Groupe de travail Réseau
Request for Comments : 2663
Catégorie : Information
Traduction Claude Brière de L'Isle

P. Srisuresh
M. Holdrege
Lucent Technologies
août 1999

Terminologie et considérations sur les traducteurs d'adresse réseau (NAT) IP

Statut de ce mémoire
Le présent mémoire apporte des informations pour 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.

Préface
Le présent document a pour objet de préciser les termes utilisés à propos des traducteurs d'adresse réseau (NAT, *Network Address Translator)*. Le terme de "traducteur d'adresse réseau" signifie des choses différentes selon le contexte. L'intention du document est de définir les diverses acceptions du NAT et de normaliser la signification des termes utilisés.

Les auteurs mentionnés sont les éditeurs de ce document et doivent son contenu aux contributions des membres du groupe de travail. De large parties du document intitulé "Le traducteur d'adresse réseau IP (NAT)" *(RFC1631)* ont été extraits presque tels quels pour constituer la base initiale de ce document. Les éditeurs tiennent à remercier les auteurs Pyda Srisuresh et Kjeld Egevang de leur travail, ainsi que Praveen Akkiraju de sa contribution à la description des scénarios de déploiement de NAT. Ils tiennent aussi à remercier les membres de l'IESG Scott Bradner, Vern Paxson et Thomas Narten de leur relecture détaillée du document et d'avoir amélioré la clarté du texte.

Résumé
La traduction d'adresse réseau est une méthode par laquelle des adresses IP sont transposées d'un domaine à un autre, pour tenter de fournir aux hôtes un acheminement transparent. Traditionnellement, les appareils de NAT sont utilisés pour connecter un domaine privé isolé qui a des adresses privées non enregistrées, à un domaine externe qui a des adresses enregistrées uniques au monde. Le présent document essaye de décrire le fonctionnement des appareils de NAT et les considérations qui y sont associées en général, et de définir la terminologie utilisée pour identifier diverses nuances de NAT.

Table des matières

1. Introduction et généralités

Le besoin de traduction des adresses IP se fait jour lorsque les adresses IP internes d'un réseau ne peuvent pas être utilisées à l'extérieur du réseau, soit parce qu'elles sont invalides à l'extérieur, soit parce que l'adressage interne doit rester confidentiel.

La traduction d'adresse permet (dans de nombreux cas, sauf comme noté aux sections 8 et 9) aux hôtes au sein d'un réseau privé de communiquer de façon transparente avec des destinations sur un réseau externe et vice versa. Il y a diverses nuances de NAT et il existe des termes pour les décrire. Le présent document tente de définir la terminologie utilisée et d'identifier diverses nuances de NAT. Il essaye aussi de décrire les autres considérations applicables aux appareils de NAT en général.

Noter cependant que le présent document n'est pas destiné à décrire le fonctionnement des divers NAT individuels ou l'applicabilité des appareils de NAT.

Les appareils de NAT tentent de fournir une solution d'acheminement transparente aux hôtes d'extrémité qui essayent de communiquer à partir de domaines d'adresses disparates. Ils le font en modifiant en chemin les adresses des nœuds d'extrémité et en conservant l'état pour ces mises à jour de telle sorte que les datagrammes appartenant à une session soient acheminés au bon nœud d'extrémité dans l'un et l'autre domaine. Cette solution ne fonctionne que lorsque les applications n'utilisent pas les adresses IP au titre du protocole lui-même. Par exemple, identifier les points d'extrémité qui utilisent les noms du DNS plutôt que les adresses rend les applications moins dépendantes des adresses réelles que choisissent les NAT et évite le besoin de traduire aussi les contenus de charge utile lorsque le NAT change une adresse IP.

La fonction de NAT ne peut pas par elle même prendre en charge de façon transparente toutes les applications et doit souvent coexister avec des passerelles de niveau application (ALG, *Application Layer Gateway*) pour cette raison. Les gens qui cherchent à déployer des solutions fondées sur les NAT doivent d'abord déterminer les exigences de leur application et s'assurer des extensions de NAT (c'est-à-dire, des ALG) nécessaires pour fournir la transparence d'application à leur environnement.

Les techniques IPsec qui sont destinées à préserver les adresses de point d'extrémité d'un paquet IP ne vont pas fonctionner avec un NAT sur leur chemin pour la plupart des applications en pratique. Des techniques comme AH et ESP protègent le contenu de l'en-tête IP (y compris les adresses de source et de destination) contre la modification. Néanmoins, le rôle fondamental du NAT est d'altérer les adresses dans l'en-tête IP d'un paquet.

2. Terminologie et concepts utilisés

Les termes le plus fréquemment utilisés dans le contexte de NAT sont définis ici pour servir de référence.

2.1 Domaine d'adresse ou domaine

Un domaine d'adresse est un domaine réseau dans lequel les adresses réseau sont allouées de façon univoque aux entités de telle façon que les datagrammes puissent leur être acheminés. Les protocoles d'acheminement utilisés au sein du domaine

réseau sont chargés de trouver les chemins vers les entités étant donnée leur adresse réseau. Noter que le présent document se limite à la description de NAT dans l'environnement IPv4 et ne traite pas de l'usage de NAT dans d'autres types d'environnements (par exemple, dans des environnements IPv6).

2.2 Acheminement transparent

Le terme "acheminement transparent" est utilisé dans tout ce document pour identifier la fonction d'acheminement que fournit un appareil de NAT. C'est différent de la fonction d'acheminement fournie par un routeur traditionnel en ce que ce dernier achemine les paquets au sein d'un seul domaine d'adresses.

L'acheminement transparent se réfère à l'acheminement d'un datagramme entre des domaines d'adresse disparates, en modifiant le contenu de l'adresse dans l'en-tête IP pour qu'elle soit valide dans le domaine d'adresse dans lequel est acheminé le datagramme. Le paragraphe 3.2 fait une description détaillée de l'acheminent transparent.

2.3 Flux de session contre flux de paquets

Les flux de connexion ou de session sont différents des flux de paquets. Un flux de session indique la direction dans laquelle la session a été initiée par référence à une interface réseau. Le flux de paquets est la direction dans laquelle le paquet a voyagé par référence à une interface réseau. Prenons pour exemple une session telnet sortante. La session telnet consiste en flux de paquets dans les deux directions entrante et sortante. Les paquets telnet sortants portent des frappes de touches de terminal et les paquets telnet entrants portent des affichages d'écran provenant du serveur telnet.

Pour les besoins de l'exposé dans le présent document, une session est définie comme l'ensemble de trafic qui est géré comme une unité pour la traduction. Les sessions TCP/UDP sont identifiées de façon univoque par le tuplet (adresse IP de source, accès TCP/UDP de source, adresse IP cible, accès TCP/UDP cible). Les sessions d'interrogation ICMP sont identifiées par le triplet (adresse IP de source, identifiant d'interrogation ICMP, adresse IP cible). Toutes les autres sessions sont caractérisées par le triplet (adresse IP de source, adresse IP cible, protocole IP).

Les traductions d'adresse effectuées par les NAT sont fondées sur la session et incluront la traduction des paquets entrants aussi bien que sortants qui appartiennent à cette session. La direction de la session est identifiée par la direction du premier paquet de cette session (voir au paragraphe 2.5).

Note : Il n'y a aucune garantie que l'idée d'une session, déterminée comme ci-dessus par le NAT, coïncide avec l'idée d'une session par l'application. Une application peut voir un faisceau de sessions (vues par le NAT) comme une seule session et peut même ne pas voir sa communication avec ses homologues comme une session. Il n'est pas garanti que toutes les applications fonctionnent à travers des domaines, même avec une ALG (définie ci-dessous au paragraphe 2.9) en chemin.

2.4 Accès TU, accès de serveur, accès de client

Dans la suite de ce document, on désigne simplement par "accès TU" les accès TCP/UDP associés à une adresse IP.

Pour la plupart des hôtes TCP/IP, l'accès TU dans la gamme 0 à 1023 est utilisé par les serveurs qui écoutent les connexions entrantes. Les clients qui essayent d'initier une connexion choisissent normalement un accès TU de source dans la gamme de 1024 à 65535. Cependant, cette convention n'est pas universelle et pas toujours suivie. Certaines stations clientes initient les connexions en utilisant un numéro d'accès TU de source dans la gamme de 0 à 1023, et il y a des serveurs qui écoutent les numéros d'accès TU dans la gamme de 1024 à 65535.

On trouvera une liste des services d'accès TU alloués dans la [RFC1700].

2.5 Début de session pour TCP, UDP et les autres

Le premier paquet de chaque session TCP essaye d'établir une session et contient des informations de démarrage de connexion. Le premier paquet d'une session TCP peut se reconnaître à la présence du bit SYN et à l'absence du bit ACK dans les fanions TCP. Tous les paquets TCP, à l'exception du premier paquet, doivent avoir le bit ACK établi.

Cependant, il n'y a aucun moyen déterminé pour reconnaître le début d'une session fondée sur UDP ou de toute session non TCP. Une approche heuristique serait de supposer que le premier paquet avec des paramètres de session jusque là non existants (comme défini au paragraphe 2.3) constitue le début d'une nouvelle session.

