Groupe de travail Réseau
Request for Comments : 3715
Catégorie : Information
Traduction Claude Brière de L'Isle

B. Aboba
W. Dixon
Microsoft
mars 2004

Exigences de compatibilité entre IPsec et la traduction d'adresse réseau (NAT)

Statut de ce mémoire
Le présent mémoire apporte des informations à la communauté de l'Internet. Il ne spécifie aucune sorte de norme de l'Internet. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé
Le présent document décrit les incompatibilités connues entre traduction d'adresse réseau (NAT, *Network Address Translation*) et IPsec, et décrit les exigences de leur traitement. L'utilisation la plus courante de IPsec est peut-être de fournir des capacités de réseautage privé virtuel. Une utilisation très populaire des réseaux privés virtuels (VPN, *Vitual Private Network*) est de fournir un accès télécommutant à l'Intranet d'entreprise. Aujourd'hui, les NAT sont largement déployés dans les passerelles domestiques, ainsi que dans d'autres localisations dont l'utilisation par les télécommutants est probable, comme les hôtels. Il en résulte que les incompatibilités IPsec-NAT sont devenues une barrière majeure au déploiement d'IPsec dans une de ses principales utilisations.

Table des matières

1. Introduction

Peut-être que l'utilisation la plus commune d'IPsec [RFC2401] est de fournir des capacités de réseautage privé virtuel (VPN, *virtual private networking*). Une utilisation très populaire des VPN est de fournir un accès télécommutant à l'Intranet d'entreprise. Les traductions d'adresse réseau (NAT, *Network Address Translation*) décrites dans les [RFC2663] et [RFC3022] sont largement déployées dans les passerelles domestiques, ainsi que dans d'autres localisations qui ont une forte probabilité d'utilisation par les télécommunicants, comme les hôtels. Il en résulte que les incompatibilités IPsec-NAT sont devenues un obstacle majeur au déploiement de IPsec dans une de ses principales utilisations. Le présent document décrit les incompatibilités connues entre NAT et IPsec, et décrit les exigences de leur traitement.

1.1 Langage des exigences

Dans ce document, les mots clés "PEUT", "DOIT, "NE DOIT PAS", "facultatif", "recommandé", "DEVRAIT", et "NE DEVRAIT PAS", sont à interpréter comme décrit dans la [RFC2119].

Prière de noter que les exigences spécifiées dans ce document sont à utiliser dans l'évaluation des soumissions de protocole. À ce titre, le langage des exigences se réfère aux capacités de ces protocoles ; les documents de protocole vont spécifier si ces caractéristiques sont exigées, recommandées, ou facultatives. Par exemple, exiger qu'un protocole prenne en charge la confidentialité n'est pas la même chose que d'exiger que tout le trafic du protocole soit chiffré.

Une soumission de protocole n'est pas conforme si elle échoue à satisfaire une ou plusieurs des exigences marquées DOIT ou NE DOIT PAS pour la capacité qu'elle met en œuvre. Une soumission de protocole qui satisfait à toutes les exigences DOIT, NE DOIT PAS, DEVRAIT, et NE DEVRAIT PAS pour cette capacité est dite "inconditionnellement conforme" ; celle qui satisfait à toutes les exigences marquées DOIT et NE DOIT PAS, mais pas à toutes celles marquées DEVRAIT ou NE DEVRAIT PAS pour ses protocoles est dite "conditionnellement conforme".

2. Incompatibilités connues entre NA(P)T et IPsec

Les incompatibilités entre NA(P)T et IPsec peuvent être divisées en trois catégories :

1) Questions intrinsèques au NA(P)T . Ces incompatibilités découlent directement de la fonctionnalité de NA(P)T décrite dans la [RFC3022]. Ces incompatibilités seront donc présentes dans tout appareil de NA(P)T.
2) Faiblesses de la mise en œuvre de NA(P)T. Ces incompatibilités ne sont pas intrinsèques au NA(P)T, mais sont présentes dans de nombreuses mises en œuvre de NA(P)T. Sont inclus dans cette catégorie les problèmes du traitement des fragments entrants ou sortants. Comme ces questions ne sont pas intrinsèques au NA(P)T, elles peuvent, en principe, être réglées par de futures mises en œuvre de NA(P)T. Cependant, comme les problèmes de mise en œuvre apparaissent largement répandus, ils doivent être pris en compte dans une solution de traversée de NA(P)T.

3) Problèmes d'assistance. Ces incompatibilités sont présentes dans les appareils de NA(P)T qui tentent de fournir la traversée de NA(P)T par IPsec. Ironiquement, cette fonction "d'assistance" crée de nouvelles incompatibilités, rendant un problème déjà difficile plus dur à résoudre. Bien que la fonction "d'assistance" de la traversée IPsec ne soit pas présente dans tous les NA(P)T, ces dispositifs sont en train de devenir suffisamment répandus pour qu'il soit aussi nécessaire de les prendre en compte dans une solution de traversée de NA(P)T.

