Groupe de travail Réseau
Request for Comments : 3947
Catégorie : En cours de normalisation

Traduction Claude Brière de L'Isle

T. Kivinen, SafeNet
B. Swander, Microsoft
A. Huttunen, F-Secure Corporation
V. Volpe, Cisco Systems
janvier 2005

Négociation de traversée de NAT dans IKE

Résumé
Le présent document décrit comment détecter un ou plusieurs appareils de traduction d'adresse réseau (NAT, *Network Address Translation*) entre des hôtes IPsec, et comment négocier l'utilisation de l'encapsulation UDP de paquets IPsec à travers des boîtes de NAT dans l'échange de clés Internet (IKE, *Internet Key Exchange*).

Table des matières

1. Introduction

Le présent document est partagé en deux parties. La première décrit ce qui est nécessaire dans IKE phase 1 pour la prise en charge de la traversée de NAT. Cela inclut de détecter si l'autre extrémité prend en charge la traversée de NAT, et si il y a un ou plusieurs NAT entre les homologues.

La seconde partie décrit comment négocier l'utilisation de paquets IPsec encapsulés dans UDP dans le mode rapide de IKE. Il décrit aussi comment transmettre les adresses originales de source et de destination à l'homologue, si nécessaire. Ces adresses sont utilisées en mode transport pour mettre à jour de façon incrémentaire les sommes de contrôle TCP/IP afin qu'elles puissent correspondre après la transformation par le NAT. (Le NAT ne peut pas faire cela parce que la somme de contrôle TCP/IP est à l'intérieur du paquet IPsec encapsulé dans UDP.)

La [RFC3948] décrit les détails de l'encapsulation dans UDP, et la [RFC3715] fournit les informations et motifs de base de la traversée de NAT en général. Combiné à la [RFC3948], le présent document représente une solution

"inconditionnellement conforme" aux exigences définies par la [RFC3715].

Dans le scénario de base de ce document, l'initiateur est derrière NA(P)T, et le répondant a une adresse IP fixe statique.

Le présent document définit un protocole qui va fonctionner même si les deux extrémités sont derrière un NAT, mais le processus par lequel chacun localise d'autre extrémité sort du domaine d'application du présent document. Dans un scénario, le répondant est derrière un NAT d'hôte statique (un seul répondant par IP, car il n'y a pas moyen d'utiliser d'autre accès de destination que 500/4500). C'est-à-dire qu'il est connu par la configuration.

2. Spécification des exigences

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].

3. Phase 1

La détection de la prise en charge de la traversée de NAT et de la détection de NAT le long du chemin entre les deux homologues IKE survient dans la phase 1 de IKE [RFC2409].

Le NAT peut changer l'accès de source UDP IKE, et les receveurs DOIVENT être capables de traiter les paquets IKE dont l'accès de source est différent de 500. Le NAT n'a pas à changer l'accès de source si :
- o un seul hôte IPsec est derrière le NAT, ou
- o pour le premier hôte IPsec, le NAT peut conserver l'accès 500, et le NAT va seulement changer le numéro d'accès pour les connexions ultérieures.

Les receveurs DOIVENT répondre à l'adresse de source provenant du paquet (voir la [RFC3715], paragraphe 2.1, cas d). Cela signifie que lorsque le répondant original fait un changement de clés ou envoie des notifications à l'initiateur d'origine, il DOIT envoyer les paquets en utilisant le même ensemble d'accès et de numéros IP qu'utilisé lors de la dernière utilisation de la SA IKE.

Par exemple, lorsque l'initiateur envoie un paquet avec l'accès de source et de destination 500, le NAT peut le changer en un paquet avec l'accès de source 12312 et l'accès de destination 500. Le répondant doit être capable de traiter le paquet dont l'accès de source est 12312. Il doit répondre avec un paquet dont l'accès de source est 500 et l'accès de destination est 12312. Le NAT va alors traduire ce paquet en l'accès de source 500 et l'accès de destination 500.

