Groupe de travail Réseau
Request for Comments : 4787
BCP : 127
Catégorie : Bonnes pratiques actuelles

F. Audet, éd., Nortel Networks
C. Jennings, Cisco Systems
janvier 2007
Traduction Claude Brière de L'Isle

Exigences de comportement des traducteurs d'adresse réseau (NAT) pour UDP en envoi individuel

Résumé
Le présent document définit la terminologie de base pour décrire différents types de comportements de traduction d'adresse réseau (NAT, *Network Address Translation*) lors du traitement de UDP en envoi individuel et définit aussi un ensemble d'exigences qui permettront à de nombreuses applications, comme les communications multimédia ou les jeux en ligne, de fonctionner de façon cohérente. Développer des NAT qui satisfont cet ensemble d'exigences va augmenter considérablement la probabilité que ces applications fonctionnent correctement.

Table des matières

1. Déclaration d'applicabilité

L'objet de la présente spécification est de définir un ensemble d'exigences pour les NAT qui devraient permettre à de nombreuses applications, comme les communications multimédia ou les jeux en ligne, de fonctionner de façon cohérente. Développer des NAT qui satisfont cet ensemble d'exigences va augmenter considérablement la probabilité que ces applications fonctionnent correctement.

Les exigences de cette spécification s'appliquent aux NAT traditionnels comme décrits dans la [RFC2663].

Le présent document est destiné à couvrir les NAT de toute taille, du petit NAT résidentiel aux grands NAT d'entreprise. Cependant, il devrait être compris que les NAT d'entreprise fournissent normalement beaucoup plus que juste les capacités de NAT ; par exemple, ils fournissent normalement des fonctions de pare-feu. Une description complète des comportements de pare-feu et des exigences associées est spécifiquement hors du domaine d'application de la présente spécification. Cependant, cette spécification couvre bien les aspects de pare-feu de base présents dans les NAT (voir la Section 5).

Les approches qui utilisent la signalisation directe du contrôle de boîtiers de médiation sont hors du domaine d'application du présent document.

Les relais UDP (par exemple, la traversée de NAT en utilisant un relais [RFC5766]) sont hors du domaine d'application du présent document.

Les aspects d'application sont hors du domaine d'application du présent document, car on se concentre ici strictement sur le NAT lui-même.

Le présent document couvre seulement les aspects de traversée de NAT relatifs à UDP en envoi individuel [RFC0768] sur IP [RFC0791] et leur dépendance aux autres protocoles.

2. Introduction

Les traducteurs d'adresse réseau (NAT, *Network Address Translator*) sont bien connus pour causer des problèmes très significatifs aux applications qui portent des adresses IP dans la charge utile (voir la [RFC3027]). Les applications qui souffrent de ce problème incluent la voix sur IP et le multimédia sur IP (par exemple, SIP [RFC3261] et [H.323]) ainsi que le jeu en ligne.

De nombreuses techniques sont utilisées pour tenter de faire fonctionner les applications multimédia en temps réel, les jeux en ligne, et autres applications à travers les NAT. Les passerelles de niveau application [RFC2663] sont un de des mécanismes. STUN [RFC5389] décrit un mécanisme d'auto réparation d'adresse unilatéral (UNSAF, *UNilateral Self-Address Fixing*) [RFC3424]. Teredo [RFC4380] décrit un mécanisme UNSAF consistant à tunneler IPv6 [RFC2460] sur UDP/IPv4. Les relais UDP ont aussi été utilisés pour permettre des applications à travers les NAT, mais ils sont généralement vus comme une solution de dernier ressort. L'établissement de connexité interactive (ICE, *Interactive Connectivity Establishment)* [RFC5245] décrit une méthodologie pour utiliser beaucoup de ces techniques et éviter un relais UDP, sauf si le type de NAT est tel qu'il force l'utilisation d'un tel relais UDP. La présente spécification définit les exigences pour améliorer les NAT. Satisfaire à ces exigences assure que les applications ne seront pas forcées d'utiliser un relais UDP.

Comme il est montré dans UNSAF [RFC3424], "D'après l'observation des réseaux déployés, il est clair que les différentes boîtes de NAT mises en œuvre varient largement en termes de façon de traiter les différents cas de trafic et d'adressage". Ce grand degré de variabilité est un facteur de la fragilité globale introduite par les NAT et cela rend extrêmement difficile de prédire comment un certain protocole va se comporter sur un réseau qui traverse un NAT. Des discussions avec de nombreux fabricants majeurs de NAT ont clairement montré qu'ils préféreraient déployer des NAT déterministes qui causent le moins de dommages aux applications tout en satisfaisant aux exigences qui ont amené en premier lieu leurs consommateurs à déployer des NAT. Le problème auquel les fabricants de NAT font face est qu'ils ne sont pas sûrs de la façon de le faire ou de comment documenter le comportement de leurs NAT.

Le but du présent document est de définir un ensemble de terminologie commune pour décrire le comportement des NAT et de produire un ensemble d'exigences sur un ensemble spécifique de comportements pour les NAT.

Le présent document formule un ensemble commun d'exigences simples et utiles pour la voix, la vidéo, et les jeux, qui peuvent être mises en œuvre par les fabricants de NAT. Le présent document va simplifier l'analyse des protocoles pour décider si ils travaillent ou non dans cet environnement et va permettre aux fournisseurs de services qui ont des problèmes de traversée de NAT de faire des déclarations sur où leurs applications vont fonctionner et où elles ne vont pas fonctionner, ainsi que de spécifier leurs propres exigences de NAT.

