Groupe de travail Réseau
Request for Comments : 2993
Catégorie : Information

T. Hain, Microsoft
novembre 2000
Traduction Claude Brière de L'Isle

Implications architecturales des NAT

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.

Résumé
À la lumière de l'intérêt croissant, et du déploiement de la traduction d'adresse réseau (NAT, *network address translation*) de la [RFC1631], le présent mémoire expose certaines des implications architecturales et des lignes directrices pour les mises en œuvre. On suppose le lecteur familiarisé avec les concepts de traduction d'adresse présentés dans la [RFC1631].

Table des Matières

1. Introduction

Rédigée par K. Egevang et P. Francis et publiée en mai 1994, la [RFC1631] définit le NAT comme un moyen de faciliter le taux de croissance de l'utilisation des adresses IPv4. Mais les auteurs sont préoccupés par l'impact de cette technologie. Plusieurs passages du document soulignent le besoin d'une expérimentation pour voir quelles applications pourraient subir des effets négatifs des manipulations d'en-tête des NAT, avant même qu'il n'y ait une expérience significative de leur fonctionnement. Ceci est encore plus mis en évidence dans une citation de la conclusion : "Les NAT ont plusieurs caractéristiques néfastes qui les rendent inappropriés comme solution à long terme, et peuvent les rendre inappropriés même comme solution à court terme."

Maintenant, six années plus tard, et en dépit de la prédiction, l'usage des NAT s'est largement répandu dans l'Internet. Certains proclament que le NAT est la solution aussi bien à court qu'à long terme de certains des problèmes de disponibilité des adresses de l'Internet et remettent en question la nécessité de continuer le développement de IPv6. L'idée est parfois avancée que les NAT "fonctionnent" sans effets sérieux sauf sur quelques vieilles applications. En même temps, d'autres voient une myriade de difficultés causées par l'utilisation croissante du NAT.

Les arguments pour et contre prennent fréquemment une tonalité religieuse, chacun campant avec passion sur ses positions.

- Les défenseurs citent souvent avec enthousiasme les applications très populaires de messagerie et des services de la Toile comme exemples lumineux de la transparence des NAT. Ils soulignent aussi que le NAT est le dispositif qui casse finalement la surcharge sémantique de l'adresse IP à la fois comme localisateur et comme identifiant mondial de point d'extrémité (EID, *endpoint identifier*).
- Un point de vue opposé sur le NAT le dépeint comme une technologie maléfique, une mauvaise herbe qui est destinée à étouffer la poursuite du développement de l'Internet. Tout en reconnaissant qu'il y a des menaces de pénurie d'adresses, les opposants au NAT le voient comme au mieux d'un fonctionnement inadéquat, frisant l'imposture comme solution d'accès à l'Internet. La réalité se trouve quelque part entre ces points de vue extrêmes.

En tout cas, il est clair que le NAT affecte la transparence d'une connexité de bout en bout pour les transports qui s'appuient sur la cohérence de l'en-tête IP, et pour les protocoles qui portent ces informations d'adresse en des endroits autres que l'en-tête IP. En utilisant un assemblage de passerelles spécifiques d'application (ALG, *application specific gateway*) configuré de façon cohérente, les points d'extrémité peuvent contourner certains des défis opérationnels lancés par le NAT. Ces défis opérationnels varient sur la base d'un certain nombre de facteurs qui incluent les topologies du réseau et d'application et les applications spécifiques utilisées. Il peut être relativement facile de traiter le cas le plus simple, avec du trafic entre deux points d'extrémité sur un réseau intermédiaire sans appareils de NAT redondants en parallèle. Mais les choses peuvent devenir rapidement assez compliquées lorsque il y a des appareils de NAT redondants en parallèle, ou lorsque il y a plus d'applications réparties et multi-point comme un partage de document entre plusieurs parties. La complexité de la coordination des mises à jour nécessaire pour contourner le NAT subit une croissance géométrique selon le nombre de points d'extrémité. Dans un environnement large, cela peut exiger des efforts concertés pour mettre simultanément à jour tous les points d'extrémité d'une application ou service donné.

L'intention architecturale du NAT est de diviser l'Internet en administrations d'adresses indépendantes, (voir aussi "Domaines d'adresses", [RFC2663]) ce qui facilite particulièrement l'utilisation au cas par cas des allocations privées d'adresse [RFC1918]. Comme l'ont noté Carpenter et autres [RFC2101], une fois que des adresses d'utilisation privée ont été déployées dans le réseau, l'ambiguïté des adresses est garantie. Par exemple, lorsque des NAT simples sont insérés dans le réseau, le processus de résolution des noms en adresse et réciproquement se met à dépendre de l'endroit d'où la question a été posée. Le résultat de cette division est la mise en application d'une architecture client/serveur (opposée à d'homologue à homologue) où les serveurs doivent exister dans le domaine d'adresse public.

Un facteur significatif du succès de l'Internet est la souplesse qui découle de quelques principes de base. Le tout premier est le principe de bout en bout (exposé plus en détails ci-dessous) qui note que certaines fonctions ne peuvent être effectuées que dans les points d'extrémité, et qu'ils ont donc le contrôle de la communication, et que le réseau devrait être un simple service de datagrammes qui déplace les bits entre ces points. Reformulé, cela veut dire que les applications des points d'extrémité sont souvent le seul endroit capable de gérer correctement le flux de données. Retirer cette question aux appareils de transmission de paquet de couche inférieure rationnalise le processus de transmission, contribuant à l'efficacité globale du système.

Un autre avantage est que le réseau ne conserve pas les informations d'état par connexion. Cela permet un changement rapide d'acheminement en cas de défaillance par des chemins de remplacement et de meilleures capacité d'adaptation du réseau global. L'absence d'état retire aussi toute exigence que les nœuds du réseau se notifient les uns aux autres que les connexions de points d'extrémité sont formées ou abandonnées. De plus, les points d'extrémité ne sont pas, et n'ont pas besoin, d'être au courant des composants du réseau en dehors du ou des routeurs de destination, du premier bond, et d'un service de résolution de nom facultatif. L'intégrité des paquets est préservée à travers le réseau, et les sommes de contrôle de transport et toutes les fonctions de sécurité qui dépendent de l'adresse sont valides de bout en bout.

Les appareils de NAT (en particulier la variété NAPT) sapent la plupart des avantages basiques du modèle de bout en bout, réduisant la souplesse blobale, en augmentant souvent la complexité du fonctionnement et en diminuant les capacités de diagnostic. Des variantes des NAT telles que RSIP [RFC3103] ont récemment été proposées pour régler certains des problèmes du bout en bout. Bien que ces propositions puissent fournir efficacement une adresse publique au nœud privé (si des accès sont disponibles) elles n'éliminent pas plusieurs problèmes comme celui de la gestion d'état par le réseau, les contraintes de couche supérieure comme l'état TCP_TIME_WAIT, ou le partage des accès bien connus. Leurs variantes de multiplexage d'accès ont aussi les mêmes limitations à l'égard du DNS que NAPT, et chaque hôte doit subir des modifications significatives de sa pile de protocoles pour permettre cette technologie (voir ci-dessous).

On doit noter que les pare-feu cassent aussi le modèle de bout en bout et soulèvent plusieurs des mêmes problèmes que les appareils de NAT, tout en en rajoutant quelques autres. Mais un avantage opérationnel avec les pare-feu est qu'ils sont généralement installés dans les reseaux avec l'intention explicite d'interférer avec le flux de trafic, de sorte que les problèmes ont plus de chances d'être compris ou au moins examinés si des questions mystérieuses se présentent. Avec les appareils de NAT, les mêmes problèmes sont parfois méconnus car ces appareils sont fréquemment présentés comme transparents aux applications.

Face à cette situation, il devrait être clairement établi que les tentatives d'utilisation d'une variante de NAT comme simple remplacement de routeur peut créer plusieurs problèmes significatifs qui devraient être réglés avant le déploiement. Le but

du présent document est de les discuter afin d'augmenter la sensibilité du lecteur à ces problèmes.

2. Terminologie

Beaucoup des termes étant définis en détails dans la [RFC2663], le présent document n'en donne que des résumés.

NAT – La traduction d'adresse réseau dans sa forme simple est une méthode par laquelle les adresses IP sont transposées d'une administration d'adresse à une autre. La fonction de NAT ignore l'applications qui la traverse, car elle ne regarde que les en-têtes IP.

ALG – La passerelle de couche application est insérée entre les homologues d'application pour simuler une connexion directe lorsque un protocole ou apparel interposé empêche l'accès direct. Elle termine le protocole de transport et peut modifier le flux de données avant la transmission.

NAT/ALG – Combine les fonctions d'ALG avec celle de NAT simple. Généralement plus utile qu'un NAT pur, parce qu'il incoropre des composants pour des applications spécifiques qui ne fonctionneraient pas sur un NAT pur.

