Groupe de travail Réseau
**Request for Comments : 3554**
Catégorie : En cours de normamisation
Traduction Claude Brière de L'Isle

S. Bellovin & J. Ioannidi, AT&T Labs - Research
A. Keromytis, Columbia University
R. Stewart, Cisco
juillet 2003

# Utilisation du protocole de transmission de contrôle de flux (SCTP) avec IPsec



**Résumé**
Le présent document décrit les exigences fonctionnelles pour IPsec (RFC2401) et l'échange de clé Internet (IKE, *Internet Key Exchange*) [RFC 2409] pour faciliter leur utilisation dans la sécurisation du trafic SCTP [RFC2960].

## 1. Introduction

Le protocole de transmission de contrôle de flux (SCTP, *Stream Control Transmission Protocol*) est un protocole de transport fiable qui fonctionne par dessus un réseau de paquets sans connexion comme IP. SCTP est conçu pour le transport des messages de signalisation du réseau téléphonique public commuté (RTPC) sur les réseaux IP, mais il est capable d'applications plus larges.

Lorsque SCTP est utilisé sur des réseaux IP, il peut utiliser la suite des protocoles de sécurité IP [RFC2402], [RFC2406] pour l'intégrité et la confidentialité. Pour établir de façon dynamique les associations de sécurité (SA, *Security Association*) IPsec, un protocole de négociation de clé tel que IKE [RFC2409] peut être utilisé.

Le présent document décrit les exigences fonctionnelles pour IPsec et IKE pour faciliter leur utilisation à la sécurisation du trafic SCTP. En particulier, on expose un soutien supplémentaire sous la forme d'un nouveau type d'identifiant dans IKE [RFC2409] et des choix de mise en œuvre dans le traitement IPsec pour s'accommoder de la multiplicité des adresses de source et de destination associées à une seule association SCTP.

### 1.1 Terminologie

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans la [RFC2119].

## 2. SCTP sur IPsec

Lorsque on utilise les protocoles d'en-tête d'authentification [RFC2402] ou d'encapsulation de charge utile de sécurité [RFC2406] pour fournir des services de sécurité aux trames SCTP, la trame SCTP est traitée comme tout autre protocole de couche transport par dessus IP (comme TCP, UDP, etc.)

Les mises en œuvre de IPsec devraient déjà être capables d'utiliser le numéro de protocole de transport SCTP alloué par l'IANA comme sélecteur dans leur base de données de politique de sécurité (SPD, *Security Policy Database*). Les mises en œuvre de SCTP existantes devraient bénéficier directement de l'extension consistant à utiliser les numéros d'accès de source et destination SCTP comme sélecteurs dans la SPD. Comme le concept d'un accès, et sa localisation dans l'en-tête de transport, sont spécifiques du protocole, le code IPsec chargé d'identifier les accès de protocole de transport a besoin d'être convenablement modifié. Cela n'est cependant pas suffisant pour prendre pleinement en charge l'utilisation de SCTP en

conjonction avec IPsec.

Comme SCTP peut négocier des ensembles d'adresses de source et de destination (pas nécessairement dans le même sous-réseau ou gamme d'adresses) cela peut être utilisé dans le contexte d'une seule association, la SPD devrait être capable de s'accommoder de cela. La façon directe, et coûteuse, est de créer une entrée de SPD pour chaque paire d'adresses de source/destination négociée. Une meilleure approche est d'associer des ensembles d'adresses aux sélecteurs de source et de destination dans chaque entrée de SPD (dans le cas de trafic non SCTP, ces ensembles contiendraient seulement un élément). Bien que ceci soit une décision de la mise en œuvre, celles–ci sont encouragées à suivre cette voie ou une approche similaire lors de la conception ou modification d'une SPD pour s'accommoder de sélecteurs spécifiques de SCTP.

De même, les SA peuvent avoir plusieurs adresses de source et destination associées. Donc, une SA est identifiée par le triplet étendu {(ensemble des adresses de destination), SPI, Protocole de sécurité}. Une recherche dans la base de données des associations de sécurité (SADB, *Security Association Database*) en utilisant le triplet (Adresse de destination, SPI, Protocole de sécurité) où "Adresse de destination" est toute adresse d'homologue négociée, DOIT retourner la même SA.