3. Terminologie

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

Le lecteur est invité à se reporter à la [RFC2663] pour la taxonomie et la terminologie de NAT. Le NAT traditionnel est le plus courant type d'appareil de NAT déployé. Le lecteur peut se reporter à la [RFC3022] pour des informations détaillées sur le NAT traditionnel. Le NAT traditionnel a deux variétés principales – le NAT de base et le traducteur d'adresse/accès réseau (NAPT, *Network Address/Port Translator*).

NAPT est de loin l'appareil de NAT le plus couramment déployé. NAPT permet à plusieurs hôtes internes de partager simultanément une seule adresse IP publique. Quand un hôte interne ouvre une session TCP ou UDP sortante à travers un NAPT, le NAPT alloue à la session une adresse IP publique et un numéro d'accès, de sorte que les paquets de réponse suivants provenant du point d'extrémité externe peuvent être reçus par le NAPT, traduits, et transmis à l'hôte interne. L'effet est que le NAPT établit une session de NAT pour traduire le couple (adresse IP privée, numéro d'accès privé) en un couple (adresse IP publique, numéro d'accès public) et vice versa, pour la durée de la session. Un problème de pertinence pour les applications d'homologue à homologue est comment le NAT se comporte quand un hôte interne initie plusieurs sessions simultanées à partir d'un seul point d'extrémité (IP privé, accès privé) avec plusieurs points d'extrémité distincts sur le réseau externe. Dans cette spécification, le terme de "NAT" se réfère aussi bien au "NAT de base" qu'au "traducteur d'adresse/accès réseau (NAPT)".

Le présent document utilise le terme "session" comme défini dans la RFC 2663 : "Les sessions TCP/ UDP sont identifiées de façon univoque par le tuple (adresse IP de source, accès TCP/UDP de source, adresse IP de cible, accès TCP/UDP de cible)".

Le présent document utilise le terme "transposition d'adresse et d'accès" comme la traduction entre une adresse et accès externes et une adresse et accès internes. Noter que ce n'est pas la même chose qu'une "ligne d'adresse" comme défini dans la RFC 2663.

Le présent document utilise la terminologie de l'IANA pour les gammes d'accès, c'est-à-dire que "accès bien connu" est de 0 à 1023, "enregistré" est de 1024 à 49151, et "dynamique et/ou privé" est de 49152 à 65535, comme défini dans http://www.iana.org/assignments/port-numbers.

STUN [RFC3489] utilisait les termes "cône complet", "cône restreint", "cône à accès restreint", et "symétrique" pour se référer aux différentes variantes de NAT applicables seulement à UDP. Malheureusement, cette terminologie a été la source d'une grande confusion car elle s'est révélée inadéquate pour décrire la réalité du comportement de NAT. La présente spécification se réfère donc aux comportements spécifiques des NAT individuels au lieu d'utiliser la terminologie cône/symétrique.

4. Comportement de traduction d'adresse et d'accès réseau

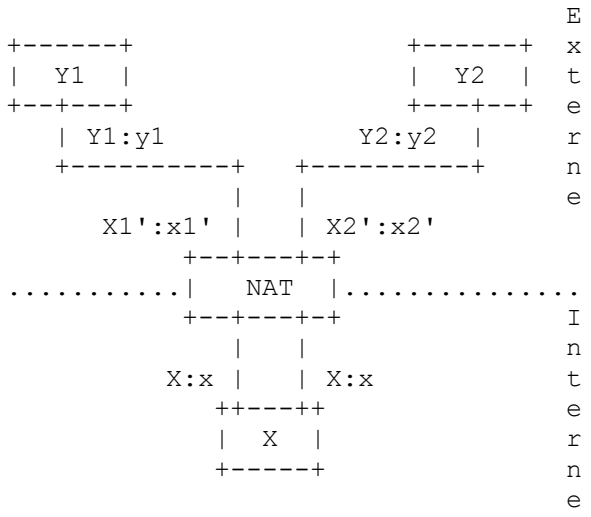
Cette Section décrit les divers comportements de NAT applicables aux NAT.

4.1 Transposition d'adresse et d'accès

Quand un point d'extrémité interne ouvre une session sortante à travers un NAT, le NAT alloue à la session une adresse IP et un numéro d'accès externes afin que les paquets de réponse suivants provenant du point d'extrémité externe puissent être reçus par le NAT, traduits, et transmis au point d'extrémité interne. C'est une transposition entre un couple adresse et accès IP internes et un couple adresse et accès IP externes. Elle établit la traduction qui va être effectuée par le NAT pour la durée de la session. Pour de nombreuses applications, il est important de distinguer le comportement du NAT quand il y a plusieurs sessions simultanées établies avec des points d'extrémité externes différents.

Le comportement clé à décrire est le critère de réutilisation d'une transposition pour de nouvelles sessions avec des points d'extrémité externes, après l'établissement d'une première transposition entre une adresse et accès internes X:x et un couple d'adresse externe Y1:y1. Supposons que l'adresse et accès IP internes X:x soient transposés en X1':x1' pour cette première session. Le point d'extrémité envoie alors à partir de X:x à une adresse externe Y2:y2 et obtient une transposition de

X2':x2' sur le NAT. La relation entre X1':x1' et X2':x2' pour les diverses combinaisons de relations entre Y1:y1 et Y2:y2 est critique pour décrire le comportement de NAT. Cet arrangement est illustré dans le diagramme suivant :



Transposition d'adresse et d'accès

Les comportements de transposition d'adresse et d'accès suivants sont définis :

Transposition indépendante du point d'extrémité : le NAT réutilise la transposition d'accès pour les paquets suivants envoyés des mêmes adresses et accès IP internes (X:x) à toutes adresses et accès IP externes. Spécifiquement, X1':x1' égale X2':x2' pour toutes les valeurs de Y2:y2.

