Groupe de travail Réseau
Request for Comments : 3456
Catégorie : En cours de normalisation

Traduction Claude Brière de L'Isle

B. Patel, Intel Corp
B. Aboba, Microsoft
S. Kelly, Airespace
V. Gupta, Sun Microsystems, Inc.
janvier 2003

Protocole de configuration dynamique des hôtes (DHCPv4) Configuration du mode tunnel IPsec

Résumé
Le présent mémoire explore les exigences pour la configuration d'hôte en mode tunnel IPsec, et décrit comment le protocole de configuration dynamique d'hôte (DHCPv4, *Dynamic Host Configuration Protocol*) peut appuyer la configuration. Dans de nombreux scénarios d'accès à distance, un mécanisme pour faire apparaître l'hôte distant sur le réseau d'entreprise local est assez utile. Cela peut être réalisé en allouant à l'hôte une adresse "virtuelle" à partir du réseau d'entreprise, puis de tunneler le trafic via IPsec à partir de l'adresse allouée par le fournisseur d'accès de l'hôte à la passerelle de sécurité de l'entreprise. Dans IPv4, DHCP assure une telle configuration d'hôte à distance.

Table des matières

1. Introduction

Dans de nombreux scénarios d'accès à distance, un mécanisme pour faire apparaître l'hôte distant sur le réseau d'entreprise local est assez utile. Cela peut être réalisé en allouant à l'hôte une adresse "virtuelle" à partir du réseau d'entreprise, puis de tunneler le trafic via IPsec à partir de l'adresse allouée par le fournisseur d'accès de l'hôte à la passerelle de sécurité de

l'entreprise. Dans IPv4, le protocole de configuration dynamique d'hôte (DHCP, *Dynamic Host Configuration Protocol*) [RFC2131] assure une telle configuration d'hôte à distance. Le présent document explore les exigences pour la configuration d'hôte en mode tunnel IPsec, et décrit comment DHCPv4 peut appuyer la configuration.

1.1 Terminologie

Le présent document utilise les termes suivants :

client DHCP : Un client DHCP ou "client" est un hôte Internet qui utilise DHCP pour obtenir des paramètres de configuration tels qu'une adresse réseau.

Serveur DHCP : Un serveur DHCP ou "serveur" est un hôte Internet qui retourne des paramètres de configuration aux clients DHCP.

1.2 Langage des exigences

Dans ce document, les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDÉ", "NON RECOMMANDÉ", "PEUT" et "FACULTATIF" sont à interpréter comme décrit dans le BCP 14, [RFC2119].

2. Exigences de configuration d'IPsec en mode tunnel

Comme décrit dans la [RFC3457], les exigences de configuration d'un hôte avec interface IPsec en mode tunnel incluent le besoin d'obtenir une adresse IPv4 et d'autres paramètres de configuration appropriés à la classe de l'hôte. En plus de satisfaire aux exigences de base de la [RFC3457], les capacités supplémentaires suivantes peuvent être souhaitables :

a. intégration avec les facilités existantes de gestion d'adresse IPv4
b. prise en charge de la gestion de réservoir d'adresses
c. reconfiguration quand nécessaire
d. prise en charge de reprise sur défaillance
e. conservation de la sécurité et de la simplicité de mise en œuvre de IKE
f. authentification quand nécessaire

2.1 Évaluation de configuration DHCP

L'appui de DHCP pour la configuration de IPsec en mode tunnel satisfait aux exigences de base décrites dans la [RFC3457]. Il fournit aussi les capacités supplémentaires décrites ci-dessus.

Configuration de base
Dans IPv4, l'appui de DHCPv4 [RFC2131] pour la configuration de IPsec en mode tunnel satisfait aux exigences de base décrites dans la [RFC3457]. Comme les paramètres de configuration exigés décrits dans la [RFC3457] sont un sous-ensemble de ceux déjà pris en charge dans les options DHCPv4 [RFC2132], aucune nouvelle option DHCPv4 n'est exigée, et aucune modifications n'est requise à DHCPv4 [RFC2131].

Intégration de la gestion d'adresse
Comme DHCPv4 est largement déployé aujourd'hui pour la gestion d'adresse, la réutilisation de DHCPv4 pour la gestion d'adresse IPsec en mode tunnel permet la compatibilité et l'intégration avec les mises en œuvre d'adressage existantes et les logiciels de gestion d'adresse IPv4.