2.1 Questions intrinsèques de NA(P)T

Les incompatibilités qui sont intrinsèques au NA(P)T incluent :

a) Incompatibilité entre IPsec AH [RFC2402] et NAT. Comme l'en-tête AH incorpore les adresses de source et de destination IP dans la vérification chiffrée d'intégrité du message, les appareils de NAT ou NAT inverse qui font des changements aux champs d'adresse vont invalider la vérification d'intégrité du message. Comme IPsec ESP [RFC2406] n'incorpore pas les adresses IP de source et de destination dans sa vérification chiffrée d'intégrité de message, cette question ne se pose pas pour ESP.

b) Incompatibilité entre sommes de contrôle et NAT. Les sommes de contrôle TCP et UDP ont une dépendance à l'égard des adresses IP de source et de destination à cause de l'inclusion du "pseudo en-tête" dans le calcul. Il en résulte que lorsque une somme de contrôle est calculée et vérifiée à réception, elle sera invalidée par un passage à travers un appareil de NAT ou de NAT inverse.

   Il en résulte que l'encapsulation de charge de sécurité IPsec (ESP, *Encapsulating Security Payload*) ne va passer sans entrave à travers un NAT que si les protocoles TCP/UDP ne sont pas impliqués (comme en mode tunnel IPsec ou en GRE protégé par IPsec) ou si les sommes de contrôle ne sont pas calculées (comme c'est possible avec IPv4 UDP). Comme décrit dans la [RFC0793], le calcul de somme de contrôle TCP et sa vérification sont exigés dans IPv4. Le calcul et la vérification de la somme de contrôle UDP/TCP est exigé dans IPv6.

   Le protocole de transmission de contrôle de flux (SDTP, *Stream Control Transmission Protocol*) comme défini dans les [RFC2960] et [RFC3309], utilise un algorithme CRC32C calculé seulement sur le paquet SCTP (en-tête commun plus tronçons) de sorte que l'en-tête IP n'est pas couvert. Il en résulte que les NAT n'invalident pas le CRC SCTP, et que le problème ne se pose pas.

Noter que comme le trafic IPsec en mode transport est protégé en intégrité et authentifié à l'aide d'une cryptographie forte, les modifications au paquet peuvent être détectées avant de vérifier les sommes de contrôle UDP/TCP. Donc, la vérification de somme de contrôle ne fournit d'assurance que contre les erreurs commises dans le traitement interne.

c) L'incompatibilité entre les identifiants d'adresse IKE et le NAT. Lorsque les adresses IP sont utilisées comme identifiants dans le protocole d'échange de clé Internet (IKE, *Internet Key Exchange*) de phase 1 [RFC2409] ou de phase 2, la modification des adresses IP de source ou de destination par les NAT ou les NAT inverses aura pour résultat une discordance entre les identifiants et les adresses dans l'en-tête IP. Comme décrit dans la [RFC2409], les mises en œuvre de IKE sont obligées de détruire de tels paquets.

Afin d'éviter l'utilisation d'adresses IO comme identifiants IKE phase 1 et phase 2, des identifiants d'utilisateur et des FQDN peuvent être utilisés à la place. Lorsque l'authentification de l'utilisateur est désirée, un type d'identifiant de ID_USER_FQDN peut être utilisé, comme décrit dans la [RFC2407]. Lorsque l'authentification de la machine est désirée, un type d'identifiant de ID_FQDN peut être utilisé. Dans l'un et l'autre cas, il est nécessaire de vérifier que l'identifiant proposé a été authentifié par suite du traitement d'un certificat d'entité d'extrémité, si des certificats sont échangés dans la phase 1. Bien que l'utilisation des types d'identité USER_FQDN ou FQDN soit possible au sein de IKE, il y a des scénarios d'utilisation (par exemple, des entrées de base de données de politique de sécurité (SPD, *Security Policy Database*) qui décrivent des sous-réseaux) qui ne peuvent pas être traités de cette façon.

Comme l'adresse de source dans les identifiants de phase 2 est souvent utilisée pour former tout un quintuplet de sélecteur de SA entrante, d'adresse de destination, de protocole, d'accès de source et d'accès de destination peut être utilisé dans le sélecteur afin de ne pas affaiblir le traitement de la SA entrante.

d) Incompatibilité entre accès de source fixe IKE et NAPT. Lorsque plusieurs hôtes derrière le NAPT initient des SA IKE pour le même répondant, un mécanisme est nécessaire pour permettre au NAPT de démultiplexer les paquets IKE entrants qui proviennent du répondant. Cela est normalement accompli par la traduction de l'accès de source IKE UDP sur les paquets sortants provenant de l'initiateur. Donc, les répondants doivent être capables d'accepter du trafic IKE provenant d'un accès de source UDP autre que 500, et ils doivent répondre à cet accès. Il faut veiller à éviter un comportement imprévisible durant les changements de clé. Si l'accès de source flottant n'est pas utilisé comme accès de destination pour le changement de clé, le NAT pourrait n'être pas capable d'envoyer les paquets de changement de clé à la destination correcte.