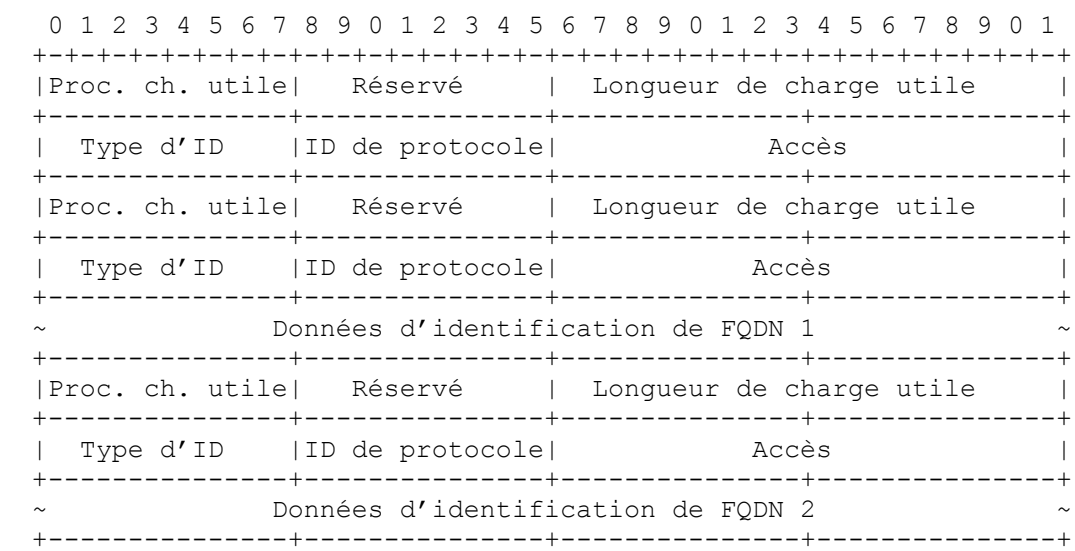
## 3. SCTP et IKE

Deux problèmes relèvent de l'utilisation de IKE lors de la négociation de la protection du trafic SCTP :

a) Comme SCTP permet que plusieurs adresses réseau de source et de destination soient associées à une association SCTP, il DOIT être possible que IKE négocie efficacement celles-ci dans l'échange de phase 2 (Mode rapide). L'approche directe est de négocier une paire de SA IPsec pour chaque combinaison d'adresses de source et de destination. Il peut en résulter un nombre inutilement grand de SA, perdant ainsi du temps (en les négociant) et de la mémoire. Toutes les mises en œuvre actuelles de IKE prennent en charge cette fonctionnalité. Cependant, une méthode pour spécifier plusieurs sélecteurs dans la phase 2 est désirable pour les besoins de l'efficacité. La conformité au présent document requiert que les mises en œuvre adhèrent aux lignes directrices du reste de cette section.

Définir un nouveau type d'identifiant, ID_LIST, qui permette une inclusion récurrente des identifiants. Donc, l'identifiant d'initiateur de IKE phase 2 pour une association SCTP PEUT être du type ID_LIST, qui contiendrait à son tour autant d'identifiants d'ID_IPV4_ADDR que nécessaire pour décrire les adresses d'initiateur ; et la même chose pour les identifiants de répondeur. Noter que d'autres types de sélecteur PEUVENT être utilisés lors de l'établissement de SA à utiliser avec SCTP, si il n'y a pas besoin d'utiliser la négociation de plusieurs adresses pour chaque point d'extrémité SCTP (c'est-à-dire, si une seule adresse est utilisée par chaque homologue d'un flux SCTP). Les mises en œuvre DOIVENT prendre en charge ce nouveau type d'identifiant.
Les identifiants de ID_LIST ne peuvent pas apparaître à l'intérieur des charges utiles d'identifiant ID_LIST. Tous les types d'identifiants définis dans la [RFC2407] peuvent être inclus à l'intérieur d'un identifiant d'ID_LIST. Chacun des identifiants contenus dans l'identifiant de ID_LIST doit comporter un en-tête Charge utile d'identification complet.

Le diagramme ci-dessous illustre le contenu de toute charge utile d'identifiant de ID_LIST qui contient deux charges utiles ID_FQDN *(Fully Qualified Domain Name,* nom de domaine complet*)*.




Le champ Prochaine charge utile dans tout identifiant inclus (pour FQDN 1 et FQDN 2) DOIT être ignoré par le répondeur.

Les champs Longueur de charge utile, Type d'identifiant, Identifiant de protocole, et Accès des charges utiles incluses devraient être réglés aux valeurs appropriées. Les champs Identifiant de protocole et Accès de la charge utile de ID_LIST devraient être réglés à zéro par l'initiateur et DOIVENT être ignorés par le répondeur.