2.6 Fin de session pour TCP, UDP et les autres

La fin d'une session TCP est détectée lorsque FIN est acquitté par les deux moitiés de la session ou quand l'une et l'autre moitiés reçoivent un segment avec le bit RST établi dans le champ Fanions TCP. Cependant, parce qu'il est impossible à un appareil de NAT de savoir si le paquet qu'il voit va réellement être livré à la destination (il peut être abandonné entre le NAT et la destination) l'appareil de NAT ne peut pas supposer en toute sécurité que les segments qui contiennent des FIN ou des SYN seront les derniers paquets de la session (c'est-à-dire, il pourrait y avoir des retransmissions). Par conséquent, une session ne peut être supposée terminée qu'après une période de 4 minutes suite à cette détection. La nécessité de cette longue période d'attente est décrite dans la [RFC0793], qui suggère une durée TIME-WAIT de 2 * MSL (Durée de vie maximum de segment, *Maximum Segment Lifetime*) ou 4 minutes.

Noter qu'il est aussi possible à une connexion TCP de se terminer sans que l'appareil de NAT devienne conscient de l'événement (par exemple, dans le cas de réamorçage de l'un ou des deux homologues). Par conséquent, le ramassage des déchets est nécessaire sur les appareils de NAT pour nettoyer les états non utilisés sur des sessions TCP qui n'existent plus. Cependant, il n'est pas possible dans le cas général de faire la distinction entre les connexions qui ont été inactives pendant longtemps de celles qui n'existent plus. Dans le cas des sessions fondées sur UDP, il n'y a pas une façon unique de déterminer quand une session se termine, car les protocoles fondés sur UDP sont spécifiques des applications.

De nombreuses approches heuristiques sont utilisées pour terminer les sessions. On peut faire l'hypothèse que les sessions TCP qui n'ont pas été utilisées pendant, disons, 24 heures, et les sessions non TCP qui n'ont pas été utilisées pendant deux minutes, sont terminées. Cette hypothèse est souvent fondée, mais pas toujours. Ces temporisations de période d'inactivité de session varient beaucoup d'une application à l'autre et pour des sessions différentes de la même application. Par conséquent, les temporisations de session doivent être configurables. Même comme cela, il n'est pas garanti qu'une valeur satisfaisante puisse être trouvée. De plus, comme mentionné au paragraphe 2.3, il n'est pas garanti que la vue du NAT d'une fin de session coïncide avec celle de l'application.

Une autre façon de traiter les terminaisons de session est d'horodater les entrées et de les conserver aussi longtemps que possible, et de retirer la session inactive depuis le plus longtemps lorsque cela devient nécessaire.

2.7 Réseau public/mondial/externe

Un réseau mondial ou public est un domaine d'adresse avec des adresses réseau univoques allouées par l'Autorité d'allocation des numéros de l'Internet (IANA) ou un registraire d'adresses équivalent. Ce réseau est aussi désigné comme réseau externe dans les discussions sur les NAT.

2.8 Réseau privé/local

Un réseau privé est un domaine d'adresse indépendant des adresses de réseau externe. Le réseau privé peut aussi être désigné autrement comme réseau local. L'acheminement transparent entre les hôtes dans un domaine privé et le domaine externe est facilité par un routeur NAT.

La [RFC1918] fait des recommandations sur l'allocation de l'espace d'adresse pour les réseaux privés. L'Autorité d'allocation des numéros de l'Internet (IANA) a trois blocs d'espace d'adresse IP, à savoir 10/8, 172.16/12, et 192.168/16 qui sont mis de côté pour les internets privés. En notation pré-CIDR, le premier bloc n'est rien d'autre qu'un seul numéro de réseau de classe A, alors que le second bloc est un ensemble de 16 réseaux contigus de classe B, et que le troisième bloc est un ensemble de 256 réseaux contigus de classe C.

Une organisation qui décide d'utiliser des adresses dans l'espace d'adresse défini ci-dessus peut le faire sans se coordonner avec l'IANA ou avec un autre registre de l'Internet tel que APNIC, RIPE et ARIN. L'espace d'adresse peut donc être utilisé de façon privée par de nombreuses organisations indépendantes en même temps. Cependant, si ces organisations indépendantes décident ultérieurement qu'elles souhaitent communiquer les unes avec les autres ou avec l'Internet public, elles devront soit renuméroter leurs réseaux, soit activer un NAT sur leurs routeurs frontières.

2.9 Passerelle de niveau application (ALG)

Toutes les applications ne se prêtent pas facilement à la traduction par les appareils de NAT ; en particulier celles qui incluent des adresses IP et des accès TCP/UDP dans la charge utile. Les passerelles de niveau application (ALG, *Application Level Gateway*) sont des agents de traduction spécifiques des applications qui permettent à une application sur

un hôte dans un domaine d'adresse de se connecter de façon transparente à sa contrepartie qui fonctionne sur un hôte dans un domaine différent. Une ALG peut interagir avec un NAT pour établir l'état, utiliser les informations d'état du NAT, modifier une charge utile spécifique de l'application et effectuer tout ce qui est par ailleurs nécessaire pour faire fonctionner l'application à travers des domaines d'adresse disparates.

Les ALG ne peuvent pas toujours utiliser les informations d'état du NAT. Elles peuvent glaner une charge utile d'application et notifier simplement au NAT d'ajouter des informations d'état supplémentaires dans certains cas. Les ALG sont similaires aux mandataires, en ce que tous deux facilitent la communication spécifique d'application entre clients et serveurs. Les mandataires utilisent un protocole particulier pour communiquer avec les clients mandataires et relaient les données de client aux serveurs et vice versa. À la différence des mandataires, les ALG n'utilisent pas un protocole spécial pour communiquer avec les clients d'application et n'exigent pas de changements des clients d'application.

3. Qu'est un NAT ?

La traduction d'adresse réseau est une méthode par laquelle les adresses IP sont transposées d'un domaine d'adresse à un autre, fournissant un acheminement transparent aux hôtes d'extrémité. Il y a de nombreuses variantes de la traduction d'adresse qui se prêtent elles-mêmes à différentes applications. Cependant, toutes les nuances d'appareils de NAT devraient partager les caractéristiques suivantes.

a) Allocation d'adresse transparente
b) Acheminement transparent à travers la traduction d'adresse. (Acheminement se réfère ici à la transmission des paquets, et non à l'échange des informations d'acheminement.)
c) Traduction de la charge utile de paquet d'erreur ICMP.

Le diagramme ci-dessous illustre un scénario dans lequel le NAT est activé sur un routeur frontière de réseau d'extrémité, connecté à l'Internet à travers un routeur régional rendu disponible par un fournisseur de service.

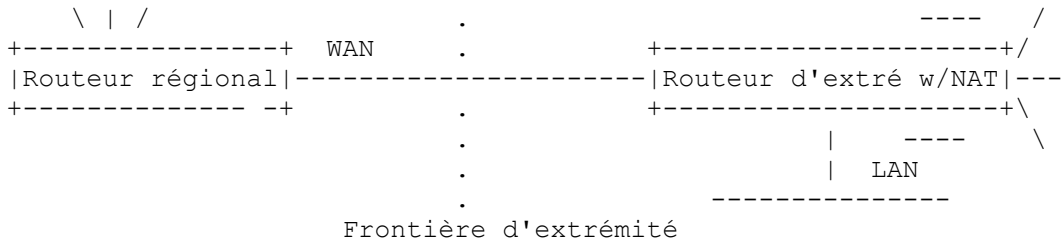


Figure 1 : Scénario typique de fonctionnement de NAT

3.1 Allocation d'adresse transparente

Le NAT lie les adresses dans le réseau privé avec les adresses dans le réseau global et vice versa pour fournir un acheminement transparent pour les datagrammes qui traversent les domaines d'adresse. Dans certains cas, le lien peut s'étendre aux identifiants de niveau transport (tels que les accès TCP/UDP). La liaison d'adresses est faite au démarrage d'une session. Les paragraphes qui suivent décrivent deux types d'allocation d'adresse.

3.1.1 Allocation statique d'adresse

Dans le cas d'allocation statique d'adresse, il y a une transposition d'adresse biunivoque pour les hôtes entre une adresse de réseau privé et une adresse de réseau externe pour la durée de vie du fonctionnement du NAT. Les allocations statiques d'adresse assurent que le NAT n'a pas à administrer la gestion d'adresses avec les flux de session.

3.1.2 Allocation dynamique d'adresse

Dans ce cas, les adresses externes sont allouées de façon dynamique aux hôtes du réseau privé ou vice versa, sur la base des exigences d'utilisation et les flux de session déterminés de façon heuristique par le NAT. Lorsque la dernière session qui utilisait une liaison d'adresse est terminée, le NAT va libérer le lien afin que l'adresse mondiale puisse être recyclée pour une utilisation ultérieure. La nature exacte de l'allocation d'adresse est spécifique de la mise en œuvre individuelle de NAT.