Gestion de réservoir d'adresses
Comme décrit dans [DHCPHB], les mises en œuvre de DHCPv4 prennent en charge le comportement conditionnel de sorte que l'adresse et les paramètres de configuration alloués peuvent dépendre des paramètres inclus dans le message DHCPDISCOVER. Cela rend possible à la passerelle de sécurité de s'assurer que l'hôte distant reçoit une allocation d'adresse IP du réservoir d'adresses approprié, comme via l'option Classe d'utilisateur, décrite dans la [RFC3004].

Reconfiguration
DHCP prend en charge le concept de prêt de configuration, et il y a une proposition de traitement de reconfiguration forcée [RFC3203].

Prise en charge de reprise sur défaillance
Avec le soutien de DHCPv4, l'état de configuration et d'adressage est conservé dans le serveur DHCP, et non au sein de la mise en œuvre IKE. Il en résulte que la perte d'un serveur tunnel n'entraîne pas la perte de l'état de configuration et d'adressage, rendant donc plus facile la prise en charge de la reprise sur défaillance [DHCPFP].

Sécurité et simplicité
Le soutien de DHCPv4 rend aussi plus facile de conserver la sécurité dans la mise en œuvre de IKE car aucune modification d'IKE n'est exigée pour la prise en charge de la configuration.

Authentification
Lorsque l'authentification DHCPv4 [RFC 3118] est requise, elle peut être prise en charge sur une interface IPsec en mode tunnel comme elle le serait sur toute autre interface.

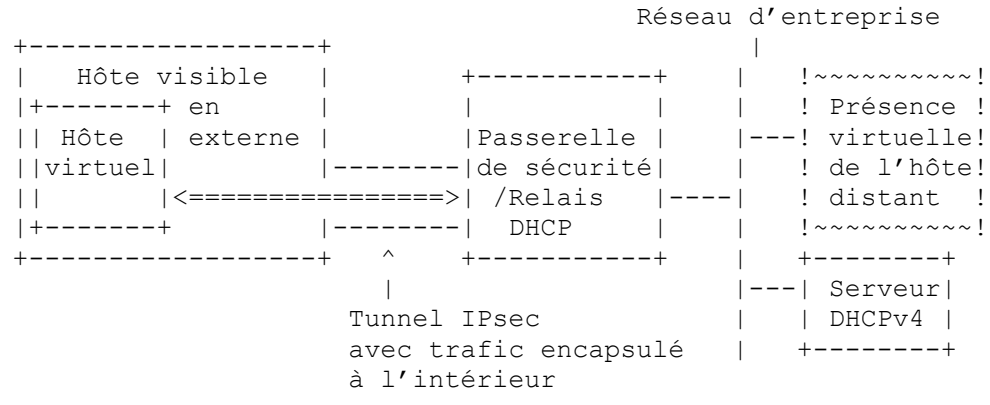
2.2 Résumé

Comme on l'a décrit, DHCPv4 [RFC2131] satisfait aux exigences de configuration de IPsec en mode tunnel [RFC3457], tout en fournissant des capacités supplémentaires. Comme décrit dans l'Appendice, IKECFG [ISAKMP] ne satisfait pas aux exigences de base, ni ne fournit les capacités supplémentaires. Il en résulte que DHCPv4 est la solution de remplacement supérieure pour la configuration de IPsec en mode tunnel.

3. Scénario d'ensemble

IPsec [RFC2401], [RFC 2402]-[RFC2409] est une suite de protocoles définie pour sécuriser la communication à la couche réseau entre les homologues communicants. Parmi les nombreuses applications à capacité IPsec, une application utile est de connecter un hôte distant à un intranet d'entreprise via une passerelle de sécurité, en utilisant IPsec en mode tunnel. Cet hôte est alors configuré de telle sorte qu'il assure une présence virtuelle sur le réseau interne. Ceci se réalise de la façon suivante :

Un hôte distant sur l'Internet va se connecter à la passerelle de sécurité puis établir un tunnel IPsec avec elle. L'hôte distant interagit alors via le tunnel IPsec avec un serveur DHCPv4 qui fournit à l'hôte distant une adresse tirée de l'espace d'adresse du réseau d'entreprise. L'hôte distant l'utilise ensuite comme adresse de source pour toutes les interactions avec les ressources de l'entreprise. Noter que cela implique que la passerelle de sécurité de l'entreprise continue de reconnaître l'adresse d'acheminement IP originale de l'hôte comme point d'extrémité du tunnel. L'identité virtuelle assumée par l'hôte distant lorsque il utilise l'adresse allouée apparaît au réseau d'entreprise comme si elle était située derrière une passerelle de sécurité portant l'adresse originale d'acheminement IP. Tout le trafic entre l'hôte distant et l'intranet sera porté sur le tunnel IPsec via la passerelle de sécurité comme le montre la figure ci-dessous :