3.1 Détection de la prise en charge de la traversée de NAT

La capacité de traversée de NAT de l'hôte distant est déterminée par un échange de charges utiles d'identifiant de fabricant. Dans les deux premiers messages de phase 1, la charge utile Identifiant de fabricant pour cette spécification DOIT être envoyée si elle est prise en charge (et elle DOIT être reçue par les deux côtés) pour que la sonde de traversée de NAT continue. Le contenu de la charge utile est le hachage MD5 de la [RFC3947].
Le contenu exact en hexadécimal pour la charge utile est :

4a131c81070358455c5728f20e95452f

3.2 Détection de la présence de NAT

La charge utile NAT-D non seulement détecte la présence de NAT entre les deux homologues IKE, mais aussi détecte où sont les NAT. La localisation de l'appareil de NAT est importante, car les messages Garder en vie doivent être initiés à partir de l'homologue qui est "derrière" le NAT.

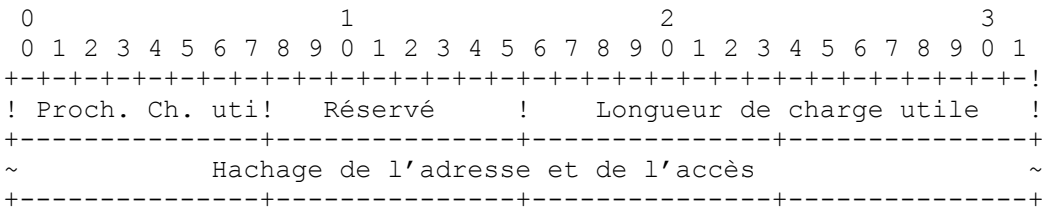
Pour détecter un NAT entre les deux hôtes, on doit détecter si l'adresse IP ou l'accès change le long du chemin. Cela se fait par l'envoi réciproque des hachages des adresses et accès IP des deux homologues IKE à partir de chaque extrémité. Si les deux extrémités calculent ces hachages et obtiennent le même résultat, elles savent qu'il n'y a pas de NAT entre elles. Si les hachages ne correspondent pas, quelqu'un a traduit l'adresse ou accès. Cela signifie qu'on doit faire une traversée de NAT pour faire passer les paquets IPsec au travers.

Si l'envoyeur du paquet ne sait pas sa propre adresse IP (dans le cas d'interfaces multiples) et si la mise en œuvre ne sait pas quelle adresse IP est utilisée pour acheminer le paquet) l'envoyeur peut inclure plusieurs hachages locaux dans le paquet (comme charges utiles NAT-D séparées). Dans ce cas, le NAT est détecté si et seulement si aucun des hachages ne correspond.

Les hachages sont envoyés comme une série de charges utiles de NAT-D (découverte de NAT). Chaque charge utile contient un hachage, de sorte qu'en cas de hachages multiples, plusieurs charges utiles NAT-D sont envoyées. Dans le cas normal, il y a seulement deux charges utiles NAT-D.

Les charges utiles NAT-D sont incluses dans les troisième et quatrième paquets de mode principal, et dans le second et le troisième paquets dans le mode agressif.

Le format du paquet NAT-D est



Le type de charge utile pour la charge utile de découverte de NAT est 20.

Le hachage HASH est calculé comme suit :

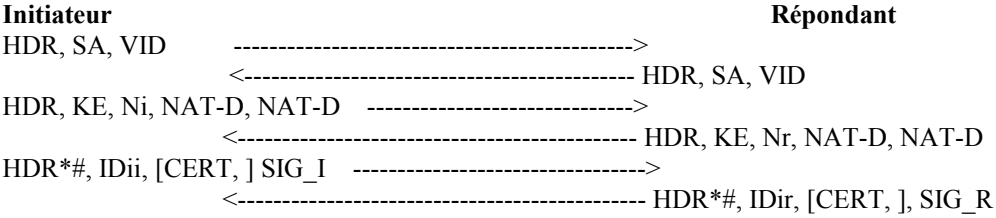
HASH = HASH(CKY-I | CKY-R | IP | Accès)

Cela utilise l'algorithme négocié HASH. Toutes les données à l'intérieur de HASH sont dans l'ordre des octets du réseau. Le IP est de 4 octets pour une adresse IPv4 et de 16 octets pour une adresse IPv6. Le numéro d'accès est codé par un nombre de deux octets dans l'ordre des octets du réseau. Le première charge utile NAT-D contient l'adresse IP et le numéro d'accès de l'extrémité distante (c'est-à-dire, l'adresse de destination du paquet UDP). Les charges utiles NAT-D restantes contiennent d'éventuelles adresses IP et numéros d'accès d'extrémité locale (c'est-à-dire, toutes les adresses de source possibles du paquet UDP).