Transposition dépendante de l'adresse : le NAT réutilise la transposition d'accès pour les paquets suivants envoyés des mêmes adresses et accès IP internes (X:x) à la même adresse IP externe, sans considération de l'accès externe. Spécifiquement, X1':x1' égale X2':x2' si et seulement si Y2 égale Y1.

Transposition dépendante de l'adresse et de l'accès : le NAT réutilise la transposition d'accès pour les paquets suivants envoyés des mêmes adresses et accès IP internes (X:x) à la même adresse et accès IP externes pendant que la transposition est encore active. Spécifiquement, X1':x1' égale X2':x2' si et seulement si Y2:y2 égale Y1:y1.

Il est important de noter que ces trois possibilités ne font pas de différence entre les propriétés de sécurité du NAT. Les propriétés de sécurité sont entièrement déterminées par les paquets que le NAT permet ou non en entrée. Ceci est déterminé par le comportement de filtrage dans les portions de filtrage du NAT.

REQ-1 : un NAT DOIT avoir un comportement de "transposition indépendante du point d'extrémité".

Justification : pour que fonctionnent les méthodes UNSAF, la recommandation 1 doit être satisfaite. Le non respect de la REQ-1 va forcer l'utilisation d'un relais UDP, ce qui est très souvent impraticable.

Certains NAT sont capables d'allouer des adresses IP à partir d'un réservoir d'adresses IP sur le côté externe du NAT, par opposition à juste une seule adresse IP. Ceci est particulièrement courant avec les plus grands NAT. Certains NAT utilisent la transposition d'adresse IP externe d'une façon arbitraire (c'est-à-dire, au hasard) : une adresse IP interne pourrait avoir plusieurs transpositions d'adresse IP externe actives au même moment pour différentes sessions. Ces NAT ont un comportement de "réservoir d'adresses IP" de "arbitraire". Certains NAT de grandes entreprises utilisent un comportement de réservoir d'adresses IP de "arbitraire" comme moyen de cacher l'adresse IP allouée à des points d'extrémité spécifiques en rendant leur allocation moins prévisible. D'autres NAT utilisent la même transposition d'adresse IP externe pour toutes les sessions associées à la même adresse IP interne. Ces NAT ont un comportement de "réservoir d'adresse IP" de "apparié". Les NAT qui utilisent le comportement de "réservoir d'adresses IP" de "arbitraire" peuvent causer des problèmes aux applications qui utilisent plusieurs accès à partir du même point d'extrémité, mais qui ne négocient pas les adresses IP individuellement (par exemple, certaines applications qui utilisent RTP et RTCP).

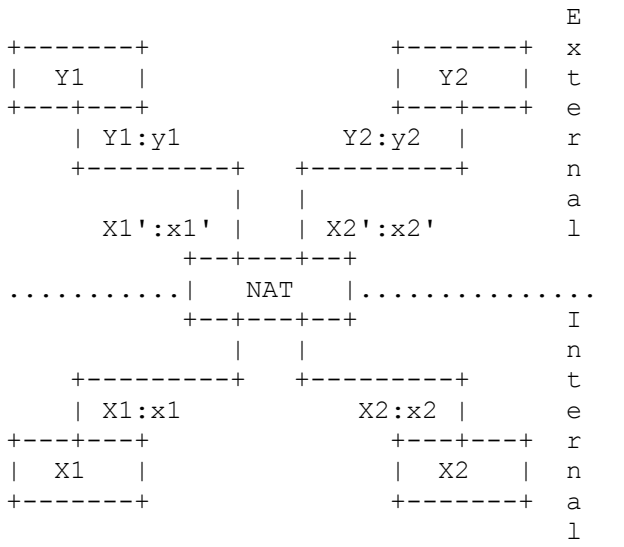
REQ-2 : il est RECOMMANDÉ qu'un NAT ait un comportement de "réservoir d'adresses IP" de "apparié". Noter que cette exigence n'est pas applicable aux NAT qui ne prennent pas en charge le réservoir d'adresses IP.

Justification : cela va permettre aux applications qui utilisent plusieurs accès originaires de la même adresse IP interne d'avoir aussi la même adresse IP externe. C'est pour éviter de casser les applications d'homologue à homologue qui ne sont pas capables de négocier l'adresse IP pour RTP et l'adresse IP pour RTCP séparément. À ce titre, il est envisagé que cette exigence devienne moins importante lorsque les applications deviennent plus amicales à l'égard des NAT au fil du temps. La principale raison de cette exigence est que dans une application d'homologue à homologue, on est soumis aux fautes de l'autre homologue. En particulier, dans le contexte de SIP, si une application prend en charge les extensions définies dans la [RFC3605] pour indiquer séparément les adresses et accès RTP et RTCP, mais pas l'autre homologue, il peut encore y avoir des cassures sous la forme d'un flux qui perd des paquets RTCP. Cette exigence va éviter la perte de RTP dans ce contexte, bien que la perte de RTCP puisse être inévitable dans cet exemple particulier. On notera aussi que la RFC 3605 n'est malheureusement pas une partie obligatoire de SIP [RFC3261]. Donc, cette exigence va concerner un problème particulièrement gênant qui va durer encore longtemps.

4.2 Allocation d'accès

4.2.1 Comportement d'allocation d'accès

Ce paragraphe se réfère au diagramme suivant.



