Groupe de travail Réseau
Request for Comments : 4303
RFC rendue obsolète : 2406
Catégorie : En cours de normalisation

S. Kent, BBN Technologies

décembre 2005
Traduction Claude Brière de L'Isle

Encapsulation de charge utile de sécurité (ESP) IP

Statut du présent mémoire

Le présent document spécifie un protocole en cours de normalisation de l'Internet pour la communauté de l'Internet, et appelle à des discussion et suggestions pour son amélioration. Prière de se référer à l'édition en cours des "Normes officielles des protocoles de l'Internet" (STD 1) pour connaître 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 du protocole d'encapsulation de charge utile de sécurité (ESP), qui est destinée à fournir un assortiment de services de sécurité dans IPv4 et IPv6. ESP est utilisé pour fournir des services de confidentialité, d'authentification d'origine des données, d'intégrité sans connexion, et d'anti répétition (une forme d'intégrité de séquence partielle) et une confidentialité limitée du flux de trafic. Le présent document rend obsolète la RFC 2406 (novembre 1998).

Table des matières

1 Introduction

Le présent document suppose que le lecteur est familier avec les termes et concepts décrits dans "Architecture de sécurité pour le protocole Internet" [RFC4301], auquel on se réfère ci-après comme au document 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) et l'en-tête d'authentification (AH), le concept d'associations de sécurité, les façons dont ESP peut être utilisé en conjonction avec AH, et les différentes options de gestion de clés 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'encapsulation de charge utile de sécurité (ESP, *Encapsulating Security Payload*) est conçu pour fournir un mélange de services de sécurité dans IPv4 et IPv6 [RFC2460]. ESP peut s'appliquer seul, en combinaison avec AH [RFC4302], 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. Pour les détails de la façon dont ESP et AH sont utilisés dans les divers environnements de réseau, voir le document sur l'architecture de sécurité [RFC4301].

L'en-tête ESP est inséré après l'en-tête IP et avant l'en-tête de protocole de prochaine couche (en mode transport) ou avant un en-tête IP encapsulé (mode tunnel). Ces modes sont décrits plus en détail ci-dessous.

ESP peut être utilisé pour assurer la confidentialité, l'authentification de l'origine des données, l'intégrité sans connexion, et un service anti-répétition (une forme d'intégrité de séquence partielle) et la confidentialité (limitée) du flux de trafic. L'ensemble des services fournis dépend des options choisies au moment de l'établissement de l'association de sécurité (SA, *Security Association*) et de la situation de la mise en œuvre dans la topologie du réseau.

L'utilisation du chiffrement seul pour la confidentialité est permis par ESP. Cependant, on devrait noter qu'en général, cela ne va défendre que contre les attaques passives. Utiliser le chiffrement sans avoir par dessus lui un fort mécanisme de défense de l'intégrité (soit dans ESP, soit séparément via AH) peut rendre le service de confidentialité non sûr contre certaines formes d'attaque active [Bel96], [Kra01]. De plus, un service sous-jacent de protection de l'intégrité, comme AH, appliqué avant le chiffrement ne protège pas nécessairement la confidentialié par chiffrement seul contre les attaques actives [Kra01]. ESP permet des SA de chiffrement seul parce que cela peut offrir des performances considérablement améliorées et fournir quand même une sécurité adéquate, par exemple, lorsque une protection d'authentification/intégrité de couche supérieure est offerte indépendamment. Cependant, la présente norme n'exige pas que les mises en œuvre de ESP offrent un service de chiffrement seul.

L'authentification de l'origine des données et l'intégrité sans connexion sont des services conjoints, qu'on regroupe ici sous le terme de "intégrité". (Ce terme est employé parce que, sur la base du paquet, le calcul effectué donne directement l'intégrité sans connexion ; l'authentification de l'origine des données est fournie indirectement par suite du lien de la clé utilisée pour vérifer l'intégrité avec l'identité de l'homologue IPsec. Normalement, ce lien est effectué au moyen de l'utilisation d'une clé symétrique partagée.) ESP en intégrité seule DOIT être offert comme option de choix de service, par exemple, il doit être négocié dans les protocoles de gestion de SA et DOIT être configurable via des interfaces de gestion. ESP en intégrité seule est une solution de remplacement interessante à AH dans de nombreux contextes, par exemple, parce qu'il est de traitement plus rapide et plus favorable au traitement en parallèle dans de nombreuses mises en œuvre.

Bien que la confidentialité et l'intégrité puissent être offertes de façon indépendante, ESP va normalement employer les deux services, c'est-à-dire, les paquets seront protégés à l'égard de la confidentialité et de l'intégrité. Donc, il y a trois combinaisons possibles de service de sécurité ESP qui impliquent ces services :

- confidentialité seule (PEUT être pris en charge)
- intégrité seule (DOIT être pris en charge)
- confidentialité et intégrité (DOIT être pris en charge)

Le service anti répétition ne peut être choisi pour une SA que si le service de protection de l'intégrité a été retenu pour cette SA. Le choix de ce service est à la seule discrétion du receveur et n'a donc pas besoin d'être négocié. Cependant, pour utiliser le dispositif de numéro de séquence étendu (ESN, *Extended Sequence Number*) de façon interopérable, ESP impose comme exigence aux protocoles de gestion de SA qu'ils soient capables de négocier ce dispositif (voir au paragraphe 2.2.1).

Le service de confidentialité du flux de trafic (TFC, *traffic flow confidentiality*) n'est généralement efficace que si ESP est employé de façon à dissimuler les adresses ultimes de source et de destination des correspondants, par exemple, en mode tunnel entre des passerelles de sécurité, et seulement si un trafic suffisant s'écoule entre les homologues IPsec (soit naturellement, soit par suite de la génération d'un trafic de masquage) pour dissimuler les caractéristiques des flux de trafic

d'abonnés individuels spécifiques. (ESP peut être employé au titre d'un système de TFC de couche supérieure, par exemple, l'acheminement en pelure d'oignon *(Onion Routing)* [Syverson], mais de tels systèmes sortent du domaine d'application de la présente norme.) Les nouvelles caractéristiques de TFC présentes dans ESP facilitent une génération et élimination efficaces du trafic factice et un meilleur bourrage du trafic réel, de façon rétro compatible.

La Section 7 passe brièvement en revue les différences entre le présent document et la RFC 2406.

2. Format de paquet d'encapsulation de charge utile de sécurité

L'en-tête (le plus externe) de protocole (IPv4, IPv6, ou Extension) qui précède immédiatement l'en-tête ESP DEVRA contenir la valeur 50 dans son champ Protocole (IPv4) ou Prochain en-tête (IPv6, Extension) (voir la page de la Toile de l'IANA à http://www.iana.org/assignments/protocol-numbers). La Figure 1 illustre le format général d'un paquet ESP. Le paquet commence par deux champs de quatre octets (Indice de paramètres de sécurité (SPI, *Security Parameters Index*) et Numéro de séquence). Ces champs sont suivis des données de charge utile, dont la sous structure dépend du choix de l'algorithme et du mode de chiffrement, et de l'utilisation du bourrage de TFC, qu'on examinera plus en détails plus loin. Suivent les champs Bourrage et Longueur de bourrage, et le champ Prochain en-tête. Le champ facultatif de valeur de vérification d'intégrité (ICV, *Integrity Check Value*) termine le paquet.

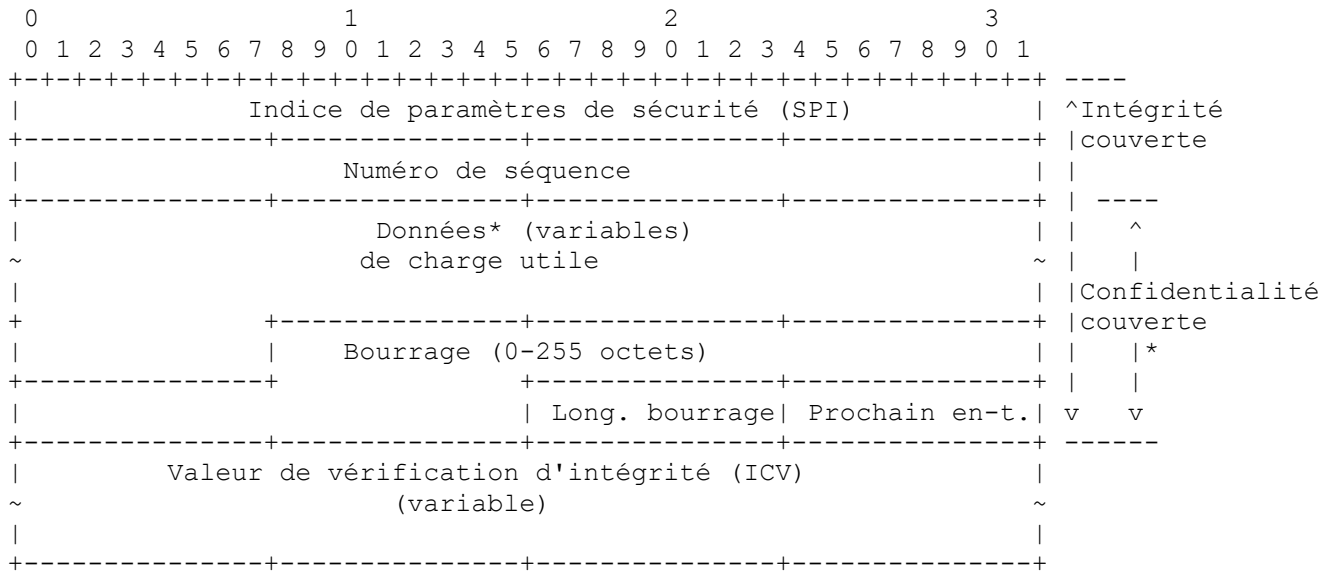


Figure 1 : Format général d'un paquet d'ESP

* Si elles sont incluses dans le champ Charge utile, les données de synchronisation cryptographiques, par exemple, une valeur d'initialisation (IV, voir au paragraphe 2.3) ne sont généralement pas chiffrées par elles-mêmes, bien qu'on y fasse souvent référence comme partie du texte chiffré.

L'en-queue ESP (transmis) consiste en les champs Bourrage *(Padding)*, Longueur de bourrage, et Prochain en-tête. Des données d'en-queue ESP supplémentaires implicites (qui ne sont pas transmises) sont incluses dans le calcul d'intégrité, comme décrit ci-dessous.

Si le service de protection de l'intégrité est choisi, le calcul d'intégrité englobe le SPI, le numéro de séquence, les données de charge utile, et l'en-queue ESP (explicite et implicite).

Si le service de confidentialité est choisi, le texte chiffré consiste en les données de charge utile (excepté toutes données de synchronisation cryptographique qui pourraient être incluses) et l'en-queue ESP (explicite).

Comme noté ci-dessus, les données de charge utile peuvent avoir une sub-structure. Un algorithme de chiffrement qui exige une valeur d'initialisation (IV) explicite, par exemple, le mode de chaînage de bloc de chiffrement (CBC, *Cipher Block Chaining*) fait souvent précéder de cette valeur les données de charge utile à protéger. Certains modes d'algorithme combinent le chiffrement et l'intégrité dans une seule opération ; le présent document se réfère à de tels modes d'algorithme comme à des "algorithmes en mode combiné". Le traitement des algorithmes en mode combiné exige que l'algorithme décrive explicitement la sub-structure de charge utile utilisée pour convoyer les données d'intégrité.

