrepassera ou sera éliminé. Chacune d'elles peut être dé corrélée (à l'exception notée plus haut des mises en œuvre d'hôte natives) pour faciliter la mise en antémémoire. Si une mise en œuvre IPsec n'accepte qu'une SPD, la SPD comporte alors les trois parties. Si plusieurs SPD sont acceptées, certaines d'entre elles peuvent être partielles, par exemple, certaines SPD pourraient ne contenir que les entrées de SPD-I, pour contrôler le trafic entrant qui outrepasse interface par interface. Le partage permet à la SPD-I d'être consultée sans avoir à consulter la SPD-S, pour un tel trafic. Comme la SPD-I est juste une partie de la SPD, si un paquet qui est recherché dans la SPD-I ne peut correspondre à une de ses entrées, le paquet DOIT alors être éliminé. Noter que pour le trafic sortant, si une correspondance n'est pas trouvée dans la SPD-S, la SPD-O doit alors être vérifiée pour voir si le trafic devrait outrepasser. De même, si la SPD-O est vérifiée d'abord et qu'aucune correspondance n'est trouvée, la SPD-S doit alors être vérifiée. Dans une SPD ordonnée, non décorrélée, les entrées pour SPD-S, SPD-I, et SPD-O sont imbriquées. Ainsi il y a une seule recherche dans la SPD.

Entrées de SPD
Chaque entrée de SPD spécifie une disposition pour le paquet : BYPASS, DISCARD, ou PROTECT. L'entrée est verrouillée par une liste d'un ou plusieurs sélecteurs. La SPD contient une liste ordonnée de ces entrées. Les types de sélecteur requis sont définis au paragraphe 4.4.1.1. Ces sélecteurs sont utilisés pour définir la granularité des SA qui sont à créer en réponse à un paquet sortant ou en réponse à une proposition provenant d'un homologue. La structure détaillée d'une entrée SPD est décrite au paragraphe 4.4.1.2. Chaque SPD DEVRAIT avoir une entrée nominale finale qui corresponde à tout ce qui ne correspond pas par ailleurs, et qu'elle élimine.

La SPD DOIT permettre à un usager ou administrateur de spécifier des entrées de politique comme suit :
- SPD-I : Pour le trafic entrant qui outrepasse ou est à éliminer, l'entrée consiste en les valeurs des sélecteurs qui s'appliquent au trafic outrepassant ou à éliminer.
- SPD-O : Pour le trafic sortant qui outrepasse ou est à éliminer, l'entrée consiste en les valeurs des sélecteurs qui s'appliquent au trafic qui outrepasse ou est éliminé.
- SPD-S : Pour le trafic qui est à protéger en utilisant IPsec, l'entrée comporte les valeurs des sélecteurs qui s'appliquent au trafic à protéger via AH ou ESP, les commandes sur comment créer des SA sur la base de ces sélecteurs, et les paramètres nécessaires pour effectuer cette protection (par exemple, les algorithmes, les modes, etc.). Noter qu'une entrée de SPD-S contient aussi des informations telle que le fanion "populate from paquet" (PFP) *(remplir à partir du paquet)* (voir ci-dessous les paragraphes sur "Comment déduire les valeurs pour une entrée de SAD") et les bits qui indiquent si la recherche de SA utilise les adresses IP locale et distante en plus des spécifications de la SPI (voir AH [RFC4302] ou de l'ESP [RFC4303]).

Représentation de la direction dans une entrée de SPD
Pour le trafic protégé par IPsec, l'adresse et les accès locaux et distants d'une entrée SPD sont échangés pour représenter une direction, selon les conventions IKE. En général, les protocoles dont s'occupe IPsec ont la propriété d'exiger des SA symétriques des adresses locale/distante bouleversées. Cependant, pour ICMP, il n'y a souvent pas de telle exigence d'autorisation bidirectionnelle. Néanmoins, au nom de l'uniformisation et de la simplicité, les entrées de SPD pour ICMP sont spécifiées de la même façon que pour les autres protocoles. Noter aussi que pour ICMP, l'en-tête de mobilité et les fragments non initiaux, il n'y a pas de champ Port dans ces paquets. ICMP a le type et code de message et l'en-tête de mobilité comme type d'en-tête de mobilité. Et donc, les entrées de SPD ont des dispositions pour exprimer les contrôles d'accès appropriés à ces protocoles, au lieu des contrôles de champ d'accès normaux. Pour le trafic qui outrepasse ou qui est éliminé, des entrées séparées pour l'entrée et la sortie sont prises en charge, par exemple, pour permettre si besoin est, des flux unidirectionnels.

OPAQUE et ANY
Pour chaque sélecteur dans une entrée SPD, en plus des valeurs littérales qui définissent une correspondance, il y a deux valeurs spéciales : ANY et OPAQUE. ANY est une valeur générique qui correspond à toute valeur dans le champ correspondant du paquet, ou qui correspond à des paquets où ce champ n'est pas présent ou est obscur. OPAQUE indique que le champ de sélecteur correspondant n'est pas disponible à l'examen parce qu'il peut n'être pas présent dans un fragment, ne pas exister pour un protocole de couche suivante donné, ou qu'une précédente application d'IPsec peut avoir chiffré la valeur. La valeur ANY englobe la valeur OPAQUE. Et donc, OPAQUE n'a besoin d'être utilisé que lorsqu'il est nécessaire de distinguer entre le cas où n'importe quelle valeur est admise pour un champ et celui de l'absence ou l'indisponibilité du champ (par exemple, due au chiffrement).

Comment déduire les valeurs d'une entrée de SAD
Pour chaque sélecteur dans une entrée SPD, l'entrée spécifie comment déduire les valeurs correspondantes pour une nouvelle entrée de base de données de SA (SAD, voir au paragraphe 4.4.2) de celles qui sont dans la SPD et le paquet. Le but est de permettre de créer une entrée de SAD et une entrée d'antémémoire de SPD sur les valeurs de sélecteur spécifiques du paquet, ou de l'entrée de SPD correspondante. Pour le trafic sortant, il y a des entrées d'antémémoire de SPD-S et des entrées d'antémémoire de SPD-O. Pour le trafic entrant non protégé par IPsec, il y a des entrées d'antémémoire de SPD-I et il y a la SAD, qui représente l'antémémoire pour le trafic entrant protégé par IPsec (voir au paragraphe 4.4.2). Si le traitement IPsec est spécifié pour une entrée, un fanion "remplir à partir du paquet" (PFP) peut être affirmé pour un ou plusieurs des sélecteurs de l'entrée de SPD (adresse IP locale ; adresse IP distante ; protocole de couche suivante ; et, selon le protocole de couche suivante, accès local et accès distant, ou type/code ICMP, ou type d'en-tête de mobilité. S'il est affirmé pour un sélecteur X donné, le fanion indique que la SA à créer devrait tirer sa valeur pour X de la valeur dans le paquet. Autrement, la SA devrait tirer sa ou ses valeurs pour X de la ou des valeurs de l'entrée de SPD. Note : Dans le cas non PFP, les valeurs de sélecteur négociées par le protocole de gestion de SA (par exemple, IKEv2) peuvent être un sous ensemble de celles qui sont dans l'entrée de SPD, selon la politique de SPD de l'homologue. Et c'est une affaire locale de savoir si un seul fanion est utilisé pour, par exemple, l'accès de source, le type/code ICMP, et le type d'en-tête de mobilité (MH, *Mobility Header*), ou si un fanion séparé est utilisé pour chacun.

L'exemple suivant illustre l'utilisation du fanion PFP dans le contexte d'une passerelle de sécurité ou d'une mise en œuvre BITS/BITW. Considérons une entrée de SPD où la valeur admise pour l'adresse distante est une gamme d'adresses IPv4 : 192.0.2.1 à 192.0.2.10. Supposons qu'un paquet sortant arrive avec une adresse de destination de 192.0.2.3, et qu'il n'existe pas de SA pour porter ce paquet. La valeur utilisée pour la SA créée pour transmettre ce paquet pourrait être l'une des deux valeurs montrées ci-dessous, selon ce que l'entrée de SPD pour ce sélecteur dit être la source de la valeur de sélecteur :

Valeur de fanion PFP pour le sélecteur d'adresse distante	**Exemple de nouvelle valeur de sélecteur d'adresse de destination de SAD**
a. PFP TRUE *(PFP vrai)*	192.0.2.3 (un hôte)
b. PFP FALSE *(PFP faux)*	192.0.2.1 à 192.0.2.10 (gamme d'hôtes)

Noter que si l'entrée de SPD ci-dessus avait une valeur de ANY pour l'adresse distante, la valeur de sélecteur de SAD aurait été ANY pour le cas (b), mais serait toujours celle illustrée par le cas (a). Et donc, le fanion PFP peut être utilisé pour prohiber le partage d'une SA, même entre des paquets qui correspondent à la même entrée de SPD.

Interface de gestion
Pour chaque mise en œuvre IPsec, il DOIT y avoir une interface de gestion qui permette à un usager ou administrateur de système de gérer la SPD. L'interface doit permettre à l'usager (ou administrateur) de spécifier le traitement de la sécurité à appliquer à chaque paquet qui traverse la frontière IPsec. (Dans une mise en œuvre d'hôte natif IPsec faisant office d'interface d'accès, la SPD peut n'avoir pas besoin d'être consultée paquet par paquet, comme noté à la fin du paragraphe 4.4.1.1 et à la section 5.) L'interface de gestion pour la SPD DOIT permettre la création d'entrées cohérentes avec les sélecteurs définis au paragraphe 4.4.1.1, et DOIT prendre en charge l'ordonnancement (total) de ces entrées, vu de cette interface. Les sélecteurs des entrées de SPD sont analogues aux filtres ACL ou de paquet qu'on trouve couramment dans un pare-feu sans état ou un routeur de filtrage de paquet et qui sont habituellement gérés de cette façon.

Dans les systèmes hôtes, les applications PEUVENT être autorisées à créer des entrées de SPD. (La signification de la signalisation de telles demandes à la mise en œuvre IPsec est en dehors du domaine d'application de la présente norme.) Cependant, l'administrateur de système DOIT être capable de spécifier si un usager ou application peut ou non outrepasser les politiques système (par défaut). La forme de l'interface de gestion n'est pas spécifiée dans le présent document et peut différer entre hôtes et passerelles de sécurité, et au sein des hôtes l'interface peut être différente pour les mises en œuvre fondées sur l'accès et celles qui sont BITS. Cependant, le présent document spécifie bien un ensemble standard d'éléments de SPD que toutes les mises en œuvre IPsec DOIVENT prendre en charge.

Décorrélation

Le modèle de traitement décrit dans le présent document suppose la capacité à décorréler les entrées de SPD qui se chevauchent pour permettre la mise en antémémoire, qui active un traitement plus efficace du trafic sortant dans les passerelles de sécurité et mises en œuvre BITS/BITW. La décorrélation [CoSa04] est seulement un moyen d'améliorer les performances et de simplifier la description du traitement. La présente RFC n'exige pas d'une mise en œuvre conforme qu'elle utilise la décorrélation. Par exemple, les mises en œuvre d'hôte natives utilisent normalement implicitement la mise en antémémoire parce qu'elles relient les SA aux interfaces d'accès, et donc il n'y a pas d'exigence qu'elles soient capables de décorréler les entrées de SPD dans ces mises en œuvre.

Note : Sauf qualification contraire, l'utilisation de "SPD" se réfère aux corps d'informations de politique à la fois dans l'état ordonné ou décorrélé (non ordonné). L'Appendice B donne un algorithme qui peut être utilisé pour décorréler les entrées de SPD, mais tout algorithme produisant une sortie équivalente peut être utilisée. Noter que quand une entrée SPD est décorrélée, toutes les entrées résultantes DOIVENT être liées entre elles, de sorte que tous les membres du groupe dérivé d'une entrée SPD individuelle (avant décorrélation) puissent tous être placés en antémémoire et dans la SAD en même temps. Par exemple, supposons qu'on commence avec une entrée A (d'une SPD ordonnée) qui lorsqu'elle est décorrélée, donne les entrées A1, A2, et A3. Lorsque un paquet arrive qui correspond, disons à A2, et déclenche la création d'une SA, le protocole de gestion de SA (par exemple, IKEv2) négocie A. Et les trois entrées décorrélées, A1, A2, et A3, sont placées dans l'antémémoire SPD-S appropriée et reliées à la SA. L'intention est que l'utilisation d'une SPD décorrélée ne devrait pas créer plus de SA qu'il n'en aurait résulté de l'utilisation de SPD non décorrélée.

Si une SPD décorrélée est employée, il y a trois options pour ce qu'un initiateur envoie à un homologue via un protocole de gestion de SA (par exemple, IKE). En envoyant l'ensemble complet d'entrées liées, décorrélées à partir de la SPD, un homologue donne les meilleures informations possibles pour permettre le choix de l'entrée de SPD appropriée à l'autre extrémité, en particulier si l'homologue a aussi décorrélé sa SPD. Cependant, si un grand nombre d'entrées décorrélées sont liées, cela peut créer de gros paquets pour la négociation de SA, et donc des problèmes de fragmentation pour le protocole de gestion de SA.

Autrement, l'entrée d'origine de la SPD (corrélée) peut être conservée et passée au protocole de gestion de SA. Passer les entrées de SPD corrélée fait de l'utilisation d'une SPD décorrélée une affaire locale, non visible par les homologues, et évite de possibles problèmes de fragmentation, bien que cela fournisse des informations moins précises au répondant pour trouver les correspondances avec la SPD du répondant.

Une approche intermédiaire est d'envoyer un sous-ensemble des entrées complètes de SPD liées, décorrélées. Cette approche peut éviter les problèmes de fragmentation cités ci-dessus et cependant fournir de meilleures informations que l'entrée originale corrélée. Le raccourci majeur de cette approche est qu'elle peut causer la création de SA additionnelles ultérieurement, car seul un sous-ensemble des entrées liées décorrélées est envoyé à un homologue. Les développeurs ont toute liberté pour employer une des approches citées ci-dessus.

Un répondant utilise les propositions de sélecteur de trafic qu'il reçoit via un protocole de gestion de SA pour choisir une entrée appropriée dans sa SPD. L'intention de cette mise en correspondance est de choisir une entrée de SPD et de créer une SA qui corresponde au plus près aux intentions de l'initiateur, de sorte que le trafic qui traverse la SA résultante soit accepté aux deux extrémités. Si le répondant emploie une SPD décorrélée, il DEVRAIT utiliser les entrées de la SPD décorrélée pour la correspondance, car il en résultera généralement la création de SA qui vont très vraisemblablement correspondre aux intentions des deux homologues. Si le répondant a une SPD corrélée, elle DEVRAIT alors correspondre aux propositions par rapport aux entrées corrélées. Pour IKEv2, l'utilisation d'une SPD décorrélée offre la meilleure opportunité au répondant de générer une réponse "rétrécie".

Dans tous les cas, lorsque une SPD décorrélée est disponible, les entrées décorrélées sont utilisées pour remplir l'antémémoire de la SPD-S. Si la SPD n'est pas décorrélée, la mise en antémémoire n'est pas admise et une recherche ordonnée de la SPD DOIT être effectuée pour vérifier que le trafic entrant qui arrive sur une SA est cohérent avec la politique de contrôle d'accès exprimée dans la SPD.

Traitement des changements de la SPD pendant le fonctionnement du système

Si un changement est fait à la SPD pendant que le système fonctionne, une vérification DEVRAIT être faite des effets de ce changement sur les SA existantes. Une mise en œuvre DEVRAIT vérifier l'impact d'un changement de SPD sur les SA existantes et DEVRAIT fournir à l'usager/administrateur un mécanisme pour configurer les actions à prendre, par exemple, supprimer une SA affectée, permettre à une SA affectée de continuer inchangée, etc.

4.4.1.1 Sélecteurs

Une SA peut être à grain fin ou à gros grain, selon les sélecteurs utilisés pour définir l'ensemble de trafic pour la SA. Par exemple, tout le trafic entre deux hôtes peut être porté via une seule SA, et offrir un ensemble uniforme de services de sécurité. Autrement, le trafic entre une paire d'hôtes peut être étalé sur plusieurs SA, selon les applications utilisées (comme défini par le protocole de couche suivante et les champs qui s'y rapportent, par exemple, les accès), avec les différents services de sécurité offerts par les différentes SA. De même, tout le trafic entre une paire de passerelles de sécurité pourrait être porté sur une seule SA, ou une SA pourrait être allouée pour chaque paire d'hôtes de la communication. Les paramètres de sélecteur suivants DOIVENT être pris en charge par toutes les mises en œuvre IPsec pour faciliter le contrôle de la granularité des SA. Noter que les adresses locales et distantes devraient être toutes deux soit IPv4 soit IPv6, mais pas un mélange de types d'adresse. Noter aussi que les sélecteurs d'accès local/distant (et le type et code de message ICMP, et le type d'en-tête de mobilité) peuvent être étiquetés comme OPAQUE pour s'accommoder de situations où ces champs sont inaccessibles à cause de la fragmentation du paquet.

- La ou les adresses IP distantes (IPv4 ou IPv6) : C'est une liste de gammes d'adresses IP (en envoi individuel, en diffusion (IPv4 uniquement)). Cette structure permet l'expression d'une seule adresse IP (via une gamme triviale) ou une liste d'adresses (chacune étant une gamme triviale) ou une gamme d'adresses (basse et haute valeurs incluses) aussi bien que les formes les plus génériques d'une liste de gammes. Les gammes d'adresse sont utilisées pour prendre en charge plus d'un système distant qui partagent la même SA, par exemple, derrière une passerelle de sécurité.
- La ou les adresses IP locales (IPv4 ou IPv6) : C'est une liste de gammes d'adresses IP (en envoi individuel, en diffusion (IPv4 uniquement)). Cette structure permet l'expression d'une seule adresse IP (via une gamme triviale) ou une liste d'adresses (chacune étant une gamme triviale) ou une gamme d'adresses (basse et haute valeurs incluses) aussi bien que les formes les plus génériques d'une liste de gammes. Les gammes d'adresses sont utilisées pour prendre en charge plus d'un système distant qui partagent la même SA, par exemple, derrière une passerelle de sécurité. Local se réfère à la ou aux adresses protégées par cette mise en œuvre (ou entrée de politique).

Note : La SPD n'inclut pas la prise en charge des entrées d'adresse en diffusion groupée. Pour prendre en charge les SA de diffusion groupée, une mise en œuvre devrait utiliser une SPD de groupe (GSPD, *Group SPD*) comme définie dans la [RFC3740]. Les entrées de GSPD exigent une structure différente, c'est-à-dire qu'on ne peut pas utiliser la relation symétrique associée à des valeurs d'adresse local et distante pour des SA en envoi individuel dans un contexte de diffusion groupée. Spécifiquement, le trafic sortant dirigé vers une adresse en diffusion groupée sur une SA ne pourrait pas être reçu sur une SA entrante avec l'adresse de diffusion groupée comme source.

- Protocole de couche suivante : Obtenu des champs IPv4 "Protocole" ou IPv6 "prochain en-tête". C'est un numéro de protocole individuel, ANY, ou pour IPv6 uniquement, OPAQUE. Le protocole de couche suivante est ce qui vient après tout en-tête d'extension IP présent. Pour simplifier la localisation du protocole de couche suivante, il DEVRAIT y avoir un mécanisme pour configurer quels en-têtes d'extension IPv6 sauter. La configuration par défaut pour les protocoles à sauter DEVRAIT inclure les protocoles suivants : 0 (options bond par bond), 43 (en-tête d'acheminement), 44 (en-tête de fragmentation), et 60 (options de destination). Note : La liste par défaut n'inclut PAS 51 (AH) ou 50 (ESP). Du point de vue de la recherche de sélecteur, IPsec traite AH et ESP comme des protocoles de couche suivante.

Plusieurs sélecteurs supplémentaires dépendent de la valeur de protocole de couche suivante :

* Si le protocole de couche suivante utilise deux accès (comme le font TCP, UDP, SCTP, et d'autres) il y a alors des sélecteurs pour l'accès local et distant. Chacun de ces sélecteurs a une liste des gammes de valeurs. Noter que les accès local et distant peuvent n'être pas disponibles dans le cas de réception d'un paquet fragmenté ou si les champs d'accès ont été protégés par IPsec (chiffrés) ; et donc, une valeur de OPAQUE DOIT aussi être acceptée. Note : Dans un fragment non initial, les valeurs d'accès ne seront pas disponibles. Si un sélecteur d'accès spécifie une valeur autre que ANY ou OPAQUE, il ne peut pas trouver la correspondance des paquets qui ne sont pas des fragments non initiaux. Si la SA exige une valeur d'accès autre que ANY ou OPAQUE, un fragment qui arrive sans accès DOIT être éliminé. (Voir à la Section 7, "Traitement des fragments".)

* Si le protocole de couche suivante est un en-tête de mobilité, il y a alors un sélecteur pour le type de message IPv6 en-tête de mobilité (type MH) [RFC3775]. C'est une valeur de 8 bits qui identifie un message de mobilité particulier. Noter que le type MH peut n'être pas disponible dans le cas de réception d'un paquet fragmenté. (Voir à la Section 7, "Traitement des fragments".) Pour IKE, le type de message IPv6 en-tête de mobilité (type MH) est placé dans les huit bits de plus fort poids des 16 bits du sélecteur de "accès" local.

* Si la valeur du protocole de couche suivante est ICMP, il y a alors un sélecteur de 16 bits pour le type et code de message ICMP. Le type de message est une valeur d'un seul huit bits, qui définit le type d'un message ICMP, ou ANY. Le code ICMP est une valeur d'un seul huit bits qui définit un sous-type spécifique pour un message ICMP. Pour IKE, le type de message est placé dans les huit bits de plus fort poids des 16 bits du sélecteur et le code est placé dans les huit

bits de moindre poids. Ce sélecteur de 16 bits peut contenir un seul type et une seule gamme de codes, un seul type et un code ANY, et un type ANY et un code ANY. Soit une entrée de politique avec une gamme de types (T-start à T-end) et une gamme de codes (C-start à C-end), et un paquet ICMP avec un type t et un code c, une mise en œuvre DOIT essayer une correspondance en utilisant (T-start*256) + C-start ≤ (t*256) + c ≤ (T-end*256) + C-end.

Noter que le type et le code de message ICMP peuvent n'être pas disponibles dans le cas de réception d'un paquet fragmenté. (Voir la Section 7, "Traitement des fragments".)

- Nom : Ce n'est pas un sélecteur comme les autres ci-dessus. Il n'est pas acquis d'un paquet. Un nom peut être utilisé comme identifiant symbolique pour une adresse locale ou distante IPsec. Les entrées de SPD nommées sont utilisées de deux façons :
  1. Une entrée de SPD nommée est utilisée par un répondant (et non par un initiateur) pour la prise en charge du contrôle d'accès lorsqu'une adresse IP ne serait pas appropriée pour le sélecteur d'adresse IP distant, par exemple, pour "road warriors". Le nom utilisé pour correspondre à ce champ est communiqué durant la négociation IKE dans la charge utile d'ID. Dans ce contexte, l'adresse IP de source de l'initiateur (en-tête IP interne en mode tunnel) est liée à l'adresse IP distante dans l'entrée de SAD créée par la négociation IKE. Cette adresse outrepasse la valeur d'adresse IP distante dans la SPD, quand l'entrée de SPD est sélectionnée de cette façon. Toutes les mises en œuvre IPsec DOIVENT prendre en charge cette utilisation des noms.
  2. Une entrée de SPD nommée peut être utilisée par un initiateur pour identifier un usager pour qui serait créée une SA IPsec (ou pour qui du trafic peut outrepasser). L'adresse IP de source de l'initiateur (provenant d'un en-tête IP interne dans le mode tunnel) est utilisée pour remplacer ce qui suit si et quand elles sont créées :
     - l'adresse locale dans l'entrée d'antémémoire de SPD
     - l'adresse locale dans l'entrée sortante de SAD
     - l'adresse distante dans l'entrée entrante de SAD.

La prise en charge de cette utilisation est facultative pour les mises en œuvre d'hôte multi usager natives et non applicables aux autres mises en œuvre. Noter que ce nom n'est utilisé que localement ; il n'est pas communiqué par le protocole de gestion de clé. Les formes de nom autres que celles utilisées pour le cas 1 ci-dessus (du répondant) sont applicables dans le contexte d'initiateur (voir ci-dessous).

Une entrée de SPD peut contenir à la fois un nom (ou une liste de noms) et aussi des valeurs pour l'adresse IP locale ou distante.