Allocation d'accès

Certains NAT tentent de préserver le numéro d'accès utilisé en interne quand ils allouent une transposition à une adresse et un accès IP externes (par exemple, x1=x1', x2=x2'). Ce comportement d'allocation d'accès est appelé "préservation d'accès". En cas de collision d'accès, ces NAT tentent diverses techniques pour y remédier. Par exemple, certains NAT vont outrepasser la précédente transposition pour conserver le même accès. D'autres NAT vont allouer une adresse IP différente à partir d'un réservoir d'adresses IP externes ; ceci n'est possible que tant que le NAT a assez d'adresses IP externes ; si l'accès est déjà utilisé sur toutes les adresses IP externes disponibles, ces NAT vont alors prendre un accès différent (c'est-à-dire, il ne font plus la préservation d'accès).

Certains NAT utilisent la "surcharge d'accès", c'est-à-dire, ils utilisent toujours la préservation d'accès même dans le cas de collision (c'est-à-dire, X1'=X2' et x1=x2=x1'=x2'). La plupart des applications vont échouer si le NAT utilise la "surcharge d'accès".

On se réfère à un NAT qui ne tente dans aucun cas de faire correspondre les numéros d'accès externes avec les numéros d'accès internes comme ne faisant "pas de préservation d'accès".

Quand des NAT allouent un nouvel accès de source, il y a la question de quelle gamme d'accès définie par l'IANA choisir. Les gammes sont "bien connu" de 0 à 1023, "enregistré" de 1024 à 49151, et "dynamique/privée" de 49152 à 65535. Pour la plupart des protocoles, ce sont des accès de destination et non des accès de source, de sorte que la transposition d'un

accès de source à un accès de source qui est déjà enregistre a peu de chances d'avoir de mauvais effets. Certains NAT peuvent choisir d'utiliser seulement l'accès dans la gamme dynamique ; le seul inconvénient de cette pratique est qu'elle limite le nombre d'accès disponibles. D'autres appareils de NAT peuvent tout utiliser sauf la gamme bien connue et peuvent préférer utiliser d'abord la gamme dynamique, ou éventuellement éviter l'accès enregistré réel dans la gamme enregistrée. D'autres NAT préservent la gamme d'accès si elle est dans la gamme bien connue. La [RFC0768] spécifie que l'accès de source est réglé à zéro si aucun paquet de réponse n'est attendu. Dans ce cas, il importe peu à quoi le NAT transpose, car l'accès de source ne va pas être utilisé. Cependant, de nombreuses API d'OS courants ne permettent pas à un utilisateur d'envoyer à partir d'un accès zéro ; les applications n'utilisent pas l'accès zéro, et le comportement de divers NAT existants à l'égard d'un paquet dont l'accès de source est zéro est inconnu. Le présent document ne spécifie aucun comportement normatif pour un NAT quand il traite un paquet avec un accès de source de zéro, ce qui signifie que les applications ne peuvent pas compter sur un comportement déterministe pour ces paquets.

REQ-3 : un NAT NE DOIT PAS avoir un comportement "d'allocation d'accès" de "surcharge d'accès".

a) Si l'accès de source de l'hôte était dans la gamme de 0 à 1023, il est RECOMMANDÉ que l'accès de source du NAT soit dans la même gamme. Si l'accès de source de l'hôte était dans la gamme de 1024 à 65535, il est RECOMMANDÉ que l'accès de source du NAT soit dans cette gamme.

Justification : cette exigence doit être satisfaite afin de permettre que deux applications sur le côté interne du NAT utilisent toutes deux le même accès pour essayer de communiquer avec la même destination. Les NAT qui mettent en œuvre la préservation d'accès ont à traiter des conflits sur l'accès, et les chemins multiples de code que cela introduit résultent souvent en un comportement non déterministe. Cependant, on devrait comprendre que quand un accès est alloué au hasard, il peut se trouver justement qu'il soit alloué par hasard au même accès. Les applications doivent donc être capables de traiter aussi bien la préservation d'accès que la non préservation d'accès.

a) Certaines applications s'attendent à ce que l'accès de source UDP soit dans la gamme bien connue. Voir par exemple la discussion des attentes d'accès de système de fichier réseau dans la [RFC2623].

4.2.2 Parité d'accès

Certains NAT préservent la parité de l'accès UDP, c'est-à-dire, un accès pair va être transposé en un accès pair et un accès impair va être transposé en un accès impair. Ce comportement respecte la règle de la [RFC3550] que RTP utilise des accès pairs, et RTCP utilise des accès impairs. La RFC 3550 permet que tout numéro d'accès soit utilisé pour RTP et RTCP si les deux numéros sont spécifiés séparément ; par exemple, en utilisant la [RFC3605]. Cependant, certaines mises en œuvre n'incluent pas la RFC 3605, et ne reconnaissent pas quand l'homologue a spécifié l'accès RTCP séparément en utilisant la RFC 3605. Si une telle mise en œuvre reçoit un numéro d'accès RTP impair de l'homologue (peut-être après avoir été traduit par un NAT) et ensuite suit la règle de la RFC 3550 pour changer l'accès RTP en le prochain numéro pair inférieur, cela va évidemment résulter en la perte de RTP. Les aspects d'application favorable au NAT sortent du domaine d'application du présent document. Il est supposé que ce problème va disparaître avec le temps, avec l'amélioration des mises en œuvre. Préserver la parité de l'accès permet de prendre en charge la communication avec les homologues qui ne prennent pas en charge la spécification explicite des deux numéros d'accès RTP et RTCP.

REQ-4 : il est RECOMMANDÉ qu'un NAT ait un comportement de "préservation de la parité d'accès" de "Oui".