Ce scénario suppose que l'hôte distant a déjà la connexité Internet et que l'interface Internet de l'hôte est configurée de façon appropriée. Les mécanismes pour la configuration de l'adresse de l'hôte distant pour l'interface Internet sont bien définis ; c'est-à-dire, le protocole de contrôle IP de PPP (IPCP, *PPP IP control protocol*) décrit dans la [RFC1332], DHCPv4, décrit dans la [RFC2131], et l'adressage statique. Les mécanismes pour l'autoconfiguration de l'intranet sont eux aussi normalisés. On supposera aussi que l'hôte distant a connaissance de la localisation de la passerelle de sécurité. Cela peut être réalisé via DNS, en utilisant des enregistrements A, KX [RFC2230], ou SRV [RFC2782].

Une configuration typique de l'hôte distant dans cette application utiliserait deux adresses : 1) une interface à connecter à l'Internet (interface Internet) et 2) une interface virtuelle à connecter à l'intranet (interface intranet). Les adresses IP des

interfaces Internet et intranet sont utilisées dans les en-têtes, respectivement externe et interne, du paquet IPsec en mode tunnel.

3.1 Étapes de configuration

La configuration de l'interface intranet de l'hôte IPsec en mode tunnel est réalisée selon les étapes suivantes :

a. L'hôte distant établit une association de sécurité IKE avec la passerelle de sécurité dans un échange en mode principal ou en mode agressif. Cette SA IKE sert alors à sécuriser des SA IPsec supplémentaires en mode rapide.

b. L'hôte distant établit une SA DHCP avec le serveur IPsec en mode tunnel dans un échange en mode rapide. La SA DHCP est une SA IPsec en mode établie pour protéger le trafic initial DHCPv4 entre la passerelle de sécurité et l'hôte distant. La SA DHCP DOIT être utilisée seulement pour le trafic DHCP. Les détails de l'établissement de cette SA sont décrits au paragraphe 4.1.

c. Les messages DHCP sont échangés entre l'hôte distant et le serveur DHCPv4. Le trafic est protégé entre l'hôte distant et la passerelle de sécurité en utilisant la SA DHCP établie à l'étape b. Après l'achèvement de la conversation DHCP, l'interface intranet de l'hôte distant obtient une adresse IP ainsi que les autres paramètres de configuration.

d. L'hôte distant PEUT demander la suppression de la SA DHCP car les futurs messages DHCP seront portés sur un nouveau tunnel IPsec. Autrement, l'hôte distant et la passerelle de sécurité PEUVENT continuer d'utiliser la même SA pour tout le trafic ultérieur en ajoutant des sélecteurs SPD temporaires de la même manière que celle utilisée pour les types d'identifiant de nom dans la [RFC2401].

e. Si un nouveau tunnel IPsec est requis, l'hôte distant établit une SA en mode tunnel avec la passerelle de sécurité dans un échange en mode rapide. Dans ce cas, la nouvelle adresse allouée via DHCPv4 DEVRAIT être utilisée dans l'identifiant de mode rapide.

À la fin de la dernière étape, l'hôte distant est prêt à communiquer avec l'intranet en utilisant un tunnel IPsec. Tout le trafic IP (y compris les futurs messages DHCPv4) entre l'hôte distant et l'intranet sont maintenant tunnelés sur cette SA IPsec en mode tunnel.

Comme les paramètres de sécurité utilisés pour les différentes SA se fondent sur les exigences uniques de l'hôte distant et de la passerelle de sécurité, elles ne sont pas décrites dans le présent document. Les mécanismes décrits ici fonctionnent le mieux lorsque le VPN est mis en œuvre en utilisant une interface virtuelle.

4. Description détaillée

Cette section donne des détails sur les messages échangés durant l'établissement et la suppression des SA DHCP.