3.2 Acheminement transparent

Un routeur NAT se tient à la frontière entre deux domaines d'adresses et traduit les adresses en en-têtes IP de sorte que lorsque le paquet quitte un domaine et entre dans un autre, il puisse être acheminé correctement. Comme les appareils de NAT ont des connexions avec plusieurs domaines d'adresses, ils doivent veiller à ne pas propager à tort des informations (par exemple, via les protocoles d'acheminement) sur les réseaux d'un domaine d'adresse à un autre, lorsque une telle annonce serait jugée inacceptable.

Il y a trois phases à la traduction d'adresse. Ces trois phases résultent en la création, la maintenance et la terminaison des états pour les sessions qui passent à travers les appareils de NAT.

3.2.1 Liaison d'adresse

La liaison d'adresse est la phase dans laquelle une adresse IP de nœud local est associée à une adresse externe ou vice versa, pour les besoins de la traduction. La liaison d'adresse est fixe avec l'allocation statique d'adresse et est dynamique au moment du démarrage de la session avec les allocations dynamiques d'adresse. Une fois que le lien est en place entre les deux adresses, toutes les sessions ultérieures générées de ou vers cet hôte vont utiliser le même lien pour la traduction de paquet fondée sur la session.

De nouveaux liens d'adresse sont faits au démarrage d'une nouvelle session, si un tel lien d'adresse n'existait pas déjà. Une fois qu'une adresse locale est liée à une adresse externe, toutes les sessions suivantes originaires de la même adresse locale ou dirigées sur la même adresse locale vont utiliser le même lien.

Le début de chaque nouvelle session va résulter en la création d'un état pour faciliter la traduction des datagrammes appartenant à la session. Il peut y avoir de nombreuses sessions simultanées originaires du même hôte, fondées sur un seul lien d'adresse.

3.2.2 Recherche et traduction d'adresse

Une fois qu'un état est établi pour une session, tous les paquets qui appartiennent à la session seront soumis à la recherche d'adresse (et dans certains cas, à la recherche d'identifiant de transport) et à la traduction. La traduction d'identifiant d'adresse ou de transport pour un datagramme va résulter en la transmission du datagramme du domaine d'adresse d'origine au domaine d'adresse de destination avec les adresses réseau mises à jour de façon appropriée.

3.2.3 Dénouement d'adresse

Le dénouement d'adresse est la phase dans laquelle une adresse privée n'est plus associée à une adresse globale pour les besoins de la traduction. Le NAT va effectuer le dénouement d'adresse lorsque il estime que la dernière session qui utilisait un lien d'adresse est terminée. Se reporter au paragraphe 2.6 pour les moyens heuristiques de traiter une fin de session.

3.3 Traduction d'un paquet d'erreur ICMP

Tous les messages d'erreur ICMP (à l'exception du type de message Redirection) auront besoin d'être modifiés, lorsque ils passent à travers un NAT. Les types de message d'erreur ICMP qui ont besoin d'une modification de NAT incluent Destination injoignable, Extinction de source, Durée excédée et Problème de paramètre. Les NAT ne devraient pas tenter de modifier un type de message Redirection.

Les changements au message d'erreur ICMP vont inclure des changements au paquet IP d'origine (ou de portions de celui-ci) incorporés dans la charge utile du message d'erreur ICMP. Afin que le NAT soit complètement transparent pour les hôtes d'extrémité, l'adresse IP de l'en-tête IP incorporé dans la charge utile du paquet ICMP doit être modifiée, le champ somme de contrôle du même en-tête IP doit être modifié en conséquence, ainsi que l'en-tête de transport associé. La somme de contrôle d'en-tête ICMP doit aussi être modifiée pour refléter les changements apportés aux en-têtes IP et de transport dans la charge utile. De plus, l'en-tête IP normal doit aussi être modifié.

4. Diverses nuances de NAT

Il y a de nombreuses variations de traduction d'adresse qui conduisent à des applications différentes. Les nuances de NAT citées dans les paragraphes suivants ne constituent en aucune façon une liste exhaustive, mais elles saisissent les différences

significatives qui foisonnent.

Le diagramme suivant sera utilisé comme modèle de base pour illustrer les nuances de NAT. L'hôte A, avec l'adresse Adr-A, est situé dans un domaine privé, représenté par le réseau N-Pri. N-Pri est isolé du réseau externe par un routeur NAT. L'hôte X, avec l'adresse Adr-X est situé dans un domaine externe, représenté par le réseau N-Ext. Le routeur NAT avec deux interfaces, rattachées chacune à un des domaines, fournit un acheminement transparent entre les deux domaines. L'adresse Adr-Nx est allouée à l'interface au domaine externe et l'adresse Adr-Np est allouée à l'interface au domaine privé. De plus, on peut comprendre que les adresses Adr-A et Adr-Np correspondent au réseau N-Pri et que les adresses Adr-X et Adr-Nx correspondent au réseau N-Ext.

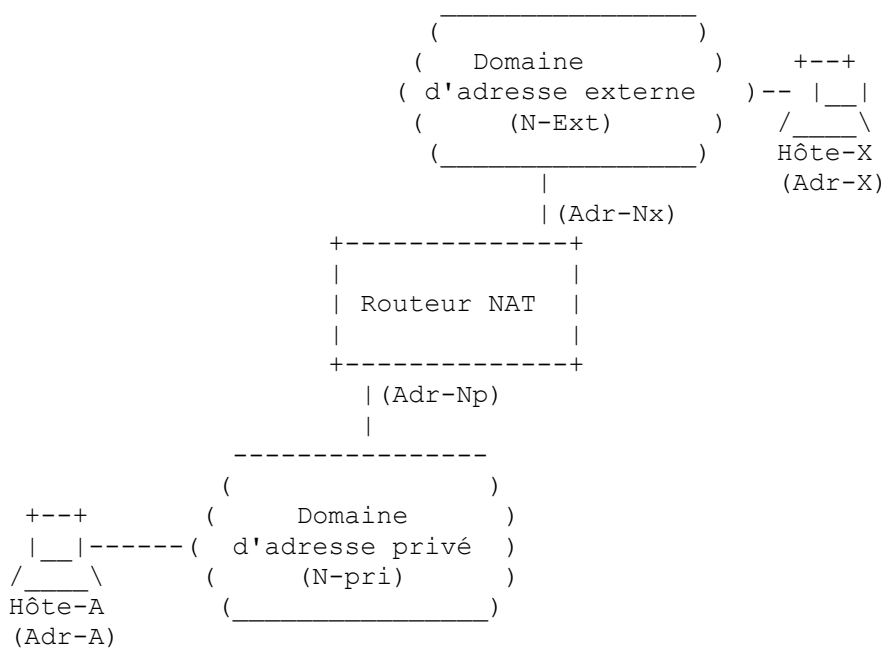


Figure 2 : Modèle de base pour illustrer les termes des NAT

4.1 NAT traditionnel (ou) NAT de sortie

Le NAT traditionnel va permettre aux hôtes au sein d'un réseau privé d'accéder de façon transparente aux hôtes qui sont dans le réseau externe, dans la plupart des cas. Dans un NAT traditionnel, les sessions sont unidirectionnelles, en sortie du réseau privé. Ceci s'oppose au NAT bidirectionnel, qui permet des sessions dans les deux directions entrante et sortante. Une description détaillée de NAT bidirectionnel se trouve au paragraphe 4.2.

Voici une description des propriétés des domaines pris en charge par les NAT traditionnels. Les adresses IP des hôtes dans le réseau externe sont uniques et valides dans les réseaux externes aussi bien que privés. Cependant, les adresses des hôtes dans un réseau privé ne sont uniques qu'au sein du réseau privé et peuvent n'être pas valides dans le réseau externe. En d'autres termes, le NAT ne va pas annoncer les réseaux privés dans le domaine externe. Mais, les réseaux du domaine externe peuvent être annoncés au sein du réseau privé. Les adresses utilisées au sein du réseau privé ne doivent pas se chevaucher avec les adresses externes. Une adresse donnée doit être soit une adresse privée, soit une adresse externe, mais pas les deux.

Un routeur NAT traditionnel dans la figure 2 permettrait à l'Hôte-A d'initier des sessions avec l'Hôte-X, mais pas l'inverse. Aussi, N-Ext est acheminable de l'intérieur de N-Pri, alors que N-Pri ne peut pas être acheminable à partir de N-Ext.

Un NAT traditionnel est principalement utilisé par des sites qui utilisent des adresses privées et qui souhaitent permettre des sessions sortantes à partir de leur site.

Il y a deux variantes du NAT traditionnel, à savoir le NAT de base et le traducteur d'adresse/accès réseau (NAPT, *Network Address/Port Translator*). Ils sont exposés dans les paragraphes suivants.

4.1.1 NAT de base

Avec le NAT de base, un bloc d'adresses externes est mis de côté pour traduire les adresses des hôtes dans un domaine privé lorsque elles sont générées par des sessions avec le domaine externe. Pour les paquets sortants du réseau privé, l'adresse IP de source et les champs qui s'y rapportent tels que les sommes de contrôle d'en-tête IP, TCP, UDP et ICMP sont traduits. Pour les paquets entrants, l'adresse IP de destination et les sommes de contrôle énumérées ci-dessus sont traduites.

Un routeur NAT de base dans la figure 2 peut être configuré pour traduire N-Pri en un bloc d'adresses externes, disons de Adr-i à Adr-n, choisies dans le réseau externe N-Ext.

