Groupe de travail Réseau
Request for Comments : 2207
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

L. Berger, FORE Systems
T. O'Malley, BBN
septembre 1997

Extensions à RSVP pour flux de données IPsec

Résumé

Le présent document présente des extensions à la version 1 de RSVP. Ces extensions permettent la prise en charge des flux de données individuels qui utilisent l'en-tête d'authentification (AH, *Authentication Header*) IP de la RFC 1826, ou l'encapsulation de charge utile de sécurité (ESP, *Encapsulating Security Payload*) IP de la RFC 1827. RSVP version 1 tel qu'il est actuellement spécifié peut prendre en charge le protocole IPsec, mais seulement adresse par adresse et protocole par protocole, et non sur la base du flux. Les extensions présentées peuvent être utilisées avec IPv4 comme IPv6.

Table des matières

1. Introduction

Des RFC en cours de normalisation publiées récemment spécifient les mécanismes de protocole pour fournir la sécurité de niveau IP. Ces protocoles de sécurité IP, ou IPsec, prennent en charge l'authentification au niveau du paquet, [RFC1826], et l'intégrité et la confidentialité [RFC1827]. Un certain nombre de mises en œuvre interopérables existent déjà et plusieurs fabricants ont annoncé les produits commerciaux qui vont utiliser ces mécanismes.

Les protocoles IPsec fournissent le service en ajoutant un nouvel en-tête entre l'en-tête IP d'un paquet et l'en-tête de protocole de transport (par exemple UDP). Les deux en-têtes de sécurité sont l'en-tête d'authentification (AH, *Authentication Header*) pour l'authentification, et l'encapsulation de charge utile de sécurité (ESP, *Encapsulating Security Payload*) pour l'intégrité et la confidentialité.

RSVP est développé comme protocole de réservation de ressources (établissement dynamique de qualité de service). Tel qu'il est actuellement spécifié par la [RFC2205], RSVP est conçu pour les paquets IP qui portent des protocoles qui ont des accès du style TCP ou UDP. Les protocoles qui n'ont pas de tels accès de type UDP/TCP, comme les protocoles IPsec,

peuvent être pris en charge, mais seulement avec des restrictions. En particulier pour les flux de paquets de données IPsec, la définition du flux ne peut être faite que sur la base de l'adresse IP, protocole par protocole.

Le présent mémoire propose des extensions à RSVP de sorte que les flux de données qui contiennent des protocoles IPsec puissent être contrôlés à une granularité similaire à celle qui est déjà spécifiée pour UDP et TCP. Les extensions proposées peuvent être utilisées avec IPv4 aussi bien que IPv6. La Section 2 de ce mémoire donne une vue d'ensemble des extensions. La Section 3 contient la description des mécanismes d'extension du protocole. La Section 4 présente les règles de traitement des extensions du protocole. La Section 5 définit les objets de données RSVP supplémentaires.

2. Vue d'ensemble des extensions

La notion de base est d'étendre RSVP à l'utilisation des indices de paramètre de sécurité IPsec (SPI, *Security Parameter Index*) à la place des accès de type UDP/TCP. Cela va exiger un nouvel objet FILTER_SPEC, qui va contenir le SPI IPsec, et un nouvel objet SESSION.

Alors que les SPI sont alloués sur la base de l'adresse de destination, ils vont être normalement associés à un envoyeur particulier. Il en résulte que deux envoyeurs à la même destination d'envoi individuel vont normalement avoir des SPI différents. Afin de prendre en charge le contrôle de plusieurs flux indépendants entre des adresses IP de source et de destination, le SPI va être inclus au titre de la FILTER_SPEC. Cependant, lorsque on utilisé le style WF *(Wildcard Filter, filtre générique)* tous les flux pour la même adresse IP de destination qui utilisent le même identifiant de protocole IP vont partager la même réservation. (Cette limitation existe parce que les en-têtes de transport IPsec ne contiennent pas de valeur de démultiplexage de destination comme l'accès de destination UDP/TCP.)