4.1 Traitement du message DHCPDISCOVER

Les événements commencent avec la génération d'un message DHCPDISCOVER par l'interface intranet de l'hôte distant. Les détails sont décrits ci-dessous :

Champ	Octets	Description
op	1	op code / type de message. 1 = BOOTREQUEST, 2 = BOOTREPLY
htype	1	Type d'adresse de matériel. Réglé à la valeur 31, signifie une interface virtuelle IPsec en mode tunnel.
hlen	1	Longueur d'adresse de matériel
hops	1	Le client le règle à zéro, utilisé facultativement par les agents de relais lors de l'amorçage via un agent de relais.
xid	4	Identifiant de transaction, nombre aléatoire choisi par le client, utilisé par le client et le serveur pour associer messages et réponses entre un client et un serveur.
secs	2	Rempli par le client, secondes écoulées depuis que le client a commencé le processus d'acquisition ou de renouvellement d'adresse.
flags	2	Fanions. Le bit Diffusion DOIT être réglé à zéro.
ciaddr	4	Adresse IP du client ; seulement rempli si le client est dans l'état BOUND, RENEW ou REBINDING.
yiaddr	4	'votre' (client) adresse IP.

siaddr	4	Adresse IP du prochain serveur à utiliser à l'amorçage ; retourné dans DHCPOFFER, DHCPACK par le serveur.
giaddr	4	Adresse IPv4 d'interface de passerelle de sécurité, utilisée à l'amorçage via un agent de relais.
chaddr	16	Adresse du matériel client. Devrait être univoque.
sname	64	Nom facultatif d'hôte serveur, chaîne terminée par zéro.
file	128	Nom de fichier d'amorçage, chaîne terminée par un zéro ; nom "générique" ou nul dans DHCPDISCOVER, nom pleinement qualifié de chemin de répertoire dans DHCPOFFER.
options	variable	Champ de paramètres facultatif.

Tableau 1 : Description des champs dans le message DHCP

La valeur de htype est réglée à 31, ce qui signifie une interface virtuelle IPsec en mode tunnel, afin de permettre au serveur DHCP de différencier les demandes de VPN des demandes non VPN. Le champ chaddr du DHCPDISCOVER DOIT inclure un identifiant unique du sous-réseau virtuel. Le client DOIT utiliser le même champ chaddr dans tous les messages suivants au sein du même échange DHCPv4. De plus, le chaddr DEVRAIT être persistant entre les réamorçages afin que le serveur DHCP soit capable de réallouer la même adresse, si désiré.

Les champs hlen et chaddr DEVRAIENT être déterminés comme suit :

a. Si une ou plusieurs interfaces de LAN sont disponibles, les champs hlen et chaddr DEVRAIENT être déterminés à partir de l'interface de LAN active qui a le plus faible numéro d'interface. Si aucune interface de LAN active n'est disponible, alors les paramètres DEVRAIENT être déterminés à partir de l'interface de LAN qui a le plus faible numéro d'interface. Cela permet au chaddr d'être persistant entre les réamorçages, tant que le matériel d'interface de LAN n'est pas retiré.

b. Si il n'y a pas d'interface de LAN, le champ chaddr DEVRAIT être déterminé par l'enchaînement de x'4000', de l'adresse IPv4 de l'interface qui fournit la connexité réseau, et d'un octet supplémentaire. La valeur x'4000' indique une adresse MAC en envoi individuel administrée en local, garantissant ainsi que la valeur de chaddr construite ne va pas entrer en conflit avec une valeur allouée mondialement.

L'octet supplémentaire (qui PEUT représenter un numéro d'interface) DEVRAIT être persistant entre les réamorçages, afin que la valeur de chaddr soit persistante à travers les réamorçages si l'adresse IPv4 allouée reste constante.

Si les prescriptions ci-dessus sont suivies, alors le chaddr sera toujours unique sur le sous-réseau virtuel pourvu que l'hôte distant construise un seul tunnel avec la passerelle de sécurité. Lorsque une interface de LAN est disponible, le chaddr sera unique au monde. Lorsque une interface non LAN est disponible et qu'une adresse Internet unique est allouée à l'hôte distant, le chaddr sera aussi unique au monde. Lorsque une adresse IP privée [RFC1918] est allouée à une interface non LAN, elle ne sera pas unique au monde. Cependant, dans ce cas, les paquets ne seront pas acheminés en va et vient entre l'hôte distant et la passerelle de sécurité sauf si le réseau externe et le réseau d'entreprise ont un plan d'adressage cohérent. Dans ce cas, l'adresse IP privée allouée à l'hôte distant sera unique sur le sous-réseau virtuel.

