Groupe de travail Réseau
Request for Comments : 4302
RFC rendue obsolètes : 2402
Catégorie : En cours de normalisation

S. Kent
BBN Technologies
décembre 2005
Traduction Claude Brière de L'Isle

En-tête d'authentification IP

Statut de ce mémoire
Le présent document spécifie un protocole Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et des suggestions pour son amélioration. Prière de se reporter à l'édition actuelle du STD 1 "Normes des protocoles officiels de l'Internet" pour connaître l'état de 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 de l'en-tête d'authentification (AH, *Authentication Header*), qui est conçue pour fournir des services d'authentification dans IPv4 et IPv6. Le présent document rend obsolète la RFC2402 (novembre 1998).

Table des Matières

1. Introduction

Le présent document suppose le lecteur familiarisé avec les termes et concepts décrits dans le document "Architecture de sécurité pour le protocole Internet" [RFC4301], auquel on se réfère ici sous le nom de document sur l'architecture de sécurité. En particulier, le lecteur devrait être familier avec les définitions des services de sécurité offerts par

l'encapsulation de charge utile de sécurité (ESP, *Encapsukating Security Payload*) [RFC4303] et l'en-tête d'authentification (AH) IP, le concept d'associations de sécurité, et les façons dont ESP peut être utilisé en conjonction avec l'en-tête d'authentification (AH) et les différentes options de gestion de clé disponibles pour ESP et AH.

Dans le présent document, les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" sont à interpréter comme décrit dans la [RFC 2119].

L'en-tête d'authentification (AH) IP est utilisé pour fournir la protection d'intégrité sans connexion et l'authentification de l'origine des données pour les datagrammes IP (ce qu'on appellera ici simplement "intégrité") et pour assurer la protection contre les répétitions. Ce dernier service, facultatif, peut être choisi par le receveur, lorsque une association de sécurité (SA, *Security Association*) est établie. (Le protocole par défaut exige que l'envoyeur incrémente le numéro de séquence utilisé pour l'anti-répétition, mais le service n'est efficace que si le receveur vérifie le numéro de séquence.) Cependant, pour faire usage du dispositif de numéro de séquence étendu d'une façon interopérable, AH impose une exigence aux protocoles de gestion de SA qui est qu'ils soient capables de négocier ce nouveau dispositif (voir au paragraphe 2.5.1).

AH fournit l'authentification pour autant de l'en-tête IP qu'il est possible, ainsi que pou les données de protocole du niveau suivant. Cependant, certains champs d'en-tête IP peuvent changer dans le transit et les valeurs de ces champs, lorsque le paquet arrive chez le receveur, peuvent n'être pas prévisibles par l'envoyeur. La valeurs de tels champs ne peut pas être protégée par AH. Donc, la protection fournie à l'en-tête IP par AH est à peu près. (Voir l'Appendice A.)

AH peut être appliqué seul, en combinaison avec l'encapsulation de charge utile de sécurité (ESP) IP [RFC4303], ou de façon incorporée (voir le document d'architecture de sécurité [RFC4301]). Les services de sécurité peuvent être fournis entre une paire d'hôtes communicants, entre une paire de passerelles de sécurité communicantes, ou entre une passerelle de sécurité et un hôte. ESP peut être utilisé pour fournir les mêmes service anti répétition et d'intégrité similaires, et il fournit aussi un service de confidentialité (chiffrement). La principale différence entre l'intégrité fournie par ESP et AH est l'extension de la couverture. Précisément, ESP ne protège aucun champ d'en-tête IP sauf si ces champs sont encapsulés par ESP (par exemple, via l'utilisation du mode tunnel). Pour des détails sur la façon d'utiliser AH et ESP dans divers environnements de réseau, voir le document d'architecture de sécurité [RFC4301].

La Section 7 donne un bref résumé des différences entre le présent document et la [RFC2402].

2. Format d'en-tête d'authentification

L'en-tête de protocole (IPv4, IPv6, ou extension IPv6) précédent immédiatement l'en-tête AH DEVRA contenir la valeur 51 dans son champ Protocole (IPv4) ou Prochain en-tête (IPv6, extension) [RFC2460]. La Figure 1 illustre le format pour AH.

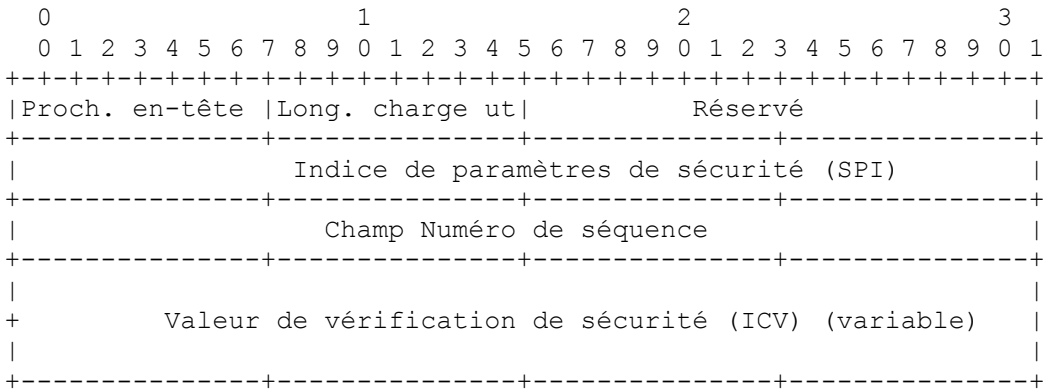


Figure 1 : Format d'AH

Le tableau suivant se réfère aux champs qui comprennent AH, (illustrés à la Figure 1) plus d'autres champs inclus dans le calcul d'intégrité, et illustre quels champs sont couverts par la ICV et ce qui est transmis.

	Nombre d'octets	Exigé [1]	Ce qui couvre l'intégrité	Ce qui est transmis
En-tête IP	variable	Oui	[2]	tout
Prochain en-tête	1	Oui	Oui	tout
Longueur de charge utile	1	Oui	Oui	tout
Réservé	2	Oui	Oui	tout
SPI	4	Oui	Oui	tout
N° de séquence (32 bits de mp)	4	Oui	Oui	tout
ICV	variable	Oui	Oui [3]	tout
datagramme IP [4]	variable	Oui	Oui	tout
N° de séquence (32 bits pf)	4	si ESN	Oui	non transmis
Bourrage ICV	variable	si nécessaire	Oui	non transmis

[1] - M = Obligatoire
[2] – Voir le paragraphe 3.3.3, "Calcul de la valeur de vérification d'intégrité", pour le détail des champs d'en-tête IP couverts.
[3] – Mis à zéro avant le calcul de l'ICV (l'ICV résultante est placée ici après le calcul)
[4] – En mode tunnel -> datagramme IP ; en mode transport -> prochain en-tête et données

Les paragraphes qui suivent définissent les champs qui composent le format AH. Tous les champs décrits ici sont obligatoires ; c'est-à-dire, ils sont toujours présents dans le format AH et sont inclus dans le calcul de la valeur de vérification d'intégrité (ICV, *Integrity Check Value*) (voir aux paragraphes 2.6 et 3.3.3).

Note : Tous les algorithmes de chiffrement utilisés dans IPsec supposent que leur entrée est dans l'ordre canonique des octets du réseau (voir l'Appendice de la [RFC0791]) et génèrent leur résultat dans l'ordre canonique des octets du réseau. Les paquets IP sont aussi transmis dans l'ordre des octets du réseau *(de gauche à droite)*.

AH ne contient pas de numéro de version, donc si il y a des soucis pour la rétro compatibilité, ils DOIVENT être réglés en utilisant un mécanisme de signalisation entre les deux homologues IPsec pour s'assurer de version d'AH compatibles, par exemple, IKE [RFC4306] ou par des mécanismes de configuration hors bande.

2.1 Prochain en-tête

Prochain en-tête est un champ de 8 bits qui identifie le type de la prochaine charge utile après l'en-tête d'authentification. La valeur de ce champ est choisie dans l'ensemble des numéros de protocole IP défini sur la page de la Toile de l'Autorité d'allocation des numéros de l'Internet (IANA). Par exemple, une valeur de 4 indique IPv4, une valeur de 41 indique IPv6, et une valeur de 6 indique TCP.

2.2 Longueur de charge utile

Ce champ de 8 bits spécifie la longueur de AH en mots de 32 bits (unités de 4 octets) moins "2". Donc, par exemple, si un algorithme d'intégrité donne une valeur d'authentification de 96 bits, ce champ Longueur sera "4" (3 mots de 32 bits de champs fixes plus 3 mots de 32 bits pour l'ICV, moins 2). Pour IPv6, la longueur totale de l'en-tête doit être un multiple d'unités de 8 octets. (Noter que bien que IPv6 [RFC2460] caractérise AH comme un en-tête d'extension, sa longueur est mesurée en mots de 32 bits, et non en mots de 64 bits utilisés par les autres en-têtes d'extension IPv6.) Voir au paragraphe 2.6, "Valeur de vérification d'intégrité (ICV)", les commentaires sur le bourrage de ce champ, et le paragraphe 3.3.3.2.1, "Bourrage d'ICV".

2.3 Réservé

Ce champ de 16 bits est réservé pour une utilisation future. Il DOIT être réglé à "zéro" par l'envoyeur, et il DEVRAIT être ignoré par le receveur. (Noter que sa valeur est incluse dans le calcul de l'ICV, mais est autrement ignorée par le receveur.)