Pour le cas 1, répondant, les identifiants employés dans les entrées de SPD nommées sont d'un des quatre types suivants :

a. une chaîne de nom d'utilisateur pleinement qualifié (messagerie électronique) par exemple, mozart@foo.example.com (cela correspond à ID_RFC822_ADDR dans IKEv2)
b. un nom DNS pleinement qualifié, par exemple, foo.example.com (ceci correspond à ID_FQDN dans IKEv2)
c un nom distinctif X.500, par exemple, [RFC2253], CN = Stephen T. Kent, O = BBN Technologies, SP = MA, C = US (ceci correspond à ID_DER_ASN1_DN dans IKEv2, après décodage)
d. une chaîne d'octets (ceci correspond à Key_ID dans IKEv2)

Pour le cas 2, initiateur, les identifiants employés dans les entrées de SPD nommées sont du type chaîne d'octets. Ils sont vraisemblablement des UID Unix, des ID de sécurité Windows, ou quelque chose de similaire, mais pourraient aussi être un nom d'utilisateur ou un nom de compte. Dans tous les cas, cet identifiant est seulement une affaire locale et n'est pas transmis.

Le contexte de la mise en œuvre IPsec détermine comment les sélecteurs sont utilisés. Par exemple, une mise en œuvre d'hôte native utilise normalement une interface d'accès. Lorsque une nouvelle connexion est établie, la SPD peut être consultée et une SA liée à l'accès. Et donc, le trafic envoyé via cet accès n'a pas besoin de faire des recherches supplémentaires dans l'antémémoire de la SPD (SPD-O et SPD-S). À l'inverse, une mise en œuvre BITS, BITW, ou passerelle de sécurité a besoin de chercher chaque paquet et d'effectuer une recherche en antémémoire de SPD-O/SPD-S sur la base des sélecteurs.

4.4.1.2 Structure d'une entrée de SPD

Ce paragraphe contient une description en prose d'une entrée de SPD. L'Appendice C donne aussi un exemple de définition en ASN.1 d'une entrée de SPD.

Ce texte décrit la SPD d'une façon qui est destinée à être transposée directement dans les charges utiles IKE pour assurer que la politique requise par les entrées de SPD peut être négociée à travers IKE. Malheureusement, la sémantique de la version de IKEv2 publiée concurremment avec le présent document [RFC4306] n'est pas précisément en ligne avec celle définie pour la SPD. Spécifiquement, IKEv2 ne permet pas la négociation d'une seule SA qui se lie à plusieurs paires d'adresses et accès locaux et distants à une seule SA. Au lieu de cela, lorsque plusieurs adresses et accès locaux et distants

sont négociés pour une SA, IKEv2 ne les traite pas comme des paires, mais comme des ensembles (non ordonnés) de valeurs locales et distantes qui peuvent être appariées arbitrairement. Jusqu'à ce que IKE fournisse un moyen qui porte la sémantique exprimée dans la SPD via des ensembles de sélecteurs (comme décrit ci-dessous) les utilisateurs NE DOIVENT PAS inclure plusieurs ensembles de sélecteurs dans une seule entrée de SPD à moins que le contrôle d'accès n'ait l'intention de s'aligner sur la sémantique IKE "mix et match". Une mise en œuvre PEUT avertir les usagers, pour les informer de ce problème si l'usager crée des entrées de SPD avec plusieurs ensembles de sélecteurs, dont la syntaxe indique des conflits possibles avec la sémantique IKE actuelle.

La gestion GUI peut offrir à l'usager d'autres formes d'entrée et d'affichage de données, par exemple, l'option d'utiliser des préfixes d'adresse aussi bien que des gammes, et des noms symboliques pour des protocoles, des accès, etc. (Ne pas confondre l'utilisation de noms symboliques dans une interface de gestion avec le sélecteur SPD "Name".) Noter que distant/local ne s'applique qu'aux adresses et accès IP, et pas au type/code de message ou au type d'en-tête de mobilité. Aussi, si la valeur réservée symbolique de sélecteur OPAQUE ou ANY est employée pour un type de sélecteur donné, seule cette valeur peut apparaître dans la liste pour ce sélecteur, et elle doit n'apparaître qu'une fois dans la liste pour ce sélecteur. Noter que ANY et OPAQUE sont des conventions syntaxiques locales -- IKEv2 négocie ces valeurs via les gammes indiquées ci-dessous :

ANY:	start = 0	end = <max>
OPAQUE:	start = <max>	end = 0

Une SPD est une liste ordonnée d'entrées dont chacune contient les champs suivants :

- Nom -- liste des identifiants. Ce quasi-sélecteur est facultatif. Les formes qui DOIVENT être acceptées sont décrites ci-dessus au paragraphe 4.4.1.1 sous "Nom".

- Fanions PFP -- un par sélecteur de trafic. Un fanion donné, par exemple, pour le protocole de couche suivante, s'applique au sélecteur pertinent à travers tous les "ensembles de sélecteurs" (voir ci-dessous) contenus dans une entrée de SPD. Lors de la création d'une SA, chaque fanion spécifie pour le sélecteur de trafic correspondant si il faut créer le sélecteur à partir du champ correspondant dans le paquet qui a déclenché la création de la SA ou à partir de la ou des valeurs dans l'entrée de SPD correspondante (voir au paragraphe 4.4.1, "Comment déduire les valeurs d'une entrée de SAD"). Savoir si un seul fanion est utilisé pour, par exemple, un accès de source, un type/code ICMP, et un type MH, ou si un fanion distinct est utilisé pour chacun d'eux, est une affaire locale. Il y a des fanions PFP pour :
  - l'adresse locale
  - l'adresse distante
  - le protocole de couche suivante
  - l'accès local, ou le type/code de message ICMP ou le type d'en-tête de mobilité (selon le protocole de couche suivante)
  - l'accès distant, ou le type/code de message ICMP ou le type d'en-tête de mobilité (selon le protocole de couche suivante),

- De un à N ensembles de sélecteur qui correspondent aux "conditions" d'application d'une action IPsec particulière. Chaque ensemble de sélecteur contient :
  - l'adresse locale
  - l'adresse distante
  - le protocole de couche suivante
  - l'accès local, ou le type/code de message ICMP ou le type d'en-tête de mobilité (selon le protocole de couche suivante)
  - l'accès distant, ou le type/code de message ICMP ou le type d'en-tête de mobilité (selon le protocole de couche suivante)

Note : Le sélecteur "protocole suivant" est une valeur individuelle (à la différence des adresses IP locales et distantes) dans une entrée d'ensemble de sélecteur. Ceci est cohérent avec la façon dont IKEv2 négocie les valeurs de sélecteur de trafic (TS, *Traffic Selector*) pour une SA. Cela a un sens parce qu'on peut avoir besoin d'associer des champs d'accès différents à des protocoles différents. Il est possible d'associer plusieurs protocoles (et accès) à une seule SA en spécifiant plusieurs ensembles de sélecteurs pour cette SA.

- Informations de traitement – sur l'action requise -- PROTECT, BYPASS, ou DISCARD. Une seule action va avec tous les ensembles de sélecteurs, et non une action distincte pour chaque ensemble. Si le traitement requis est PROTECT, l'entrée contient les informations suivantes :
  - Mode IPsec -- tunnel ou transport
  - (En mode tunnel) adresse locale de tunnel -- Pour un hôte non mobile, si il n'y a qu'une seule 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.

- (En mode tunnel) adresse distante de tunnel – Il n'y a pas de façon standard de la déterminer. Voir § 4.5.3, "Localisation d'une passerelle de sécurité".
- Numéro de séquence étendu – Est-ce la SA qui utilise les numéros de séquence étendus ?
- Vérification dynamique de fragment -- Cette SA utilise-t-elle la vérification dynamique de fragment ? (Voir les détails à la Section 7.)
- Outrepasser le bit DF (T/F) -- applicable aux SA en mode tunnel
- Outrepasser DSCP (T/F) ou transposer en valeurs DSCP non protégées (matrice) si nécessaire pour restreindre l'outrepassement de valeurs DSCP -- applicable aux SA en mode tunnel
- Protocole IPsec -- AH ou ESP
- Algorithmes – lesquels utiliser pour AH, lesquels utiliser pour ESP, lesquels utiliser pour le mode combiné, ordonnés par priorité décroissante.

Savoir quelles informations sont conservées par rapport au traitement des SA existantes lorsque la SPD est changée est une affaire locale.

4.4.1.3 Plus de champs concernés associés aux protocoles de couche suivante

Des sélecteurs supplémentaires sont souvent associés à des champs dans l'en-tête de protocole de couche suivante. Un protocole de couche suivante particulier peut avoir zéro, un, ou deux sélecteurs. Il peut y avoir des situations où il n'y a pas à la fois un sélecteur local et un sélecteur distant pour les champs qui dépendent du protocole de couche suivante. L'en-tête de mobilité IPv6 a seulement un type de message en-tête de mobilité. AH et ESP n'ont pas d'autre champ de sélecteur. Un système peut vouloir envoyer un type et code de message ICMP qu'il ne veut pas recevoir. Dans les descriptions ci-dessous, "port" est utilisé pour parler d'un champ qui dépend du protocole de couche suivante.

A. Si un protocole de couche suivante n'a pas de sélecteur "port", les sélecteurs "port" local et distant sont réglés à OPAQUE dans l'entrée de SPD pertinente, par exemple,

   Local
   protocole de couche suivante = AH
   sélecteur de "port" = OPAQUE
   Distant
   protocole de couche suivante = AH
   sélecteur de "port" = OPAQUE

B. Même si un protocole de couche suivante a seulement un sélecteur, par exemple, type d'en-tête de mobilité, les sélecteurs de "port" local et distant sont utilisés pour indiquer si un système veut envoyer et/ou recevoir du trafic avec les valeurs de "port" spécifiées. Par exemple, si les en-têtes de mobilité d'un type spécifié sont autorisés à l'envoi et reçus via une SA, l'entrée de SPD pertinente serait alors réglée comme suit :

   Local
   protocole de couche suivante = en-tête de mobilité
   sélecteur de "port" = type de message d'en-tête de mobilité
   Distant
   protocole de couche suivante = en-tête de mobilité
   sélecteur de "port" = type de message d'en-tête de mobilité

Si l'envoi d'en-têtes de mobilité d'un type spécifié est permis mais PAS la réception via une SA, l'entrée de SPD pertinente serait alors réglée comme suit :

   Local
   protocole de couche suivante = en-tête de mobilité
   sélecteur de "port" = type de message d'en-tête de mobilité
   Distant
   protocole de couche suivante = en-tête de mobilité
   sélecteur de "port" = OPAQUE

Si la réception d'en-têtes de mobilité d'un type spécifié est permis mais PAS l'envoi via une SA, l'entrée de SPD pertinente serait alors réglée comme suit :

   Local
   protocole de couche suivante = en-tête de mobilité
   sélecteur de "port" = OPAQUE
   Distant
   protocole de couche suivante = en-tête de mobilité
   sélecteur de "port" = type de message d'en-tête de mobilité

C. Si un système veut envoyer du trafic avec une valeur de "port" particulière mais PAS recevoir du trafic avec cette sorte

de valeur d'accès, les sélecteurs de trafic du système sont réglés comme suit dans les entrées de SPD pertinentes :

Local
protocole de couche suivante = ICMP
sélecteur de "port" = <type & code ICMP spécifiques>
Distant
protocole de couche suivante = ICMP
sélecteur de "port" = OPAQUE

D. Pour indiquer qu'un système veut recevoir du trafic avec une valeur de "port" particulière mais PAS envoyer cette sorte de trafic, les sélecteurs de trafic du système sont réglés comme suit dans l'entrée de SPD pertinente :

Local
protocole de couche suivante = ICMP
sélecteur de "port" = OPAQUE
Distant
protocole de couche suivante = ICMP
sélecteur de "port" = <type & code ICMP spécifiques>

Par exemple, si une passerelle de sécurité veut permettre aux systèmes derrière elle d'envoyer des traceroutes ICMP, mais ne veut pas laisser les systèmes extérieurs faire des traceroutes ICMP aux systèmes qui sont derrière elle, les sélecteurs de trafic de la passerelle de sécurité seront réglés comme suit dans l'entrée de SPD pertinente :

Local
protocole de couche suivante = 1 (ICMPv4)
sélecteur de "port" = 30 (traceroute)
Distant
protocole de couche suivante = 1 (ICMPv4)
sélecteur de "port" = OPAQUE

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

Dans chaque mise en œuvre IPsec, il y a une base de données d'association de sécurité (SAD) nominale, dans laquelle chaque entrée définit les paramètres associés à une SA. Chaque SA a une entrée dans la SAD. Pour les traitements sortants, chaque entrée de SAD est visée par les entrées de la partie SPD-S de l'antémémoire de la SPD. Pour le traitement entrant, pour les SA en envoi individuel, la SPI est utilisée soit seule pour rechercher une SA, soit en conjonction avec le type de protocole IPsec. Si une mise en œuvre IPsec accepte la diffusion groupée, la SPI plus l'adresse de destination, ou la SPI plus les adresses de destination et de source sont utilisées pour rechercher la SA. (Voir au paragraphe 4.1 des précisions sur l'algorithme qui DOIT être utilisé pour transposer les datagrammes IPsec entrants en SA.) Les paramètres suivants sont associés à chaque entrée dans la SAD. Ils devraient tous être présents sauf indication contraire, par exemple, dans l'algorithme d'authentification AH. Cette description ne prétend pas être une MIB, mais seulement une spécification des éléments de données minimales requises pour prendre en charge une SA dans une mise en œuvre IPsec.

Pour chacun des sélecteurs définis au paragraphe 4.4.1.1, l'entrée dans la SAD pour une SA entrante DOIT être remplie initialement avec la ou les valeurs négociées à la création de la SA. (Voir au paragraphe 4.4.1 l'alinéa sous "Traitement des changements à la SPD pendant le fonctionnement du système" des indications sur l'effet de changements à la SPD sur les SA existantes.) Pour un receveur, ces valeurs sont utilisées pour vérifier que les champs d'en-tête d'un paquet entrant (après traitement IPsec) correspondent aux valeurs de sélecteur négociées pour la SA. Et donc, la SAD agit comme une antémémoire pour vérifier les sélecteurs de trafic entrant qui arrivent sur les SA. Pour le receveur, cela fait partie de la vérification qu'un paquet arrivant sur une SA est cohérent avec la politique pour la SA. (Voir à la Section 6 les règles pour les messages ICMP.) Ces champs peuvent avoir la forme de valeurs spécifiques, de gammes, ANY, ou OPAQUE, comme décrit au paragraphe 4.4.1.1, "Sélecteurs". Noter aussi qu'il y a quelques situations dans lesquelles la SAD peut avoir des entrées pour des SA qui n'ont pas d'entrée correspondante dans la SPD. Comme le présent document ne rend pas obligatoire que la SAD soit nettoyée de façon sélective lors de changements de la SPD, les entrées de SAD peuvent demeurer alors que les entrées de SPD qui les ont créées sont changées ou supprimées. Aussi, si une SA frappée à la main est créée, il pourrait y avoir une entrée de SAD pour cette SA qui ne corresponde à aucune entrée de SPD.

Note : La SAD peut prendre en charge des SA en diffusion groupée, si elles sont configurées manuellement. Une SA sortante en diffusion groupée a la même structure qu'une SA en envoi individuel. L'adresse de source est celle de l'envoyeur, et l'adresse de destination est l'adresse du groupe de diffusion groupée. Une SA entrante en diffusion groupée doit être configurée avec les adresses de source de chaque homologue autorisé à transmettre la SA de diffusion groupée en question. La valeur de SPI pour une SA en diffusion groupée est fournie par un contrôleur de groupe de diffusion groupée, et non par le receveur, comme pour une SA en envoi individuel. Parce qu'une entrée de SAD peut être requise de s'accommoder de plusieurs adresses de source IP individuelles qui faisaient partie d'une entrée de SPD (pour des SA en envoi individuel) la facilité exigée pour les SA entrantes en diffusion groupée est un

dispositif qui est déjà présent dans une mise en œuvre IPsec. Cependant, comme la SPD n'a aucune disposition pour s'accommoder d'entrées en diffusion groupée, le présent document ne spécifie pas une façon automatique de créer une entrée de SAD pour une SA entrante en diffusion groupée. Seules les entrées de SAD configurées manuellement peuvent être créées pour traiter le trafic entrant en diffusion groupée.

Lignes directrices pour la mise en œuvre : Le présent document né spécifie pas comment une entrée de SPD-S se réfère à l'entrée de SAD correspondante, car c'est un détail spécifique de la mise en œuvre. Cependant, certaines mises en œuvre (fondées sur l'expérience de la RFC2401) ont reconnu avoir des problèmes à cet égard. En particulier, mémoriser simplement la paire (adresse IP d'en-tête de tunnel distant, SPI distante) dans l'antémémoire de la SPD n'est pas suffisant, car la paire n'identifie pas toujours de façon univoque une seule entrée de SAD. Par exemple, deux hôtes derrière le même NAT pourraient choisir la même valeur de SPI. Cette situation peut aussi survenir si une adresse IP précédemment utilisée par un hôte est allouée à un autre hôte (par exemple, via DHCP) et si les SA associées au vieil hôte n'ont pas encore été supprimées par le mécanisme de détection des homologues morts. Cela peut conduire à ce que des paquets soient envoyés sur la mauvaise SA ou, si la gestion de clé assure que la paire est unique, à dénier une création de SA autrement valide. Et donc, les développeurs devraient mettre en œuvre des liaisons entre l'antémémoire de SPD et la SAD de façon à ne pas engendrer de tels problèmes.

4.4.2.1 Éléments de données dans la SAD

Les éléments de données suivants DOIVENT être dans la SAD :

- Indice de paramètre de sécurité (SPI) : une valeur de 32 bits choisie par l'extrémité de réception d'une SA pour identifier de façon univoque la SA. Dans une entrée de SAD pour une SA sortante, le SPI est utilisé pour construire l'en-tête AH ou ESP du paquet. Dans une entrée de SAD pour une SA entrante, le SPI est utilisé pour transposer le trafic aux SA appropriées (voir le texte sur envoi individuel/diffusion groupée au paragraphe 4.1).
- Compteur de numéro de séquence : un compteur à 64 bits utilisé pour générer le champ Numéro de séquence dans les en-têtes AH ou ESP. Les numéros de séquence à 64 bits sont par défaut, mais des numéros de séquence à 32 bis sont également pris en charge s'ils sont négociés.
- Débordement de compteur de séquence : c'est un fanion qui indique si le débordement du compteur de numéros de séquence devrait générer un événement d'audit et empêcher la transmission de paquets supplémentaires sur la SA, ou si le retour à zéro est permis. L'entrée d'enregistrement d'audit pour cet événement DEVRAIT inclure la valeur de SPI, la date/heure en cours, l'adresse locale, l'adresse distante, et les sélecteurs provenant de l'entrée pertinente de SAD.
- Fenêtre anti-répétition : un compteur de 64 bits et un codage binaire (ou équivalent) utilisé pour déterminer si un paquet AH ou ESP entrant est une répétition.

Note : Si l'anti-répétition a été désactivée par le receveur pour une SA, par exemple, dans le cas de SA frappée à la main, la fenêtre anti-répétition est alors ignorée pour la SA en question. Les numéros de séquence sont de 64 bits par défaut, mais cette taille de compteur accepte aussi bien les numéros de séquence de 32 bits.

- Algorithme d'authentification AH, clé, etc. Ceci n'est exigé que si AH est pris en charge.
- Algorithme de chiffrement ESP, clé, mode, IV, etc. Si un algorithme de mode combiné est utilisé, ces champs ne seront pas applicables.
- Algorithme d'intégrité ESP, clés, etc. Si le service d'intégrité n'est pas choisi, ces champs ne seront pas applicables. Si un algorithme de mode combiné est utilisé, ces champs ne seront pas applicables.
- Algorithmes ESP de mode combiné, clé(s), etc. Ces données sont utilisées lorsqu'un algorithme de mode combiné (chiffrement et intégrité) est utilisé avec ESP. Si un algorithme de mode combiné n'est pas utilisé, ces champs ne seront pas applicables.
- Durée de vie de cette SA : intervalle de temps après lequel une SA doit être remplacée par une nouvelle SA (et un nouvel SPI) ou terminée, plus une indication de laquelle de ces actions devrait survenir. Ce peut être exprimé comme une durée ou un compte d'octets, ou par l'utilisation simultanée des deux avec la première durée de vie à arriver à expiration qui a la préséance. Une mise en œuvre conforme DOIT prendre en charge ces deux types de durée de vie, et DOIT prendre en charge l'utilisation simultanée des deux. Si la durée est employée, et si IKE emploie des certificats X.509 pour l'établissement de SA, la durée de vie de SA doit être contrainte par les intervalles de validité des certificats, et la NextIssueDate *(prochaine date d'édition)* des listes de révocation de certificats (CRL, *Certificate Revocation List*) utilisée dans l'échange IKE pour la SA. L'initiateur et le répondant sont tous deux responsables des contraintes sur la durée de vie de la SA selon ce modèle. Note : Les détails de la façon de traiter le rafraîchissement des clés lorsque les SA arrivent à expiration sont des affaires locales. Cependant, une approche raisonnable est :
  (a) Si le compte d'octets est utilisé, la mise en œuvre DEVRAIT alors compter le nombre d'octets auxquels l'algorithme cryptographique IPsec est appliqué. Pour ESP, c'est l'algorithme de chiffrement (y compris le chiffrement Null) et pour AH, c'est l'algorithme d'authentification. Il inclut les octets de bourrage, etc. Noter que les mises en œuvre DOIVENT être capables de faire face à une situation où les compteurs aux extrémités d'une SA perdent la synchronisation, par exemple, à cause de pertes de paquet ou parce que les mises en œuvre à chaque extrémité de la SA ne traitent pas les choses de la même façon.
  (b) Il DEVRAIT y avoir deux sortes de durée de vie – une durée de vie douce, qui prévient la mise en œuvre

d'entreprendre une action telle que d'établir une SA de remplacement, et une durée de vie dure quand la SA en cours se termine et est détruite.

(c) Si le paquet entier n'est pas livré pendant la durée de vie de la SA, le paquet DEVRAIT être éliminé.

- o Mode de protocole IPsec : tunnel ou transport. Il indique quel mode, de AH ou de ESP, est appliqué au trafic sur cette SA.
- o Fanion de vérification dynamique de fragment : Indique si la vérification dynamique de fragment s'applique ou non à cette SA.
- o Outrepasser le bit DF (T/F) -- applicable aux SA en mode tunnel où les en-tête interne et externes sont tous deux IPv4.
- o Valeurs DSCP – ensemble des valeurs DSCP admises pour les paquets portés sur cette SA. Si aucune valeur n'est spécifiée, aucun filtrage spécifique de DSCP n'est appliqué. Si une ou plusieurs valeurs sont spécifiées, elles sont utilisées pour choisir une SA parmi plusieurs qui satisfont au sélecteurs de trafic pour un paquet sortant. Noter que ces valeurs ne sont PAS vérifiées par rapport au trafic entrant qui arrive sur la SA.
- o Outrepasser DSCP (T/F) ou transposer en valeurs DSCP non protégées (matrice) si nécessaire pour restreindre l'outrepassement des valeurs DSCP -- applicable aux SA en mode tunnel. Ce dispositif transpose les valeurs de DSCP provenant d'un en-tête interne en valeurs dans un en-tête externe, par exemple, pour traiter les problèmes de signalisation de canal caché.
- o MTU de chemin : toute MTU de chemin observé et les variables de vieillissement.
- o Adresse IP de source et destination d'en-tête de tunnel – les deux adresses doivent être soit IPv4 soit IPv6. La version implique le type d'en-tête IP à utiliser. N'est utilisée que lorsque le mode de protocole IPsec est tunnel.

4.4.2.2 Relations entre SPD, fanion PFP, paquet, et SAD

Pour chaque sélecteur, les tableaux suivants montrent les relations entre la valeur dans la SPD, le fanion PFP, la valeur dans le paquet déclencheur, et la valeur résultante dans la SAD. Noter que l'interface administrative pour IPsec peut utiliser diverses options syntaxiques pour faciliter l'entrée des règles par l'administrateur. Par exemple, bien que IKEv2 envoie une liste de gammes, il sera plus clair et il y aura moins d'erreurs si l'usager entre une seule adresse IP ou préfixe d'adresse IP.

Sélecteur	Entrée de SPD	PFP	Valeur du paquet déclencheur	Entrée de SAD résultante
adresse locale	liste de gammes	0	adresse IP "S"	liste de gammes
	ANY	0	adresse IP "S"	ANY
	liste de gammes	1	adresse IP "S"	"S"
	ANY	1	adresse IP "S"	"S"
adresse distante	liste de gammes	0	adresse IP "D"	liste de gammes
	ANY	0	adresse IP "D"	ANY
	liste de gammes	1	adresse IP "D"	"D"
	ANY	1	adresse IP "D"	"D"
protocole	liste de protocoles*	0	protocole "P"	liste de protocoles*
	ANY**	0	protocole "P"	ANY
	OPAQUE****	0	protocole "P"	OPAQUE
	liste de protocoles*	0	non disponible	éliminer le paquet
	ANY**	0	non disponible	ANY
	OPAQUE****	0	non disponible	OPAQUE
	liste de protocoles*	1	protocole"P"	"P"
	ANY**	1	protocole "P"	"P"
	OPAQUE****	1	protocole "P"	***
	liste de protocoles*	1	non disponible	éliminer le paquet
	ANY**	1	non disponible	éliminer le paquet
	OPAQUE****	1	non disponible	***

Si le protocole est un de ceux qui a deux ports, il y aura alors des sélecteurs pour les deux ports Local et Distant.