Pour l'utilisation de configuration DHCPv4 de IPsec en mode tunnel, l'option Identifiant de client DOIT être incluse, DOIT être unique au sein du sous-réseau virtuel et DEVRAIT être persistante à travers les réamorçages. Les possibilités incluent :

a. La combinaison htype/chaddr. Si elle est allouée comme décrit ci-dessus, elle sera unique sur le sous-réseau virtuel. Elle sera persistante à travers les réamorçages pour une interface de LAN. Si une interface non LAN est utilisée, elle peut n'être pas persistante à travers les réamorçages si l'adresse IP allouée change.
b. Le FQDN de machine enchaîné avec un numéro d'interface. En supposant que le FQDN de machine n'est pas en conflit avec celui d'une autre machine, cela sera unique sur le sous-réseau virtuel ainsi que persistant à travers les réamorçages.
c. Le NAI d'usager enchaîné avec un numéro d'interface. En supposant que l'usager est connecté au VPN en seulement une localisation, cela sera unique sur le sous-réseau ainsi que persistant à travers les réamorçages.

Afin de livrer le paquet DHCPDISCOVER de l'interface intranet à la passerelle de sécurité, une SA IKE phase 1 est établie entre l'interface Internet et la passerelle de sécurité. Une SA phase 2 (mode rapide) DHCP en mode tunnel est alors établie. La durée de vie de clé pour la SA DHCP DEVRAIT être de l'ordre de quelques minutes car elle sera seulement temporaire. L'hôte distant DEVRAIT utiliser une charge utile IDci de 0.0.0.0/accès UDP 68 dans l'échange en mode rapide. La passerelle de sécurité va utiliser une charge utile IDcr de sa propre adresse Internet/accès UDP 67. La SA DHCP est établie comme SA en mode tunnel avec les filtres réglés comme suit :

- d'hôte distant à passerelle de sécurité : de tous à tous, destination : accès UDP 67
- de passerelle de sécurité à hôte distant : de tous à tous, destination : accès UDP 68

Noter que ces filtres vont fonctionner non seulement pour un client sans configuration, mais aussi avec un client qui a obtenu précédemment un prêt de configuration, et tente de la renouveler. Dans ce dernier cas, la SA DHCP va être

initialement utilisée pour envoyer un message DHCPREQUEST plutôt que DHCPDISCOVER. Le message DHCPv4 initial (DHCPDISCOVER ou DHCPREQUEST) est alors tunnelé à la passerelle de sécurité en utilisant la SA en mode tunnel. Noter que comme le paquet DHCPDISCOVER a une adresse de destination en diffusion, les mises en œuvre IPsec sur l'hôte distant et sur la passerelle de sécurité doivent tous deux être capables de traiter cela.

4.2 Comportement de relais DHCP

Bien que d'autres configurations soient possibles, normalement, le serveur DHCPv4 ne va pas résider sur la même machine que la passerelle de sécurité, qui va agir comme un relais DHCPv4, insérant son adresse dans le champ "giaddr". Dans ce cas, la passerelle de sécurité relaie les paquets entre le client et le serveur DHCPv4, mais ne demande ou ne renouvelle pas d'adresses au nom du client. Lorsque elle agit comme relais DHCP, la passerelle de sécurité PEUT mettre en œuvre l'équilibrage de charge de relais DHCP comme décrit dans la [RFC3074].

Comme les relais DHCP sont sans état, la passerelle de sécurité DEVRAIT insérer les informations appropriées dans le message DHCP avant de transmettre à un ou plusieurs serveurs DHCP. Cela permet à la passerelle de sécurité d'acheminer le ou les messages DHCPOFFER correspondants à l'hôte distant sur le tunnel IPsec correct, sans avoir à garder l'état appris du message DISCOVER, comme un tableau des xid, chaddr et tunnel.

Si la passerelle de sécurité entretient un sous-réseau séparé pour chaque tunnel IPsec, cela peut alors être réalisé en insérant l'adresse d'interface appropriée dans le champ giaddr. Autrement, la passerelle de sécurité peut utiliser l'option Informations d'agent de relais DHCP de la [RFC3046]. Dans ce cas, le numéro d'accès virtuel du tunnel est inséré dans la sous-option Identifiant de circuit d'agent (code de sous-option 1).

Pour apprendre l'adresse IP interne du client afin de lui acheminer les paquets, la passerelle de sécurité va normalement surveiller le champ yiaddr au sein de DHCPACK et sonder un chemin correspondant au titre du traitement de relais DHCP.

Lorsque il n'est pas possible d'allouer un sous-réseau séparé à chaque tunnel, et lorsque le serveur DHCP ne prend pas en charge l'option Informations d'agent de relais, le comportement d'agent de relais sans état ne sera pas possible. Dans de tels cas, les mises en œuvre PEUVENT inventer une transposition entre xid, chaddr, et tunnel afin d'acheminer la réponse du serveur DHCP au point d'extrémité de tunnel approprié. Noter que ceci est particulièrement indésirable dans les grands serveurs de VPN où l'état résultant sera substantiel.