4.1.2 Traducteur d'accès d'adresse réseau

Le NAPT étend d'un pas la notion de traduction en traduisant aussi l'identifiant de transport (par exemple, les numéros d'accès TCP et UDP, les identifiants d'interrogation ICMP). Cela permet de multiplexer les identifiants de transport d'un certain nombre d'hôtes privés dans les identifiants de transport d'une seule adresse externe. Le NAPT permet à un ensemble d'hôtes de partager une seule adresse externe. Noter que le NAPT peut être combiné avec un NAT de base de façon qu'un réservoir d'adresses externes soit utilisé en conjonction avec la traduction de l'accès.

Pour les paquets sortants du réseau privé, le NAPT va traduire l'adresse IP de source, l'identifiant de transport de source et les champs en rapport tels que IP, TCP, UDP et les sommes de contrôle d'en-tête ICMP. L'identifiant de transport peut être celui d'un accès TCP/UDP ou l'identifiant d'interrogation ICMP. Pour les paquets entrants, l'adresse IP de destination, l'identifiant de transport de destination et les sommes de contrôle d'en-tête de transport sont traduits.

Un routeur NAPT dans la figure 2 peut être configuré pour traduire des sessions générées de N-Pri en une seule adresse externe, disons Adr-i.

Très souvent, l'adresse Adr-Nx de l'interface externe du routeur NAPT est utilisée comme celle en laquelle transposer N-Pri.

4.2 NAT bidirectionnel

Avec un NAT bidirectionnel, les sessions peuvent être initiées à partir des hôtes dans le réseau public aussi bien que dans le réseau privé. Les adresses de réseau privé sont liées à des adresses uniques au monde, de façon statique ou dynamique lorsque les connexions sont établies dans l'une ou l'autre direction. L'espace de noms (c'est-à-dire, leurs noms de domaine pleinement qualifié) entre les hôtes dans les réseaux privés et externes est supposé être unique de bout en bout. Les hôtes dans le domaine externe accèdent aux hôtes du domaine privé en utilisant le DNS pour la résolution d'adresse. Une ALG DNS doit être utilisée en conjonction avec un NAT bidirectionnel pour faciliter la transposition de nom en adresse. Précisément, l'ALG DNS doit être capable de traduire les adresses de domaine privé en interrogations et réponses du DNS dans leurs liens d'adresse de domaine externe, et vice versa, lorsque les paquets DNS traversent entre domaines privé et externe.

Les exigences d'espace d'adresse mentionnées pour les routeurs NAT traditionnels sont également applicables ici.

Un routeur NAT bidirectionnel dans la figure 2 permettrait à l'Hôte-A d'initier des sessions avec l'Hôte-X, et à l'Hôte-X d'initier des sessions avec l'Hôte-A. Comme avec un NAT traditionnel, N-Ext est acheminable de l'intérieur de N-Pri, mais N-Pri peut n'être pas acheminable à partir de N-Ext.

4.3 NAT double

Le NAT double *(Twice-NAT)* est une variante de NAT où les adresses de source et de destination sont toutes deux modifiées par le NAT lorsque un datagramme traverse les domaines d'adresse. Ceci diffère du NAT traditionnel et du NAT bidirectionnel, où une seule des adresses (de source ou de destination) est traduite. Noter qu'il n'y a pas de terme du genre "NAT une fois".

Le NAT double est nécessaire lorsque des domaines privés et externes ont des collisions d'adresses. Le cas le plus courant où cela va arriver est quand un site a (à tort) numéroté ses nœuds internes en utilisant des adresses publiques qui ont été allouées à une autre organisation. Autrement, un site peut avoir changé de fournisseur de service, mais avoir choisi de garder (en interne) les adresses qui lui avaient été allouées par le premier fournisseur. Ce fournisseur pourrait ensuite avoir réalloué ces adresses à quelqu'un d'autre. Le problème clé dans ces cas là est que les adresses de l'hôte du domaine externe peuvent avoir été allouées à la même adresse qu'un hôte au sein du site local. Si cette adresse devait apparaître dans un

paquet, il serait transmis au nœud interne plutôt qu'au domaine externe à travers l'appareil de NAT. Le NAT double essaye d'établir un pont entre ces domaines en traduisant les deux adresses de source et de destination d'un paquet IP, lorsque le paquet change de domaine. Le NAT double fonctionne comme suit. Lorsque l'Hôte-A souhaite initier une session avec l'Hôte-X, il produit une interrogation DNS sur l'Hôte-X. Une ALG DNS intercepte l'interrogation DNS, et dans la réponse retournée à l'Hôte-A, l'ALG DNS remplace l'adresse de l'Hôte-X par une correctement acheminable dans le site local (disons Hôte-XPRIME). L'Hôte-A initie alors une communication avec l'Hôte-XPRIME. Lorsque les paquets traversent l'appareil de NAT, l'adresse IP de source est traduite (comme dans le cas du NAT traditionnel) et l'adresse de destination est traduite en Hôte-X. Une traduction similaire est effectuée sur les paquets de retour qui viennent de l'Hôte-X.

Voici une description des propriétés des domaines pris en charge par le NAT double. L'adresse réseau des hôtes dans le réseau externe est unique dans les réseaux externes, mais pas au sein du réseau privé. De même, l'adresse réseau des hôtes dans le réseau privé n'est unique qu'au sein du réseau privé. En d'autres termes, l'espace d'adresse utilisé dans le réseau privé pour localiser les hôtes dans les réseaux privés et publics est sans relation avec l'espace d'adresse utilisé dans le réseau public pour localiser les hôtes dans les réseaux privés et publics. Le NAT double ne serait pas autorisé à annoncer les réseaux locaux au réseau externe ou vice versa. Un routeur NAT double dans la figure 2 permettrait à l'Hôte-A d'initier des sessions pour l'Hôte-X, et à l'Hôte-X d'initier des sessions pour l'Hôte-A. Cependant, N-Ext (ou un sous ensemble de N-Ext) n'est pas acheminable à partir de l'intérieur de N-Pri, et N-Pri n'est pas acheminable à partir de N-Ext.

Le NAT double est normalement utilisé lorsque l'espace d'adresse utilisé dans un réseau privé se chevauche avec celui des adresses utilisé dans l'espace public. Par exemple, disons qu'un site privé utilise l'espace d'adresse 200.200.200.0/24 qui est officiellement alloué à un autre site dans l'Internet public. L'Hôte_A (200.200.200.1) dans l'espace privé cherche à se connecter à l'Hôte_X (200.200.200.100) dans l'espace public. Pour faire fonctionner cette connexion, l'adresse de l'Hôte_X est transposée en une adresse différente pour l'Hôte_A et vice versa. Le NAT double situé à la frontière du site privé peut être configuré comme suit :

Privé à public : 200.200.200.0/24 ---> 138.76.28.0/24
Public à privé : 200.200.200.0/24 ---> 172.16.1.0/24

Flux de datagrammes :	Hôte_A(Privé) ---> Hôte_X(Public)
a) Au sein du réseau privé :	A : 172.16.1.100 SA : 200.200.200.1
b) Après traduction du NAT double :	A : 200.200.200.100 SA : 138.76.28.1

Flux de datagrammes :	Hôte_X (Public) ---> Hôte_A (Privé)
a) Au sein du réseau public :	DA : 138.76.28.1 SA : 200.200.200.100
b) Après traduction du NAT double, dans le réseau privé	
	SA : 200.200.200.1 DA : 172.16.1.100

4.4 NAT multi rattachement

Il y a des limitations à l'utilisation des NAT. Par exemple, les demandes et les réponses qui appartiennent à une session doivent être acheminées via le même routeur NAT, car un routeur NAT conserve les informations d'état sur les sessions établies à travers lui. Pour cette raison, il est souvent suggéré que les routeurs NAT soient mis en œuvre sur un routeur frontière unique pour un domaine d'extrémité, où tous les paquets IP sont originaires du domaine ou destinés au domaine. Cependant, une telle configuration transformerait un routeur NAT en un seul point de défaillance.

Pour qu'un réseau privé s'assure de ce que la connexité avec les réseaux externes est conservée même en cas de défaillance d'une des liaisons avec le NAT, il est souvent souhaitable de faire plusieurs rattachements du réseau privé au même ou à plusieurs fournisseurs de service avec plusieurs connexions provenant du domaine privé, que ce soit du même boîtier de NAT ou de boîtiers différents.

Par exemple, un réseau privé pourrait avoir des liaisons avec deux fournisseurs différents et les sessions provenant des hôtes privés pourraient s'écouler à travers le routeur NAT avec la meilleure métrique pour une destination. Lorsque un des routeurs NAT connaît une défaillance, l'autre peut acheminer le trafic pour toutes les connexions.

Les boîtiers de NAT multiples ou les liaisons multiples sur le même boîtier de NAT, partageant la même configuration de NAT, peuvent fournir une sauvegarde contre les défaillances l'un de l'autre. Dans un tel cas, il est nécessaire que l'appareil de NAT de sauvegarde échange les informations d'état de sorte qu'un NAT de sauvegarde puisse prendre en charge les sessions de façon transparente lorsque le NAT principal tombe en panne. La sauvegarde de NAT devient plus simple lorsque la configuration se fonde sur des transpositions statiques.