2.4 Indice de paramètre de sécurité

L'indice de paramètre de sécurité (SPI, *Security Parameter Index*) est une valeur arbitraire de 32 bits qui est utilisée par un receveur pour identifier la SA à laquelle est lié un paquet entrant. Pour une SA d'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 (dans ce cas AH). Comme pour les SA en envoi individuel, la valeur du SPI est générée par le receveur, que la valeur soit suffisante pour identifier une SA par elle-même ou qu'elle doive être utilisée en conjonction avec la valeur du protocole IPsec est une affaire locale. Le champ SPI est obligatoire, et ce mécanisme de transposition du trafic entrant en SA en envoi individuel décrit ci-dessus DOIT être pris en charge par toutes les mises en œuvre de AH.

Si une mise en œuvre IPsec prend en charge la diffusion groupée, elle DOIT alors prendre en charge les SA en diffusion groupée en utilisant l'algorithme ci-dessous pour transposer les datagrammes IPsec entrants en SA. Les mises en œuvre qui ne prennent en charge 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 sûre, par exemple, de la [RFC3740], un contrôleur de groupe/serveur de clé central alloue unilatéralement les SPI des associations de sécurité du groupe. Cette allocation de SPI n'est ni négociée ni coordonnée avec les sous-systèmes de gestion de clés (par exemple, IKE) qui résident dans les systèmes d'extrémité individuels qui englobent le groupe. Par conséquent, il est possible qu'une association de sécurité de groupe et une association de sécurité d'envoi individuel puissent simultanément utiliser le même SPI. Une mise en œuvre IPsec capable de diffusion groupée DOIT correctement démultiplexer le trafic entrant même dans le contexte de collisions de SPI.

Chaque entrée dans la base de données d'associations de sécurité (SAD, *Security Association Database*) [RFC4301] doit indiquer si la recherche de SA fait usage des adresses IP de destination, ou 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, alors, l'entrée qui correspond aussi sur la base de la comparaison d'adresse de destination, ou de destination et de source (comme indiqué dans l'entrée de SAD) est la "plus longue" correspondance. Cela implique un rangement logique de la recherche dans la SAD, comme suit :

1. Chercher dans la SAD une correspondance {SPI, adresse de destination, adresse de source}. Si une entrée de SAD correspond, traiter alors le paquet AH entrant avec cette entrée de SAD correspondante. Autrement, passer à l'étape 2.

2. Chercher dans la SAD une correspondance {SPI, adresse de destination}. Si une entrée de SAD correspond, traiter alors le paquet AH entrant avec cette entrée de SAD correspondante. Autrement, passer à l'étape 3.

3. Chercher dans la SAD une correspondance seulement sur {SPI} si le receveur a choisi de tenir un seul espace de SPI pour AH et ESP, ou autrement sur {SPI, protocole}. Si une entrée de SAD correspond, traiter alors le paquet AH entrant avec cette entrée de SAD correspondante. Autrement, éliminer le paquet et enregistrer un événement à examiner.

En pratique, une mise en œuvre PEUT choisir toute méthode qui accélère cette recherche, bien que son comportement visible de l'extérieur DOIVE être fonctionnellement équivalent à avoir cherché dans la SAD dans l'ordre ci-dessus. Par exemple, une mise en œuvre logicielle pourrait indexer par le SPI dans un tableau de hachage par le SPI. Les entrées de SAD dans chaque liste reliée de baquet de tableau de hachage sont conservées triées pour avoir en premier les entrées de SAD qui ont les plus longs identifiants de SA. Les entrées de SAD qui ont les plus courts identifiants de SA sont triés de façon à ce qu'elles soient les dernières entrées dans la liste reliée. Une mise en œuvre fondée sur le matériel peut être capable d'effectuer intrinsèquement la recherche de la plus longue correspondance, en utilisant des caractéristiques de mémoire ternaire à contenu adressable (TCAM, *Ternary Content-Addressable Memory*) couramment disponibles.

L'indication qu'il est exigé que l'adresse de source et de destination correspondent à la transposition du trafic IPsec entrant vers les SA DOIT être réglée soit comme un effet collatéral de la configuration manuelle de SA, soit via la négociation en utilisant un protocole de gestion de SA, par exemple, IKE ou le domaine d'interprétation de groupe (GDOI, *Group Domain of Interpretation*) [RFC3547]. Normalement, les groupes de diffusion groupée spécifique de source (SSM, *Source-Specific Multicast*) [RFC4607] utilisent un triplet d'identifiant de SA composé d'un SPI, d'une adresse de diffusion groupée de destination, et d'une adresse de source. Une SA de groupe de diffusion groupée toute source exige seulement un SPI et une adresse de diffusion groupée de destination comme identifiant.

L'ensemble des valeurs de SPI dans la gamme de 1 à 255 est réservé par l'autorité d'allocation des numéros de l'Internet (IANA) pour de futures utilisations ; une valeur de SPI réservée ne sera normalement pas allouée par l'IANA sauf si l'utilisation de la valeur de SPI est spécifiée dans une RFC. La valeur de SPI de zéro (0) est réservée pour une utilisation locale, spécifique d'une mise en œuvre et NE DOIT PAS être envoyée sur le réseau. (Par exemple, une mise en œuvre de gestion de clé pourrait utiliser la valeur de SPI zéro pour signifier "Il n'existe pas d'association de sécurité" durant la période où la mise en œuvre de IPsec a demandé que son entité de gestion de clé établisse une nouvelle SA, mais où la SA n'a pas encore été établie.)

2.5 Numéro de séquence

Ce champ de 32 bits non signé contient une valeur de compteur qui augmente de un pour chaque paquet envoyé, c'est-à-dire, un numéro de séquence de paquet par SA. Pour une SA d'envoi individuel ou une SA de diffusion groupée d'un seul

envoyeur, l'envoyeur DOIT incrémenter ce champ pour chaque paquet transmis. Il est permis de partager une SA entre plusieurs envoyeurs, bien que ce soit généralement non recommandé. AH ne fournit pas de moyen de synchroniser les compteurs de paquet entre plusieurs envoyeurs ou de gérer de façon raisonnable un compteur de réception de paquet et une fenêtre dans le contexte d'envoyeurs multiples. Donc, pour une SA multi envoyeurs, le dispositif anti répétition de AH n'est pas disponible (voir aux paragraphes 3.3.2 et 3.4.3).

Le champ est obligatoire et DOIT toujours être présent même si le receveur ne choisit pas d'activer le service anti-répétition pour une SA spécifique. Le traitement du champ Numéro de séquence est à la discrétion du receveur, mais toutes les mises en œuvre de AH DOIVENT être capables d'effectuer le traitement décrit au paragraphe 3.3.2, "Génération du numéro de séquence", et du paragraphe 3.4.3, "Vérification du numéro de séquence". Donc, l'envoyeur DOIT toujours transmettre ce champ, mais le receveur n'a pas besoin d'agir dessus.

Les compteurs de l'envoyeur et du receveur sont initialisés à 0 lors de l'établissement d'une SA. (Le premier paquet envoyé en utilisant une certaine SA va avoir un numéro de séquence de 1 ; voir au paragraphe 3.3.2 les détails sur la façon dont le numéro de séquence est généré.) Si l'anti-répétition est activée (par défaut) le numéro de séquence transmis ne doit jamais revenir à zéro. Donc, les compteurs de l'envoyeur et du receveur DOIVENT être réinitialisés (en établissant une nouvelle SA et donc une nouvelle clé) avant la transmission du 2^32ème paquet sur une SA.

2.5.1 Numéro de séquence étendu (64 bits)

Pour prendre en charge les mises en œuvre IPsec à haut débit, une nouvelle option pour les numéros de séquence DEVRAIT être offerte, comme extension à l'actuelle, un champ de numéro de séquence de 32 bits. L'utilisation d'un numéro de séquence étendu (ESN, *Extended Sequence Number*) DOIT être négociée par un protocole de gestion de SA. Noter que dans IKEv2, cette négociation est implicite ; le réglage par défaut est ESN sauf si les numéros de séquence de 32 bits sont explicitement négociés. (Le dispositif ESN est applicable aux SA de diffusion groupée aussi bien que d'envoi individuel)

La facilité ESN permet l'utilisation d'un numéro de séquence de 64 bits pour une SA. (Voir l'Appendice B, "Numéros de séquence étendus (64 bits)", pour les détails.) Seuls les 32 bits de moindre poids du numéro de séquence sont transmis dans l'en-tête AH de chaque paquet, minimisant ainsi la tare du paquet. Les 32 bits de poids fort sont conservés au titre du compteur de numéros de séquence par l'émetteur et le receveur et sont inclus dans le calcul de l'ICV, mais ne sont pas transmis.