Sélecteur	Entrée de SPD	PFP	Vaeur du paquet déclencheur	Entrée de SAD résultante
accès local	liste de gammes	0	accès de source "s"	liste de gammes
	ANY	0	accès de source "s"	ANY
	OPAQUE	0	accès de source "s"	OPAQUE
	liste de gammes	0	non disponible	éliminer le paquet
	ANY	0	non disponible	ANY
	OPAQUE	0	non disponible	OPAQUE
	liste de gammes	1	accès de source "s"	"s"
	ANY	1	accès de source "s"	"s"
	OPAQUE	1	accès de source "s"	***
	liste de gammes	1	non disponible	éliminer le paquet

	ANY	1	non disponible	éliminer le paquet
	OPAQUE	1	non disponible	***
accès distant	liste de gammes	0	accès de destination "d"	liste de gammes
	ANY	0	accès de destination "d"	ANY
	OPAQUE	0	accès de destination "d"	OPAQUE
	liste de gammes	0	non disponible	éliminer le paquet
	ANY	0	non disponible	ANY
	OPAQUE	0	non disponible	OPAQUE
	liste de gammes	1	accès de destination "d"	"d"
	ANY	1	accès de destination "d"	"d"
	OPAQUE	1	accès de destination "d"	***
	liste de gammes	1	non disponible	éliminer le paquet
	ANY	1	non disponible	éliminer le paquet
	OPAQUE	1	non disponible	***

Si le protocole est en-tête de mobilité, il y aura alors un sélecteur pou le type mh.

Sélecteur	Entrée de SPD	PFP	Valeur du paquet déclencheur	Entrée de SAD résultante
type mh	liste de gammes	0	type mh "T"	liste de gammes
	ANY	0	type mh "T"	ANY
	OPAQUE	0	type mh "T"	OPAQUE
	liste de gammes	0	non disponible	éliminer le paquet
	ANY	0	non disponible	ANY
	OPAQUE	0	non disponible	OPAQUE
	liste de gammes	1	type mhe "T"	"T"
	ANY	1	type mh "T"	"T"
	OPAQUE	1	type mhe "T"	***
	liste de gammes	1	non disponible	éliminer le paquet
	ANY	1	non disponible	éliminer le paquet
	OPAQUE	1	non disponible	***

Si le protocole est ICMP, il y aura alors un sélecteur de 16 bits pour le type ICMP et le code ICMP. Noter que type et code sont liés l'un à l'autre, c'est-à-dire qu'un code s'applique à un type particulier. Ce sélecteur de 16 bits peut contenir un seul type et une gamme de codes, un seul type et ANY code, et ANY type et ANY code.

Sélecteur	Entrée de SPD	PFP	Valeur du paquet déclencheur	Entrée de SAD résultante
type et code ICMP	un seul type & gamme de codes	0	type "t" & code "c"	un seul type & gamme de codes
	un seul type & ANY code	0	type "t" & code "c"	un seul type & ANY code
	ANY type & ANY code	0	type "t" & code "c"	ANY type & ANY code
	OPAQUE	0	type "t" & code "c"	OPAQUE
	un seul type & gamme de codes	0	non disponible	éliminer le paquet
	un seul type & ANY code	0	non disponible	éliminer le paquet
	ANY type & ANY code	0	non disponible	ANY type & ANY code
	OPAQUE	0	non disponible	OPAQUE
	ICMP	1	type "t" & code "c"	"t" et "c"
	un seul type & ANY code	1	type "t" & code "c"	"t" et "c"
	ANY type & ANY code	1	type "t" & code "c"	"t" et "c"
	OPAQUE	1	type "t" & code "c"	***
	un seul type & gamme de codes	1	non disponible	éliminer le paquet
	un seul type & ANY code	1	non disponible	éliminer le paquet
	ANY type & ANY code	1	non disponible	éliminer le paquet
	OPAQUE	1	non disponible	***

Si le sélecteur name est utilisé :

Sélecteur	Entrée de SPD	PFP	Valeur dans le paquet déclencheur	Entrée de SAD résultante
name	liste de noms d'usager ou de système	non disponible	non disponible	non disponible

* "Liste de protocoles" est l'information, pas la façon qu'ont la SPD, SAD ou IKEv2 de représenter cette information.
** 0 (zéro) est utilisé par IKE pour indiquer ANY pour le protocole.
*** L'utilisation de PFP=1 avec une valeur OPAQUE est une erreur et DEVRAIT être interdite par une mise en œuvre

IPsec.
**** Le champ protocole ne peut pas être OPAQUE dans IPv4. Cette entrée de tableau ne s'applique que dans IPv6.

4.4.3 Base de données d'autorisations d'homologues (PAD)

La base de données d'autorisation d'homologues (PAD, *Peer Authorization Database*) fait le lien entre la SPD et un protocole de gestion d'associations de sécurité tel que IKE. Il incorpore plusieurs fonctions essentielles :
- o identifier les homologues ou groupes d'homologues qui sont autorisés à communiquer avec cette entité IPsec,
- o spécifier le protocole et la méthode utilisés pour authentifier chaque homologue,
- o fournir les données d'authentification pour chaque homologue,
- o imposer des contraintes aux types et valeurs des identifiants qui peuvent être affirmés par un homologue par rapport à la création de SA dérivées, pour s'assurer que l'homologue n'affirme pas des identités à rechercher dans la SPD qu'il n'est pas autorisé à représenter, lorsque des SA dérivées (filles) sont créées,
- o des informations de localisation de passerelle homologue, par exemple, adresses IP ou noms DNS, PEUVENT être incluses pour les homologues connus pour être "derrière" une passerelle de sécurité.

La PAD fournit ces fonctions pour un homologue IKE lorsque l'homologue agit comme initiateur ou répondant.

Pour effectuer ces fonctions, la PAD contient une entrée pour chaque homologue ou groupe d'homologues avec qui va communiquer l'entité IPsec. Une entrée désigne un homologue individuel (usager, système d'extrémité ou passerelle de sécurité) ou spécifie un groupe d'homologues (en utilisant les règles de correspondance d'identifiant définies ci-dessous). L'entrée spécifie le protocole d'authentification (par exemple, IKEv1, IKEv2, KINK) la méthode utilisée (par exemple, certificats ou secrets prépartagés) et les données d'authentification (par exemple, le secret prépartagé ou l'ancre de confiance par rapport auquel le certificat de l'homologue sera 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 dépôt de CRL ou sur le nom d'un serveur de protocole d'état de certificat en ligne (OSCP, *Online Certificate Status Protocol*) associé à l'homologue ou à l'ancre de confiance associée à l'homologue.

Chaque entrée spécifie aussi si la charge utile d'identifiant IKE sera utilisée comme nom symbolique pour la recherche de SPD, ou si l'adresse IP distante fournie dans les charges utiles de sélecteur de trafic sera utilisée pour les recherches de SPD lors de la création de SA filles.

Noter que les informations de PAD PEUVENT être utilisées pour soutenir la création de plus d'une SA en mode tunnel à un moment donné entre deux homologues, par exemple, deux tunnels pour protéger les mêmes adresses/hôtes, mais avec des points d'extrémité de tunnel différents.

4.4.3.1 Identifiants d'entrée de PAD et règles de correspondance

La PAD est une base de données ordonnée, où l'ordre est défini par un administrateur (ou un usager dans le cas d'un système d'extrémité à un seul usager). Habituellement, le même administrateur sera responsable à la fois de la PAD et de la SPD, car les deux bases de données doivent être coordonnées. L'exigence d'ordre de la PAD relève des mêmes raisons que pour la SPD, c'est-à-dire, à cause de l'utilisation d'entrées avec des caractères génériques qui permet des chevauchements dans l'ensemble des identifiants IKE qui pourraient correspondre à une entrée spécifique.

Six types d'identifiants sont pris en charge pour les entrées dans la PAD, qui sont cohérents avec les types de nom symbolique et les adresses IP utilisées pour identifier les entrées de SPD. L'identifiant pour chaque entrée agit comme l'indice pour la PAD, c'est-à-dire qu'il est la valeur utilisée pour choisir une entrée. Tous ces types d'identifiant sont utilisés pour établir la correspondance des types de charge utile d'identifiant IKE. Les six types sont :
- o nom DNS (spécifique ou partiel)
- o nom distinctif (complet ou contraint par un sous-arbre)
- o adresse de messagerie électronique de la RFC 822 (complète ou qualifiée partiellement)
- o adresse IPv4 (gamme)
- o adresse IPv6 (gamme)
- o identifiant de clé (correspondance exacte seulement).

Les trois premiers types de nom peuvent s'accommoder d'une correspondance de sous-arbre aussi bien que de correspondances exactes. Un nom DNS peut être pleinement qualifié et donc correspondre exactement à un nom, par exemple, foo.example.com. Autrement, le nom peut renfermer un groupe d'homologues en étant spécifié partiellement, par exemple, la chaîne ".example.com" pourrait être utilisée pour correspondre à tout nom DNS se terminant par ces deux composants de nom de domaine.

De même, un nom distinctif peut spécifier un nom distinctif complet pour qu'il corresponde exactement à une entrée, par exemple, CN = Stephen, O = BBN Technologies, SP = MA, C = US. Autrement, une entrée peut renfermer un groupe

d'homologues en spécifiant un sous-arbre, par exemple, une entrée de la forme "C = US, SP = MA" pourrait être utilisée pour établir la correspondance avec tous les noms DN qui contiennent ces deux attributs comme noms distinctifs relatifs (RDN, *Relative Distinguished Names*) de sommet.

Pour les adresses de messagerie électronique de la RFC 822, les mêmes options existent. Une adresse complète comme foo@example.com correspond à une entité, mais un nom de sous-arbre comme "@example.com" pourrait être utilisé pour correspondre à toutes les entités ayant des noms qui se terminent avec les deux noms de domaine à droite du @.

La syntaxe spécifique utilisée par une mise en œuvre pour s'accommoder de la correspondance de sous-arbre pour les noms distinctifs, les noms de domaine ou les adresses de messagerie électronique de la RFC 822 est une affaire locale. Mais, au minimum, la correspondance de sous-arbre décrite ci-dessus DOIT être prise en charge. (La correspondance de sous-chaîne au sein d'un nom distinctif, nom DNS, ou adresse de la RFC 822 PEUT être acceptée, mais n'est pas exigée.)

Pour les adresses IPv4 et IPv6, la même syntaxe de gamme d'adresse qu'utilisée pour les entrées de SPD DOIT être acceptée. Cela permet la spécification d'une adresse individuelle (via une gamme triviale), d'un préfixe d'adresse (en choisissant une gamme qui suive un style de préfixe d'acheminement inter-domaine sans classe (CIDR, *Classless Inter-Domain Routing*), ou une gamme d'adresses arbitraire.

Le champ Identifiant de clé *(Key ID)* se définit comme une chaîne OCTET dans IKE. Pour ce type de nom, seule une syntaxe de correspondance exacte DOIT être acceptée (car il n'y a pas de structure explicite pour ce type d'identifiant). Des fonctions de correspondance supplémentaires PEUVENT être acceptées pour ce type d'identifiant.

4.4.3.2 Données d'authentication d'homologue de IKE

Une fois qu'une entrée est localisée sur la base d'une recherche ordonnée dans la PAD fondée sur la correspondance des champs d'identifiant, il est nécessaire de vérifier l'assertion d'identité, c'est-à-dire, d'authentifier l'ID affirmé. Pour chaque entrée de PAD, il y a l'indication du type d'authentification à effectuer. Le présent document exige la prise en charge des deux types de données d'authentification :

- certificat X.509
- secret prépartagé

Pour l'authentification fondée sur un certificat X.509, l'entrée de PAD contient une ancre de confiance via laquelle le certificat de l'entité d'extrémité (EE, *end entity*) pour l'homologue doit être vérifiable, soit directement soit via un chemin de certificat. Voir à la RFC3280 la définition d'une ancre de confiance. Une entrée utilisée avec une authentification fondée sur un certificat PEUT inclure des données supplémentaires pour faciliter l'état de révocation de certificat, par exemple, une liste des répondants OCSP appropriés ou de dépôts de CRL, et les données d'authentification associées. Pour l'authentification fondée sur un secret prépartagé, la PAD contient le secret prépartagé à utiliser par IKE.

Le présent document n'exige pas que l'identifiant IKE affirmé par un homologue soit syntaxiquement en relation avec un champ spécifique dans un certificat d'entité terminale employé pour authentifier l'identité de cet homologue. Cependant, il sera souvent approprié d'imposer une telle exigence, par exemple, lorsque une seule entrée représente un ensemble d'homologues dont chacun peut avoir une entrée de SPD distincte. Et donc, les mises en œuvre DOIVENT fournir à un administrateur les moyens d'exiger une correspondance entre un identifiant IKE affirmé et le nom de sujet ou subject alt name dans un certificat. Le premier est applicable aux identifiants IKE exprimés comme noms distinctif ; le dernier est approprié pour les noms du DNS, les adresses de messagerie électronique de la RFC822, et les adresses IP. Comme l'identifiant KEY est destiné à identifier un homologue authentifié via un secret prépartagé, il n'y a pas d'exigence de correspondance entre ce type d'identifiant et un champ de certificat.

Voir IKEv1 [RFC2409] et IKEv2 [RFC4306] pour des précisions sur la façon dont IKE effectue l'authentification d'homologues en utilisant des certificats ou des secrets prépartagés.

Le présent document ne rend obligatoire la prise en charge d'aucune autre méthode d'authentification, bien que de telles méthodes PUISSENT être employées.

4.4.3.3 Données d'autorisation de SA fille

Une fois qu'un homologue IKE est authentifié, les SA filles peuvent être créées. Chaque entrée de PAD contient des données pour restreindre l'ensemble des identifiants qui peuvent être affirmés par un homologue IKE, pour établir la correspondance avec la SPD. Chaque entrée de PAD indique si l'identifiant IKE est à utiliser comme un nom symbolique pour la correspondance avec la SPD, ou si une adresse IP établie dans une charge utile de sélecteur de trafic est à utiliser.

Si l'entrée indique que l'identifiant IKE est à utiliser, le champ d'identifiant d'entrée de PAD définit alors l'ensemble d'identifiants autorisés. Si l'entrée indique que des sélecteurs de trafic de SA filles sont à utiliser, un élément de données

supplémentaire est alors requis, sous la forme de gammes d'adresses IPv4 et/ou IPv6. (Un homologue peut être autorisé pour les deux types d'adresses, aussi DOIT-il y avoir des dispositions pour les deux gammes d'adresses v4 et v6.)

4.4.3.4 Comment utiliser la PAD

Durant l'échange IKE initial, l'initiateur et le répondant affirment chacun leur identité via la charge utile IKE ID et envoient une charge utile AUTH pour vérifier l'identité affirmée. Une ou plusieurs charges utiles CERT peuvent être transmises pour faciliter la vérification de chaque identité affirmée.

Lorsque une entité IKE reçoit une charge utile d'identifiant IKE, elle utilise l'identifiant affirmé pour localiser une entrée dans la PAD, en utilisant les règles de correspondance décrites ci-dessus. L'entrée de PAD spécifie la méthode d'authentification à employer pour l'homologue identifié. Cela assure que la bonne méthode est utilisée pour chaque homologue et que des méthodes différentes peuvent être utilisées pour les différents homologues. L'entrée spécifie aussi les données d'authentification qui seront utilisées pour vérifier l'identité affirmée. Ces données sont employées en conjonction avec la méthode spécifiée pour authentifier l'homologue, avant qu'aucune SA fille ne soit créée.

Les SA filles sont créées sur la base des échanges de charges utiles de sélecteur de trafic, soit à la fin de l'échange IKE initial soit dans des échanges CREATE_CHILD_SA ultérieurs. L'entrée de PAD pour l'homologue IKE (maintenant authentifié) est utilisée pour restreindre la création de SA filles ; précisément, l'entrée de PAD spécifie comment se fait la recherche dans la SPD en utilisant une proposition de sélecteur de trafic provenant d'un homologue. Le choix est le suivant : soit l'identifiant IKE affirmé par l'homologue est utilisé pour trouver une entrée SPD via son nom symbolique, soit les adresses IP d'homologue affirmées dans les charges utiles de sélecteur de trafic sont utilisées pour les recherches de SPD sur la base de la portion champ d'adresse IP distante d'une entrée de SPD. Il est nécessaire d'imposer ces contraintes sur la création de SA filles pour empêcher un homologue authentifié d'usurper les identifiants associés à d'autres homologues légitimes.

Noter que parce que la PAD est vérifiée avant la recherche d'une entrée de SPD, cette sauvegarde protège un initiateur contre les attaques d'usurpation. Par exemple, supposons que IKE A reçoive un paquet sortant destiné à l'adresse IP X, un hôte servi par une passerelle de sécurité. La [RFC2401] et le présent document ne spécifient pas comment A détermine l'adresse de l'homologue IKE servant X. Cependant, tout homologue contacté par A comme représentant présumé de X doit être enregistré dans la PAD afin de permettre d'authentifier l'échange IKE. De plus, lorsque l'homologue authentifié affirme représenter X dans son échange de sélecteur de trafic, la PAD sera consultée pour déterminer si l'homologue en question est autorisé à représenter X. Et donc, la PAD fournit une liaison des gammes d'adresses (ou de sous-espace de nom) aux homologues, pour contrer de telles attaques.

4.5 SA et gestion de clés

Toutes les mises en œuvre IPsec DOIVENT prendre en charge la gestion de SA et de clé de chiffrement aussi bien manuelle qu'automatisée. Les protocoles IPsec, AH et ESP, sont largement indépendants des techniques de gestion de SA associées, bien que les techniques impliquées affectent effectivement certains des services de sécurité offerts par les protocoles. Par exemple, le service facultatif anti-répétition disponible pour AH et ESP exige une gestion automatisée de SA. De plus, la granularité de la distribution de clé employée avec IPsec détermine la granularité de l'authentification fournie. En général, l'authentification d'origine des données en AH et ESP est limitée par l'extension du partage des secrets utilisés avec l'algorithme d'intégrité (ou avec un protocole de gestion de clé qui crée de tels secrets) entre plusieurs sources possibles.

Le texte qui suit décrit les exigences minimum pour les deux types de gestion de SA.

4.5.1 Techniques manuelles

La forme de gestion la plus simple est la gestion manuelle, dans laquelle une personne configure manuellement chaque système avec les données de matériel de clés et de gestion de SA pertinentes pour sécuriser la communication avec les autres systèmes. Les techniques manuelles sont praticables dans des petits environnements statiques mais ils ne s'étendent pas bien. Par exemple, une compagnie pourrait créer un réseau privé virtuel (VPN) en utilisant IPsec dans des passerelles de sécurité sur plusieurs sites. Si le nombre de sites est faible, et si tous les sites sont du ressort d'un seul domaine administratif, ce peut être un contexte acceptable pour des techniques de gestion manuelle. Dans ce cas, la passerelle de sécurité peut protéger le trafic de façon sélective de et vers les autres sites au sein de l'organisation en utilisant une clé configurée manuellement, tout en ne protégeant pas le trafic pour les autres destinations. Cela pourrait aussi être approprié lorsque seules des communications choisies ont besoin d'être sécurisées. Un argument similaire peut s'appliquer à l'utilisation de IPsec entièrement au sein d'une organisation pour un petit nombre d'hôtes et/ou passerelles. Les techniques de gestion manuelles emploient souvent des clés symétriques configurées de façon statique, bien que d'autres options existent aussi.

4.5.2 SA automatisée et gestion de clés

Le large développement de l'utilisation de IPsec exige un protocole de gestion de SA Internet standard, modulable et automatisé. Une telle prise en charge est nécessaire pour faciliter l'utilisation des dispositifs anti-répétition de AH et ESP, et pour traiter la création de SA à la demande, par exemple, pour la création de clés orientées usager et orientées session. (Noter que la notion de "renouvellement de clés" d'une SA implique en réalité la création d'une nouvelle SA avec un nouvel SPI, processus qui implique généralement l'utilisation d'un protocole de gestion de SA/clé automatisé.)

Le protocole de gestion de clé automatisé par défaut choisi pour être utilisé avec IPsec est IKEv2 [RFC4306]. Le présent document suppose la disponibilité de certaines fonctions de la part du protocole de gestion de clés qui ne sont pas prises en charge par IKEv1. D'autres protocoles de gestion de SA automatisés PEUVENT être employés.

Lorsque un protocole automatisé de gestion de SA/clé est employé, le résultat de ce protocole est utilisé pour générer plusieurs clés pour une seule SA. Cela arrive aussi parce que des clés distinctes sont utilisées pour chacune des deux SA créées par IKE. Si l'intégrité et la confidentialité sont toutes deux employées, un minimum de quatre clés est alors nécessaire. De plus, certains des algorithmes cryptographiques peuvent requérir plusieurs clés, par exemple, 3DES.

Le système de gestion de clés fournit une chaîne binaire séparée pour chaque clé ou il peut générer une chaîne binaire d'où toutes les clés sont extraites. Si une seule chaîne binaire est fournie, il faut veiller à s'assurer que les parties du système qui transpose la chaîne binaire en les clés requises le fait de la même façon aux deux extrémités de la SA. Pour s'assurer que les mises en œuvre IPsec à chaque extrémité de la SA utilisent les mêmes bits pour les mêmes clés, et sans égard à la partie du système qui divise la chaîne binaire en clés individuelles, les clés de chiffrement DOIVENT être tirées des premiers bits (le plus à gauche, de plus fort poids) et les clés d'intégrité DOIVENT être tirées des bits restants. Le nombre de bits pour chaque clé est défini dans la RFC de spécification d'algorithme cryptographique pertinente. Dans le cas de plusieurs clés de chiffrement ou plusieurs clés d'intégrité, la spécification de l'algorithme cryptographique doit spécifier l'ordre dans lequel elles sont à sélectionner à partir d'une seule chaîne de bits fournie à l'algorithme cryptographique.

4.5.3 Localisation d'une passerelle de sécurité

Ce paragraphe expose les questions qui se rapportent à la façon dont un hôte apprend l'existence des passerelles de sécurité pertinentes, et, une fois qu'un hôte a contacté ces passerelles de sécurité, comment il sait que ce sont les passerelles de sécurité correctes. Les détails de l'endroit où sont mémorisées les informations requises sont une affaire locale, mais la base de données d'autorisations d'homologues (PAD) décrite au paragraphe 4.4 est le candidat le plus vraisemblable.
(Note : S* indique un système qui fonctionne avec IPsec, par exemple, SH1 et SG2 ci-dessous.)

Considérons une situation dans laquelle un hôte distant (SH1) utilise l'Internet pour obtenir l'accès à un serveur ou autre machine (H2) et qu'il y a une passerelle de sécurité (SG2), par exemple, un pare-feu, à travers lequel le trafic de H1 doit passer. Un exemple de cette situation serait celle d'un hôte mobile qui traverse l'Internet depuis le pare-feu (SG2) de son organisation de rattachement. Cette situation soulève plusieurs problèmes :

1. Comment SH1 apprend-il l'existence de la passerelle de sécurité SG2 ?
2. Comment authentifie-t-il SG2, et une fois qu'il a authentifié SG2, comment confirme-t il que SG2 a été autorisée à représenter H2 ?
3. Comment SG2 authentifie-t-elle SH1 et vérifie que SH1 est autorisé à contacter H2 ?
4. Comment SH1 apprend-t-il l'existence de passerelles supplémentaires qui fournissent des chemins de remplacement pour H2 ?

Pour régler ces problèmes, un hôte ou passerelle de sécurité qui prend en charge IPsec DOIT avoir une interface administrative qui permette à l'usager/administrateur de configurer l'adresse d'une ou plusieurs passerelles de sécurité pour des gammes d'adresses de destination qui exigent cette utilisation. Cela inclut la capacité de configurer les informations de localisation et d'authentification d'une ou plusieurs passerelles de sécurité et de vérifier l'autorisation de ces passerelles à représenter l'hôte de destination. (La fonction d'autorisation est implicite dans la PAD.) Le présent document ne traite pas de la question de savoir comment automatiser la découverte/vérification des passerelles de sécurité.

