Groupe de travail Réseau
Request for Comments : 3948
Catégorie : En cours de normalisation
janvier 2005
Traduction Claude Brière de L'Isle

A. Huttunen, F-Secure Corporation
B. Swander, Microsoft
V. Volpe, Cisco Systems
L. DiBurro, Nortel Networks
M. Stenberg

Encapsulation UDP de paquets ESP IPsec

Résumé
La présente spécification de protocole définit des méthodes pour encapsuler et désencapsuler les paquets de charge utile de sécurité encapsulés dans IP (ESP, *Encapsulating Security Payload*) à l'intérieur de paquets UDP pour la traversée de traducteurs d'adresse réseau. L'encapsulation ESP, comme définie dans le présent document, peut être utilisée dans des scénarios IPv4 et IPv6. Chaque fois qu'elle est négociée, l'encapsulation est utilisée avec l'échange de clés Internet (IKE, *Internet Key Exchange*).

Table des matières

1. Introduction

La présente spécification de protocole définit des méthodes pour encapsuler et désencapsuler des paquets ESP à l'intérieur de paquets UDP pour la traversée des traducteurs d'adresse réseau (NAT, *Network Address Translator*) (Voir le cas i du paragraphe 2.2 de la [RFC3715]). Les numéros d'accès UDP sont les mêmes que ceux utilisés par le trafic IKE, tel que défini dans la [RFC3947].

Le partage des numéros d'accès pour les deux trafics IKE et ESP encapsulé dans UDP a été choisi parce qu'il offre de meilleures qualités d'adaptation (une seule transposition de NAT dans le NAT ; il n'est pas besoin d'envoyer des Garder en

vie IKE séparés) une configuration facile (un seul accès à configurer dans les pare-feu) et une mise en œuvre facile.

Les besoins d'un client devraient déterminer si le mode transport ou le mode tunnel est à prendre en charge (voir la [RFC3715], Section 3, "Scénario de télécommutant"). Les clients L2TP/IPsec DOIVENT prendre en charge les modes définis dans la [RFC3193]. Les clients IPsec en mode tunnel DOIVENT accepter le mode tunnel.

Une mise en œuvre IKE qui prend en charge la présente spécification NE DOIT PAS utiliser le champ ESP SPI zéro pour les paquets ESP. Cela assure que les paquets IKE et les paquets ESP peuvent être distingués les uns des autres.

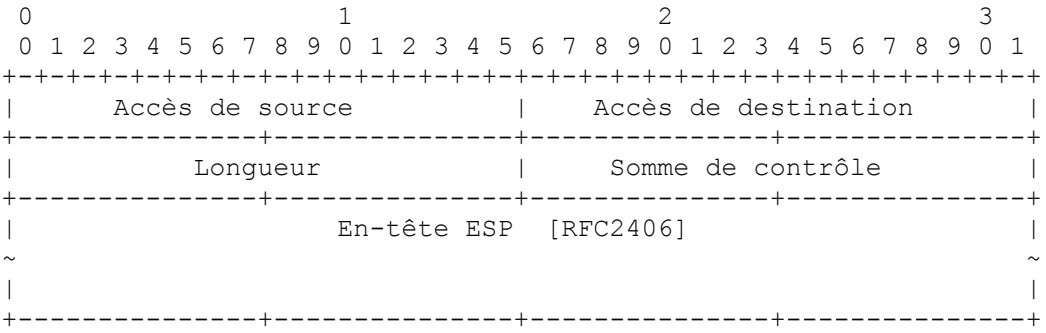
Comme défini dans le présent document, l'encapsulation UDP de paquets ESP est écrite en termes d'en-têtes IPv4. Il n'y a pas de raison technique pour qu'un en-tête IPv6 ne puisse pas être utilisé comme en-tête externe et/ou comme en-tête interne.

Parce que la protection des adresses IP externes dans l'AH *(Authentication Header, en-tête d'authentification)* IPsec est par nature incompatible avec le NAT, le AH IPsec a été laissé en dehors du champ d'application de la présente spécification. Le présent protocole suppose aussi que IKE [RFC2401] ou IKEv2 [RFC4306] est utilisé pour négocier les SA IPsec. La gestion de clés manuelle n'est pas acceptée.