5. IP spécifique du domaine (RSIP)

IP spécifique du domaine (RSIP, *Realm Specific IP*) est utilisé pour caractériser la fonctionnalité d'un hôte à capacité étendue sur le domaine dans un domaine privé, qui suppose une adresse IP spécifique du domaine pour communiquer avec les hôtes dans le domaine privé ou externe.

Un "client IP spécifique du domaine" (client RSIP) est un hôte dans un réseau privé qui adopte une adresse dans un domaine externe lorsque il se connecte à des hôtes dans ce domaine pour mener une communication de bout en bout. Les paquets générés par les hôtes sur l'une ou l'autre extrémité dans un tel réglage seront fondés sur les adresses qui sont uniques de bout en bout dans le domaine externe et ne requièrent pas de traduction par un processus intermédiaire.

Un serveur IP spécifique du domaine" (serveur RSIP) est un nœud résident sur les deux domaines privé et externe, qui peut faciliter l'acheminement des paquets du domaine externe au sein d'un domaine privé. Ces paquets peuvent avoir été générés par un client RSIP ou dirigés sur un client RSIP. Un serveur RSIP peut aussi être le même nœud qui alloue les adresses de domaine externe aux clients RSIP.

Il y a deux variantes de RSIP, à savoir, IP à adresse spécifique du domaine (RSA-IP) et IP à adresse et accès spécifiques du domaine (RSAP-IP). Ces variantes font l'objet des paragraphes qui suivent.

5.1 IP à adresse spécifique du domaine (RSA-IP)

Un client IP à adresse spécifique du domaine (RSA-IP) adopte une adresse IP de l'espace d'adresse externe lorsque il se connecte à un hôte dans le domaine externe. Une fois qu'un client RSA-IP a adopté une adresse externe, aucun autre hôte dans le domaine privé ou externe ne peut adopter la même adresse, jusqu'à ce que cette adresse soit libérée par le client RSA-IP.

Voici les différentes solutions d'acheminement qui peuvent être suivies par les paquets RSA-IP de bout en bout au sein du domaine privé. Une approche serait de tunneler le paquet vers sa destination. L'en-tête externe peut être traduit par le NAT comme un paquet normal sans affecter les adresses utilisées dans l'en-tête interne. Une autre approche serait d'établir un tunnel bidirectionnel entre le client RSA-IP et le routeur frontière, enjambant les deux domaines d'adresses. Les paquets de et vers le client seraient tunnelés, mais les paquets seraient transmis comme des paquets normaux entre le routeur frontière et la destination distante. Noter que le tunnel du client VERS le routeur frontière peut n'être pas nécessaire. On peut être capable de transmettre le paquet directement. Cela devrait fonctionner tant que le réseau interne ne filtre pas les paquets sur la base des adresses de source (qui dans ce cas seraient des adresses externes).

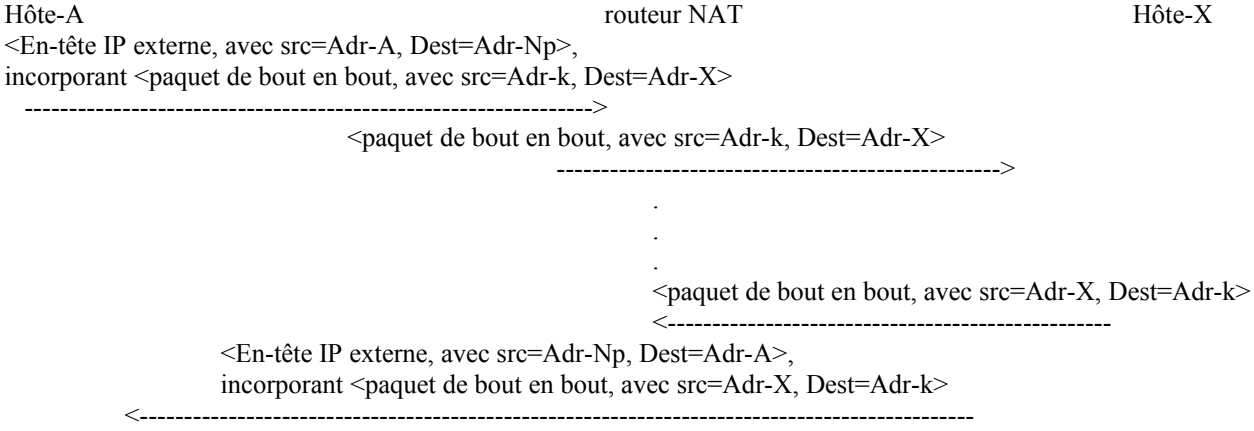
Par exemple, l'Hôte-A de la figure 2 ci-dessus pourrait adopter une adresse Adr-k dans le domaine externe et agir comme client RSA-IP pour permettre des sessions de bout en bout entre Adr-k et Adr-X. La traversée des paquets de bout en bout au sein du domaine privé peut être illustrée comme suit :

Première méthode, en utilisant le routeur NAT sur le chemin pour traduire :

```
==========================================================
Hôte-A                                routeur NAT                                Hôte-X
<En-tête IP externe, avec src=Adr-A, Dest=Adr-X>,
incorporant <paquet de bout en bout, avec src=Adr-k, Dest=Adr-X>
---------------------------------------------------------->
                          <En-tête IP externe, avec src=Adr-k, Dest=Adr-X>,
                          incorporant <paquet de bout en bout, avec src=Adr-k,  Dest=Adr-X>
                                       ------------------------------------------------------------------->
                                                .
                                                .
                                                .
                                                     <En-tête IP externe, avec src=Addr-X, Dest=Addr-k>,
                                              incorporant <paquet de bout en bout, avec src=Adr-X, Dest=Adr-k>
                                                <-------------------------------------------------
    <En-tête IP externe, avec src=Adr-X, Dest=Adr-A>,
    incorporant <paquet de bout en bout, avec src=Adr-X, Dest=Adr-k>
     <------------------------------------------------------------
```

Seconde méthode, en utilisant un tunnel au sein du domaine privé :

```
==================================================
```



Il peut y avoir d'autres approches pour poursuivre.

Un client RSA-IP a les caractéristiques suivantes. L'ensemble collectif des opérations effectuées par un client RSA-IP peut être appelé "RSA-IP".

1. Conscient du domaine auquel appartiennent les nœuds avec lesquels il échange du trafic,

2. Adopte une adresse provenant du domaine externe lors des communications avec des hôtes de ce domaine. Une telle adresse peut être allouée de façon statique ou obtenue de façon dynamique (par un protocole restant à définir) d'un nœud capable d'allouer des adresses à partir d'un domaine externe. Le serveur RSA-IP pourrait être le nœud qui coordonne l'allocation d'adresses de domaine externe.

3. Achemine les paquets vers les hôtes externes en utilisant une approche acceptable pour le serveur RSA-IP. En tous cas, le client RSA-IP va vraisemblablement devoir agir comme un point d'extrémité de tunnel, capable d'encapsuler les paquets de bout en bout tout en les transmettant et en les désencapsulant sur le chemin de retour.

Un "serveur d'adresse IP spécifique d'un domaine" (serveur RSA-IP) est un nœud qui réside sur les deux domaines privé et externe, qui facilite l'acheminement de paquets de domaine externe spécifique des clients RSA-IP à l'intérieur d'un domaine privé. Un serveur RSA-IP peut être décrit comme ayant les caractéristiques suivantes.

1. Il peut être configuré pour allouer des adresses d'un domaine externe aux clients RSA-IP, de façon statique ou dynamique.

2. Il doit être un routeur résidant sur les deux domaines d'adresses privé et externe.

3. Il doit être capable de fournir un mécanisme pour acheminer les paquets de domaine externe au sein du domaine privé. Des deux approches décrites, la première exige que le serveur RSA-IP soit un routeur NAT qui fournisse un acheminement transparent pour l'en-tête externe. Cette approche exige que l'homologue externe soit un point d'extrémité de tunnel.

Avec la seconde approche, un serveur RSA-IP pourrait être tout routeur (y compris un routeur NAT) qui peut être un point d'extrémité de tunnel avec les clients RSA-IP. Il va détunneler les paquets de bout en bout sortis des clients RSA-IP et les transmettre aux hôtes externes. Sur le chemin de retour, il va localiser le tunnel client RSA-IP, sur la base de l'adresse de destination du paquet de bout en bout et encapsuler le paquet dans un tunnel à transmettre au client RSA-IP.

Les clients RSA-IP peuvent suivre n'importe quelle technique IPsec, à savoir l'authentification et la confidentialité en mode transport ou tunnel en utilisant les en-têtes AH et ESP sur les paquets incorporés. Toutes les techniques de tunnelage peuvent être adaptées pour l'encapsulation entre le client RSA-IP et le serveur RSA-IP ou entre le client RSA-IP et l'hôte externe. Par exemple, l'encapsulation en mode tunnel IPsec est un type valide d'encapsulation qui assure l'authentification et la confidentialité IPsec pour les paquets incorporés de bout en bout.