Bien que le format de message RESV ne change pas, le traitement de RESV va exiger des modifications. Le traitement de la nouvelle FILTER_SPEC IPsec va dépendre de l'utilisation du nouvel objet SESSION et de l'identifiant de protocole contenu dans la définition de session. Lorsque le nouvel objet FILTER_SPEC est utilisé, tous les quatre octets du SPI vont devoir être extraits de la FILTER_SPEC pour l'usage du classeur de paquet. La localisation du SPI dans l'en-tête de transport des paquets IPsec dépend du champ Identifiant de protocole.

L'extension va aussi exiger un changement du traitement de PATH, précisément dans l'usage du champ d'accès dans une définition de session. Une session RSVP est définie par le triplet : (AdresseDeDestination, Identifiant de protocole, AccèsDeDestination). La [RFC2205] comporte la définition d'un type d'objet SESSION, elle contient les accès de destination UDP/TCP, à savoir "une quantité de 16 bits portée au décalage d'octet +2 dans l'en-tête de transport" ou zéro pour les protocoles qui n'ont pas un tel champ. Les protocoles IPsec ne contiennent pas un tel champ, mais il reste une exigence pour les sessions de démultiplexage au delà de l'adresse de destination IP. Pour satisfaire à cette exigence, un accès de destination virtuel, dit vDstPort, est introduit. La valeur de vDstPort va être portée dans le nouvel objet SESSION mais pas dans l'en-tête de transport IPsec. Le vDstPort permet la différenciation de plusieurs sessions IPsec destinées à la même adresse IP. Voir à la Section 5 l'exposé sur les gammes de vDstPort.

Dans les messages PATH, le SENDER_TEMPLATE pour les flux IPsec aura le même format que la FILTER_SPEC modifiée. Mais un nouvel objet SESSION sera utilisé pour distinguer sans ambiguïté l'utilisation d'un accès de destination virtuel.

Le trafic sera transposé (classé) dans des réservations sur la base des SPI dans les FILTER_SPEC. Cela signifie, bien sûr, que lorsque WF est utilisé, tous les flux pour la même adresse de destination IP et avec le même identifiant de protocole IP vont partager la même réservation.

Les avantages de l'approche décrite sont qu'elle n'exige aucun changement aux RFC1826 et 1827 et qu'il n'y a pas de redondance supplémentaire par paquet de données. L'Appendice A contient un exposé des avantages de cette approche par rapport à plusieurs autres solutions de remplacement. Cette approche ne tire pas parti du champ Étiquette de flux IPv6, de sorte qu'une efficacité supérieures serait possible pour les flux IPv6. Les détails de l'utilisation de l'étiquette de flux IPv6 feront l'objet de travaux à venir.

3. Définition d'objet

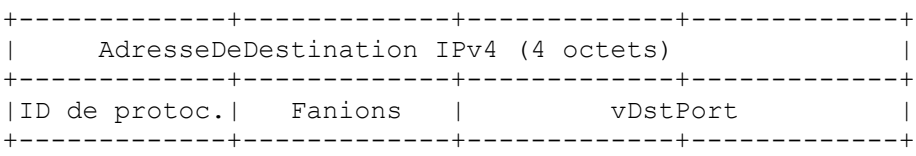
Les objets FILTER_SPEC et SENDER_TEMPLATE utilisés avec les protocoles IPsec vont contenir un champ de quatre octets qui sera utilisé pour porter le SPI. Plutôt que d'étiqueter le champ modifié avec une étiquette spécifique de IPsec, le SPI, l'étiquette "Identifiant d'accès généralisé" *(GPI, Generalized Port Identifier)* sera telle que ces objets puissent être réutilisés à l'avenir pour des usages non IPsec. Le nom de ces objets est IPv4/GPI FILTER_SPEC, IPv6/GPI FILTER_SPEC, IPv4/GPI SENDER_TEMPLATE, et IPv6/GPI SENDER_TEMPLATE. De même, les nouveaux objets

SESSION seront le IPv4/GPI SESSION et le IPv6/GPI SESSION. Quand on se réfère aux nouveaux objets, la version IP ne sera pas incluse sauf si une distinction spécifique est faite entre IPv4 et IPv6.