Certains algorithmes en mode combiné fournissent l'intégrité seule pour les données qui sont chiffrées, tandis que d'autres peuvent fournir l'intégrité pour des données supplémentaires qui ne sont pas chiffrées pour la transmission. Parce que les champs SPI et Numéro de séquence exigent la protection de l'intégrité au titre du service de protection de l'intégrité, et qu'ils ne sont pas chiffrés, il est nécessaire de s'assurer qu'ils peuvent s'offrir la protection de l'intégrité chaque fois que le service est choisi, sans considération du style de mode d'algorithme combiné employé.

Lorsque un algorithme en mode combiné est employé, l'algorithme lui-même est supposé retourner le texte source déchiffré et une indication de réussite/échec pour la vérification d'intégrité. Pour les algorithmes en mode combiné, l'ICV qui apparaîtrait normalement à la fin du paquet ESP (lorsque l'intégrité est choisie) peut être omise. Quand l'ICV est omise et que l'intégrité est choisie, il est de la responsabilité de l'algorithme en mode combiné de coder au sein des données de charge utile un moyen équivalent à l'ICV pour vérifier l'intégrité du paquet.

Si un algorithme en mode combiné offre l'intégrité seule aux données qui sont chiffrées, il sera nécessaire de dupliquer le SPI et le numéro de séquence au titre des données de charge utile.

Finalement, une nouvelle disposition est faite pour insérer du bourrage pour la confidentialité des flux de trafic après les données de charge utile et avant l'en-queue ESP. La Figure 2 illustre cette sub-structure pour les données de charge utile. (Note : ce diagramme montre les bits sur le réseau. De sorte que même si les numéros de séquence étendus sont utilisés, seuls 32 bits du numéro de séquence seront transmis (voir le paragraphe 2.2.1).)

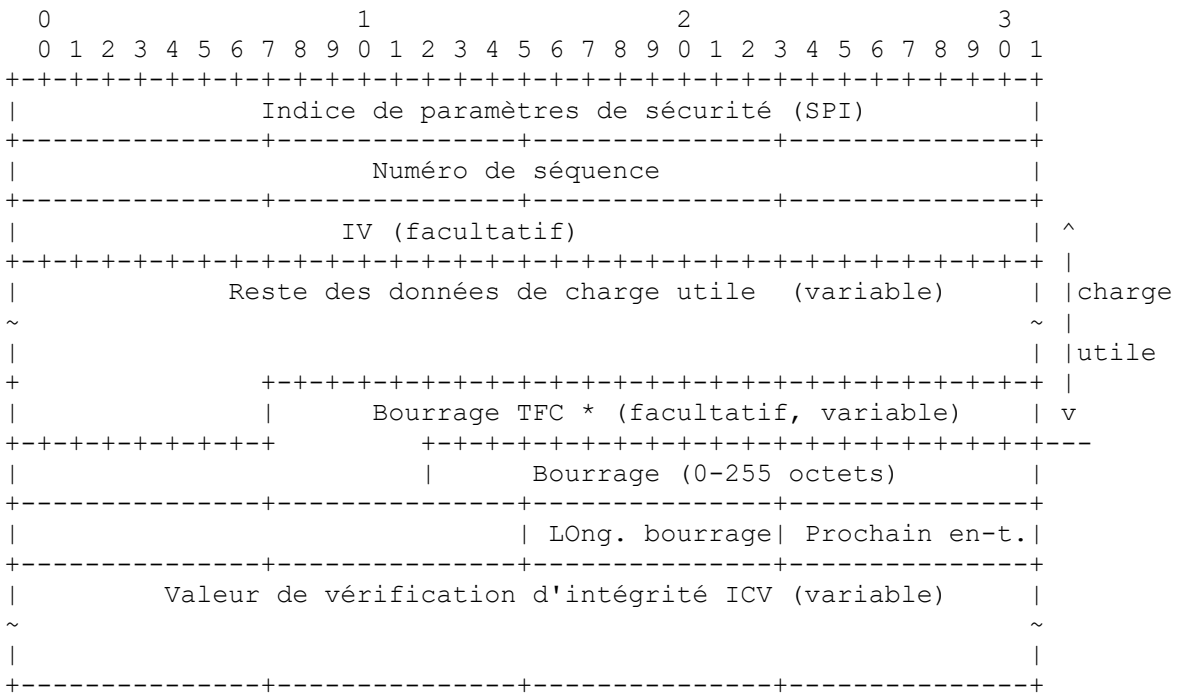


Figure 2 : Sous structure des données de charge utile

* Si le mode tunnel est utilisé, la mise en œuvre IPsec peut alors ajouter le bourrage de confidentialité de flux de trafic (TFC, *Traffic Flow Confidentiality*) (voir le paragraphe 2.4) après les données de charge utile et avant le champ Bourrage (0-255 octets).

Si un algorithme en mode combiné est employé, l'ICV explicite montrée aux Figures 1 et 2 peut être omise (voir le paragraphe 3.3.2.2). Parce que les algorithmes et modes sont fixés quand une SA est établie, le format détaillé des paquets ESP pour une certaine SA (incluant la sous structure de données de charge utile) est fixé, pour tout le trafic sur la SA.

Les tableaux ci-dessous se réfèrent aux champs des figures précédantes et illustrent comment plusieurs categories d'options algorithmiques, chacune ayant un modèle de traitement différent, affectent les champs notés ci-dessus. Les détails du traitement sont décrits dans les paragraphes qui suivent.

Tableau 1 : Algorithmes séparés de chiffrement et d'intégrité

Champ	Nombre d'octets	Exigence	Couvert par chiffrement	Couvert par intégrité	Ce qui est émis
SPI	4	Obligé		oui	txt source
N° séquence(bits mp)	4	Obligé		oui	txt source
IV	variable	Facultatif		oui	txt source }charge
Datagramme IP [2]	variable	Obligé ou factice	oui	oui	chiffré [3] } utile
Bourrage TFC[4]	variable	Facultatif	oui	oui	chiffré [3] }
Bourrage	0-255	Obligé	oui	oui	chiffré [3]
Longueur bourrage	1	Obligé	oui	oui	chiffré [3]
Prochain en-tête	1	Obligé	oui	oui	chiffré [3]
N° séquence (bits pf)	4	si ESN [5]		oui	non émis
Bourrage ICV	variable	si nécessaire		oui	non émis
ICV	variable	Obligé [6]			txt source

[2] Si mode tunnel -> datagramme IP. Si mode transport -> prochain en-tête et données
[3] Texte chiffré si le chiffrement a été choisi
[4] Ne peut être utilisé que si la charge utile spécifie sa longueur "réelle"
[5] Voir au paragraphe 2.2.1
[6] Obligatoire si un algorithme d'intégrité séparé est utilisé

Tableau 2 : Algorithmes en mode combiné

Champ	Nombre d'octets	Exigence	Couvert par chiffrement	Couvert par intégrité	Ce qui est émis
SPI	4	Obligé			txt source
N° séqu. (bits mp)	4	Obligé			txt source
IV	variable	Facultatif		oui	txt source }charge
Datagr. IP [2]	variable	Obligé ou factice	oui	oui	chiffré } utile
Bourrage TFC[3]	variable	Facultatif	oui	oui	chiffré }
Bourrage	0-255	Obligé	oui	oui	chiffré
Longueur bourrage	1	Obligé	oui	oui	chiffré
Prochain en-tête	1	Obligé	oui	oui	chiffré
N° séqu. (bits pf)	4	si ESN [4]		oui	[5]
Bourr. ICV	variable	si nécessaire		oui	[5]
ICV	variable	Facultatif [6]			txt source

[2] Si mode tunnel -> datagramme IP. Si mode transport -> prochain en-tête et données
[3] Ne peut être utilisé que si la charge utile spécifie sa longueur "réelle"
[4] Voir au paragraphe 2.2.1
[5] Le choix de l'algorithme détermine si ils sont émis, mais dans tous les cas, le résultat est invisible à ESP
[6] La spécification de l'algorithme détermine si le champ est présent

Les paragraphes qui suivent décrivent les champs dans le format d'en-tête. "Facultatif" signifie que le champ est omis si l'option n'est pas choisie, c'est-à-dire, il n'est présent ni dans le paquet transmis ni comme formaté pour le calcul d'une ICV (voir le paragraphe 2.7). Qu'une option soit choisie ou non est déterminé au titre de l'établissement de l'association de sécurité (SA, *Security Association*). Donc, le format des paquets ESP pour une certaine SA est fixe, pour la durée de la SA. À l'opposé, les champs "obligés" sont toujours présents dans le format de paquet ESP, pour toutes les SA.

Note : Tous les algorithmes cryptographiques utilisés dans IPsec attendent leur entrée 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.

ESP ne contient pas de numéro de version, et si il y a des problèmes de rétro compatibilité, ils DOIVENT être traités en utilisant un mécanisme de signalisation entre les deux homologues IPsec pour s'assurer de versions compatibles de ESP (par exemple, échange de clé Internet (IKEv2) [RFC4306]) ou un mécanisme de configuration hors bande.

2.1 Indice de paramètres de sécurité (SPI)

Le SPI est une valeur arbitraire de 32 bits qui est utilisée par un receveur pour identifier la SA à laquelle est lié un paquet entrant. Le champ SPI est obligé.

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, ESP). Parce que la valeur du SPI est générée par le receveur pour une SA d'envoi individuel, si la valeur est suffisante pour identifier une SA par elle-même ou si elle doit être utilisée en conjonction avec la valeur de protocole IPsec est une affaire locale. Ce mécanisme pour transposer le trafic entrant en SA d'envoi individuel DOIT être pris en charge par toutes les mises en œuvre de ESP.

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 entrants en SA. Les mises en œuvre qui prennent en charge seulement 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, [RFC3740]), un contrôleur de groupe/serveur de clés central alloue unilatéralement le SPI de l'association de sécurité de groupe. Cette allocation de SPI n'est ni négociée ni coordonnée avec les sous systèmes de gestion de clé (par exemple, IKE) qui résident dans les systèmes d'extrémité individuels qui composent 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 des associations de sécurité (SAD, *Security Association Database*) [RFC4301] doit indiquer si la recherche de SA peut utiliser les 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 façon telle qu'elle trouve l'entrée qui correspond au "plus long" identifiant de SA. Dans ce contexte, si deux ou plusieurs entrées de SAD correspondent sur la base de la valeur du SPI, 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 la SAD) est la "plus longue" correspondance. Cela implique un ordre logique de la recherche dans la SAD :

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

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

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

En pratique, une mise en œuvre PEUT choisir toute méthode pour accélérer cette recherche, bien que le 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 fondée sur le logiciel pourrait indexer par SPI dans un tableau. Les entrées de SAD dans chaque liste reliée d'un baquet de table de hachage sont triées pour avoir en premier les entrées de SAD qui ont les plus longs identifiants de SA dans cette liste reliée. Les entrées de SAD qui ont les plus courts identifiants de SA sont triés de telle sorte qu'elles soient les dernières entrées dans la liste reliée. Une mise en œuvre fondée sur le matériel peut être capable d'effectuer la recherche de la plus longue correspondance de façon intrinsèque, en utilisant les dispositifs couramment disponibles de mémoire ternaire à contenu adressable (TCAM, *Ternary Content-Addressable Memory*).