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 [RFC2119].

2. Formats de paquet

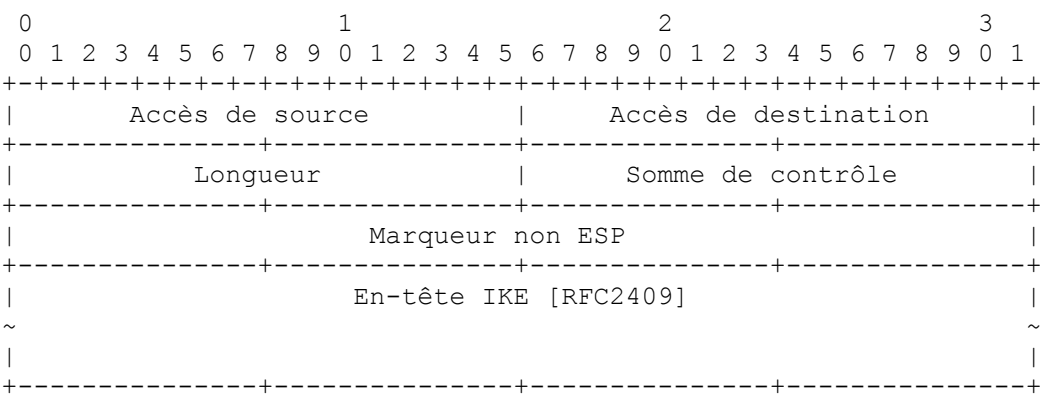
2.1 Format d'en-tête ESP encapsulé dans UDP



L'en-tête UDP est un en-tête standard [RFC0768], où
- o l'accès de source et l'accès de destination DOIVENT être les mêmes que ceux utilisés par le trafic IKE,
- o la somme de contrôle UDP IPv4 DEVRAIT être transmise comme valeur de zéro, et
- o les receveurs NE DOIVENT PAS dépendre de ce que la somme de contrôle UDP soit une valeur de zéro.

Le champ SPI dans l'en-tête ESP NE DOIT PAS avoir une valeur de zéro.

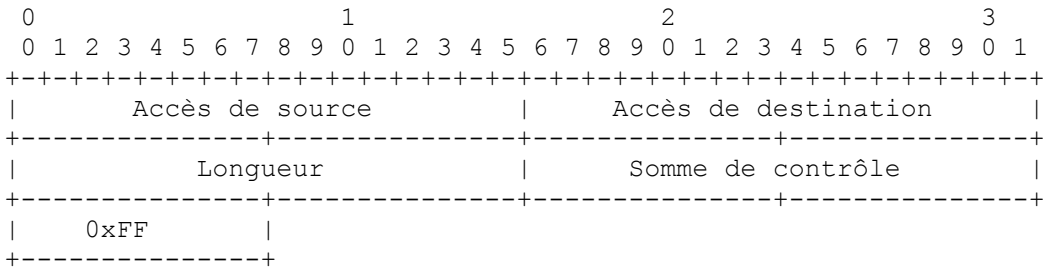
2.2 Format d'en-tête IKE pour l'accès 4500



L'en-tête UDP est un en-tête standard [RFC0768] et il est utilisé comme défini dans la [RFC3947]. Le présent document n'établit aucune nouvelle exigence pour le traitement de la somme de contrôle d'un paquet IKE.

Un marqueur non ESP est constitué de quatre octets de valeur zéro qui s'alignent sur le champ SPI d'un paquet ESP.

2.3 Format de paquet Garder en vie de NAT



L'en-tête UDP est un en-tête standard [RFC0768], où
- o l'accès de source et l'accès de destination DOIVENT être les mêmes que ceux utilisés pour l'encapsulation UDP-ESP du paragraphe 2.1,
- o la somme de contrôle UDP IPv4 DEVRAIT être transmise comme valeur zéro, et
- o les receveurs NE DOIVENT PAS dépendre de ce que la somme de contrôle UDP soit de valeur zéro.

L'envoyeur DOIT utiliser une charge utile d'un octet avec la valeur 0xFF. Le receveur DEVRAIT ignorer un paquet de NAT Garder en vie reçu.

