Équipe d'ingénierie de l'Internet (IETF)
Request for Comments: 5685
Catégorie : Sur la voie de la normalisation
ISSN: 2070-1721

V. Devarapalli, WiChorus
K. Weniger

novembre 2009
Traduction Claude Brière de L'Isle

Mécanisme de redirection pour le protocole d'échange de clé Internet, version 2 (IKEv2)

Résumé
Le protocole d'échange de clé Internet, version 2 (IKEv2, *Internet Key Exchange Protocol version 2*) est un protocole pour établir des tunnels de réseau virtuel privé (VPN, *Virtual Private Network*) à partir d'une localisation distante à une passerelle afin que le client de VPN puisse accéder à des services dans le réseau derrière la passerelle. Le présent document définit une extension à IKEv2 qui permet à une passerelle de VPN surchargée ou à une passerelle de VPN qui est en train de fermer pour sa maintenance, de rediriger le client de VPN pour se rattacher à une autre passerelle. Le mécanisme proposé peut aussi être utilisé dans IPv6 mobile pour permettre à l'agent de rattachement de rediriger le nœud mobile sur un autre agent de rattachement.

Statut de ce mémoire
Ceci est un document de l'Internet sur la voie de la normalisation.

Le présent document a été produit par l'équipe d'ingénierie de l'Internet (IETF). Il représente le consensus de la communauté de l'IETF. Il a subi une révision publique et sa publication a été approuvée par le groupe de pilotage de l'ingénierie de l'Internet (IESG). Tous les documents approuvés par l'IESG ne sont pas candidats à devenir une norme de l'Internet ; voir la Section 2 de la RFC5741.

Les informations sur le statut actuel du présent document, tout errata, et comment fournir des réactions sur lui peuvent être obtenues à http://www.rfc-editor.org/info/rfc5685

Table des matières

1. Introduction

IKEv2 [RFC4306] est utilisé pour établir des VPN fondés sur IPsec [RFC4301]. L'adresse IP de la passerelle de VPN peut être configurée sur le VPN client. Mais cela ne s'adapte pas bien quand le nombre de passerelles de VPN est grand. La découverte dynamique de passerelles de VPN en utilisant le DNS est aussi assez largement utilisée. Cependant, l'utilisation du DNS n'est pas souple quand on en vient à allouer une passerelle de VPN au VPN client sur la base de la charge des passerelles de VPN. Le VPN client essaye normalement de se connecter à l'adresse IP de la passerelle de VPN qui apparaît d'abord dans la réponse du DNS. Si l'établissement du VPN tunnel échoue, alors le VPN client essaye de se rattacher aux autres passerelles de VPN retournées dans la réponse du DNS.

Le présent document propose un mécanisme de redirection pour IKEv2 qui permet à une passerelle de VPN de rediriger le VPN client sur une autre passerelle de VPN, par exemple, fondée sur la condition de charge. La redirection peut être faite durant l'échange IKE_SA_INIT ou IKE_AUTH. La redirection initiée par la passerelle au milieu d'une session est aussi prise en charge. Le mécanisme de redirection peut aussi être utilisé en conjonction avec des adresses d'envoi à la cantonade. Dans ce cas, une adresse d'envoi à la cantonade pour la grappe de passerelles de VPN est mémorisée dans le DNS au lieu d'une liste d'adresses IP en envoi individuel des passerelles de VPN.

La redirection peut aussi arriver pour des raisons administratives ou d'optimisation de l'acheminement. Le présent document ne tente pas de fournir une liste exhaustive des raisons de la redirection d'un VPN client sur une autre passerelle de VPN.

2. 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 le BCP 14, [RFC2119].

3. Échange IKEv2 initial avec redirection

Cette section décrit l'utilisation du mécanisme de redirection durant l'échange IKE_SA_INIT. La redirection initiée par une passerelle durant une session active et l'utilisation d'une redirection durant l'échange IKE_AUTH sont expliquées dans les sections suivantes.

Le VPN client indique la prise en charge du mécanisme de redirection IKEv2 et sa volonté d'être redirigé en incluant un message de notification REDIRECT_SUPPORTED dans la demande initiale IKE_SA_INIT (voir au paragraphe 9.1). La passerelle DOIT garder trace des clients qui ont indiqué la prise en charge du mécanisme de redirection et de ceux qui ne l'ont pas fait.