2.6 Valeur de vérification d'intégrité

La valeur de vérification d'intégrité (ICV, *Integrity Check Value*) pour ce paquet est un champ de longueur variable. Le champ doit être un multiple entier de 32 bits (IPv4 ou IPv6). Les détails du traitement de l'ICV sont décrits au paragraphe 3.3.3, "Calcul de la valeur de la vérification d'intégrité", et au paragraphe 3.4.4, "Vérification de la valeur de la vérification d'intégrité". Ce champ peut inclure un bourrage explicite, si nécessaire pour s'assurer que la longueur de l'en-tête AH est un multiple entier de 32 bits (IPv4) ou 64 bits (IPv6). Toutes les mises en œuvre DOIVENT accepter un tel bourrage et DOIVENT insérer seulement assez de bourrage pour satisfaire les exigences d'alignement de IPv4/IPv6. Les détails de la façon de calculer la longueur du bourrage requis sont donnés au paragraphe 3.3.3.2, "Bourrage". La spécification de l'algorithme de vérification de l'intégrité DOIT spécifier la longueur de l'ICV, les règles de comparaison et les étapes du traitement pour la validation.

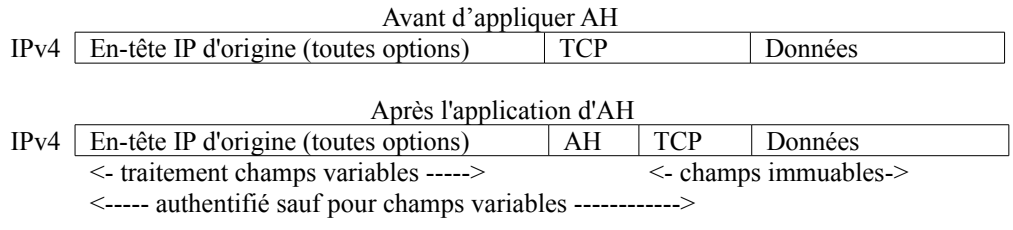
3. Traitement de l'en-tête d'authentification

3.1 Localisation de l'en-tête d'authentification

AH peut être employé de deux façons : en mode transport ou en mode tunnel. (Voir dans le document Architecture de sécurité la description de quand chacune devrait être utilisée.)

3.1.1 Mode Transport

En mode transport, AH est inséré après l'en-tête IP et avant un protocole de la couche suivante (par exemple, TCP, UDP, ICMP, etc.) ou avant tout autre en-tête IPsec qui a déjà été inséré. Dans le contexte de IPv4, cela appelle à placer AH après l'en-tête IP (et toutes options qu'il contient) mais avant le protocole de la couche suivante. (Noter que le terme "mode transport" ne devrait pas être mal construit en restreignant son utilisation à TCP et UDP.) Le diagramme suivant illustre le positionnement du mode transport AH pour un paquet IPv4 normal, sur la base de "avant et après".



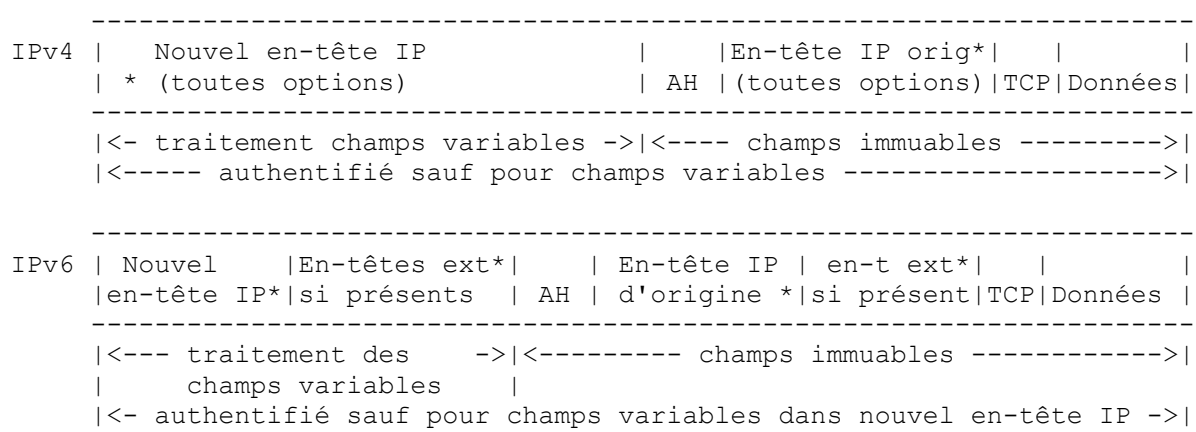
* = si présent, pourrait être avant AH, après AH, ou les deux

Les en-têtes ESP et AH peuvent être combinés dans divers modes. Le document d'architecture IPsec décrit les combinaisons d'associations de sécurité qui doivent être prises en charge.

Noter qu'en mode transport, pour les mises en œuvre "prises dans la pile" ou "prises sur le réseau", comme défini dans le document d'architecture de sécurité, les fragments IP entrants et sortants peuvent exiger qu'une mise en œuvre IPsec effectue un réassemblage/fragmentation IP supplémentaire afin de se conformer à la présente spécification et fournir une prise en charge IPsec transparente. Une attention particulière est requise pour effectuer de telles opérations au sein de ces mises en œuvre lorsque plusieurs interfaces sont utilisées.

3.1.2 Mode Tunnel

En mode tunnel, l'en-tête IP "interne" porte les adresses ultimes (IP) de source et de destination, tandis qu'un en-tête IP "externe" contient les adresses des "homologues IPsec", par exemple, les adresses des passerelles de sécurité. Des adresses internes et externes de versions IP mixtes sont permises, c'est-à-dire, IPv6 sur IPv4 et IPv4 sur IPv6. En mode tunnel, AH protège le paquet IP interne entier, y compris l'en-tête IP interne entier. La position de AH en mode tunnel, par rapport à l'en-tête IP externe, est la même que pour AH en mode transport. Le diagramme qui suit illustre le positionnement de AH en mode tunnel pour les paquets IPv4 et IPv6 normaux.



* = si présent, la construction des en-têtes/extensions IP externes et de la modification de l'en-tête/extensions IP internes

sont discutées dans le document d'architecture de sécurité.

3.2 Algorithmes d'intégrité

L'algorithme d'intégrité employé pour le calcul de l'ICV est spécifié par la SA. Pour une communication en point à point, les algorithmes d'intégrité convenables incluent les codes d'authentification de message (MAC, *Message Authentication Code*) chiffrés fondés sur des algorithmes de chiffrement symétriques (par exemple, [AES]) ou sur des fonctions de hachage unidirectionnel (par exemple, MD5, SHA-1, SHA-256, etc.). Pour une communication en diffusion groupée, diverses stratégies cryptographiques ont été développées pour assurer l'intégrité et les recherches continuent sur ce domaine.

3.3 Traitement de paquet sortant

En mode transport, l'envoyeur insère l'en-tête AH après l'en-tête IP et avant un en-tête de protocole de la couche suivante, comme décrit ci-dessus. En mode tunnel, les en-têtes/extensions IP externes et internes peuvent être en inter relation de diverses façons. La construction des en-têtes/extensions IP externes durant le processus d'encapsulation est décrite dans le document d'architecture de sécurité.

3.3.1 Recherche d'association de sécurité

AH s'applique à un paquet sortant seulement après qu'une mise en œuvre IPsec a déterminé que le paquet est associé à une SA qui invoque le traitement AH. Le processus de détermination de quel, s'il en est, traitement IPsec est appliqué au trafic sortant est décrit dans le document d'architecture de sécurité.

3.3.2 Génération de numéro de séquence

Le compteur de l'envoyeur est initialisé à 0 lorsque une SA est établie. L'envoyeur incrémente le numéro de séquence (ou ESN) pour cette SA et insère les 32 bits de moindre poids de la valeur dans le champ Numéro de séquence. Donc, le premier paquet envoyé en utilisant une certaine SA va contenir un numéro de séquence de 1.

Si l'anti répétition est activée (par défaut) l'envoyeur s'assure que le compteur n'a pas fait un cycle complet avant d'insérer la nouvelle valeur dans le champ Numéro de séquence. En d'autres termes, l'envoyeur NE DOIT PAS envoyer un paquet sur une SA si le faisant il causerait le retour à zéro du numéro de séquence. Une tentative de transmettre un paquet qui résulterait en un débordement du numéro de séquence est un événement qui doit faire l'objet d'un enregistrement dans le journal d'événements. L'entrée de l'enregistrement pour cet événement DEVRAIT inclure la valeur de SPI, la date et l'heure courantes, l'adresse de source, l'adresse de destination, et (dans IPv6) l'identifiant de flux en clair.

L'envoyeur suppose que l'anti répétition est activée par défaut, sauf notification contraire du receveur (voir au paragraphe 3.4.3) ou si la SA a été configurée en utilisant la gestion de clé manuelle. Donc, le comportement normal d'une mise en œuvre AH invite l'envoyeur à établir une nouvelle SA lorsque le numéro de séquence (ou ESN) revient à zéro, ou en anticipation de la fin de cycle de cette valeur.

Si l'anti répétition est désactivée (comme noté ci-dessus) l'envoyeur n'a pas besoin de surveiller ou rétablir le compteur, par exemple, dans le cas de gestion de clé manuelle (voir à la Section 5). Cependant, l'envoyeur incrémente quand même le compteur et lorsque il atteint la valeur maximum, le compteur revient à zéro. (Ce comportement est recommandé pour les SA multi envoyeurs, en diffusion groupée, sauf si des mécanismes anti répétition sortant du cadre de la présente norme ont été négociés entre l'envoyeur et le receveur.)