5.2 IP à adresse et accès spécifiques du domaine (RSAP-IP)

IP à adresse et accès spécifiques du domaine (RSAP-IP) est une variante de RSIP en ce que plusieurs hôtes privés utilisent

une seule adresse externe, en multiplexant les identifiants de transport (c'est-à-dire, les numéros d'accès TCP/UDP et les identifiants d'interrogation ICMP).

Le "client RSAP-IP " peut être défini de façon similaire à celle du client RSA-IP avec la variante que le client RSAP-IP suppose un couple de (adresse externe, identifiant de transport) lorsque il se connecte aux hôtes dans le domaine externe pour conduire une communication de bout en bout. À ce titre, la communication avec les nœuds externes pour un client RSAP-IP peut être limitée à des sessions TCP, UDP et ICMP.

Le "serveur RSAP-IP " est similaire au serveur RSA-IP en ce qu'il facilite l'acheminement des paquets du domaine externe spécifiques des clients RSAP-IP à l'intérieur d'un domaine privé. Normalement, un serveur RSAP-IP serait aussi celui auquel sont alloués les couples de transport pour les clients RSAP-IP.

Un routeur NAPT sur le chemin pourrait tenir lieu de serveur RSAP-IP, lorsque l'encapsulation externe est fondée sur TCP/UDP et est adressée entre le client RSAP-IP et l'homologue externe. Cette approche requiert que l'homologue externe soit le point d'extrémité du tunnel fondé sur TCP/UDP. Avec cette approche, les clients RSAP-IP peuvent suivre toutes les techniques d'IPsec, à savoir l'authentification et la confidentialité en mode transport ou tunnel en utilisant les en-têtes AH et ESP sur les paquets incorporés. Noter cependant que le mode tunnel IPsec n'est pas un type valide d'encapsulation, car un routeur NAPT ne peut pas fournir la transparence de l'acheminement aux protocoles AH et ESP.

Autrement, les paquets peuvent être tunnelés entre client RSAP-IP et serveur RSAP-IP de telle façon que le serveur RSAP-IP détunnelle les paquets sortant des clients RSAP-IP et les transmette aux hôtes externes. Sur le chemin de retour, le serveur RSAP-IP va localiser le tunnel client RSAP-IP, sur la base du couple (adresse de destination, identifiant de transport) et encapsuler le paquet d'origine au sein d'un tunnel pour transmission au client RSAP-IP. Avec cette approche, il n'y a pas de limitation à la technique de tunnelage employée entre client RSAP-IP et serveur RSAP-IP. Cependant, il y a des limitations à l'application de la sécurité fondée sur IPsec pour les paquets de bout en bout. L'authentification et l'intégrité fondées sur le mode transport peuvent être atteintes. Mais la confidentialité ne peut être permise parce que le serveur RSAP-IP doit être capable d'examiner l'identifiant de transport de destination afin d'identifier le tunnel RSAP-IP auquel transmettre les paquets entrants. Pour cette raison, seuls les paquets en mode transport TCP, UDP et ICMP protégés par l'authentification AH et ESP peuvent traverser un serveur RSAP-IP en utilisant cette approche.

Par exemple, disons que l'Hôte-A de la figure 2 ci-dessus, obtient un couple de (Adr-Nx, accès TCP T-Nx) du routeur NAPT pour agir comme client RSAP-IP pour initier des sessions TCP de bout en bout avec l'Hôte-X. La traversée des paquets de bout en bout au sein du réseau privé peut être illustrée comme suit. Dans la première méthode, la couche externe du paquet sortant de l'Hôte-A utilise (adresse privée Adr-A, accès de source T-Na) comme couple de source pour communiquer avec l'Hôte-X. Le routeur NAPT sur le chemin traduit ce couple en (Adr-Nx, accès T-Nxa). Cette traduction est indépendante des paramètres du couple du client RSAP-IP utilisés dans le paquet incorporé.

Première méthode, utilisant le routeur NAPT en chemin pour traduire :
==========

Hôte-A **routeur NAT** **Hôte-X**

<Paquet TCP/UDP externe, avec src=Adr-A, , Src Port=T-Na, Dest=Adr-Np>,
incorporant <paquet de bout en bout, avec src=Adr-Nx, Src Port=T-Nx, Dest=Adr-X>
---------->

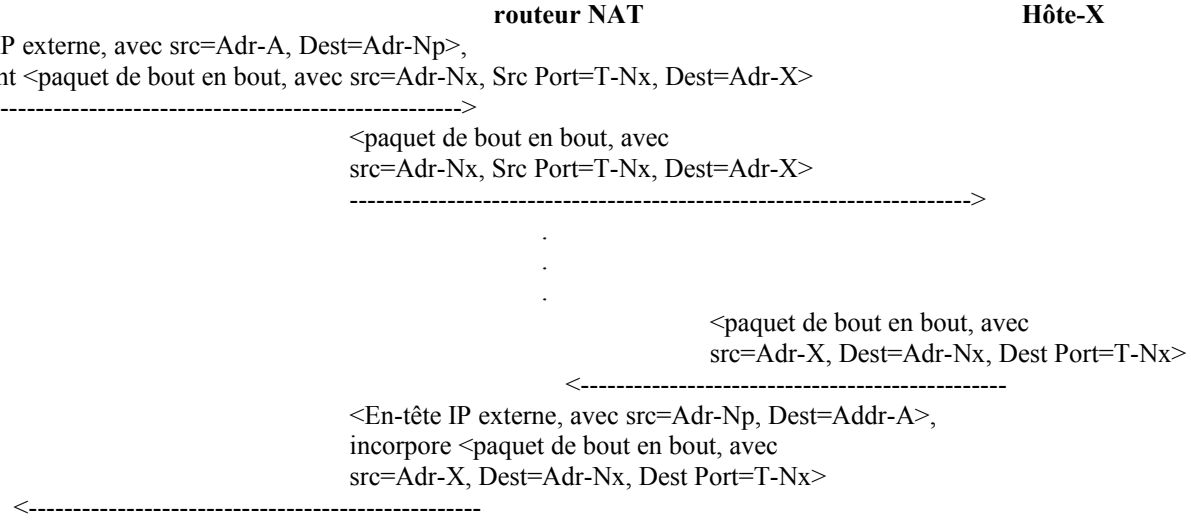
<Paquet TCP/UDP externe, avec src=Adr-Nx, Src Port=T-Nxa, Dest=Adr-X>,
incorporant <paquet de bout en bout, avec src=Adr-Nx, Src Port=T-Nx, Dest=Adr-X>
---------->

.
.
.

<Paquet TCP/UDP externe, avec src=Adr-X, Dest=Adr-Nx, Dest Port=T-Nxa>,
incorporant <paquet de bout en bout, avec src=Adr-X, Dest=Adr-Nx, Dest Port=T-Nx>
<----------

<Paquet TCP/UDP externe, avec src=Adr-X, Dest=Adr-A, Dest Port=T-Na>,
incorporant <paquet de bout en bout, avec src=Adr-X, Dest=Adr-Nx, Dest Port=T-Nx>
<----------

Seconde méthode, utilisant un tunnel au sein du domaine privé :
==========



6. Réseaux privés et tunnels

Considérons maintenant le cas où le réseau privé est connecté au monde extérieur via des tunnels. Dans un tel cas, le trafic encapsulé dans le tunnel peut ou non contenir des paquets traduits selon les caractéristiques des domaines d'adresses que relie le tunnel.

Les paragraphes qui suivent exposent deux scénarios où les tunnels sont utilisés (a) en conjonction avec la traduction d'adresse, et (b) sans traduction.

6.1 Tunnelage des paquets traduits

Toutes les variantes de traduction d'adresse exposées dans les sections précédentes peuvent être applicables aux liaisons directement connectées aussi bien qu'aux tunnels et aux réseaux privés virtuels (VPN).

Par exemple, un réseau privé connecté à un partenaire commercial par un VPN peut employer un NAT traditionnel pour communiquer avec le partenaire. De même, il est possible d'employer un NAT double, si l'espace d'adresse du partenaire se chevauche avec celui du réseau privé. Il pourrait y avoir un appareil de NAT sur une extrémité du tunnel ou sur les deux. Dans tous les cas, le trafic à travers le VPN peut être chiffré pour les besoins de la sécurité. Sécurité se réfère ici à la sécurité du trafic à travers les seuls VPN. La sécurité de bout en bout exige la confiance envers les appareils de NAT au sein du réseau privé.

6.2 Réseaux privés éclatés

Il y a de nombreuses instances de réseaux privés (comme un réseau d'entreprise) éclatés sur différents sites et qui utilisent le réseau public pour les communications entre ces sites. Dans de tels cas, il n'est pas souhaitable de faire la traduction d'adresse, à la fois parce que un grand nombre d'hôtes peuvent vouloir communiquer avec le réseau général, ce qui exige donc de gros tableaux d'adresses, et parce qu'il y aura plus d'applications qui dépendent des adresses configurées, plutôt que d'aller voir un serveur de noms. On appelle un tel réseau privé un réseau privé éclaté.