e) Incompatibilités entre entrées de SPD en chevauchement et le NAT. Lorsque des hôtes initiateurs derrière un NAT utilisent leurs adresses IP de source dans des identifiants de phase 2, ils peuvent négocier des entrées de SPD en chevauchement avec la même adresse IP de répondant. Le répondant pourrait alors envoyer des paquets sur la mauvaise SA IPsec. Cela se produit parce que chez le répondant, les SA IPsec paraissent être équivalentes, car elles existent entre les mêmes points d'extrémité et peuvent être utilisées pour passer le même trafic.

f) Incompatibilités entre choix de SPI (*Security Parameter Index,* indice de paramètre de sécurité) IPsec et NAT. Comme le trafic IPsec ESP est chiffré et donc opaque au NAT, le NAT doit utiliser les éléments des en-têtes IP et IPsec pour démultiplexer le trafic IPsec entrant. La combinaison de l'adresse de destination IP, du protocole de sécurité (AH/ESP) et du SPI IPsec est normalement utilisée à cette fin.

Cependant, comme les SPI entrants et sortants sont choisis indépendamment, le NAT n'a pas de moyen pour déterminer quel SPI entrant correspond à quel hôte de destination simplement en inspectant le trafic sortant. Donc, lorsque deux hôtes derrière le NAT tentent de créer des SA IPsec simultanément pour la même destination, il est possible que le NAT livre les paquets IPsec entrants à la mauvaise destination.

Noter que ceci n'est pas une incompatibilité avec IPsec en soi, mais plutôt avec la façon dont il est normalement mis en œuvre. Aussi bien avec AH qu'avec ESP, l'hôte receveur spécifie le SPI à utiliser pour une certaine SA, choix qui n'a de signification que pour le receveur. À présent, la combinaison de la destination IP, du SPI, et du protocole de sécurité (AH, ESP) identifie de façon univoque l'association de sécurité. Aussi, les valeurs de SPI dans la gamme de 1 à 255 sont réservées à l'IANA et pourraient être utilisées à l'avenir. Cela signifie que lors de la négociation avec le même hôte ou passerelle externe, l'hôte interne derrière le même NAPT peut choisir la même valeur de SPI, de sorte qu'une SA entrante d'hôte ait (SPI = 470, Destination IP interne = 192.168.0.4) et qu'une SA entrante d'un hôte différent ait (SPI = 470, Destination IP interne = 192.168.0.5). Le NAPT receveur ne sera pas capable de déterminer à quel hôte interne un paquet IPsec entrant avec le SPI = 470 devrait être transmis.

Il est aussi possible que l'hôte receveur alloue un SPI unique à chaque association de sécurité en envoi individuel. Dans ce cas, l'adresse IP de destination a seulement besoin d'être vérifiée pour voir si elle est "toute adresse IP d'envoi individuel valide pour cet hôte", et non vérifiée pour voir si elle est l'adresse IP de destination spécifique utilisée par l'hôte envoyeur. En utilisant cette technique, le NA(P)T peut être assuré d'une chance faible, mais supérieure à zéro, de transmettre les paquets au mauvais hôte interne, même lorsque deux hôtes ou plus établissent des SA avec le même hôte externe.

Cette approche est complètement rétro-compatible, et exige seulement que l'hôte receveur particulier change son allocation de SPI et de code IPsec_esp_input(). Cependant, les appareils NA(P)T peuvent n'être pas capables de détecter ce comportement sans subir les problèmes associés à l'analyse des charges utiles IKE. Et un hôte peut encore être obligé d'utiliser un SPI dans la gamme réservée de l'IANA pour les besoins d'allocation.

g) Incompatibilités entre les adresses IP incorporées et le NAT. Comme la charge utile est protégée en intégrité, toute les adresses IP incluses au sein des paquets IPsec ne seront pas traduisibles par un NAT. Cela rend inefficaces les passerelles de couche application (ALG, *Application Layer Gateway*) mises en œuvre au sein des NAT. Les protocoles qui utilisent des adresses IP incorporées incluent FTP, IRC, SNMP, LDAP, H.323, SIP, SCTP (facultativement) et de nombreux jeux. Pour traiter ce problème, il est nécessaire d'installer les ALG sur l'hôte ou des passerelles de sécurité qui puissent fonctionner sur le trafic d'application avant l'encapsulation IPsec et après la désencapsulation IPsec.

h) La directionnalité implicite du NA(P)T. Les NA(P)T exigent souvent qu'un paquet sortant initial s'écoule à travers eux afin de créer un état de transposition entrant. La directionnalité interdit l'établissement non sollicité de SA IPsec dans les hôtes derrière le NA(P)T.

i) Vérification de sélecteur de SA entrante. En supposant que IKE négocie les sélecteurs de phase 2, le traitement de SA entrante va éliminer le paquet désencapsulé, car la [RFC2401] exige que l'adresse de source d'un paquet corresponde à la valeur du sélecteur de la SA, que le traitement par le NA(P)T d'un paquet ESP va changer.