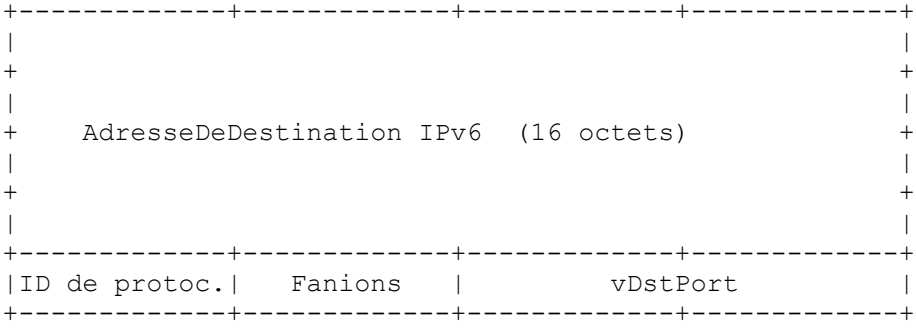
3.1 Classe de SESSION

La classe de SESSION est 1.

o objet SESSION IPv4/GPI : Classe = 1, C-Type = 3



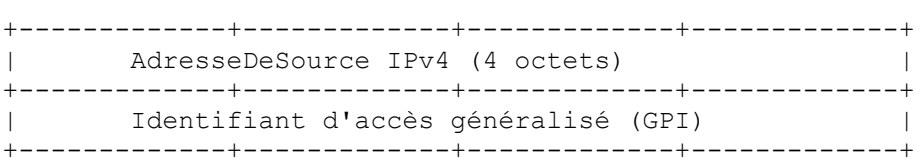
o objet SESSION IPv6/GPI : Classe = 1, C-Type = 4



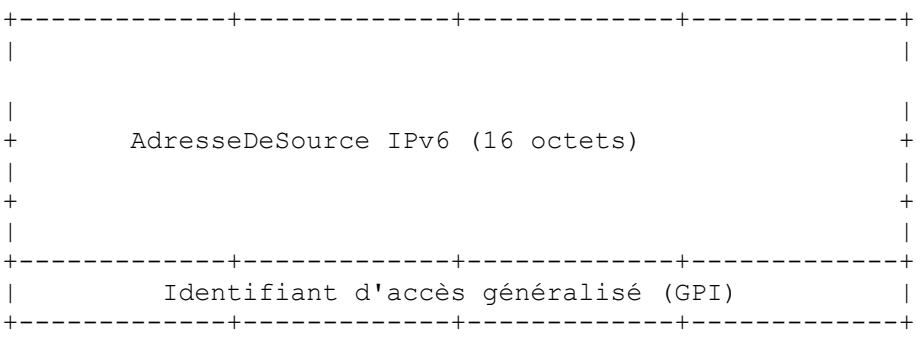
3.2 Classe de FILTER_SPEC

La classe de FILTER_SPEC est 10.

o Objet FILTER_SPEC IPv4/GPI : Classe = 10, C-Type = 4



o Objet FILTER_SPEC IPv6/GPI : Classe = 10, C-Type = 5



3.3 Classe SENDER_TEMPLATE

Classe SENDER_TEMPLATE = 11.

o Objet IPv4/GPI SENDER_TEMPLATE : Classe = 11, C-Type = 4

Même définition que pour l'objet IPv4/GPI FILTER_SPEC.

o Objet IPv6/GPI SENDER_TEMPLATE : Classe = 11, C-Type = 5

Même définition que pour l'objet IPv6/GPI FILTER_SPEC.