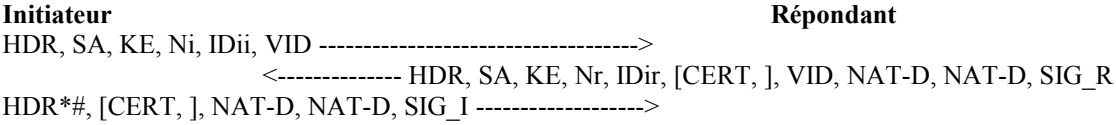
Si il n'y a pas de NAT entre les homologues, la première charge utile NAT-D reçue devrait correspondre à une des charges utiles NAT-D locales (c'est-à-dire, les charges utiles NAT-D locales que cet hôte envoie) et une des autres charges utiles NAT-D doit correspondre à l'adresse IP et au numéro d'accès de l'extrémité distante. Si la première vérification échoue (c'est-à-dire, si la première charge utile NAT-D ne correspond pas à une des adresses IP et numéros d'accès locaux) cela signifie qu'il y a un NAT dynamique entre les homologues, et que cette extrémité devrait commencer d'envoyer des messages Garder en vie comme défini dans la [RFC3948] (cette extrémité est derrière le NAT).

Le CKY-I et le CKY-R sont les mouchards initiateur et répondant. Ils sont ajoutés au hachage pour rendre impossibles les attaques de précalcul sur l'adresse et l'accès IP.

L'exemple suivant est un échange de phase 1 qui utilise la traversée de NAT en mode principal (authentification avec signatures) :



L'exemple suivant est un échange de phase 1 qui utilise la traversée de NAT en mode agressif (authentification avec signatures):



Le signe # indique que ces paquets sont envoyés à l'accès changé si le NAT est détecté.

4. Changement pour de nouveaux accès

Les NAT à capacité IPsec peuvent causer des problèmes (voir au paragraphe 2.3 de la [RFC3715]). Certains NAT ne vont pas changer l'accès de source IKE 500 même si il y a plusieurs clients derrière le NAT (voir au paragraphe 2.3 de la [RFC3715], cas n). Ils peuvent aussi utiliser des mouchards IKE pour démultiplexer le trafic au lieu d'utiliser l'accès de source (voir le paragraphe 2.3 de la [RFC3715], cas m). Tous deux sont problématiques pour la transparence de NAT générique, car il est difficile pour IKE de découvrir les capacités du NAT. La meilleure approche est simplement de sortir le trafic IKE de l'accès 500 aussitôt que possible pour éviter tout cas particulier de NAT à capacité IPsec.

Prenons le cas courant de l'initiateur derrière le NAT. L'initiateur doit changer rapidement pour l'accès 4500 dès que le NAT a été détecté pour minimiser l'opportunité de problèmes de NAT à capacité IPsec.

En mode principal, l'initiateur DOIT changer les accès lors de l'envoi de charge utile ID si il y a un NAT entre les hôtes. L'initiateur DOIT régler les deux accès UDP de source et de destination à 4500. Tous les paquets suivants envoyés à cet homologue (y compris les notifications d'informations) DOIVENT être envoyées sur l'accès 4500. De plus, les données IKE DOIVENT être précédées d'un marqueur non ESP permettant le démultiplexage du trafic, comme défini dans la [RFC3948].

Donc, le paquet IKE ressemble maintenant à :

IP UDP(4500,4500) <marqueur non ESP> HDR*, IDii, [CERT,] SIG_I

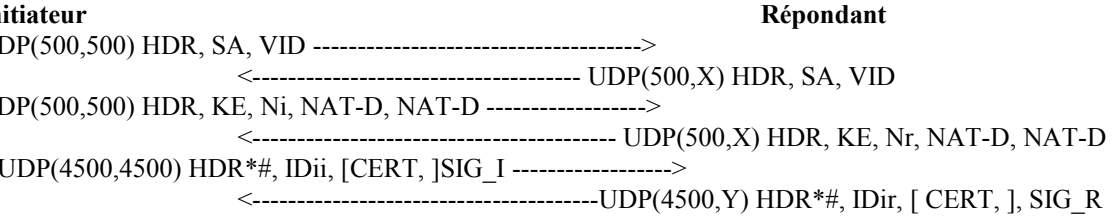
Cela suppose une authentification utilisant des signatures. Les quatre octets de marqueur non ESP sont définis dans la [RFC3948].