2.2 Faiblesses de mise en œuvre des NA(P)T

Les problèmes de mise en œuvre présents dans de nombreux NA(P)T incluent :

j) L'incapacité à traiter le trafic non UDP/TCP. Certains NA(P)T éliminent le trafic non UDP/TCP ou effectuent une traduction de la seule adresse lorsque il y a un seul hôte derrière le NAT. De tels NAPT sont incapables de permettre le trafic SCTP, ESP (protocole 50), ou AH (protocole 51).

k) Temporisation de transposition de NAT. Les NA(P)T connaissent des variations quant au délai pendant lequel une transposition UDP sera conservée en l'absence de trafic. Donc, même lorsque les paquets IKE peuvent être correctement traduits, l'état de traduction peut être retiré de façon prématurée.

l) Incapacité à traiter les fragments sortants. La plupart des NA(P)T peuvent correctement fragmenter les paquets IP sortants dans le cas où la taille du paquet IP excède la MTU sur l'interface sortante. Cependant, une traduction correcte des paquets sortants qui sont déjà fragmentés est difficile et la plupart des NAPT ne traitent pas cela correctement. Comme noté au paragraphe 6.3 de la [RFC3022], lorsque deux hôtes génèrent des paquets fragmentés pour la même destination, les identifiants de fragment peuvent se chevaucher. Comme l'hôte de destination s'appuie sur l'identifiant de fragmentation et le décalage de fragment pour le réassemblage, le résultat sera la corruption des données. Peu de NA(P)T protègent contre les collisions d'identifiants en prenant en charge la traduction d'identifiant. Les collisions d'identifiant ne posent pas de problèmes lorsque les NAT effectuent la fragmentation, car l'identifiant de fragment a seulement besoin d'être unique au sein d'une paire d'adresses IP source/destination.

   Comme un fragment peut être de seulement 68 octets [RFC0791], il n'est pas garanti que le premier fragment contienne un en-tête TCP complet. Donc, un NA(P)T qui cherche à recalculer la somme de contrôle TCP peut avoir besoin de modifier un fragment suivant. Comme les fragments peuvent être réordonnés, et que les adresses IP peuvent être incorporées et éventuellement partagées entre des fragments, le NA(P)T aura besoin d'effectuer le réassemblage avant d'achever la traduction. Peu de NA(P)T prennent cela en charge.

m) Incapacité à traiter les fragments entrants. Comme seul le premier fragment va normalement contenir un en-tête IP/UDP/SCTP/TCP complet, les NAPT doivent être capables d'effectuer la traduction sur la base des seules adresses IP de source/destination et de l'identifiant de fragment. Comme les fragments peuvent être réordonnés, les en-têtes pour un certain identifiant de fragment peuvent n'être pas connus si un fragment suivant arrive avant le fragment initial, et les en-têtes peuvent être partagés entre les fragments. Il en résulte que le NAPT peut avoir besoin d'effectuer le réassemblage avant de terminer la traduction. Peu de NAPT prennent cela en charge. Noter qu'avec un NAT, l'adresse IP de source/destination suffit pour déterminer la traduction, de sorte que ceci n'apparaît pas. Cependant, il est possible que l'en-tête IPsec ou IKE soit partagé entre les fragments, de sorte que le réassemblage peut être quand même requis.

2.3 Incompatibilités d'assistance

Les incompatibilités entre IPsec et la fonction "d'assistance" de NAT incluent :

n) Inspection d'en-tête du protocole Internet d'association de sécurité et de gestion de clé (ISAKMP, *Internet Security Association and Key Management Protocol*). Aujourd'hui certaines mises en œuvre de NAT tentent d'utiliser des mouchards *(cookies)* IKE pour démultiplexer le trafic IKE entrant. Comme avec le démultiplexage d'accès de source, le démultiplexage de mouchard IKE résulte en problèmes avec le changement de clé, car les changements de clé de phase 1 ne vont normalement pas utiliser les mêmes mouchards que le trafic antérieur.

o) Traitement particulier de l'accès 500. Comme certaines mises en œuvre IKE sont incapables de traiter les accès de source UDP non 500, certains NAT ne traduisent pas les paquets qui ont l'accès de source UDP de 500. Cela signifie que ces NAT sont limités à un client IPsec par passerelle de destination, sauf si ils inspectent les détails de l'en-tête ISAKMP pour examiner les mouchards qui créent le problème noté ci-dessus.

p) Inspection de la charge utile ISAKMP. Les mises en œuvre de NA(P)T qui tentent d'analyser les charges utiles ISAKMP peuvent ne pas traiter toutes les combinaisons de rangement de charge utile, ou ne pas prendre en charge les charges utiles de vendor_id pour la négociation d'option IKE.

3. Exigences pour la compatibilité IPsec-NAT

Le but d'une solution de compatibilité IPsec-NAT est d'étendre la gamme des fonctionnalités IPsec utilisables au delà de la solution disponible dans le mode tunnel IPsec compatible NAT décrite au paragraphe 2.3.

En évaluant une solution pour l'incompatibilité IPsec-NAT, les critères suivants devraient être pris en compte :

Déploiement

Comme IPv6 va régler le problème de la rareté des adresses qui conduit fréquemment à utiliser des NA(P)T avec IPv4, la question de la compatibilité IPsec-NAT est un problème transitoire qui sera résolu dans le cours du temps avant qu'IPv6 connaisse un large déploiement. Donc, pour être utile, une solution à la compatibilité IPsec-NAT DOIT pouvoir être déployée sur une échelle de temps plus courte que IPv6.