Les bouts de réseau éclatés devraient se comporter comme si ils n'étaient pas éclatés. C'est à dire que les routeurs dans toutes les partitions devraient conserver les chemins vers les espaces d'adresses locaux de toutes les partitions. Bien sûr, le cœur de réseau (public) ne conserve pas le chemin vers les adresses locales. Donc, les routeurs frontières doivent tunneler (en utilisant les VPN) à travers les cœurs de réseau en se servant de l'encapsulation. Pour ce faire, chaque boîtier de NAT va mettre de côté une adresse mondiale pour le tunnelage.

Lorsque un boîtier de NAT x dans une partition d'extrémité X souhaite livrer un paquet à la partition d'extrémité Y, il va encapsuler le paquet dans un en-tête IP avec l'adresse de destination réglée à l'adresse mondiale du boîtier NAT y qui a été réservée pour l'encapsulation. Lorsque le boîtier NAT y reçoit un paquet avec cette adresse de destination, il désencapsule l'en-tête IP et achemine le paquet en interne. Noter qu'il n'y a pas de traduction d'adresse dans le processus, simplement le

transfert de paquets du réseau privé sur un cœur de réseau en tunnel à travers le réseau externe.

7. Caractéristiques du fonctionnement des NAT

Les appareils de NAT sont ignorants de l'application en ce que les traductions sont limitées aux seuls en-têtes IP/TCP/UDP/ICMP et messages d'erreur ICMP. Les appareils de NAT ne changent pas la charge utile des paquets, car les charges utiles tendent à être spécifiques de l'application.

Les appareils de NAT (en y incluant les ALG) n'examinent pas ni ne modifient la charge utile de transport. Pour cette raison, les appareils de NAT sont transparents aux applications dans de nombreux cas. Il y a cependant deux zones dans lesquelles les appareils de NAT causent souvent des difficultés : 1) lorsque une charge utile d'application comporte une adresse IP, et 2) lorsque la sécurité de bout en bout est nécessaire. Noter que cette liste n'est pas exhaustive.

Les techniques de sécurité de couche application qui n'utilisent pas ou ne dépendent pas des adresses IP vont fonctionner correctement en présence de NAT (par exemple, TLS, SSL et ssh). À l'opposé, ce n'est pas le cas pour les techniques de couche transport telles que IPSec en mode transport ou l'option signature MD5 de TCP [RFC2385].

Dans le mode transport IPSec, AH et ESP ont tous deux une vérification d'intégrité qui couvre la totalité de la charge utile. Lorsque la charge utile est TCP ou UDP, la somme de contrôle TCP/UDP est couverte par la vérification d'intégrité. Lorsque un appareil de NAT modifie une adresse, la somme de contrôle n'est plus valide par rapport à la nouvelle adresse. Normalement, le NAT met aussi à jour la somme de contrôle, mais c'est inefficace lorsque AH et ESP sont utilisés. Par conséquent, les receveurs vont éliminer un paquet soit parce qu'il échoue à la vérification d'intégrité IPSec (si l'appareil de NAT met à jour la somme de contrôle) soit parce que la somme de contrôle est invalide (si l'appareil de NAT laisse la somme de contrôle sans modification).

Noter que ESP en mode tunnel IPsec est permissible pour autant que le contenu du paquet incorporé n'est pas affecté par la traduction de l'en-tête IP externe. Bien que cette technique ne fonctionne pas dans les développements de NAT traditionnels (c'est-à-dire, lorsque les hôtes ne sont pas conscients de la présence du NAT) la technique est applicable à IP spécifique du domaine comme décrit à la Section 5.

Noter aussi que l'authentification et la confidentialité en mode transport fondée sur ESP de bout en bout sont aussi permises pour les paquets tels que ICMP, dont le contenu de charge utile IP reste non affecté par la traduction de l'en-tête IP externe.

Les appareils de NAT ne sont pas compatibles avec les hypothèses fondamentales des infrastructures de distribution de clés publiques telles que le DNS sécurisé [RFC2535] et les certificats X.509 avec signature par clés publiques. Dans le cas de DNS sécurisé, chaque RRset du DNS est signé avec une clé provenant de l'intérieur de la zone. De plus, l'authenticité d'une clé spécifique est vérifiée en suivant une chaîne de confiance qui va jusqu'à la racine du DNS. Lorsque une ALG DNS modifie les adresses (par exemple, comme dans le cas du NAT double) la vérification des signatures échoue.

Il peut être intéressant de noter que IKE (le protocole de négociation de clés de session) est un protocole de couche session fondé sur UDP et qu'il n'est pas protégé par la sécurité IPsec fondée sur le réseau. Seule une portion des charges utiles individuelles est protégée au sein de IKE. Il en résulte que les sessions IKE sont permissibles à travers un NAT pour autant que la charge utile IKE ne contienne pas d'adresses et/ou d'identifiants de transport spécifiques d'un domaine et pas de l'autre. Étant donné que IKE est utilisé pour établir les associations IPSec, et qu'il n'y a à présent aucun moyen connu de faire fonctionner IPSec à travers une fonction de NAT, il reviendra à de futurs sujets de travail de tirer parti de IKE à travers un boîtier de NAT.

Une des applications les plus populaires de l'Internet, "FTP", ne devrait pas fonctionner avec la définition du NAT décrite ici. Les paragraphes qui suivent sont consacrés à la description de la façon dont FTP est pris en charge sur les appareils de NAT. L'ALG FTP fait partie intégrante de la plupart des mises en œuvre de NAT. Certains fabricants peuvent choisir d'inclure des ALG supplémentaires pour prendre en charge d'autres applications sur l'appareil de NAT.

7.1 Prise en charge de FTP

La commande "PORT" et la réponse "PASV" dans la charge utile de contrôle de FTP identifie l'adresse IP et l'accès TCP qui doivent être utilisés pour la session de données qu'elle prend en charge. Les arguments pour la commande PORT et la réponse PASV sont une adresse IP et un accès TCP en ASCII. Une ALG FTP est obligée de surveiller et mettre à jour la charge utile de session de contrôle FTP de telle sorte que les informations contenues dans la charge utile soient pertinentes

pour les nœuds d'extrémité. L'ALG doit aussi mettre à jour le NAT avec les tuplets de session de données appropriés et les orientations de session de telle sorte que le NAT puisse établir les informations d'état pour les sessions de données FTP.

Comme l'adresse et l'accès TCP sont codés en ASCII, il peut en résulter un changement de taille du paquet. Par exemple, 10,18,177,42,64,87 fait 18 caractères ASCII, tandis que 193,45,228,137,64,87 fait 20 caractères ASCII. Si la nouvelle taille est la même que celle de la précédente, seule la somme de contrôle TCP devra subir un ajustement par suite du changement des données. Si la nouvelle taille est inférieure ou supérieure à la précédente, les numéros de séquence TCP doivent aussi être changés pour refléter le changement de longueur de la portion de données de contrôle FTP. Un tableau spécial peut être utilisé par l'ALG pour corriger la séquence TCP et accuser réception des numéros. La correction du numéro de séquence et de l'accusé de réception devra être faite sur tous les paquets futurs de la connexion.

8. Limitations des NAT

8.1 Applications avec un contenu d'adresse IP

Toutes les applications ne se prêtent pas facilement à la traduction par les appareils de NAT. En particulier, les applications qui portent une adresse IP (et un accès TU, dans le cas de NAPT) à l'intérieur de la charge utile. Les passerelles de niveau application (ALG, *Application Level Gateway*) doivent être utilisées pour effectuer les traductions sur les paquets qui relèvent de telles applications. Les ALG peuvent facultativement utiliser les allocations d'adresse (et d'accès TU) faites par le NAT et effectuer des traductions spécifiques de l'application. La combinaison de la fonction de NAT et de l'ALG ne va pas apporter la sécurité de bout en bout assurée par IPsec. Cependant, IPsec en mode tunnel peut être accompli avec le routeur NAT servant de point d'extrémité de tunnel.

SNMP est une de ces applications qui ont un contenu d'adresse dans la charge utile. Les routeurs NAT ne vont pas traduire les adresses IP au sein des charges utiles SNMP. Il n'est pas si inhabituel qu'une ALG spécifique de SNMP réside sur un routeur NAT pour effectuer des traductions de MIB SNMP propres au réseau privé.

8.2 Applications avec contrôle inter dépendant et sessions de données

Les appareils de NAT fonctionnent sous l'hypothèse que chaque session est indépendante. Les caractéristiques de session telles que l'orientation, les adresses IP de source et de destination, le protocole de session, et les identifiants de niveau transport de source et de destination sont déterminés indépendamment au début de chaque nouvelle session.

Cependant, il y a des applications comme H.323 qui utilisent une ou plusieurs sessions de contrôle pour régler les caractéristiques des sessions à suivre dans leur charge utile de session de contrôle. De telles applications requièrent l'utilisation d'ALG spécifiques d'application qui puissent interpréter et traduire la charge utile, si nécessaire. L'interprétation de la charge utile va aider le NAT à être prêt pour les sessions de données à suivre.

8.3 Considérations sur le débogage

Le NAT augmente la probabilité d'un mauvais adressage. Par exemple, la même adresse locale peut être liée à des adresses mondiales différentes à des moments différents et vice versa. Il en résultera que toute étude de flux de trafic fondée uniquement sur les adresses mondiales et les accès TU pourrait être trompeuse et conduire à mal interpréter ses résultats.