L'indication qu'il est exigé que la correspondance d'adresse de source et de destination transpose le trafic IPsec entrant en des 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 identifiant de SA en triplet composé d'un SPI, d'une adresse de destination de diffusion groupée, et d'une adresse de source. Une SA de groupe de diffusion groupée toutes sources exige seulement un SPI et une adresse 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, *Internet Assigned Numbers Authority*) pour des utilisations futures ; une valeur réservée de SPI ne sera normalement pas allouée par l'IANA sans que l'utilisation de la valeur de SPI allouée soit spécifiée dans une RFC. La

valeur de SPI de zéro (0) est réservée pour une utilisation spécifique de mise en œuvre locale et NE DOIT PAS être envoyée sur le réseau. (Par exemple, une mise en œuvre de gestion de clé peut utiliser la valeur de SPI de zéro pour signifier "aucune association de sécurité n'existe" durant la période où la mise en œuvre IPsec a demandé que son entité de gestion de clé établisse une nouvelle SA, mais où la SA n'a pas encore été établie.)

2.2 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 généralement non recommandé. ESP ne fournit pas de moyen pour synchroniser les compteurs de paquet parmi de multiples envoyeurs ou de gérer de façon significative un compteur de paquets en réception et une fenêtre dans le contexte d'envoyeurs multiples. Donc, pour une SA multi envoyeurs, le dispositif anti répétition de ESP n'est pas disponible (voir les paragraphes 3.3.3 et 3.4.3.)

Ce champ est obligé 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 de numéro de séquence est à la discrétion du receveur, mais toutes les mises en œuvre ESP DOIVENT être capables d'effectuer le traitement décrit aux paragraphes 3.3.3 et 3.4.3. Donc, l'envoyeur DOIT toujours transmettre ce champ, mais le receveur n'a pas besoin d'agir sur lui (voir la discussion de la vérification de numéro de séquence au paragraphe 3.4.3 "Traitement de paquet entrant".

Les compteurs de l'envoyeur et du receveur sont initialisés à 0 quand une SA est établie. (Le premier paquet envoyé en utilisant une certaine SA aura un numéro de séquence de 1 ; voir au paragraphe 3.3.3 plus de 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 être admis à revenir à zéro. Donc, le compteur de l'envoyeur et le compteur du receveur DOIVENT être remis à zéro par l'établissement d'une nouvelle SA et d'une nouvelle clé avant la transmission du 2^32ème paquet sur une SA.

2.2.1 Numéro de séquence étendu (64 bits)

Pour prendre en charge les mises en œuvre IPsec à grande vitesse, les numéros de séquence étendus (ESN) DEVRAIENT être mis en œuvre, comme extension au champ actuel de 32 bits de numéro de séquence. L'utilisation d'un ESN DOIT être négociée par un protocole de gestion de SA. Noter que dans IKEv2, cette négociation est implicite ; ESN est par défaut sauf si les numéros de séquence à 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 de numéros de séquence de 64 bits pour une SA. (Voir les détails à l'Appendice A, "Numéros de séquence étendus (64 bits)".) Seuls les 32 bits de moindre poids du numéro de séquence sont transmis dans l'en-tête ESP en texte source de chaque paquet, minimisant donc les frais généraux par paquet. Les 32 bits de poids fort sont conservés au titre du compteur de numéro de séquence par l'émetteur et le receveur et sont inclus dans le calcul de l'ICV (si le service de protection de l'intégrité est choisi). Si un algorithme séparé d'intégrité est employé, les bits de poids forts sont inclus dans l'en-queue ESP implicite, mais ne sont pas transmis, comme les bits de bourrage des algorithmes d'intégrité. Si un algorithme en mode combiné est employé, le choix de l'algorithme détermine si les bits ESN de poids fort sont transmis ou sont inclus implicitement dans le calcul. Voir au paragraphe 3.3.2.2 les détails du traitement.

2.3 Données de charge utile

Données de charge utile est un champ de longueur variable contenant les données (provenant du paquet IP original) décrit par le champ Prochain en-tête. Le champ Données de charge utile est obligatoire et a un nombre entier d'octets. Si l'algorithme utilisé pour chiffrer la charge utile exige des données de synchronisation cryptographiques, par exemple, une valeur d'initialisation (IV), ces données doivent alors être portées explicitement dans le champ Charge utile, mais il n'est pas invoqué comme un champ séparé dans ESP, c'est-à-dire, la transmission d'une IV explicite est invisible à ESP. (Voir la Figure 2.) Tout algorithme de chifffrement qui exige de telles données de synchronisation explicites par paquet DOIT indiquer la longueur, toute structure de telles données, et la localisation de ces données, au titre d'une RFC spécifiant comment l'algorithme est utilisé avec ESP. Normalement, la IV précède immédiatement le texte chiffré. (Voir la Figure 2.) Si de telles données de synchronisation sont implicites, l'algorithme pour déduire les données DOIT faire partie de la RFC de définition de l'algorithme. (Si elles sont incluses dans le champ Charge utile, les données de synchronisation cryptographique, par exemple, une valeur d'initialisation (IV) ne sont généralement par chiffrées par elles-même (voir les Tableaux 1 et 2) bien que parfois on s'y réfère comme faisant partie du texte chiffré.)

Noter que le début de l'en-tête du protocole de couche suivante DOIT être aligné par rapport au début de l'en-tête ESP comme suit. Pour IPv4, cet alignement est un multiple de 4 octets. Pour IPv6, l'alignement est un multiple de 8 octets.

En ce qui concerne la vérification de l'alignement du texte chiffré (réel) en présence d'une IV, noter que :

- Pour certains modes de fonctionnement fondés sur l'IV, le receveur traite l'IV comme début du texte chiffré, le fournissant directement à algorithme. Dans ces modes, l'alignement du début du texte chiffré (réel) n'est pas un problème chez le receveur.
- Dans certains cas, le receveur lit la IV séparément du texte chiffré. Dans ce cas, la spécification de l'algorithme DOIT indiquer comment l'alignement du texte chiffré réel doit être réalisé.

2.4 Bourrage (pour chiffrement)

Deux principaux facteurs exigent ou motivent l'utilisation du champ Bourrage.

- Si on emploie un algorithme de chiffrement qui exige que le texte source soit un multiple d'un certain nombre d'octets, par exemple, la taille de bloc d'un chiffrement par blocs, le champ Bourrage est utilisé pour compléter le texte source (consistant en les champs Données de charge utile, Bourrage, Longueur de bourrage , et Prochain en-tête) à la taille requise par l'algorithme.

- Le bourrage peut aussi être requis, sans considération des exigences de l'algorithme de chiffrement, pour s'assurer que le texte chiffré résultant se termine sur une limite de 4 octets. Précisément, les champs Longueur de bourrage et Prochain en-tête dovenit être alignés à droite au sein d'un mot de 4 octets, comme illustré dans les figures de format de paquet ESP ci-dessus, pour s'assurer que le champ ICV (si présent) est aligné sur une limite de 4 octets.

Un bourrage au delà de ce qui est requis pour l'algorithme ou pour les raisons d'alignement citées ci-dessus pourrait être utilisé pour dissimuler la longueur réelle de la charge utile, à l'appui de TFC. Cependant, le champ Bourrage décrit est trop limité pour être efficace pour TFC et donc ne devrait pas être utilisé à cette fin. À la place, le mécanisme distinct décrit ci-dessous (voir le paragraphe 2.7) devrait être utilisé quand TFC est exigé.

L'envoyeur PEUT ajouter de 0 à 255 octets de bourrage. L'inclusion du champ Bourrage dans un paquet ESP est facultative, sous réserve des exigences notées ci-dessus, mais toutes les mises en œuvre DOIVENT prendre en charge la génération et la consommation du bourrage.

- Afin de s'assurer que les bits à chiffrer sont un multiple de la taille de bloc de l'algorithme (premier facteur ci-dessus) le calcul du bourrage s'applique aux données de charge utile à l'exclusion de toute IV, mais incluant les champs de queue d'ESP. Si un algorithme en mode combiné exige la transmission du SPI et du numéro de séquence pour effectuer la protection de l'intégrité, par exemple, duplication du SPI et du numéro de séquence dans les données de charge utile, alors les versions dupliquées de ces éléments de données, et toutes données associées équivalentes à l'ICV sont incluses dans le calcul de la longueur de bourrage. (Si l'option ESN est choisie, les 32 bits de poids fort de ESN vont aussi entrer dans le calcul, si l'algorithme en mode combiné exige leur transmission pour l'intégrité.)

- Afin de s'assurer que l'ICV est aligné sur une limite de quatre octets (second facteur ci-dessus) le calcul du bourrage s'applique aux données de charge utile incluant les champs IV, Longueur de bourrage, et Prochain en-tête. Si un algorithme en mode combiné est utilisé, toutes les données dupliquées et les données équivalentes à l'ICV sont incluses dans les données de charge utile couvertes par le calcul du bourrage.

Si des octets de bourrage sont nécessaires mais si l'algorithme de chiffrement ne spécifie pas le contenu du bourrage, le traitement par défaut suivant DOIT être utilisé. Les octets de bourrage sont initialisés avec une série de valeurs d'entier (non signés, d'un octet). Le premier octet de bourrage ajouté au texte source est numéroté 1, et les octets de bourrage suivants formant une séquence à croissance monotone : 1, 2, 3, ... Quand ce schéma de bourrage est employé, le receveur DEVRAIT inspecter le champ Bourrage. (Ce schéma a été choisi à cause de sa relative simplicité, de la facilité de mise en œuvre dans les matériels, et parce qu'il offre une protection limitée contre certaines formes d'attaques de "couper coller" en l'absence d'autres mesures de protection de l'intégrité si le receveur vérifie les valeurs de bourrage au déchiffrement.)

Si un algorithme de chiffrement ou en mode combiné impose des contraintes sur les valeurs des octets utilisés pour le bourrage, elles DOIVENT être spécifiées par la RFC qui définit comment l'algorithme est employé avec ESP. Si l'algorithme exige de vérifier les valeurs des octets utilisés pour le bourrage, cela DOIT aussi être spécifié dans cette RFC.

2.5 Longueur de bourrage

Le champ Longueur de bourrage indique le nombre d'octets de bourrage qui le précèdent immédiatement dans le champ Bourrage. La gamme des valeurs valides est de 0 à 255, où une valeur de zéro indique qu'aucun octet de bourrage n'est présent. Comme noté ci-dessus, cela n'inclut aucun octet de bourrage TFC. Le champ Longueur de bourrage est obligatoire.

2.6 Prochain en-tête

Le champ Prochain en-tête de 8 bits est obligatoire, il identifie le type de données contenues dans le champ Données de charge utile, par exemple, un paquet IPv4 ou IPv6, ou un en-tête et des données de la couche suivante. La valeur de ce champ est choisie dans l'ensemble des numéros de protocole IP définis sur la page d'accueil de l'IANA, par exemple, une valeur de 4 indique IPv4, une valeur de 41 indique IPv6, et une valeur de 6 indique TCP.

Pour faciliter la génération et l'élimination rapide du trafic de bourrage à l'appui de la confidentialité des flux de trafic (voir le paragraphe 2.4) la valeur de protocole 59 (qui signifie "pas de prochain en-tête") DOIT être utilisée pour désigner un paquet "factice". Un émetteur DOIT être capable de générer des paquets factices marqués de cette valeur dans le champ Prochain protocole, et un receveur DOIT être prêt à éliminer de tels paquets, sans indiquer une erreur. Tous les autres champs d'en-tête et d'en-queue ESP (SPI, Numéro de séquence, Bourrage, Longueur de bourrage, Prochain en-tête, et ICV) DOIVENT être présents dans les paquets factices, mais la portion de texte source de la charge utile, à part ce champ Prochain en-tête, n'a pas besoin d'être bien formée, par exemple, le reste des données de charge utile peut consister seulement en octets aléatoires. Les paquets factices sont éliminés sans dommage.