Comme le déploiement d'IPv6 exige des changements aux routeurs tout autant qu'aux hôtes, une solution potentielle à la compatibilité IPsec-NAT, qui requiert des changements aussi bien dans les routeurs que dans les hôtes, sera déployable à peu près en même temps que IPv6. Donc, une solution à la compatibilité IPsec-NAT DEVRAIT n'exiger de changements que chez les hôtes, et pas chez les routeurs.

Entre autres choses, cela implique que la communication entre l'hôte et le NA(P)T NE DEVRAIT PAS être exigée par une solution à la compatibilité IPsec-NAT, car cela exigerait des changements aux NA(P)T, et aux essais d'interopérabilité entre l'hôte et les mises en œuvre de NA(P)T. Pour permettre la déploiement à court terme, il est nécessaire que la solution fonctionne avec le routeur existant et les produits de NA(P)T au sein de l'infrastructure déployée.

Compatibilité de protocole

Une solution IPsec de traversée de NAT n'est pas supposée résoudre les problèmes avec les protocoles qui ne peuvent pas traverser un NA(P)T lorsque il n'est pas sécurisé avec IPsec. Donc, des ALG peuvent être encore nécessaires pour certains protocoles, même lorsque est disponible une solution IPsec de traversée de NAT.

Sécurité

Comme la directionnalité du NA(P)T sert une fonction de sécurité, les solutions IPsec de traversée de NA(P)T ne devraient pas permettre que soit reçu du trafic entrant arbitraire IPsec ou IKE provenant de n'importe quelle adresse IP par un hôte derrière le NA(P)T, bien que l'état de transposition doive être conservé une fois que la communication bidirectionnelle IKE et IPsec est établie.

Scénario télécommutant

Comme une des principales utilisations de IPsec est l'accès à distance des Intranets d'entreprise, une solution de traversée de NA(P)T DOIT prendre en charge la traversée de NA(P)T, via soit le mode tunnel IPsec, soit le mode transport L2TP sur IPsec [RFC3193]. Cela inclut la prise en charge de la traversée de plus d'un NA(P)T entre le client distant et la passerelle de VPN.

Le client peut avoir une adresse acheminable et la passerelle VPN peut être derrière au moins un NA(P)T, ou autrement, le client et la passerelle VPN peuvent être tous deux derrière un ou plusieurs NA(P)T. Les télécommutants peuvent utiliser la même adresse IP privée, chacun derrière son propre NA(P)T, ou de nombreux télécommutants peuvent résider sur un

réseau privé derrière le même NA(P)T, chacun avec sa propre adresse privée unique, se connectant à la même passerelle de VPN. Comme IKE utilise l'accès UDP 500 comme destination, il n'est pas nécessaire d'activer plusieurs passerelles de VPN fonctionnant derrière la même adresse IP externe.

Scénario de passerelle à passerelle

Dans un scénario de passerelle à passerelle, un réseau à adressage privé (DMZ) peut être inséré entre le réseau d'entreprise et l'Internet. Dans ce concept, les passerelles de sécurité IPsec qui connectent des portions du réseau d'entreprise peuvent résider dans la DMZ et avoir des adresses privées dans leurs interfaces externes (DMZ). Un NA(P)T connecte le réseau DMZ à l'Internet.

Scénario de bout en bout

Une solution NAT-IPsec DOIT permettre une communication sûre TCP/IP d'hôte à hôte via IPsec, ainsi que des communications d'hôte à passerelle. Un hôte sur un réseau privé DOIT être capable de monter une ou plusieurs connexions TCP protégées par IPsec ou des sessions UDP avec un autre hôte avec un ou plusieurs NA(P)T entre eux. Par exemple, des NA(P)T peuvent être déployés au sein de filiales, les connectant au réseau d'entreprise, avec un NA(P)T supplémentaire connectant le réseau d'entreprise à l'Internet. De même, des NA(P)T peuvent être déployés au sein d'un réseau d'entreprise, LAN ou WAN, pour connecter des clients sans fils ou distants au réseau d'entreprise. Cela peut exiger un traitement spécial du trafic TCP et UDP sur l'hôte.

Amener des connexions SCTP à un autre hôte avec un ou plusieurs NA(P)T entre eux peut présenter des défis particuliers. SCTP prend en charge le multi-rattachement. Si plus d'une adresse IP est utilisée, ces adresses sont transportées au titre du paquet SCTP durant l'établissement d'association (dans les tronçons INIT et INIT-ACK). Si seulement des points d'extrémité SCTP à rattachement unique sont utilisés, la [RFC2960] paragraphe 3.3.2.1 déclare :
"Noter que ne pas utiliser de paramètre Adresse IP dans le INIT et l'INIT-ACK est une solution de remplacement à la création d'une association qui a plus de chances de fonctionner à travers une boîte de NAT."