4.3 Traitement du message DHCPREQUEST

Après que l'interface Internet a reçu le message DHCPOFFER, elle le transmet à l'interface intranet après le traitement IPsec. L'interface intranet répond alors en créant un message DHCPREQUEST qui est tunnelé à la passerelle de sécurité en utilisant la SA DHCP.

4.4 Traitement du message DHCPACK

Le serveur DHCPv4 répond alors par un message DHCPACK ou DHCPNAK qui est transmis le long de la SA DHCP par la passerelle de sécurité. L'interface Internet de l'hôte distant transmet alors le message DHCPACK ou DHCPNAK à l'interface intranet après le traitement IPsec.

Après traitement du DHCPACK, l'interface intranet est configurée et l'interface Internet peut établir une nouvelle SA IPsec en mode tunnel avec la passerelle de sécurité. L'hôte distant peut maintenant supprimer la SA DHCP en mode tunnel. Tous les futurs messages DHCP envoyés par le client, y compris DHCPREQUEST, DHCPINFORM, DHCPDECLINE, et DHCPRELEASE vont utiliser la SA VPN nouvellement établie. De même, tous les messages DHCP envoyés par le serveur DHCPv4 seront transmis par la passerelle de sécurité (agissant comme relais DHCP) en utilisant la SA IPsec en mode tunnel, y compris les messages DHCPOFFER, DHCPACK, et DHCPNAK.

Il DEVRAIT être possible de configurer l'hôte distant à transmettre tout le trafic lié à l'Internet à travers le tunnel. Bien que cela ajoute de la redondance au temps d'aller-retour entre l'hôte distant et l'Internet, cela ajoute par contre de la sécurité, en ce que la passerelle de sécurité du réseau d'entreprise peut maintenant filtrer le trafic comme si l'hôte distant était situé physiquement sur le réseau d'entreprise.

4.5 Politique de configuration

Plusieurs mécanismes peuvent être utilisés pour permettre d'allouer aux hôtes distants des configurations différentes. Par exemple, les clients peuvent utiliser l'option Classe d'usager de la [RFC3004] pour demander divers profils de configuration. Le serveur DHCPv4 peut aussi prendre en compte un certain nombre d'autres variables, y compris le htype/chaddr, l'option Nom d'hôte, l'option Identifiant de client, l'option Informations d'agent de relais DHCP de la [RFC3046], l'option Identifiant de classe de fabricant, l'option Informations spécifiques du fabricant, ou l'option Choix du sous-réseau de la [RFC3011].

La configuration conditionnelle des clients, décrite dans [DHCPHB], peut être utilisée pour résoudre un certain nombre de problèmes, y compris d'allouer des options sur la base du système d'exploitation du client, d'allouer à des groupes de clients des gammes d'adresses utilisées ensuite pour déterminer la qualité de service, d'allouer des gammes d'adresse particulières aux hôtes distants, d'allouer des chemins statiques aux clients [RFC3442], etc. Comme noté dans les considérations pour la sécurité, ces mécanismes, bien qu'utiles, n'améliorent pas la sécurité car ils peuvent être esquivés par un hôte distant qui choisit sa propre adresse IP.

5. Considérations pour la sécurité

Le présent protocole est sécurisé à l'aide de IPsec, et il en résulte que les paquets DHCP qui s'écoulent entre l'hôte distant et la passerelle de sécurité sont authentifiés et que leur intégrité est protégée.

Cependant, comme la passerelle de sécurité agit comme un relais DHCP, aucune protection n'est accordée aux paquets DHCP dans la portion du chemin entre la passerelle de sécurité et le serveur DHCP, sauf si l'authentification DHCP est utilisée.

Noter que DHCP authentifié ne peut pas être utilisé comme mécanisme de contrôle d'accès. Cela parce que un hôte distant peut toujours établir sa propre adresse IP et donc éviter toutes les mesures de sécurité fondées sur l'authentification DHCP.

Il en résulte que l'adresse allouée NE DOIT PAS dépendre de la sécurité. La passerelle de sécurité peut plutôt utiliser une autre technique, telle que les filtres d'instances de paquets ou les sélecteurs de mode rapide sur la base du tunnel.