Les mises en œuvre DEVRAIT fournir des commandes de gestion locales pour permettre l'utilisation de cette capacité SA par SA. Les commandes devraient permettre à l'utilisateur de spécifier si cette caractéristique est à utiliser et fournir aussi des commandes paramétriques ; par exemple, les commandes pourraient permettre à un administrateur de générer des paquets factices de longueur aléatoire ou fixe.

Discussion : Les paquets factices peuvent être insérés à des intervalles aléatoires pour masquer l'absence de trafic réel. On peut aussi "formater" le trafic réel pour correspondre à une certaine distribution à laquelle le trafic factice est ajouté comme indiqué par les paramètres de distribution. Comme avec la facilité de bourrage de la longueur de paquet pour la sécurité des flux de trafic (TFS, *Traffic Flow Security*) l'approche la plus sûre serait de générer des paquets factices au taux nécessaire pour maintenir un taux constant sur une SA. Si les paquets sont tous de la même taille, la SA présente alors l'apparence d'un flux de données à taux binaire constant, analogue à ce qu'un chiffrement de liaison offrirait aux couches 1 ou 2. Cependant, il est peu probable que cela soit praticable dans de nombreux contextes, par exemple, quand il y a plusieurs SA actives, parce que cela impliquerait de réduire la bande passante admise pour un site, sur la base du nombre de SA, et cela détruirait les avantages de la commutation de paquets. Les mises en œuvre DEVRAIENT fournir des commandes pour permettre aux administrateurs locaux de gérer la génération des paquets factices pour les besoins de TFC.

2.7 Bourrage de confidentialité du flux de trafic (TFC)

Comme noté ci-dessus, le champ Bourrage est limité en longueur à 255 octets. Cela ne va généralement pas être adéquat pour cacher les caractéristiques du trafic par rapport aux exigences de confidentialité des flux de trafic. Un champ facultatif, au sein des données de charge utile, est spécifiquement fourni pour traiter cette exigence de TFC.

Une mise en œuvre IPsec DEVRAIT être capable de bourrer le trafic en ajoutant des octets après la fin des données de charge utile, avant le début du champ Bourrage. Cependant, ce bourrage (qu'on appelle ici bourrage TFC) ne peut être ajouté que si le champ Données de charge utile contient une spécification de la longueur du datagramme IP. Ceci est toujours vrai en mode tunnel, et peut être vrai en mode transport selon que le protocole de la prochaine couche (par exemple, IP, UDP, ICMP) contient des informations explicites de longueur. Ces informations de longueur vont permettre au receveur d'éliminer le bourrage TFC, parce que la vraie longueur des données de charge utile sera connue. (Les champs d'en-queue ESP sont localisés en comptant à rebours depuis la fin du paquet ESP.) En conséquence, si le bourrage TFC est ajouté, le champ qui contient la spécification de la longueur du datagramme IP NE DOIT PAS être modifié pour refléter ce bourrage. Aucune exigence sur la valeur de ce bourrage n'est établie par la présente norme.

En principe, les mises en œuvre IPsec existantes auraient pu utiliser cette capacité antérieurement, de façon transparente. Cependant, parce que les receveurs peuvent n'avoir pas été préparés à traiter ce bourrage, le protocole de gestion de SA DOIT négocier ce service avant qu'un émetteur l'emploie, pour s'assurer de la rétro compatibilité. Combiné avec les

convention décrites au paragraphe 2.6, sur l'utilisation de l'identifiant de protocole 59, une mise en œuvre ESP est capable de générer des paquets factices et réels qui présentent une bien plus grande variabilité de longueur, à l'appui de TFC.

Les mises en œuvre DEVRAIENT fournir des commandes de gestion locales pour permettre l'utilisation de cette capacité SA par SA. Les commandes devraient permettre à l'utilisateur de spécifier si cette caractéristique doit être utilisée et aussi fournir des commandes paramétriques pour cette caractéristique.

2.8 Valeur de vérification d'intégrité

Valeur de vérifiation d'intégrité (ICV, *Integrity Check Value*) est un champ de longueur variable calculé sur les champs En-tête ESP, Charge utile, et En-queue ESP. Les champs implicites d'en-queue ESP (bourrage d'intégrité et bits ESN de poids fort, si applicables) sont inclus dans le calcul d'ICV. Le champ ICV est facultatif. Il n'est présent que si le service de protection de l'intégrité est choisi et il est fourni par un algorithme d'intégrité séparé ou un algorithme en mode combiné qui utilise une ICV. La longueur du champ est spécifiée par l'algorithme d'intégrité choisi et associé à la SA. La spécification de l'algorithme d'intégrité DOIT spécifier la longueur de l'ICV et les règles de comparaison et les étapes de traitement pour la validation.

3. Traitement de l'encapsulation de protocole de sécurité

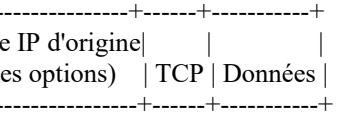
3.1 Situation de l'en-tête ESP

ESP peut être employé de deux façons : en mode transport ou en mode tunnel.

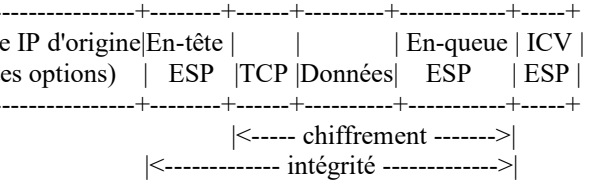
3.1.1 Traitement du mode transport

En mode transport, ESP est inséré après l'en-tête IP et avant un protocole de prochaine couche, par exemple, TCP, UDP, ICMP, etc. Dans le contexte de IPv4, cela se traduit par le placement d'ESP après l'en-tête IP (et toutes les options qu'il contient) mais avant le protocole de prochaine couche. (Si AH est aussi appliqué à un paquet, c'est appliqué à l'en-tête ESP, à la charge utile, à l'en-queue ESP, et à l'ICV, si présente.) (Noter que le terme de mode "transport" ne devrait pas être mal interprété comme restreignant son utilisation à TCP et UDP.) Le diagramme suivant illustre le positionnement du mode transport ESP pour un paquet IPv4 normal, fondé sur "avant et après". (Ce diagramme et le suivant montrent le champ ICV, dont la présence est fonction des services de sécurité et de l'algorithme/mode choisis.)

Avant l'application de ESP

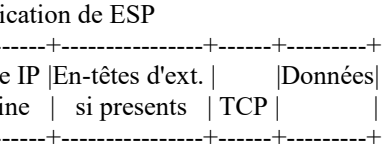


Après l'application de ESP

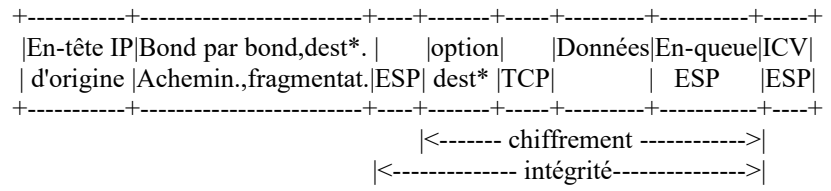


Dans le contexte IPv6, ESP est vu comme une charge utile de bout en bout, et donc devrait apparaître après les en-têtes bond par bond, acheminement, et extension de fragmentation. Le ou les en-têtes d'extension d'options de destination pourraient apparaître avant, après, ou à la fois avant et après l'en-tête ESP selon la sémantique désirée. Cependant, comme ESP protège seulement les champs après l'en-tête ESP, il sera généralement désirable de placer les en-têtes d'options de destination après l'en-tête ESP. Le diagramme suivant illustre le positionnement d'ESP en mode transport pour un paquet IPv6 normal.

Avant l'application de ESP



Après l'application de ESP



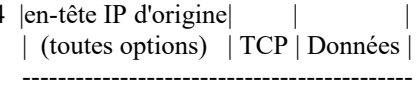
* = si present, pourrait être avant ESP, après ESP, ou les deux,

Noter qu'en mode transport, pour les mises en œuvre "prises dans la pile" ou "prises dans le réseau", comme défini dans le document d'architecture de la 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 transparente d'IPsec. Une attention particulière est requise pour effectuer de telles opérations au sein de ces mises en œuvre quand plusieurs interfaces sont utilisées.

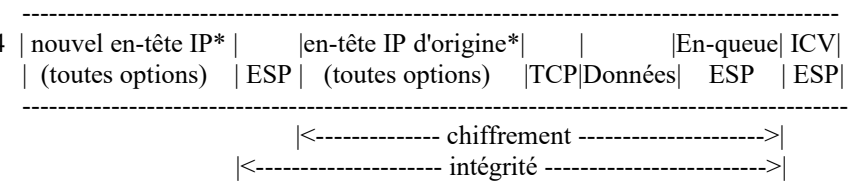
3.1.2 Traitement en mode tunnel

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

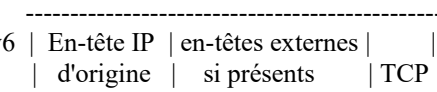
Avant l'application de ESP



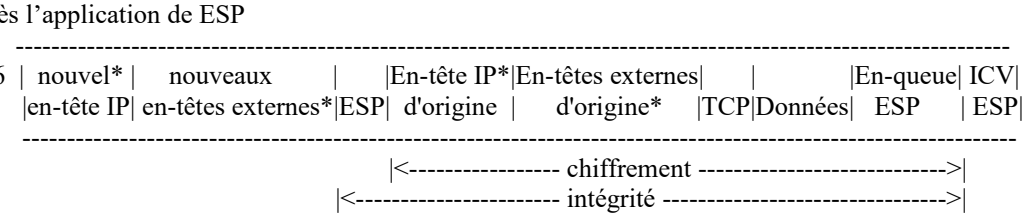
Après l'application de ESP



Avant l'application de ESP



Après l'application de ESP



* = si présent, la construction des en-têtes/extensions IP externes et la modification des en-têtes/extensions IP internes est discutée dans le document d'architecture de sécurité.

3.2 Algorithmes

Les algorithmes de mise en œuvre obligatoire pour l'utilisation avec ESP sont décrits dans une RFC séparée, pour faciliter la mise à jour des exigences des algorithmes indépendement du protocole lui-même. Des algorithmes supplémentaires, au

delà de ceux obligatoires pour ESP, PEUVENT être pris en charge. Noter que bien que la confidentialité et l'intégrité soient toutes deux facultatives, au moins un de ces services DOIT être choisi, donc les deux algorithmes NE DOIVENT PAS être simultanément NULS.

3.2.1 Algorithmes de chiffrement

L'algorithme de chiffrement employé pour protéger un paquet ESP est spécifié par la SA via laquelle le paquet est transmis/reçu. Parce que les paquets IP peuvent arriver déclassés, et que tous les paquets peuvent ne pas arriver (perte de paquet) chaque paquet doit porter toutes les données requises pour permettre au receveur d'établir la synchronisation cryptographique pour le déchiffrement. Ces données peuvent être portées explicitement dans le champ Charge utile, par exemple, comme une IV (comme décrit ci-dessus) ou les données peuvent être déduites de portions de texte source de l'en-tête de paquet (IP ou ESP externe). (Noter que si les informations d'en-tête de texte source sont utilisées pour déduire une IV, ces informations peuvent devenir critiques pour la sécurité et donc la limite de protection associée au processus de chiffrement peut croître. Par exemple, si on utilise le numéro de séquence ESP pour déduire une IV, la logique de génération de numéro de séquence (matérielle ou logicielle) devra être évaluée au titre de la mise en œuvre de l'algorithme de chiffrement. Dans le cas de FIPS 140-2 [NIST01], cela peut étendre significativement la portée de l'évaluation du module de chiffrement.) Parce que ESP a des dispositions pour le bourrage du texte source, les algorithmes de chiffrement employés avec ESP peuvent présenter des caractéristiques de mode de bloc ou de flux. Noter que parce que le chiffrement (confidentialité) PEUT être un service facultatif (par exemple, ESP en intégrité seule) cet algorithme PEUT être "NUL" [RFC4301].