Justification : ceci est pour éviter de casser les applications d'homologue à homologue qui ne spécifient pas explicitement et séparément les numéros d'accès RTP et RTCP et qui suivent la règle de la RFC 3550 de décrémenter un accès RTP impair pour le rendre pair. Les mêmes considérations s'appliquent pour l'exigence de réservoir d'adresse IP.

4.2.3 Contiguïté d'accès

Certains NAT tentent de préserver la règle de contiguïté des accès de RTCP = RTP + 1. Ces NAT font des choses comme l'allocation séquentielle ou la réservation d'accès. L'allocation séquentielle d'accès suppose que l'application va ouvrir une transposition pour RTP d'abord et ensuite pour RTCP. Il n'est pas pratique d'appliquer cette exigence sur toutes les applications. De plus, il y a un problème d'encombrement si de nombreuses applications (ou points d'extrémité) essayent d'ouvrir simultanément des transpositions. La préservation d'accès est aussi problématique car elle est coûteuse, en particulier si on considère qu'un NAT ne peut pas fiablement distinguer entre les paquets RTP sur UDP et les autres paquets UDP lorsque il n'y a pas de règle de contiguïté. Pour ces raisons, il serait trop complexe de tenter de préserver la

règle de contiguïté en suggérant un comportement spécifique de NAT, et cela casserait certainement la règle de comportement déterministe.

Afin de prendre en charge RTP et RTCP, il va donc être nécessaire que les applications suivent les règles de négociation séparée de RTP et RTCP, et de tenir compte de la possibilité très réelle que la règle RTCP = RTP + 1 soit violée. Comme c'est une exigence d'application, cela sort du domaine d'application du présent document.

4.3 Rafraîchissement de transposition

Les mises en œuvre de temporisation de transposition de NAT varient, mais incluent la valeur du temporisateur et la façon dont le temporisateur de transposition est rafraîchi pour garder la transposition en vie.

Le temporisateur de transposition est défini comme le temps pendant lequel une transposition va rester active sans paquet traversant le NAT. Il y a une grande variété dans les valeurs utilisées par les différents NAT.

REQ-5 : un temporisateur de transposition UDP de NAT NE DOIT PAS expirer en moins de deux minutes, sauf si la REQ-5a s'applique.

a) Pour un accès de destination spécifique dans la gamme d'accès bien connus (accès 0 à 1023) un NAT PEUT avoir des temporisateurs de transposition UDP plus courts que ce qui est spécifique des applications enregistrées par l'IANA fonctionnant sur cet accès de destination spécifique.
b) La valeur du temporisateur de transposition UDP de NAT PEUT être configurable.
c) Une valeur par défaut de cinq minutes ou plus pour le temporisateur de transposition UDP de NAT est RECOMMANDÉE.

Justification : Cette exigence est destinée à s'assurer que la fin de temporisation est assez longue pour éviter de trop fréquents paquets de rafraîchissement de temporisateur.

a) Certains protocoles UDP utilisent des connexions de très courte durée. Il peut y avoir un grand nombre de ces connexions ; les conserver toutes dans un tableau des connexions pourrait causer une charge considérable sur le NAT. Avoir de plus courts temporisateurs pour ces applications spécifiques est donc une technique d'optimisation. Il est important que les temporisateurs plus courts appliqués à des protocoles spécifiques soient utilisés avec parcimonie, et seulement pour les protocoles qui utilisent des accès de destination bien connus qui sont connus pour avoir une temporisation plus courte, et qui sont connus pour n'être pas utilisés par des applications pour d'autres objets.

b) La configuration est désirable pour s'adapter à des réseaux et des corrections d'anomalies spécifiques.

c) Cette valeur par défaut est pour éviter de trop fréquents paquets de rafraîchissement de temporisateur.

Certains NAT gardent la transposition active (c'est-à-dire, rafraîchissent la valeur du temporisateur) quand un paquet va du côté interne du NAT au côté externe du NAT. Ceci est appelé avoir un comportement de rafraîchissement de NAT en sortie de "vrai".

Certains NAT gardent la transposition active quand un paquet va du côté externe du NAT au côté interne du NAT. Ceci est appelé avoir un comportement de rafraîchissement de NAT entrant de "vrai".

Certains NAT gardent la transposition active dans les deux cas, et alors les deux propriétés sont "vrai".

REQ-6 : La direction de rafraîchissement de transposition de NAT DOIT avoir un "comportement de rafraîchissement de NAT sortant" de "vrai".

a) La direction de rafraîchissement de transposition de NAT PEUT avoir un "comportement de rafraîchissement de NAT sortant" de "vrai".

Justification : le rafraîchissement sortant est nécessaire pour permettre au client de garder la transposition en vie.

a) le rafraîchissement sortant peut être utile aux applications sans trafic UDP sortant. Cependant, permettre le rafraîchissement entrant peut permettre à un attaquant externe ou une application au mauvais comportement de garder une transposition en vie indéfiniment. Cela peut être un risque pour la sécurité. Aussi, si le processus est répété sur différents accès, cela pourrait au fil du temps utiliser tous les accès sur le NAT.

4.4 Conflit d'espace d'adresse IP interne et externe

De nombreux NAT, en particulier des appareils de niveau consommateur conçus pour être déployés par des utilisateurs non techniciens, obtiennent de façon habituelle leur adresse IP externe, le routeur par défaut, et les autres informations de configuration IP pour leur interface externe, dynamiquement à partir d'un réseau externe, comme un FAI en amont. Le NAT à son tour, établit automatiquement son propre sous réseau interne dans un des espaces d'adresses IP privés alloués à cette fin dans la [RFC1918], fournissant normalement des services de configuration IP dynamiques aux hôtes de ce réseau interne.