Comme décrit dans la [RFC3046], un certain nombre de problèmes surviennent lors de la transmission de demandes de client DHCP provenant de sources qui ne sont pas de confiance. Cela inclut les attaques en épuisement de DHCP, et l'usurpation de l'option Identifiant de client ou d'adresse MAC de client. Ces questions peuvent être réglées partiellement par l'utilisation de l'option Informations de relais DHCP de la [RFC3046].

6. Considérations relatives à l'IANA

Le présent document exige qu'une valeur de htype soit allouée pour être utilisée avec IPsec en mode tunnel, comme décrit au paragraphe 4.1. Noter que DHCP s'appuie sur le registre des paramètre arp pour la définition des deux paramètres hrd dans ARP et htype dans BOOTP/DHCP. Il en résulte qu'une allocation dans le registre des paramètres arp est nécessaire, même si IPsec-DHCP ne va jamais utiliser ce paramètre pour les besoins d'ARP, car conceptuellement BOOTP/DHCP et ARP partagent le registre des paramètres arp.

Le présent document ne crée aucun nouvel espace de numéros pour l'administration de l'IANA.

7. Considérations de propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourrait être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur le répertoire en ligne des IPR de l'IETF à http://www.ietf.org/ipr.

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf- ipr@ietf.org.

8. Références

8.1 Références normatives

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

[RFC2131] R. Droms, "Protocole de configuration dynamique d'hôte", mars 1997. *(Mise à jour par* RFC3396 *et* 4361*)*

[RFC2132] S. Alexander et R. Droms, "Options DHCP et Extensions de fabricant BOOTP", mars 1997.

[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* 4306*)*

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

[RFC3118] R. Droms et W. Arbaugh, "Authentification des messages DHCP", juin 2001.

8.2 Références pour information

[DHCPFP] Droms, R., Kinnear, K., Stapp, M., Volz, B., Gonczi, S., Rabil, G., Dooley, M. et A. Kapur, "DHCP Failover Protocol", *(Non publiée)*

[DHCPHB] Droms, R., et Lemon, T., "The DHCP Handbook", Macmillan, Indianapolis, Indiana, 1999.

[ISAKMP] Dukes, D. et R. Pereira, "The ISAKMP Configuration Method", *(Non publiée)*

[RFC1332] G. McGregor, "Protocole de contrôle de protocole Internet point à point (IPCP)", mai 1992. *(MàJ 3241)*

[RFC1877] S. Cobb, "Extensions du protocole de contrôle de réseau pour la configuration d'adresses de serveurs de noms sur IP en PPP", décembre 1995. *(Information)*

[RFC1918] Y. Rekhter et autres, "Allocation d'adresse pour les internets privés", BCP 5, février 1996.

[RFC2230] R. Atkinson, "Enregistrement de délégation d'échange de clé pour le DNS", novembre 1997. *(Information)*

[RFC2782] A. Gulbrandsen, P. Vixie et L. Esibov, "RR DNS pour la spécification de la localisation des services (DNS SRV)", février 2000.

[RFC3004] G. Stump et autres, "Option classe d'utilisateur pour DHCP", novembre 2000. *(P.S.)*

[RFC3011] G. Waters, "Option de sélection de sous-réseau IPv4 pour DHCP", novembre 2000. *(P.S.)*

[RFC3046] M. Patrick, "Option DHCP Information d'agent de relais", janvier 2001. (*MàJ par* RFC6607)

[RFC3074] B. Volz et autres, "Algorithme DHC d'équilibrage de charge", février 2001. *(P.S.)*

[RFC3203] Y. T'Joens, C. Hublet, P. De Schrijver, "Extension DHCP Reconfigure", décembre 2001. (*MàJ par* RFC6704) *(P.S.)*

[RFC3442] T. Lemon, S. Cheshire, B. Volz, "Option Route statique sans classe pour le protocole de configuration dynamique d'hôte (DHCP) version 4", décembre 2002. *(P.S.)*

[RFC3457] S. Kelly, S. Ramamoorthi, "Exigences pour les scénarios d'accès distant IPsec", janvier 2003. *(Information)*

9. Remerciements

Le présent document a été enrichi par les commentaires de John Richardson et Prakash Iyer de Intel, et de Gurdeep Pall et Peter Ford de Microsoft.

Appendice – Évaluation d'IKECFG

Des solutions de remplacement à DHCPv4, telles que ISAKMP CFG, décrit dans [ISAKMP], ne satisfont pas aux exigences de base décrites dans la [RFC3457], ni ne fournissent les capacités supplémentaires de DHCPv4.