Pour permettre à une mise en œuvre d'ESP de calculer le bourrage de chiffrement exigé par un algorithme de chiffrement en mode bloc, et pour déterminer l'impact de la MTU de l'algorithme, la RFC pour chaque algorithme de chiffrement utilisé avec ESP doit spécifier le module de bourrage pour l'algorithme.

3.2.2 Algorithmes d'intégrité

L'algorithme d'intégrité employé pour le calcul de l'ICV est spécifié par la SA via laquelle le paquet est transmis/reçu. Comme c'était le cas pour les algorithmes de chiffrement, tout algorithme d'intégrité employé avec ESP doit prendre des dispositions pour permettre le traitement des paquets qui arrivnt déclassés et pour s'accommoder de la perte de paquets. Le même avertissement que ci-dessus s'applique à l'utilisation de toutes les données de texte source pour faciliter la synchronisation des algorithmes d'intégrité par le receveur. Noter que parce que le service de protection de l’intégrité PEUT être facultatif, cet algorithme peut être "NUL".

Pour permettre à une mise en œuvre ESP de calculer tout bourrage implicite d'algorithme d'intégrité requis, la RFC pour chaque algorithme utilisé avec ESP doit spécifier le module de bourrage pour l'algorithme

3.2.3 Algorithmes de mode combiné

Si un algorithme en mode combiné est employé, les deux services de protection de la confidentialité et de l’intégrité sont fournis. Comme c'était le cas pour les algorithmes de chiffrement, un algorithme en mode combiné doit présenter des dispositions pour la synchronisation du chiffrement paquet par paquet, pour permettre le déchiffrement des paquets qui arrivent déclassés et pour s'accommoder de la perte de paquets. Les moyens par lesquels un algorithme en mode combiné fournit l'intégrité pour la charge utile, et pour le SPI et les champs de numéro de séquence (étendus) peuvent varier pour des choix différents d'algorithmes. Afin de fournir une approche uniforme, indépendante de l'algorithme pour l'invocation des algorithmes en mode combiné, aucune sous structure de charge utile n'est définie. Par exemple, les champs SPI et Numéro de séquence peuvent être dupliqués au sein de l'enveloppe de texte chiffré et une ICV peut être ajoutée à l'en-queue ESP. Aucun de ces détails ne devrait être observable en externe.

Pour permettre à une mise en œuvre ESP de déterminer l'impact de la MTU d'un algorithme en mode combiné, la RFC pour chaque algorithme utilisé avec ESP doit spécifier une formule (simple) qui donne la taille chiffrée de la charge utile, comme fonction de la taille de la charge utile et du numéro de séquence du texte source.

3.3 Traitement du paquet sortant

En mode transport, l'envoyeur encapsule les informations de protocole de prochaine couche entre les champs d'en-tête et d'en-queue ESP, et conserve l'en-tête IP spécifié (et tous en-têtes d'extension IP dans le contexte IPv6). En mode tunnel, les en-têtes/extensions IP externe et interne peuvent être en interrelation de diverses façons. La construction des en-têtes/extensions IP externe interne durant le processus d'encapsulation est décrit dans le document d'architecture de la sécurité.

3.3.1 Recherche d'association de sécurité

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

3.3.2 Calcul de valeur de vérification de chiffrement et d'intégrité de paquet

Dans ce paragraphe le chiffrement est toujours appliqué à cause des implications de formatage. Ceci implique en sous entendu que la "non confidentialité" est offerte en utilisant l'algorithme de chiffrement NUL (RFC 2410). Il y a plusieurs options algorithmiques.

3.3.2.1 Algorithmes séparés de confidentialité et d'intégrité

Si des algorithmes séparés de confidentialité et d'intégrité sont employés, l'envoyeur procède comme suit :

1. Encapsuler (dans le champ Charge utile ESP) :
   - pour le mode transport -- juste les informations de protocole original de prochaine couche.
   - pour le mode tunnel – le datagramme IP original entier.

2. Ajouter le bourrage nécessaire – bourrage TFC facultatif et bourrage (de chiffrement),

3. Chiffrer le résultat en utilisant la clé, l'algorithme de chiffrement, et le mode d'algorithme spécifiés pour la SA et en utilisant toutes les données de synchronisation cryptographiques requises.
   - Si des données explicites de synchronisation cryptographiques, par exemple, une IV, sont indiquées, elles sont entrées dans l'algorithme de chiffrement selon la spécification de l'algorithme et placées dans le champ Charge utile.
   - Si des données implicites de synchronisation cryptographiques sont employées, elles sont construites et entrées à l'algorithme de chiffrement selon la spécification de l'algorithme.
   - Si l'intégrité est choisie, le chiffrement est effectué d'abord, avant l'application de l'algorithme d'intégrité, et le chiffrement n'englobe pas le champ ICV. Cet ordre de traitement facilite la détection rapide et le rejet des paquets répétés ou mal formés par le receveur, avant de déchiffrer le paquet, réduisant donc potentiellement l'impact d'attaques de déni de service (DoS). Cela permet aussi un possible traitement en parallèle des paquets chez le receveur, c'est-à-dire, le déchiffrement peut avoir lieu en parallèle avec la vérification d'intégrité. Noter que parce que l'ICV n'est pas protégée par le chiffrement, un algorithme d'intégrité chiffré doit être employé pour la calculer.

4. Calculer l'ICV sur le paquet ESP moins le champ ICV. Donc, le calcul de l'ICV englobe le SPI, le numéro de séquence, les données de charge utile, le bourrage (si présent), la longueur de bourrage et le prochain en-tête. (Noter que les 4 derniers champs vont être en forme de texte chiffré, parce que le chiffrement est effectué d'abord.) Si l'option ESN est activée pour la SA, les 32 bits de poids fort du numéro de séquence sont ajoutés après le champ Prochain en-tête pour les besoins de ce calcul, mais ils ne sont pas transmis.

Pour certains algorithmes d'intégrité, la chaîne d'octets sur laquelle est effectué le calcul de l'ICV doit être un multiple d'une taille de bloc spécifiée par l'algorithme. Si la longueur du paquet ESP (comme décrite ci-dessus) ne correspond pas aux exigences de taille de bloc pour l'algorithme, un bourrage implicite DOIT être ajouté à la fin du paquet ESP. (Ce bourrage est ajouté après le champ Prochain en-tête, ou après les 32 bits de poids fort du numéro de séquence, si ESN est choisi.) La taille de bloc (et donc la longueur du bourrage) est spécifiée par la spécification de l'algorithme d'intégrité. Ce bourrage n'est pas transmis avec le paquet. Le document qui définit un algorithme d'intégrité DOIT être consulté pour déterminer si le bourrage implicite est requis comme décrit ci-dessus. Si le document ne spécifie pas une réponse à cette question, on doit supposer par défaut que le bourrage implicite est exigé (comme nécessaire pour faire correspondre la longueur de paquet à la taille de bloc de l'algorithme.) Si des 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.

3.3.2.2 Algorithmes combinés de confidentialité et d'intégrité

Si un algorithme combiné de confidentialité/intégrité est employé, l'envoyeur procède comme suit :

1. Encapsuler dans le champ ESP Données de charge utile :
   - pour le mode transport -- juste les informations de protocole original de prochaine couche.
   - pour le mode tunnel -- le datagramme IP original entier.

2. Ajouter tout bourrage nécessaire – inclus le bourrage TFC facultatif et le bourrage (de chiffrement).

3. Chiffrer et protéger en intégrité le résultat en utilisant la clé et l'algorithme en mode combiné spécifié pour la SA et en utilisant toutes les données requises pour la synchronisation cryptographique.

- Si des données explicites de synchronisation cryptographique, par exemple, une IV, sont indiquées, elles sont entrées à l'algorithme en mode combiné selon la spécification de l'algorithme et placées dans le champ Charge utile.
- Si des données implicites de synchronisation cryptographique sont employées, elles sont construites et entrées à l'algorithme de chiffrement conformément à la spécification de l'algorithme.
- Le numéro de séquence (ou le numéro de séquence étendu, comme approprié) et le SPI sont entrés à l'algorithme, car ils doivent être inclus dans le calcul de vérification d'intégrité. Les moyens par lesquels ces valeurs sont incluses dans ce calcul sont fonction de l'algorithme en mode combiné employé et donc non spécifiés dans cette norme.
- Le champ (explicite) ICV PEUT faire partie du format de paquet ESP quand un algorithme en mode combiné est employé. Si il n'est pas utilisé, un champ analogue va généralement faire partie de la charge utile de texte chiffré. La localisation de tous les champs d'intégrité, et les moyens par lesquels le numéro de séquence et le SPI sont inclus dans le calcul de l'intégrité, DOIVENT être définis dans une RFC sur l'utilisation de l'algorithme en mode combiné avec ESP.

3.3.3 Génération de numéro de séquence

Le compteur de l'envoyeur est initialisé à 0 quand une SA est établie. L'envoyeur incrémente le compteur de 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 vérifie que le compteur n'a pas fait un tour 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 la fin du cycle des numéros de séquence. Une tentative de transmission d'un paquet qui résulterait en un débordement de numéro de séquence est un événement à signaler dans le journal. L'enregistrement à entrer pour cet événement DEVRAIT inclure la valeur de SPI, la date et l'heure en cours, l'adresse de source, l'adresse de destination, et (dans IPv6) l'identifiant de flux du texte source.

L'envoyeur suppose que l'anti répétition est activée par défaut, sauf notification contraire du receveur (voir au paragraphe 3.4.3). Donc, le comportement normal d'une mise en œuvre ESP invite l'envoyeur à établir une nouvelle SA quand le numéro de séquence (ou ESN) a accompli un cycle, ou en anticipation de l'accomplissement du cycle par cette valeur.

Si la clé utilisée pour calculer une ICV est distribuée manuellement, une mise en œuvre conforme NE DEVRAIT PAS fournir de service anti répétition. Si un utilisateur choisit d'employer l'anti répétition en conjonction avec des SA qui sont chiffrées manuellement, le compteur de numéros de séquence chez l'envoyeur DOIT être correctement conservé à travers les réinitialisations locales, etc., jusqu'à ce que la clé soit remplacée. (Voir la Section 5.)

Si l'anti répétition est désactivée (comme noté ci-dessus) l'envoyeur n'a pas besoin de surveiller ou réinitialiser le compteur. Cependant, l'envoyeur incrémente toujours le compteur et quand 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 qui sortent du domaine d'application de la présente norme, sont négociés entre envoyeur et receveur.)

Si ESN (voir l'Appendice) est choisi, seuls les 32 bits de moindre poids du numéro de séquence sont transmis dans le champ Numéro de séquence, bien que envoyeur et receveur tiennent tous deux des compteurs ESN complets de 64 bits. Les 32 bits de poids fort sont inclus dans la vérification d'intégrité d'une façon spécifique de l'algorithme/mode, par exemple, les 32 bits de poids fort peuvent être ajoutés après le champ Prochain en-tête quand on emploie un algorithme d'intégrité séparé.

Note : 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 le besoin que le receveur gère une fenêtre d'anti répétition (afin de déterminer la valeur correcte pour les 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.