L'auto configuration des NAT et des réseaux privés peut être cependant problématique si le réseau externe du NAT est aussi dans l'espace d'adresse privé de la RFC 1918. Dans un scénario courant, un FAI place ses consommateurs derrière un NAT et leur attribue des adresses privées de la RFC 1918. Certains de ces consommateurs, à leur tour, déploient des NAT de niveau consommateur, qui, en effet, agissent comme des NAT de "second niveau", multiplexant leurs propres sous réseaux privés de la RFC 1918 sur la seule adresse IP de la RFC 1918 fournie par le FAI. Il n'est pas absolument garanti dans ce cas que le réseau "intermédiaire" à adresses privées du FAI et le réseau interne à adresses privées du consommateur ne vont pas utiliser des sous réseaux IP de la RFC 1918 numériquement identiques ou se chevauchant. De plus, les consommateurs de NAT de niveau consommateur ne peuvent pas être supposés avoir les connaissances techniques permettant d'empêcher ce scénario de se produire en configurant manuellement leur réseau interne avec des sous réseaux de la RFC 1918 qui ne soient pas en conflit.

Les fabricants de NAT doivent concevoir leurs NAT de façon à s'assurer qu'ils fonctionnent correctement et de façon robuste même dans des scénarios aussi problématiques. Une solution possible est que le NAT s'assure que chaque fois que sa liaison externe est configurée avec une adresse IP privée de la RFC 1918, le NAT choisit automatiquement un sous réseau IP différent, non en conflit pour son réseau interne. Un inconvénient de cette solution est que, si l'interface externe du NAT est configurée de façon dynamique ou reconfigurée après que son réseau interne est déjà en service, alors le NAT peut devoir renuméroter dynamiquement tout son réseau interne si il détecte un conflit.

Une autre solution est que le NAT soit conçu de telle façon qu'il puisse traduire et transmettre correctement le trafic, même quand ses interfaces externes et internes sont configurées avec des sous réseaux IP qui se chevauchent numériquement. Dans ce scénario, par exemple, si il a été alloué à l'interface externe du NAT une adresse IP dans l'espace de la RFC 1918, il peut aussi y avoir un nœud interne I ayant la même adresse IP privée P de la RFC 1918. Un paquet IP avec l'adresse de destination P sur le réseau externe est dirigée sur le NAT, tandis qu'un paquet IP avec la même adresse de destination P sur le réseau interne est dirigée sur le nœud I. Le NAT a donc besoin de maintenir une claire distinction opérationnelle entre les "adresses IP externes" et les "adresses IP internes" pour éviter de confondre le nœud interne I avec sa propre interface externe. En général, le NAT a besoin de permettre à tous ses nœuds internes (I inclus) de communiquer avec tous les nœuds externes qui ont des adresses IP publiques (non de la RFC 1918) ou qui ont des adresses IP privées qui ne sont pas en conflit avec les adresses utilisées par son réseau interne.

REQ-7 : un appareil de NAT dont l'interface IP externe peut être configurée dynamiquement DOIT soit (1) s'assurer automatiquement que son réseau interne utilise des adresses IP qui ne sont pas en conflit avec son réseau externe, soit (2) être capable de traduire et transmettre le trafic entre tous les nœuds internes et tous les nœuds externes dont les adresses IP sont en conflit numérique avec le réseau interne.

Justification : si les interfaces externes et internes d'un NAT sont configurées avec des sous réseaux IP qui se chevauchent, il n'y a alors aucun moyen pour un hôte interne qui a l'adresse IP Q de la RFC 1918 d'initier une session de communication directe avec un nœud externe ayant la même adresse Q de la RFC 1918, ou avec les autres nœuds externes ayant des adresses IP en conflit numérique avec le sous réseau interne. Ces nœud peuvent quand même ouvrir des sessions de communication indirectement via les techniques de traversée de NAT, cependant, avec l'aide d'un serveur tiers, comme un serveur STUN ayant une adresse IP publique, non de la RFC 1918. Dans ce cas, les nœuds ayant des adresses privées de la RFC 1918 en conflit sur le côté opposé du NAT de second niveau peuvent communiquer les uns avec les autres via leurs points d'extrémité publics temporaires respectifs sur l'Internet mondial, pour autant que leur NAT de premier niveau commun (par exemple, le NAT du FAI en amont) prenne en charge le comportement d'épingle à cheveux, décrit à la Section 6.

5. Comportement de filtrage

Cette Section décrit divers comportements de filtrage observés dans les NAT.

Quand un point d'extrémité interne ouvre une session sortante à travers un NAT, le NAT alloue une règle de filtrage pour la transposition entre un couple d'accès IP interne (X:x) et externe (Y:y).

Le comportement clé à décrire est quels critères sont utilisés par le NAT pour filtrer les paquets originaire de points d'extrémité externes spécifiques.

Filtrage indépendant du point d'extrémité : le NAT filtre seulement les paquets qui ne sont pas destinés à l'adresse et accès internes X:x, sans considération de l'adresse et accès IP externes de source (Z:z). Le NAT transmet tous les paquets destinés à X:x. En d'autres termes, l'envoi des paquets provenant du côté interne du NAT à toute adresse IP externe est suffisant pour permettre le retour de tous paquets au point d'extrémité interne.