4.6 SA et diffusion groupée

L'orientation de la SA vers le receveur implique que, dans le cas de trafic en envoi individuel, le système de destination va choisir la valeur du SPI. En ayant la valeur du SPI choisie par la destination, il n'y a pas de possibilité qu'une SA configurée manuellement entre en conflit avec des SA configurées automatiquement (par exemple, via un protocole de gestion de clés) ou pour des SA provenant de plusieurs sources, d'entrer en conflit les unes les autres. Pour le trafic en diffusion groupée, il y a plusieurs systèmes de destination qui sont associés à une seule SA. Ainsi certains systèmes ou certaines personnes auront besoin de coordination entre tous les groupes de diffusion groupée pour choisir un ou des SPI au

nom de chaque groupe de diffusion groupée, puis de communiquer les informations IPsec du groupe à tous les membres légitimes de ce groupe de diffusion groupée via des mécanismes qui ne sont pas définis ici.

Les envoyeurs multiples à un groupe de diffusion groupée DEVRAIENT utiliser une seule association de sécurité (et donc un seul SPI) pour tout le trafic vers ce groupe lorsque un algorithme de chiffrement ou d'intégrité à clé symétrique est employé. Dans de telles circonstances, tout ce que sait le receveur est que le message vient d'un système qui possède la clé pour ce groupe de diffusion groupée. Dans de telles circonstances, un receveur ne sera généralement pas capable d'authentifier le système qui a envoyé le trafic en diffusion groupée. Les spécifications pour d'autres approches, plus générales, sont renvoyées au groupe de travail Sécurité de la diffusion groupée de l'IETF.

5 Traitement du trafic IP

Comme mentionné au paragraphe 4.4.1, "Base de données de politiques de sécurité (SPD)", la SPD (ou les antémémoires associées) DOIT être consultée durant le traitement de tout le trafic qui traverse la frontière de la protection IPsec, y compris le trafic de gestion IPsec. Si aucune politique n'est trouvée dans la SPD qui corresponde à un paquet (pour le trafic entrant ou sortant) le paquet DOIT être éliminé. Pour simplifier le traitement, et pour permettre des recherches très rapides de SA (pour SG/BITS/BITW) le présent document introduit la notion d'antémémoire de SPD pour tout le trafic sortant (SPD-O plus SPD-S) et d'antémémoire pour le trafic entrant, non protégé par IPsec (SPD-I). (Comme mentionné plus haut, la SAD agit comme une antémémoire pour vérifier les sélecteurs de trafic entrant protégé par IPsec qui arrive sur les SA.) Il y a nominalement une antémémoire par SPD. Pour les besoins de la présente spécification, on suppose que chaque entrée d'antémémoire sera transposée en exactement une SA. Noter, cependant, que des exceptions apparaissent lorsque on utilise plusieurs SA pour porter du trafic de priorités différentes (par exemple, comme indiqué par des valeurs DSCP distinctes) mais avec les mêmes sélecteurs. Noter aussi qu'il y a quelques situations dans lesquelles la SAD peut avoir des entrées pour des SA qui n'ont pas d'entrées correspondantes dans la SPD. Comme le présent document ne rend pas obligatoire que la SAD soit nettoyée sélectivement quand la SPD est changée, les entrées de SAD peuvent rester quand les entrées de SPD qui les ont créées sont changées ou supprimées. Aussi, si une SA entrée manuellement est créée, il pourrait y avoir une entrée de SAD pour cette SA qui ne corresponde à aucune entrée de SPD.

Comme les entrées de SPD peuvent se chevaucher, on ne peut pas mettre ces entrées en antémémoire en toute sécurité en général. Une simple mise en antémémoire pourrait avoir pour résultat une correspondance avec une entrée d'antémémoire, alors qu'une recherche ordonnée de la SPD aurait donné une correspondance avec une entrée différente. Mais, si les entrées de la SPD sont d'abord décorrélées, les entrées résultantes peuvent être mises en antémémoire en toute sécurité. Chaque entrée d'antémémoire aura l'indication que le trafic correspondant devrait être outrepassé ou éliminé, selon le cas. (Note : l'entrée de SPD originale peut résulter en plusieurs SA, par exemple, à cause du PFP.) Sauf mention contraire, toutes les références ci-dessous à "SPD" ou "antémémoire de SPD" ou "antémémoire" le sont à une SPD décorrélée (SPD-I, SPD-O, SPD-S) ou à l'antémémoire de SPD qui contient les entrées provenant de la SPD décorrélée.

Note : Dans une mise en œuvre d'hôte IPsec fondée sur des accès, la SPD sera consultée chaque fois qu'un nouvel accès est créé pour déterminer quel traitement IPsec, s'il en est, sera appliqué au trafic qui va s'écouler sur cet accès. Cela fournit un mécanisme implicite de mise en antémémoire, et les portions de la discussion précédente qui traitent de mise en antémémoire peuvent être ignorées dans de telles mises en œuvre.

Note : On suppose qu'on commence avec une SPD corrélée parce que c'est comme cela que les utilisateurs et administrateurs sont habitués à gérer ces sortes de listes de contrôle d'accès ou règles de filtre de pare-feu. L'algorithme de décorrélation est appliqué pour construire une liste d'entrées de SPD capables d'être mises en antémémoire. La décorrélation est invisible à l'interface de gestion.

Pour le trafic IPsec entrant, l'entrée de SAD choisie par le SPI sert d'antémémoire pour les sélecteurs pour être comparée aux paquets IPsec qui arrivent, après avoir effectué le traitement AH ou ESP.

5.1 Traitement du trafic IP sortant (protégé à non protégé)

Considérons d'abord le chemin pour le trafic entrant dans la mise en œuvre via une interface protégée et sortant via une interface non protégée.

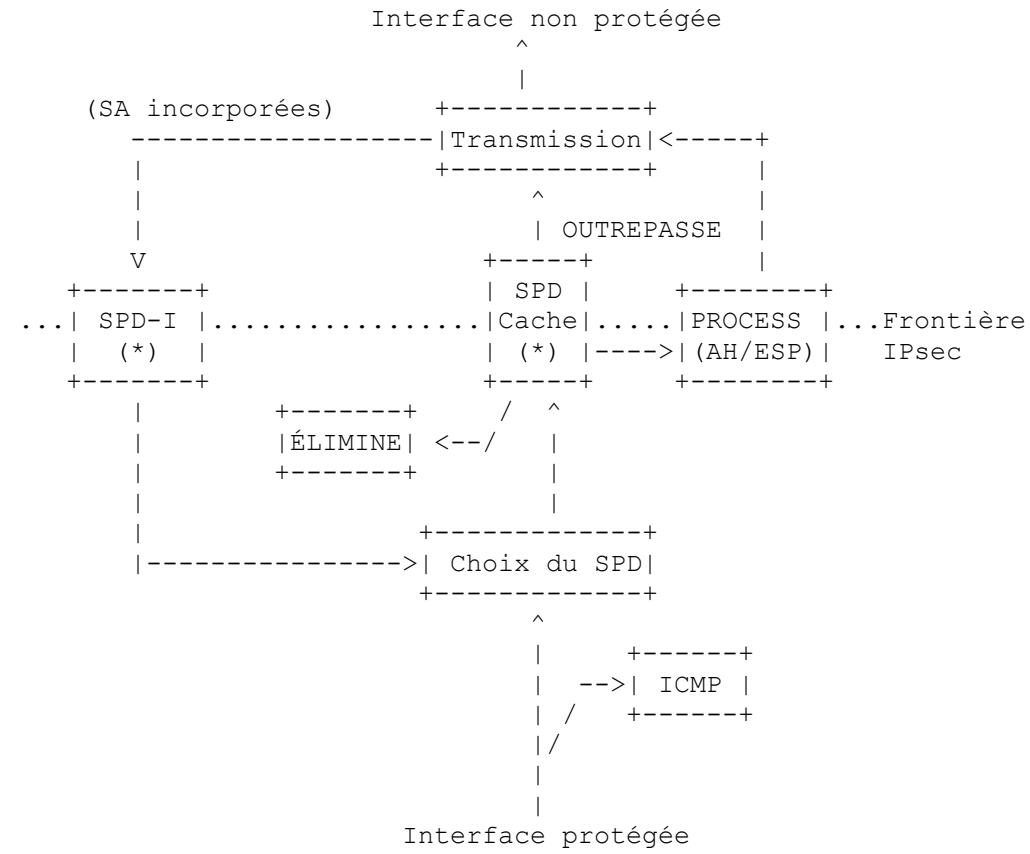


Figure 2. Modèle de traitement pour le trafic sortant

(*) = Les antémémoires de SPD sont figurées ici. S'il manque une antémémoire, la SPD est vérifiée. Il n'y a pas d'exigence qu'une mise en œuvre mette le paquet en mémoire tampon si il manque une antémémoire.

IPsec DOIT effectuer les étapes suivantes lors du traitement des paquets sortants :

1. Lorsqu'un paquet arrive de l'interface d'abonné (protégée), invoquer la fonction de sélection de la SPD pour obtenir l'identifiant de SPD nécessaire pour choisir la SPD appropriée. Si la mise en œuvre n'utilise qu'une seule SPD, cette étape est sans objet.)

2. Comparer les en-têtes du paquet à l'antémémoire pour la SPD spécifiée par l'identifiant de SPD de l'étape 1. Noter que cette antémémoire contient des entrées provenant de SPD-O et SPD-S.

3a. Si il y a une correspondance, traiter alors le paquet comme spécifié par l'entrée d'antémémoire correspondante, c'est-à-dire, OUTREPASSE, ÉLIMINE, ou PROTEGE, en utilisant AH ou ESP. Si le traitement IPsec est appliqué, il y a un lien de l'entrée d'antémémoire SPD à l'entrée pertinente de SAD (qui spécifie mode, algorithmes cryptographiques, clés, SPI, PMTU, etc.). Le traitement IPsec est celui défini précédemment, pour les modes transport et tunnel, et pour AH ou ESP, comme spécifié dans leurs RFC respectives [RFC4302], [RFC4303]. Noter que la valeur de PMTU de la SA, plus la valeur du fanion de vérification dynamique de fragment (et du bit DF dans l'en-tête IP du paquet sortant) déterminent si le paquet peut (il le doit) être fragmenté avant ou après le traitement IPsec, ou si il doit être éliminé et un message PMTU ICMP envoyé.

3b. Si aucune correspondance n'est trouvée dans l'antémémoire, rechercher dans la SPD (parties SPD-S et SPD-O) spécifiées par le SPD-ID. Si l'entrée de SPD appelle BYPASS ou DISCARD, créer une ou plusieurs nouvelles entrées d'antémémoire de SPD sortantes et si c'est BYPASS, créer une ou plusieurs nouvelles entrées d'antémémoire de SPD entrantes. (Plus d'une entrée d'antémémoire peuvent être créées car une entrée de SPD décorrélée peut être liée à d'autres entrées semblables crées par un effet collatéral du processus de décorrélation.) Si l'entrée de SPD appelle PROTECT, c'est-à-dire, création d'une SA, le mécanisme de gestion de clés (par exemple, IKEv2) est invoqué pour créer la SA. Si la création de SA réussit, une nouvelle entrée d'antémémoire sortante (SPD-S) est créée, avec les entrées de SAD entrante et sortante, autrement le paquet est éliminé. (Un paquet qui déclenche une recherche de SPD PEUT être éliminé par la mise en œuvre, ou il PEUT être traité par rapport à l'entrée d'antémémoire nouvellement créée, s'il en a été créée une.) Comme les SA sont créées par paires, une entrée de SAD pour la SA entrante correspondante est aussi créée, et elle contient les valeurs de sélecteur déduites de l'entrée de SPD (et du paquet, si des fanions PFP étaient "vrai") utilisée pour créer la SA entrante, à utiliser dans la vérification du trafic entrant livré via la SA.

4. Le paquet est passé à la fonction de transmission sortante (qui fonctionne en dehors de la mise en œuvre IPsec), pour choisir l'interface sur laquelle le paquet sera dirigé. Cette fonction peut être cause que le paquet soit repassé à travers la frontière IPsec, pour un traitement IPsec supplémentaire, par exemple, à l'appui de SA incorporées. S'il en est ainsi, il DOIT y avoir une entrée dans la base de données SPD-I qui permette un outrepassement entrant du paquet, autrement le paquet sera éliminé. Si nécessaire, c'est-à-dire, si il y a plus de une SPD-I, le trafic repassant en boucle PEUT être étiqueté comme venant de cette interface interne. Cela permettrait l'utilisation d'une SPD-I différente pour le trafic externe "réel" de celle utilisée pour le trafic en boucle, si nécessaire.

Note : À l'exception du mode transport IPv4 et IPv6, une mise en œuvre SG, BITS, ou BITW PEUT fragmenter les paquets avant d'appliquer IPsec. (Ceci ne s'applique qu'à IPv4. Pour les paquets IPv6, seul le générateur est autorisé à les fragmenter.) L'appareil DEVRAIT avoir un réglage de configuration pour désactiver cela. Les fragments résultants sont évalués par rapport à la SPD de la façon normale. Et donc, les fragments qui ne contiennent pas de numéro d'accès (ou type et code de message ICMP, ou type d'en-tête de mobilité) vont seulement correspondre à des règles ayant des sélecteurs d'accès (ou type et code de message ICMP, ou type MH) de OPAQUE ou ANY. Voir la Section 7 pour des précisions.)

Note : À l'égard de la détermination et de la mise en application de la PMTU d'une SA, le système IPsec DOIT suivre les étapes décrites au paragraphe 8.2.

5.1.1 Traitement d'un paquet sortant qui doit être éliminé

Si un système IPsec reçoit un paquet sortant dont il trouve qu'il doit l'éliminer, il DEVRAIT être capable de générer et envoyer un message ICMP pour indiquer à l'envoyeur du paquet sortant qui celui-ci a été éliminé. Le type et code du message ICMP va dépendre de la raison de l'élimination du paquet, comme spécifié ci-dessous.
La raison DEVRAIT être enregistrée dans le journal d'audit. L'entrée de journal d'audit pour cet événement DEVRAIT inclure la raison, la date/heure en cours, et les valeurs de sélecteur tirées du paquet.

a. Les sélecteurs du paquet correspondaient à une entrée de SPD exigeant que le paquet soit éliminé.
   IPv4 Type = 3 (destination inaccessible) Code = 13 (Communication administrativement prohibée)
   IPv6 Type = 1 (destination inaccessible) Code = 1 (Communication avec destination administrativement prohibée)

b1. Le système IPsec a réussi à atteindre l'homologue distant mais a été incapable de négocier la SA requise par l'entrée de SPD correspondant au paquet parce que, par exemple, l'homologue distant est administrativement interdit de communication avec l'initiateur, l'homologue initiateur a été incapable de s'authentifier à l'homologue distant, l'homologue distant a été incapable de s'authentifier auprès de l'homologue initiateur, ou la SPD de l'homologue distant ne possédait pas d'entrée convenable.
   IPv4 Type = 3 (destination inaccessible) Code = 13 (Communication administrativement prohibée)
   IPv6 Type = 1 (destination inaccessible) Code = 1 (Communication avec destination administrativement prohibée)

b2. Le système IPsec était incapable d'établir la SA requise par l'entrée de SPD correspondant au paquet parce que l'homologue IPsec à l'autre extrémité de l'échange n'a pas pu être contacté.
   IPv4 Type = 3 (destination inaccessible) Code = 1 (hôte inaccessible)
   IPv6 Type = 1 (destination inaccessible) Code = 3 (adresse inaccessible)

Noter qu'un attaquant derrière une passerelle de sécurité pourrait envoyer des paquets avec une adresse de source déguisée, W.X.Y.Z, à une entité IPsec, l'amenant à envoyer des messages ICMP à W.X.Y.Z. Cela crée une opportunité d'attaque de déni de service (DoS) contre les hôtes derrière une passerelle de sécurité. Pour régler ce problème, une passerelle de sécurité DEVRAIT inclure un contrôle de gestion pour permettre à un administrateur de configurer une mise en œuvre IPsec pour envoyer ou pas les messages ICMP dans ces circonstances, et si cette facilité est choisie, de limiter le débit de transmission de telles réponses ICMP.

5.1.2 Construction d'en-tête pour le mode tunnel

Ce paragraphe décrit le traitement des en-têtes IP internes et externes, des en-têtes d'extension, et des options pour les tunnels AH et ESP, à l'égard du traitement du trafic sortant. Cela inclut la façon de construire l'en-tête IP d'incorporation (sortant) de traiter les champs pour l'en-tête IP interne, et que les autres actions devraient être entreprises pour le trafic sortant en mode tunnel. Le processus général décrit ici est modélisé d'après la [RFC2003], "Encapsulation IP au sein d'IP" :

o Les en-têtes IP externes Adresse de source et Adresse de destination identifient les "points d'extrémité" du tunnel (l'encapsuleur et le désencapsuleur). Les en-têtes IP internes Adresse de source et Adresse de destination identifient respectivement l'envoyeur et le receveur d'origine du datagramme (du point de vue de ce tunnel). (Voir la note de bas

de page 3 après le tableau du paragraphe 5.1.2.1 pour des précisions sur l'encapsulation de l'adresse IP de source.)

- L'en-tête IP interne n'est pas changé excepté comme noté ci-dessous pour les champs TTL (ou la limite de bond) et DS/ECN. L'en-tête IP interne reste autrement inchangé durant sa livraison au point de sortie du tunnel.

- Aucun changement aux en-têtes IP d'options ou d'extension dans l'en-tête interne n'intervient durant la livraison du datagramme encapsulé à travers le tunnel.

Note : Le mode tunnel IPsec est différent de la mise en tunnel IP dans IP [RFC2003] de plusieurs façons :

- IPsec offre certains contrôles à un administrateur de sécurité pour gérer les canaux cachés (qui ne devraient normalement pas poser de problème pour la mise en tunnel) et s'assurer que le receveur examine les bonnes portions du paquet reçu par rapport à l'application du contrôle d'accès. Une mise en œuvre IPsec PEUT être configurable eu égard à la façon de traiter le champ DS externe pour les paquets transmis en mode tunnel. Pour le trafic sortant, un réglage de configuration pour le champ DS externe va fonctionner comme décrit dans les paragraphes suivants sur le traitement d'en-tête IPv4 et IPv6 pour les tunnels IPsec. Un autre réglage permettra au champ DS externe d'être transposé en une valeur fixe, qui PEUT être configurée SA par SA. (La valeur peut être en fait fixée pour tout le trafic sortant d'un appareil, mais la granularité SA par SA le permet aussi.) Cette option de configuration permet à un administrateur local de décider si le canal caché fourni en copiant ces bits vaut la peine de la copie.

- IPsec décrit comment traiter ECN ou DS et donne la capacité de contrôle et la propagation des changements dans ces champs entre domaines non protégés et protégés. En général, la propagation d'un domaine protégé à un domaine non protégé se fait par un canal caché et donc des commandes sont fournies pour gérer la bande passante de ce canal. La propagation des valeurs d'ECN dans l'autre direction est contrôlée de sorte que seuls les changements d'ECN légitimes (qui indiquent l'occurrence d'encombrements entre les points d'extrémité du tunnel) soient propagés. Par défaut, la propagation de DS d'un domaine non protégé à un domaine protégé n'est pas permise. Cependant, si l'envoyeur et le receveur ne partagent pas le même espace de code DS, et si le receveur n'a aucun moyen d'apprendre comment transposer entre les deux espaces, il peut alors être approprié de s'écarter de la situation par défaut. En particulier, on PEUT configurer dans une mise en œuvre IPsec comment traiter le champ DS externe pour le mode tunnel en réception de paquets. Elle peut être configurée pour éliminer la valeur DS externe (par défaut) OU pour remplacer le champ DS interne par le champ DS externe. Si l'option est offerte, le comportement élimination contre remplacement PEUT être configuré SA par SA. Cette option de configuration permet à un administrateur local de décider si les faiblesses créées par la copie de ces bits valent la peine de la copie. Voir la [RFC2983] pour des informations complémentaires sur le moment où chacun de ces comportements peut être utile, et aussi le besoin possible du conditionnement de trafic diffserv avant ou après le traitement IPsec (y compris la désencapsulation du tunnel).

- IPsec permet à la version IP de l'en-tête d'encapsulation d'être différente de celle de l'en-tête interne.

Les tableaux des paragraphes qui suivent montrent le traitement des différents champs d'en-tête/option ("construit" signifie que la valeur dans le champ externe est construite indépendamment de la valeur dans le champ interne).

5.1.2.1 IPv4 : Construction d'en-tête pour le mode tunnel

<-- Comment l'en-tête externe se rapporte à l'en-tête interne -->			
IPv4		En-tête externe à l'encapsuleur	En-tête interne au désencapsuleur
Champs d'en-tête :		----------	----------
	version	4 (1)	pas de changement
	longueur d'en-tête	construit	pas de changement
	Champ DS	copié de l'en-tête interne (5)	pas de changement
	Champ ECN	copié de l'en-tête interne	construit (6)
	longueur totale	construit	pas de changement
	ID	construit	pas de changement
	fanions (DF, MF)	construit, DF (4)	pas de changement
	décalage de fragment	construit	pas de changement
	TTL	construit (2)	décrémenté (2)
	protocole	AH, ESP	pas de changement
	somme de contrôle	construit	construit (2)(6)
	adresse de source	construit (3)	pas de changement
	adresse de destination	construit (3)	pas de changement
Options		jamais copié	pas de changement

Notes:

(1) La version IP dans l'en-tête d'encapsulation peut être différente de la valeur de l'en-tête interne.
(2) La TTL dans l'en-tête interne est décrémentée par l'encapsuleur avant la transmission et par le désencapsuleur si il transmet le paquet. (La somme de contrôle IPv4 change quand la TTL change.) Note : Décrémenter la valeur de TTL fait normalement partie de la transmission d'un paquet. Et donc, un paquet originaire du même nœud que l'encapsuleur n'a pas sa TTL décrémentée, car le nœud d'envoi est à l'origine du paquet plutôt qu'à sa transmission. Ceci s'applique aux mises en œuvre BITS et IPsec natives dans les hôtes et les routeurs. Cependant, le modèle de traitement IPsec inclut une capacité de transmission externe. Le traitement de la TTL peut être utilisé pour empêcher la mise en boucle de paquets, par exemple, du fait d'erreurs de configuration, dans le contexte de ce modèle de traitement.
(3) Les adresses locales et distantes 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. Note : Pour le trafic en diffusion groupée, l'adresse de destination, ou les adresses de source et de destination, peuvent être exigées pour le démultiplexage. Dans ce cas, il est important de s'assurer de la cohérence de la durée de vie de la SA en s'assurant que l'adresse de source qui apparaît dans l'en-tête du tunnel d'encapsulation est la même que celle qui a été négociée durant le processus d'établissement de la SA. Il y a une exception à cette règle générale, à savoir qu'une mise en œuvre IPsec mobile va mettre à jour son adresse de source lorsqu'elle se déplace.
(4) La configuration détermine si il faut copier à partir de l'en-tête interne (seulement IPv4), effacer, ou établir le DF.
(5) Si le paquet entre immédiatement dans un domaine pour lequel la valeur de DSCP dans l'en-tête externe n'est pas appropriée, cette valeur DOIT être transposée dans une valeur appropriée pour le domaine [RFC2474]. Voir la [RFC2475] pour des informations complémentaires.
(6) Si le champ ECN dans l'en-tête interne est réglé à ECT(0) ou ECT(1), où ECT est transport à capacité ECN (ECT, *ECN-Capable Transport*), et si le champ ECN dans l'en-tête externe est réglé à encombrement rencontré (CE, *Congestion Experienced*), le réglage du champ ECN dans l'en-tête interne est alors CE ; autrement, ne faire aucun changement au champ ECN dans l'en-tête interne. (La somme de contrôle IPv4 change lorsque l'ECN change.) Note : IPsec ne copie pas les options de l'en-tête interne dans l'en-tête externe, pas plus qu'il ne construit les options dans l'en-tête externe. Cependant, un code post-IPsec PEUT insérer/construire des options pour l'en-tête externe.