Si ESN (voir l'Appendice B) est choisi, seuls les 32 bits de moindre poids du numéro de séquence sont transmis dans le champ Numéro de séquence, bien que l'envoyeur et le receveur tiennent tous deux des compteurs ESN complets de 64 bits. Cependant, les 32 bits de poids fort sont inclus dans le calcul de l'ICV. Noter que si un receveur choisit de ne pas activer l'anti répétition pour une SA, le receveur NE DEVRAIT alors PAS négocier ESN dans un protocole de gestion de SA. L'utilisation de ESN crée pour les receveurs le besoin de gérer la fenêtre d'anti répétition (afin de déterminer la valeur correcte des bits de poids fort de l'ESN, qui sont employés dans le calcul de l'ICV) ce qui est généralement contraire à la notion de désactivation de l'anti répétition pour une SA.

3.3.3 Calcul de la valeur de la vérification d'intégrité

L'ICV AH est calculé sur :

- les champs d'en-tête IP ou d'extension avant l'en-tête AH qui sont soit immuables dans le transit, soit sont de valeur prévisible à l'arrivée au point d'extrémité pour la SA AH,

- o l'en-tête AH (Prochain en-tête, Longueur de charge utile, Réservé, SPI, Numéro de séquence (32 bits de moindre poids), et le ICV (qui est réglé à zéro pour ce calcul) et les octets explicites de bourrage (s'il en est)),
- o tout ce qui est après AH est supposé être immuable dans le transit,
- o les bits de poids fort de l'ESN (si il est employé) et tout bourrage implicite exigé par l'algorithme d'intégrité.

3.3.3.1 Traitement de champs variables

Si un champ peut être modifié durant le transit, la valeur du champ est réglée à zéro pour les besoins du calcul de l'ICV. Si un champ est mutable, mais si sa valeur au receveur (IPsec) est prévisible, cette valeur est alors insérée dans le champ pour les besoins du calcul de l'ICV. Le champ Valeur de vérification d'intégrité (ICV, *Integrity Check Value*) est aussi réglé à zéro en préparation de ce calcul. Noter qu'en remplaçant chaque valeur de champ par zéro, plutôt que d'omettre le champ, l'alignement est préservé pour le calcul de l'ICV. Aussi, l'approche du remplissage par des zéros assure que la longueur des champs qui sont ainsi traités ne peut pas être changée durant le transit, même si leur contenu n'est pas explicitement couvert par l'ICV.

Lorsque un nouvel en-tête d'extension ou d'option IPv4 sera créé, il sera défini dans sa propre RFC et DEVRAIT inclure (dans la Section des considérations sur la sécurité) des directives sur la façon dont il devrait être traité lors du calcul de l'ICV AH. Si la mise en œuvre IP (v4 ou v6) rencontre un en-tête d'extension qu'elle ne reconnaît pas, elle va éliminer le paquet et envoyer un message ICMP. IPsec ne va jamais voir le paquet. Si la mise en œuvre IPsec rencontre une option IPv4 qu'elle ne reconnaît pas, elle devrait mettre à zéro toute l'option, en utilisant le second octet de l'option comme longueur. Les options IPv6 (dans les en-têtes d'extension de destination ou les en-têtes d'extension bond par bond) contiennent un fanion qui indique la mutabilité, ce qui détermine le traitement approprié pour de telles options.

3.3.3.1.1 Calcul de l'ICV pour IPv4

3.3.3.1.1.1 Champs d'en-tête de base

Les champs d'en-tête IPv4 de base sont classés comme suit :

Immuables :
- o Version
- o Longueur d'en-tête Internet
- o Longueur totale
- o Identification
- o Protocole (ce devrait être la valeur pour AH.)
- o Adresse de source
- o Adresse de destination (sans acheminement de source lâche ou strict)

Mutable mais prévisible
- o Adresse de destination (avec acheminement de source lâche ou strict)

Mutable (mis à zéro avant le calcul d'ICV)
- o Codet de services différenciés (DSCP, *Differentiated Services Code Point*) (6 bits, voir [RFC2474])
- o Notification d'encombrement explicite (ECN, *Explicit Congestion Notification*) (2 bits, voir [RFC3168])
- o Fanions
- o Décalage de fragment
- o Durée de vie (TTL, *Time to Live*)
- o Somme de contrôle d'en-tête

DSCP – Les routeurs peuvent réécrire le champ DS comme nécessaire pour fournir un serveur local ou de bout en bout désiré, donc sa valeur à réception ne peut pas être prédite par l'envoyeur.

ECN – Cela va changer si un routeur sur le chemin subit de l'encombrement, et donc sa valeur à réception ne peut être prédite par l'envoyeur.

Fanions – Ce champ est exclu parce qu'un routeur intermédiaire peut établir le bit DF, même si la source ne l'a pas choisi.

Décalage de fragment - Comme AH est seulement appliqué aux paquets IP non fragmentés, le champ Décalage doit toujours être à zéro, et il est donc exclu (bien qu'il soit prévisible).

TTL – Il est changé en route par le traitement normal des routeurs, et donc sa valeur chez le receveur n'est pas prévisible par l'envoyeur.

Somme de contrôle d'en-tête – Elle va changer si il y a des changements dans les autres champs, et donc sa valeur à

réception ne peut pas être prédite par l'envoyeur.

3.3.3.1.1.2 Options

Pour IPv4 (à la différence de IPv6) il n'y a pas de mécanisme pour étiqueter les options comme mutables dans le transit. Donc, les options IPv4 sont énumérées explicitement à l'Appendice A et classées comme immuable, mutable mais prévisible, ou mutable. Pour IPv4, l'option entière est vue comme une unité ; de sorte que même si les champs de type et de longueur dans la plupart des options sont immuables dans le transit, si une option est classée comme mutable, l'option entière est mise à zéro pour les besoins du calcul de l'ICV.

3.3.3.1.2 Calcul d'ICV pour IPv6

3.3.3.1.2.1 Champs d'en-tête de base

Les champs d'en-tête IPv6 de base sont classés comme suit :

Immuable
- o Version
- o Longueur de charge utile
- o Prochain en-tête
- o Adresse de source
- o Adresse de destination (sans en-tête d'extension d'acheminement)

Mutable mais prévisible
- o Adresse de destination (avec en-tête d'extension d'acheminement)

Mutable (mis à zéro avant le calcul d'ICV)
- o DSCP (6 bits, voir la [RFC2474])
- o ECN (2 bits, voir la [RFC3168])
- o Étiquette de flux (*)
- o Limite de bonds

(*) L'étiquette de flux décrite dans AHv1 était mutable, et dans la [RFC2460] potentiellement mutable. Pour garder la compatibilité avec les mises en œuvre existantes de AH, l'étiquette de flux n'est pas incluse dans l'ICV dans AHv2.

3.3.3.1.2.2 En-têtes d'extension contenant des options

Les options IPv6 dans les en-têtes d'extension Bond par bond et Destination contiennent un bit qui indique si l'option peut changer (de façon imprévisible) durant le transit. Pour toute option dont le contenu peut changer en route, le champ "Données d'option" entier doit être traité comme des octets de valeur zéro lors du calcul ou lors de la vérification de l'ICV. Type d'option et Longueur des données d'option sont inclus dans le calcul d'ICV. Toutes les options pour lesquelles le bit indique l'immuabilité sont inclus dans le calcul d'ICV. Pour plus d'informations, voir la spécification d'IPv6 [RFC2460].

3.3.3.1.2.3 En-têtes d'extension ne contenant pas d'options

Les en-têtes d'extension IPv6 qui ne contiennent pas d'option sont explicitement mentionnés à l'Appendice A et classés comme immuable, mutable mais prévisible, ou mutable.

3.3.3.2 Bourrage et numéros de séquence étendus

3.3.3.2.1 Bourrage d'ICV

Comme mentionné au paragraphe 2.6, le champ ICV peut inclure un bourrage explicite si c'est exigé pour s'assurer que l'en-tête AH est un multiple de 32 bits (IPv4) ou 64 bits (IPv6). Si le bourrage est requis, sa longueur est déterminée par deux facteurs :
- la longueur de l'ICV,
- la version de protocole IP (v4 ou v6)

Par exemple, si le résultat de l'algorithme choisi est 96 bits, aucun bourrage n'est requis pour IPv4 ou IPv6. Cependant, si une longueur d'ICV différente est générée, due à l'utilisation d'un algorithme différent, un bourrage peut alors être nécessaire selon la longueur et la version du protocole IP. Le contenu du champ Bourrage est choisi arbitrairement par l'envoyeur. (Le bourrage est arbitraire, mais ne doit pas être aléatoire pour réaliser la sécurité.) Ces octets de bourrage sont inclus dans le calcul d'ICV, comptés au titre de la longueur de charge utile, et transmis à la fin du champ ICV pour permettre au receveur d'effectuer le calcul de l'ICV. L'inclusion de bourrage en plus de la quantité minimum requise pour satisfaire aux exigences d'alignement IPv4/IPv6 est interdite.

3.3.3.2.2. Bourrage de paquet implicite et ESN

Si l'option ESN est choisie pour une SA, les 32 bits de poids fort de l'ESN doivent être inclus dans le calcul de l'ICV. Pour les besoins du calcul de l'ICV, ces bits sont ajoutés (implicitement) immédiatement après la fin de la charge utile, et avant tout bourrage implicite de paquet.