DNS/ALG – Cas particulier de NAT/ALG, où un ALG pour le service DNS interagit avec le composant NAT pour modifier le contenu d'une réponsse du DNS.

Pare-feu – Point de contrôle d'accès qui peut être un cas particulier d'une ALG, ou un filtre de paquets.

Mandataire – Service de relais conçu au sein d'un protocole, plutôt qu'inséré arbitrairement. À la différence d'une ALG, l'application sur au moins une des deux extrémités doit être consciente de la présence du mandataire.

NAT statique – Fournit une transposition biunivoque stable entre les espaces d'adresses.

NAT dynamique – Fournit une transposition dynamique entre des espaces d'adresses normalement utilisés avec un nombre relativement grand d'adresses d'un côté (espace privé) et peu d'adresses de l'autre (espace public).

NAPT – *(Network Address Port Translation)* La traduction d'accès d'adresse réseau accomplit la traduction en multiplexant les identifiants de niveau transport de plusieurs adresses provenant d'un côté, simultanément en identifiants de transport d'une seule adresse de l'autre côté. Voir le paragraphe 4.1.2 de la RFC2663. Cela permet que plusieurs points d'extrémité partagent, et apparaissent comme, une seule adresse IP.

RSIP – *(Realm Specific IP)* IP spécifique du domaine permet aux points d'extrémité d'acquérir et d'utiliser à la source l'adresse publique et le numéro d'accès. Cela comporte des mécanismes pour que le nœud privé demande en une fois plusieurs ressources. Les clients RSIP doivent connaître les frontières de l'administration d'adresses, dans quelle zone administrative spécifique réside son homologue pour chaque application, et la topologie pour atteindre l'homologue. Pour achever une connexion, le client du nœud privé demande une ou plusieurs adresses et/ou accès au serveur RSIP approprié, puis initie une connexion via ce serveur RSIP en utilisant les ressources publiques acquises. Les hôtes doivent être mis à jour avec le logiciel RSIP spécifique pour prendre en charge les fonctions de tunnelage.

VPN – *(Virtual Private Network)* Pour les besoins de ce document, un réseau privé virtuel traite techniquement une infrastructure IP comme un substrat de multiplexage, permettant aux points d'extrémité de construire des chemins de transit virtuels, sur lesquels fonctionne une autre instance d'IP. La seconde instance d'IP utilise fréquemment un jeu d'adresses IP différent.

AH – En-tête d'authentification IP de la [RFC2401], qui fournit l'intégrité des données, l'authentification de l'origine des données, et un service facultatif d'anti répétition

ESP – *(Encapsulating Security Payload)* Protocole d'encapsulation de charge utile de sécurité de la [RFC2401], il peut fournir la confidentialité des données (par chiffrement), et une confidentialité limitée du flux de trafic. Il peut aussi fournir l'intégrité des données, l'authentification de l'origine des données, et un service d'anti répétition.

Administration d'adresse – C'est la coordination d'un réservoir d'adresses allouées à une collection de routeurs et systèmes d'extrémité.

Domaine d'adressage – *(Addressing realm)* Collection de routeurs et de systèmes d'extrémité qio échangent la connaissance de localisations localement uniques. (Voir la définition complète dans la [RFC2663] sur la terminologie des NAT.) Le NAT est utilisé comme moyen pour répartir l'autorité d'allocation des adresses et fournir un mécanisme pour transposer les adresses d'une administration d'adresse dans celles d'une autre administration.

3. Domaine d'application

Quand on discute de l'impact architectural des NAT sur l'Internet, la première tâche est de définir la portée de l'Internet. La définition la plus basique est un enchaînement de réseaux construits en utilisant des technologies définies par l'IETF. Cette simple description ne fait pas de distinction entre le réseau public connu comme l'Internet, et les réseaux privés construits en utilisant les mêmes technologies (y compris ceux qui sont connectés via un NAT). Dans la [RFC1918], Rekhter et autres définissent les hôtes comme publics lorsque ils ont besoin de l'accès à la couche réseau en-dehors de l'entreprise, en utilisant une adresse mondialement non ambiguë. Ceux qui ont besoin d'un accès limité ou pas d'accès du tout sont définis comme privés. Une autre façon de voir cela est en termes de transparence de la connexion entre un nœud et le reste de l'Internet.

La résolution finale de la question public ou privé se trouve dans les intentions du réseau en question. Les réseaux qui n'ont généralement pas l'intention de faire partie du grand Internet vont utiliser des technologie d'écran pour insérer une barrière. Historiquement, les appareils pour établir une barrière entre les réseaux public et privé étaient connus sous le noms de "pare-feu" ou "passerelle d'application", et étaient conçus pour permettre le trafic approuvé tout en bloquant tout le reste. De plus en plus, une partie de la technologie écran est un NAT, qui gère le localisateur réseau entre les espaces d'adresse à usage public et privé, puis, en utilisant les ALG, ajoute la prise en charge des protocoles qui sont incompatibles avec le NAT. (L'utilisation de NAT au sein d'un réseau privé est possible, et n'est traitée ici que dans le contexte où certains composants du réseau privé sont utilisés comme service de transit commun entre les bouts de réseau rattachés au NAT.)

La [RFC1631] a limité la portée des discussions sur les NAT au rattachement des réseaux d'extrémité à un Internet public, c'est-à-dire de réseaux qui ont une seule connexion avec le reste de l'Internet. L'utilisation de NAT dans des situations dans lesquelles un réseau a plusieurs connexions au reste de l'Internet est significativement plus complexe que quand il y a seulement une connexion car les NAT doivent être coordonnés pour assurer la cohérence de la transposition des adresses entre les appareils individuels

4. Modèle de bout en bout

Le concept de modèle de bout en bout est revisité par Carpenter dans "Transparence de l'Internet" [RFC2775]. Un des points clés est que «l'état ne devrait être conservé que dans les points d'extrémité, de telle façon que l'état ne puisse être détruit que lorsque le point d'extrémité s'interrompt lui-même» ; c'est ce que l'on appelle le "sort partagé". Le but du sort partagé est d'assurer la robustesse. Avec la croissance de la taille des réseaux, la probabilité que la défaillances de composants affecte une connexion devient de plus en plus grande. Si des défaillances conduisent à la perte de la communication, parce que l'état clé est perdu, le réseau devient de plus en plus fragile, et son utilité se dégrade. Cependant, si un point d'extrémité est lui-même défaillant, il n'y a alors de toutes façons aucun espoir de communication. Le modèle de bout en bout avance donc qu'autant que possible, seuls les points d'extrémité devraient détenir l'état critique.

Pour les NAT, cet aspect du modèle de bout en bout se traduit par la transformation du NAT en élément critique de l'infrastructure : si il est défaillant, toute la communication à travers lui échoue, et sauf à consacrer grand soin à assurer une mémorisation stable et cohérente de son état, même lorsque il récupère, la communication qui passait à travers lui va encore échouer (parce que le NAT ne la traduit plus en utilisant la même transposition). Noter que ce dernier type de défaillance est plus sévère que la défaillance d'un routeur ; lorsque un routeur récupère, toute communication qu'il était précédemment en train de transmettre peut continuer avec succès à travers lui.

Il y a d'autres facettes importantes du modèle de bout en bout :

- lorsque l'état est détenu à l'intérieur du réseau, le trafic qui dépend de cet état ne peut pas être acheminé lorsque survient une défaillance si d'une façon ou d'une autre l'état n'est restitué aux points qui ont subi la défaillance, ce qui peut être très difficile à faire de façon cohérente, efficace et à temps.
- un principe clé de l'adaptation des réseaux aux grandes dimensions est de repousser la conservation d'état hors des limites du réseau. Si l'état est conservé par des éléments au cœur du réseau, lorsque le réseau croît, la quantité d'état que les éléments doivent conserver croît en conséquence. Les capacités des éléments peuvent devenir de sévères points de blocage et le nombre de connexions affectées par une défaillance croît également.
- si l'état de sécurité doit être conservé à l'intérieur du réseau (voir l'exposé qui suit) les modèles de confiance possibles que le réseau peut prendre en charge se restreignent.

Un réseau pour lequel les points d'extrémité n'ont pas besoin de faire confiance au service réseau apporte bien plus de souplesse dans la sécurité que ceux qui sont obligés de s'y fier. (Imaginons, par exemple, un voyageur de commerce qui se connecte depuis sa chambre d'hôtel à son bureau : peut-il faire confiance aux clés de sécurité des employés du service de télécommunications de l'hotel ?, ou aux employés du FAI qui fournit le service de télécommunications de l'hotel ? Qu'en est-il lorsque le voyageur se connecte à un réseau sans fil dans un aéroport ?)

En rapport avec cela, la [RFC2101] note :

Comme les en-têtes d'authentification de sécurité IP supposent que les adresses sont préservées de bout en bout dans le

réseau, on ne sait pas très bien comment on peut prendre en charge l'authentification fondée sur la sécurité IP entre une paire d'hôtes qui communiquent à travers une ALG ou un NAT.