5.1.2.2 IPv6 : Construction d'en-tête pour le mode tunnel

<-- Comment l'en-tête externe se rapporte à l'en-tête interne -->		
IPv6	En-tête externe à l'encapsuleur	En-tête interne au désencapsuleur
Champs d'en-tête :	----------	----------
version	6 (1)	pas de changement
Champ DS	copié de l'en-tête interne (5)	pas de changement (9)
Champ ECN	copié de l'en-tête interne	construite (6)
étiquette de flux	copié ou configuré (8)	pas de changement
longueur de charge utile	construit	pas de changement
en-tête suivant	AH, ESP, en-tête d'acheminement	pas de changement
limite de bond	construit (2)	décrémenté (2)
adresse de source	construit (3)	pas de changement
adresse de destination	construit (3)	pas de changement
En-têtes d'extension	jamais copiés (7)	pas de changement

Notes :
(1) à (6) voir au paragraphe 5.1.2.1.
(7) IPsec ne copie pas les en-têtes d'extension du paquet interne dans les en-têtes externes, ni ne construit d'en-têtes d'extension dans l'en-tête externe. Cependant, un code post-IPsec PEUT insérer/construire des en-têtes d'extension pour l'en-tête externe.
(8) Voir [RFC3697]. Copier n'est acceptable que pour les systèmes d'extrémité, par pour les SG. Si un SG copie des étiquettes de flux de l'en-tête interne dans l'en-tête externe, il peut en résulter des collisions.
(9) Une mise en œuvre PEUT choisir de fournir la facilité de passer la valeur de DS de l'en-tête externe à l'en-tête interne, SA par SA, pour les paquets reçus en mode tunnel. La motivation de la fourniture d'une telle facilité est de s'accommoder de situations dans lesquelles l'espace de code DS chez le receveur est différent de celui de l'envoyeur et où le receveur n'a aucun moyen de savoir comment traduire à partir de l'espace de l'envoyeur. Il a un danger à copier cette valeur de l'en-tête externe à l'en-tête interne, car cela permet à un attaquant de modifier la valeur DSCP externe d'une façon qui peut affecter d'autre trafic chez le receveur. Et donc, le comportement par défaut pour les mises en œuvre IPsec est de NE PAS permettre un telle copie.

5.2 Traitement du trafic IP entrant (non protégé à protégé)

Le traitement entrant est quelque peu différent du traitement sortant, à cause de l'utilisation des SPI pour transposer le trafic protégé par en SA. L'antémémoire de SPD entrant (SPD-I) n'est appliquée qu'au trafic qui outrepasse ou est éliminé. Si un paquet arrivant apparaît être un fragment IPsec provenant d'une interface non protégée, le réassemblage est effectué avant

le traitement IPsec. L'intention de toute mise en antémémoire de SPD est qu'un paquet qui échoue à trouver une correspondance avec une entrée soit rapporté à la SPD correspondante. Chaque SPD DEVRAIT avoir une entrée nominale finale qui attrape tout ce qui n'est pas autrement en correspondance, et l'élimine. Cela garantit que le trafic non protégé par IPsec qui arrive et ne correspond à aucune entrée de SPD-I sera éliminé.

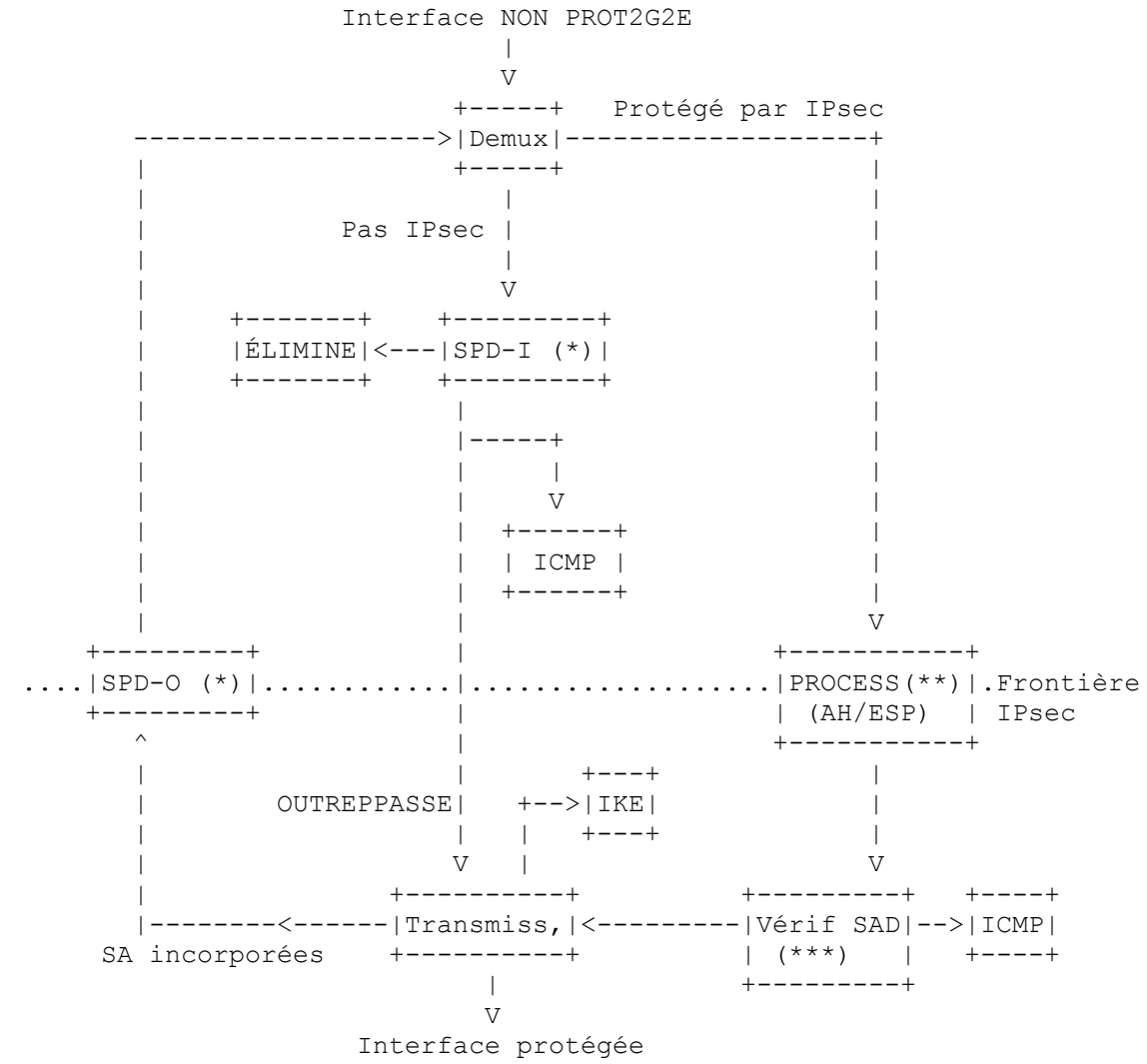


Figure 3. Modèle de traitement pour le trafic entrant

(*) Les antémémoires sont montrées ici. Si il y a un manque dans l'antémémoire, la SPD est sollicitée. Il n'est pas exigé qu'une mise en œuvre mette le paquet en mémoire tampon dans ce cas.

(**) Ce traitement inclut l'utilisation des SPI du paquet, etc., pour rechercher la SA dans la SAD, qui forment une antémémoire de la SPD pour les paquets entrants (excepté pour les cas notés au paragraphe 4.4.2 et à la Section 5). Voir l'étape 3a ci-dessous.

(***) Cette vérification de SAD se réfère à l'étape 4 ci-dessous.

Avant d'effectuer le traitement AH ou ESP, tous les fragments IP qui arrivent via l'interface non protégée sont réassemblés (par IP). Chaque datagramme IP entrant auquel le traitement IPsec sera appliqué est identifié par l'apparition des valeurs AH ou ESP dans le champ Prochain protocole IP (ou de AH ou ESP comme prochain protocole de couche dans le contexte IPv6).

IPsec DOIT effectuer les étapes suivantes :

1 Lorsqu'un paquet arrive, il peut être étiqueté avec l'identifiant de l'interface (physique ou virtuelle) via laquelle il est arrivé, si nécessaire, pour prendre en charge plusieurs antémémoires SPD et SPD-I associées. L'identifiant d'interface est transposé en un SPD-ID correspondant.)

2 Le paquet est examiné et démultiplexé en une des deux catégories suivantes :
   - S'il apparaît que le paquet est protégé par IPsec et qu'il est adressé à cet appareil, on fait un essai pour 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 SAD, par exemple, dans le cas de protocoles tels que SCTP.

- Le trafic non adressé à cet appareil, ou adressé à cet appareil et qui n'est pas AH ou ESP, est dirigé sur la recherche SPD-I. (Cela implique que le trafic IKE DOIT avoir une entrée BYPASS explicite dans la SPD.) Si plusieurs SPD sont employées, l'étiquette allouée au paquet dans l'étape 1 est utilisée pour choisir la SPD-I appropriée (et l'antémémoire) où chercher. La recherche de SPD-I détermine si l'action est DISCARD ou BYPASS.

3a Si le paquet est adressé à l'appareil IPsec et si AH ou ESP est le protocole spécifié, le paquet est examiné dans la SAD. Pour le trafic en envoi individuel, on utilise seulement le SPI (ou SPI plus le protocole). Pour le trafic en diffusion groupée, on utilise le SPI plus la destination ou SPI plus adresses de destination et de source, comme spécifié au paragraphe 4.1. Dans l'un et l'autre cas (envoi individuel ou diffusion groupée) si il n'y a pas de correspondance, éliminer le trafic. C'est un événement d'audit. L'entrée de journalisation d'audit pour cet événement DEVRAIT inclure la date/heure en cours, le SPI, la source et destination du paquet, le protocole IPsec, et toutes autres valeurs de sélecteur du paquet disponibles. Si le paquet est trouvé dans la SAD, le traiter en conséquence (étape 4).

3b Si le paquet n'est pas adressé à l'appareil ou est adressé à cet appareil et n'est pas AH ou ESP, rechercher l'en-tête du paquet dans l'antémémoire de SPD-I (appropriée). S'il y a une correspondance et si le paquet est à éliminer ou doit outrepasser, le faire. S'il n'y a pas de correspondance d'antémémoire, rechercher le paquet dans la SPD-I correspondante et créer une entrée d'antémémoire selon le cas. (Aucune SA n'est créée en réponse à la réception d'un paquet qui exige la protection IPsec ; seules les entrées d'antémémoire BYPASS ou DISCARD peuvent être créées de cette façon.) S'il n'y a pas de correspondance, éliminer le trafic. Ceci est un événement d'audit. L'entrée de journalisation d'audit pour cet événement DEVRAIT inclure la date/heure en cours, le SPI s'il est disponible, le protocole IPsec si disponible, la source et la destination du paquet, et toutes autres valeurs de sélecteur du paquet disponibles.

3c Le traitement de ces messages ICMP est supposé prendre place sur le côté non protégé de la frontière IPsec. Les messages ICMP non protégés sont examinés et la politique locale est appliquée pour déterminer d'accepter ou rejeter ces messages et, si ils sont acceptés, quelle action entreprendre. Par exemple, si un message ICMP inaccessible est reçu, la mise en œuvre doit décider d'agir sur lui, de le rejeter, ou d'agir sur lui avec des contraintes. (Voir Section 6.)

4 Appliquer le traitement AH ou ESP comme spécifié, en utilisant l'entrée de SAD choisie à l'étape 3a ci-dessus. Puis confronter le paquet aux sélecteurs entrants identifiés par l'entrée de SAD pour vérifier que le paquet reçu est approprié pour la SA via laquelle il a été reçu.

5 Si un système IPsec reçoit un paquet entrant sur une SA et si les champs d'en-tête du paquet ne sont pas cohérents avec les sélecteurs pour la SA, il DOIT éliminer le paquet. Ceci est un événement d'audit. L'entrée de journalisation d'audit pour cet événement DEVRAIT inclure la date/heure en cours, le SPI, le ou les protocoles IPsec, la source et destination du paquet, toutes autres valeurs de sélecteur du paquet disponibles, et les valeurs de sélecteur provenant de l'entrée de SAD pertinente. Le système DEVRAIT aussi être capable de générer et envoyer une notification INVALID_SELECTORS de IKE à l'envoyeur (homologue IPsec), indiquant que le paquet reçu a été éliminé à cause de son échec à passer les vérifications des sélecteurs.

Pour minimiser l'impact d'une attaque de déni de service, ou d'une mauvaise configuration d'un homologue, le système IPsec DEVRAIT inclure un contrôle de gestion pour permettre à un administrateur de configurer la mise en œuvre IPsec de façon à envoyer ou pas cette notification IKE, et si cette facilité est choisie, de limiter le débit de transmission de telles notifications.

Après que le trafic a outrepassé IPsec ou a été traité par lui, il est mis à disposition de la fonction de transmission. Cette fonction peut causer l'envoi du paquet (sortant) à travers la frontière IPsec pour un traitement IPsec interne supplémentaire, par exemple, à l'appui de SA incorporées. S'il en est ainsi, comme avec tout le trafic sortant qui doit outrepasser, le paquet DOIT être confronté à une entrée de SPD-O. Finalement, le paquet devrait être transmis à l'hôte de destination ou traité pour mise à disposition.

6 Traitement du trafic ICMP

La présente section décrit le traitement IPsec du trafic ICMP. Il y a deux catégories de trafic ICMP : les messages d'erreur (par exemple, type = destination inaccessible) et les messages qui ne sont pas d'erreur (par exemple, type = écho). La présente section s'applique exclusivement aux messages d'erreur. La disposition de messages ICMP qui ne sont pas d'erreur (qui ne sont pas adressés à la mise en œuvre IPsec elle-même) DOIT être explicitement prise en compte par l'utilisation d'entrées de SPD.

L'exposé de la présente section s'applique à ICMPv6 aussi bien qu'à ICMPv4. Aussi, un mécanisme DEVRAIT être fourni pour permettre à un administrateur de faire que les messages d'erreur ICMP (choisis, tous, ou aucun) soit enregistrés pour aider au diagnostic des problèmes.

6.1 Traitement des messages d'erreur ICMP dirigés sur une mise en œuvre IPsec

6.1.1 Messages d'erreur ICMP reçus sur le côté non protégé de la frontière

La Figure 3 du paragraphe 5.2 montre un module de traitement ICMP distinct sur le côté non protégé de la frontière IPsec, pour le traitement des messages ICMP (erreur ou autres) qui sont adressés à l'appareil IPsec et qui ne sont pas protégés via AH ou ESP. Un message ICMP de cette sorte n'est pas authentifié, et son traitement peut résulter en un déni de service ou une dégradation du service. Ceci suggère qu'en général, il serait souhaitable d'ignorer de tels messages. Cependant, de nombreux messages ICMP seront reçus par des hôtes ou passerelles de sécurité de la part de sources non authentifiées, par exemple, de routeurs de l'Internet public. Ignorer ces messages ICMP peut dégrader le service, par exemple, à cause du non traitement des messages de PMTU et de redirection. Et donc, il y a des raisons d'accepter et d'agir sur des messages ICMP non authentifiés.

Pour s'accommoder des deux extrémités du spectre, une mise en œuvre IPsec conforme DOIT permettre à un administrateur local de configurer une mise en œuvre IPsec pour qu'elle accepte ou rejette le trafic ICMP non authentifié. Cette commande DOIT être à la granularité du type ICMP et PEUT être à la granularité du type et code ICMP. De plus, une mise en œuvre DEVRAIT incorporer des mécanismes et paramètres pour traiter un tel trafic. Par exemple, il pourrait y avoir la capacité à établir une PMTU minimum pour le trafic (destination par destination) pour empêcher la réception d'un message ICMP non authentifié provenant d'un réglage de la PMTU à une taille triviale.

Si un message ICMP de PMTU passe les vérifications ci-dessus et si le système est configuré pour l'accepter, il y a alors deux possibilités. Si la mise en œuvre applique la fragmentation sur le côté texte chiffré de la frontière, les informations de PMTU acceptées sont passées au module de transmission (en dehors de la mise en œuvre IPsec) qui les utilise pour gérer la fragmentation de paquet sortant. Si la mise en œuvre est configurée pour effectuer la fragmentation du côté du texte en clair, les informations de PMTU sont alors passées au côté du texte en clair et traitées comme décrit au paragraphe 8.2.

6.1.2 Messages d'erreur ICMP reçus du côté protégé de la frontière

Ces messages ICMP ne sont pas authentifiés, mais ils viennent effectivement de sources situées sur le côté protégé de la frontière IPsec. Et donc, ces messages sont généralement considérés comme étant plus "dignes de confiance" que leurs contreparties qui arrivent de sources sur le côté non protégé de la frontière. Le principal souci de sécurité est ici qu'un hôte ou routeur compromis pourrait émettre des messages d'erreur ICMP erronés qui pourraient dégrader le service pour d'autres appareils "derrière" la passerelle de sécurité, ou qui pourraient même résulter en violations de la confidentialité. Par exemple, si un message ICMP redirect frauduleux était absorbé par une passerelle de sécurité, il pourrait causer la modification du tableau de transmission du côté protégé de la frontière de façon à livrer le trafic à une destination inappropriée "derrière" la passerelle. Et donc, les développeurs DOIVENT fournir des commandes pour permettre aux administrateurs locaux de restreindre le traitement des messages d'erreur ICMP reçus du côté protégé de la frontière, et dirigés sur la mise en œuvre IPsec. Ces commandes sont du même type que celui employé sur le côté non protégé, décrit ci-dessus au paragraphe 6.1.1.

6.2 Traitement des messages d'erreur ICMP protégés en transit

Lorsque un message d'erreur ICMP est transmis via une SA à un appareil "derrière" une mise en œuvre IPsec, la charge utile et l'en-tête du message ICMP exigent tous deux une vérification du point de vue du contrôle d'accès. Si un de ces messages est transmis à un hôte derrière une passerelle de sécurité, la mise en œuvre d'hôte IP qui reçoit va prendre des décisions sur la base de la charge utile, c'est-à-dire, l'en-tête de paquet qui est supposé avoir déclenché la réponse d'erreur. Et donc, on DOIT pouvoir configurer une mise en œuvre IPsec pour vérifier que ces informations d'en-tête de charge utile sont cohérentes avec la SA via laquelle elles arrivent. (Cela signifie que l'en-tête de charge utile, avec les champs adresse et accès de source et destination inversés, correspond aux sélecteurs de trafic pour la SA.) Si cette sorte de vérification n'est pas effectuée, alors, par exemple, quiconque a avec le système IPsec récepteur (A) une SA active pourrait envoyer un message ICMP Destination inaccessible se référant à tout hôte/réseau avec lequel A est en train de communiquer, et donc effectuer une attaque de déni de service extrêmement efficace à l'égard des communications avec les autres homologues de A. Le traitement IPsec normal de réception du trafic n'est pas suffisant pour protéger contre de telles attaques. Cependant, tous les contextes n'exigent pas de telles vérifications, aussi il est nécessaire de permettre à un administrateur local de configurer une mise en œuvre pour NE PAS effectuer de telles vérifications.

Pour s'accommoder des deux politiques, la convention suivante est adoptée. Si un administrateur veut permettre que des messages d'erreur ICMP soient portés par une SA sans inspection de la charge utile, il configure alors une entrée de SPD qui permet explicitement le portage d'un tel trafic. Si un administrateur veut qu'IPsec vérifie la cohérence de la charge utile des messages d'erreur ICMP, il ne créera aucune entrée de SPD qui prenne le portage d'un tel trafic sur la base de l'en-tête de paquet ICMP. Cette convention motive la description de traitement qui suit.

Les envoyeurs et receveurs IPsec DOIVENT prendre en charge les traitements suivants des messages d'erreur ICMP qui sont envoyés et reçus via des SA.

S'il existe une SA qui s'accommode des messages d'erreur ICMP sortants, le message est alors transposé dans la SA et seuls les en-têtes IP et ICMP sont vérifiés à réception, tout comme ce serait le cas pour un autre trafic. S'il n'existe pas de SA qui corresponde aux sélecteurs de trafic associés à un message d'erreur ICMP, une recherche est alors faite dans la SPD pour déterminer si une telle SA peut être créée. S'il en est ainsi, la SA est créée et le message d'erreur ICMP est transmis via cette SA. À réception, ce message est soumis aux vérifications habituelles de sélecteur de trafic chez le receveur. Ce traitement est exactement ce qui se passe pour le trafic en général, et donc ne représente aucune particularité pour le traitement des messages d'erreur ICMP.

S'il n'existe pas de SA qui puisse porter le message ICMP sortant en question, et si aucune entrée de SPD ne permet le portage de ce message d'erreur ICMP sortant, une mise en œuvre IPsec DOIT alors transposer ce message à la SA qui doit porter le trafic de retour associé au paquet qui a déclenché le message d'erreur ICMP. Ceci exige qu'une mise en œuvre IPsec détecte les messages d'erreur ICMP sortant qui ne se transposent dans aucune SA ou entrée de SPD existante, et les traite de façon particulière à l'égard de la création et de la recherche de SA. La mise en œuvre extrait l'en-tête pour le paquet qui a déclenché l'erreur (à partir de la charge utile de message ICMP), inverse les champs adresse IP de source et de destination, extrait le champ protocole, et inverse les champs d'accès (s'ils sont accessibles). Elle utilise ensuite ces informations extraites pour localiser une SA active sortante appropriée, et transmet le message d'erreur via cette SA. S'il n'existe pas une telle SA, aucune n'est créée, et c'est un événement d'audit.

Si une mise en œuvre IPsec reçoit un message d'erreur ICMP entrant sur une SA, et si les en-têtes IP et ICMP de ce message ne correspondent pas aux sélecteurs de trafic pour la SA, le receveur DOIT traiter le message reçu d'une façon particulière. Précisément, le receveur doit extraire l'en-tête du paquet déclencheur de la charge utile ICMP, et inverser les champs comme décrit ci-dessus pour déterminer si le paquet est cohérent avec les sélecteurs pour la SA via laquelle le message d'erreur ICMP a été reçu. Si le paquet échoue à cette vérification, la mise en œuvre IPsec NE DOIT PAS transmettre le message ICMP à la destination. Ceci est un événement d'audit.

7 Traitement des fragments (sur le côté protégé de la frontière IPsec)

Les précédentes sections du présent document décrivent les mécanismes pour (a) fragmenter un paquet sortant après l'application du traitement IPsec et le réassembler chez le receveur avant le traitement IPsec et (b) traiter les fragments entrants reçus du côté non protégé de la frontière IPsec. La présente section décrit comment une mise en œuvre devrait assurer le traitement des fragments de texte en clair sortant sur le côté protégé de la frontière IPsec. (Voir l'Appendice D, "Raisons du traitement des fragments".) En particulier, elle s'intéresse :

- o à la transposition d'un fragment sortant non initial dans la bonne SA (ou à trouver la bonne entrée de SPD)
- o à vérifier qu'un fragment non initial reçu est autorisé pour la SA via laquelle il a été reçu
- o à transposer les fragments non initiaux entrants et sortant sur la bonne entrée de SPD-O/SPD-I ou l'entrée d'antémémoire pertinente, pour le trafic BYPASS/DISCARD

Note : Au paragraphe 4.1, les SA en mode transport ont été définies comme ne portant pas de fragments (IPv4 ou IPv6). Noter aussi qu'au paragraphe 4.4.1, deux valeurs particulières, ANY et OPAQUE, ont été définies pour les sélecteurs et que ANY inclut OPAQUE. Le terme "non trivial" est utilisé pour signifier que le sélecteur a une valeur autre que OPAQUE ou ANY.

Note : Le terme "fragment non initial" est utilisé ici pour indiquer un fragment qui ne contient pas toutes les valeurs de sélecteur qui peuvent être nécessaires pour le contrôle d'accès. Comme observé au paragraphe 4.4.1, selon le protocole de couche suivante, en plus des accès, le type/code ou le type en-tête de mobilité de message ICMP pourrait manquer dans les fragments non initiaux. Aussi, pour IPv6, même le premier fragment pourrait NE PAS contenir le protocole de couche suivante ou les accès (ou le type/code ou le type en-tête de mobilité de message ICMP) selon la sorte et le nombre d'en-têtes d'extension présents. Si un fragment non initial contient l'accès (ou le type et code ICMP ou le type d'en-tête de mobilité) mais pas le protocole de couche suivante, alors, sauf s'il y a une entrée SPD pour les adresses locales/distantes avec ANY pour le protocole de couche suivante et l'accès (ou le type et code ICMP ou le type d'en-tête de mobilité) le fragment ne contiendrait pas toutes les informations de sélecteur nécessaires pour le contrôle d'accès.

Pour régler les problèmes ci-dessus, trois approches ont été définies :

- o Les SA en mode tunnel qui portent des fragments initiaux et non initiaux (voir le paragraphe 7.1.)
- o Les SA en mode tunnel séparé pour les fragments non initiaux (voir le paragraphe 7.2.)
- o La vérification dynamique de fragment (voir le paragraphe 7.3.)