Pour rediriger une session IKEv2 sur une autre passerelle de VPN, la passerelle de VPN qui a initialement reçu la demande IKE_SA_INIT choisit une autre passerelle de VPN (comment le choix est fait sort du domaine d'application du présent document) et répond avec une réponse IKE_SA_INIT contenant un message de notification REDIRECT (voir le paragraphe 9.2). La notification inclut des informations sur la passerelle de VPN choisie et les données de nom occasionnel provenant de la charge utile Ni dans la demande IKE_SA_INIT. Si la demande IKE_SA_INIT n'indiquait pas la prise en

charge du mécanisme de redirection, le répondeur NE DOIT PAS envoyer la charge utile REDIRECT au VPN client. Ceci est applicable à tous les scénarios de REDIRECT décrits dans le présent document.

Noter que quand la réponse IKE_SA_INIT inclut la notification REDIRECT, l'échange ne résulte pas en la création d'une IKE_SA et l'indice de paramètre de sécurité (SPI, *Security Parameter Index*) du répondeur va être zéro.

Initiateur **Répondeur (passerelle de VPN initiale)**

```
(IP_I:500 -> Initial_IP_R:500)
  HDR(A,0), SAi1, KEi, Ni,   -->
  N(REDIRECT_SUPPORTED)

                                        (Initial_IP_R:500 -> IP_I:500)
                                <-- HDR(A,0), N(REDIRECT, New_GW_ID, Ni_data)
```

Quand le client reçoit la réponse IKE_SA_INIT, il DOIT vérifier que les données de nom occasionnel correspondent à la valeur envoyée dans la demande IKE_SA_INIT. Si les valeurs ne correspondent pas, le client DOIT éliminer en silence la réponse (et continuer d'attendre une autre réponse). Cela empêche certaines attaques de déni de service (DoS) sur l'initiateur qui seraient causées par un attaquant injectant des réponses IKE_SA_INIT avec des charges utiles REDIRECT.

Après la vérification des données du nom occasionnel, le client initie un nouvel échange IKE_SA_INIT avec la passerelle de VPN mentionnée dans la charge utile REDIRECT, pourvu que ce soit permis par ses entrées de base de données d'autorisation d'homologue (PAD, *Peer Authorization Database*). Dans l'échange IKE_SA_INIT avec la nouvelle passerelle de VPN, le client DOIT inclure la charge utile REDIRECTED_FROM (voir le paragraphe 9.3). Le VPN client inclut l'adresse IP de la passerelle de VPN originale qui a redirigé le client dans la notification REDIRECTED_FROM. L'échange IKEv2 se poursuit alors comme si il se serait passé avec la passerelle de VPN originale.

Initiateur **Répondeur (passerelle de VPN choisie)**

```
(IP_I:500 -> IP_R:500)
  HDR(A,0), SAi1, KEi, Ni,   -->
  N(REDIRECTED_FROM, Initial_IP_R)

                                        (IP_R:500 -> IP_I:500)
                                <-- HDR(A,B), SAr1, KEr, Nr,[CERTREQ]

(IP_I:500 -> IP_R:500)
  HDR(A,B), SK {IDi, [CERT,] [CERTREQ,]
  [IDr,]AUTH, SAi2, TSi, TSr} -->

                                        (IP_R:500 -> IP_I:500)
                                <-- HDR(A,B), SK {IDr, [CERT,] AUTH, SAr2, TSi, TSr}
```

Le client PEUT être redirigé à nouveau par la nouvelle passerelle de VPN si la nouvelle passerelle de VPN ne peut pas non plus servir le client. Le client n'a pas à inclure à nouveau la charge utile REDIRECT_SUPPORTED dans l'échange IKE_SA_INIT avec la nouvelle passerelle après une redirection. La présence de la charge utile REDIRECT_FROM dans l'échange IKE_SA_INIT avec la nouvelle passerelle indique à la nouvelle passerelle que le client prend en charge le mécanisme de redirection.

Quand le client est redirigé, il DOIT utiliser les mêmes entrées de PAD et de base de données de politique de sécurité (SPD, *Security Policy Database*) que celles qu'il aurait utilisées avec la passerelle originale. Recevoir une notification de redirection NE DOIT PAS résulter en la modification d'entrées de PAD ou de SPD. En pratique, cela signifie que la nouvelle passerelle doit utiliser la même identité de répondeur (IDr) que la passerelle originale, ou que les deux devraient faire partie d'un groupe de répondeurs qui sont autorisés par la même entrée de PAD. Voir le paragraphe 4.4.3.1 de la [RFC4301] sur l'utilisation des noms du DNS pour représenter un groupe d'homologues dans une entrée de PAD.