Pour certains algorithmes de protection de l'intégrité, la chaîne d'octets sur laquelle est fait le calcul d'ICV doit être un multiple de la taille de bloc spécifiée par l'algorithme. Si la longueur du paquet IP (incluant AH et les 32 bits de poids fort de l'ESN, si il est activé) ne correspond pas à la taille de bloc exigée par l'algorithme, un bourrage implicite DOIT être ajouté à la fin du paquet, avant le calcul d'ICV. Les octets de bourrage DOIVENT avoir une valeur de zéro. La taille de bloc (et donc la longueur du bourrage) est spécifiée par la spécification de l'algorithme. Ce bourrage n'est pas transmis avec le paquet. Le document qui définit un algorithme d'intégrité DOIT être consulté pour déterminer si un bourrage implicite est requis comme décrit ci-dessus. Si le document ne spécifie pas de réponse à cette interrogation, on supposera par défaut que le bourrage implicite est exigé (autant que nécessaire pour faire correspondre la longueur du paquet à la taille de bloc de l'algorithme). Si les octets de bourrage sont nécessaires, mais si l'algorithme ne spécifie pas le contenu du bourrage, les octets de bourrage DOIVENT avoir une valeur de zéro.

3.3.4 Fragmentation

Si nécessaire, la fragmentation IP survient après le traitement AH au sein d'une mise en œuvre IPsec. Donc, le mode transport AH est seulement appliqué aux datagrammes IP entiers (pas aux fragments IP). Un paquet IPv4 auquel AH a été appliqué peut lui-même être fragmenté par les routeurs en chemin, et de tels fragments doivent être réassemblés avant le traitement AH chez un receveur. (Cela ne s'applique pas à IPv6, où il n'y a pas de fragmentation initiée par un routeur.) En mode tunnel, AH est appliqué à un paquet IP, dont la charge utile peut être un paquet IP fragmenté. Par exemple, une passerelle de sécurité ou une mise en œuvre IPsec "prise dans la pile" ou "prise sur le fil" (voir le document d'architecture de sécurité pour les détails) peut appliquer le mode tunnel AH à de tels fragments.

Note : Pour le mode transport -- comme mentionné à la fin du paragraphe 3.1.1, les mises en œuvre prises dans la pile et prises sur le fil peuvent devoir faire d'abord réassembler un paquet fragmenté par la couche IP locale, puis appliquer IPsec, et ensuite fragmenter le paquet résultant.

Note : Pour IPv6 -- pour les mises en œuvre prises dans la pile et prises sur le fil, il sera nécessaire d'examiner tous les en-tête d'extensions pour déterminer si il y a un en-tête de fragmentation et si le fanion More ou le Décalage de fragment sont différents de zéro. Si il en est ainsi, ce paquet doit être réassemblé avant le traitement IPsec.

La fragmentation, qu'elle soit effectuée par une mise en œuvre IPsec ou par des routeurs le long du chemin entre les homologues IPsec, réduit significativement les performances. De plus, l'exigence qu'un receveur AH accepte les fragments pour le réassemblage crée des vulnérabilités au déni de service. Donc, une mise en œuvre de AH PEUT choisir de ne pas prendre en charge la fragmentation et peut marquer les paquets transmis avec le bit DF, pour faciliter la découverte de la MTU de chemin (PMTU, *Path MTU*). Dans tous les cas, une mise en œuvre AH DOIT prendre en charge la génération de messages PMTU ICMP (ou l'équivalent en signalisation interne pour les mises en œuvre d'hôte natives) pour minimiser la probabilité de fragmentation. Les détails de la prise en charge requise pour la gestion de la MTU figurent dans le document d'architecture de sécurité.

3.4 Traitement de paquet entrant

Si plus d'un en-tête IPsec/extension est présent, le traitement pour chacun ignore (ne met pas à zéro, n'utilise pas) tous les en-têtes IPsec appliqués après l'en-tête traité.

3.4.1 Réassemblage

Si il est exigé, le réassemblage est effectué avant le traitement AH. Si un paquet offert au traitement AH apparaît être un fragment IP, c'est-à-dire, si le champ OFFSET n'est pas à zéro ou si le fanion MORE FRAGMENTS est établi, le receveur DOIT éliminer le paquet ; ceci est un événement enregistrable. L'entrée d'enregistrement pour cet événement DEVRAIT inclure la valeur du SPI, la date/heure, l'adresse de source, l'adresse de destination, et (dans IPv6) l'identifiant de flux.

Note : Pour le réassemblage de paquet, la spécification IPv4 actuelle N'EXIGE PAS la mise à zéro du champ OFFSET ni la mise à zéro du fanion MORE FRAGMENTS. Afin qu'un paquet réassemblé soit traité par IPsec (par opposition à être éliminé comme un fragment apparent) le code IP doit faire ces deux choses après le réassemblage d'un paquet.

3.4.2 Recherche d'association de sécurité

À réception d'un paquet contenant un en-tête d'authentification IP, le receveur détermine la SA appropriée (unidirectionnelle) via une recherche dans la SAD. Pour une SA d'envoi individuel, cette détermination se fonde sur le SPI ou le SPI plus le champ Protocole, comme décrit au paragraphe 2.4. Si une mise en œuvre prend en charge le trafic de diffusion groupée, l'adresse de destination est aussi employée dans la recherche (en plus du SPI) et l'adresse de l'envoyeur peut aussi être employée, comme décrit au paragraphe 2.4. Ce processus est décrit plus en détails dans le document d'architecture de sécurité. L'entrée de SAD pour la SA indique aussi si le champ Numéro de séquence sera vérifié et si des numéros de séquence de 32 ou 64 bits sont employés pour la SA. L'entrée de SAD pour la SA spécifie aussi le ou les algorithmes employés pour le calcul de l'ICV, et indique la clé requise pour valider l'ICV.

Si aucune association de sécurité valide n'existe pour ce paquet, le receveur DOIT éliminer le paquet ; ceci est un événement enregistrable. L'entrée d'enregistrement pour cet événement DEVRAIT inclure la valeur de SPI, la date/heure, l'adresse de source, l'adresse de destination, et (dans IPv6) l'identifiant de flux.

(Noter que le trafic de gestion de SA, comme les paquets IKE, n'a pas besoin d'être traité sur la base du SPI, c'est-à-dire, on peut démultiplexer ce trafic séparément sur la base des champs Prochain protocole et Accès, par exemple.)

3.4.3 Vérification du numéro de séquence

Toutes les mises en œuvre de AH DOIVENT prendre en charge le service anti répétition, bien que son utilisation puisse être activée ou désactivé par le receveur pour chaque SA. L'anti répétition est applicable aux SA d'envoi individuel aussi bien que de diffusion groupée. Cependant, la présente norme ne spécifie pas de mécanisme pour assurer l'anti répétition pour une SA multi envoyeurs (en envoi individuel ou en diffusion groupée). En l'absence de négociation (ou de configuration manuelle) d'un mécanisme d'anti répétition pour une telle SA, il est recommandé qu'envoyeur et receveur vérifient que le numéro de séquence pour la SA soit désactivé (via négociation ou configuration manuelle) comme noté ci-dessous.

Si le receveur n'active pas l'anti répétition pour une SA, aucune vérification d'entrée n'est effectuée sur le numéro de séquence. Cependant, du point de vue de l'envoyeur, on suppose par défaut que l'anti répétition est activée chez le receveur. Pour éviter que l'envoyeur fasse une surveillance inutile de numéro de séquence et d'établissement de SA (voir au paragraphe 3.3.2, "Génération de numéro de séquence") si un protocole d'établissement de SA comme IKE est employé, le receveur DEVRAIT le notifier à l'envoyeur, durant l'établissement de SA, si le receveur ne fournit pas de protection anti répétition.

Si le receveur a activé le service d'anti répétition pour cette SA, le compteur de réception de paquets pour la SA DOIT être initialisé à zéro lors de l'établissement de la SA. Pour chaque paquet reçu, le receveur DOIT vérifier que le paquet contient un numéro de séquence qui ne duplique pas le numéro de séquence de tous les autres paquets reçus durant la vie de cette SA. Ceci DEVRAIT être la première vérification AH appliquée à un paquet après qu'il a été confronté à une SA, pour accélérer le rejet des paquets dupliqués.

Les dupliqués sont rejetés par l'utilisation d'une fenêtre de réception glissante. La mise en œuvre de la fenêtre est une affaire locale, mais le texte qui suit décrit les fonctions que la mise en œuvre doit posséder.

Le bord "droit" de la fenêtre représente la plus forte valeur de numéro de séquence validée reçue sur cette SA. Les paquets qui contiennent des numéros de séquence inférieurs au bord "gauche" de la fenêtre sont rejetés. Les paquets qui entrent dans la fenêtre sont confrontés à une liste de paquets reçus dans la fenêtre.

Si l'option ESN est choisie pour une SA, seuls les 32 bits de moindre poids du numéro de séquence sont explicitement transmis, mais le receveur emploie le numéro de séquence complet calculé en utilisant les 32 bits de poids fort pour la SA indiquée (à partir de son compteur local) lorsque il vérifie le numéro de séquence reçu par rapport à la fenêtre de réception. En construisant le numéro de séquence complet, si les 32 bits de moindre poids portés dans le paquet sont de valeur inférieure au 32 bits de moindre poids du compteur de numéro de séquence du receveur, celui-ci suppose que les 32 bits de poids fort ont été incrémentés, passant à un nouveau sous espace de numéro de séquence. (Cet algorithme s'accommode des trous de réception pour une seule SA jusqu'à 2**32-1 paquets. Si un trou plus grand se produit, des vérifications heuristiques supplémentaires pour la resynchronisation du compteur de numéros de séquence du receveur PEUVENT être employées, comme décrit à l'Appendice B.)