7.1 SA en mode tunnel qui portent des fragments initiaux et non initiaux

Toutes les mises en œuvre DOIVENT prendre en charge les SA en mode tunnel qui sont configurées pour passer le trafic sans égard aux valeurs du champ accès (ou type/code ICMP ou type d'en-tête de mobilité). Si la SA va porter du trafic pour des protocoles spécifiés, le sélecteur mis pour la SA DOIT spécifier les champs accès (ou type/code ICMP ou type d'en-tête de mobilité) à ANY. Une SA définie de cette façon va porter tous les trafics y compris les fragments initiaux et non initiaux pour les adresses locales/distantes indiquées et le ou les protocoles de couche suivante spécifiés. Si la SA porte du trafic sans égard à une valeur de protocole spécifique (c'est-à-dire, ANY est spécifié comme valeur de sélecteur de protocole (couche suivante)) les valeurs du champ accès sont alors indéfinies et DOIVENT être réglées aussi à ANY. (Comme noté au paragraphe 4.4.1, ANY inclut OPAQUE ainsi que toutes les valeurs spécifiques.)

7.2 SA en mode tunnel séparé pour les fragments non initiaux

Une mise en œuvre PEUT prendre en charge les SA en mode tunnel qui vont ne porter que des fragments non initiaux, séparés des paquets non fragmentés et des fragments initiaux. La valeur OPAQUE sera utilisée pour spécifier les sélecteurs du champ accès (ou type/code ICMP ou type d'en-tête de mobilité) pour qu'une SA porte de tels fragments. Les receveurs DOIVENT effectuer une vérification de décalage minimum sur les fragments IPv4 (non initiaux) pour se protéger contre les attaques de chevauchement de fragment lorsque des SA de ce type sont employées. Comme de telles vérifications ne peuvent être effectuées sur des fragments IPv6 non initiaux, les usagers et administrateurs sont avisés que le portage de tels fragments peut être dangereux, et les développeurs peuvent choisir de NE PAS accepter de telles SA pour le trafic IPv6. Aussi, une SA de cette sorte va porter tous les fragments non initiaux qui correspondent à une paire spécifique d'adresses locale/distante et valeur de protocole, c'est-à-dire, les fragments portés sur cette SA appartiennent aux paquets qui, s'ils n'étaient pas fragmentés, auraient pu aller sur des SA séparées de sécurité différente. Donc, les usagers et administrateurs sont avisés de protéger un tel trafic en utilisant ESP (avec intégrité) et les algorithmes d'intégrité et de chiffrement "les plus forts" en usage entre les deux homologues. (La détermination des algorithmes "les plus forts" exige d'imposer un classement des algorithmes disponibles, détermination locale à la discrétion de l'initiateur de la SA.)

Des valeurs de sélecteur d'accès (ou type/code ICMP ou type d'en-tête de mobilité) spécifiques seront utilisées pour définir des SA pour porter des fragments initiaux et des paquets non fragmentés. Cette approche peut être utilisée si un usager ou administrateur veut créer une ou plusieurs SA en mode tunnel entre les mêmes adresses locale/distante qui se différencient sur la base des champs d'accès (ou type/code ICMP ou type d'en-tête de mobilité). Ces SA DOIVENT avoir des valeurs de sélecteur de protocole non triviales, autrement l'approche n° 1 ci-dessus DOIT être utilisée.

Note : En général, pour l'approche décrite dans ce paragraphe, on a seulement besoin d'une SA entre deux mises en œuvre pour porter tous les fragments non initiaux. Cependant, si on choisit d'avoir plusieurs SA entre les deux mises en œuvre pour la différentiation de qualité de service, on peut aussi vouloir que plusieurs SA portent les fragments sans accès, une pour chaque classe de QS prise en charge. Comme la prise en charge de la QS via des SA distinctes est aussi une affaire locale, que le présent document ne rend pas obligatoire, le choix d'avoir plusieurs SA pour porter les fragments non initiaux devrait aussi être local.

7.3 Vérification dynamique de fragment

Une mise en œuvre PEUT prendre en charge certaines formes de vérification dynamique de fragment pour une SA en mode tunnel avec des valeurs de champ d'accès (ou type/code ICMP ou type d'en-tête de mobilité) non triviales (ni ANY ni OPAQUE). Les mises en œuvre qui vont transmettre des fragments non initiaux sur une SA en mode tunnel qui fait usage de sélecteurs d'accès (ou ICMP type/code ou MH type) non triviaux DOIT le notifier à un homologue via la charge utile IKE NOTIFY NON_FIRST_FRAGMENTS_ALSO.

L'homologue DOIT rejeter cette proposition si il ne va pas accepter de fragments non initiaux dans ce contexte. Si une mise en œuvre ne réussit pas à négocier la transmission de fragments non initiaux pour une telle SA, elle NE DOIT PAS envoyer de tels fragments sur la SA. La présente norme ne spécifié pas combien d'homologues vont traiter de tels fragments, par exemple, via le réassemblage ou d'autres moyens, chez l'envoyeur ou chez le receveur. Cependant, un receveur DOIT éliminer les fragments non initiaux qui arrivent sur une SA avec des valeurs de sélecteur d'accès (ou type/code ICMP ou type d'en-tête de mobilité) non triviaux à moins que ce dispositif ait été négocié. Aussi, le receveur DOIT éliminer les fragments non initiaux qui ne se conforment pas à la politique de sécurité appliquée à la globalité du paquet. Éliminer de tels paquets est un événement d'audit. Noter que dans les configurations de réseau où les fragments d'un paquet peuvent être envoyés ou reçus via différentes passerelles de sécurité ou mises en œuvre BITW, les stratégies dynamiques pour suivre les fragments peuvent échouer.

7.4 Trafic BYPASS/DISCARD

Toutes les mises en œuvre DOIVENT prendre en charge l'élimination des fragments en utilisant les mécanismes normaux

de classification de paquets de SPD. Toutes les mises en œuvre DOIVENT prendre en charge la vérification dynamique de fragment pour s'accommoder du trafic BYPASS pour lequel une gamme d'accès non triviale est spécifiée. Le souci est que l'outrepassement d'un fragment non initial de texte en clair qui arrive à une mise en œuvre IPsec pourrait mettre en danger la sécurité offerte à un trafic protégé par IPsec qui serait dirigé vers la même destination. Par exemple, considérons une mise en œuvre IPsec configurée avec une entrée SPD qui appelle à la protection IPsec du trafic entre une paire spécifique source/adresse de destination, et pour un protocole et port de destination spécifique, par exemple, trafic TCP sur l'accès 23 (Telnet). Supposons que la mise en œuvre permette aussi l'outrepassement du trafic provenant de la même paire source/adresse de destination et protocole, mais pour un accès de destination différent, par exemple, l'accès 119 (NNTP). Un attaquant pourrait envoyer un fragment non initial (avec une adresse de source falsifiée) qui, si elle outrepasse, pourrait se chevaucher avec le trafic protégé par IPsec et provenant de la même source, et donc violer l'intégrité du trafic protégé par IPsec. Exiger une vérification dynamique de fragment pour les entrées qui outrepassent avec des gammes d'accès non triviales empêche les attaques de cette sorte. Comme noté plus haut, dans les configurations de réseau où les fragments d'un paquet peuvent être envoyées ou reçues via différentes passerelles de sécurité ou mises en œuvre BITW, des stratégies dynamiques pour suivre les fragments peuvent échouer.

8 Traitement des MTU/DF de chemin

L'application de AH ou ESP à un paquet sortant accroît la taille d'un paquet et donc peut être cause qu'un paquet excède la PMTU pour la SA via laquelle le paquet va voyager. Une mise en œuvre IPsec peut aussi recevoir un message ICMP de PMTU non protégée et, si elle choisit d'agir sur le message, le résultat va affecter le traitement du trafic sortant. La présente section décrit le traitement requis d'une mise en œuvre IPsec pour traiter ces deux problèmes de PMTU.

8.1 Bit DF

Toutes les mises en œuvre IPsec DOIVENT prendre en charge l'option de copier le bit DF d'un paquet sortant dans l'en-tête de mode tunnel qu'elle émet, quand le trafic est porté via une SA en mode tunnel. Cela signifie qu'il DOIT être possible de configurer le traitement du bit DF de la mise en œuvre (établir, supprimer, copier de l'en-tête interne) pour chaque SA. Ceci s'applique aux SA où les deux en-têtes interne et externe sont IPv4.

8.2 Découverte de chemin de MTU (PMTU)

La présente section discute du traitement IPsec pour les messages de découverte de MTU de chemin non protégés. La PMTU ICMP est utilisée ici pour se référer à un message ICMP pour :
IPv4 ([RFC0792]) :
- Type = 3 (Destination inaccessible)
- Code = 4 (Fragmentation nécessaire et DF établi)
- MTU de prochain bond dans les 16 bits de faible poids du second mot de l'en-tête ICMP (étiqueté "unused" dans la RFC 792), avec les 16 bits de plus fort poids mis à zéro)

IPv6 ([RFC2463]) :
- Type = 2 (Paquet trop gros)
- Code = 0 (Fragmentation nécessaire)
- MTU de prochain bond dans le champ MTU de 32 bits du message ICMPv6

8.2.1 Propagation de PMTU

Lorsqu'une mise en œuvre IPsec reçoit un message de PMTU non authentifié, et qu'elle est configurée pour traiter (par opposition à ignorer) de tels messages, elle transpose le message dans la SA à laquelle il correspond. Cette transposition est effectuée en extrayant l'en-tête d'information de la charge utile du message de PMTU et en appliquant la procédure décrite au paragraphe 5.2. La PMTU déterminée par ce message est utilisée pour mettre à jour le champ PMTU de la SAD, en tenant compte de la taille de l'en-tête AH ou ESP qui sera appliqué, de toutes données de crypto synchronisation, et de la redondance imposée par un en-tête IP supplémentaire, dans le cas d'une SA en mode tunnel.

Dans une mise en œuvre d'hôte native, il est possible de maintenir les données de PMTU à la même granularité que pour une communication non protégée, de sorte qu'il n'y ait pas de perte de fonctionnalité. La signalisation des informations de PMTU est interne à l'hôte. Pour toutes les autres mises en œuvre d'options IPsec, les données de PMTU doivent être propagées via une PMTU ICMP synthétisée. Dans ces cas, la mise en œuvre IPsec DEVRAIT attendre que le trafic sortant soit transposé dans l'entrée de SAD. Lorsqu'un tel trafic arrive, si le trafic devait excéder la valeur de PMTU mise à jour, le trafic DOIT être traité comme suit :

Cas 1 : Le paquet original (en clair) est IPv4 et a le bit DF mis. La mise en œuvre DEVRAIT éliminer le paquet et envoyer un message ICMP de PMTU.

Cas 2 : Le paquet original (en clair) est IPv4 et le bit DF ôté. La mise en œuvre DEVRAIT fragmenter (avant ou après le chiffrement selon sa configuration) puis transmettre les fragments. Elle NE DEVRAIT PAS envoyer un message ICMP de PMTU.

Cas 3 : Le paquet original (en clair) paquet est IPv6. La mise en œuvre DEVRAIT éliminer le paquet et envoyer un message ICMP de PMTU.

8.2.2 Péremption de PMTU

Dans toutes les mises en œuvre IPsec, la PMTU associée à une SA DOIT être "vieillie" et un mécanisme est nécessaire pour mettre à jour la PMTU à temps, en particulier pour découvrir si la PMTU est plus petite que ce qui est exigé par les conditions existantes dans le réseau. Une PMTU donnée doit rester en place assez longtemps pour qu'un paquet aille de la source de la SA à l'homologue, et propage un message d'erreur ICMP si la PMTU en cours est trop grosse.

Les mises en œuvre DEVRAIENT utiliser l'approche décrite dans le document Découverte de la MTU de chemin ([RFC1191], paragraphe 6.3), qui suggère un réglage périodique de la PMTU à la MTU de liaison de données du premier bond, puis de laisser le processus normal de découverte de PMTU mettre à jour la PMTU en tant que de besoin. La période DEVRAIT être configurable.

9 Audit

Les mises en œuvre IPsec ne sont pas obligées de prendre en charge l'audit. Pour sa plus grande part, la granularité de l'audit est une affaire locale. Cependant, plusieurs événements d'audit sont identifiés dans le présent document, et pour chacun de ces événements un ensemble minimum d'informations qui DEVRAIENT être incluses dans une journalisation d'audit est défini. Des informations supplémentaires PEUVENT aussi être incluses dans la journalisation d'audit pour chacun de ces événements, et des événements supplémentaires non explicitement mentionnés dans la présente spécification, PEUVENT aussi résulter en des entrées de journalisation d'audit. Il n'y a pas d'exigence que le receveur transmette de message à l'émetteur supposé en réponse à la détection d'un événement d'audit, à cause du potentiel de déni de service induit via une telle action.

10 Exigences de conformité

Toutes les mises en œuvre IPsec IPv4 DOIVENT se conformer à toutes les exigences du présent document. Toutes les mises en œuvre IPv6 DOIVENT se conformer à toutes les exigences du présent document.

11 Considérations sur la sécurité

L'objet du présent document est la sécurité ; et donc les considérations de sécurité imprègnent cette spécification.

IPsec impose des contraintes strictes à l'outrepassement des données d'en-tête IP dans les deux directions, à travers la frontière IPsec, en particulier lorsque les SA en mode tunnel sont employées. Certaines contraintes sont absolues, alors que d'autres sont soumises à des contrôles administratifs locaux, souvent SA par SA. Pour le trafic sortant, ces contraintes sont conçues pour limiter la bande passante de canal caché. Pour le trafic entrant, les contraintes sont conçues pour empêcher un adversaire qui aurait la capacité d'altérer un flux de données (sur le côté non protégé de la frontière IPsec) d'affecter de façon hostile les autres flux de données (sur le côté protégé de la frontière). L'exposé de la Section 5 sur le traitement des valeurs DSCP pour les SA en mode tunnel illustre ce souci.

Si une mise en œuvre IPsec est configurée pour passer des messages d'erreur ICMP sur des SA sur la base des valeurs d'en-tête ICMP, sans vérifier les informations d'en-tête provenant de la charge utile du message ICMP, de sérieuses faiblesses peuvent apparaître. Considérons un scénario dans lequel plusieurs sites (A, B, et C) sont connecté à un autre via des tunnels protégés par ESP : A-B, A-C, et B-C. Supposons aussi que les sélecteurs de trafic pour chaque tunnel spécifient ANY pour les champs de protocole et d'accès et pour les gammes d'adresse IP de destination/source qui mettent en application la gamme d'adresse pour les systèmes derrière les passerelles de sécurité servant chaque site. Ceci permettrait à un hôte au site B d'envoyer un message ICMP Destination inaccessible à tout hôte du site A, qui déclarerait que tous les hôtes sur le réseau au site C sont inaccessibles. C'est une attaque de déni de service très efficace qui pourrait avoir été empêchée si les

messages d'erreur ICMP avaient été soumis aux vérifications fournies par IPsec, si la SPD est convenablement configurée, comme décrit au paragraphe 6.2.

12 Considérations relatives à l'IANA

L'IANA a alloué la valeur (3) au registre des modules asn1 et a alloué l'identifiant d'objet 1.3.6.1.5.8.3.1 au module SPD. Voir à l'Appendice C, "ASN.1 pour une entrée de SPD".

13 Différences avec la RFC 2401

Le présent document d'architecture diffère substantiellement de la RFC 2401 dans les détails et dans son organisation, mais les notions fondamentales restent inchangées.

- Le modèle de traitement a été révisé pour inclure de nouveaux scénarios IPsec, améliorer les performances, et simplifier la mise en œuvre. Ceci entraîne une séparation entre transmission (acheminement) et choix de la SPD, plusieurs changements de SPD, et l'ajout d'une antémémoire de SPD sortante et d'une antémémoire de SPD entrante pour le trafic qui outrepasse ou est éliminé. Il y a aussi une nouvelle base de données, la base de données d'autorisation d'homologue (PAD). Elle fait le lien entre un protocole de gestion de SA (comme IKE) et la SPD.

- Il n'y a plus d'exigence de prendre en charge les SA incorporées ou "faisceaux de SA". À la place, cette fonctionnalité peut être obtenue par la SPD et la configuration du tableau de transmission. Un exemple de configuration a été ajouté à l'Appendice E.

- Les entrées de SPD ont été redéfinies pour donner plus de souplesse. Chaque entrée de SPD consiste maintenant en 1 à N ensembles de sélecteurs, où chaque ensemble de sélecteurs contient un protocole et une "liste de gammes" peut maintenant être spécifiée pour l'adresse IP locale, l'adresse IP distante, et tous les champs (s'il en est) qui sont associés au protocole de couche suivante (accès local, accès distant, type et code de message ICMP, et type d'en-tête de mobilité). Une valeur individuelle pour un sélecteur est représentée via une gamme triviale et ANY est représenté via une gamme qui s'étend sur toutes les valeurs pour le sélecteur. Un exemple de description en ASN.1 figure à l'Appendice C.

- TOS (IPv4) et Classe de trafic (IPv6) ont été remplacés par DSCP et ECN. La section tunnel a été mise à jour pour expliquer comment traiter les bits DSCP et ECN.

- Pour les SA en mode tunnel, une mise en œuvre SG, BITS, ou BITW est maintenant autorisée à fragmenter les paquets avant d'appliquer IPsec. Ceci ne vaut que pour IPv4. Pour les paquets IPv6, seule l'origine a le droit de les fragmenter.

- Lorsque la sécurité est souhaitée entre deux systèmes intermédiaires le long d'un chemin ou entre un système intermédiaire et un système terminal, le mode transport peut maintenant être utilisé entre passerelles de sécurité et entre une passerelle de sécurité et un hôte.

- Le présent document précise que pour tout trafic qui traverse la frontière IPsec, y compris le trafic de gestion IPsec, la SPD ou les antémémoires associées doivent être consultées.

- Le présent document définit comment traiter la situation d'une passerelle de sécurité avec plusieurs abonnés qui exigent des contextes IPsec séparés.

- Ajout d'une définition des SPI réservés.

- Ajout d'un texte expliquant pourquoi TOUS les paquets IP doivent être vérifiés -- IPsec inclut une fonctionnalité minimale de pare-feu pour effectuer le contrôle d'accès à la couche IP.

- La section tunnel a été mise à jour pour préciser comment traiter le champ options IP et les en-têtes d'extension IPv6 lors de la construction de l'en-tête externe.

- Mise à jour de la transposition de SA pour le trafic entrant pour la cohérence avec les changements faits dans AH et ESP pour la prise en charge des SA en envoi individuel et en diffusion groupée.

- Des conseils d'utilisation ont été ajoutés sur la façon de traiter le canal caché créé en mode tunnel en copiant la valeur de DSCP dans l'en-tête externe.

- La prise en charge de AH à la fois en IPv4 et en IPv6 n'est plus exigée.
- Le traitement de la PMTU a été mis à jour. L'appendice sur PMTU/DF/Fragmentation a été supprimé.
- Trois approches ont été ajoutées pour le traitement des fragments en clair sur le côté protégé de la frontière IPsec. L'Appendice D expose les raisons qui les sous-tendent.
- Ajout d'un texte révisé qui décrit comment déduire les valeurs de sélecteur pour les SA (à partir de l'entrée de SPD ou à partir du paquet, etc.)
- Ajout d'un nouveau tableau pour décrire les relations entre valeurs de sélecteur dans une entrée de SPD, le fanion PFP, et les valeurs de sélecteur résultantes dans l'entrée de SAD correspondante.
- Ajout de l'Appendice B pour décrire la décorrélation.
- Ajout du texte qui décrit comment traiter un paquet sortant qui doit être éliminé.
- Ajout du texte qui décrit comment traiter un paquet entrant DISCARDED, c'est-à-dire, un paquet qui ne correspond pas à la SA sur laquelle il est arrivé.
- L'en-tête de mobilité IPv6 a été ajouté comme protocole de couche suivante possible. Le type de message En-tête de mobilité IPv6 a été ajouté comme sélecteur.
- Le type et code de message ICMP ont été ajoutés comme sélecteurs.
- Le sélecteur "niveau de sensibilité des données" a été retiré pour simplifier les choses.
- Le texte décrivant le traitement des messages d'erreur ICMP a été mis à jour. L'appendice sur la "Catégorisation des messages ICMP" a été supprimé.
- Le texte sur le nom du sélecteru a été mis à jour et précisé.
- Le "protocole de couche suivante" a été mieux expliqué et une liste par défaut de protocoles à sauter lors de la recherche du protocole de couche suivante a été ajoutée.
- Le texte a été amendé pour dire que le présent document suppose l'utilisation de IKEv2 ou d'un protocole de gestion de SA ayant des dispositions comparables.
- Un texte a été ajouté pour préciser l'algorithme de transposition des datagrammes IPsec entrants en SA en présence de SA de diffusion groupée.
- L'appendice "Exemple de code de fenêtre d'espace de séquence" a été supprimé.
- En ce qui concerne les adresses et accès IP, les termes "local" et "distant" sont utilisés pour les règles de politique (source et destination de remplacement). "Local" se réfère à l'entité qui est protégée par une mise en œuvre IPsec, c'est-à-dire, l'adresse/accès de "source" du paquet sortant ou l'adresse/accès de "destination" des paquets entrants. "Distant" se réfère à un ou des entités homologues. Les termes "source" et "destination" sont encore utilisés pour les champs d'en-tête de paquet.

14 Remerciements

Les auteurs tiennent à remercier de leurs contributions Ran Atkinson, qui a joué un rôle essentiel dans les activités initiales d'IPsec, et qui est l'auteur de la première série des normes IPsec : les RFC 1825-1827; et Charlie Lynn, qui a fait des contributions significatives à la seconde série des normes IPsec (les RFC 2401, 2402, et 2406) et aux versions actuelles, en particulier sur les questions concernant IPv6. Les auteurs tiennent aussi à remercier les membres des groupes de travail IPsec et MSEC qui ont contribué au développement de cette spécification de protocole.

Appendice A Glossaire

La présente section donne les définitions de plusieurs termes clés qui sont employés dans le présent document. D'autres documents donnent des définitions supplémentaires et des informations de base pertinentes pour cette technologie, par exemple, [RFC2828], [VK83], et [RFC1704]. Ce glossaire comporte les termes génériques des services de sécurité et mécanismes de sécurité, plus des termes spécifiques de IPsec.

Contrôle d'accès *(Access Control)*
Service de sécurité qui empêche l'utilisation non autorisée d'une ressource, y compris la prévention de l'utilisation d'une ressource d'une façon non autorisée. Dans le contexte IPsec, la ressource à laquelle l'accès est contrôlé est souvent :
- o pour un hôte, des cycles ou données de calcul
- o pour une passerelle de sécurité, un réseau derrière la passerelle ou de la bande passante sur le réseau.

Anti répétition *(Anti-replay)*
Voir à "Intégrité" ci-dessous.

Authentification
Utilisé de façon informelle pour se référer à la combinaison de deux services de sécurité nominalement distincts, l'authentification de l'origine des données et l'intégrité de bout en bout. Voir ci-dessous les définitions de chacun de ces services.

Disponibilité *(Availability)*
Vue comme un service de sécurité, elle vise les problèmes de sécurité engendrés par des attaques contre les réseaux qui empêchent ou dégradent le service. Par exemple, dans le contexte IPsec, l'utilisation de mécanismes anti-répétition dans AH et ESP soutient la disponibilité.

Confidentialité
C'est le service de sécurité qui protège les données contre la divulgation non autorisée. Le principal souci de confidentialité dans la plupart des instances est la divulgation non autorisée de données de niveau application, mais la divulgation des caractéristiques externes d'une communication peut aussi poser problème dans certaines circonstances. La confidentialité des flux de trafic est le service qui répond à ce dernier souci en dissimulant les adresses de source et de destination, la longueur du message, ou la fréquence de communication. Dans le contexte IPsec, l'utilisation de ESP en mode tunnel, particulièrement à une passerelle de sécurité, peut fournir un certain niveau de confidentialité du flux de trafic. (Voir aussi à "Analyse du trafic" ci-dessous.)

Authentification des données d'origine *(Data Origin Authentication)*
Service de sécurité qui vérifie l'identité de la source alléguée des données. Ce service est normalement couplé au service d'intégrité de bout en bout.

Chiffrement *(Encryption)*
Mécanisme de sécurité utilisé pour transformer les données d'une forme intelligible (en clair) en une forme inintelligible (texte chiffré) pour fournir la confidentialité. Le processus de transformation inverse est appelé "déchiffrement". Le terme "chiffrement" est souvent utilisé pour une référence générique aux deux processus.

Intégrité
Service de sécurité qui garantit que les modifications aux données sont détectables. L'intégrité peut correspondre de diverses façons aux exigences d'application. IPsec prend en charge deux formes d'intégrité : de bout en bout et une forme d'intégrité de séquence partielle. L'intégrité de bout en bout est un service qui détecte les modifications d'un datagramme IP individuel, sans égard à l'ordre du datagramme dans un flux de trafic. La forme d'intégrité de séquence partielle offerte dans IPsec se réfère à une intégrité anti répétition, et elle détecte l'arrivée du datagrammes IP dupliqués (au sein d'une fenêtre restreinte). Ceci diffère de l'intégrité orientée connexion, qui impose des exigences de séquencement plus strictes au trafic, par exemple, d'être capable de détecter des messages perdus ou réordonnés. Bien que les services d'authentification et d'intégrité soient souvent cités séparément, en pratique, ils sont intimement connectés et presque toujours offerts en tandem.