Lorsque le répondant obtient ce paquet, le déchiffrement et traitement usuels des diverses charge utiles sont effectués. Si ceux-ci réussissent, le répondant DOIT mettre à jour l'état local de façon que tous les paquets suivants (y compris les notifications d'information) à l'homologue utilisent le nouvel accès, et éventuellement la nouvelle adresse IP obtenue du paquet valide entrant. L'accès sera généralement différent, car le NAT va transposer UDP(500,500) en UDP(X,500) et UDP(4500,4500) en UDP(Y,4500). L'adresse IP sera rarement différente de l'adresse IP avant le changement. Le répondant DOIT répondre en utilisant UDP(4500,Y) pour tous les paquets IKE suivants pour cet homologue.

De même, si le répondant doit changer les clés de la SA de phase 1, la négociation de changement de clé DOIT débuter en utilisant UDP(4500,Y). Toute mise en œuvre qui prend en charge la traversée de NAT DOIT prendre en charge les négociations qui commencent sur l'accès 4500. Si une négociation commence sur l'accès 4500, il n'est pas besoin de changer ailleurs dans l'échange.

Une fois que le changement d'accès est survenu, si un paquet est reçu sur l'accès 500, ce paquet est périmé. Si le paquet est un paquet d'information, il PEUT être traité si la politique locale le permet. Si le paquet est en mode principal ou en mode agressif (avec les mêmes mouchards que les paquets précédents) il DEVRAIT être éliminé. Si le paquet est un nouvel échange en mode principal ou agressif, il est alors traité normalement (l'autre extrémité peut avoir été réamorcée, et cela commence un nouvel échange).

Voici un exemple d'échange de phase 1 utilisant la traversée de NAT en mode principal (authentification avec signatures) avec changement d'accès :



La procédure pour le mode agressif est très similaire. Après que le NAT a été détecté, l'initiateur envoie IP UDP(4500,4500) <4 octets de marqueur non ESP> HDR*, [CERT,], NAT-D, NAT-D, et SIG_I. Le répondant fait un traitement similaire à celui de ci-dessus, et si il réussit, DOIT mettre à jour ses accès IKE internes. Le répondant DOIT répondre en utilisant UDP(4500,Y) sur tous les paquets IKE suivants à cet homologue.

```
Initiateur                                                    Répondant
UDP(500,500) HDR, SA, KE, Ni, IDii, VID ---------------------------------->
      <----------------------------- UDP(500,X) HDR, SA, KE, Nr, IDir, [CERT, ], VID, NAT-D, NAT-D, SIG_R
UDP(4500,4500) HDR*#, [CERT, ], NAT-D, NAT-D, SIG_I ---------------->
                          <------------------------------------------ UDP(4500, Y) HDR*#, ...
```

Si la prise en charge de la traversée de NAT est activée, l'accès dans la charge utile ID dans le mode principal/agressif DOIT être réglé à 0.

Le cas le plus commun pour le répondant derrière le NAT est si le NAT fait simplement une traduction d'adresse 1:1. Dans ce cas, l'initiateur change quand même les deux accès en 4500. Le répondant utilise un algorithme identique à celui de ci-dessus, bien que dans ce cas, Y soit égal à 4500, car aucune traduction d'accès ne survient.

Un cas différent de changement d'accès implique la découverte hors bande des accès à utiliser. Ces méthodes de découverte sortent du domaine d'application du présent document. Par exemple, si le répondant est derrière un NAT traducteur d'accès, et si l'initiateur a besoin de le contacter en premier, l'initiateur devra alors déterminer quel accès utiliser, normalement en contactant quelque autre serveur. Une fois que l'initiateur sait quel accès utiliser pour traverser le NAT, généralement quelque chose comme UDP(Z,4500), il commence en utilisant ces accès. Cela est similaire au cas de changement de clé du répondant ci-dessus en ce que les accès à utiliser sont déjà connus dès le début, et aucun autre changement n'a à être effectué. Aussi, le premier temporisateur de garde en vie commence après le changement pour le nouvel accès, et aucun message Garder en vie n'est envoyé à l'accès 500.

5. Mode rapide

Après la phase 1, les deux extrémités savent si il y a un NAT présent entre elles. La décision finale d'utiliser la traversée de NAT est laissée au mode rapide. L'utilisation de la traversée de NAT est négociée à l'intérieur des charges utiles SA de mode rapide. En mode rapide, les deux extrémités peuvent aussi envoyer les adresses originales des paquets IPsec (dans le cas du mode transport) de l'autre extrémité de sorte que chacune puisse corriger le champ de somme de contrôle TCP/IP après la transformation par le NAT.