3. Procédures d'encapsulation et de désencapsulation

3.1 Procédures auxiliaires

3.1.1 Procédure de NAT de désencapsulation de mode tunnel

Lorsque un mode tunnel a été utilisé pour transmettre des paquets (voir la section 3, critères "Prise en charge du mode" et "Scénario de télécommutant" de la [RFC3715]) l'en-tête IP interne peut contenir des adresses qui ne conviennent pas pour le réseau en question. Cette procédure définit comment ces adresses sont à convertir en adresses convenables pour le réseau en cause.

Selon la politique locale, une des procédures suivantes DOIT être appliquée :
1. Si un espace d'adresses IP de source valide a été défini dans la politique pour les paquets encapsulés provenant de l'homologue, vérifier que l'adresse IP de source du paquet interne est valide selon cette politique.
2. Si une adresse a été allouée pour l'homologue distant, vérifier que l'adresse IP de source utilisée dans le paquet interne est l'adresse IP allouée.
3. La traduction d'adresse réseau est effectuée pour le paquet, le rendant acceptable au transport dans le réseau local.

3.1.2 Procédure de NAT de désencapsulation de mode Transport

Lorsque le mode transport a été utilisé pour transmettre des paquets, les en-têtes TCP ou UDP contenus auront des sommes de contrôle incorrectes du fait des changements de parties de l'en-tête IP durant le transit. Cette procédure définit comment corriger ces sommes de contrôle (voir le cas b du paragraphe 2.1 de la [RFC3715]).

Selon la politique locale, une des procédures suivantes DOIT être effectuée :
1. Si l'en-tête de protocole après l'en-tête ESP est un en-tête TCP/UDP et si l'adresse IP réelle de source et de destination de l'homologue a été reçue conformément à la [RFC3947], recalculer de façon incrémentaire la somme de contrôle TCP/UDP:
   - * Soustraire de la somme de contrôle l'adresse IP de source dans le paquet reçu.
   - * Ajouter l'adresse IP de source réelle reçue via IKE à la somme de contrôle (obtenue du NAT-OA)
   - * Soustraire de la somme de contrôle l'adresse IP de destination du paquet reçu.
   - * Ajouter l'adresse IP de destination réelle reçue via IKE à la somme de contrôle(obtenue du NAT-OA).

Note : Si l'adresse reçue et l'adresse réelle sont les mêmes pour une certaine adresse (par exemple, disons l'adresse de

source) les opérations s'annulent et n'ont pas besoin d'être effectuées.
2. Si l'en-tête de protocole après l'en-tête ESP est un en-tête TCP/UDP, recalculer le champ Somme de contrôle dans l'en-tête TCP/UDP.
3. Si l'en-tête de protocole après l'en-tête ESP est un en-tête UDP, régler le champ Somme de contrôle à zéro dans l'en-tête UDP. Si l'en-tête de protocole après l'en-tête ESP est un en-tête TCP, et si il y a une option pour étiqueter la pile disant que la somme de contrôle TCP n'a pas besoin d'être calculée, ce fanion peut alors être utilisé. Cela ne DEVRAIT être fait que pour le mode transport, et si le paquet est protégé en intégrité. Les sommes de contrôle TCP en mode tunnel DOIVENT être vérifiées. (Ceci n'est pas une violation de l'esprit du paragraphe 4.2.2.7 de la [RFC1122] parce qu'une somme de contrôle est générée par l'envoyeur et vérifiée par le receveur. Cette somme de contrôle est la vérification de l'intégrité sur le paquet effectuée par IPsec.)

De plus, une mise en œuvre PEUT corriger tout protocole contenu qui a été cassé par le NAT (voir le cas g du paragraphe 2.1 de la [RFC3715]).