De plus, il y a des applications réparties qui supposent que les adresses IP ont une portée mondiale, acheminable mondialement, et que tous les hôtes et applications ont la même vision de ces adresses. Bien sûr, une technique standard pour que de telles applications gèrent leurs connexions de contrôle et de données supplémentaires est qu'un hôte envoie à un autre l'adresse et l'accès auxquels le second hôte devrait se connecter. Les NAT font échec à ces applications. De même, il y a d'autres applications qui supposent que tous les accès de couche supérieure provenant d'une adresse IP donnée se transposent en le même point d'extrémité, et les technologies de multiplexage d'accès comme NAPT et RSIP rompent avec cela. Par exemple, un serveur de la Toile peut souhaiter associer une connexion à l'accès 80 avec une sur l'accès 443, mais suite à l'éventuelle présence d'un NATPT, la même adresse IP ne garantit plus le même hôte.

Limiter de telles applications n'est pas une mince affaire : une grande part du succès de l'Internet est dû aujourd'hui à la facilité avec laquelle de nouvelles applications peuvent fonctionner sur les points d'extrémité sans exiger d'abord la mise à jour des éléments d'infrastructure. Si de nouvelles applications doivent mettre à niveau les NAT afin de réaliser un large déploiement, cela entrave la rapidité du déploiement et le rythme de l'innovation en est ralenti.

5. Avantages des NAT

Un rapide regard à la popularité des NAT en tant que technologie montre qu'ils s'attaquent à plusieurs problèmes du monde réel lorsque ils sont utilisés à la frontière d'un domaine d'extrémité.

- En masquant les changements d'adresse qui ont lieu, provenant du fournisseur ou de l'accès numéroté, ils minimisent l'impact sur le réseau local en évitant la renumérotation.
- Les adresses à acheminement mondial peuvent être réutilisées pour les utilisateurs à accès intermittant. Cela pousse la demande d'adresses vers le nombre de nœuds actifs plutôt que vers le nombre total de nœuds.
- Il est possible que les NAT fournis et gérés par les FAI diminuent le fardeau de la prise en charge car ce peut être un appareil simple et cohérent dont la configuration est connue du côté utilisateur d'une interface d'accès.
- Casser l'Internet en une collection d'autorités d'adresses limite le besoin continuel de justification des allocations et permet aux gestionnaires de réseau d'éviter l'utilisation des techniques d'acheminement les plus sophistiqués tels que les sous-réseaux de longueur variable.
- Des changements chez les hôtes peuvent n'être pas nécessaires pour les applications qui ne s'appuient pas sur l'intégrité de l'en-tête de paquet, ou portent les adresses IP dans la charge utile.
- Comme les pare-feu de filtrage de paquets, NAPT et RSIP bloquent les connexions entrantes sur tous les accès jusqu'à ce qu'ils soient transposés administrativement.

Pris tous ensemble, cela explique certaines des fortes motivations du déploiement rapide des NAT. Le NAT traditionnel [RFC1631] procure une fonction relativement simple qui est comprise facilement.

Retirer les hôtes qui ne sont pas actuellement actifs diminue les demandes d'adresses à l'Internet public. Dans les cas où les fournisseurs finiraient autrement avec des allocations d'adresses qui ne pourraient pas être agrégées, cela améliore la charge qui pèse sur le système d'acheminement tout en prolongeant la durée de vie de l'espace d'adresses IPv4. Alors que la reprise des adresses inactives est un sous produit naturel de l'allocation dynamique existante, les appareils à accès par numérotation, dans le cas de connexions dédiées ce service pourrait être fourni à travers un NAT *(sic)*. Dans le cas d'un NAPT, le potentiel d'agrégation est encore supérieur car plusieurs systèmes terminaux partagent une seule adresse publique.

En réduisant les options de connexion potentielles du consomnateur et en minimisant la matrice de prise en charge, il serait possible que les NAT fournis par les FAI diminuent les coûts de prise en charge.

Une partie du motif des NAT est d'éviter le coût élevé du dénumérotage inhérent à l'Internet IPv4 actuel. Les lignes directrices pour l'allocation des adresses IPv4 [RFC2050] signifient que les clients d'un FAI sont actuellement obligés de changer leur numéro si ils veulent passer à un nouveau fournisseur d'accès. Utiliser un NAT (ou un pare-feu avec des fonctions de NAT) signifie que seules les adresses IP qui font face à Internet doivent être changées et les nœuds du réseau interne n'ont pas besoin d'être reconfigurés. Localiser l'administration des adresses au NAT minimise les coûts du dénumérotage, et fournit simultanément un bien plus grand réservoir d'adresses qu'il n'en est disponibles selon les lignes directrices d'allocation actuelles. (Les lignes directrices pour les registraires sont destinées à prolonger la durée de vie de l'espace d'adresses IPv4 et à gérer la croissance des tableaux d'acheminement jusqu'à ce que IPv6 soit prêt ou que de nouvelles technologie d'acheminement réduisent la pression sur les tableaux d'acheminement Cela est accomplis en gérant les allocations pour qu'elles correspondent à la demande réelle et à mettre en application l'adressage hiérarchique. Un sous produit malheureux des lignes directrices actuelles est qu'elles peuvent finir par entraver la croissance dans des zones où il est difficile de faire le tri entre besoin réel et thésaurisation potentielle.) Le NAT est efficace pour masquer le changement de fournisseur ou d'autres exigences pour changer les adresses, atténuant ainsi certains des problèmes posés par la croissance.

Les déploiements de NAT ont attiré l'attention des concepteurs de protocoles qui sont intéressés à s'assurer que leurs produits fonctionnent de bout en bout. Casser la surcharge sémantique de l'adresse IP force les applications à trouver un mécanisme plus approprié pour l'identification des points d'extrémité et décourager le transport du localisateur dans le flux des données. Comme cela ne va pas fonctionner pour les applications traditionnelles, la [RFC1631] discute de la façon de regarder à l'intérieur du paquet et de rendre la NAT transparent pour l'application (c'est-à-dire, de créer une passerelle d'application). Ce n'est pas possible pour toutes les applications (comme pour l'authentification fondée sur IP dans SNMP) et même avec des passerelles d'application sur le chemin, il peut être nécessaire de modifier chaque hôte d'extrémité pour qu'il sache quand il y a des intermédiaires qui modifient les données.

Une autre pratique populaire est de cacher une collection d'hôtes qui fournissent un service combiné derrière une seule adresse IP (c'est-à-dire, le partage de la charge d'hébergement de la Toile). Dans de nombreuses mises en œuvre c'est architecturalement un NAT, car les adresses sont transposées au vol en leur destination réelle. Lorsque l'intégrité de l'en-tête du paquet ne court pas de risque, ce type d'hôte virtuel n'exige pas de modification dans les applications distantes car le client final n'est pas au courant de l'activité de transposition. Alors que l'hôte virtuel a les caractéristiques de performance de CPU de l'ensemble total des machines, les capacités de traitement et d'entrée/sortie de l'appareil de NAT/ALG limitent les performances globales lorsque il avale les paquets dans les deux sens.

6. Problèmes des NAT

- Les NAT cassent le modèle souple de bout en bout de l'Internet.
- Les NAT créent un seul point de partage des sorts, dans l'appareil qui maintient l'état de connexion et les informations de transposition dynamique.
- Les NAT compliquent l'utilisation du multi-rattachement par un site afin d'augmenter la fiabilité de leur connexité Internet. (Alors que les routeurs seuls sont des points de partage de sort, le manque d'état dans un routeur rend triviale la création de redondances. Bien sûr, c'est une des raisons pour lesquelle la suite des protocoles Internet s'est développée en utilisant un service de datagrammes sans connexion pour sa couche réseau.)
- Les NAT inhibent la mise en œuvre de la sécurité au niveau IP.
- Les NAT permettent l'utilisation fortuite d'adresses privées. Ces adresses non coordonnées sont sujettes à des collisions lorsque fusionnent des compagnies qui utilisent ces adresses ou qu'elles veulent s'interconnecter directement en utilisant des VPN *(réseaux privés virtuels)*.
- Les NAT facilitent la concaténation des espaces de noms privés existants avec le DNS public.
- Les différentes versions d'accès (NAPT et RSIP) augmentent la complexité du fonctionnement lorsque des services ouverts au public résident sur le côté privé.
- Les NAT compliquent ou même rendent invalide le mécanisme d'authentification de SNMPv3.
- Des produits peuvent s'incorporer dans une fonction de NAT sans l'identifier comme telle.

Par sa conception, le NAT impose des limitations à la flexibilité. À ce titre, on invite à une réflexion approfondie sur les complications introduites. C'est particulièrement vrai pour les produits où la fonction de NAT est un service caché, comme les routeurs d'équilibrage de charge qui réécrivent l'adresse IP en d'autres adresses publiques. Comme les adresses peuvent être toutes dans l'espace administré publiquement, ils sont rarement reconnus comme des NAT, mais ils cassent l'intégrité du modèle de bout en bout de la même façon.