Si le paquet reçu tombe dans la fenêtre et n'est pas un dupliqué, ou si le paquet est à droite de la fenêtre, le receveur procède alors à la vérification de l'ICV. Si la validation de l'ICV échoue, le receveur DOIT éliminer le datagramme IP reçu comme invalide. C'est un événement enregistrable. L'entrée d'enregistrement pour cet événement DEVRAIT inclure la valeur de SPI, la date/heure, l'adresse de source, l'adresse de destination, le numéro de séquence, et (dans IPv6) l'identifiant de flux. La fenêtre de réception n'est mise à jour que si la vérification d'ICV réussit.

Une taille MINIMUM de fenêtre de 32 paquets DOIT être supportée, mais une taille de fenêtre de 64 est préféré et DEVRAIT être employée par défaut. Une autre taille de fenêtre (plus grande que le MINIMUM) PEUT être choisie par le receveur. (Le receveur NE notifie PAS à l'envoyeur la taille de fenêtre.) La fenêtre de réception devrait être augmentée pour les environnements à grande vitesse, sans considération des questions d'assurance. Les valeurs minimum et recommandées de taille de fenêtre de réception pour les appareils à très grande vitesse (par exemple, plusieurs gigabit/s) ne sont pas spécifiées par la présente norme.

3.4.4 Valeur de vérification d'intégrité

Le receveur calcule l'ICV sur les champs appropriés du paquet, en utilisant l'algorithme d'intégrité spécifié, et vérifie que c'est le même que l'ICV inclus dans le champ ICV du paquet. Les détails du calcul sont donnés ci-dessous.

Si l'ICV calculé et reçu correspond, le datagramme est alors valide, et est accepté. Si l'essai échoue, le receveur DOIT alors éliminer le datagramme IP reçu comme invalide. C'est un événement enregistrable. L'entrée d'enregistrement DEVRAIT inclure la valeur de SPI, la date/heure de réception, l'adresse de source, l'adresse de destination, et (dans IPv6) l'identifiant de flux.

Note de mise en œuvre : les mises en œuvre peuvent utiliser toutes les étapes qui aboutissent au même résultat que l'ensemble d'étapes suivant.
Commencer par sauvegarder la valeur d'ICV et la remplacer (mais sans aucun champ de bourrage de l'ICV) par des zéros. Mettre à zéro tous les autres champs qui peuvent avoir été modifiés durant le transit. (Voir au paragraphe 3.3.3.1, "Traitement de champs mutables", une discussion des champs mis à zéro avant d'effectuer le calcul d'ICV.) Si l'option ESN est choisie pour cette SA, ajouter les 3 bits de poids fort de l'ESN après la fin du paquet. Vérifier la longueur totale du paquet (comme décrit ci-dessus) et si elle exige un bourrage implicite sur la base des exigences de l'algorithme d'intégrité, ajouter des octets à zéro à la fin du paquet (après l'ESN si il est présent) comme nécessaire. Effectuer le calcul d'ICV et comparer le résultat à la valeur sauvegardée, en utilisant les règles de comparaison définies par la spécification de l'algorithme. (Par exemple, si une signature numérique et un hachage unidirectionnel sont utilisés pour le calcul de l'ICV, le processus de confrontation est plus complexe.)

4. Révision

Tous les systèmes qui mettent en œuvre AH vont appliquer la révision. Cependant, si AH est incorporé dans un système qui accepte la révision, la mise en œuvre AH DOIT aussi accepter la révision et DOIT permettre à un administrateur de système d'activer ou de désactiver la révision pour AH. Pour la plus grande part, la granularité de la révision est une affaire locale. Cependant, plusieurs événement qui peuvent faire l'objet de révision sont identifiés dans la présente spécification, et pour chacun de ces événements un ensemble minimum d'informations qui DEVRAIENT être incluses dans un enregistrement de révision est défini. Des information supplémentaires PEUVENT aussi être incluses dans l'enregistrement de révision pour chacun de ces événements, et des événements supplémentaires, non explicitement invoqués dans cette spécification, PEUVENT aussi résulter en des entrées d'enregistrement de révision. Il n'est pas exigé que le receveur transmette de message à l'envoyeur prétendu en réponse à la détection d'un événement susceptible de révision, à cause du potentiel de déni de service induit par une telle action.

5. Exigences de conformité

Les mises en œuvre qui revendiquent la conformité à la présente spécification DOIVENT pleinement mettre en œuvre la syntaxe et le traitement de AH décrits ici pour le trafic en envoi individuel, et DOIVENT se conformer à toutes les exigences du document d'architecture de sécurité [RFC4301]. De plus, si une mise en œuvre prétend prendre en charge le trafic en diffusion groupée, elle DOIT se conformer aux exigences supplémentaires spécifiées pour la prise en charge d'un tel trafic. Si la clé utilisée pour calculer un ICV est distribuée manuellement, le provisionnement correct du service anti répétition exigera une maintenance correcte de l'état du compteur chez l'envoyeur, jusqu'à ce que la clé soit remplacée, et il n'y aura vraisemblablement pas de disposition de récupération automatique du compteur si le débordement du compteur est imminent. Donc, une mise en œuvre conforme NE DEVRAIT PAS fournir ce service en conjonction avec des SA qui sont chiffrées manuellement.

Les algorithmes de mise en œuvre obligatoire à utiliser avec AH sont décrits dans une RFC distincte [RFC4305], pour faciliter la mise à jour des exigences d'algorithmes indépendamment du protocole lui-même. Des algorithmes supplémentaires, au delà de ceux obligatoires pour AH, PEUVENT être pris en charge.

6. Considérations pour la sécurité

La sécurité est au centre de la conception de ce protocole, et ces considérations de sécurité imprègnent la présente spécification. Des aspects supplémentaires de la sécurité concernant l'utilisation du protocole IPsec sont exposés dans le document d'architecture de la sécurité.

7. Différences avec la RFC 2402

Le présent document diffère de la [RFC2402] sous les aspects suivants.

- o SPI – modifié pour spécifier un algorithme uniforme pour la recherche de SAD pour les SA en envoi individuel et en diffusion groupée, couvrant une plus large gamme de technologies de diffusion groupée. Pour l'envoi individuel, le SPI peut être utilisé seul pour choisir une SA, ou peut être combiné avec le protocole, au choix du receveur. Pour les SA de diffusion groupée, le SPI est combiné avec l'adresse de destination, et facultativement avec l'adresse de source pour choisir une SA.
- o Numéro de séquence étendu – ajoute une nouvelle option de numéro de séquence à 64 bits pour les communications à très grande vitesse. Les exigences pour le traitement d'envoi et de réception pour les SA de diffusion groupée et d'envoyeur multiple sont précisées.
- o Les références à des algorithmes obligatoires sont renvoyées à un document distinct [RFC4305].

8. Remerciements

L'auteur tient à remercier de ses contributions Ran Atkinson, qui a joué un rôle critique dans les activités IPsec initiales, et qui est l'auteur de la première série de normes IPsec : les RFC 1825 à 1827. Karen Seo mérite des remerciements particuliers pour avoir apporté son aide à l'édition de cette version de la spécification ainsi que des précédentes. Ont aussi droit à la gratitude de l'auteur les membres des groupes de travail IPsec et MSEC qui ont contribué au développement de la spécification de ce protocole.

9. Références

9.1 Références normatives

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

[RFC1108] S. Kent, "Options de sécurité du Ministère US de la défense pour le protocole Internet", novembre 1991. *(Historique)*

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

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

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

[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)

9.2 Références pour information

[AES] National Institutes of Standards et Technology, "Advanced Encryption Standard (AES)", Federal Information Processing Standard 197, , 26 novembre 2001.

[RFC1063] J. Mogul, C. Kent, C. Partridge et K. McCloghrie, "Options IP de découverte de MTU", juillet 1988. (*Obsolète,* voir RFC1191)

[RFC1122] R. Braden, "Exigences pour les hôtes Internet – couches de communication", STD 3, octobre 1989. *(MàJ par la* RFC6633)

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

[RFC1385] Z. Wang, "EIP : le protocole Internet étendu", novembre 1992. *(Information, Remplacée par la* RFC6814)

[RFC1393] G. Malkin, "Traceroute en utilisant une option IP", janvier 1993. *(Expérimentale, Remplacée par la* RFC6814)

[RFC1770] C. Graff , "Option IPv4 pour livraison multi-destination dirigée par l'envoyeur", mars 1995. *(Remplacée par* RFC6814)

[RFC2113] D. Katz, "Option d'alerte de routeur IP", février 1997.

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

[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.)*

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

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

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

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

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

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

Appendice A Mutabilité des en-têtes IP Options/Extension

A1 Options IPv4

Ce tableau montre comment les options IPv4 sont classées par rapport à la "mutabilité". Lorsque deux références sont fournies, la seconde supplante la première. Ce tableau se fonde en partie sur les informations fournies dans la RFC 1700, "Numéros alloués", (octobre 1994).