3.2 Encapsulation ESP en mode transport

```
              AVANT D'APPLIQUER ESP/UDP
            ----------------------------
      IPv4  |En-tt IP orig|     |       |
            |(tts options)| TCP |Données|
            ----------------------------

              APRES APPLICATION D'ESP/UDP
            ------------------------------------------------------
      IPv4  |en-tt IP orig|en-tt|en-tt|     |       |En-queue |Auth|
            |(tts options)| UDP | ESP | TCP |Données|  ESP    | ESP|
            ------------------------------------------------------
                                  |<----- chiffré   ----->|
                                |<------ authentifié   ------>|
```

1. La procédure ordinaire d'encapsulation ESP est utilisée.
2. Un en-tête UDP correctement formaté est inséré à l'endroit indiqué.
3. Les champs Longueur totale, Protocole, et Somme de contrôle d'en-tête (pour IPv4) dans l'en-tête IP sont édités pour correspondre au paquet IP résultant.

3.3 Désencapsulation ESP en mode Transport

1. L'en-tête UDP est retiré du paquet.
2. Les champs Longueur totale, Protocole, et Somme de contrôle d'en-tête (pour IPv4) dans le nouvel en-tête IP sont édités pour correspondre au paquet IP résultant.
3. La procédure ordinaire d'encapsulation ESP est utilisée.
4. La procédure de désencapsulation de NAT en mode Transport est utilisée.

3.4 Encapsulation ESP en mode Tunnel

```
              AVANT D'APPLIQUER ESP/UDP
            ----------------------------
      IPv4  |En-tt IP orig|     |       |
            |(tts options)| TCP |Données|
            ----------------------------

              APRES APPLICATION D'ESP/UDP
          ------------------------------------------------------------
    IPv4 |nv e-t|en-tt|en-tt|En-tt IP orig|     |       |en-queue|Auth|
         |(opts)| UDP | ESP |(tts options)| TCP |Données|  ESP   | ESP|
          ------------------------------------------------------------
                           |<------------ chiffré   ----------->|
                       |<------------- authentifié   ------------>|
```

1. La procédure ordinaire d'encapsulation ESP est utilisée.
2. Un en-tête UDP correctement formaté est inséré à l'endroit indiqué.
3. Les champs Longueur totale, Protocole, et Somme de contrôle d'en-tête (pour IPv4) dans le nouvel en-tête IP sont édités pour correspondre au paquet IP résultant.

3.5 Désencapsulation ESP en mode Tunnel

1. L'en-tête UDP est retiré du paquet.
2. Les champs Longueur totale, Protocole, et Somme de contrôle d'en-tête (pour IPv4) dans le nouvel en-tête IP sont édités pour correspondre au paquet IP résultant.
3. La procédure ordinaire de désencapsulation ESP est utilisée.
4. La procédure de désencapsulation de NAT en mode Tunnel est utilisée.

4. Procédure Garder en vie de NAT

Le seul objet de l'envoi de paquets Garder en vie de NAT est de conserver les transpositions de NAT actives pour la durée d'une connexion entre les homologues (voir le cas j du paragraphe 2.2 de la [RFC3715]). La réception de paquets Garder en vie de NAT NE DOIT PAS être utilisée pour détecter si une connexion est active.

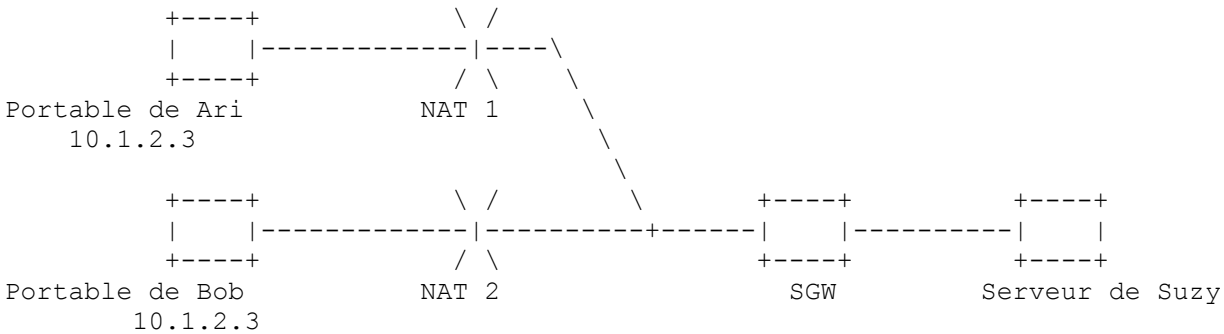
Un homologue PEUT envoyer un paquet Garder en vie de NAT si une ou plusieurs SA de phase I ou de phase II existent entre les homologues, ou si une telle SA a existé au plus N minutes plus tôt. N est un paramètre configurable en local avec une valeur par défaut de 5 minutes.