3.3.4 Fragmentation

Si necessaire, la fragmentation est effectuée après le traitement ESP au sein d'une mise en œuvre IPsec. Donc, le mode transport ESP n'est appliqué qu'aux datagrammes IP complets (pas aux fragments IP). Un paquet IP auquel ESP a été appliqué peut lui-même être fragmenté par les routeurs en chemin, et de tels fragments doivent être rassembleés avant le traitement ESP chez un receveur. En mode tunnel, ESP est appliqué à un paquet IP, qui peut être un fragment d'un datagramme IP. Par exemple, une passerelle de sécurité ou une mise en œuvre IPsec "prise dans la pile" ou "prise dans le réseau" (comme défini dans le document d'architecture de sécurité) peut appliquer ESP en mode tunnel 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 dans le réseau peuvent avoir d'abord à rassembler un paquet fragmenté par la couche IP locale, puis d'appliquer IPsec, et ensuite de fragmenter le paquet résultant.

Note : pour IPv6 -- pour les mises en œuvre prises dans la pile et prises dans le réseau, il sera nécessaire d'examiner tous les en-têtes d'extension pour déterminer si il y a un en-tête de fragmentation et donc si le paquet doit être réassemblié avant le traitement IPsec.

La fragmentation, qu'elle soit effectuée par une mise en œuvre IPsec ou par les routeurs sur le chemin entre homologues IPsec, réduit significativement les performances. De plus, l'exigence qu'un receveur ESP accepte les fragments au réassemblage crée des vulnérabilités au déni de service. Donc, une mise en œuvre ESP PEUT choisir de ne pas prendre en charge la fragmentation et peut marquer les paquets transmis avec le bit DF *(ne pas fragmenter)* pour faciliter la découverte de la MTU de chemin (PMTU, *Path MTU*). Dans tous les cas, une mise en œuvre ESP DOIT prendre en charge la génération des messages PMTU ICMP (ou leur 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 sont contenus dans le document d'architecture de sécurité.

3.4 Traitement de paquet entrant

3.4.1 Réassemblage

Si exigé, le réassemblag est effectué avant le traitement ESP. Si un paquet offert pour traitement à ESP paraît être un fragment IP, c'est-à-dire, si le champ OFFSET n'est pas zéro ou si le fanion Plus de fragments est établi, le receveur DOIT éliminer le paquet ; ceci est un événement auditable. L'entrée d'enregistrement d'audit pour cet événement DEVRAIT inclure la valeur de SPI, la date/heure de réception, l'adresse de source, l'adresse de destination, le numéro de séquence, et (dans IPv6) tl'identifiant de flux.

Note : pour le réassemblage de paquet, la spécification IPv4 actuelle N'EXIGE PAS la mise à zéro du champ Décalage ni l'a mise à zéro du fanion Plus de fragments. Afin qu'un paquet réassemblé soit traité par IPsec (par opposition à éliminé comme fragment apparent) le code IP doit faire ces deux choses après avoir rassemblé un paquet.

3.4.2 Recherche d'association de sécurité

À réception d'un paquet contenant un en-tête ESP, 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 2.1. 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 2.1. (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 va être vérifié, si des numéros de séquence de 32 ou 64 bits sont employés pour la SA, et si le champ ICV (explicite) devrait être présent (et sa taille si c'est le cas). Aussi, l'entrée de SAD va spécifier les algorithmes et les clés à employer pour le déchiffrement et le calcul d'ICV (si c'est applicable).

Si il n'existe aucune association de sécurité valide pour ce paquet, le receveur DOIT éliminer le paquet; c'est un événement qui peut faire l'objet d'un examen. L'entrée d'enregistrement d'audit pour cet événement DEVRAIT inclure la valeur du SPI, la date/heure de réception, l'adresse de source, l'adresse de destination, le numéro de séquence, et (en IPv6) l'identifiant de flux du texte source.

(Noter que le trafic de gestion de SA, comme les paquets IKE, n'ont pas besoin d'être traités 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 de numéro de séquence

Toutes les mises en œuvre ESP DOIVENT prendre en charge le service anti répétition, bienque son utilisation puisse être activée ou désactivée par le receveur SA par AS. Ce service NE DOIT PAS être activé à moins que le service ESP de protection de l'intégrité soit aussi activé pour la SA, parce que autrement le champ Numéro de séquence n'a pas été protégé en intégrité. L'anti répétition est applicable aux SA en envoi individuel aussi bien qu'en diffusion groupée. Cependant, la présente norme ne spécifie aucun mécanisme pour fournir l'anti répétition pour une SA multi envoyeurs (en envoi individuel ou en diffusion groupée). En l'absence de négociation (ou configuration manuelle) d'un mécanisme anti répétition pour une telle SA, il est recommandé que l'envoyeur et le receveur vérifient que le numéro de séquence pour la SA est désactivê (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 au receveur. Pour éviter que l'envoyeur fasse une surveillance non nécessaire des numéros de séquence et d'établissement de SA (voir le paragraphe 3.3.3) si un protocole d'établissement de SA est employé, le receveur DEVRAIT notifier à l'envoyeur, durant l'établissement de SA, si le receveur ne va pas fournir de protection anti répétition.

Si le receveur a activé le service anti répétition pour cette SA, le compteur de réception de paquets pour la SA DOIT être initialisé à zéro quand la SA est établie. Pour chaque paquet reçu, le receveur DOIT vérifier que le paquet contient un numéro de séquence qui ne duplique pas le numéro de séquence d'un autre paquet reçu durant la vie de cette SA. Cela DEVRAIT être la première vérification ESP appliquée à un paquet après qu'il a été confronté à une SA, pour accélérer le rejet des paquets dupliqués.

ESP permet une vérification en deux étapes des numéros de séquence des paquets. Cette capacité est importante chaque fois qu'une mise en œuvre ESP (normalement sa portion de module cryptographique) n'est pas capable d'effectuer le déchiffrement et/ou la vérification d'intégrité au même rythme que la ou les interfaces avec des réseaux non protégés. Si la mise en œuvre est capable d'un tel fonctionnement "au débit de ligne", il n'est alors pas nécessaire d'effectuer l'étape de vérification préliminaire décrite ci-dessous.

La vérification préliminaire du numéro de séquence est effectuée en utilisant la valeur de numéro de séquence dans l'en-tête ESP et est effectuée avant de vérifier l'intégrité et le déchiffrement. Si cette vérification préliminaire échoue, le paquet est éliminé, évitant donc d'avoir besoin d'aucune opération cryptographique de la part du receveur. Si la vérification préliminaire est réussie, le receveur ne peut pas encore modifier son compteur local, parce que l'intégrité du numéro de séquence n'a pas encore été vérifiée à ce moment.

Les dupliqués sont rejetés au moyen d'une fenêtre de réception glissante. Comment la fenêtre est mise en œuvre est une affaire locale, mais le texte qui suit décrit la fonctionnalité que doit exhiber la mise en œuvre.

Le bord "droit" de la fenêtre représente la plus haute 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 tombent dans la fenêtre sont vérifiés par rapport à une liste de paquets reçus au sein de 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) quand 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 inférieurs en valeur aux 32 bits de moindre poids du numéro de séquence du receveur, le receveur va supposer que les 32 bits de poids fort ont été incrémentés, passant à un nouveau sous espace de numéros de séquence. (Cet algorithme s'accommode de trous de réception pour une seule SA de jusqu'à 2**32-1 paquets. Si un trou plus grand se produit, des vérifications heuristiques supplémentaires pour la re-synchronisation du compteur de numéro de séquence du receveur PEUVENT être employées, comme décrit dans l'Appendice.)

Si le paquet reçu tombe dans la fenêtre et n'est pas un dupliqué, ou si le paquet est à droite de la fenêtre, et si un algorithme d'intégrité séparé est employé, le receveur procède alors à une vérification d'intégrité. Si un algorithme en mode combiné est employé, la vérification d'intégrité est effectuée avec le déchiffrement. Dans l'un et l'autre cas, la vérification d'intégrité échoue, le receveur DOIT éliminer le datagramme IP reçu comme invalide ; c'est un événement susceptible d'un examen. L'entrée d'enregistrement d'audit pour cet événement DEVRAIT inclure la valeur du SPI, la date/heure de réception, 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'intégrité réussit. (Si un algorithme en mode combiné est utilisé, le numéro de séquence protégé en intégrité doit aussi correspondre au numéro de séquence utilisé pour la protection anti répétition.)

Une taille minimum de fenêtre de 32 paquets DOIT être prise en charge quand des numéros de séquence de 32 bits sont employés ; une taille de fenêtre de 64 est préférée et DEVRAIT être employée par défaut. Une autre taille de fenêtre (supérieure au minimum) PEUT être choisie par le receveur. (Le receveur NE notifie PAS à l'envoyeur la taille de fenêtre.) La taille de la fenêtre de réception devrait être augmentée pour les environnements de haut débit, sans considération des questions d'assurance. Les valeurs pour les tailles minimum et recommandées de fenêtre de réception pour chaque appareil à haut débit (par exemple, plusieurs gigabit/s) ne sont pas spécifiés par la présente norme.

3.4.4 Vérification de la valeur de vérification d'intégrité

Comme avec le processus sortant, il y a plusieurs options pour le traitement entrant, fondées sur les caractéristiques des algorithmes employés.

3.4.4.1 Algorithmes séparés de confidentialité et d'intégrité

Si des algorithmes sépares de confidentialité et d'intégrité sont employés, le traitement se fait comme suit :

1. Si l'intégrité a été choisie, le receveur calcule la ICV sur le paquet ESP moins l'ICV, en utilisant l'algorithme d'intégrité spécifié et vérifie qu'elle est la même que l'ICV portée dans le paquet. Les détails du calcul sont données ci-dessous.

Si l'ICV calculée et celle reçue correspondent, le datagramme est alors valide, et il est accepté. Si l'essai échoue, le receveur DOIT alors éliminer le datagramme IP reçu comme invalide ; c'est un événement qui peut faire l'objet d'un examen. Les données enregistrées DEVRAIENT inclure la valeur du SPI, la date/heure de réception, l'adresse de source, l'adresse de destination, le numéro de séquence, et (pour IPv6) l'identifiant de flux en texte source.

Note de mise en œuvre : Les mises en œuvre peuvent utiliser tout ensemble d'étapes qui résulte en le même résultat que l'ensemble d'étapes suivant. Commencer par retirer et sauvegarder le champ ICV. Vérifier ensuite la longueur totale du paquet ESP moins le champ ICV. Si un bourrage implicite est requis, sur la base de la taille de bloc de l'algorithme d'intégrité, ajouter des octets de zéros à la fin du paquet ESP directement après le champ Prochain en-tête, ou après les 32 bits de poids fort du numéro de séquence si ESN est choisi. 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.

2. Le receveur déchiffre les données ESPde charge utile, le bourrage, la longueur de bourrage, et le prochain en-tête en utilisant la clé, l'algorithme de chiffrement, le mode d'algorithme, et les données de synchronisation cryptographique (si il en est) indiqués par la SA. Comme au paragraphe 3.3.2, on parle ici en termes de chiffrement toujours appliqué à cause des implications de formatage. Ceci est fait en comprenant que "pas de confidentialité" est offert en utilisant l'algorithme de chiffrement NUL (RFC 2410).
   - Si des données de synchronisation cryptographique explicites, par exemple, une IV, sont indiquées, elles sont tirées du champ Charge utile et entrées dans l'algorithme de déchiffrement conformément à la spécification de l'algorithme.
   - Si des données de synchronisation cryptographique implicites sont indiquées, une version locale de l'IV est construite et entrée à l'algorithme de déchiffrement conformément à la spécification de l'algorithme.