Filtrage dépendant de 'adresse : le NAT filtre les paquets qui ne sont pas destinés à l'adresse IP interne X:x. De plus, le NAT va filrer les paquets provenant de Y:y destinés au point d'extrémité interne X:x si X:x n'a pas envoyé précédemment de paquets à Y:y (indépendamment de l'accès utilisé par Y). En d'autres termes, pour recevoir des paquets d'un point d'extrémité externe spécifique, il est nécessaire que le point d'extrémité interne envoie d'abord des paquets à l'adresse IP de ce point d'extrémité externe spécifique.

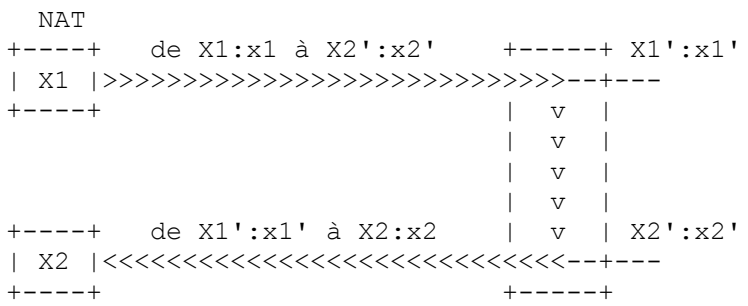
Filtrage dépendant de l'adresse et de l'accès : ceci est similaire au comportement précédent, sauf que l'accès externe est aussi pertinent. Le NAT filtre les paquets qui ne sont pas destinés à l'adresse interne X:x. De plus, le NAT va filtrer les paquets provenant de Y:y destinés au point d'extrémité interne X:x si X:x n'a pas envoyé précédemment de paquets à Y:y. En d'autres termes, pour recevoir des paquets d'un point d'extrémité externe spécifique, il est nécessaire que le point d'extrémité interne envoie d'abord des paquets à l'adresse et accès IP de ce point d'extrémité externe.

REQ-8 : si la transparence d'application est très importante, il est RECOMMANDÉ qu'un NAT ait un comportement de "filtrage indépendant du point d'extrémité". Si un comportement de filtrage plus contraignant est très important, il est RECOMMANDÉ qu'un NAT ait un comportement de "filtrage dépendant de l'adresse".
a) Le comportement de filtrage PEUT être une option configurable par l'administrateur du NAT.

Justification : la recommandation d'utiliser le filtrage indépendant du point d'extrémité vise à maximiser la transparence d'application ; en particulier, pour les applications qui reçoivent simultanément des supports de plusieurs localisations (par exemple, de jeux) ou des applications qui utilisent des techniques de rendez-vous. Cependant, il est aussi possible que, dans certaines circonstances, il soit préférable d'avoir un comportement de filtrage plus contraignant. Le filtrage indépendant du point d'extrémité externe n'est pas aussi sûr : un paquet non autorisé pourrait passer à travers d'un accès spécifique alors que l'accès est resté ouvert si il a eu la chance de trouver l'accès ouvert. En théorie, le filtrage fondé sur l'adresse et l'accès IP est plus sûr que le filtrage fondé seulement sur l'adresse IP (parce que le point d'extrémité externe pourrait, en réalité, être deux points d'extrémité derrière un autre NAT, où un des deux points d'extrémité est un attaquant). Cependant, une telle politique pourrait interférer avec des applications qui s'attendent à recevoir des paquets UDP sur plus d'un accès UDP. Utiliser le filtrage indépendant du point d'extrémité ou le filtrage dépendant de l'adresse au lieu du filtrage dépendant de l'adresse et de l'accès sur un NAT (disons, le NAT-A) a aussi des avantages quand l'autre point d'extrémité est derrière un NAT au comportement non conforme (disons, le NAT-B) qui ne prend pas en charge la REQ-1. Quand les points d'extrémité utilisent ICE, si le NAT-A utilise le filtrage dépendant de l'adresse et de l'accès, la connexité va exiger un relais UDP. Cependant, le si NAT-A utilise le filtrage indépendant du point d'extrémité ou le filtrage dépendant de l'adresse, ICE va finalement trouver la connexité sans exiger de relais UDP. Avoir le comportement de filtrage comme option configurable par l'administrateur du NAT assure qu'un NAT peut être utilisé dans la plus large variété de scénarios de déploiement.

6. Comportement d'épingle à cheveux

Si deux hôtes (appelés X1 et X2) sont derrière le même NAT et échangent du trafic, le NAT peut allouer une adresse sur l'extérieur du NAT pour X2, appelée X2':x2'. Si X1 envoie du trafic à X2':x2', il va au NAT, qui doit relayer le trafic de X1 à X2. Ceci est appelé une épingle à cheveux et est illustré ci-dessous.



Comportement en épingle à cheveux

L'épingle à cheveux permet à deux points d'extrémité sur le côté interne du NAT de communiquer même si il utilisent seulement les adresses et accès IP externes l'un de l'autre.

Plus formellement, un NAT qui prend en charge l'épingle à cheveux transmet les paquets originaires d'une adresse interne, X1:x1, destinés à une adresse externe X2':x2' qui a une transposition active en une adresse interne X2:x2, en retour à cette adresse interne, X2:x2. Noter que normalement X1' est le même que X2'.

De plus, le NAT peut présenter le paquet qui fait l'épingle à cheveux avec une adresse et accès IP de source internes (X1:x1) ou externes (X1':x1'). Donc, le comportement de NAT en épingle à cheveux peut être soit "adresse et accès IP de source externes", soit "adresse et accès IP de source internes". Une "adresse et accès IP de source internes" peut causer des problèmes pour les mises en œuvre qui attendent une adresse et accès IP externes.

REQ-9 : un NAT DOIT prendre en charge le "comportement d'épingle à cheveux".
a) Un comportement d'épingle à cheveux de NAT DOIT être "adresse et accès IP de source externes".