Le présent document permet au client d'être redirigé dans plusieurs états du protocole. Dans certains d'entre eux, la passerelle est déjà authentifiée au point de redirection ; dans d'autres, elle ne l'est pas. On souligne que les règles ci-dessus concernant l'identité de la nouvelle passerelle et les entrées de PAD et de SPD s'appliquent également à tous ces scénarios.

4. Utilisation d'adresses d'envoi à la cantonade avec le mécanisme de redirection

L'utilisation d'adresses d'envoi à la cantonade va éviter d'avoir besoin de configurer l'adresse IP d'une passerelle de VPN particulière dans le DNS. À la place, l'adresse d'envoi à la cantonade qui représente le groupe de passerelles de VPN est mémorisée dans le DNS. Quand le VPN client effectue une recherche dans le DNS sur la passerelle de VPN, il reçoit

l'adresse d'envoi à la cantonade de la passerelle de VPN dans la réponse du DNS.

Si une adresse d'envoi à la cantonade est retournée dans la réponse de résolution du DNS d'un nom de domaine pleinement qualifié (FQDN, *Fully Qualified Domain Name*) le VPN client envoie la demande IKE_SA_INIT à l'adresse d'envoi à la cantonade. La charge utile REDIRECT_SUPPORTED est incluse dans la demande IKE_SA_INIT envoyée à l'adresse d'envoi à la cantonade. La demande IKE_SA_INIT est acheminée à une des passerelles de VPN qui fait partie du groupe d'envoi à la cantonade. La passerelle de VPN qui reçoit la demande IKE_SA_INIT répond avec une réponse IKE_SA_INIT à partir de l'adresse d'envoi à la cantonade.

Initiateur **Répondeur (toute passerelle de VPN)**

(IP_I:500 -> ANYCAST:500)
HDR(A,0), SAi1, KEi, Ni) -->
N(REDIRECT_SUPPORTED)

(ANYCAST:500 -> IP_I:500)
<-- HDR(A,0), N(REDIRECT, New_GW_ID, Ni_data)

Si l'adresse de destination sur la demande IKE_SA_INIT est une adresse d'envoi à la cantonade, la passerelle de VPN qui a reçu la demande IKE_SA_INIT DOIT inclure la charge utile REDIRECT pour rediriger le VPN client sur une adresse d'envoi individuel d'une des passerelles de VPN. La passerelle de VPN qui a reçu la demande IKE_SA_INIT PEUT rediriger le client sur sa propre adresse d'envoi individuel si elle n'est pas surchargée.

Le reste de l'échange IKEv2 est le même que celui décrit à la Section 3.

5. Redirection durant une session active

Le mécanisme de redirection peut aussi être utilisé par une passerelle de VPN pour rediriger le client sur une autre passerelle de VPN au milieu d'une session. Pour rediriger un client, la passerelle devrait envoyer un message INFORMATIONAL avec la charge utile Notify REDIRECT. La charge utile REDIRECT DOIT porter des informations sur la nouvelle passerelle de VPN. La passerelle NE DOIT PAS inclure de données de nom occasionnel dans la charge utile REDIRECT, car c'est une redirection initiée par la passerelle et elle est protégée par l'association de sécurité IKEv2. Quand le client reçoit ce message, il envoie une réponse (généralement vide) à la passerelle. La passerelle retransmet le message de redirection INFORMATIONAL comme décrit dans la [RFC4306], jusqu'à ce qu'il obtienne une réponse. On illustre ci-dessous l'échange de message INFORMATIONAL pour la redirection initiée par la passerelle.

Initiateur (VPN client) **Répondeur (passerelle de VPN)**

<-- HDR, SK {N(REDIRECT, New_GW_ID)}

HDR, SK {} -->

L'échange de message INFORMATIONAL décrit ci-dessus est protégé par les SA IKEv2 existanes entre le client et la passerelle

Une fois que le client a envoyé un accusé de réception à la passerelle, il DEVRAIT supprimer les associations de sécurité existantes avec la vieille passerelle en envoyant un message INFORMATIONAL avec une charge utile DELETE. La passerelle PEUT aussi décider de supprimer les associations de sécurité sans signalisation de la part du client, là encire en envoyant un message INFORMATIONAL avec une charge utile DELETE ; cependant, il devrait permettre au client un temps suffisant pour qu'il établisse les associations de sécurité exigées avec la nouvelle passerelle de sécurité. Cette durée devrait être configurable sur la passerelle.