5.1 Négociation de l'encapsulation de traversée de NAT

La négociation de la traversée de NAT se fait en ajoutant deux nouveaux modes d'encapsulation. Ces modes d'encapsulation sont :

UDP-Encapsulated-Tunnel	3
UDP-Encapsulated-Transport	4

Il n'est normalement pas utile de proposer à la fois le mode normal tunnel ou transport et les modes encapsulés dans UDP. L'encapsulation UDP est nécessaire pour réparer l'incapacité à traiter le trafic non UDP/TCP par les NAT (voir le cas i du paragraphe 2.2 de la [RFC3715]).

Si il y a une boîte de NAT entre les hôtes, les encapsulations normales de tunnel ou de transport ne peuvent pas fonctionner. Dans ce cas, l'encapsulation UDP DEVRAIT être utilisée.

Si il n'y a pas de boîte de NAT entre, il n'y a pas de raison de gâcher de la bande passante en ajoutant l'encapsulation UDP des paquets. Donc, l'encapsulation UDP NE DEVRAIT PAS être utilisée.

Aussi, l'initiateur NE DEVRAIT PAS inclure à la fois le mode tunnel ou transport normal et le tunnel à encapsulation UDP ou le transport à encapsulation UDP dans ses propositions.

5.2 Envoi des adresses originales de source et de destination

Pour effectuer les mises à jour incrémentaires de sommes de contrôle TCP, les deux homologues peuvent avoir besoin de savoir les adresses IP originales utilisées par leurs homologues lorsque ils ont construit le paquet (voir le cas b du paragraphe 2.1 de la [RFC3715]). Pour l'initiateur, l'adresse d'initiateur originale est définie comme étant l'adresse IP de l'initiateur. L'adresse originale du répondant est définie comme étant l'adresse IP perçue de l'homologue. Pour le

répondant, l'adresse originale de l'initiateur est définie comme étant l'adresse perçue de l'homologue. L'adresse originale du répondant est définie comme étant l'adresse IP du répondant.

Les adresses originales sont envoyées en utilisant les charges utiles NAT-OA (Adresse originale de NAT).

La charge utile NAT-OA d'initiateur est la première. La charge utile NAT-OA de répondant est la seconde.

Exemple 1 :

```
Initiateur <---------> NAT <---------> Répondant
          ^              ^            ^
        Iaddr          NatPub       Raddr
```

L'initiateur est derrière un NAT et parle au répondant qui est publiquement disponible. L'initiateur et le répondant ont les adresses IP Iaddr et Raddr. Le NAT a l'adresse IP publique NatPub.

Initiateur :
NAT-OAi = Iaddr
NAT-OAr = Raddr

Répondant :
NAT-OAi = NATPub
NAT-OAr = Raddr

Exemple 2 :

```
Initiateur <------> NAT1 <---------> NAT2 <-------> Répondant
          ^            ^            ^               ^
        Iaddr        Nat1Pub     Nat2Pub          Raddr
```

Ici, le NAT2 "publie" Nat2Pub pour le répondant et transmet tout le trafic pour cette adresse au répondant.

Initiateur :
NAT-OAi = Iaddr
NAT-OAr = Nat2Pub

Répondant :
NAT-OAi = Nat1Pub
NAT-OAr = Raddr

Dans le cas du mode transport, les deux extrémités DOIVENT envoyer à la fois les adresses originales d'initiateur et de répondant à l'autre extrémité. Pour le mode tunnel, les deux extrémités NE DEVRAIENT PAS envoyer les adresses originales à l'autre extrémité.

Les charges utiles NAT-OA sont envoyées à l'intérieur des premiers et seconds paquets du mode rapide. L'initiateur DOIT envoyer les charges utiles si il propose un mode transport encapsulé UDP, et le répondant DOIT envoyer la charge utile seulement si il a sélectionné le mode transport encapsulé UDP. Il est possible que l'initiateur envoie la charge utile NAT-OA mais propose à la fois le mode transport et le mode tunnel encapsulé UDP. Le répondant choisit alors le mode tunnel encapsulé UDP et ne renvoie pas la charge utile NAT-OA.