Un homologue DEVRAIT envoyer un paquet Garder en vie de NAT si son besoin est détecté conformément à la [RFC3947] et si aucun autre paquet destiné à l'homologue n'a été envoyé dans les M secondes. M est un paramètre configurable en local avec une valeur par défaut de 20 secondes.

5. Considérations pour la sécurité

5.1 Conflit de mode Tunnel

Les mises en œuvre sont averties qu'il est possible que l'homologue distant négocie des entrés qui se chevauchent avec une passerelle de sécurité (SGW, *security gateway*) problème qui affecte le mode tunnel (voir le cas e du paragraphe 2.1 de la [RFC3715]).



Comme la passerelle de sécurité va maintenant voir deux SA possibles pour aller à 10.1.2.3, cela peut créer une confusion sur la façon d'envoyer les paquets qui viennent du serveur de Suzy. Les mises en œuvre DOIVENT imaginer les moyens d'empêcher cela d'arriver.

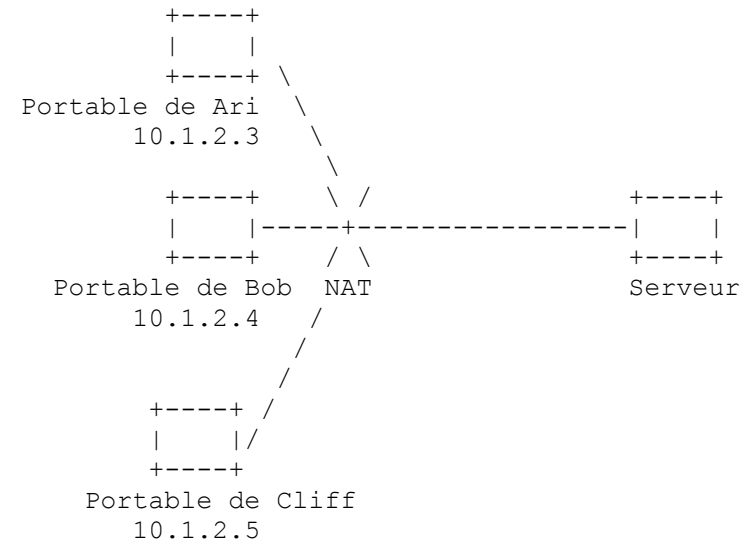
Il est RECOMMANDÉ que les SGW allouent localement des adresses IP uniques à l'ordinateur portable de Ari et de Bob (en utilisant un protocole tel que DHCP sur IPsec) ou d'utiliser le NAT pour changer les adresses IP de source des ordinateurs portables de Ari et de Bob en des adresses localement uniques avant d'envoyer les paquets transmis au serveur de Suzy. Cela couvre le critère "Adaptabilité" de la section 3 de la [RFC3715].

Prière de se reporter à l'Appendice A.

5.2 Conflit de mode Transport

Un autre problème similaire peut survenir en mode transport avec deux clients, Ari et Bob, derrière le même NAT parlant en toute sécurité au même serveur (voir le cas e du paragraphe 2.1 de la [RFC3715]).

Cliff veut parler en clair au même serveur.



Maintenant les SA de transport sur le serveur vont ressembler à :

Pour Ari : de serveur à NAT, <trafic desc1>, UDP encap <4500, Y>
Pour Bob : de serveur à NAT, <trafic desc2>, UDP encap <4500, Z>
Le trafic de Cliff est en clair, de sorte qu'il n'y a pas de SA.

<trafic desc> sont les informations de protocole et d'accès. Les accès UDP encap sont les accès utilisés dans le format ESP à encapsulation UDP du paragraphe 2.1. Y et Z sont les accès dynamiques alloués par le NAT durant la négociation IKE. Ainsi, le trafic IKE provenant de l'ordinateur portable de Ari sort sur UDP <4500,4500>. Il atteint le serveur comme UDP <Y,4500>, où Y est l'accès alloué de façon dynamique.