3. Le receveur traite tout bourrage comme spécifié dans la spécification de l'algorithme de chiffrement. Si le schéma de bourrage par défaut (voir le paragraphe 2.4) a été employé, le receveur DEVRAIT inspecter le champ Bourrage avant de retirer le bourrage et de passer les données déchiffrées à la couche suivante.

4. Le receveur vérifie le champ Prochain en-tête. Si la valeur est "59" (pas de prochain en-tête) le paquet (factice) est éliminé sans autre traitement.

5. Le receveur reconstruit le datagramme IP original à partir :
   - pour le mode transport -- l'en-tête IP externe plus les informations originales de protocole de prochaine couche dans le champ Charge utile ESP,
   - pour le mode tunnel -- le datagramme IP entier dans le champ Charge utile ESP.

Les étapes exactes pour reconstruire le datagramme original dépendent du mode (transport ou tunnel) et sont décrites dans le document d'architecture de sécurité. Au minimum, dans un contexte IPv6, le receveur DEVRAIT s'assurer que les données déchiffrées sont alignées sur huit octets, pour faciliter le traitement par le protocole identifié dans le champ Prochain en-tête. Ce traitement "élimine" tout bourrage TFC (facultatif) qui a été ajouté pour la confidentialité du flux de trafic. (Si présent, il aura été inséré après le datagramme IP (ou trame de couche transport) et avant le champ Bourrage (voir le paragraphe 2.4).)

Si les vérifications d'intégrité et de chiffrement sont effectuées en parallèle, la vérification d'intégrité DOIT être achevée avant que le paquet déchiffré soit passé à la suite du traitement. Cet ordre de traitement facilite une rapide détection et rejet des paquets répété ou bogués par le receveur, avant de déchiffrer le paquet, réduisant donc potentiellement l'impact d'attaques de déni de service.

Note : Si le receveur effectue le déchiffrement en parallèle à la vérification d'intégrité, il faut faire attention à éviter de possibles conditions de compétition entre l'accès au paquet et l'extraction du paquet déchiffré.

3.4.4.2 Algorithmes combinés de confidentialité et d'intégrité

Si un algorithme combiné de confidentialité et d'intégrité est employé, le receveur procède alors comme suit :

1. Il déchiffre et vérifie l'intégrité des données de charge utile ESP, du bourrage, longueur de bourrage, et prochain en-tête, en utilisant la clé, l'algorithme, le mode d'algorithme, et les données de synchronisation cryptographique (si il en est) indiqués par la SA. Le SPI provenant de l'en-tête ESP, et la valeur du compteur de paquets (du receveur) (ajustée

comme requis par le traitement décrit au paragraphe 3.4.3) sont entrés à cet algorithme, comme ils sont requis pour la vérification d'intégrité.
- Si des données de synchronisation cryptographique explicite, par exemple, une IV, sont indiquées, elle sont prises dans le champ Charge utile et entrées à l'algorithme de déchiffrement conformément à la spécification de l'algorithme.
- Si des données de synchronisation cryptographique implicites, par exemple, une IV, sont indiquées, une version locale de l'IV est construite et entrée à l'algorithme de déchiffrement conformément à la spécification de l'algorithme.

2. Si la vérification d'intégrité effectuée par l'algorithme en mode combiné échoue, le receveur DOIT éliminer le datagramme IP reçu comme invalide ; c'est un événement qui peut faire l'objet d'un examen. Les données enregistrées DEVRAIENT inclure la valeur de SPI, la date/heure de réception, l'adresse de source, l'adresse de destination, le numéro de séquence, et (en IPv6) l'identifiant de flux du texte source.

3. Il traite tous les bourrages comme spécifié dans la spécification de l'algorithme de chiffrement, si cet algorithme ne l'a pas déjà fait.

4. Le receveur vérifie le champ Prochain en-tête. Si la valeur est "59" (pas de prochain en-tête) le paquet (factice) est éliminé sans autre traitement.

5. Il extrait le datagramme IP d'origine (mode tunnel) ou la trame de couche transport (mode transport) du champ Données de charge ESP. Cela élimine implicitement tout bourrage (facultatif) qui aurait été ajouté pour assurer la confidentialité du flux de trafic. (Si il est présent, le bourrage TFC devra être inséré après la charge utile IP et avant le champ Bourrage (voir le paragraphe 2.4).)

4. Révision

Tous les systèmes qui mettent en œuvre ESP ne vont pas mettre en œuvre de fonction d'audit. Cependant, si ESP est incorporé dans un système qui prend en charge une telle fonction, la mise en œuvre ESP DOIT alors aussi la prendre en charge et DOIT permettre à l'administrateur de système d'activer ou désactiver l'audit pour ESP. Pour la plus grande part, la granularité de l'examen est une affaire locale. Cependant, plusieurs événements pouvant faire l'objet d'un examen ont été identifiés dans la présente spécification et pour chacun de ces événements un ensemble minimum d'informations qui DEVRAIT être inclus dans un enregistrement d'audit est défini.

- Aucune association de sécurité valide n'existe pour une session. L'entrée d'enregistrement d'audit pour cet événement DEVRAIT inclure la valeur de SPI, la date/heure de réception, l'adresse de source, l'adresse de destination, le numéro de séquence, et (pour IPv6) l'identifiant de flux du texte source.

- Un paquet offert à ESP pour traitement paraît être un fragment IP, c'est-à-dire, le champ OFFSET n'est pas zéro ou le fanion Plus de fragments est établi. L'entrée d'enregistrement d'audit pour cet événement DEVRAIT inclure la valeur de SPI, la date/heure de réception, l'adresse de source, l'adresse de destination, le numéro de séquence, et (pour IPv6) l'identifiant de flux.

- Tentative de transmission d'un paquet qui résulterait en débordement de numéro de séquence. L'entrée d'enregistrement d'audit pour cet événement DEVRAIT inclure la valeur de SPI, la date/heure de réception, l'adresse de source, l'adresse de destination, le numéro de séquence, et (pour IPv6) l'identifiant de flux du texte source.

- Le paquet reçu échoue aux essais d'anti répétition. L'entrée d'enregistrement d'audit pour cet événement DEVRAIT inclure la valeur de SPI, la date/heure de réception, l'adresse de source, l'adresse de destination, le numéro de séquence, et (pour IPv6) l'identifiant de flux.

- La vérification d'intégrité échoue. L'entrée d'enregistrement d'audit pour cet événement DEVRAIT inclure la valeur de SPI, la date/heure de réception, l'adresse de source, l'adresse de destination, le numéro de séquence, et (pour IPv6) l'identifiant de flux.

Des informations supplémentaires PEUVENT aussi être incluses dans l'enregistrement d'audit pour chacun de ces événements, et des événements supplémentaires, non explicitement invoqués dans la présente spécification, PEUVENT aussi résulter en entrées d'enregistrements d'audit. Il n'est pas exigé que le receveur transmette de message à l'envoyeur prétendu en réponse à la détection d'un événement auditable, à cause du potentiel d'induction d'attaque de déni de service via une telle action.

5. Exigences de conformité

Les mises en œuvre qui revendiquent la conformité à la présente spécification DOIVENT mettre en œuvre la syntaxe ESP et le traitement décrits ici pour le trafic en envoi individuel, et DOIVENT se conformer à toutes les exigences supplémentaires de traitement de paquet posées par le document d'architecture de sécurité [RFC4301]. De plus, si une mise en œuvre prend en charge le trafic de 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 une ICV est distribuée manuellement, la fourniture correcte du service anti répétition exige une maintenance correcte de l'état du compteur chez l'envoyeur (à travers les réamorçages locaux, etc.) jusqu'à ce que la clé soit remplacée, et il est probable qu'il n'y a pas de disposition de récupération automatique si le débordement du compteur est imminent. Donc, une mise en œuvre conforme NE DEVRAIT PAS fournir de service anti répétition conjointement avec des SA qui sont chiffrées manuellement.

Les algorithmes de mise en œuvre obligatoire avec ESP sont décrits dans un document séparé [RFC4305], pour faciliter la mise à jour des exigences de l'algorithme indépendamment du protocole lui-même. Des algorithmes supplémentaires, au delà de ceux obligatoires pour ESP, PEUVENT être pris en charge.

Parce que l'utilisation du chiffrement dans ESP est facultative, la prise en charge de l'algorithme de chiffrement "NUL" est aussi exigée pour garder la cohérence avec la façon dont les services ESP sont négociés. La prise en charge de la version de service de confidentialité de ESP est facultative. Si une mise en œuvre offre ce service, elle DOIT aussi prendre en charge la négociation de l'algorithme d'intégrité "NUL". Noter que bien que intégrité et chiffrement puissent chacun être "NUL" dans les circonstances notées ci-dessus, ils NE DOIVENT PAS être "NUL" tous les deux.

6. Considérations pour la sécurité

La sécurité est centrale pour la conception de ce protocole, et donc les considérations de sécurité imprègnent cette spécification. Des aspects supplémentaires pertinents pour la sécurité de l'utilisation du protocole IPsec sont discutés dans le document d'architecture de sécurité.

7. Différences avec la RFC 2406

Le présent document diffère de la RFC 2406 d'un certain nombre de façons significatives.

- Service de confidentialité seule – maintenant un PEUT, non un DOIT.
- SPI – modifié pour spécifier un algorithme uniforme pour la recherche de SAD pour les SA en envoi individuel et en diffusion groupée, couvrant une gamme plus large 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 l'adresse de source, pour choisir une SA.
- Numéro de séquence étendu – ajout d'une nouvelle option pour un numéro de séquence à 64 bits pour les communications à très haut débit. Les exigences de traitement de l'envoyeur et du receveur ont été précisées pour les SA de diffusion groupée et multi envoyeurs.
- Données de charge utile – le modèle a été élargi pour s'accommoder des algorithmes en mode combiné.
- Bourrage pour une confidentialité améliorée du flux de trafic – une exigence a été ajoutée pour être capable d'ajouter des octets après la fin de la charge utile IP, avant le début du champ Bourrage.
- Prochain en-tête – ajout d'une exigence pour être capable de générer et éliminer les paquets factices de bourrage (Prochain en-tête = 59)
- ICV – modèle élargi pour s'accommoder des algorithmes en mode combiné.
- Algorithmes – Ajout des algorithmes de mode combiné de confidentialité.
- Déplacement des références aux algorithmes obligatoires dans un document séparé.
- Traitement de paquet entrant et sortant – il y a maintenant deux chemins :
  (1) algorithmes séparés de confidentialité et d'intégrité et
  (2) algorithmes de mode combiné de confidentialité. À cause de l'ajout des algorithmes en mode combiné, les sections de chiffrement/déchiffrement et d'intégrité ont été combinées pour le traitement des paquets entrants et sortants.

8. Considérations pour la rétro-compatibilité

Cette caractéristique n'existe pas dans ESP et aucun mécanisme ne permet aux homologues IPsec de découvrir ou négocier quelle version de ESP chacun utilise ou devrait utiliser. Cette section discute des problèmes de rétro-compatibilité qui en découlent.

D'abord, si aucune des nouvelles caractéristiques disponibles dans ESP v3 n'est employée, le format d'un paquet ESP est alors identique dans ESP v2 et v3. Si un algorithme de chiffrement en mode combiné est employé, caractéristique prise en charge seulement dans ESP v3, le format de paquet résultant peut différer de celui de la spécification ESP v2. Cependant, un homologue qui ne met en œuvre que ESP v2 ne va jamais négocier un tel algorithme, car ils sont définis pour la seule utilisation dans le contexte ESP v3.