4. Règles de traitement

La présente section présente les ajouts aux règles de traitement présentées dans la [RFC2209]. Ces ajouts sont exigés afin de traiter correctement les objets GPI SESSION et FILTER_SPEC. Les valeurs des codes d'erreur référencés se trouvent dans la [RFC2205]. Comme dans les autres documents RSVP, les valeurs pour les erreurs rapportées en interne (API) ne sont pas définies.

4.1 Changements exigés

Le traitement de RESV et de PATH devra être changé pour prendre en charge les nouveaux objets. Les changements assurent la cohérence et étendent le traitement d'accès.

Les changements suivants du traitement du message PATH sont nécessaires :

o Lorsque une session est définie comme utilisant l'objet GPI SESSION, seul le GPI SENDER_TEMPLATE peut être utilisé. Lorsque cette condition est violée, les stations d'extrémité devraient rapporter l'erreur d'API "Conflit de C-Type" à l'application.

o Pour les messages PATH qui contiennent l'objet GPI SESSION, les stations d'extrémité doivent vérifier que l'identifiant de protocole correspond à un protocole connu pour utiliser l'objet GPI SESSION. Les valeurs 51 (AH) ou 50 (ESP) doivent être prises en charge par les mises en œuvre qui acceptent les extensions IPsec décrites. Si un identifiant de protocole inconnu est utilisé, l'API devrait alors rapporter une "Erreur d'API" à l'application.

o Pour de tels messages, la valeur vDstPort devrait être enregistrée. La valeur vDstPort fait partie de l'état enregistré et est utilisée pour établir la correspondance avec les messages Resv, mais elle n'est pas passée au contrôle de trafic. Une valeur différente de zéro de vDstPort est exigée. Cette exigence assure qu'un objet SESSION non GPI ne va jamais fusionner avec un objet SESSION GPI. La violation de cette condition cause une erreur d'API "Accès de destination invalide".

Les changements au traitement du message RESV sont :

o Lorsque un message RESV contient une FILTER_SPEC GPI, la session doit être définie comme utilisant l'objet SESSION GPI. Autrement, c'est une erreur de formatage de message.

o Le GPI contenu dans la FILTER_SPEC doit correspondre au GPI contenu dans le SENDER_TEMPLATE. Autrement, une erreur "Pas d'informations d'envoyeur pour ce message Resv" est générée.

o Lorsque la FILTER_SPEC GPI est utilisée, chaque nœud doit créer un classeur de données pour le flux décrit par le quartet: (AdresseDeDestination, Identifiant de protocole, AdresseDeSource, GPI). Le classeur de données aura besoin de chercher les quatre octets de GPI au décalage d'en-tête de transport +4 pour AH, et au décalage d'en-tête de transport +0 pour ESP.

4.2 Fusion des Flowspec

Quand on utilise cette extension pour les flux de données IPsec, les sessions RSVP sont définies par le triplet : (AdresseDeDestination, Identifiant de protocole, vDstPort). De même, un envoyeur est défini par la paire : (AdresseDeSource, GPI), où le champ GPI sera une représentation sur quatre octets d'un accès de source généralisé. Ces extensions ont des ramifications qui dépendent du style de réservation.

4.2.1 Styles FF et SE

Dans les styles FF et SE, l'objet FILTER_SPEC contient la paire (AdresseDeSource, GPI). Cela permet au receveur d'identifier de façon univoque les envoyeurs sur la base des deux éléments de la paire. Lors de la fusion de descripteurs d'envoyeur explicites, les envoyeurs ne peuvent être considérés comme identiques que lorsque les deux éléments sont identiques.

4.2.2 Style WF

Ces extensions ne fournissent qu'un service très limité lorsque elles sont utilisées avec des réservations de style WF. Comme décrit plus haut, les objets SENDER_TEMPLATE et FILTER_SPEC contiennent chacun le GPI. Dans une réservation de style WF, le message RESV ne contient pas de FILTER_SPEC (après tous, c'est un filtre générique) et l'objet SENDER_TEMPLATE est ignoré (encore une fois, parce que tout envoyeur est permis). Il en résulte que les classeurs peuvent faire correspondre tous les paquets qui contiennent à la fois l'adresse IP de destination et l'identifiant de protocole de la session avec de telles réservations WF.