Cela implique que les adresses IP ne devraient pas être placées dans le paquet SCTP sauf nécessité. Si des NAT sont présents et si des adresses IP sont incluses, l'établissement d'association va alors échouer. La [RFC5061] a été récemment proposée qui permet la modification de l'adresse IP une fois qu'une association a été établie. Les messages de modification ont aussi des adresses IP dans le paquet SCTP, et elles seront donc affectées par les NAT.

Compatibilité de pare-feu

Comme les pare-feu sont largement déployés, une solution de compatibilité NAT-IPsec DOIT permettre à un administrateur de pare-feu de créer des règles simples d'accès statique pour permettre ou refuser au trafic IKE et IPsec la traversée de NA(P)T. Cela implique, par exemple, que l'allocation dynamique d'accès de destination IKE ou IPsec est à éviter.

Adaptabilité

Une solution de compatibilité IPsec-NAT devrait être capable de se déployerau sein d'une installation consistant en milliers de télécommutants. Dans cette situation, il n'est pas possible de supposer que seulement un hôte est en train de communiquer avec une certaine destination à un instant donné. Donc, une solution de compatibilité IPsec-NAT DOIT régler la question du chevauchement des entrées de SPD et de démultiplexage des paquets entrants.

Prise en charge du mode

Au minimum, une solution de compatibilité IPsec-NAT DOIT prendre en charge la traversée des modes IKE et IPsec requis pour la prise en charge des [RFC2401] et [RFC2409]. Par exemple, une passerelle IPsec DOIT accepter que le mode tunnel ESP traverse le NA(P)T, et un hôte IPsec DOIT accepter que le mode transport IPsec traverse le NA(P)T. L'objet de AH est de protéger des champs immuables au sein de l'en-tête IP (y compris les adresses) et le NA(P)T traduit les adresses, invalidant la vérification d'intégrité AH. Il en résulte que NA(P)T et AH sont fondamentalement incompatibles et il n'est pas exigé qu'une solution de compatibilité IPsec-NAT prenne en charge le mode transport pour tunnel AH.

Rétro-compatibilité et interopérabilité

Une solution de compatibilité IPsec-NAT DOIT être interopérable avec les mises en œuvre IKE/IPsec existantes, afin qu'elles puissent communiquer lorsque aucun NA(P)T n'est présent. Cela implique qu'une solution de compatibilité IPsec-NAT DOIT être rétro-compatible avec IPsec comme défini dans la [RFC2401] et avec IKE comme défini dans la [RFC2409]. De plus, elle DEVRAIT être capable de détecter la présence d'un NA(P)T, afin que la prise en charge de la traversée de NA(P)T ne soit utilisée que lorsque nécessaire. Cela implique qu'il DOIT être possible de déterminer si une mise en œuvre IKE existante ne prend pas en charge la traversée de NA(P)T, afin qu'une conversation IKE standard puisse avoir lieu, comme décrit dans les [RFC2407], [RFC2408], et [RFC2409]. Noter que bien que cela implique l'initiation de IKE sur l'accès 500, il n'est pas exigé d'accès de source spécifique, de sorte que l'accès de source UDP 500 peut être utilisé ou non.

Sécurité

Une solution de compatibilité IPsec-NAT NE DOIT PAS introduire de faiblesses de sécurité supplémentaires à IKE ou à IPsec. Par exemple, un solution acceptable doit démontrer qu'elle n'introduit pas de nouvelles faiblesses face au déni de service ou à l'usurpation. IKE DOIT être autorisé à changer les clés de façon bidirectionnelle, comme décrit dans la [RFC2408].

4. Solutions existantes

4.1 Mode Tunnel IPsec

Dans un ensemble limité de circonstances, il est possible à une mise en œuvre d'IPsec en mode tunnel, telle que celle décrite dans la [RFC3456], de réussir à traverser un NA(P)T. Cependant, les exigences pour la réussite d'une traversée sont suffisamment limitées pour qu'une solution plus générale soit nécessaire :

1) IPsec ESP. Les tunnels IPsec ESP ne couvrent pas l'en-tête IP externe au sein de la vérification d'intégrité du message, et ils ne subiront donc pas l'invalidation de l'authentification des données à cause de la traduction d' adresse. Les tunnels IPsec n'ont pas non plus à se préoccuper d'invalidation de somme de contrôle.

2) Pas de validation d'adresse. La plupart des mises en œuvre actuelles d'IPsec en mode tunnel n'effectuent pas de validation d'adresse de source de sorte que les incompatibilités entre les identifiants IKE et les adresses de source ne seront pas détectées. Cela introduit des faiblesses de sécurité comme décrit à la Section 5.

3) Entrées de SPD "de tous à tous". Les clients IPsec en mode tunnel peuvent négocier des SPD "de tous à tous", qui ne sont pas invalidés par la traduction d'adresse. Cela empêche effectivement l'utilisation des SPD pour le filtrage d trafic tunnel admis.

4) Fonctionnement d'un seul client. Avec seulement un client derrière un NAT, il n'y a pas de risque de chevauchement de SPD. Comme le NAT n'aura pas besoin d'arbitrer entre des clients rivaux, il n'y a pas non plus de risque de mauvaise traduction de changement de clé, ou de SPI entrant incorrect, ou de démultiplexage de mouchard.