Si un hôte abuse de l'Internet de quelque façon (comme d'essayer d'attaquer une autre machine ou même en envoyant de grosses quantités de pourriels ou d'autre chose) il est plus difficile d'épingler la source des troubles parce que l'adresse IP de l'hôte est cachée dans un routeur NAT.

8.4 Traduction de paquets de contrôle FTP fragmentés

La traduction des paquets de contrôle FTP fragmentés est délicate quand les paquets contiennent la commande "PORT" ou la réponse à la commande "PASV". C'est clairement un cas pathologique. Le routeur NAT va avoir besoin d'assembler d'abord les fragments puis de traduire avant la transmission.

Encore un autre cas sera celui où chaque caractère des paquets qui contiennent la commande "PORT" ou la réponse à "PASV" est envoyé dans un datagramme séparé, non fragmenté. Dans ce cas, le NAT va devoir simplement laisser passer les paquets, sans traduire la charge utile TCP. Bien sûr, l'application va échouer si la charge utile aurait dû être altérée. L'application pourrait encore fonctionner dans quelques cas, lorsque le contenu de la charge utile peut être valide dans les deux domaines, sans modification en chemin. Par exemple, du FTP généré dans un hôte privé va encore fonctionner lors de

la traversée d'un NAT traditionnel ou d'un appareil de NAT bidirectionnel, pour autant que la session de contrôle FTP ait employé la commande PASV pour établir les sessions de données. La raison en est que l'adresse et le numéro d'accès spécifiés par le serveur FTP dans la réponse à PASV (envoyée sous forme de plusieurs paquets non fragmentés) est valide pour l'hôte privé, telle quelle. L'appareil de NAT va simplement voir la session de données qui s'ensuit (qui est aussi générée par l'hôte privé) comme une session TCP indépendante.

8.5 Intensité du calcul

Le NAT est gourmand en calcul, même avec l'aide d'un algorithme habile d'ajustement de la somme de contrôle, car chaque paquet de données est soumis à l'examen du NAT et à modifications. Il en résulte que le débit de transmission du routeur pourrait être considérablement ralenti. Cependant, tant que la capacité de traitement de l'appareil de NAT excède le taux de traitement en ligne, cela ne devrait pas être un problème.

9. Considérations pour la sécurité

De nombreuses personnes voient le routeur NAT traditionnel comme un filtre de trafic unidirectionnel (par session) qui empêche les sessions provenant des hôtes externes d'accéder à leurs machines. De plus, lorsque l'allocation d'adresse dans un routeur NAT est faite de façon dynamique, cela rend plus difficile qu'un attaquant pointe un hôte spécifique dans le domaine du NAT. Les routeurs NAT peuvent être utilisés en conjonction avec des pare-feu pour filtrer le trafic non désiré.

Si l'appareil de NAT et les ALG ne sont pas dans une frontière de domaine de confiance, il y a un problème de sécurité majeur, car les ALG peuvent fureter dans la charge utile du trafic de l'utilisateur final. La charge utile de niveau session peut être chiffrée de bout en bout, pour autant que la charge utile ne contienne pas d'adresses IP et/ou d'identifiants de transport qui ne soient valides que dans un des domaines. À l' exception de RSIP, la sécurité de niveau réseau IP de bout en bout par les techniques IPsec actuelles ne peut pas être atteinte avec des appareils de NAT interposés. Une des extrémités doit être un boîtier de NAT. Voir à la section 7 l'exposé sur la raison pour laquelle la sécurité IPsec de bout en bout ne peut pas être assurée avec des appareils de NAT le long du chemin.

La combinaison de la fonction de NAT, des ALG et des pare-feu va fournir un environnement de travail transparent pour un domaine de réseautage privé. À l'exception de RSIP, la sécurité réseau de bout en bout assurée par IPsec ne peut pas être atteinte pour les hôtes d'extrémité au sein du réseau privé (voir à la Section 5 le fonctionnement RSIP). Dans tous les autres cas, si on veut utiliser IPsec de bout en bout, il ne peut pas y avoir d'appareil de NAT sur le chemin. Si on fait l'hypothèse que les appareils de NAT font partie d'une frontière de confiance, IPsec en mode tunnel peut être réalisé avec un routeur NAT (ou une combinaison de NAT, ALG et pare-feu) servant de point d'extrémité de tunnel.

Les appareils de NAT lorsque combinés avec des ALG, peuvent assurer que les datagrammes injectés dans l'Internet n'ont pas d'adresses privées dans leurs en-têtes ou charge utile. Les applications qui ne satisfont pas ces exigences peuvent abandonner l'usage des filtres pare-feu. Pour cette raison, il n'est pas anormal de trouver les fonctions de NAT, ALG et pare-feu qui coexistent pour fournir la sécurité aux frontières d'un réseau privé. Les passerelles NAT peuvent être utilisées comme points d'extrémité de tunnel pour fournir un transport des paquets de données par réseau privé virtuel sécurisé à travers un domaine de réseau externe.

Voici quelques considérations supplémentaires sur la sécurité associées aux routeurs NAT.

1. Les sessions UDP sont non sûres par nature. Les réponses à un datagramme pourraient venir d'une adresse différente de l'adresse cible utilisée par l'envoyeur ([RFC1123]). Il en résulte qu'un paquet UDP entrant ne peut satisfaire qu'en partie à une session sortante d'une routeur NAT traditionnel (l'adresse de destination et le numéro d'accès UDP du paquet correspondent, mais pas l'adresse et le numéro d'accès de source). Dans un tel cas, il y a pour l'appareil de NAT une compromission potentielle de la sécurité à permettre l'entrée de paquets qui ne correspondent que partiellement. Ce problème de sécurité avec UDP est aussi inhérent aux pare-feu.

   Les mises en œuvre de NAT traditionnel qui ne suivent pas les datagrammes sur la base de la session mais globalisent les états de multiples sessions UDP en utilisant les mêmes liens d'adresses dans une seule session unifiée pourraient compromettre encore plus la sécurité. Cela parce que la granularité de la confrontation des paquets serait encore plus limitée à la seule adresse de destination des paquets UDP entrants.

2. Les sessions de diffusion groupée (fondées sur UDP) sont une autre source de faiblesse pour la sécurité pour les routeurs NAT traditionnels. Une fois encore, les pare-feu sont confrontés au même dilemme que les routeurs NAT.

Disons qu'un hôte sur un réseau privé initie une session en diffusion groupée. Le datagramme envoyé par l'hôte privé peut déclancher des réponses dans la direction inverse de la part de multiples hôtes externes. Les mises en œuvre de NAT traditionnel qui utilisent un seul état pour suivre une session de diffusion groupée ne peuvent pas déterminer avec certitude si le paquet UDP entrant est en réponse à une session de diffusion groupée existante ou le début d'une nouvelle session UDP initiée par un attaquant.

3. Les appareils de NAT peuvent être la cible d'attaques.

   Comme les appareils de NAT sont des hôtes Internet, ils peuvent être la cible d'un certain nombre d'attaques différentes, telles que les attaques par inondation de SYN ou de ping. Les appareils de NAT devraient employer la même sorte de techniques de protection que celles des serveurs de l'Internet.

Références

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

[RFC0792] J. Postel, "Protocole du message de contrôle Internet – Spécification du protocole du programme Internet DARPA", STD 5, septembre 1981.

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

[RFC0950] J. Mogul et J. Postel, "Procédure standard de sous-réseautage Internet", (STD 5) août 1985.

[RFC0959] J. Postel et J. Reynolds, "Protocole de transfert de fichiers (FTP)", STD 9, octobre 1985.

[RFC1122], R. Braden, "Exigences pour les hôtes Internet – couches de communication"STD 3, octobre 1989.

[RFC1123] R. Braden, éditeur, "Exigences pour les hôtes Internet – Application et prise en charge", STD 3, octobre 1989.

[RFC1700], J. Reynolds et J. Postel, "Numéros alloués"STD 2, octobre 1994. *(Historique)*

[RFC1812] F. Baker, "Exigences pour les routeurs IP version 4", juin 1995. *(Mise à jour par la RFC 2644)*

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

[RFC2101] B. Carpenter, J. Crowcroft, Y. Rekhter, "Comportement actuel des adresses IPv4", février 1997. *(Info.)*

[RFC2385] A. Heffernan, "Protection des sessions de BGP via l'option de signature MD5 de TCP", août 1998. *(P.S.) (Remplacée par* RFC5925)

[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*)*

[RFC2535] D. Eastlake, 3rd, "Extensions de sécurité du système des noms de domaines", mars 1999. (*Obsolète, voir* RFC4033, RFC4034, RFC4035) *(P.S.)*

Adresse des auteurs

Pyda Srisuresh
Lucent Technologies
4464 Willow Road
Pleasanton, CA 94588-8519
téléphone : (925) 737-2153
fax : (925) 737-2110
mél : srisuresh@lucent.com

Matt Holdrege
Lucent Technologies
1701 Harbor Bay Parkway
Alameda, CA 94502
téléphone : (510) 769-6001
mél : holdrege@lucent.com
Matt Holdrege

Déclaration de droits de reproduction

Remerciement

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