Bien qu'on ne propose pas de solution pour cette limitation, cette question n'est pas considérée comme significative car les applications IPsec vont vraisemblablement peu utiliser les réservations de style WF.

5 Considérations relatives à l'IANA

La gamme des valeurs de vDstPort possibles est coupée en tronçons, de la même façon que les gammes d'accès UDP/TCP.

0	Valeur illégale
1 – 10	Réservée. Contacter les auteurs.
11 – 8191	Allouées par l' IANA
8192 – 65535	Allocation dynamique

L'IANA est chargée d'allouer les vDstPorts bien connus en utilisant les critères suivants :
Toute personne qui demande l'allocation d'un vDstPort doit fournir
a) un point de contact,
b) une brève description de l'utilisation prévue, et
c) un nom abrégé à associer à l'allocation (par exemple "ftp").

6 Considérations pour la sécurité

Les mêmes considérations que celles des [RFC2205], [RFC1826], et [RFC1827] s'appliquent aux extensions décrites dans la présente note. Deux points supplémentaires se rapportent à ces extensions.

Tout d'abord, le mécanisme vDstPort représente un autre élément de données sur le flux IP qui pourrait être accessible à un adversaire. De telles données peuvent être utiles à un adversaire qui effectue une analyse de trafic en surveillant non seulement les paquets de données du flux IP mais aussi les messages de contrôle RSVP associés à ce flux. La protection contre les attaques d'analyse de trafic sort du domaine d'application du présent mécanisme. Une approche possible pour empêcher de telles attaques serait le déploiement et l'utilisation de mécanismes appropriés de confidentialité de couche liaison, tels que le chiffrement.

Ensuite, les changements des valeurs de SPI pour un flux donné vont affecter les flux et les réservations RSVP. Les changements vont survenir chaque fois que le flux change son association de sécurité. De tels changements vont survenir chaque fois que les clés d'un flux sont recalculées (c'est-à-dire qu'il utilise une nouvelle clé). Les intervalles de calcul de nouvelles clés sont normalement réglés sur la base des niveaux de trafic, de la taille de la clé, des menaces qui pèsent sur l'environnement, et de l'algorithme de chiffrement utilisé. Lorsque un changement de SPI survient, il va dans la plupart des cas être nécessaire de mettre à jour (d'envoyer) les objets SENDER_TEMPLATE et FILTER_SPEC correspondants. Les mises en œuvre d'IPsec, les applications RSVP, et les mises en œuvre de stations d'extrémité RSVP devront tenir compte de la possibilité de changements de SPI pour assurer que leur comportement de réservation est approprié. Ce problème paraît tolérable, dans la mesure ou les intervalles de recalcul des clés sont sous le contrôle des administrateurs locaux.

Beaucoup des sessions RSVP, sinon la plupart, n'auront pas besoin de se confronter à ce problème de recalcul de clés. Pour ces applications qui n'ont pas besoin de traiter des changements de SPI durant une session, l'impact de l'envoi de nouveaux messages PATH et RESV va varier en fonction du style de réservation utilisé. Ceux qui construisent de telles applications peuvent vouloir choisir le style de réservation sur la base des interactions avec les changements de SPI.

Le moindre impact d'un changement de SPI sera sur les réservations de style WF. Pour de telles réservations, un nouvel objet SENDER_TEMPLATE devra être envoyé, mais aucune nouvelle RESV n'est nécessaire. Pour les réservations de style SE, un nouveau SENDER_TEMPLATE et une nouvelle RESV devront tous deux être envoyés. Il en résultera un changement d'état, mais cela ne devrait en aucune façon affecter la livraison du paquet de données ou l'allocation réelle des ressources. Le style FF sera le plus impacté. Comme avec SE, les messages PATH et RESV vont tous deux devoir être envoyés. Mais, comme les réservations de style FF ont pour résultat que l'envoyeur reçoit sa propre allocation de ressource, les ressources seront allouées deux fois pour une certaine période. Ou, encore pire, il n'y aura pas assez de ressources pour prendre en charge le nouveau flux sans préalablement libérer l'ancien.