Copie	Classe	N° d'option	Nom	Référence
IMMUABLE – incluse dans le calcul d'ICV				
0	0	0	Fin de liste d'options	[RFC791]
0	0	1	Pas de fonctionnement	[RFC791]
1	0	2	Sécurité	[RFC1108] (historique mais utilisée)
1	0	5	Sécurité étendue	[RFC1108] (historique mais utilisée)
1	0	6	Sécurité commerciale	
1	0	20	Alerte de routeur	[RFC2113]
1	0	21	Livraison multi destination dirigée par l'envoyeur	[RFC1770]
MUTABLE – mise à zéro				
1	0	3	Route de source lâche	[RFC791]
0	2	4	Horodatage	[RFC791]
0	0	7	Chemin enregistré	[RFC791]
1	0	9	Route de source stricte	[RFC791]
0	2	18	Traceroute	[RFC1393]
EXPERIMENTAL, SUPERCEDED – mise à zéro				
1	0	8	Identifiant de flux	[RFC791, RFC1122 (Host Req)]
0	0	11	Sondage de MTU	[RFC1063, RFC1191 (PMTU)]
0	0	12	Réponse de MTU	[RFC1063, RFC1191 (PMTU)]
1	0	17	Protocole Internet étendu	[RFC1385, RFC2460 (IPv6)]
0	0	10	Mesure expérimentale	
1	2	13	Contrôle de flux expérimental	
1	0	14	Contrôle d'accès expérimental	
0	0	15	???	
1	0	16	Descripteur de trafic IMI	
1	0	19	Extension d'adresse	

Note : L'utilisation de l'option Alerte de routeur est potentiellement incompatible avec l'utilisation de IPsec. Bien que l'option soit immuable, son utilisation implique que chaque routeur le long du chemin d'un paquet va "traiter" le paquet et par conséquent peut le changer. Cela va se produire bond par bond lorsque le paquet va d'un routeur à

l'autre. Avant d'être traité par l'application à laquelle le contenu de l'option est destiné (par exemple, protocole de réservation de ressource (RSVP)/protocole de gestion de groupe Internet (IGMP)) le paquet devrait rencontrer le traitement AH. Cependant, le traitement AH va exiger que chaque routeur le long du chemin soit membre d'une SA de diffusion groupée définie par le SPI. Cela peut poser problème aux paquets qui ne sont pas strictement à acheminement de source, et cela exige des techniques de prise en charge de la diffusion groupée qui ne sont pas disponibles actuellement.

Note : L'ajout ou la suppression d'étiquettes de sécurité (par exemple, Option de sécurité de base (BSO, *Basic Security Option*), Option de sécurité étendue (ESO, *Extended Security Option*), ou Option de sécurité commerciale du protocole Internet (CIPSO, *Commercial Internet Protocol Security Option*)) par des systèmes sur le chemin d'un paquet entre en conflit avec la classification de ces options IP comme immuables et est incompatible avec l'utilisation d'IPsec.

Note : Les options Fin de liste d'options DEVRAIENT être répétées autant que nécessaire pour s'assurer que l'en-tête IP se termine sur une limite de quatre octets afin de s'assurer qu'il n'y a pas d'octet non spécifié qui pourrait être utilisé pour un canal couvert.

A.2 En-têtes d'extension IPv6

Ce tableau montre comment les en-têtes d'extension IPv6 sont classés par rapport à la "mutabilité".

Nom d'option/extension	**Référence**
Mutable mais prévisible – inclus dans le calcul d'ICV : Routing (Type 0)	
	RFC2460]
Le bit indique si l'option est mutable (changement imprévisible durant le transit) : Hop-by-Hop options Destination options	
	RFC2460]
	RFC2460]
Non applicable : Fragmentation	
	RFC2460]

Options – Les options IPv6 dans les en-têtes d'extension Bond par bond et Destination contiennent un bit qui indique si l'option peut changer (de façon imprévisible) durant le transit. Pour toute option pour laquelle le contenu peut changer en route, le champ entier "Données d'option" doit être traité comme des octets de valeur zéro lors du calcul ou de la vérification de l'ICV. Le Type d'option et Longueur de données d'option sont inclus dans le calcul d'ICV. Toutes les options pour lesquelles le bit indique l'immuabilité sont incluses dans le calcul de l'ICV. Voir plus d'informations dans la spécification d'IPv6 [RFC2460].

Routing (Type 0) – L'en-tête d'acheminement IPv6 "Type 0" va réarranger les champs d'adresse dans le paquet durant le transit de source à destination. Cependant, le contenu du paquet comme il va apparaître au receveur est connu de l'envoyeur et de tous les bons intermédiaires. Donc, l'en-tête d'acheminement IPv6 "Type 0" est inclus dans le calcul de la valeur de vérification d'intégrité (ICV) comme mutable mais prévisible. L'envoyeur doit ordonner le champ afin qu'il apparaisse comme il le fera chez le receveur, avant d'effectuer le calcul de l'ICV.

Fragmentation – La fragmentation se produit après le traitement de sortie IPsec (paragraphe 3.3) et le réassemblage intervient avant le traitement IPsec d'entrée (paragraphe 3.4). De sorte que l'en-tête d'extension Fragmentation, si il existe, n'est pas vu par IPsec.

Noter que sur le côté receveur, la mise en œuvre IP pourrait laisser l'en-tête d'extension Fragmentation en place lorsque elle fait le réassemblage. Si cela arrive, lorsque AH reçoit le paquet, avant de faire le traitement de l'ICV, AH DOIT "retirer" (ou sauter) cet en-tête et changer le champ "Prochain en-tête" de l'en-tête précédent pour qu'il soit le champ "Prochain en-tête" dans l'en-tête d'extension Fragmentation.

Noter que du côté envoyeur, la mise en œuvre IP pourrait donner au code IPsec un paquet avec un en-tête d'extension Fragmentation avec un décalage de 0 (premier fragment) et un fanion Fragments à suivre de 0 (dernier fragment). Si cela arrive, avant de faire le traitement d'ICV, AH DOIT alors d'abord "retirer" (ou sauter) cet en-tête et changer le champ "Prochain en-tête" de l'en-tête précédent en le champ "Prochain en-tête" dans l'en-tête d'extension Fragmentation.

Appendice B Numéros de séquence étendus (64 bits)

B.1 Généralités

Le présent appendice décrit un schéma de numéro de séquence étendu (ESN, *Extended Sequence Number*) à utiliser avec IPsec (ESP et AH) qui emploie un numéro de séquence de 64 bits, mais dans lequel seulement les 32 bits de moindre poids sont transmis au titre de chaque paquet. Il couvre le schéma de fenêtre utilisé pour détecter les paquets répétés et la détermination des bits de poids fort du numéro de séquence qui sont utilisés à la fois pour le rejet des répétés et pour le calcul de l'ICV. Il expose aussi un mécanisme pour traiter les pertes de synchronisation relatives aux bits de poids fort (non transmis).

B.2 Fenêtre anti-répétition

Le receveur va tenir une fenêtre anti répétition de taille W. Cette fenêtre va limiter la quantité de déclassement que peut subir un paquet par rapport au paquet de plus fort numéro de séquence qui a été authentifié jusqu'alors. (Aucune exigence n'est établie quant aux tailles minimum ou recommandées de cette fenêtre, au delà des valeurs de 32 et 64 paquets déjà établies pour la fenêtre de numéro de séquence de 32 bits. Cependant, il est suggéré qu'une mise en œuvre adapte ces valeurs en accord avec la vitesse de l'interface supportée par une mise en œuvre qui utilise l'option ESN. Aussi, l'algorithme décrit ci-dessous suppose que la fenêtre n'est pas supérieure à 2^31 paquets en largeur.) Tous les 2^32 numéros de séquence associés à une valeur fixée pour les 32 bits de poids fort (Seqh) seront ci-après appelés un sous espace de numéro de séquence. Le tableau qui suit fait la liste des variables pertinentes et leur définition.

Nom de la variable	Taille (en bits)	Signification
W	32	Taille de fenêtre
T	64	Plus fort numéro de séquence authentifié jusque là, limite supérieure de fenêtre
Tl	32	32 bits de moindre poids de T
Th	32	32 bits de poids fort de T
B	64	Limite inférieure de fenêtre
Bl	32	32 bits de moindre poids de B
Bh	32	32 bits de poids fort de B
Seq	64	Numéro de séquence du paquet reçu
Seql	32	32 bits de moindre poids de Seq
Seqh	32	32 bits de poids fort de Seq

Quand on effectue la vérification d'anti répétition, ou quand on détermine quels bits de poids fort utiliser pour authentifier un paquet entrant, il y a deux cas :

- Cas A : Tl ≥ (W - 1). Dans ce cas, la fenêtre est dans un sous espace de numéro de séquence. (Figure 2)
- Cas B : Tl < (W - 1). Dans ce cas, la fenêtre s'étend sur deux sous espaces de numéro de séquence. (Figure 2)

Dans les figures ci-dessous, la ligne du bas ("----") montre deux sous espaces consécutifs de numéro de séquence, les zéros indiquant le début de chaque sous espace. Les deux lignes plus courtes au dessus d'elle montrent les bits de poids fort qui s'appliquent. La ligne "====" représente la fenêtre. La ligne "****" représente les futurs numéros de séquence, c'est-à-dire, ceux au delà du plus fort numéro de séquence authentifié courant (ThTl).