Si la <trafic desc1> se chevauche avec la <trafic desc2>, de simples recherches de filtre peuvent alors n'être pas suffisantes pour déterminer quelle SA doit être utilisée pour envoyer le trafic. Les mises en œuvre DOIVENT traiter cette situation, soit en interdisant les conflits de connexions, soit par d'autres moyens.

Supposons maintenant que Cliff veuille se connecter en clair au serveur. Cela va être difficile à configurer, car le serveur a déjà une politique (du serveur à l'adresse externe du NAT) pour sécuriser <trafic desc>. Pour les descriptions de trafic totalement non chevauchantes, cela est possible.

Un exemple de politique de serveur pourrait être comme suit :

Pour Ari : De serveur à NAT, tout UDP, sûr
Pour Bob : De serveur à NAT, tout TCP, sûr
Pour Cliff : De serveur à NAT, tout ICMP, texte en clair

Noter que cette politique laisse aussi Ari et Bob envoyer de l'ICMP en clair au serveur.

Le serveur voit tous les clients derrière le NAT comme la même adresse IP, de sorte qu'établir des politiques différentes pour le même descripteur de trafic est en principe impossible.

Un exemple de configuration problématique sur le serveur serait comme suit :

De serveur à NAT, TCP, sûr (pour Ari et Bob)
De serveur à NAT, TCP, en clair (pour Cliff)

Le serveur ne peut pas appliquer cette politique, car il est possible que Bob se comporte mal en envoyant du trafic en clair. Cela ne peut pas se distinguer de quand Cliff envoie du trafic en clair. De sorte qu'il est impossible de garantir la sécurité à partir de certains clients derrière un NAT, tout en permettant du texte en clair provenant de différents clients derrière le MEME NAT. Cependant, si la politique de sécurité du serveur permet cela, il peut offrir une sécurité au mieux: Si le client de derrière le NAT initie la sécurité, sa connexion sera sécurisée. Si il envoie en clair, le serveur va quand même accepter ce texte en clair.

Pour une sécurité garantie, le scénario problématique ci-dessus NE DOIT PAS être permis sur les serveurs. Pour la sécurité au mieux, ce scénario PEUT être utilisé.

Prière de voir à l'Appendice A.

6. Considérations en rapport avec l'IAB

Les questions d'UNSAF [RFC3424] sont traitées par le document sur les exigences de compatibilité IPsec-NAT [RFC3715].

7. Remerciements

Merci à Tero Kivinen et William Dixon qui ont contribué activement au présent document.

Merci à Joern Sierwald, Tamir Zegman, Tatu Ylonen, et Santeri Paavolainen, qui ont contribué aux précédents documents sur la traversée de NAT.

8. Références

8.1 Références normatives

[RFC0768] J. Postel, "Protocole de datagramme d'utilisateur (UDP)", (STD 6), 28 août 1980.

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

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

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

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

[RFC3947] T. Kivinen et autres, "Négociation de traversée de NAT dans IKE", janvier 2005. *(P.S.)*

8.2 Références pour information

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

[RFC3193] B. Patel et autres, "Sécuriser L2TP avec IPsec", novembre 2001. *(P.S.)*

[RFC3424] L. Daigle, éd., IAB, "Considérations de l'IAB sur la fixation d'auto adressage unilatéral (UNSAF) à travers la traduction d'adresse réseau", novembre 2002. *(Information)*

[RFC3715] B. Aboba, W. Dixon, "Exigences de compatibilité entre IPsec et la traduction d'adresse réseau (NAT)", mars 2004. *(Info.)*

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

Appendice A Précisions sur des solutions potentielles de client multiple de NAT

Le présent appendice donne des précisions sur des solutions potentielles au problème de clients multiples derrière le même NAT se connectant simultanément à la même adresse IP de destination.

Les paragraphes 5.1 et 5.2 disent qu'on DOIT éviter ce problème. Comme ce n'est pas un problème de protocole réseau, mais de mise en œuvre locale, les mécanismes n'appartiennent pas à la spécification du protocole lui-même. Ils sont énumérés dans le présent appendice.