Il existe une façon de se sortir de ce problème du changement du SPI dans le style FF. Les applications qui veulent le style de réservation FF peuvent utiliser plusieurs réservations SE. Chaque envoyeur réel aura une définition distincte de SESSION (vDstPort). Lorsque viendra le moment de changer les SPI, une réservation partagée pourrait être faite pour le nouveau SPI alors que le vieux SPI est encore actif. Une fois que le nouveau SPI est en service, la vieille réservation pourrait être éliminée. Ceci est sous optimal, mais fournira un service sans interruption pour bon nombre d'applications.

7. Références

[RFC2205] R. Braden, éd., L. Zhang, S. Berson, S. Herzog, S. Jamin, "Protocole de réservation de ressource (RSVP) -- version 1, spécification fonctionnelle", septembre 1997. (*MàJ par* RFC2750, RFC3936, RFC4495) *(P.S.)*

[RFC2209] R. Braden, L. Zhang, "Protocole de réservation de ressource (RSVP) -- version 1 : règles de traitement de message", septembre 1997. *(Information)*

[RFC1825] R. Atkinson, "Architecture de sécurité pour le protocole Internet", RFC 1825, août 1995. *(Rendue obsolète par la RFC2401, elle-même remplacée par la RFC4301)*

[RFC1826] R. Atkinson, "En-tête d'authentification IP", RFC 1826, août 1995. *(Rendue obsolète par la RFC2402, elle-même remplacée par les RFC4302, 4305)*

[RFC1827] R. Atkinson, "Encapsulation dans IP de charge utile de sécurité (ESP)", RFC 1827, août 1995. *(Obsolète, voir RFC2406; elle-même remplacée par la RFC4303)*

8 Remerciements

La présente note comporte des idées émises et révisées par un certain nombre de personnes qui n'ont pas participé à sa rédaction. Les auteurs tiennent à les remercier de leur contribution. Nous remercions Ran Atkinson <rja@cisco.com>, Fred Baker <fred@cisco.com>, Greg Troxel <gdt@bbn.com>, John Krawczyk <jkrawczyk@BayNetworks.com> de leurs apports et retours très appréciés. Des remerciements tout particuliers à Bob Braden <braden@isi.edu> pour ses commentaires rédactionnels et techniques détaillés. Nous remercions aussi Buz Owen, Claudio Topolcic, Andy Veitch et Luis Sanchez de leur aide sur le développement de l'approche proposée. Si des erreurs existent dans cette note, elles ne proviennent que des auteurs.

9 Adresse des auteurs

Lou Berger
FORE Systems
6905 Rockledge Drive
Suite 800
Bethesda, MD 20817
téléphone : 301-571-2534
mél : lberger@fore.com

Tim O'Malley
BBN Corporation
10 Moulton Street
Cambridge, MA 02138

téléphone : 617-873-3076
mél : timo@bbn.com

Appendice A Options prises en compte

Le présent appendice passe en revue les autres approches qui ont été explorée dans le développement des extensions décrites. Elles sont incluses ici pour apporter des éléments de contexte supplémentaires au problème général. Toutes les options citées ont été rejetées par le groupe de travail.

Quatre autres options ont été examinées :

1. Encapsulation UDP
   Ajouter un en-tête UDP entre l'en-tête IP et les en-têtes IPsec AH ou ESP.

2. Encapsulation d'en-tête d'identifiant de flux
   Ajouter un nouveau type d'en-tête entre l'en-tête IP et les en-têtes IPsec AH ou ESP.

3. Modification de IPsec
   Modifier les en-têtes IPsec de telle sorte qu'il y ait des champs appropriés aux mêmes endroits que les accès UDP et TCP.