6. Redirection durant l'échange IKE_AUTH

Si la passerelle décide de rediriger le client durant l'échange IKE_AUTH, sur la base de l'identité présentée par le client dans le message de demande IKE_AUTH, cela empêche la création d'une SA fille et envoie la charge utile REDIRECT dans la réponse IKE_AUTH. La passerelle DOIT vérifier la charge utile AUTH du client avant d'envoyer la charge utile REDIRECT, et le client DOIT vérifier la charge utile AUTH de la passerelle avant d'agir sur la charge utile REDIRECT. Comme les charges utiles AUTH ont été échangées et vérifiées avec succès, l'association de sécurité IKEv2 est valide. Quand le client reçoit la réponse IKE_AUTH avec la charge utile REDIRECT, il DEVRAIT supprimer l'association de sécurité IKEv2 avec la passerelle en envoyant un message INFORMATIONAL avec une charge utile DELETE.

```
Initiateur                                   Répondeur (passerelle de VPN )
(IP_I:500 -> IP_R:500)
  HDR(A,0), SAi1, KEi, Ni,   -->
  N(REDIRECTED_SUPPORTED)
                                                    (IP_R:500 -> IP_I:500)
                                        <-- HDR(A,B), SAr1, KEr, Nr,[CERTREQ]
(IP_I:500 -> IP_R:500)
  HDR(A,B), SK {IDi, [CERT,] [CERTREQ,]
  [IDr,]AUTH, SAi2, TSi, TSr} -->
                                                    (IP_R:500 -> IP_I:500)
                                        <-- HDR(A,B), SK {IDr, [CERT,] AUTH, N(REDIRECT, New_GW_ID)}
```

Dans le cas où l'échange IKE_AUTH implique l'authentification par le protocole d'authentification extensible (EAP, *Extensible Authentication Protocol*) (comme décrit au paragraphe 2.16 de la [RFC4306]) ou plusieurs méthodes d'authentification (comme décrit dans la [RFC4739]) la passerelle peut décider de rediriger le client sur la base de l'interaction avec le serveur d'authentification, autorisation et comptabilité (AAA, *Authentication, Authorization, and Accounting*) ou avec le serveur d'authentification externe. Dans ce cas, la passerelle DOIT envoyer la charge utile Notify REDIRECT dans la première ou la dernière réponse IKE_AUTH. Le client et la passerelle DOIVENT vérifier les charges utiles AUTH comme décrit ci-dessus.

Quand EAP est utilisé, la passerelle PEUT aussi rediriger le client sur la base de l'identité non authentifiée présentée par le client lui-même dans le premier échange IKE_AUTH. Comme EAP est utilisé comme mécanisme d'authentification, le client n'inclut pas de charge utile AUTH pour authentifier son identité, mais le serveur DOIT quand même inclure sa propre charge utile AUTH, et le client DOIT la vérifier. Noter que la SA IKEv2 n'est pas créée dans ce cas et le client n'a pas à supprimer explicitement la SA IKEv2.

Dans tous les cas ci-dessus, le client DOIT accepter la notification REDIRECT seulement dans la première réponse IKE_AUTH ou la dernière réponse IKE_AUTH. Il NE DOIT PAS accepter de notification REDIRECT dans une réponse IKE_AUTH intermédiaire.

7. Traitement des boucles de redirection

Le client pourrait finir par être redirigé plusieurs fois de suite, soit à cause d'une mauvaise configuration soit d'une attaque de DoS. Le client pourrait même finir dans une boucle avec deux passerelles ou plus qui redirigent le client sur chaque autre. Cela pourrait dénier le service au client. Pour empêcher cela, le client DEVRAIT être configuré à ne pas accepter plus qu'un certain nombre de redirections (MAX_REDIRECTS) sur une courte période (REDIRECT_LOOP_DETECT_PERIOD) pour un réglage particulier de SA IKEv2. La valeur par défaut pour la variable de configuration MAX_REDIRECTS est 5. La valeur par défaut pour la variable de configuration REDIRECT_LOOP_DETECT_PERIOD est 300 secondes. Les mises en œuvre de client peuvent permettre de configurer ces variables, selon un déploiement ou configuration de système spécifique.