Le choix d'une option va vraisemblablement dépendre des scénarios pour lesquels on utilise/prend en charge le NAT-T IPsec. Cette liste n'est pas conçue comme étant exhaustive, de sorte que d'autres solutions peuvent exister. On décrit d'abord les choix génériques qui résolvent le problème pour tous les protocoles de couche supérieure.

Choix génériques pour ESP en mode transport :

Tr1) Met en œuvre une NAT (traduction d'adresse réseau) incorporée par dessus la désencapsulation IPsec.

Tr2) Met en œuvre une NAPT (traduction d'accès d'adresse réseau) incorporée par dessus la désencapsulation IPsec.

Tr3) Un initiateur peut décider de ne pas demander le mode transport une fois que le NAT est détecté et peut à la place demander une SA en mode tunnel. Cela peut être un nouvel essai après que le mode transport a été refusé par le répondant, ou l'initiateur peut choisir de proposer dès le début une SA tunnel. Cela n'est pas plus difficile que de savoir si il faut proposer le mode transport ou le mode tunnel sans NAT. Si pour une raison quelconque, le répondant préfère ou exige le mode tunnel pour la traversée de NAT, il doit rejeter la proposition de SA en mode rapide au profit du mode transport.

Choix génériques pour ESP en mode tunnel :

Tn1) Même chose que pour Tr1.

Tn2) Même chose que pour Tr2.

Tn3) Cette option est possible si un initiateur peut recevoir une adresse à travers sa SA tunnel, le répondant utilisant DHCP. L'initiateur peut demander au départ une adresse interne via la méthode DHCP-IPsec, qu'il sache ou non qu'il est derrière un NAT. Il peut réinitier une négociation IKE de mode rapide pour une SA tunnel DHCP après que le répondant a échoué à donner suite à la proposition de SA en mode rapide de mode transport. Cela arrive soit quand une charge utile NAT-OA est envoyée, soit parce qu'il découvre d'après une NAT-D que l'initiateur est derrière un NAT et que sa configuration/politique locale va seulement accepter une connexion de NAT lorsqu'on lui alloue une adresse à travers DHCP-IPsec.

Il y a aussi des choix de mise en œuvre qui offrent une interopérabilité limitée. Les mises en œuvre devraient spécifier quelles applications ou protocoles devraient fonctionner si ces options sont choisies. Noter que ni Tr4 ni Tn4, tels que décrits ci-dessous, ne sont supposés fonctionner avec du trafic TCP.

Choix d'interopérabilité limités pour ESP en mode transport :

Tr4) Met en œuvre la connaissance du protocole de couche supérieure de la SA IPsec entrante et sortante de sorte qu'il n'utilise pas la source IP et l'accès de source comme identifiant de session (par exemple, un identifiant de session L2TP transposé en paire de SA IPsec qui n'utilise pas l'accès de source UDP ou l'adresse IP de source pour l'unicité de l'homologue).

Tr5) Met en œuvre l'intégration d'application avec initiation IKE de sorte qu'il peut se relier à un accès de source différent si la proposition de SA en mode rapide IKE est rejetée par le répondant ; puis il peut reproposer le nouveau sélecteur QM.

Choix d'interopérabilité limités pour ESP en mode tunnel :

Tn4) Même chose que pour Tr4.

Adresse des auteurs

Ari Huttunen
F-Secure Corporation
Tammasaarenkatu 7
HELSINKI FIN-00181
FI
mél : Ari.Huttunen@F-Secure.com

Brian Swander
Microsoft
One Microsoft Way
Redmond, WA 98052
US
mél : briansw@microsoft.com

Victor Volpe
Cisco Systems
Suite 205, 124 Grove Street
Franklin, MA 02038
US
mél : vvolpe@cisco.com

Larry DiBurro
Nortel Networks
80 Central Street
Boxborough, MA 01719
US
mél : ldiburro@nortelnetworks.com

Markus Stenberg
FI
mél : markus.stenberg@iki.fi

Déclaration complète de droits de reproduction

Propriété intellectuelle

Remerciement

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