Les NAT font peser des contraintes sur le déploiement d'applications qui portent des adresses IP (ou des dérivés d'adresse) dans le flux des données, et ils fonctionnent avec l'hypothèse que chaque session est indépendante. Cependant, il y a des applications telles que FTP et 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. D'autres exemples sont les MIB de SNMP pour la configuration, et les messages de politique COPS. Les applications ou protocoles comme ceux-là supposent l'intégrité de bout en bout des adresses et vont échouer lors de la traversée d'un NAT. (TCP a été spécifiquement conçu pour tirer parti de, et réutiliser, l'adresse IP en combinaison avec son accès pour l'utiliser comme adresse de transport.) Pour réparer la façon dont les NAT cassent de telles applications, une passerelle de niveau application (ALG, *Application Level Gateway*) doit exister au sein ou à côté de chaque NAT. Un service de passerelle supplémentaire est nécessaire pour chaque application qui peut incorporer une adresse dans le flux de données. Le NAT peut aussi devoir assembler des datagrammes fragmentés pour permettre la traduction du flux d'application, puis ajuster les numéros de séquence TCP, avant de transmettre.

Comme noté plus haut, les NAT cassent le principe de base de l'Internet que les points d'extrémité sont aux commandes de la communication. Le concept original met le contrôle de l'état dans les points d'extrémité de façon qu'il n'y ait par nature pas d'autre point de défaillance. Déplacer l'état des points d'extrémité à des nœuds spécifiques dans le réseau réduit la souplesse, tout en augmentant l'impact d'un point de défaillance seul. Voir d'autres explications dans l'illustration 1 ci-dessous.

De plus, les NAT ne sont pas transparents pour toutes les applications, et la gestion de mises à jour simultanées sur un grand dispositif d'ALG peut excéder le coût d'acquisition d'adresses à acheminement mondial supplémentaires. Ceci est développé sous l'illustration 2 ci-dessous.

Bien que RSIP traite les questions de transparence et d'ALG, pour le cas spécifique d'un hôte individuel privé qui a besoin d'un accès public, il y a toujours un nœud qui a besoin d'un état pour conserver la connexion.

Le NAT dynamique et RSIP vont finalement violer les hypothèses de couches supérieures sur la réutilisation des numéros d'adresse/accès définies dans les [RFC0793], [RFC1323]. L'état TCP, TCP_TIME_WAIT, est spécifiquement conçu pour empêcher la répétition des paquets entre les quadruplets de IP et d'accès pour une paire d'adresses IP. Comme l'automate à états TCP d'un nœud ne connaît pas les utilisations antérieures de RSIP, sa tentative de connexion au même service distant que son voisin vient juste de libérer (qui est encore un TCP_TIME_WAIT) peut échouer, ou avec un plus gros numéro de séquence peut ouvrir la connexion précédente directement à partir de l'état TCP_TIME_WAIT, au prix de la perte de la protection offerte par l'état TCP_TIME_WAIT (exposé plus en détails au paragraphe 2.6 de la [RFC2663]).

Pour que les traducteurs d'adresses (qui ne traduisent pas les accès) se conforment aux exigences de TCP_TIME_WAIT, ils doivent s'interdire d'allouer la même adresse à un hôte différent tant qu'une période de 2*MSL ne s'est pas écoulée depuis la dernière utilisation de l'adresse, où (MSL, *Maximum Segment Lifetime*) est la durée de vie maximum de segment définie dans la [RFC0793] comme étant de deux minutes. Pour que les traducteurs d'adresse et d'accès se conforment à cette exigence, ils doivent de la même façon s'interdire d'allouer la même paire hôte/accès tant que 2*MSL ne se sont pas écoulées depuis la fin de sa première utilisation. Bien que ces exigences soient simples à formuler, elles peuvent poser de gros problèmes au NAT, parce qu'elles réduisent temporairement le réservoir d'adresses et d'accès disponibles. Par conséquent, il serait tentant pour les mises en œuvre de NAT d'ignorer ou de réduire les exigences de TCP_TIME_WAIT au prix d'un peu de la forte fiabilité de TCP. Noter que dans le cas où la forte fiabilité est en fait compromise par l'apparition d'un vieux paquet, la défaillance peut se manifester elle-même lorsque le receveur accepte des données incorrectes. Voir des explications complémentaires sous l'illustration 3 ci-dessous.

On avance parfois que les NAT fonctionnent simplement pour faciliter les “domaines d'acheminement”, où chaque domaine est chargé de trouver les adresses à l'intérieur des ses frontières. Un tel point de vue dissimule les limitations créées par le NAT avec un besoin mieux compris de la gestion de l'acheminement. La compartementalisation des informations d'acheminement est bien une fonction des protocoles d'acheminement et de leur portée d'application. Le NAT est simplement un moyen pour répartir l'autorité d'allocation des adresses et fournir un mécanisme pour transposer les adresses d'un domaine d'adresses dans un autre domaine.

En particulier, on croit parfois à tort que les NAT servent à fournir l'isolement de l'acheminement. En fait, si quelqu'un devait définir une ALG OSPF, il serait réellement possible d'acheminer à travers une frontière de NAT. Plutôt que ce soit le NAT qui trace la frontière, c'est l'opérateur expérimenté qui sait comment délimiter la topologie du réseau pour éviter la fuite des adresses à travers un NAT. C'est une nécessité opérationnelle étant donné le potentiel que les fuites d'adresses introduisent des incohérences dans l'infrastructure publique.

Un des plus gros souci à propos de l'explosion des NAT est l'impact sur les efforts touchants pour déployer la sécurité IP de bout en bout à la couche réseau. Une question fondamentale pour IPSec est qu'aussi bien avec AH que ESP, la vérification pour l'authentification couvre la somme de contrôle TCP/UDP (qui à son tour couvre l'adresse IP). Lorsque un NAT change l'adresse IP, le calcul de la somme de contrôle échoue, et il est donc garanti que l'authentification échoue. Tenter d'utiliser le NAT comme barrière de sécurité échoue lorsque l'exigence est le chiffrement de bout en bout à la couche réseau, car seuls les points d'extrémité ont accès aux clés. Voir des compléments sous l'illustration 4 ci-dessous.

Finalement, alors que les variantes de NAT à multiplexage d'accès (populaires parce qu'elles permettent l'accès Internet par une seule adresse) fonctionnent modestement bien pour connecter des hôtes privés à des services publics, elles créent des problèmes de gestion pour les applications qui se connectent à partir du public vers le privé. Le concept d'accès bien connu est sapé parce que seul un système avec une face privée peut être transposé à la fois à travers un seul numéro d'accès du côté public. Cela va affecter les réseaux d'entreprise, lorsque des applications comme les jeux Internet à plusieurs joueurs ne peuvent être joués que sur un système à la fois. Cela affectera aussi les petites entreprises lorsque un seul système peut fonctionner à la fois sur l'accès standard pour fournir les services de la Toile. Cela peut paraître des restrictions de peu d'importance pour le présent, mais comme il s'agit d'une propriété de base de l'Internet, qu'on ne va pas changer dans les années à venir, c'est très indésirable. La question est que l'usage public contre l'usage privé exige une transposition administrative pour chaque cible avant la connexion. Si le FAI choisit de fournir une version normalisée de cela pour réduire les options de configuration, on pourrait trouver que le coût de gestion des ALG va excéder le coût de l'espace d'adresse supplémentaire. Voir des compléments sous l'illustration 6 ci-dessous.

7. Illustrations

7.1 Point de défaillance unique

Une caractéristique des appareils à états pleins comme les NAT est la création d'un seul point de défaillance. Les tentatives d'éviter cela en établissant des NAT redondants créent un nouvel ensemble de problèmes qui se rapportent au moment de la communication de l'état, et aux défaillances relatives à l'acheminement. Cele englobe plusieurs questions telles que la fréquence de mise à jour, l'impact sur les performances de mises à jour fréquentes, la fiabilité de la transaction de mise à jour de l'état, la connaissance à priori de tous les nœuds qui ont besoin de ces informations d'état, et la notification des

solutions de remplacement aux nœuds d'extrémité. (Cette notification pourrait être accomplie avec un protocole d'acheminement qui pourrait demander des modifications aux hôtes pour qu'ils écoutent.)