8. Utilisation du mécanisme de redirection avec IPv6 mobile

IPv6 mobile [RFC3775] peut utiliser IKEv2 pour l'authentification mutuelle entre le nœud mobile et l'agent de rattachement, pour la configuration d'adresse de rattachement, et pour établir les associations de sécurité destinées à protéger les messages de signalisation IPv6 mobile [RFC5026]. L'échange IKEv2, si IKEv2 est utilisé, précède l'échange de messages de signalisation de IPv6 mobile. Donc, le mécanisme décrit dans le présent document peut aussi être utilisé par un agent de rattachement IPv6 mobile pour rediriger un nœud mobile sur un autre agent de rattachement.

Un mécanisme de commutation d'agent de rattachement est disponible pour rediriger un nœud mobile sur un autre agent de rattachement, décrit dans la [RFC5142]. Le mécanisme de commutation d'agent de rattachement peut seulement être utilisé après la création de l'antémémoire de liens chez l'agent de rattachement pour le nœud mobile. L'inconvénient de ce mécanisme est que cela crée beaucoup d'état sur l'agent de rattachement avant que le nœud mobile puisse être redirigé sur un autre agent de rattachement. Le mécanisme décrit dans le présent document peut être utilisé pour rediriger un nœud mobile avant toute création d'état relatif au lien de IPv6 mobile sur l'agent de rattachement.

Quand IKEv2 fonctionne entre un nœud mobile (MN) IPv6 mobile et un agent de rattachement (HA) la redirection de l'échange IKEv2 sur un autre HA n'est pas suffisante ; la signalisation IPv6 doit aussi être envoyée à l'adresse du nouveau HA. Le MN PEUT traiter les informations reçues dans la réponse IKE_SA_INIT d'une façon similaire à celle dont il traiterait les informations de découverte de HA reçues d'autres sources non authentifiées (et potentiellement non fiables) (comme des recherches du DNS non protégées avec DNSSEC). Cependant, si le MN a des informations authentifiées sur son agent de rattachement, il NE DOIT PAS être mis à jour sur la base de la réponse IKE_SA_INIT.

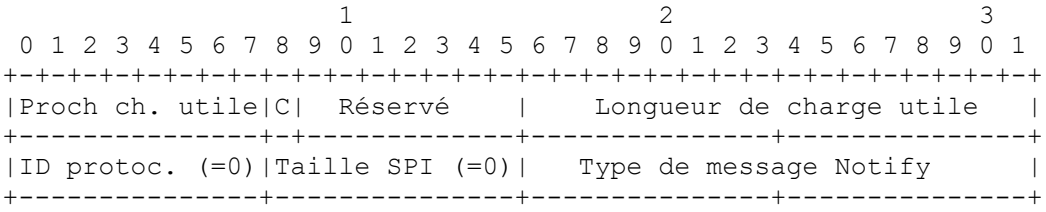
Si la notification REDIRECT est reçue durant l'échange IKE_AUTH (après l'authentification du HA ; voir la Section 6) le MN PEUT passer la nouvelle adresse à IPv6 mobile et la traiter d'une façon similaire aux informations provenant du message de commutation d'agent de rattachement [RFC5142].

Les notifications REDIRECT initiées par la passerelle échangées dans des échanges INFORMATIONAL (voir la Section 5) NE DOIVENT PAS résulter en la mise à jour de l'état IPv6 mobile. Dans ce cas, le message de commutation d'agent de rattachement spécifié dans la [RFC5142] est utilisé à la place.

9. Messages Redirect

9.1 REDIRECT_SUPPORTED

La charge utile REDIRECT_SUPPORTED est incluse dans la demande initiale IKE_SA_INIT par l'initiateur pour indiquer la prise en charge du mécanisme de redirection IKEv2 décrit dans le présent document.