4. Transparence de AH
   Sauter le traitement de classeur de paquet d'en-tête d'authentification.

A.1 Encapsulation UDP

Comme les objets SESSION et FILTER actuels attendent des accès UDP ou TCP, cette proposition dit de les donner. Le concept de base est d'ajouter un accès UDP entre les en-têtes IP et AH/ESP. Les accès UDP fourniraient la granularité de contrôle nécessaire pour associer les flux spécifiques aux réservations.

Les accès de source et de destination seraient utilisés, comme c'est normal, dans la définition et le contrôle de session RSVP. Les champs d'accès devraient aussi être utilisés pour identifier le protocole de niveau transport réel (par exemple ESP) utilisé. Comme aussi de nombreux accès UDP sont alloués tout autant que des accès connus, l'utilisation de numéros d'accès serait limité. Ainsi, les champs d'accès devraient être utilisés pour identifier de façon non ambiguë 1) le protocole du prochain niveau, 2) la session RSVP, et 3) la réservation RSVP.

L'avantage de cette option est qu'aucun changement à RSVP n'est nécessaire. L'inconvénient est que, comme les en-têtes ne sont pas à l'endroit attendu, les RFC 1826 et 1827 sont violées.

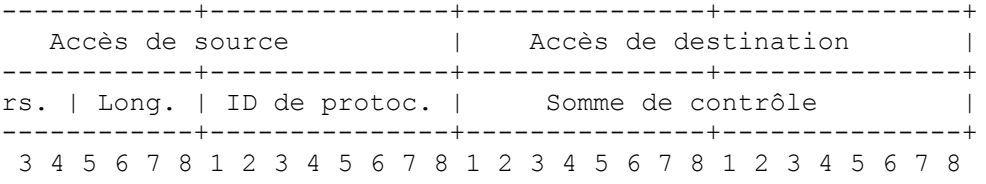
A.2 Encapsulation d'en-tête d'identifiant de flux

[Cette option a été proposée à l'origine par Greg Troxel <gdt@bbn.com>.]

Cette option est très similaire à l'option 1, mais elle est plus générique et aurait pu être adoptée comme solution standard. Le concept est d'utiliser des accès de style UDP dans le seul but d'identification du flux. RSVP traiterait ce nouveau protocole exactement comme UDP.

La différence avec l'encapsulation UDP est dans le traitement de l'hôte de destination. Celui-ci ignorerait essentiellement les informations d'accès et utiliserait un nouveau champ, Identifiant de protocole, pour identifier le protocole qui devrait traiter le prochain paquet. Des exemples d'identifiants de protocole correspondent à TCP, UDP, ESP, ou AH.

Le format de l'en-tête Identifiant de flux serait :



Accès de source de 2 octets
Accès de destination de 2 octets
Version sur 4 bits (1)
Longueur sur 4 bits 32 (2)
Identifiant de protocole de 8 bits
Somme de contrôle de 16 bits

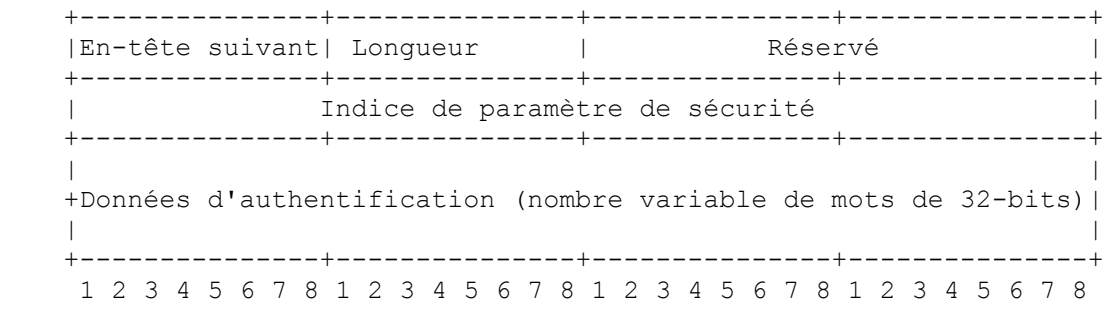
L'avantage de ce protocole est que l'identification de flux est séparée de tous les autres traitements de protocole. L'inconvénient est que l'ajout d'un en-tête viole les RFC 1826 et 1827, et aussi que les applications qui utilisent RSVP vont avoir besoin d'ajouter cet en-tête supplémentaire sur tous les paquets de données dont les en-têtes de transport n'ont pas d'accès de style UDP/TCP.