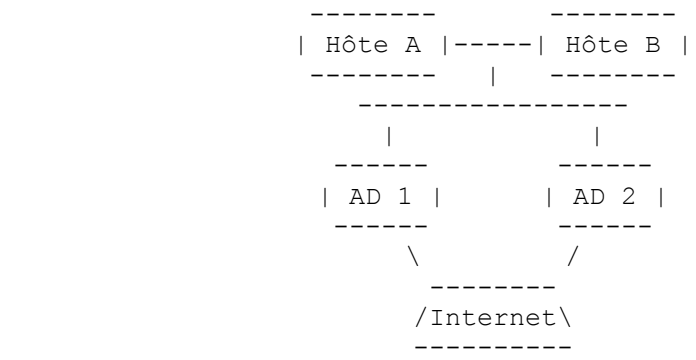

Illustration 1

Dans le cas traditionnel où les appareils d'accès (AD, *Access Device*) 1 & 2 sont des routeurs, le seul point de défaillance est l'hôte d'extrémité, et le seul effort nécessaire pour maintenir les connexions à travers une défaillance de routeur ou de liaison est une simple mise à jour d'acheminement de la part du routeur survivant. Dans le cas où les AD sont une variété de NAT, il y aura de l'état de connexion maintenu dans le chemin actif qui devra être partagé avec les NAT de remplacement. Lorsque les hôtes ont ouvert des connexions à travers l'un ou l'autre NAT, et qu'elles échouent, les connexions d'application vont tomber sauf si l'état a été préalablement passé au NAT survivant. Les hôtes vont encore avoir besoin d'acquérir une redirection d'acheminement. Dans le cas de RSIP, le réservoir d'adresses côté public va aussi avoir besoin d'être partagé entre les AD pour permettre le mouvement. Ce partage crée une autre complexité opérationnelle en temps réel pour empêcher des conflits d'allocation à l'établissement de la connexion. La technologie du NAT crée un point de partage de sort en dehors des points d'extrémité, en contradiction directe avec les buts de la conception originale de l'Internet.

7.2 ALG complexes

Dans l'exemple suivant d'un réseau d'entreprise supposé, chaque NAT/ALG serait un ou plusieurs appareils sur chaque localisation physique, et il y aurait plusieurs localisations physiques par connexion du diagramme. La simple logistique de la mise à jour des logiciels à cette échelle est très lourde, même quand tous les appareils sont du même modèle du même fabricant. Bien que ce puisse aussi être vrai avec les routeurs, il serait inutile que tous les appareils fonctionnent avec des versions compatibles pour qu'une application fonctionne à travers un chemin arbitraire.

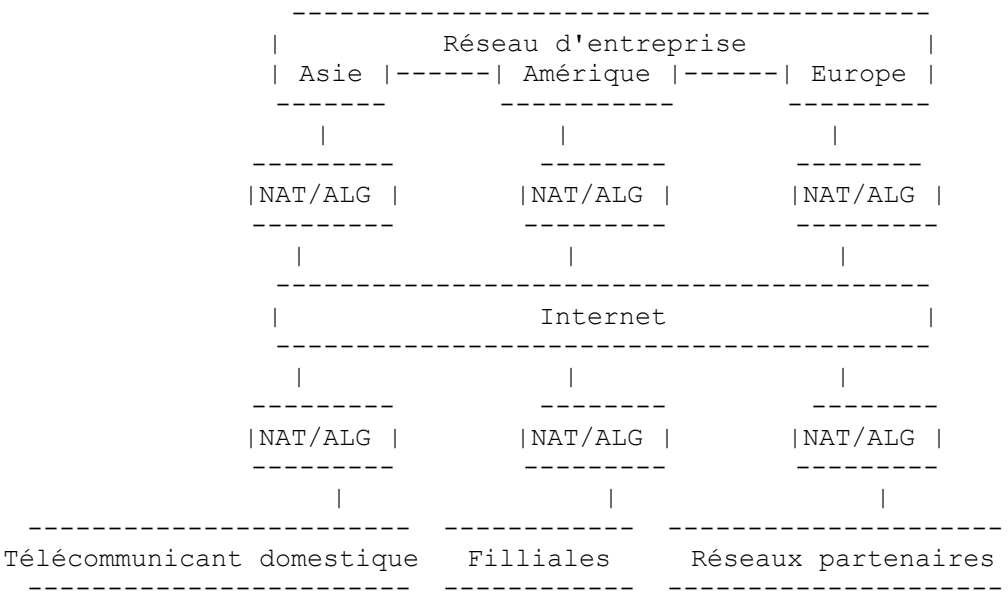

Illustration 2

7.3 Violations d'état TCP

La gamme complète des hypothèse architecturales de couche supérieure qui sont violées par les technologies de NAT peut n'être pas bien comprise sans un déploiement à très grande échelle, parce que cela exige parfois la diversité qui découle de l'utilisation à grande échelle pour decouvrir des modes de défaillances inhabituels. L'exemple suivant illustre une instance

du problème exposé à la section 6 ci-dessus.

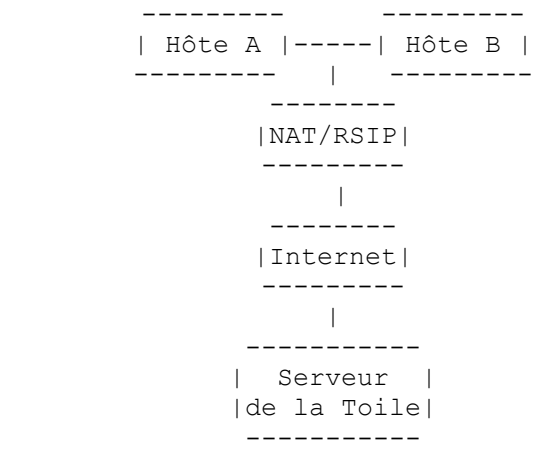

Illustration 3

L'hôte A achève sa transaction et ferme le service de la Toile sur l'accès TCP 80, et le RSIP libère l'adresse de côté public utilisée pour l'hôte A. L'hôte B tente d'ouvrir une connexion avec le même service de la Toile, et le NAT lui alloue alors la première adresse libre côté public qui est celle que A vient juste de libérer. Les règles de sélection d'accès de source de l'hôte B le conduisent au même choix que celui retenu par A. La demande de connexion de l'hôte B est rejetée parce que le serveur de la Toile, se conformant aux spécifications TCP, a ce quadruplet de TIME_WAIT pour 4 minutes. Le temps qu'un appel de l'hôte B parvienne jusqu'au bureau d'aide pour se plaindre de ne pas avoir d'accès, le nouvel essai va fonctionner, de sorte que le problème est marqué comme résolu, alors qu'en fait c'est un problème en cours, mais intermittent.

7.4 Gestion d'état symétrique

La gestion du fonctionnement de réseaux qui incorporent un appareil qui modifie les paquets à état plein est considérablement plus facile si les paquets entrants et sortants traversent le même chemin. (Autrement, c'est un casse-tête de conserver synchronisé l'état dans les deux directions.) Bien que facile à dire, même avec une planification attentive, cela peut être difficile à faire en utilisant un protocole sans connexion comme IP. Le problème de la création de connexions redondantes est de s'assurer que les chemins annoncés au côté privé atteignent les nœuds d'extrémité et se transposent en le même appareil que celui des annonces d'acheminement du côté public. Cet état doit persister pendant toute la durée de vie des sessions qui traversent le NAT, en dépit de brassages fréquents ou simultanés de topologie interne et externe. Examinons le cas suivant où les liaisons -X- sont interrompues, ou en train de rendre l'âme.

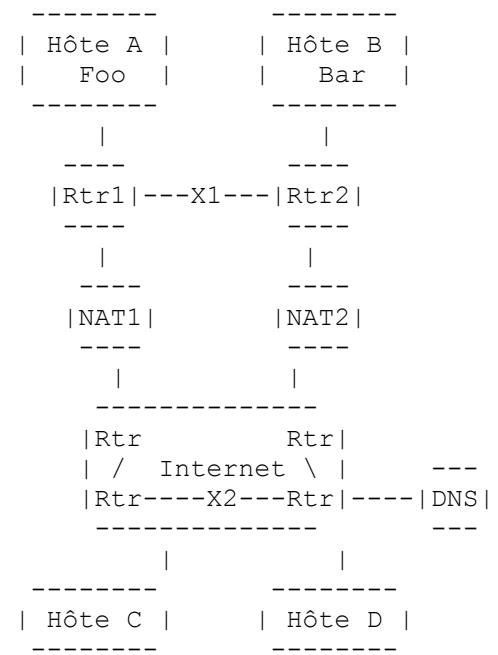

Illustration 4

Pour préserver la cohérence de l'acheminement, le meilleur chemin vers l'Internet pour les routeurs 1 & 2 est via le NAT1, tandis qu'on dit à l'Internet que le chemin pour le réservoir d'adresses géré par les NAT sera mieux trouvé par le NAT1. Lorsque le chemin X1 lache, le routeur 2 va essayer de passer à NAT2, mais le chemin de retour externe sera toujours par NAT1. C'est pour cela que l'apprareil NAT1 annonce la disponibilité d'un réservoir d'adresses. Les routeurs directement connectés dans la même situation annonceraient les chemins spécifiques qui existent après la perte. Dans ce cas, la redondance est sans objet.