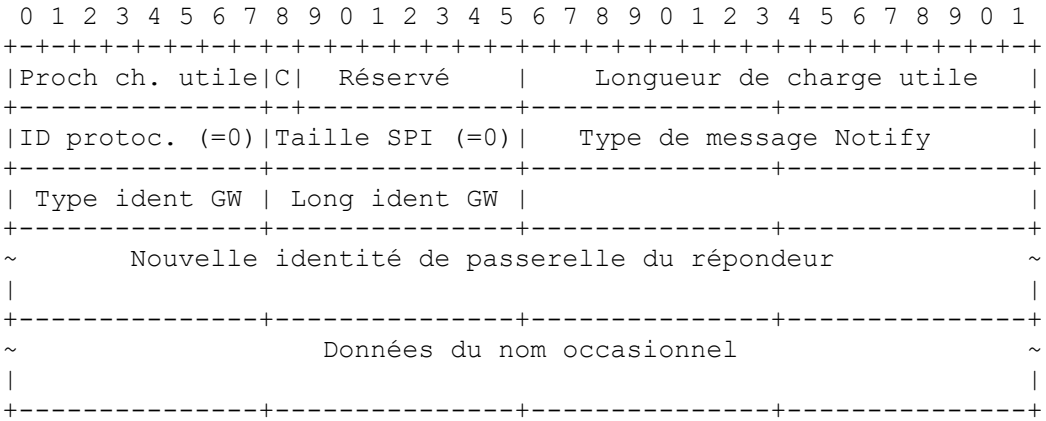


Les champs "Prochaine charge utile"', "Longueur de charge utile", "Identifiant de protocole", "Taille de SPI", et "Type de message Notify" sont les mêmes que décrits au paragraphe 3.10 de la [RFC4306]. Le champ "Taille de SPI" DOIT être réglé à 0 pour indiquer que le SPI n'est pas présent dans ce message. L'identifiant de protocole DOIT être réglé à 0, car la notification n'est pas spécifique d'une association de sécurité particulière.

Le champ "Longueur de charge utile" est réglé à la longueur en octets de la charge utile entière, incluant l'en-tête générique de charge utile. Le champ "Type de message Notify" est réglé à indiquer la charge utile REDIRECT_SUPPORTED (16406).

9.2 REDIRECT

Quand le répondeur veut rediriger l'initiateur sur une autre passerelle de VPN, la charge utile REDIRECT est incluse dans une réponse IKE_SA_INIT provenant du répondeur ou dans un message INFORMATIONAL provenant du répondeur. Le message inclut la nouvelle adresse IP ou le nouveau nom DNS du répondeur.



Les champs "Prochaine charge utile"', "Longueur de charge utile", "Identifiant de protocole", "Taille de SPI", et "Type de message Notify" sont les mêmes que décrits au paragraphe 3.10 de la [RFC4306]. Le champ "Taille de SPI" DOIT être réglé à 0 pour indiquer que le SPI n'est pas présent dans ce message. L'identifiant de protocole DOIT être réglé à 0, car la notification n'est pas spécifique d'une association de sécurité particulière.

Le champ "Longueur de charge utile" est réglé à la longueur en octets de la charge utile entière, incluant l'en-tête générique de charge utile. Le champ "Type de message Notify" est réglé à indiquer la charge utile REDIRECT (16407). Le champ "Type d'identité de GW" indique le type d'informations envoyées pour identifier la nouvelle passerelle de VPN. Les valeurs suivantes sont valides dans la charge utile REDIRECT.

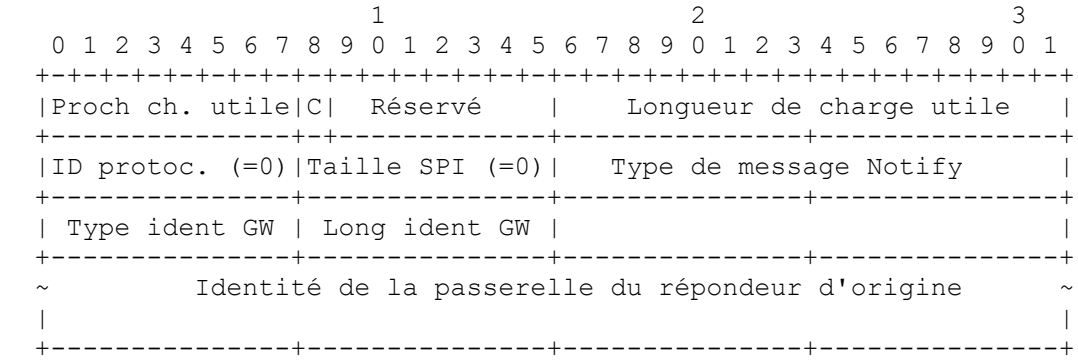
1 - adresse IPv4 de la nouvelle passerelle de VPN
2 - adresse IPv6 de la nouvelle passerelle de VPN
3 - FQDN de la nouvelle passerelle de VPN

Le champ "Longueur d'identité de passerelle" est réglé à la longueur des informations d'identité de la passerelle. L'identité de la nouvelle passerelle de VPN est portée dans le champ "Nouvelle identité de passerelle du répondeur". L'adresse IPv4, l'adresse IPv6, ou le FQDN de la nouvelle passerelle de VPN DOIVENT être codées comme décrit au paragraphe 3.5 de la [RFC4306].