A.3 Modification du protocole IPsec

La notion de base de cette option est de laisser RSVP tel que spécifié actuellement et d'utiliser l'identifiant d'association de sécurité (SPI) trouvé dans les en-têtes IPsec pour l'identification du flux. L'utilisation du SPI pose deux problèmes. Le premier est que le SPI est situé au mauvais endroit quand on utilise l'en-tête d'authentification (AH). Le second problème est celui de la façon d'utiliser le SPI.

Le premier problème est facile à régler, mais en violant la RFC 1826. UDP et TCP ont des allocations d'accès dans les quatre premiers octets de leurs en-têtes, longs chacun de deux octets, la source vient en premier, puis la destination. L'en-tête ESP a le SPI ou même endroit que les accès UDP/TCP, pas l'AH.

L'en-tête d'authentification IP a la syntaxe suivante :



En inversant simplement les quatre premiers octets avec le SPI, on aura le SPI à l'endroit que RSVP attend. Cela serait non standard, ou exigerait un changement majeur (c'est-à-dire, non rétro compatible) à la RFC 1826 sur RSVP.

Le second problème est comment utiliser le SPI. Selon la spécification RSVP actuelle, les deux premiers octets du SPI d'un flux doivent être portés dans le message PATH et les deux octets suivants dans le message RESV. Le plus gros problème est que le SPI est normalement choisi par le receveur et va vraisemblablement être différent pour CHAQUE envoyeur. (Il y a un cas particulier où le même SPI est utilisé par tous les envoyeurs dans un groupe de diffusion groupée. Mais c'est un cas particulier.) Il est possible que le SPI soit choisi avant de commencer la session. RSVP Cela va fonctionner dans le cas de l'envoi individuel et dans le cas particulier de la diffusion groupée. Mais utiliser cette approche signifie que le temps d'établissement sera normalement étendu d'au moins un délai d'aller-retour. On ne voit pas très bien comment prendre en charge les réservations de style FF et WF.

L'avantage de cette approche est de ne pas changer RSVP. L'inconvénient est que cela apporte des modifications à la RFC1827 et que cela limite la prise en charge des styles de réservation RSVP.

A.4 Transparence de AH

La source du problème de la prise en charge par RSVP des protocoles IPsec est que l'en-tête réel de transport ne se trouve pas à l'endroit attendu. Avec les paquets ESP, les accès réels de source et de destination sont chiffrés et donc sans utilité pour RSVP. Ce n'est pas le cas pour l'authentification. Pour AH, l'en-tête réel suit directement l'en-tête d'authentification. Il serait ainsi possible d'utiliser l'en-tête de transport réel pour la définition et la réservation de session RSVP.

Pour utiliser l'en-tête de transport, tout ce qui devrait être fait est que le classeur de flux saute AH avant de classer les paquets. Aucune modification des formats RSVP ou du traitement d'établissement ne serait nécessaire. Les applications feraient les réservations sur la base des accès de transport (c'est-à-dire, UDP ou TCP) comme d'habitude.

Les avantages de cette approche sont qu'il n'y a de changement ni aux protocoles IPsec ni aux formats RSVP. L'inconvénient majeur est que les routeurs et les hôtes doivent sauter tous les AH avant de classer les paquets. Le groupe de travail a décidé qu'il était préférable d'avoir une solution cohérente à la fois pour AH et pour ESP.