Considérons le cas où le chemin entre les routeurs 1 & 2 est ouvert, et où une liaison X2 distante dans le réseau est défaillante. On suppose aussi que le DNS retourne des adresses pour les deux NAT lorsque on l'interroge sur les hôtes A ou B. Lorsque l'hôte D essaye de contacter l'hôte B, la demande passe par le NAT2, mais du fait de l'acheminement interne, la réponse passe par le NAT1. Comme les informations d'état pour cette connexion sont dans le NAT2, NAT1 va fournir une nouvelle transposition. Même si le chemin distant est restauré, la connexion ne sera pas faite parce que les demandes sont pour l'IP public de NAT2, alors que les réponses viennent de l'IP public de NAT1.

Dans un troisième cas, les hôtes A & B veulent tous deux contacter l'hôte D, lorsque lache la liaison distante X2 dans l'Internet. Tant que le chemin X1 est défaillant, l'hôte B est capable de se connecter, mais l'hôte A est coupé. Sans une compréhension précise de la topologie distante (ce qui est peu vraisemblable car les fournisseurs Internet tendent à considérer que ce sont des informations sensibles qui doivent rester confidentielles) l'administrateur des hôtes A & B ne va pas avoir d'indice sur la raison pour laquelle l'une fonctionne et l'autre pas. Tout ce qu'il peut dire est que les chemins redondants à travers les NAT sont ouverts mais qu'une seule connexion fonctionne. Encore une fois, ceci est dû au manque de visibilité de la topologie inhérent à une situation où un appareil à états pleins est annoncé comme disponible à un pôle plutôt que les réseaux connectés en réalité.

Dans toute topologie de réseau, les défaillances d'un routeur individuel ou d'une liaison peuvent poser des problèmes par une redondance insuffisante, mais les exigences de maintenance d'état du NAT constituent une charge supplémentaire qui n'est pas si facile à comprendre ou résoudre.

7.5 Besoin d'un FQDN unique au monde pour l'annonce des services au public

La caractéristique principae des NAT est la "simple" capacité à connecter des réseaux privés à l'Internet public. Lorsque le réseau privé existe avant d'installer le NAT, il est improbable et inutile que son résolveur de noms utilise un domaine enregistré. Comme on le note dans la [RFC1123] les interrogations du DNS peuvent être résolues via la diffusion groupée locale. Connecter l'appareil de NAT, et reconfigurer son résolveur en mandataire pour toutes les demandes externes permet l'accès au réseau public des hôtes du réseau privé. Configurer le DNS public pour l'ensemble des hôtes privés qui ont besoin de connexions entrantes exigerait un domaine enregistré (soit privé, soit derrière le FAI qui fait la connexion) et un nom univoque. À ce point, l'espace de nom partitionné est concaténé et les hôtes vont avoir des noms différents selon que l'interrogation est entrante ou sortante.

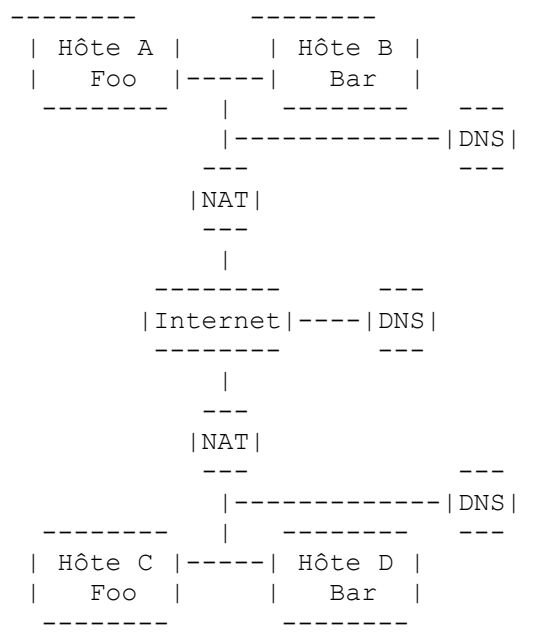

Illustration 5

Tout dans ce simple exemple va fonctionner jusqu'à ce qu'une application incorpore un nom. Par exemple, un service de la Toile fonctionnant sur l'hôte D pourrait présenter un URL incorporé de la forme http://D/bar.html, qui fonctionnerait à

partir de l'hôte C, mais plongerait sérieusement l'hôte A dans l'embarras. Si le nom incorporé se résout en l'adesse publique, l'hôte A serait heureux, mais l'hôte C va chercher une machine distante. Pour utiliser la résolution de FQDN public afin d'établir une connexion de l'hôte C à D, le NAT devrait chercher la destination plutôt que de simplement transmettre le paquet au routeur. (Le mode de fonctionnement normal pour un NAT est de traduire et transmettre à travers l'autre interface, alors que les routeurs ne renvoient pas les paquets sur la même interface que celle par laquelle ils sont entrés.) Le NAT n'a pas créé la fragmentation de l'espace de noms, mais il facilite les tentatives de fusion des réseaux qui ont des administrations de noms indépendantes.

7.6 Les tunnels L2TP augmentent la fréquence des collisions d'adresse

La croissance massive récente de l'Internet a été tirée par le soutien de la publication à faible coût via la Toile. La prochaine grosse poussée paraît être prise en charge par les réseaux virtuels privés (VPN, *Virtual Private Network*) fréquemment réalisés à l'aide de L2TP. Techniquement, les tunnels VPN traitent une infrastructure IP comme un substrat de multiplexage qui permet aux points d'extrémité de construire ce qui paraît être un chemin libre d'un bout à l'autre. Ces tunnels redéfinissent la visibilité du réseau et augmentent la probabilité de collision d'adresses lors de la traversée de plusieurs NAT. La gestion des adresses dans l'espace privé derrière les NAT va devenir une charge significative, car il n'y a pas d'organisme central capable de le faire, ou qui veuille le faire. La plus faible charge pour les FAI est en fait un transfert de la charge au niveau local, parce que l'administration des adresses et des noms devient à la fois répartie et plus compliquée.

Comme le note la [RFC1918], la fusion des espaces d'adresse privés peut causer un chevauchement de l'utilisation des adresses, créant un problème. Les tunnels L2TP vont augmenter la probabilité et la fréquence de cette fusion grâce à la simplicité de leur établissement. Il y a plusieurs configurations de chevauchement d'adresses qui vont causer des défaillances, mais dans le simple exemple qu'on donne ci-dessous, l'adresse d'usage privé de l'hôte B correspond à l'adresse d'usage privé du pôle de VPN utilisé par l'hôte A pour les connexions entrantes. Lorsque l'hôte B essaye d'établir l'interface du VPN, l'hôte A va lui allouer une adresse tirée de son réservoir pour les connexions entrantes, et identifier la passerelle à utiliser par l'hôte B. Dans l'exemple, l'hôte B ne sera pas capable de distinguer l'adresse de passerelle du VPN distant de l'hôte A de sa propre adresse privée sur l'interface physque, et donc la connexion va échouer. Comme les adresses à usage privé sont par définition non coordonnées publiquement, avec l'augmentation de la complexité du maillage de VPN augmente la probabilité que survienne une collision qui ne peut être résolue.

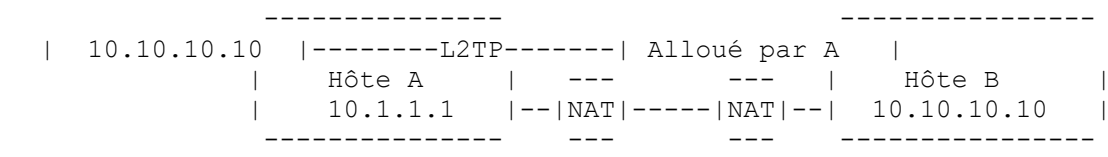

Illustration 6

7.7 Un système centralisé de collecte des données rapporte les corrélations

Il a été rapporté que les NAT introduisent des défis supplémentaires lorsque des systèmes de détection d'intrusion tentent de corréler des rapports entre des capteurs à l'intérieur et à l'extérieur du NAT. Bien que les détails des systèmes individuels sortent du domaine d'application du présent document, il est clair qu'un système centralisé avec des agents de surveillance de chaque côté du NAT va aussi avoir besoin d'un accès aux transpositions actuelles du NAT pour le faire bien. Il serait aussi critique que les données résultantes soient indexées correctement si il y avait des agents derrière plusieurs NAT qui utilisaient la même gamme d'adresses pour le côté privé.

Cela s'applique aussi aux données de gestion collectées via SNMP. Chaque fois que le flux de données porte une adresse IP ; le collecteur central ou l'ALG va avoir besoin de manipuler les données sur la base des transpositions actuelles dans le NAT.

8. IPv6

Il a été avancé que IPv6 n'est plus nécessaire parce que les NAT libèrent les contraintes de l'espace d'adresses et permettent à l'Internet de continuer sa croissance. La réalité est que cela souligne plus clairement que jamais la nécessité d'IPv6. Des gens essayent de connecter plusieurs machines à travers une seule ligne d'accès à leur FAI et voudraient abandonner certaines fonctionnalités pour obtenir cela au coût minimum.