La négociation de numéros de séquence étendus (ESN) est prise en charge par IKE v2 et a été traitée pour IKE v1 par l'Addendum ESN au domaine d'interprétation de IKE v1.

Dans le nouvel ESP (v3), on fait deux dispositions pour mieux prendre en charge la confidentialité des flux de trafic :
- bourrage arbitraire après la fin d'un paquet IP
- une convention d'élimination qui utilise Prochain en-tête = 59

La première caractéristique ne devrait pas causer de problèmes à un receveur, car le champ Longueur totale IP indique où se termine le paquet IP. Donc, tous les octets de bourrage TFC après la fin du paquet devraient être retirés à un certain point du traitement du paquet IP, après le traitement ESP, même si le logiciel IPsec ne retire pas un tel bourrage. Donc, c'est une caractéristique ESP v3 qu'un envoyeur peut employer sans considération de si le receveur met en œuvre ESP v2 ou v3.

La seconde caractéristique permet à un envoyeur d'envoyer une charge utile qui est une chaîne arbitraire d'octets qui ne constitue pas nécessairement un paquet IP bien formé, à l'intérieur d'un tunnel, pour les besoins de TFC. La question de savoir ce qu'un receveur ESP v2 va faire avec le champ Prochain en-tête dans un paquet ESP qui contient la valeur "59" reste ouverte. Il peut éliminer le paquet quand il trouve un en-tête IP mal formé, et enregistrer cet événement, mais il ne devrait certainement pas avoir une défaillance, parce que un tel comportement constituerait une vulnérabilité aux attaques de DoS par rapport au trafic reçu des homologues authentifiés. Donc cette caractéristique est une optimisation qu'un envoyeur ESP v3 peut utiliser sans considération de si un receveur met en œuvre ESP v2 ou ESP v3.

9. Remerciements

L'auteur tient à remercier de ses contributions Ran Atkinson, qui a joué un rôle éminent dans les activités IPsec initiales, et qui est l'auteur des premières séries des normes IPsec : les RFC 1825 à 1827. Karen Seo mérite des remerciements particuliers pour l'aide qu'elle a apportée à l'édition de la présente version de cette spécification ainsi que de la précédente. L'auteur tient aussi à remercier les membres des groupes de travail IPSEC et MSEC qui ont contribué au développement de cette spécification de protocole.

10. Références

10.1 Références normatives

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

[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)

10.2 Références pour information

[Bel96] Steven M. Bellovin, "Problem Areas for the IP Security Protocols", Proceedings of the Sixth Usenix Unix Security Symposium, juillet 1996.

[Kra01] Krawczyk, H., "The Order of Encryption et Authentication for Protecting Communications (Or: How Secure Is SSL?)", CRYPTO' 2001.

[NIST01] Federal Information Processing Standards Publication 140-2 (FIPS PUB 140-2), "Security Requirements for Cryptographic Modules", Information Technology Laboratory, National Institute of Standards et Technology, 25 mai 2001.

[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.

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

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

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

[Syverson] P. Syverson, D. Goldschlag, et M. Reed, "Anonymous Connections et Onion Routing", Proceedings of the Symposium on Security et Privacy, Oakland, CA, mai 1997, pages 44-54.

Appendice A Numéros de séquence étendus (64 bits)

A1 Généralités

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

A2 Fenêtre anti répétition

Le receveur va tenir une fenêtre anti répétition de taille W. Cette fenêtre va limiter l'importance du déclassement que peut avoir un paquet, par rapport au paquet avec le plus fort numéro de séquence qui a été authentifié jusqu'alors. (Aucune exigence n'est établie pour des tailles minimum ou recommandées pour cette fenêtre, au delà des valeurs de 32 et 64 par paquet déjà établies pour la fenêtre de numéro de séquence de 32 bits.
Cependant, il est suggéré qu'un développeur évalue ces valeurs par rapport au débit de l'interface prise en charge par une mise en œuvre qui utilise l'option ESN. Aussi, l'algorithme décrit ci-dessous suppose que la fenêtre ne dépasse pas 2^31 paquets.) 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 de leur définition.

Nom de variable	Taille (bits)	Signification
W	32	Taille de fenêtre
T	64	Plus grand numéro de séquence authentifié, 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 une vérification 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 seul sous espace de numéro de séquence. (Voir la Figure 1)
+ Cas B : Tl < (W - 1). Dans ce cas, la fenêtre s'étend sur deux sous espaces de numéro de séquence. (Voir la Figure 2)

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

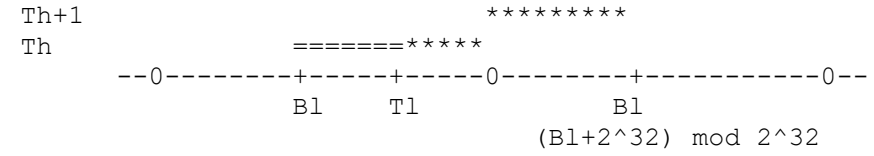


Figure 1 -- Cas A

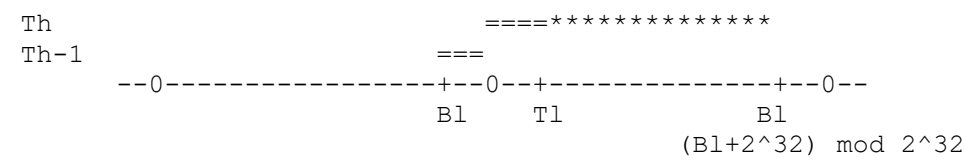


Figure 2 -- Cas B

A2.1 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 la valeur de 2^32 - 1. Le bit plancher correspond à B et le bit plafond 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 été reçu ou non et authentifié, de sorte que les répétitions puissent être détectées et rejetées.

Quand un paquet qui a un numéro de séquence (Seq) de 64 bits supérieur à T est reçu et validé,
+ B est augmenté de (Seq - T)
+ (Seq - T) bits sont éliminés de l'extrémité inférieure de la fenêtre
+ (Seq - T) bits sont ajoutés à l'extrémité supérieure de la fenêtre
+ le bit plafond est établi pour indiquer qu'un paquet avec ce numéro de séquence a été reçu et authentifié
+ les nouveaux bits entre T et le bit plafond sont établis pour indiquer qu'aucun paquet avec ces numéros de séquence n'a encore été reçu.
+ T est réglé au nouveau numéro de séquence

En vérifiant si des paquets sont répétés,
+ Dans le cas A :
Si Seql ≥ Bl (où Bl = Tl - W + 1) ET Seql ≤ Tl, on vérifie le bit correspondant dans la fenêtre pour voir si ce Seql a déjà été vu. Si oui, rejeter le paquet. Si non, effectuer une vérification d'intégrité (voir le paragraphe A2.2. Sur 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. Si non, effectuer une vérification d'intégrité (voir le paragraphe A2.2. Sur la détermination de Seqh).

A2.2 Détermination des bits de poids fort (Seqh) du numéro de séquence

Comme seul `Seql' va être transmis avec le paquet, le receveur doit déduire et tracer le sous espace de numéro de séquence dans lequel chaque paquet entre, c'est-à-dire, déterminer la valeur de Seqh. Les équations suivantes définissent comment choisir Seqh dans des conditions "normales" ; voir le paragraphe A3 pour une discussion de comment récupérer d'une perte extrême de paquets.

+ Dans le cas A (Figure 1) :

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

A2.3 Exemple de pseudo-code

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

```
Si (Tl ≥ W - 1)                    Cas A
   Si (Seql ≥ Tl - W + 1)
      Seqh = Th
      Si (Seql ≤ Tl)
         Si (passe la vérification de répétition)
            Si (passe la vérification d'intégrité)
               Établir le bit correspondant à Seql
               Passer le paquet
            Sinon rejeter le paquet
         Sinon rejeter le paquet
      Sinon
         Si (passe la vérification d'intégrité)
            Tl = Seql (faire glisser les bits)
            Établir le bit correspondant à Seql
            Passer le paquet
         Sinon rejeter le paquet
   Sinon
      Seqh = Th + 1
      Si (passe la vérification d'intégrité)
         Tl = Seql (faire glisser les bits)
         Th = Th + 1
         Établir le bit correspondant à Seql
         Passer le paquet
      Sinon rejeter le paquet
Sinon                              Cas B
   Si (Seql ≥ Tl - W + 1)
      Seqh = Th - 1
      Si (passe la vérification de répétition)
         Si (passe la vérification d'intégrité)
            Établir le bit correspondant à Seql
            Passer le paquet
         Sinon rejeter le paquet
      Sinon rejeter le paquet
   Sinon
      Seqh = Th
      Si (Seql ≤ Tl)
         Si (passe la vérification de répétition)
            Si (passe la vérification d'intégrité)
               Établir le bit correspondant à Seql
               Passer le paquet
            Sinon rejeter le paquet
         Sinon rejeter le paquet
      Sinon
         Si (passe la vérification d'intégrité)
            Tl = Seql (faire glisser les bits)
            Établir le bit correspondant à Seql
            Passer le paquet
         Sinon rejeter le paquet
```

A.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 paquets consécutifs ou plus 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 A2.2 vont échouer à donner la valeur correcte. Sauf si ce problème est détecté et réglé, les paquets suivants sur cette SA vont échouer à l'authentification et être 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 va probablement être détectée aux couches supérieures dans la plupart des cas, avant qu'IPsec doive invoquer le mécanisme de re-synchronisation décrit en A3.1 et A3.2. Si une fraction significative du trafic sur la SA en question est sur TCP, la source va échouer à recevoir les ACK et va arrêter d'envoyer bien avant que 2^32 paquets soient perdus. Aussi, pour toute application bidirectionnelle, même celles qui fonctionnent sur UDP, une telle panne étendue va probablement résulter en le déclenchement d'une certaine forme de fin de temporisation. Cependant, une application unidirectionnelle, fonctionnant sur UDP, peut manquer des retours qui causeraient une détection automatique d'une perte de cette ampleur, d'où les motivations pour développer une méthode de récupération pour ce cas.

Noter que les observations ci-dessus s'appliquent aux SA entre passerelles de sécurité, ou entre hôtes, ou entre hôte et passerelles de sécurité.

La solution choisie a été retenue pour :
+ minimiser l'impact sur le traitement du trafic normal,
+éviter de créer une opportunité pour une nouvelle attaque de déni de service comme il pourrait se produire si on permet à un attaquant de forcer un détournement de ressources sur un processus de re-synchronisation,
+ limiter le mécanisme de récupération au receveur – parce que l'anti répétition est un service pour le seul receveur, et que l'émetteur n'est généralement pas au courant de si le receveur utilise les numéros de séquence à l'appui de ce service facultatif, il est préférable que les mécanismes de récupération soit locaux chez le receveur. Cela permet aussi la rétro compatibilité.

A3.1 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 re-synchronisation, qui devrait être effectué en arrière plan, ou en utilisant un processeur séparé. La réception d'un paquet valide sur la SA remet le compteur à zéro. La valeur utilisée pour déclencher le processus de re-synchronisation est un paramètre local. Il n'est pas exigé de prendre en charge des valeurs de déclenchement distinctes pour des SA différentes, bien qu'une mise en œuvre puisse choisir de le faire.

A3.2 Processus de resynchronisation

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

Cette solution n'exige de soutien que de la part du receveur, permettant par là la rétro compatibilité. Aussi, comme l'effort de re-synchronisation va se produire en arrière plan ou utiliser un autre processeur, 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 complète de droits de reproduction

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