Protégé et non protégé
"Protégé" se réfère aux systèmes ou interfaces qui sont à l'intérieur de la frontière de protection IPsec, et "non protégé" se réfère aux systèmes ou interfaces qui sont en dehors de la frontière de protection IPsec. IPsec fournit une frontière à travers laquelle passe le trafic. Il y a une asymétrie dans cette barrière, qui se reflète dans le modèle de traitement. Les données sortantes, si elles ne sont pas éliminées ou si elle outrepassent, sont protégées via l'application de AH ou ESP et l'ajout des en-têtes correspondants. Les données entrantes, si elles ne sont pas éliminées ou si elles outrepassent, sont traitées via le retrait des en-têtes AH ou ESP. Dans le présent document, le trafic entrant entre dans une mise en œuvre IPsec par

l'interface "non protégée". Le trafic sortant entre dans la mise en œuvre via l'interface "protégée", ou est générée en interne par la mise en œuvre sur le côté "protégé" de la frontière et dirigé vers l'interface "non protégée". Une mise en œuvre IPsec peut prendre en charge plus d'une interface sur un ou sur les deux côtés de la frontière. L'interface protégée peut être interne, par exemple, dans une mise en œuvre d'hôte de IPsec. L'interface protégée peut assurer la liaison avec une interface de couche d'accès présentée par le système d'exploitation.

Association de sécurité (SA)
Connexion logique simplex (unidirectionnelle), créée pour les besoins de la sécurité. Tout le trafic qui traverse une SA reçoit le même traitement de sécurité. Dans IPsec, une SA est une abstraction de couche Internet mise en œuvre par l'utilisation de AH ou ESP. Les données d'état associées à une SA sont représentées dans la base de données des SA (SAD).

Passerelle de sécurité *(Security Gateway)*
Système intermédiaire qui agit comme l'interface de communications entre deux réseaux. L'ensemble des hôtes (et réseaux) sur le côté externe de la passerelle de sécurité est dit non protégé (ils sont, en général, moins protégés que ceux qui sont "derrière" la SG) alors que réseaux et hôtes du côté interne sont considérés comme protégés. Les sous-réseaux et hôtes internes servis par une passerelle de sécurité sont présumés être de confiance car ils partagent une administration de sécurité commune, locale. Dans le contexte IPsec, une passerelle de sécurité est un point auquel AH et/ou ESP sont mis en œuvre afin de servir un ensemble d'hôtes internes, de fournir des services de sécurité pour ces hôtes quand ils communiquent avec des hôtes externes qui utilisent aussi IPsec (directement ou via une autre passerelle de sécurité).

Indice des paramètres de sécurité (SPI, *Security Parameters Index*)
Valeur arbitraire de 32 bits qui est utilisée par un receveur pour identifier la SA à laquelle devrait être lié un paquet entrant. Pour une SA en envoi individuel, le SPI peut être utilisé par lui-même pour spécifier une SA, ou il peut être utilisé en conjonction avec le type de protocole IPsec. Les informations d'adresse IP supplémentaires sont utilisées pour identifier les SA en diffusion groupée. Le SPI est porté dans les protocoles AH et ESP pour permettre au système qui reçoit de choisir la SA sous laquelle le paquet reçu sera traité. Un SPI n'a qu'une signification locale, telle que définie par le créateur de la SA (habituellement le receveur du paquet qui porte le SPI) et donc, un SPI est généralement vu comme une chaîne binaire opaque. Cependant, le créateur d'une SA peut choisir d'interpréter les bits dans un SPI pour faciliter le traitement local.

Analyse de trafic
C'est l'analyse du flux de trafic réseau dans le but de déduire des informations utiles à un adversaire. Des exemples de telles informations sont la fréquence de transmission, les identités des parties, la taille des paquets, et les identifiants de flux [Sch94].

Appendice B Décorrélation

Le présent appendice se fonde sur le travail effectué pour la mise en antémémoire des politiques dans le groupe de travail politique de sécurité IP par Luis Sanchez, Matt Condell, et John Zao.

Deux entrées de SPD sont corrélées si il y a une intersection non nulle entre les valeurs des sélecteurs correspondants dans chaque entrée. La mise en antémémoire d'entrées de SPD corrélées peut conduire à une mise en application incorrecte de la politique. Une solution à ce problème, qui permet toujours la mise en antémémoire, est de retirer les ambiguïtés en décorrélant les entrées. C'est à dire que les entrées de SPD doivent être réécrites de telle sorte que pour chaque paire d'entrées il existe un sélecteur pour lequel il y a une intersection nulle entre les valeurs des deux entrées. Une fois que les entrées sont décorrélées, il n'y a plus d'exigence d'ordre entre elles, car seule une entrée peut correspondre à une recherche. Le paragraphe suivant décrit plus en détail la décorrélation et présente un algorithme qui peut être utilisé pour mettre en œuvre la décorrélation.

B.1 Algorithme de décorrélation

L'algorithme de décorrélation de base prend chaque entrée dans une SPD corrélée et la divise en un ensemble d'entrées en utilisant une structure arborescente. Les nœuds de l'arbre sont les sélecteurs qui peuvent se chevaucher entre les politiques. À chaque nœud, l'algorithme crée une branche pour chaque valeur du sélecteur. Il crée aussi une branche pour le complément de l'union de toutes les valeurs de sélecteur. Les politiques sont alors formées en traversant l'arbre de la racine jusqu'à chaque feuille. Les politiques au niveau des feuilles sont comparées à l'ensemble des règles de politique déjà décorrélées. Chaque politique au niveau d'une feuille est soit complètement écrasée par une politique dans l'ensemble déjà décorrélé et est éliminée ou est décorrélée avec toutes les politiques dans l'ensemble décorrélé et lui est ajoutée.

L'algorithme de base ne garantit pas un ensemble optimal d'entrées décorrélées. C'est à dire que les entrées peuvent être

divisées en ensembles plus petits qu'il n'est nécessaire, bien qu'elles fournissent encore toutes les informations de politique nécessaires. Certaines extensions à l'algorithme de base sont décrites plus loin pour améliorer cela ainsi que les performances de l'algorithme.

C un ensemble d'entrées ordonnées, corrélées (une SPD corrélée).
Ci la i[ème] entrée dans C.
U l'ensemble des entrées décorrélées construites à partir de C.
Ui la i[ème] entrée dans U.
Sik la k[ème] sélection pour la politique Ci.
Ai l'action pour la politique Ci.

Une politique (entrée de SPD) P peut être exprimée par une séquence de valeurs de sélecteur et une action (BYPASS, DISCARD, ou PROTECT):

Ci = Si1 x Si2 x ... x Sik -> Ai

1) Mettre C1 dans l'ensemble U comme U1

Pour chaque politique Cj (j > 1) in C

2) Si Cj est décorrélée d'avec chaque entrée dans U, l'ajouter alors à U.

3) Si Cj est corrélée avec une ou plusieurs entrées dans U, créer un arbre dont la racine est la politique Cj qui partage Cj en un ensemble d'entrées décorrélées. L'algorithme commence avec un nœud racine où aucun sélecteur n'a encore été choisi.

A) Choisir un sélecteur dans Cj, Sjn, qui n'a pas déjà été choisi en traversant l'arbre depuis la racine jusqu'à ce nœud. Si il n'y a pas de sélecteur qui ait été déjà utilisé, continuer jusqu'au prochain embranchement non terminé jusqu'à ce que toutes les branches soient complétées. Quand tout l'arbre est complété, passer à l'étape D.

T est l'ensemble des entrées dans U qui sont corrélées avec l'entrée à ce nœud.

L'entrée à ce nœud est l'entrée formée par les valeurs de sélecteur de chacune des branches entre la racine et ce nœud. Toutes les valeurs de sélecteur qui ne sont pas encore représentées par des branches supposent la valeur du sélecteur correspondant dans Cj, car les valeurs dans Cj représentent la valeur maximum pour chaque sélecteur.

B) Ajouter une branche à l'arbre pour chaque valeur du sélecteur Sjn qui apparaît dans toute entrée en T. (Si la valeur est un sur-ensemble de la valeur de Sjn dans Cj, utiliser alors la valeur dans Cj, car cette valeur représente l'ensemble universel.) Ajouter aussi une branche pour le complément de l'union de toutes les valeurs du sélecteur Sjn dans T. Quand on prend le complément, se souvenir que l'ensemble universel est la valeur de Sjn dans Cj. Une branche n'a pas besoin d'être créée pour l'ensemble nul.

C) Répéter A et B jusqu'à ce que l'arbre soit complété.

D) L'entrée de chaque feuille représente maintenant une entrée qui est un sous-ensemble de Cj. Les entrées au niveau des feuilles de la partition Cj sont achevées de telle sorte que chaque entrée soit complètement recouverte par une entrée dans U, ou soit décorrélé avec les entrées dans U.

Ajouter toutes les entrées décorrélées des feuilles de l'arbre à U.

4) Prendre le Cj suivant et aller en 2.

5) Lorsque toutes les entrées en C ont été traitées, U contient alors une version décorrélée de C.

Il y a plusieurs optimisations qui peuvent être faites à cet algorithme. Quelques unes d'entre elles sont présentées ici.

Il est possible d'optimiser, ou au moins d'améliorer, la quantité d'embranchements qui surviennent en choisissant soigneusement l'ordre des sélecteurs utilisés pour la branche suivante. Par exemple, si un sélecteur Sjn peut être choisi de telle sorte que toutes les valeurs pour ce sélecteur dans T soient égales ou soient un sur-ensemble de la valeur de Sjn dans Cj, il ,'est alors besoin de créer qu'une seule branche (car le complément sera nul).

Les branches de l'arbre n'ont pas à traiter l'algorithme de décorrélation entier. Par exemple, si un nœud représente une entrée qui est décorrélée avec toutes les entrées dans U, il n'y a alors aucune raison de continuer à décorréler cette branche.

Aussi, si une branche est complètement écrasée par une entrée dans U, il n'y a alors aucune raison de continuer à décorréler la branche.

Une optimisation supplémentaire est de vérifier pour voir si une branche est écrasée par une des entrées corrélées dans l'ensemble C qui a déjà été décorrélé. C'est à dire que si la branche fait partie du Cj décorrélé, on vérifie alors pour voir si elle a été écrasée par une entrée Cm, m < j. C'est une vérification valide, car toutes les entrées Cm sont déjà exprimées en U.

Avec la vérification pour voir si une entrée est déjà décorrélée à l'étape 2, vérifier si Cj est écrasé par une entrée dans U. Si c'est le cas, la sauter car cela ne sert à rien. Une entrée x est écrasée par une autre entrée y si chaque sélecteur dans x est égal à, ou est un sur-ensemble des sélecteurs correspondants dans l'entrée y.

Appendice C ASN.1 pour une entrée de SPD

Cet appendice est inclus comme une façon supplémentaire de décrire les entrées de SPD, comme défini au paragraphe 4.4.1. Il utilise la syntaxe ASN.1 dont la compilation a été faite avec succès. Cette syntaxe est simplement une illustration et il n'est pas nécessaire de l'employer dans une mise en œuvre pour réaliser la conformité. La description de SPD du paragraphe 4.4.1 est normative.

```
SPDModule

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

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

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

    -- Une SPD est une liste des politiques en ordre de préférence décroissante
    SPD ::= SEQUENCE OF SPDEntry

    SPDEntry ::= CHOICE {
       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 du paquet
                     -- S'applique à TOUS les sélecteurs de trafic correspondants dans les SelectorLists
       condition   SelectorLists,  -- Politique "condition"
       processing  Processing      -- Politique "action"
       }

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

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

```
NameSets ::= SEQUENCE {
   passed     SET OF Names-R,  -- Confronté à l'identifiant IKE par celui qui répond
   local      SET OF Names-I } – Utilisé en interne par l'initiateur IKE

Names-R ::= CHOICE {                -- IKEv2 IDs
   dName      RDNSequence,          -- ID_DER_ASN1_DN
   fqdn       FQDN,                 -- ID_FQDN
   rfc822     [0] RFC822Name,       -- ID_RFC822_ADDR
   keyID      OCTET STRING }        -- KEY_ID

Names-I ::= OCTET STRING       -- Utilisé en interne par l'initiateur IKE

FQDN ::= IA5String

RFC822Name ::= IA5String

PacketFlags ::= BIT STRING {
        -- s'il est mis, prendre la valeur de sélecteur dans le paquet qui établit la SA ou autrement utiliser une valeur dans
        l'entrée de SPD
   localAddr  (0),
   remoteAddr (1),
   protocol   (2),
   localPort  (3),
   remotePort (4)  }

SelectorLists ::= SET OF SelectorList

SelectorList ::= SEQUENCE {
   localAddr   AddrList,
   remoteAddr  AddrList,
   protocol    ProtocolChoice }

Processing ::= SEQUENCE {
   extSeqNum   BOOLEAN,      -- VRAI, compteur de 64 bits, FAUX, de 32 bits
   seqOverflow BOOLEAN,       -- VRAI, changer les clés, FAUX, terminer & audit
   fragCheck   BOOLEAN,       -- VRAI, vérification dynamique de fragment,
                              -- FAUX, pas de vérification dynamique de fragment
   lifetime    SALifetime,
   spi         ManualSPI,
   algorithms  ProcessingAlgs,
   tunnel      TunnelOptions FACULTATIF } -- si absent, utiliser le mode transport

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

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

KeyIDs ::= SEQUENCE OF OCTET STRING

ProcessingAlgs ::= CHOICE {
   ah         [0] IntegrityAlgs,  -- AH
   esp        [1] ESPAlgs}        -- ESP

ESPAlgs ::= CHOICE {
   integrity       [0] IntegrityAlgs,       -- integrité seulement
   confidentiality [1] ConfidentialityAlgs, -- confidentialité seulement
   both            [2] IntegrityConfidentialityAlgs,
   combined        [3] CombinedModeAlgs }
```

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

-- Algorithmes d'intégrité, ordonnés par préférence décroissante
IntegrityAlgs ::= SEQUENCE OF IntegrityAlg

-- Algorithmes de confidentialité, ordonnés par préférence décroissante
ConfidentialityAlgs ::= SEQUENCE OF ConfidentialityAlg

-- Integrity Algorithms
IntegrityAlg ::= SEQUENCE {
   algorithm   IntegrityAlgType,
   parameters  ANY -- DEFINED BY algorithm -- FACULTATIF }

IntegrityAlgType ::= INTEGER {
   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)
--  tbd (6..65535)
   }

-- Confidentiality Algorithms
ConfidentialityAlg ::= SEQUENCE {
   algorithm   ConfidentialityAlgType,
   parameters  ANY -- DEFINED BY algorithm -- 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 OF CombinedModeAlg

CombinedModeAlg ::= SEQUENCE {
   algorithm   CombinedModeType,
   parameters  ANY -- DEFINED BY algorithm} – défini en-dehors du présent document pour les modes AES.

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

TunnelOptions ::= SEQUENCE {
   dscp       DSCP,
   ecn        BOOLEAN,    -- VRAI, Copier CE sur l'en-tête interne
   df         DF,
```

```
   addresses   TunnelAddresses }

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

IPv4Pair ::= SEQUENCE {
   local      OCTET STRING (SIZE(4)),
   remote     OCTET STRING (SIZE(4)) }

IPv6Pair ::= SEQUENCE {
   local      OCTET STRING (SIZE(16)),
   remote     OCTET STRING (SIZE(16)) }

DSCP ::= SEQUENCE {
   copy     BOOLEAN,          -- VRAI, Copier CE à partir de l'en-tête interne
                              -- FAUX, ne pas copier
   mapping   OCTET STRING FACULTATIF} -- pointe sur le tableau s'il n'y a pas de copie

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

ProtocolChoice::= CHOICE {
   anyProt  AnyProtocol,                  -- pour ANY protocole
   noNext   [0] NoNextLayerProtocol,      -- pas d'élément couche suivante
   oneNext  [1] OneNextLayerProtocol,     -- un élément couche suivante
   twoNext  [2] TwoNextLayerProtocol,     -- deux éléments couche suivante
   fragment FragmentNoNext }              -- pas d'informationsde couche suivante

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

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

NoNextLayerProtocol ::= ENTIER (2..254)

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

OneNextLayerProtocol ::= SEQUENCE {
   id         ENTIER (1..254),   -- ICMP, MH, ICMPv6
   nextLayer   NextLayerChoice }   -- Type ICMP *256 + Code
                           -- MH   Type*256

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

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

-- Repréentation deNY dans le champ couche suivante
AnyNextLayer ::= SEQUENCE {
   start      ENTIER (0),
   end        ENTIER (65535) }
```

```
-- Repréentation de OPAQUE dans le champ couche suivante.
-- Correspond à la convention IKE
OpaqueNextLayer ::= SEQUENCE {
   start      ENTIER (65535),
   end        ENTIER (0) }

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

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

-- Représentations d'adresse IPv4
IPv4List ::= SEQUENCE OF IPv4Range

IPv4Range ::= SEQUENCE {    -- proche, mais pas tout à fait ...
   ipv4Start   OCTET STRING (SIZE (4)),
   ipv4End     OCTET STRING (SIZE (4)) }

-- Représentations d'adresse IPv6
IPv6List ::= SEQUENCE OF IPv6Range

IPv6Range ::= SEQUENCE {    -- proche, mais pas tout à fait ...
   ipv6Start   OCTET STRING (SIZE (16)),
   ipv6End     OCTET STRING (SIZE (16)) }

END
```

Appendice D Raisons du traitement de fragment

Trois questions doivent être résolues concernant le traitement des fragments (en clair) dans IPsec :
- transposition d'un fragment non initial sortant à la bonne SA (ou trouver la bonne entrée de SPD)
- vérifier qu'un fragment non initial reçu est autorisé pour la SA via laquelle il est reçu
- transposition de fragments non initiaux entrants et sortants à la bonne entrée de SPD/antémémoire, pour le trafic BYPASS/DISCARD.

Les premières et troisièmes questions se posent parce qu'on a besoin d'un algorithme déterministe pour transposer le trafic aux SA (et entrées de SPD/antémémoire). Les trois questions sont importantes parce que on veut être sûr que les fragments non initiaux qui traversent la frontière IPsec ne causent pas de violation des politiques de contrôle d'accès en place chez le receveur (ou celui qui transmet).

D.1 Mode de transport et fragments

D'abord, nous notons que les SA en mode transport ont été définies comme ne portant pas de fragments. Ceci est hérité de la [RFC2401], où les SA en mode transport sont toujours terminées à des points d'extrémité. C'est une exigence fondamentale parce que, dans le plus mauvais cas, un fragment IPv4 auquel est appliqué IPsec pourrait alors être fragmenté (comme un paquet de texte chiffré) en route vers la destination. Les procédures IP de réassemblage de fragment chez le receveur IPsec ne seraient pas capables de distinguer entre les fragments pré IPsec et les fragments créés après le traitement IPsec.

Pour IPv6, seul l'envoyeur est autorisé à fragmenter un paquet. Comme pour IPv4, une mise en œuvre IPsec est autorisée à fragmenter les paquets en mode tunnel après le traitement IPsec, parce que c'est l'envoyeur par rapport à l'en-tête de tunnel (externe). Cependant, à la différence de IPv4, il serait faisable de porter un fragment en clair sur une SA en mode transport, parce que l'en-tête de fragment dans IPv6 apparaîtrait après l'en-tête AH ou ESP, et ne causerait donc pas de confusion chez le receveur pour ce qui est du réassemblage. Précisément, le receveur n'essayerait pas de réassembler les fragments jusqu'à la fin du traitement IPsec. Pour rester simple, la présente spécification interdit le portage de fragments sur les SA en

mode transport pour le trafic IPv6.

Lorsque seuls des systèmes d'extrémité utilisaient des SA en mode transport, la prohibition du portage de fragments n'était pas un problème, car on suppose que le système d'extrémité pouvait être configuré de façon à ne pas offrir de fragment à IPsec. Pour une mise en œuvre d'hôte native, cela semble raisonnable, et, comme il l'a parfois été noté, la RFC2401 avertissait qu'une mise en œuvre BITS pouvait avoir à réassembler des fragments avant d'effectuer une recherche de SA. (Elle aurait ensuite appliqué AH ou ESP et pouvait refragmenter le paquet après le traitement IPsec.) Comme une mise en œuvre BITS est supposée être capable d'avoir accès à tous les trafics émanant de cet hôte, même si l'hôte a plusieurs interfaces, cela paraissait une obligation raisonnable.

Dans la présente spécification, il est acceptable d'utiliser le mode transport dans les cas où la mise en œuvre IPsec n'est pas la destination ultime, par exemple, entre deux passerelles de sécurité. En principe, cela crée une nouvelle opportunité pour que les fragments en clair soient transposés sur une SA en mode transport pour le traitement IPsec. Cependant, dans ces nouveaux contextes dans lesquels l'utilisation d'une SA en mode transport est maintenant approuvée, il semble vraisemblable qu'on puisse continuer à prohiber la transmission de fragments, tels qu'ils sont vus par IPsec, c'est-à-dire, des paquets qui ont un "en-tête externe" avec un champ de décalage de fragment différent de zéro. Par exemple, dans un réseau IP de recouvrement, les paquets qui sont envoyés sur des SA en mode transport sont tunnelés IP dans IP et donc ont l'en-tête interne nécessaire pour s'accommoder de la fragmentation avant le traitement IPsec. Lorsqu'ils sont portés via une SA en mode transport, IPsec ne va pas examiner l'en-tête IP interne pour un tel trafic, et donc ne va pas considérer le paquet comme un fragment.

D.2 Mode tunnel et fragments

Pour les SA en mode tunnel, le cas s'est toujours présenté de fragments sortants qui arrivent pour être traités à une application IPsec. Le besoin de s'accommoder de paquets sortants fragmentés peut poser un problème parce qu'un fragment non initial ne va généralement pas contenir les champs d'accès associés à un protocole de couche suivante tel que TCP, UDP, ou SCTP. Et donc, selon la configuration de la SPD pour une mise en œuvre IPsec donnée, des fragments en clair peuvent ou non poser problème.

Par exemple, si la SPD requiert que tout le trafic entre deux gammes d'adresses reçoive la protection IPsec (aucune entrée de SPD BYPASS ou DISCARD ne s'applique à cette gamme d'adresses) il devrait alors être facile de porter des fragments non initiaux sur la SA définie pour cette gamme d'adresses, car l'entrée de SPD implique une intention de porter TOUT le trafic entre les gammes d'adresses. Mais, si il y a plusieurs entrées de SPD qui pourraient correspondre à un fragment, et si ces entrées font référence à des sous-ensembles différents de champs d'accès (par opposition à ANY) il n'est alors pas possible de transposer un fragment non initial sortant à la bonne entrée, sans ambiguïté. (Si on choisit de permettre le portage de fragments sur des SA en mode transport pour IPv6, les problèmes surviennent aussi dans ce contexte.)

Ce problème a largement, bien que pas exclusivement, motivé la définition de OPAQUE comme valeur de sélecteur pour les champs d'accès dans la RFC2401. L'autre raison de OPAQUE est l'observation que les champs d'accès pourraient n'être pas accessibles du fait de l'application d'IPsec. Par exemple, si un hôte applique IPsec à son trafic et que ce trafic arrive à une passerelle de sécurité, ces champs seront chiffrés. L'algorithme spécifié pour localiser le "protocole de couche suivante" décrit dans la RFC2401 a aussi motivé l'utilisation de OPAQUE pour s'accommoder d'un champ protocole de couche suivante chiffré dans de telles circonstances. Néanmoins, la principale utilisation de la valeur OPAQUE était de satisfaire aux champs de sélecteur de trafic dans des paquets qui ne contenaient pas de champ d'accès (fragments non initiaux) ou paquets dans lesquels les champs d'accès étaient déjà chiffrés (par suite d'une application incorporée d'IPsec). La RFC2401 était ambiguë dans l'exposé sur l'utilisation de OPAQUE ou ANY, en suggérant à certains endroits que ANY pouvait être une solution de remplacement à OPAQUE.

On obtient des capacités de contrôle d'accès supplémentaires en définissant les deux valeurs ANY et OPAQUE. OPAQUE peut être défini pour ne correspondre qu'aux champs qui ne sont pas accessibles. On pourrait définir ANY comme le complément de OPAQUE, c'est-à-dire, il correspondrait à toutes les valeurs mais seulement pour les champs d'accès accessibles. Nous avons donc simplifié la procédure employée pour localiser le protocole de couche suivante dans le présent document, de sorte que nous traitons ESP et AH comme des protocoles de couche suivante. Il en résulte que la notion de champ de protocole de couche suivante chiffré a disparu, et qu'il n'est plus nécessaire de s'inquiéter non plus des champs d'accès chiffrés. Et en conséquence, OPAQUE ne sera applicable qu'aux fragments non initiaux.