Le format du paquet NAT-OA est :

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
! Proch. Ch. uti!   Réservé     !    Longueur de charge utile   !
+---------------+---------------+---------------+---------------+
| ID Type       | Réservé       | Réservé                       |
+---------------+---------------+---------------+---------------+
|           Adresse IPv4 (4 octets) ou IPv6 (16 octets)         |
+---------------+---------------+---------------+---------------+
```

Le type de charge utile pour la charge utile Adresse originale de NAT est 21.

Le type ID est défini dans la [RFC2407]. Seuls les types ID_IPV4_ADDR et ID_IPV6_ADDR sont admis. Les deux champs réservé après le type ID doivent être à zéro.

L'exemple qui suit est en mode rapide en utilisant les charges utiles NAT-OA :

```
Initiateur                                                    Répondant
HDR*, HASH(1), SA, Ni, [, KE] [, IDci, IDcr ] [, NAT-OAi, NAT-OAr] -------->
        <---------------------- HDR*, HASH(2), SA, Nr, [, KE] [, IDci, IDcr ] [, NAT-OAi, NAT-OAr]
HDR*, HASH(3) ------------------------------------------------------------------>
```

6. Notifications de contact initial

La source IP et l'adresse d'accès de la notification INITIAL-CONTACT pour l'hôte derrière le NAT ne sont pas significatives (car le NAT peut les changer) de sorte que l'adresse IP et le numéro d'accès NE DOIVENT PAS être utilisés pour déterminer quelles SA IKE/IPsec retirer (voir le cas c du paragraphe 2.1 de la [RFC3715]). La charge utile ID envoyée de l'autre extrémité DEVRAIT être utilisée à la place ; c'est-à-dire, lorsque une notification INITIAL-CONTACT est reçue de l'autre extrémité, le côté qui reçoit DEVRAIT retirer toutes les SA associées à la même charge utile ID.

7. Récupération de l'expiration des transpositions de NAT

Il y a des cas où la boîte de NAT décide de retirer les transpositions qui sont toujours actives (par exemple, lorsque l'intervalle de garder en vie est trop long, ou lorsque la boîte de NAT est réinitialisée). Pour récupérer de cela, les extrémités qui ne SONT PAS derrière le NAT DEVRAIENT utiliser le dernier paquet valide IKE ou IPsec encapsulé dans UDP provenant de l'autre extrémité pour déterminer quelles adresses IP et d'accès devraient être utilisées. L'hôte derrière un NAT dynamique NE DOIT PAS faire cela, car autrement, il ouvre une possibilité d'attaque de DoS parce que l'adresse IP ou l'accès de l'autre hôte ne va pas changer (il n'est pas derrière un NAT).

Les messages Garder en vie ne peuvent pas être utilisés à cette fin, car ils ne sont pas authentifiés, mais tout paquet IKE authentifié par IKE ou paquet ESP peut être utilisé pour détecter si l'adresse IP ou l'accès a changé.

8. Considérations pour la sécurité

Chaque fois que des changements à des parties fondamentales d'un protocole de sécurité sont proposés, l'examen des implications pour la sécurité ne peut pas être évité. Donc, voici quelques observations sur les effets, et sur l'importance qu'on doit y prêter.

- Les sondes IKE révèlent la prise en charge de la traversée de NAT à toute personne qui observe le trafic. La divulgation de la prise en charge de la traversée de NAT n'introduit pas de nouvelles vulnérabilités.

- La valeur des mécanismes d'authentification fondés sur les adresses IP disparaît une fois que les NAT entrent en scène. Cela n'est pas nécessairement une mauvaise chose (pour une sécurité réelle, des mesures d'authentification autres que les adresses IP devraient être utilisées). Cela signifie que l'authentification avec des clés prépartagées ne peut pas être utilisée en mode principal sans utiliser des clés partagées par le groupe pour tous ceux qui sont derrière la boîte de NAT. Utiliser des clés partagées par un groupe est un risque énorme parce que cela permet à tous les membres du groupe de s'authentifier auprès de toute autre partie et de prétendre être tout membre du groupe ; par exemple, un utilisateur normal pourrait se faire passer pour une passerelle vpn et agir comme personne interposée, et lire/modifier tout le trafic de/vers les autres membres du groupe. L'utilisation de clés de groupe partagées EST DÉCONSEILLÉE.