Le champ "Données de nom occasionnel" porte les données de nom occasionnel provenant de la charge utile Ni envoyée par l'initiateur. La taille du nom occasionnel DOIT être entre 16 et 256 octets, comme décrit au paragraphe 3.9 de la [RFC4306]. Le champ "Données de nom occasionnel" est présent dans la charge utile REDIRECT seulement quand la charge utile REDIRECT est envoyée dans le message de réponse IKE_SA_INIT. Il NE DOIT PAS être inclus dans la charge utile REDIRECT si il est envoyé dans une réponse IKE_AUTH ou dans un message de redirection initié par la passerelle.

9.3 REDIRECTED_FROM

La charge utile Notify REDIRECTED_FROM est incluse dans la demande IKE_SA_INIT provenant de l'initiateur à la nouvelle passerelle de VPN pour indiquer l'adresse IP de la passerelle de VPN d'origine qui a redirigé l'initiateur. L'adresse IP de la passerelle de VPN originale est incluse dans le message. Si la demande IKE_SA_INIT a été envoyée à une adresse d'envoi à la cantonade (voir la Section 4) alors l'adresse d'envoi à la cantonade est incluse dans le message. Cette charge utile sert aussi à indiquer la prise en charge du mécanisme de redirection à la nouvelle passerelle de VPN après une redirection.



Les champs "Prochaine charge utile"', "Longueur de charge utile", "Identifiant de protocole", "Taille de SPI", et "Type de message Notify" sont les mêmes que décrits au paragraphe 3.10 de la [RFC4306]. Le champ "Taille de SPI" DOIT être réglé à 0 pour indiquer que le SPI n'est pas présent dans ce message. L'identifiant de protocole DOIT être réglé à 0, car la notification n'est pas spécifique d'une association de sécurité particulière.

Le champ "Longueur de charge utile" est réglé à la longueur en octets de la charge utile entière, incluant l'en-tête générique de charge utile. Le champ "Type de message Notify" est réglé à indiquer la charge utile REDIRECTED_FROM (16408). Le champ "Type d'identité de GW" indique le type d'informations envoyées pour identifier la nouvelle passerelle de VPN. Les valeurs suivantes sont valides dans la charge utile REDIRECTED_FROM :
1 - adresse IPv4 de la passerelle de VPN originale
2 - adresse IPv6 de la passerelle de VPN originale.

Le champ "Longueur de l'identité de la passerelle" est réglé à la longueur des informations d'identité de la passerelle. L'identité de la passerelle de VPN d'origine est portée dans le champ "Identité de la passerelle du répondeur d'origine".

10. Utilisation du mécanisme de redirection entre homologues IKEv2

Le mécanisme de redirection décrit dans le présent document est principalement destiné à être utilisé dans les scénarios de client à passerelle. Cependant, le mécanisme peut aussi être utilisé entre deux homologues IKEv2. Mais ce protocole est asymétrique, ce qui signifie que seulement le répondeur d'origine peut rediriger l'initiateur d'origine sur un autre serveur.

11. Considérations sur la sécurité

Un espion sur le chemin entre un client et un serveur de VPN peut envoyer une redirection au client à réception d'un message IKE_SA_INIT provenant de ce client. Ce n'est pas un problème en ce qui concerne les attaques de DoS pour la connexion de VPN, car un attaquant sur le chemin peut aussi éliminer des demandes IKE_SA_INIT pour empêcher l'accès du VPN au client. Mais un espion sur le chemin entre le client et le serveur de VPN peut rediriger un grand nombre de clients sur une victime, qui est alors inondée de demandes IKE_SA_INIT. L'inondation ne se produit que si de nombreux clients initient un échange IKEv2 presque en même temps, ce qui est considéré comme un événement rare. Cependant, cela peut arriver si un agent de rattachement / serveur de VPN est fermé pour maintenance et si tous les clients ont besoin de rétablir les connexions de VPN avec un autre agent de rattachement / serveur de VPN, ou si l'attaquant sur le chemin force toutes les associations de sécurité IPsec à expirer en éliminant tous les messages IKEv2 reçus.

L'utilisation de la charge utile REDIRECTED_FROM est destinée à décourager une passerelle de VPN félonne de rediriger un grand nombre de VPN clients sur une passerelle de VPN particulière. Cela n'empêche pas une telle attaque de DoS.

Le mécanisme de redirection NE DOIT PAS mettre à jour d'état sur le client à part les informations de passerelle de VPN. Quand il est utilisé avec IPv6 mobile, il faut faire attention à s'assurer que les informations d'agent de rattachement que le nœud mobile a configurées ne sont pas modifiées à tort par le message de redirection.