Comme nous avons adopté la définition ci-dessus pour ANY et OPAQUE, il est nécessaire de préciser comment ces valeurs fonctionnent lorsque le protocole spécifié n' pas de champs d'accès, et quand ANY est utilisé pour le sélecteur de protocole. En conséquence, si une valeur spécifique de protocole est utilisée comme sélecteur, et si ce protocole n'a pas de champ d'accès, le sélecteur de champ d'accès doit être ignoré et ANY DOIT être spécifié comme valeur pour les champs d'accès. (Dans ce contexte, les valeurs de TYPE et CODE ICMP sont groupées comme un seul champ d'accès (pour la négociation IKEv2, comme l'est la valeur de type d'en-tête de mobilité IPv6.) Si le sélecteur de protocole est ANY, cela devrait alors

être traité comme équivalent à la spécification d'un protocole pour lequel aucun champ d'accès n'est défini, et donc, les sélecteurs d'accès devraient être ignorés, et DOIVENT être réglés à ANY.

D.3 Le problème des fragments non initiaux

Pour une mise en œuvre de passerelle de sécurité, il est évident que des fragments peuvent arriver des systèmes d'extrémité derrière la passerelle. Une mise en œuvre BITW peut aussi rencontrer des fragments provenant d'un hôte ou passerelle derrière lui. (Comme noté plus haut, des mises en œuvre d'hôte natives et des mises en œuvre BITW peuvent probablement éviter les problèmes décrits ci-dessous.) Dans le pire des cas, les fragments provenant d'un paquet pourraient arriver à des mises en œuvre BITW ou SG distinctes et donc empêcher la solution de l'option de réassemblage. Et donc, dans la RFC 2401 nous avons adopté l'exigence générale que les fragments soient traités en mode tunnel pour toutes les mises en œuvre. Cependant, la RFC2401 ne fournissait pas une solution parfaite. L'utilisation de OPAQUE comme valeur de sélecteur pour les champs d'accès (DEVRAIT dans la RFC2401) permettait à une SA de porter des fragments non initiaux.

En utilisant les caractéristiques définies dans la RFC2401, si on définissait une SA entre deux mises en œuvre IPsec (SG ou BITW) utilisant la valeur OPAQUE pour les deux champs d'accès, tous les fragments non initiaux satisfaisant aux adresses de source/destination (S/D) et aux valeurs de protocole pour la SA seraient transposés dans cette SA. Les fragments initiaux NE seraient PAS transposés dans cette SA, si nous adoptons une définition stricte de OPAQUE. Cependant, la RFC2401 ne donnait pas de lignes directrices détaillées sur ce point et donc il pouvait n'être pas apparent que l'utilisation de ce dispositif créerait essentiellement une SA de "fragment non initial exclusivement".

Dans le cours des discussions sur l'approche des SA "seulement de fragment", il a été noté que certains problèmes subtils, non pris en compte dans la RFC2401, pouvaient être évités. Par exemple, une SA de cette sorte doit être configurée pour offrir la "meilleure qualité" de services de sécurité pour tout trafic entre les adresses S/D indiquées (pour le protocole spécifié). Ceci est nécessaire pour garantir que tout trafic capturé par une SA seulement de fragment ne se voit pas offrir une sécurité dégradée par rapport à ce qui lui aurait été offert si le paquet n'avait pas été fragmenté. Un problème possible à ce niveau est qu'on peut n'être pas en mesure d'identifier la "meilleure qualité" de services de sécurité définie pour l'utilisation entre deux mises en œuvre IPsec, car le choix des protocoles de sécurité, des options, et des algorithmes est un ensemble entrelacé non totalement ordonné. (On peut dire en toute sécurité que BYPASS < AH < ESP w/integrity, mais cela devient compliqué si il y a plusieurs options de chiffrement ESP ou d'algorithmes d'intégrité.) Aussi on doit imposer un ordonnancement total de ces paramètres de sécurité pour que cela fonctionne, mais cela peut être fait localement.

Cependant, cette stratégie conservatrice n'est pas sans effets possibles sur les performances. Si la plupart du trafic qui traverse une mise en œuvre IPsec pour une paire donnée d'adresses S/D (et le protocole spécifié) outrepasse IPsec, une SA seulement de fragment pour cette paire d'adresses pourrait causer un accroissement dramatique du volume de trafic à chiffrer. Si la mise en œuvre du chiffre ne peut pas accepter de tels débits, cela peut causer des problèmes. (Une mise en œuvre IPsec qui serait capable de performances de chiffrement au niveau du débit de la ligne ou proches, ne serait pas affectée par cette approche de la configuration de SA. Néanmoins, l'impact sur les performances est un souci potentiel, spécifique des capacités de la mise en œuvre.)

Un autre souci est que des fragments non initiaux envoyés sur une SA dédiée pourraient être utilisés pour effectuer des attaques par chevauchement du réassemblage, lorsqu'elles sont combinées avec un fragment initial apparemment acceptable. (Cette sorte d'attaque suppose la création de fragments fautifs et n'est pas un effet collatéral de la fragmentation normale.) Ce problème est facilement réglé dans IPv4, en vérifiant la valeur de décalage du fragment pour s'assurer qu'aucun fragment non initial n'a un décalage suffisamment petit pour chevaucher les champs d'accès qui devraient être contenus dans le fragment initial. Rappelons que la MTU minimum de IPv4 est de 576 octets, et que la longueur maximale d'en-tête IP est de 60 octets, de sorte que tous les accès devraient être présents dans le fragment initial. Si nous exigeons que tous les fragments non initiaux aient un décalage de, disons, 128 ou plus, pour se donner une marge de sécurité, ceci devrait empêcher la réussite de telles attaques. Si l'intention est seulement de se protéger contre cette sorte d'attaque de réassemblage, il n'est nécessaire de ne mettre en œuvre cette vérification que chez le receveur.

IPv6 a aussi un décalage de fragment, porté dans l'en-tête d'extension de fragmentation. Cependant, les en-têtes d'extension IPv6 ont des longueurs variables et il n'y a pas d'analogue de la valeur de longueur maximale d'en-tête qu'on pourrait utiliser pour vérifier les fragments non initiaux, pour rejeter ceux qui pourraient être utilisés pour une attaque du type mentionné ci-dessus. Un receveur aurait besoin de maintenir un état analogue à l'état de réassemblage, pour fournir une protection équivalente. Ainsi, ce n'est que pour IPv4 qu'il est possible d'imposer une vérification de décalage de fragment qui rejetterait les attaques conçues pour circonvenir les vérifications de champ d'accès par IPsec (ou les pare-feu) lors du passage de fragments non initiaux.

Un autre souci possible est que dans certaines topologies et configurations de SPD, cette approche peut déboucher sur un coup de main contre le contrôle d'accès. L'idée est que si on crée une SA pour porter TOUS les fragments (non initiaux), cette SA portera du trafic qui pourrait autrement arriver en clair par un chemin séparé, par exemple, un chemin surveillé par

un pare-feu mandataire. Mais, ce souci n'apparaît que si l'autre chemin permet à des fragments initiaux de le traverser sans exiger de réassemblage, ce qui est plutôt une mauvaise idée pour un pare-feu mandataire. Néanmoins, ceci représente bien un problème potentiel dans certaines topologies et sous certaines hypothèses par rapport à SPD et (autres) ensembles de règles de pare-feu, et les administrateurs doivent être avertis de cette possibilité.

Un souci moins sérieux est que les fragments non initiaux envoyés sur une SA seulement à fragment non initial peuvent représenter une opportunité d'attaque de déni de service, en ce que ils peuvent être envoyés alors qu'aucun fragment initial valide ne va jamais arriver. Ceci peut être utilisé pour attaquer des hôtes derrière une SG ou appareil BITW. Cependant, le risque incrémental posé par cette sorte d'attaque, qui ne peut être montée que par des hôtes derrière une SG ou appareil BITW, semble faible.

Si on interprète la valeur du sélecteur ANY comme mettant en application OPAQUE, une seule SA avec des valeurs ANY pour les deux champs d'accès serait alors capable de s'accommoder de tout le trafic correspondant aux adresses de source et de destination et aux sélecteurs de trafic du protocole, en solution de remplacement à l'utilisation de la valeur OPAQUE. Mais, utiliser ANY ici empêche plusieurs SA distinctes entre les mêmes mises en œuvre IPsec pour les mêmes paires d'adresse et protocole. Ainsi, ce n'est pas exactement une solution de remplacement équivalente.

Fondamentalement, les problèmes du traitement des fragments ne surviennent que lorsque plus d'une SA est définie avec les mêmes valeurs de sélecteur d'adresse S/D et protocole, mais avec des valeurs de sélecteur de champ d'accès différentes.

D.4 Trafic BYPASS/DISCARD

Nous devons aussi nous intéresser à la question du traitement du fragment non initial pour les entrées BYPASS/DISCARD, indépendamment du traitement de la SA. Ceci est largement un problème local pour deux raisons :

1) Nous n'avons aucun moyen de coordonner les entrées de SPD pour un tel trafic entre mises en œuvre IPsec car IKE n'est pas invoqué.
2) Nombre de ces entrées se réfèrent à du trafic qui N'EST PAS dirigé vers ou reçu par une localisation qui utilise IPsec. Aussi n'y a t-il pas de mise en œuvre IPsec homologue avec laquelle se coordonner d'une façon ou d'une autre.

Cependant, le présent document devrait donner une ligne de conduite sur ce point, cohérente avec notre but d'offrir une fonction de contrôle d'accès bien définie pour tout le trafic, à propos de la frontière IPsec. À cette fin, le présent document dit que les mises en œuvre DOIVENT prendre en charge le réassemblage de fragment pour le trafic BYPASS/DISCARD lorsque les champs d'accès sont spécifiés. Une mise en œuvre DOIT aussi permettre à un usager ou administrateur d'accepter un tel trafic ou rejeter ce trafic en utilisant les conventions SPD décrites au paragraphe 4.4.1. Le problème est que faire outrepasser (BYPASS) un fragment non initial en clair qui arrive à une mise en œuvre IPsec pourrait porter atteinte à la sécurité offerte au trafic protégé par IPsec qui est dirigé sur la même destination. Par exemple, considérons une mise en œuvre IPsec configurée avec une entrée de SPD qui appelle à la protection IPsec du trafic entre une paire spécifique source/adresse de destination, et à un protocole et accès de destination spécifiques, par exemple, du trafic TCP sur l'accès 23 (Telnet). Supposons que la mise en œuvre permette aussi l'outrepassement du trafic provenant de la même paire source/adresse de destination et protocole, mais pour un accès de destination différent, par exemple, l'accès 119 (NNTP). Un attaquant pourrait envoyer un fragment non initial (avec une fausse adresse de source) qui, si il outrepasse, pourrait se chevaucher avec du trafic protégé par IPsec provenant de la même source et ainsi violer l'intégrité du trafic protégé par IPsec. Exiger la vérification dynamique de fragment pour les entrées BYPASS avec des gammes d'accès non triviales empêche des attaques de cette sorte.

D.5 Dire simplement non aux accès ?

Il a été suggéré qu'on pourrait éviter les problèmes décrits ci-dessus en ne permettant pas aux sélecteurs de champ d'accès d'être utilisés en mode tunnel. Mais la discussion ci-dessus montre que ce serait une approche excessivement stricte, car aucun problème n'apparaît pour les mises en œuvre OS et BITS natives. De plus, certains membres du groupe de travail ont décrit des scénarios où l'utilisation de SA en mode tunnel avec des sélecteurs de champ d'accès (non triviaux) est appropriée. Ainsi le défi est de définir une stratégie qui puisse régler ce problème dans les contextes BITW et SG. Noter aussi que les entrées BYPASS/DISCARD dans la SPD qui utilisent des accès posent le même problème, sans égard aux notions de mode tunnel ou mode transport.

Certains ont suggéré qu'on devrait laisser un pare-feu derrière une SG ou BITW pour mettre en application des contrôles d'accès de niveau port et les effets de la fragmentation. Cependant, cela semble une suggestion incongrue en ce que ailleurs dans IPsec (par exemple, dans les charges utiles IKE) on a le problème des pare-feu qui éliminent toujours les fragments. Si de nombreux pare-feu ne passent pas en général les fragments, pourquoi devrait on s'attendre à ce qu'ils traitent les fragments dans ce cas ? Ainsi, la présente analyse rejette la suggestion d'interdire l'usage des sélecteurs de champ d'accès avec les SA en mode tunnel.

D.6 Suggestion d'autres solutions

Une suggestion est de réassembler les fragments à la mise en œuvre IPsec d'envoi, et donc d'éviter entièrement le problème. Cette approche est invisible au receveur et pourrait donc être adoptée comme option de mise en œuvre purement locale.

Une version plus sophistiquée de cette suggestion appelle à l'établissement et au maintien d'un état minimal à partir de chaque fragment initial rencontré, pour permettre de faire correspondre les fragments non initiaux aux bonnes SA ou entrées de SPD/antémémoire. Ceci implique une extension du modèle de traitement actuel (et de l'ancien). La mise en œuvre IPsec intercepterait tous les fragments ; saisie des adresses IP de source/destination, protocole, identifiant de paquet, et champs d'accès provenant des fragments initiaux, et utiliserait ensuite ces données pour transposer les fragments non initiaux dans les SA qui exigent des champs d'accès. Si cette approche est employée, le receveur doit utiliser un schéma équivalent, comme il doit aussi vérifier que les fragments reçus sont cohérents avec les valeurs de sélecteur de la SA. Un fragment non initial qui arrive avant un fragment initial pourrait être mis en antémémoire ou éliminé, en attendant l'arrivée du fragment initial correspondant.

Un inconvénient des deux approches notées ci-dessus est qu'elles ne vont pas toujours fonctionner. Lorsqu'un appareil BITW ou SG est configuré dans une topologie qui pourrait permettre de traiter certains fragments d'un paquet sur des SG ou appareils BITW différents, il n'y a alors aucune garantie que tous les fragments arrivent jamais au même appareil IPsec. Cette approche soulève aussi des problèmes de traitement possibles. Si l'envoyeur met en antémémoire des fragments non initiaux jusqu'à ce que le fragment initial correspondant arrive, des problèmes de mémoire tampon vont surgir, en particulier à grande vitesse. Si les fragments non initiaux sont éliminés plutôt que mis en antémémoire, il n'est pas garanti que le trafic va passer, par exemple, la retransmission va résulter en différents identifiants de paquet qui ne vont pas correspondre à des transmissions antérieures. Dans tous les cas, les procédures d'entretien seront nécessaires pour décider du moment où il faut supprimer les données d'état de fragment, ce qui ajoute de la complexité au système. Néanmoins, c'est une solution viable dans certaines topologies, et ce sont vraisemblablement des topologies courantes.

Le groupe de travail a rejeté une version antérieure de la convention de création d'une SA pour porter seulement des fragments non initiaux, ce qui avait été soutenu implicitement dans le modèle de la RFC2401 via l'utilisation du champ d'accès OPAQUE, mais n'était jamais clairement formulé dans la RFC2401. Le texte (rejeté) demandait que chaque fragment non initial soit traité comme protocole 44 (l'identifiant de protocole d'en-tête de fragment IPv6) par l'envoyeur et le receveur. Cette approche permet de rendre le traitement de fragment IPv4 et IPv6 plus uniforme, mais elle ne change pas fondamentalement le problème, ni ne résout la question du traitement de fragment pour le trafic BYPASS/DISCARD. Étant donné le problème de l'attaque de chevauchement de fragment posé par IPv6, il ne semble pas que cela vaille la peine d'adopter cette stratégie.

D.7 Cohérence

Précédemment, le groupe de travail s'était mis d'accord pour permettre à un appareil BITS, BITW, ou SG IPsec d'effectuer la fragmentation avant le traitement IPsec. Si cette fragmentation est effectuée après la recherche de SA chez l'envoyeur, il n'y a pas de problème de "transposer dans la bonne SA". Mais le receveur a toujours besoin d'être capable de vérifier que les fragments non initiaux sont cohérents avec la SA via laquelle ils sont reçus. Comme le fragment initial pourrait être perdu en route, le receveur rencontre tous les problèmes potentiels notés ci-dessus. Et donc, si on veut être cohérent, il faut dire comment un receveur va traiter le fragment non initial qui arrive.

D.8 Conclusions

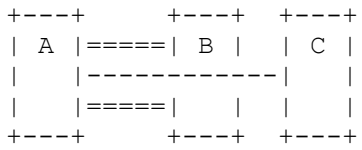
Il n'y a pas une façon simple, uniforme, de traiter les fragments dans tous les contextes. Différentes approches fonctionnent mieux dans des contextes différents. Et donc, le présent document offre trois choix -- un DOIT et deux PEUT. À l'avenir, si la communauté acquiert de l'expérience avec les deux PEUT, ils pourront devenir des DEVRAIT ou des DOIT, ou d'autres approches pourront être proposées.

Appendice E Exemple de prise en charge de SA incorporées via SPD et entrées de tableau de transmission

Le présent appendice donne un exemple de la façon de configurer la SPD et les tableaux de transmission pour la prise en charge d'une paire d'associations de sécurité incorporées, cohérente avec le nouveau modèle de traitement. Pour simplifier, cet exemple suppose une seule SPD-I.

Le but de cet exemple est de mettre en scène une SA en mode transport de A à C, portée sur une SA en mode tunnel de A à

B. Par exemple, A pourrait être un ordinateur portable connecté à l'Internet public, B pourrait être un pare-feu qui protège un réseau d'entreprise, et C pourrait être un serveur sur le réseau d'entreprise qui demande l'authentification de bout en bout du trafic de A.



La SPD de A contient des entrées de la forme :

Couche suivante				
Règle	Local	Distant	Protocole	Action
1	C	A	ESP	BYPASS
2	A	C	ICMP, ESP	PROTECT (ESP, tunnel, entier + conf)
3	A	C	ANY	PROTECT (ESP, transport, entier-seul)
4	A	B	ICMP, IKE	BYPASS

Le côté non protégé du tableau de transmission de A est réglé de sorte que les paquets sortants destinés à C soient en boucle sur le côté protégé. Le côté protégé du tableau de transmission de A est réglé de sorte que les paquets ESP entrants soient en boucle sur le côté non protégé. Les tableaux de transmission de A contiennent des entrées de la forme :

Côté non protégé du tableau de transmission

Règle	Local	Distant	Protocole	Action
1	A	C	ANY	En boucle sur le côté protégé
2	A	B	ANY	Transmettre à B

Côté protégé du tableau de transmission

Règle	Local	Distant	Protocole	Action
1	A	C	ESP	En boucle sur le côté non protégé

Un paquet TCP sortant de A à C correspondra à la règle 3 de la SPD et c'est le mode transport ESP qui s'appliquera à lui. Le tableau de transmission du côté non protégé renverra alors le paquet en boucle. Le paquet est comparé à la SPD-I (voir la Figure 2) et correspond à la règle 1 de la SPD, et donc il outrepasse. Le paquet est traité comme paquet sortant et comparé à la SPD pour la troisième fois. Cette fois, il correspond à la règle 2 de la SPD2, et donc ESP est appliqué en mode tunnel. Cette fois, le tableau de transmission ne remet pas le paquet en boucle, parce que l'adresse de destination externe est B, aussi le paquet part sur le réseau.

Un paquet TCP entrant de C à A est encadré par deux en-têtes ESP ; l'en-tête externe (ESP en mode tunnel) montre B comme source, alors que l'en-tête interne (ESP en mode transport) montre C comme source. À l'arrivée à A, le paquet devrait être transposé en SA sur la base du SPI, avoir l'en-tête externe retiré, et être déchiffré et vérifié en intégrité. Il serait ensuite confronté aux sélecteurs de la SAD pour cette SA, qui spécifierait C comme source et A comme destination, déduite de la règle 2 de la SPD. La fonction de transmission du côté protégé le renverrait alors du côté non protégé sur la base des adresses et du protocole de couche suivante (ESP) qui indique l'incorporation. Il est comparé à la SPD-O (voir la Figure 3) et trouvé correspondre à la règle 1 de la SPD, aussi outrepasse t-il. Le paquet est transposé dans une SA sur la base du SPI, vérifié en intégrité, et comparé aux sélecteurs de la SAD déduits de la règle 3 de la SPD. La fonction de transmission le passe alors à la couche suivante, parce qu'il n'est pas un paquet ESP.

Références normatives

[RFC0791] J. Postel, éd., "Protocole Internet - Spécification du protocole du programme Internet", STD 5, septembre 1981.

[RFC0792] J. Postel, "Protocole du message de contrôle Internet – Spécification du protocole du programme Internet DARPA", STD 5, septembre 1981.

[RFC1191] J. Mogul et S. Deering, "Découverte de la MTU de chemin", novembre 1990.

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

[RFC2253] M. Wahl, S. Kille et T. Howes, "Protocole léger d'accès à un répertoire (LDAPv3) : Représentation de chaîne UTF-8 des noms distinctifs", décembre 1997.

[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, D.S)*

[RFC2463] A. Conta, S. Deering, "Protocole de message de contrôle Internet (ICMPv6) pour le protocole Internet version 6 (IPv6)", décembre 1998. (*Obsolète, voir* RFC4443) *(D.S.)*

[RFC2475] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang et W. Weiss, "Architecture pour services différenciés", décembre 1998. *(MàJ par* RFC3260*)*

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

[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.

[RFC4305] D. Eastlake 3rd, "Exigences de mise en œuvre d'algorithme cryptographique pour l'encapsulation de charge utile de sécurité (ESP) et l'en-tête d'authentification (AH)", décembre 2005. *(P.S.)*(*Obsolète, voir* RFC4835)

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

[RFC4307] J. Schiller, "Algorithmes cryptographiques à utiliser avec la version 2 de l'échange de clés sur Internet (IKEv2)", décembre 2005. *(P.S.)*

Références informatives

[CoSa04] M. Condell et L. Sanchez, "Mise en application déterministe des politiques de sécurité non ordonnées", BBN Technical Memo 1346, mars 2004.

[RFC1704] N. Haller et R. Atkinson, "Authentification sur l'Internet", octobre 1994. *(Information)*

[RFC2003] C. Perkins, "Encapsulation de IP dans IP", RFC 2003, octobre 1996.

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

[RFC2474] K. Nichols, S. Blake, F. Baker et D. Black, "Définition du champ Services différenciés (DS) dans les en-têtes IPv4 et IPv6", décembre 1998. (*MàJ par* RFC3168, RFC3260) *(P.S.)*

[RFC2784] D. Farinacci, T. Li, S. Hanks, D. Meyer et P. Traina, "Encapsulation d'acheminement générique (GRE)", mars 2000.

[RFC2828] R. Shirey, "Glossaire de la sécurité sur l'Internet", FYI 36, mai 2000.

[RFC2983] D. Black, "Services différenciés et tunnels", octobre 2000. *(Information)*

[RFC3168] K. Ramakrishnan et autres, "Ajout de la notification explicite d'encombrement (ECN) à IP", septembre 2001. *(P.S.)*

[RFC3173] A. Shacham et autres, "Protocole de compression de charge utile IP (IPComp)", septembre 2001. *(P.S.)*

[RFC3260] D. Grossman, "Nouvelle terminologie et précisions pour Diffserv", avril 2002. *(Information)*

[RFC3697] J. Rajahalme et autres, "Spécification d'étiquette de flux IPv6", mars 2004. *(P.S.)*

[RFC3547] M. Baugher, B. Weis, T. Hardjono et H. Harney, "Le domaine d'interprétation de groupe", juillet 2003.

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

[RFC3884] J. Touch, L. Eggert, Y. Wang, "Utilisation du mode de transport IPsec pour l'acheminement dynamique", septembre 2004. *(Information)*

[RFC4607] H. Holbrook, B. Cain, "Diffusion groupée spécifique de source pour IP", août 2006. *(P.S.)*

[Sch94] B. Schneier, "Applied Cryptography", paragraphe 8.6, John Wiley & Sons, New York, NY, 1994.

[VK83] V.L. Voydock & S.T. Kent, "Security Mechanisms in High-level Networks", ACM Computing Surveys, Vol. 15, No. 2, juin 1983.

Adresse des auteurs

Stephen Kent
BBN Technologies
10 Moulton Street
Cambridge, MA 02138
USA
tél : +1 (617) 873-3988
mél : kent@bbn.com

Karen Seo
BBN Technologies
10 Moulton Street
Cambridge, MA 02138
USA
tél : +1 (617) 873-3152
mél : kseo@bbn.com

Remerciement

Le financement de la fonction d'édition des RFC est actuellement fourni par l'activité de soutien administratif de l'IETF (IASA, *Administrative Support Activity*).