5) Pas de fragmentation. Lorsque l'authentification de certificat est utilisée, on peut rencontrer la fragmentation IKE. Cela peut se produire lorsque des chaînes de certificats sont utilisées, ou même lors de l'échange d'un seul certificat si la taille de clé, ou la taille d'autres champs de certificats (comme le nom distinctif et les autres extensions) est assez grand. Cependant, lorsque des clés prépartagées sont utilisées pour l'authentification, la fragmentation est moins probable.
6) Sessions actives. La plupart des sessions de VPN entretiennent normalement le flux de trafic en cours durant leur durée de vie de sorte que les transpositions d'accès UDP ne seront probablement pas supprimées à cause de l'inactivité.

4.2 RSIP

RSIP, décrit dans les [RFC3102] et [RFC3103], comporte des mécanismes pour la traversée d'IPsec, comme décrit dans la [RFC3104]. En permettant la communication d'hôte à NA(P)T, RSIP règle les problèmes de démultiplexage de SPI IPsec, ainsi que de chevauchement de SPD. Il convient donc à l'utilisation dans les entreprises, ainsi que dans les scénarios de réseautage domestique. En permettant aux hôtes derrière un NAT de partager l'adresse IP externe du NA(P)T (la passerelle RSIP) cette approche est compatible avec les protocoles qui incluent des adresses IP incorporées.

En tunnelant les paquets IKE et IPsec, RSIP évite des changements aux protocoles IKE et IPsec, bien que des changements majeurs soient requis des mises en œuvre d'hôte IKE et IPsec pour les faire bénéficier de la compatibilité RSIP. Il est donc compatible avec tous les protocoles (AH/ESP) et modes (transport et tunnel) existants.

Afin de traiter le démultiplexage des changements de clés IKE, RSIP exige le flottement de l'accès de source IKE, ainsi que le changement de clé vers l'accès flottant. Il en résulte que l'interopérabilité avec les mises en œuvre IPsec existantes n'est pas assurée.

RSIP ne satisfait pas aux exigences de déploiement d'une solution de compatibilité IPsec-NAT parce que un hôte à capacité RSIP exige une passerelle correspondante à capacité RSIP afin d'établir une SA IPsec avec un autre hôte. Comme RSIP n'exige de changement que des clients et des routeurs et non des serveurs, il est moins difficile à déployer que IPv6. Cependant, pour les fabricants, la mise en œuvre de RSIP exige une fraction substantielle des ressources exigées pour la prise en charge de IPv6. Donc, RSIP résout un problème "transitoire" sur une échelle à long terme, ce qui n'est pas très utile.

4.3 6à4

6à4, comme décrit dans la [RFC3056] peut constituer la base d'une solution à la traversée IPsec-NAT. Dans cette approche, le NAT fournit aux hôtes IPv6 un préfixe IPv6 déduit de l'adresse IPv4 externe du NAT, et encapsule les paquets IPv6 dans IPv4 pour la transmission aux autres hôtes 6à4 ou relais 6à4. Ceci permet qu'un hôte IPv6 qui utilise IPsec communique librement avec d'autres hôtes au sein des nuages IPv6 ou 6à4.

Bien que 6à4 soit une solution élégante et robuste lorsque un seul NA(P)T sépare un client et une passerelle VPN, il n'est pas universellement applicable. Comme 6à4 requiert l'allocation d'une adresse IPv4 acheminable au NA(P)T afin de permettre la formation d'un préfixe IPv6, il n'est pas utilisable lorsque plusieurs NA(P)T existent entre le client et la passerelle VPN. Par exemple, un NA(P)T avec une adresse privée sur son interface externe ne peut pas être utilisé par les clients derrière lui pour obtenir un préfixe IPv6 via 6à4.

Bien que 6à4 n'exige que peu de soutien supplémentaire de la part des hôtes qui prennent déjà en charge IPv6, il exige des changements sur les NAT, qui doivent être mis à niveau pour prendre en charge 6à4. Il en résulte que 6à4 peut ne pas convenir pour un déploiement à court terme.

5. Considérations pour la sécurité

Par définition, la compatibilité IPsec-NAT exige que les hôtes et routeurs qui mettent en œuvre IPsec soient capables de traiter en toute sécurité les paquets dont les en-têtes IP ne sont pas protégés cryptographiquement. Un certain nombre de problèmes en découlent qui valent d'être exposés.

Comme IPsec AH ne peut pas passer à travers un NAT, un des effets collatéraux de la fourniture d'une solution à la compatibilité IPsec-NAT peut être d'utiliser IPsec ESP avec chiffrement nul au lieu de AH lorsque un NAT existe entre la source et la destination. Cependant, on devrait noter que ESP avec chiffrement nul ne procure pas les mêmes propriétés de sécurité que AH. Par exemple, il y a des risques de sécurité qui se rapportent à l'acheminement de source IPv6 et qui sont empêchés par AH, mais pas par ESP avec chiffrement nul.