Fréquemment, la raison de l'augmentation des coûts est la rareté perçue (donc une augmentation de valeur) des adresses IPv4, qui seraient éliminées par le déploiement d'IPv6. Cette mentalité de crise crée un marché pour une solution à un problème déjà résolu avec une plus grande souplesse par IPv6.

Si le NAT n'avait jamais été défini, la motivation pour résoudre le déclin de l'espace d'adresses IPv4 serait bien plus forte. Étant donné que les NAT permettent que de nouveaux hôtes non révélés se rattachent chaque jour à l'Internet, il est difficile

de vérifier l'impact réel sur la durée de vie d'IPv4, mais les NAT l'ont certainement rallongé. Il est aussi difficile de déterminer la mesure du retard que les NAT causent à IPv6, à la fois en relâchant la pression, et en redirigeant les cycles intellectuels loin de la solution à plus long terme.

Mais en même temps, la fonctionnalité de NAT peut être un facilitateur critique dans le déploiement d'IPv6. Il y a déjà 100 million ou plus d'ordinateurs qui fonctionnent avec IPv4 sur les réseaux de données. Certains de ces réseaux sont connectés et font donc partie de l'Internet, et certains sont sur des réseaux privés isolés. Il est inconcevable qu'on ait un "jour J" où on convertirait au même moment tous les nœuds IPv4 existants à IPv6. Il y aura une très longue période de coexistence pendant laquelle IPv4 et IPv6 seront tous deux utilisés dans l'Internet et dans les réseaux privés. Le plan de transition original d'IPv6 repose fortement sur l'existence de nouveaux nœuds IPv6 capables aussi de fonctionner avec IPv4 – une approche "double pile". Lorsque le nœud à double pile cherche un autre nœud dans le DNS, il va obtenir une adresse IPv4 ou IPv6 en réponse. Si la réponse est une adresse IPv4, le nœud utilisera alors IPv4 pour contacter l'autre nœud. Et si la réponse est une adresse IPv6, IPv6 peut alors être utilisé pour établir le contact. Transformer le NAT en un routeur "6 à 4" [RFC1752] permet un large déploiement d'IPv6 tout en fournissant un chemin IPv4 si IPv6 est indisponible. Alors que cela conserve l'ensemble actuel des questions pour les connexions IPv4, cela rétablit le principe de bout en bout pour les connexions IPv6.

Une méthodologie de remplacement serait de traduire les paquets entre IPv6 et IPv4 à la frontière entre les réseaux qui prennent en charge IPv4 et ceux qui prennent en charge IPv6. Le besoin de cette fonctionnalité a été reconnu dans la [RFC1752], le document qui recommandait à l'IETF que IPv6 soit développé et qui recommandait qu'un ensemble de groupes de travail soient établis pour travailler sur un certain nombre de problèmes spécifiques. La traduction des en-têtes (c'est-à-dire, le NAT) était un de ces problèmes.

Bien sûr, les NAT dans un environnement de traductian IPv6 en IPv4 rencontrent tous les mêmes problèmes que les NAT rencontrent dans un pur environnement IPv4 et les avertissements du présent document s'appliquent aux deux situations.

9. Considérations pour la sécurité

Le NAT (en particulier NAPT) peut en fait diminuer la sécurité globale parce qu'il crée l'illusion d'une barrière de sécurité, mais le fait sans les intentions de gestion d'un pare-feu. Les mécanismes de sécurité appropriés sont mis en œuvre dans l'hôte d'extrémité, sans fiabilité des hypothèses sur les supports d'acheminement, les filtres des pare-feu, ou les traductions de NAT manquantes, qui peuvent changer au fil du temps pour permettre un service avec un hôte du voisinage. En général, les barrières de sécurité définies supposent que toute menace est externe, ce qui conduit à des pratiques qui rendent les attaques internes beaucoup plus faciles.

IPsec [RFC2401] définit un ensemble de mécanismes pour prendre en charge l'authentification et le chiffrement au niveau du paquet pour les utiliser dans les réseaux IP. Cela peut être moins efficace que la sécurité de niveau application mais selon les termes de la [RFC1752] "la prise en charge de l'authentification de base de niveau paquet servira pour l'adoption d'une infrastructure de sécurité très nécessaire, largement répandue dans tout l'Internet."

Les NAT cassent les technologies IPsec d'authentification et de chiffrement parce que ces technologies dépendent de la cohérence de bout en bout des adresses IP dans les en-têtes IP, et donc ils peuvent arrêter la poursuite du déploiement de l'amélioration de la sécurité à travers l'Internet. Les NAT soulèvent un certain nombre de problèmes spécifiques par rapport à IPsec. Par exemple :

- l'utilisation de AH n'est pas possible via un NAT car le hachage protège l'adresse IP dans l'en-tête ;
- les certificats authentifiés peuvent contenir l'adresse IP au titre du nom du sujet à des fins d'authentification ;
- les structures en mode rapide chiffré *(Encrypted Quick Mode)* peuvent contenir des adresses et accès IP pour les vérifications de politique ;
- le mode révisé de chiffrement de clés publiques inclut l'identité de l'homologue dans la charge utile chiffrée.

Il serait possible de réaménager les NAT pour IPsec au cas par cas, mais au prix d'une restriction du modèle de confiance, comme on l'a exposé à la section 4 ci-dessus. Avec toutes les restrictions mises à la souplesse du déploiement, les NAT présentent un obstacle significatif à l'intégration de la sécurité dans l'Internet d'aujourd'hui.

Comme le note la [RFC2694], une ALG/DNS ne peut pas prendre en charge les serveurs de noms DNS sécurisés dans le domaine privé. Les transferts de zone entre les serveurs DNSsec seront rejetés quand des modifications nécessaires sont tentées. Il est aussi vrai que les ALG/DNS vont casser toutes les réponses signées modifiées. Ce sera le cas pour toutes les interrogations côté public des nœuds privés, lorsque le serveur DNS est sur le côté privé. Ce serait aussi vrai pour toute interrogation de côté privé pour des nœuds privés, lorsque le serveur DNS est du côté public. Les enregistrements à signature numérique pourraient être modifiés par l'ALG/DNS si elle avait accès à la clé d'authentification de source. DNSsec a été spécifiquement conçu pour éviter la distribution de cette clé, pour conserver l'authenticité de la source. De sorte que les NAT qui utilisent une ALG/DNS pour réparer les résolutions d'espace de noms vont soit casser la sécurité lorsqu'elle modifie l'enregistrement, soit exiger l'accès à toutes les clés de source pour les résolutions requises.

Les mécanismes de sécurité qui ne protègent pas ou s'appuient sur les adresses IP comme identifiants, comme TLS

[RFC2246], [SSL], ou SSH [RFC4251] peuvent fonctionner dans des environnements qui contiennent des NAT. Pour les applications qui peuvent établir et marquer l'utilisation de ce type de connexion de transport, les NAT ne créent aucune complication supplémentaire. Ces technologies peuvent ne pas apporter une protection suffisante pour toutes les applications car l'en-tête est exposé, ce qui permet des actions subversives comme les rétablissements de TCP. La [RFC2385] expose la question plus en détails.

Les arguments comme quoi les NAT peuvent fonctionner en mode sécurisé empêchent la vraie sécurité de bout en bout, car le NAT devient le point d'extrémité de sécurité. Du point de vue du fonctionnement, le NAT doit être géré au titre du domaine de la sécurité et dans ce mode, les paquets sur le côté non sûr du NAT sont en pleine exposition.

10. Lignes directrices de mise en œuvre

Étant donné le rythme rapide du déploiement des appareils de NAT, des lignes directrices seront utiles. La plupart sont par nature des avertissements qui sont conçus pour s'assurer que le lecteur comprend pleinement les implications de l'utilisation des NAT dans leur environnement.