La redirection fondée sur des identités non authentifiées provenant du client peut laisser fuir des informations sur l'utilisateur quand un attaquant actif, prétendant être un VPN client, peut obtenir des informations sur la passerelle à laquelle l'utilisateur réel a été redirigé. Si la redirection est fondée sur des informations internes de l'utilisateur, cela pourrait faire échapper des informations (qui ne seraient autrement pas disponibles) sur l'utilisateur à l'attaquant. Pour empêcher ce type d'attaques, la redirection fondée sur des identifiants non authentifiés devrait être évitée et ne devrait être faite qu'après que le client s'est aussi authentifié.

12. Considérations relatives à l'IANA

Le présent document définit trois nouveaux types de message Notify IKEv2, comme décrit à la Section 9. Les trois types de message Notify ont reçu les valeurs suivantes :
16406 - REDIRECT_SUPPORTED
16407 - REDIRECT
16408 - REDIRECTED_FROM

Le présent document crée un nouvel espace de noms appelé "Type d'identité de passerelle". Il est utilisé pour indiquer le type des informations concernant la passerelle de VPN qui sont portées dans les charges utiles Notify REDIRECT (paragraphe 9.2) et REDIRECTED_FROM (paragraphe 9.3). Les valeurs suivantes ont été allouées :
1 - adresse IPv4 de la passerelle de VPN
2 - adresse IPv6 de la passerelle de VPN
3 - FQDN de la passerelle de VPN

La valeur "0" est réservée. Les valeurs 4 à 240 ne sont pas allouées. De nouvelles valeurs peuvent être allouées par revue d'expert [RFC5226]. Les valeurs de 241 à 255 sont mises de côté pour utilisation privée. Une spécification qui étend ce registre DOIT aussi mentionner quelles nouvelles valeurs sont valides dans quelle charge utile Notify.

13. Remerciements

L'utilisation des adresses d'envoi à la cantonade avec IKEv2 a d'abord été proposée par K. Weniger et F. Dupont dans le contexte d'une allocation d'agent de rattachement dans l'amorçage IPv6 mobile / mobilité de réseau (NEMO). Elle a ensuite été ajouté à une version précoce de la [RFC5026] et supprimée ultérieurement avant la publication de la RFC. Les auteurs de la RFC 5026 en sont remerciés.

Merci à Pasi Eronen, avec qui la solution décrite dans le présent document a été longuement discutée. Merci à Tero Kivinen d'avoir suggéré l'utilisation de la charge utile REDIRECTED_FROM et d'autre commentaires qui ont aidé à améliorer le document. Les auteurs tiennent aussi à remercier Yaron Sheffer, Sunil Kumar, Fan Zhao, Yoav Nir, Richard Graveman, Kanagavel Rajan, Srini Addepalli, Raj Singh, et Arnaud Ebalard de leur relecture et de leurs commentaires.

14. Références

14.1 Références normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. DOI 10.17487/RFC2119, *(MàJ par* RFC8174)

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

14.2 Références pour information

[RFC3775] D. Johnson, C. Perkins, J. Arkko, "Prise en charge de la mobilité dans IPv6", juin 2004. *(P.S.) (Obs., voir* RFC6275)

[RFC4301] S. Kent et K. Seo, "Architecture de sécurité pour le protocole Internet", DOI 10.17487/RFC4301, décembre 2005. *(P.S.) (Remplace la* RFC2401)

[RFC4739] P. Eronen, J. Korhonen, "Échanges d'authentification multiples dans le protocole d'échange de clés Internet (IKEv2)", novembre 2006. *(Expérimentale)*

[RFC5026] G. Giaretta et autres, "Amorçage IPv6 mobile dans un scénario de partage", octobre 2007. *(P.S.)*

[RFC5142] B. Haley et autres, "Message d'en-tête de mobilité pour changer d'agent de rattachement", janvier 2008. *(P.S.)*

[RFC5226] T. Narten et H. Alvestrand, "Lignes directrices pour la rédaction d'une section Considérations relatives à l'IANA dans les RFC", BCP 26, mai 2008. (*Remplace* RFC2434 *; remplacée par* RFC8126)

Adresse des auteurs

Vijay Devarapalli
WiChorus
3590 North First St
San Jose, CA 95134
USA
mél : vijay@wichorus.com

Kilian Weniger
mél : kilian.weniger@googlemail.com