De plus, comme ESP avec toute transformation ne protège pas contre l'usurpation d'adresse de source, il est nécessaire d'opérer une certaine forme de vérification de bonne santé de l'adresse IP de source. L'importance de la vérification anti usurpation n'est pas très bien comprise. Il y a normalement une vérification anti-usurpation sur l'adresse IP de source au titre de IPsec_{esp,ah}_input(). Cela assure que l'origine du paquet a bien la même adresse que prétendu au sein des associations de sécurité IKE phase 1 et phase 2 originales. Lorsque un hôte receveur est derrière un NAT, cette vérification pourrait n'être pas aussi strictement significative pour les sessions en envoi individuel, tandis que dans l'Internet mondial, cette vérification est important pour que les session en mode tunnel en envoi individuel empêchent une attaque en usurpation décrite dans [AuthSource], qui peut survenir lorsque les contrôles d'accès chez le receveur dépendent de l'adresse IP de source des paquets ESP vérifiés après la désencapsulation. Les schémas de compatibilité IPsec-NAT devraient fournir une protection contre l'usurpation si ils utilisent les adresses de source pour les contrôles d'accès.

Considérons deux hôtes, A et C, tous deux derrière des NAT (différents) et qui négocient des SA IPsec en mode tunnel avec le routeur B. Les hôtes A et C peuvent avoir des privilèges différents ; par exemple, l'hôte A peut appartenir à un employé de confiance pour accéder à la plus grande partie de l'intranet d'entreprise, tandis que C pourrait être un co-contractant autorisé seulement à accéder à un site spécifique de la Toile.

Si l'hôte C envoie un paquet en mode tunnel qui usurpe l'adresse IP de A comme source, il est important qu'il ne soit pas accordé à ce paquet les privilèges correspondants à A. Si une authentification et une vérification d'intégrité sont effectuées, mais pas de vérification anti-usurpation (vérifiant que l'adresse IP d'origine correspond au SPI) alors l'hôte C peut être admis à atteindre des parties du réseau qui lui sont interdites. Il en résulte qu'un schéma de compatibilité IPsec-NAT DOIT assurer un certain degré de protection contre l'usurpation.

6. Références

6.1 Références normatives

[RFC0791] J. Postel, éd., "Protocole Internet - Spécification du protocole du programme Internet", STD 5, septembre 1981.

[RFC0793] J. Postel (éd.), "Protocole de commande de transmission – Spécification du protocole du programme Internet DARPA", STD 7, septembre 1981.

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

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

[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)

[RFC2663] P. Srisuresh, M. Holdrege, "Terminologie et considérations sur les traducteurs d'adresse réseau IP (NAT)", août 1999. *(Information)*

[RFC3022] P. Srisuresh, K. Egevang, "Traducteur d'adresse réseau IP traditionnel", janvier 2001. *(Information)*

6.2 Références pour information

[AuthSour] Kent, S., "Authenticated Source Addresses", Archives du groupe de travail IPsec (ftp://ftp.ans.net/pub/archive/IPsec), Message-Id : <v02130517ad121773c8ed@[128.89.0.110]>, 5 janvier 1996.

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

[RFC2960] R. Stewart et autres, "Protocole de transmission de commandes de flux", octobre 2000. (*Obsolète, voir* RFC4960) (*MàJ par* RFC3309) *(P.S.)*

[RFC3056] B. Carpenter, K. Moore, "Connexion des domaines IPv6 via des nuages IPv4", février 2001. *(P.S.)*

[RFC3102] M. Borella et autres, "IP spécifique de domaine : le cadre", octobre 2001. *(Expérimentale)*

[RFC3103] M. Borella et autres, "IP spécifique de domaine : Spécification du protocole", octobre 2001. *(Expérimentale)*

[RFC3104] G. Montenegro, M. Borella, "Prise en charge par RSIP d'IPsec de bout en bout", octobre 2001. *(Expérimentale)*

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

[RFC3309] J. Stone, R. Stewart, D. Otis, "Changement de somme de contrôle du protocole de transmission de commandes de flux (SCTP)". septembre 2002. (*Obsolète, voir* RFC4960) *(P.S.)*

[RFC3456] B. Patel et autres, "Protocole de configuration dynamique des hôtes (DHCPv4) Configuration du mode tunnel IPsec", janvier 2003. *(P.S.)*

[RFC5061] R. Stewart et autres, "Reconfiguration dynamique d'adresse pour le protocole de transmission de contrôle de flux (SCTP)", septembre 2007. *(P.S.)*

7. Remerciements

Merci à Steve Bellovin de AT&T Research, Michael Tuexen de Siemens, Peter Ford de Microsoft, Ran Atkinson de Extreme Networks, et Daniel Senie pour les discussions utiles sur cet espace de problème.

8. Adresse des auteurs

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
téléphone : +1 425 706 6605
mél : bernarda@microsoft.com

William Dixon
V6 Security, Inc.
601 Union Square, Suite #4200-300
Seattle, WA 98101
mél : ietf-wd@v6security.com

9. Déclaration complète de droits de reproduction

Propriété intellectuelle

Remerciement

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