- Déterminer le mécanisme pour la résolution des noms, et s'assurer que la réponse appropriée est donnée pour chaque administration d'adresse. Incorporer le serveur DNS, ou une ALG/DNS dans l'appareil de NAT devrait vraisemblablement être plus gérable que d'essayer de synchroniser des systèmes DNS indépendants à travers les administrations.
- Le NAT est t-il configuré pour des transpositions statiques biunivoques, ou va t-il les gérer de façon dynamique ? Dans ce dernier cas, s'assurer que le TTL des réponses du DNS est mis à 0, et que les clients prêtent attention à la notification "don’t cache" *(ne pas mettre en antémémoire)*.
- Y aura t-il un seul appareil de NAT, ou des appareils en parallèle avec des chemins multiples ? Si c'est un seul, considérer l'impact d'une défaillance de l'appareil. Si il y en a plusieurs, considérer comment l'acheminement va des deux côtés assurer que les paquets s'écoulent par la même boîte pendant toute la durée de vie de la connexion des applications.
- Examiner les applications qui vont avoir besoin de traverser le NAT et vérifier leur immunité aux changements d'adresse. Si nécessaire, fournir une ALG appropriée ou établir un VPN pour isoler l'application du NAT.
- Déterminer le besoin de connexions publiques plutôt que privées, la variabilité des destinations du côté privé, et le potentiel d'utilisation simultanée de numéros d'accès du côté public. Les NAPT augmentent les coûts d'administration si cela s'applique.
- Déterminer si les applications qui traversent le NAPT ou RSIP s'attendent à ce que tous les accès provenant de l'adresse IP publique soient sur le même point d'extrémité. Les contrôles administratifs pour empêcher des accès simultanés à partir de plusieurs hôtes privés seront nécessaires si c'est le cas.
- Si il y a des charges utiles chiffrées, les contenus ne peuvent pas être modifiés sauf si le NAT est un point d'extrémité de sécurité, agissant comme une passerelle entre les domaines de sécurité. Cela empêche la confidentialité de bout en bout, car le chemin entre le NAT et le point d'extrémité est exposé.
- Déterminer le chemin des résolutions de nom. Si les hôtes sur le côté privé d'un serveur NAPT ou RSIP ont besoin de visibilité mutuelle, un serveur DNS du côté privé peut être nécessaire.
- Si l'environnement utilise des enregistrements DNS sécurisés, l'ALG/DNS va requérir l'accès aux clés d'authentification de source pour tous les enregistrements à traduire.
- Lors de l'utilisation de VPN sur des NAT, identifier une "chambre de compensation" pour que les adresses du côté privé évitent les collisions.
- S'assurer que les applications utilisées aussi bien en interne qu'en externe évitent les noms incorporés, ou en utilisent qui sont uniques au monde.
- En utilisant RSIP, reconnaître que la portée est limitée au réseau privé individuel qui se connecte à l'Internet public. Si d'autres NAT sont dans le chemin (y compris des appareils d'équilibrage de la charge des serveurs de la Toile) le bénéfice de RSIP (utilisation d'une paire adresse/accès de bout en bout) est perdu.
- Pour RSIP, déterminer la probabilité de collisions de TCP_Time_Wait lorsque des hôtes ultérieurs du côté privé tentent de contacter un service récemment déconnecté du côté public.

11. Résumé

Durant la période de six années écoulée depuis la publication de la [RFC1631], la base expérimentale s'est accrue, faisant naître de nouvelles questions dans l'esprit des auteurs d'origine. Le NAT casse une hypothèse fondamentale de la conception de l'Internet : les points d'extrémité sont aux commandes. Un autre principe de la conception, "rester simple" se trouve mis à mal puisque de plus en plus de dispositifs sont ajoutés au réseau pour contourner les complications créées par les NAT. Finalement, la souplesse et la gérabilité globales sont amoindries et les coûts de prise en charge croissent pour faire face aux problèmes introduits.

Les évangélistes, pour et contre cette technologie, présentent leur cas comme justifié tout en n'écoutant aucune réfutation.

- Les NAT sont un "fait de la vie", et ils vont proliférer comme une amélioration de l'infrastructure IPv4 existante.
- Les NAT sont un "mal nécessaire" et créent une charge administrative dont il n'est pas facile de se débarasser. Plus significatif, ils inhibitent la mise en place de IPsec, ce qui à son tour ralentit la croissance d'applications qui exigent une infrastructure sécurisée.

Dans l'un et l'autre cas, les NAT requièrent de fortes déclarations d'applicabilité, établissant clairement ce qui fonctionne et ce qui ne fonctionne pas.

Voici un tableau des avantages et des inconvénients :

Avantages du NAT	**Inconvénients du NAT**
Masque les changements d'adresse globaux.	Casse le modèle de bout en bout.
Facilite le dénumérotage lors des changements de fournisseur.	Facilite la concaténation de plusieurs espaces de noms.
	Casse IPsec
	Points de défaillance à états pleins.
Les administrations d'adresses évitent les justifications aux registraires.	Exige une réponse DNS spécifique de la source ou DNS/ALG
	DNS/ALG casse les réponses DNSsec.
Diminue l'utilisation d'adresses.	Permet les conflits d'adresses de bout en bout
Diminue la charge qui pèse sur les FAI.	Augmente la charge et la complexité de la prise en charge locale
Transparent aux systèmes d'extrémité dans certains cas.	Développement unique pour chaque application.
Partage de charge comme hôte virtuel.	Limitation croissante des performances.
Besoin de délais pour le remplacement de IPv4.	Peut compliquer l'intégration de IPv6

Il y a eu de nombreuses discussions récemment sur l'intérêt de poursuivre le développement de IPv6 alors que le marché est largement en faveur du déploiement des NAT IPv4. Une vision à court terme manquerait le fait que tous deux ont un rôle, parce que les NAT visent des problèmes du monde réel d'aujourd'hui, alors que IPv6 est ciblé sur la solution de problèmes fondamentaux, tout autant que d'avancer. Il faut reconnaître qu'il y aura une longue coexistence avec les applications et services développés pour IPv6, alors que la durée de vie des systèmes IPv4 existants va probablement se mesurer en décades. Les NAT sont une diversion du mouvement vers l'avant, mais il permettent effectivement une plus large participation à l'état présent. Ils cassent aussi une classe d'applications, ce qui crée le besoin de scénarios de contournement complexes.

Les efforts pour améliorer la sécurité générale dans l'Internet incluent IPsec et DNSsec. Ces technologies fournissent une diversité de services à la fois pour authentifier et protéger les informations durant le transit. En cassant ces technologies, le NAT et l'ALG/DNS détournent, entravent le déploiement d'une amélioration de la sécurité dans tout l'Internet.

Il y a eu aussi de nombreuses questions sur la probabilité que des VPN soient établis qui peuvent soulever certaines des questions évoquées. Bien qu'il soit difficile de prédire l'avenir, une façon d'éviter des ALG pour chaque application est d'établir un L2TP sur les NAT. Cela restreint la visibilité du NAT aux en-têtes des paquets tunnelés, et supprime ses effets dans toutes les applications. Bien que cela résolve la question de l'ALG, cela soulève le problème de la probabilité de collisions d'adresses lorsque des connexions arbitraires sont établies entre des espaces d'adresses non coordonnés. Cela crée aussi un problème collatéral sur la façon dont une application établit le nécessaire tunnel.

L'architecture IP d'origine est puissante parce qu'elle fournit un mécanisme général sur lequel peuvent construire les autres choses (non encore imaginées). Bien qu'il soit possible de construire un château de cartes, le temps et l'expérience ont conduit à construire des normes avec plus d'intégrité structurelle. IPv6 est la solution à long terme qui revient au principe de la transparence de bout en bout. Le NAT est une déviation technologique pour prolonger la durée de vie de IPv4.

12. Références

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

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

[RFC1185] V. Jacobson, R. Braden et L. Zhang, "Extension TCP pour chemins à grande vitesse", octobre 1990.

[RFC1631] K. Egevang, P. Francis, "Le traducteur d'adresse réseau (NAT) IP", juin 1994. *(Info., remplacé par 3022)*

[RFC1752] S. Bradner, A. Mankin, "Recommandation pour le protocole IP de prochaine génération", janvier 1995. *(P.S.)*

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

[RFC2026] S. Bradner, "Le processus de normalisation de l'Internet—Révision 3", (BCP0009) octobre 1996. *(Remplace* RFC1602, RFC1871) (*MàJ par* RFC3667, RFC3668, RFC3932, RFC3979, RFC3978, RFC5378)

[RFC2050] K. Hubbard, M. Kosters, D. Conrad, D. Karrenberg, J. Postel, "Lignes directrices pour l'allocation des adresses IP par les registraires Internet", novembre 1996. *(Remplace* RFC1466) (BCP0012)

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

[RFC2246] T. Dierks et C. Allen, "Protocole TLS version 1.0", janvier 1999.

[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)

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

[RFC2694] P. Srisuresh, G. Tsirtsis, P. Akkiraju, A. Heffernan, "Extensions du DNS aux traducteurs d'adresse réseau (DNS_ALG)", septembre 1999. *(Information)*

[RFC2775] B. Carpenter, "Transparence de l'Internet", février 2000. *(Information)*

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

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

[RFC4251] T. Ylonen et C. Lonvick, "Architecture du protocole Secure Shell (SSH)", janvier 2006.. *(P.S.)*

[SSL] http://home.netscape.com/eng/ssl3/ssl-toc.html, mars 1996.

13. Remerciements

Des contributions précieuses au présent document sont venues de l'IAB, de Vern Paxson (lbl), Scott Bradner (harvard), Keith Moore (utk), Thomas Narten (ibm), Yakov Rekhter (cisco), Pyda Srisuresh, Matt Holdrege (lucent), et de Eliot Lear (cisco).

14 Adresse de l'auteur

Tony Hain
Microsoft
One Microsoft Way
Redmond, Wa. USA
téléphone : 1-425-703-6619
mél : tonyhain@microsoft.com

Déclaration de droits de reproduction

Remerciement

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