Différents types d'identifiants (par exemple, un ID_FQDN et un ID_IPV4_ADDR) peuvent être inclus à l'intérieur du même identifiant d'ID_LIST. Si un type d'identifiant inclus dans une charge utile d'identifiant de ID_LIST est invalide dans le contexte où l'identifiant de ID_LIST est utilisé, la ID_LIST toute entière devrait être considérée comme fautive, par exemple, si une charge utile d'identifiant de ID_LIST qui contient un ID_FQDN et un ID_IPV4_ADDR est reçue durant un échange IKE en mode rapide, le répondeur devrait signaler une faute à l'initiateur et cesser le traitement du message (le même comportement qu'il adopterait si un ID_FQDN était simplement reçu à la place).

Le numéro alloué par l'IANA pour l'identifiant de ID_LIST est 12.

b) Pour que IKE soit capable de valider les sélecteurs de phase 2, il doit être possible d'échanger des informations suffisantes durant la phase 1. Actuellement, IKE peut directement s'accommoder du cas simple de deux homologues qui se parlent, en utilisant les identifiants de phase 1 qui correspondent à leurs adresses IP, et en codant ces mêmes adresses dans le SubjAltName des certificats utilisés pour authentifier l'échange de phase 1. Pour des scénarios plus compliqués, il faut consulter une politique externe (ou quelque autre mécanisme) pour valider les sélecteurs de phase 2 et les paramètres de SA. Toutes les adresses présentées dans les sélecteurs de phase 2 DOIVENT être validées. C'est-à-dire que des preuves suffisantes doivent être présentées au répondeur que l'initiateur est autorisé à recevoir du trafic pour toutes les adresses qui apparaissent dans les sélecteurs de phase 2. Ces preuves peuvent être déduites des certificats échangés durant la phase 1 (si possible) ; autrement, elles doivent être acquises par des moyens hors bande (par exemple, des mécanismes de politique, configurés par l'administrateur, etc.).

Pour s'accommoder du même scénario simple dans le contexte d'adresses de source/destination multiples dans une association SCTP, il DOIT être possible de :

1) Spécifier plusieurs identifiants de phase 1, qui sont utilisés pour valider les paramètres de phase 2 (en particulier, les sélecteurs de phase 2). Conformément à la discussion sur le type d'identifiant de ID_LIST, il est possible d'utiliser la même méthode pour spécifier plusieurs identifiants de phase 1.

2) Authentifier les divers identifiants de phase 1. En utilisant l'authentification de clé pré partagées, ceci est possible en associant la même clé partagée avec tous les identifiants de phase 1 d'homologue acceptable. Dans le cas de certificats, on a deux solutions :
   a) Le même certificat peut contenir plusieurs identifiants codés dans le champ SubjAltName, comme une séquence ASN.1. Comme ceci est déjà possible, c'est la solution préférée et toute mise en œuvre conforme DOIT l'accepter.
   b) Plusieurs certificats PEUVENT être passés durant l'échange de phase 1, dans plusieurs charges utiles CERT. Cette caractéristique est aussi prise en charge par la spécification actuelle. Comme une seule signature peut être produite par échange IKE phase 1, il est nécessaire que tous les certificats contiennent la même clé que leur sujet. Cependant, cette approche n'offre aucun avantage significatif par rapport à (a), donc les mises en œuvre PEUVENT la prendre en charge.

Dans l'un et l'autre cas, une mise en œuvre de IKE a besoin de vérifier la validité de l'identifiant de phase 1 revendiqué par un homologue, pour tous les identifiants ainsi reçus au cours d'un échange.

Bien que SCTP ne prenne actuellement pas en charge la modification des adresses associées à une association SCTP (lorsque celle-ci est en cours d'utilisation) c'est une caractéristique qui pourrait être prise en charge à l'avenir. Sauf si l'ensemble d'adresses change extrêmement souvent, il est suffisant de faire un échange de phase 1 et de phase 2 complet pour établir les sélecteurs et SA appropriés.

La dernière question à l'égard de SCTP et IKE relève de l'offre initiale de sélecteurs de phase 2 (les identifiants) par l'initiateur. Selon la spécification IKE actuelle, le répondeur doit envoyer dans le second message du mode rapide les identifiants reçus dans le premier message. Donc, on suppose que l'initiateur connaît déjà tous les sélecteurs pertinents pour cette association SCTP. Cependant, dans la plupart des cas, le répondeur a une connaissance plus précise de ses diverses adresses. Donc, les sélecteurs IPsec établis peuvent être potentiellement insuffisants ou inappropriés.