Configuration de base
Bien que ISAKMP CFG puisse fournir l'allocation d'adresse IP ainsi que la configuration de quelques paramètres supplémentaires tels que les adresses des serveurs DNS et WINS, les riches facilités de configuration de DHCPv4 ne sont pas prises en charge. L'expérience passée avec des mécanismes de configuration similaires au sein de PPP IPCP [RFC1877] nous a enseigné qu'il n'est pas viable de simplement prendre en charge la configuration minimale. Finalement, soit la plupart des fonctionnalités incorporées dans les options DHCPv4 [RFC2132] sont dupliquées, soit la prise en charge de DHCPINFORM [RFC2131] sera requise.

Intégration de la gestion d'adresse
Comme IKECFG n'est pas intégré aux facilités existantes de gestion d'adresse IP, il est difficile de l'intégrer à des services de gestion de politique qui peuvent ne pas dépendre du lien entre l'usager et l'adresse IP.

Gestion de réservoir d'adresses
IKECFG ne fournit pas de mécanisme permettant à l'hôte distant d'indiquer une préférence pour un réservoir d'adresses particulier. Cela rend difficile la prise en charge de la gestion de réservoir d'adresses.

Reconfiguration
IKECFG ne prend pas en charge le concept de prêt de configuration ou de reconfiguration.

Prise en charge de la reprise sur défaillance
Comme IKECFG crée un état distinct de réservoir d'adresses, cela complique l'approvisionnement fiable d'utilitaires réseau, à la fois dans le système de gestion d'adresses IP et dans les passerelles de sécurité elles-mêmes.

Sécurité et simplicité
Comme le démontre l'histoire avec PPP IPCP, une fois qu'il est décidé de fournir des facilités non intégrées de gestion et de configuration d'adresses au sein de IKE, il sera difficile de limiter la duplication des effort pour traiter l'allocation. Il sera plutôt tentant de dupliquer aussi les facilités de configuration, d'authentification et de reprise sur défaillance de DHCPv4. Cette duplication va considérablement augmenter la portée du travail à accomplir, compromettant finalement la sécurité de IKE.

Authentification
Alors que IKECFG peut prendre en charge l'authentification mutuelle des points d'extrémité du tunnel IPsec, il est difficile d'intégrer IKECFG avec l'authentification DHCPv4 [RFC3118]. Cela parce que la passerelle de sécurité n'aura normalement pas accès aux accréditifs de client nécessaires pour produire une option d'authentification DHCPv4 au nom du client.

Il en résulte que les passerelles de sécurité qui mettent en œuvre IKECFG demandent normalement l'allocation d'une adresse IP en leur nom propre, et l'allouent ensuite au client via IKECFG. Comme IKECFG ne prend pas en charge le concept de prêt d'adresse, la passerelle de sécurité va devoir faire le renouvellement elle-même. Cela complique le processus de renouvellement.

Comme la [RFC2131] suppose qu'une DHCPREQUEST ne va pas contenir un champ giaddr rempli lorsque il est généré

durant l'état RENEWING, le DHCPACK sera envoyé directement au client, qui ne va pas s'y attendre. Il en résulte qu'il est soit nécessaire que la passerelle de sécurité ajoute un code spécial pour éviter de transmettre de tels paquets, soit d'attendre jusqu'à l'état REBINDING. Comme la [RFC2131] ne spécifie pas que le champ giaddr peut ne pas être rempli dans l'état REBINDING, la passerelle de sécurité peut mettre sa propre adresse dans le champ giaddr lorsque elle est dans l'état REBINDING, assurant par là qu'elle peut recevoir la réponse de renouvellement sans la traiter comme un cas particulier.

Adresse des auteurs

Baiju V. Patel	Bernard Aboba	Scott Kelly
Intel Corp	Microsoft Corporation	Airespace
2511 NE 25th Ave	One Microsoft Way	110 Nortech Pkwy
Hillsboro, OR 97124	Redmond, WA 98052	San Jose CA 95134 USA
téléphone : +1 503 712 2303	téléphone : +1 425 706 6605	téléphone : +1 (408) 941-0500
mél : baiju.v.patel@intel.com	mél : bernarda@microsoft.com	mél : scott@hyperthought.com

Vipul Gupta
Sun Microsystems, Inc.
MS UMTV29-235
2600 Casey Avenue
Mountain View, CA 94303
téléphone : +1 650 336 1681
mél : vipul.gupta@sun.com

Déclaration complète de droits de reproduction

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