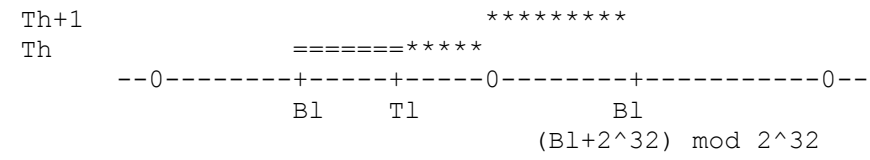


Figure 2 -- Cas A

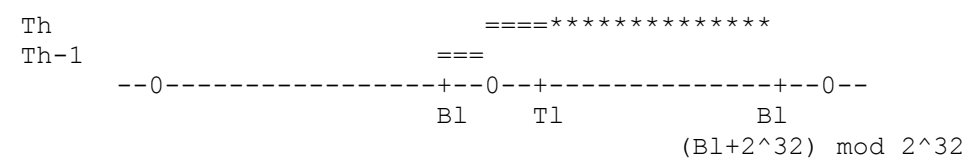


Figure 2 -- Cas B

B.2.1 Gestion et utilisation de la fenêtre anti-répétition

La fenêtre anti répétition peut être vue comme une chaîne de bits où "W" définit la longueur de la chaîne. W = T - B + 1 et ne peut pas excéder 2^32 - 1 en valeur. Le bit du bas correspond à B et le bit du haut correspond à T, et chaque numéro de séquence de Bl à Tl est représenté par un bit correspondant. La valeur du bit indique si un paquet avec ce numéro de séquence a ou non été reçu et authentifié, de sorte que les répétitions peuvent être détectées et rejetées.

Quand un paquet avec un numéro de séquence de 64 bits (Seq) supérieur à T est reçu et validé,
+ B est augmenté de (Seq - T)
+ (Seq - T) bits sont abandonnés sur le côté inférieur de la fenêtre
+ (Seq - T) bits sont ajoutés sur le côté supérieur de la fenêtre
+ Le bit supérieur est réglé à indiquer qu'un paquet avec ce numéro de séquence a été reçu et authentifié
+ Les nouveaux bits entre T et le bit supérieur sont réglé à indiquer qu'aucun paquet avec ces numéros de séquence n'ont encore été reçus.
+ T est réglé au nouveau numéro de séquence

Quand on vérifie les paquets répétés,
+ Dans le cas A : si Seql ≥ Bl (où Bl = Tl - W + 1) ET Seql ≤ Tl, on vérifie alors le bit correspondant dans la fenêtre pour voir si ce Seql a déjà été vu. Si oui, rejeter le paquet. Sinon, effectuer une vérification d'intégrité (voir à l'Appendice B2.2 la détermination de Seqh).
+ Dans le cas B : Si Seql ≥ Bl (où Bl = Tl - W + 1) OU Seql ≤ Tl, on vérifie alors le bit correspondant dans la fenêtre pour voir si ce Seql a déjà été vu. Si oui, rejeter le paquet. Sinon, effectuer une vérification d'intégrité (voir à l'Appendice B2.2 la détermination de Seqh).

B.2.2 Détermination des bits de poids fort (Seqh) du numéro de séquence

Comme seulement "Seql" sera transmis avec le paquet, le receveur doit déduire et retracer le sous espace de numéro de séquence dans lequel tombe chaque paquet, c'est-à-dire, déterminer la valeur de Seqh. Les équations suivantes définissent comment choisir Seqh dans des conditions "normales"; voir à l'Appendice B3 une discussion sur la façon de récupérer d'une perte extrême de paquets.

+ Dans le cas A (Figure 2) :
  Si Seql ≥ Bl (où Bl = Tl - W + 1), alors Seqh = Th
  Si Seql < Bl (où Bl = Tl - W + 1), alors Seqh = Th + 1

+ Dans le cas B (Figure 2) :
  Si Seql ≥ Bl (où Bl = Tl - W + 1), alors Seqh = Th - 1
  Si Seql < Bl (où Bl = Tl - W + 1), alors Seqh = Th

B.2.3 Exemple de pseudo-code

Le pseudo-code suivant illustre les algorithmes ci-dessus pour les vérifications d'anti répétition et d'intégrité. Les valeurs pour "Seql", "Tl", "Th", et "W" sont des entiers de 32 bits non signés. L'arithmétique est modulo 2^32.

```
Si (Tl ≥ W - 1)                    Cas A
   Si (Seql≥ Tl - W + 1)
      Seqh = Th
      Si (Seql ≤ Tl)
         Si (vérification de répétition réussie)
            Si (vérification d'intégrité réussie)
               Régler le bit correspondant à Seql
               Passer le paquet
            Autrement rejeter le paquet
         Autrement rejeter le paquet
      Autrement
         Si (vérification d'intégrité réussie)
            Tl = Seql (déplacer les bits)
            Régler le bit correspondant à Seql
            Passer le paquet
         Autrement rejeter le paquet
   Autrement
      Seqh = Th + 1
      Si (vérification d'intégrité réussie)
```

```
        Tl = Seql (déplacer les bits)
        Th = Th + 1
        Régler le bit correspondant à Seql
        Passer le paquet
      Autrement rejet le paquet
Autrement                          Cas B
  Si (Seql ≥ Tl - W + 1)
    Seqh = Th - 1
    Si (vérification de répétition réussie)
      Si (vérification d'intégrité réussie)
        Régler le bit correspondant à Seql
        Passer le paquet
      Autrement rejeter le paquet
```

B.3 Traitement de la perte de synchronisation due à une perte de paquet significative

Si il y a une perte de paquets non détectée de 2^32 ou plus paquets consécutifs sur une seule SA, l'émetteur et le receveur vont perdre la synchronisation des bits de poids fort, c'est-à-dire, les équations du paragraphe B2.2. vont échouer à donner la valeur correcte. Si ce problème n'est pas détecté et traité, les paquets suivants sur cette SA vont échouer aux vérifications d'authentification et seront éliminés. La procédure suivante DEVRAIT être appliquée par toute mise en œuvre IPsec (ESP ou AH) qui prend en charge l'option ESN.

Noter que cette sorte de perte de trafic étendue semble improbable si une fraction significative du trafic sur la SA en question est sur TCP, parce que la source ne recevrait pas de ACK et arrêterait d'envoyer bien avant que 2^32 paquets aient été perdus. Aussi, pour toute application bidirectionnelle, même celles qui fonctionnent avec UDP, une telle panne étendue résulterait probablement à déclencher une forme de fin de temporisation. Cependant, une application unidirectionnelle fonctionnant avec UDP peut manquer des retours qui causeraient la détection automatique d'une perte de cet ordre de grandeur, d'où la raison du développement d'une méthode de récupération pour ce cas.

La solution choisie est destinée à :

+ minimiser l'impact sur le traitement normal du trafic ;
+ éviter de créer une opportunité de nouvelle attaque de déni de service comme ce pourrait arriver en permettant à un attaquant de forcer une diversion de ressources pour un processus de resynchronisation ;
+ limiter le mécanisme de récupération au receveur parce que l'anti répétition est un service seulement pour le receveur, et que l'émetteur n'est généralement pas informé de si le receveur utilise des numéros des séquence pour la prise en charge de ce service facultatif. Il est préférable que le mécanisme de récupération soit local chez le receveur. Cela permet aussi la rétro compatibilité.

B.3.1 Déclenchement de la resynchronisation

Pour chaque SA, le receveur enregistre le nombre de paquets consécutifs qui échouent à l'authentification. Ce compte est utilisé pour déclencher le processus de resynchronisation, qui devrait être effectué en arrière plan ou en utilisant un processeur distinct. La réception d'un paquet valide sur la SA remet le compteur à zéro. La valeur utilisée pour déclencher le processus de resynchronisation est un paramètre local. Il n'est pas exigé de prendre en charge des valeurs distinctes de déclenchement pour des SA différentes, bien qu'une mise en œuvre puisse choisir de le faire.

B.3.2 Processus de resynchronisation

Lorsque le point de déclenchement ci-dessus est atteint, un "mauvais" paquet est choisi pour lequel l'authentification est réessayée en utilisant des valeurs successivement croissantes pour la moitié supérieure de numéro de séquence (Seqh). Ces valeurs sont générées en les incrémentant de un à chaque essai. Le nombre d'essais devrait être limité, pour le cas où ce paquet serait "passé" ou bogué. La valeur limite est un paramètre local. (Comme la valeur de Seqh est implicitement placée après la charge utile AH (ou ESP) il est possible d'optimiser cette procédure en exécutant l'algorithme d'intégrité sur le paquet jusqu'au point d'extrémité de la charge utile, puis de calculer les différents ICV candidats en faisant varier la valeur de Seqh.) La réussite de l'authentification d'un paquet via cette procédure remet à zéro le compte des échecs consécutifs et établit la valeur de T à celle du paquet reçu.

Cette solution n'exige que la prise en charge de la part du receveur, permettant ainsi la rétro compatibilité. Aussi, comme les efforts de resynchronisation se produiraient en arrière plan ou utiliseraient un processeur supplémentaire, cette solution n'impacte pas le traitement du trafic et une attaque de déni de service ne peut pas détourner des ressources du traitement du trafic.

Adresse de l’auteur

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

Déclaration de droits de reproduction

Propriété intellectuelle

Remerciement

Le financement de la fonction d’édition des RFC est actuellement fourni par l’activité de soutien administratif (IASA) de l’IETF.