Si l'ensemble de sélecteurs proposé n'est pas approprié du point de vue du répondeur, ce dernier peut commencer un nouvel échange en mode rapide. Dans ce nouvel échange en mode rapide, les rôles d'initiateur et de répondeur ont été inversés ; le nouvel initiateur DOIT copier la SA et les sélecteurs de l'ancien message de mode rapide, et modifier son ensemble de sélecteurs pour correspondre à la réalité. Toutes les mises en œuvre IKE qui prennent en charge SCTP DOIVENT être capables de faire cela.

## 4. Considérations sur la sécurité

Le présent document expose l'utilisation d'un protocole de sécurité (IPsec) dans le contexte d'un nouveau protocole de transport (SCTP). SCTP, avec ses dispositions pour la mobilité, ouvre la possibilité d'attaques en redirection du trafic par lesquelles un attaquant X prétend que son adresse devrait être ajoutée à une session SCTP entre les homologues A et B, et être utilisée pour la suite des communications. De cette manière, le trafic entre A et B peut être vu de X. Si X n'est pas dans le chemin de communication entre A et B, SCTP lui offre de nouvelles capacités d'attaques. Donc, toutes ces mises à jour d'adresses de sessions SCTP devraient être authentifiées. Comme IKE négocie les SA IPsec pour les utiliser dans ces sessions, IKE DOIT valider toutes les adresses rattachées à un point d'extrémité SCTP soit en validant les certificats qui lui sont présentés durant l'échange de phase 1, soit par une méthode hors bande.

Le répondeur dans un échange de phase 2 DOIT vérifier l'autorité de l'initiateur à recevoir le trafic pour toutes les adresses qui apparaissent dans les sélecteurs de phase 2 de l'initiateur. Ne pas le faire permettrait que tout homologue valide du répondeur (c'est-à-dire, tous ceux qui peuvent réussir à établir une SA de phase 1 avec le répondeur) voit tout le trafic d'un autre homologue valide en revendiquant son adresse.

## 5. Considérations relatives à l'IANA

L'IANA a alloué le numéro 12 à ID_LIST (défini à la Section 3) dans le registre "Type d'identification IPsec" tiré du tableau des identifiants du protocole d'association de sécurité Internet et de gestion de clés (ISAKMP, *Internet Security Association and Key Management Protocol*).

## 6. Notice de propriété intellectuelle



## Références normatives

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

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

[RFC2406] S. Kent et R. Atkinson, "Encapsulation de charge utile de sécurité IP (ESP)", novembre 1998. *(Obsolète, voir* RFC4303)

[RFC2407] D. Piper, "Le domaine d'interprétation de sécurité IP de l'Internet pour ISAKMP", novembre 1998. *(Obsolète, voir la* RFC4306)

[RFC2408] D. Maughan, M. Schertler, M. Schneider et J. Turner, "Association de sécurité Internet et protocole de gestion de clés (ISAKMP)", novembre 1998. *(Obsolète, voir la* RFC4306)

[RFC2409] D. Harkins et D. Carrel, "L'échange de clés Internet (IKE)", novembre 1998. *(Obsolète, voir la* RFC4306)

[RFC2960] R. Stewart et autres, "Protocole de transmission de commandes de flux", octobre 2000. (*Obs., voir* RFC4960)*(P.S.)*

## Adresses des auteurs

Steven M. Bellovin
AT&T Labs - Research
180 Park Avenue
Florham Park, New Jersey 07932-0971
téléphone : +1 973 360 8656
mél : smb@research.att.com

John Ioannidis
AT&T Labs - Research
180 Park Avenue
Florham Park, New Jersey 07932-0971
mél : ji@research.att.com

Angelos D. Keromytis
Columbia University, CS Department
515 CS Building
1214 Amsterdam Avenue, Mailstop 0401
New York, New York 10027-7003
téléphone : +1 212 939 7095
mél : angelos@cs.columbia.edu

Randall R. Stewart
24 Burning Bush Trail.
Crystal Lake, IL 60012
téléphone : +1-815-477-2127
mél : rrs@cisco.com

## Déclaration complète de droits de reproduction



**Remerciement**
Le financement de la fonction d'édition des RFC est actuellement fourni par l'Internet Society.