- Comme l'espace d'adresse interne est seulement de 32 bits et est habituellement très clairsemé, il serait possible à l'attaquant de trouver l'adresse interne utilisée derrière la boîte de NAT en essayant toutes les adresses IP possibles pour trouver le hachage correspondant. Le numéro d'accès est normalement fixé à 500, et les mouchards peuvent être extraits du paquet. Cela limite le calcul du hachage à 2^32. Si une conjecture intelligente de l'espace d'adresse privé est faite, le nombre de calculs de hachages nécessaire pour découvrir l'adresse IP interne tombe à 2^24 + 2 * (2^16).

- Ni les charges utiles NAT-D ni les charges utiles Identifiant de fabricant ne sont authentifiées en mode principal ou en mode agressif. Cela signifie qu'un attaquant peut retirer ces charges utiles, les modifier, ou les ajouter. En les ajoutant ou les retirant, l'attaquant peut causer des attaques de déni de service. En modifiant les paquets NAT-D, l'attaquant peut

causer l'utilisation par les deux côtés des modes d'encapsulation UDP au lieu d'utiliser directement le mode tunnel ou transport, gaspillant ainsi de la bande passante.

- L'envoi de l'adresse de source originale dans le mode rapide révèle l'adresse IP interne derrière le NAT à l'autre extrémité. Dans ce cas, on a déjà authentifié l'autre extrémité et l'envoi de l'adresse de source originale n'est nécessaire qu'en mode transport.

- Mettre à jour les adresses et accès IP d'encapsulation UDP de SA/ESP IKE pour chaque paquet authentifié valide peut causer un déni de service si un attaquant peut écouter tout le trafic du réseau, changer l'ordre des paquets, et injecter de nouveaux paquets avant le paquet qu'il a déjà vu. En d'autres termes, l'attaquant peut prendre un paquet authentifié provenant de l'hôte derrière le NAT, changer les accès de source ou destination ou les adresses IP du paquet UDP et l'envoyer à l'autre extrémité avant que le paquet réel ne l'atteigne. L'hôte qui n'est pas derrière le NAT va mettre à jour sa transposition d'adresse et accès IP et envoyer le trafic ultérieur au mauvais hôte ou accès. Cette situation est corrigée immédiatement lorsque l'attaquant cesse de modifier les paquets, car le premier paquet réel va corriger la situation. Les mises en œuvre DEVRAIENT examiner l'événement chaque fois que la transposition est changée, car cela ne devrait pas arriver si souvent.

9. Considérations relatives à l'IANA

Le présent document contient deux nouveaux "numéros magiques" alloués dans le registre existant de l'IANA pour IPsec et il renomme l'accès existant enregistré sous le numéro 4500. Le présent document définit aussi deux nouveaux types de charge utile pour IKE.

Ci-après sont les nouveaux éléments qui ont été ajoutés dans le registre des "Identifiants d'association de sécurité Internet et de protocoles de gestion de clés (ISAKMP, *Internet Security Association and Key Management Protocol*)" en mode encapsulation :

Nom	Valeur	Référence
UDP-Encapsulated-Tunnel	3	[RFC3947]
UDP-Encapsulated-Transport	4	[RFC3947]

Changement dans le registre des accès enregistrés :

Mot clé	Décimal	Description	Référence
ipsec-nat-t	4500/tcp	IPsec NAT-Traversal	[RFC3947]
ipsec-nat-t	4500/udp	IPsec NAT-Traversal	[RFC3947]

Nouveaux numéros de charge utile IKE qui doivent être ajoutés au registre de prochain type de charge utile :

NAT-D	20	Charge utile Découverte de NAT
NAT-OA	21	Charge utile Adresse originale de NAT

10. Considérations de l'IAB

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

11. Remerciements

Merci à Markus Stenberg, Larry DiBurro, et William Dixon, qui ont contribué activemement au présent document.

Merci à Tatu Ylonen, Santeri Paavolainen, et Joern Sierwald, qui ont contribué au document qui a servi de base au présent document.

12. Références

12.1 Références normatives

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

[RFC2407] D. Piper, "Le domaine d'interprétation de sécurité IP de l'Internet pour ISAKMP", novembre 1998. *(Obsolète, voir 4306)*

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

[RFC3948] A. Huttunen et autres, "Encapsulation UDP de paquets ESP d'IPsec", janvier 2005. *(P.S.)*

12.2 Références pour information

[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.)*

Adresse des auteurs

Tero Kivinen
SafeNet, Inc.
Fredrikinkatu 47
FIN-00100 HELSINKI
Finland
mél : kivinen@safenet-inc.com

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

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

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