Justification : cette exigence est pour permettre les communications entre deux points d'extrémité derrière le même NAT quand ils essayent l'adresse IP externe de l'autre.

a) Utiliser l'adresse IP externe de source est nécessaire pour les applications qui ont une politique restrictive de ne pas accepter de paquets provenant d'adresses IP qui diffèrent de ce qui est attendu.

7. Passerelles de niveau application

Certains NAT ont mis en œuvre des passerelles de niveau application (ALG, *Application Level Gateway*) pour divers protocoles, incluant des protocoles pour négocier des sessions d'homologue à homologue, comme SIP.

Certains NAT ont ces ALG activées en permanence, d'autres les ont activées par défaut mais leur permettent d'être désactivées, et d'autres les ont désactivées par défaut mais leur permettent d'être activées.

Les ALG de NAT peuvent interférer avec les méthodes UNSAF ou des protocoles qui essayent d'être avertis des NAT et donc doivent être utilisés avec d'extrêmes précautions.

REQ-10 : pour éliminer l'interférence avec les mécanismes UNSAF de traversée de NAT et permettre la protection de l'intégrité des communications UDP, les ALG de NAT pour les protocoles fondés sur UDP DEVRAIENT être désactivées. De futures spécifications sur la voie de la normalisation qui définissent des ALG pourraient mettre à jour cela pour recommander que les ALG qu'elle définissent soient activées par défaut.
a) Si un NAT inclut des ALG, il est RECOMMANDÉ que le NAT permette à l'administrateur du NAT d'activer ou désactiver séparément chaque ALG.

Justification : les ALG de NAT peuvent interférer avec les méthodes UNSAF.
a) Cette exigence permet à l'utilisateur d'activer les ALG qui sont nécessaires pour aider au fonctionnement de certaines applications sans activer les ALG, qui interfèrent avec le fonctionnement des autres applications.

8. Propriétés déterministes

La classification des NAT est encore compliquée par le fait que, dans certaines conditions, le même NAT va présenter des comportements différents. On a vu cela avec les NAT qui préservent l'accès ou ont des algorithmes spécifiques pour choisir un accès autre qu'un accès libre. Si l'accès externe que le NAT souhaite utiliser est déjà utilisé par une autre session, le NAT doit choisir un accès différent. Il en résulte des chemins de code différents pour ce cas de conflit, qui résulte en un comportement différent.

Par exemple, si trois hôtes X1, X2, et X3 envoient tous à partir du même accès x, à travers un NAT qui préserve l'accès avec seulement une adresse IP externe, appelée X1', le premier qui envoie (c'est-à-dire, X1) va obtenir un accès externe de x, mais les deux suivants vont obtenir x2' et x3' (qui ne sont pas égaux à x). Ce sont des NAT où les caractéristiques de transposition de NAT externes et les caractéristiques de filtre externes changent entre la transposition X1:x et la transposition X2:x. Pour empirer les choses, il y a des NAT où le comportement peut être le même sur les transpositions X1:x et X2:x, mais différent sur la troisième transposition X3:x.

Un autre exemple est que certains NAT ont une "transposition indépendante du point d'extrémité", combinée avec la "surcharge d'accès", tant que les deux points d'extrémité n'établissent pas de sessions pour la même direction externe, mais changent alors leur comportement en "transposition dépendant de l'adresse et de l'accès" sans "préservation de l'accès" quand ils détectent ces établissements de sessions conflictuels.

Tout NAT qui change la transposition de NAT ou le comportement de filtrage sans changement de configuration, à un moment quelconque, dans des conditions particulières, est appelé un NAT "non déterministe". Les NAT qui ne le font pas sont appelés "déterministes".

Les NAT non déterministes changent généralement de comportement quand un conflit d'une certaine sorte se produit, c'est-à-dire, quand l'accès qui devrait normalement être utilisé est déjà utilisé par une autre transposition. La transposition de NAT et le filtrage externe en l'absence de conflit est appelé le comportement primaire. On se réfère au comportement après le premier conflit comme secondaire et après le second conflit comme tertiaire. Aucun NAT n'a été observé qui change sur d'autres conflits, mais il est certainement possible qu'il en existe.

REQ-11 : un NAT DOIT avoir un comportement déterministe, c'est-à-dire, il NE DOIT changer le comportement de traduction de NAT (Section 4) ou de filtrage (Section 5) à aucun moment, ou sous aucune condition particulière.

Justification : les NAT non déterministes sont très difficile à réparer parce qu'ils exigent des essais plus intensifs. Ce comportement non déterministe est la cause de la plupart des incertitudes que les NAT introduisent quand à savoir si les applications vont ou non fonctionner.

9. Comportement en cas de destination ICMP injoignable

Quand un NAT envoie un paquet à un hôte sur l'autre côté du NAT, un message ICMP peut être envoyé en réponse à ce paquet. Ce message ICMP peut être envoyé par l'hôte de destination ou par un routeur le long du chemin du réseau. La configuration par défaut du NAT NE DEVRAIT PAS filtrer les messages ICMP sur la base de leur adresse IP de source. Ces messages ICMP DEVRAIENT être réécrits par le NAT (précisément, les en-têtes IP et la charge utile ICMP) et transmis à l'hôte interne ou externe approprié. Le NAT a besoin d'effectuer cette fonction aussi longtemps que la transposition UDP est active. La réception de toute sorte de message ICMP NE DOIT PAS détruire la transposition de NAT. Un NAT qui effectue les fonctions décrites ci-dessus est désigné comme "prenant en charge le traitement ICMP".

Il n'y a pas d'avantage de sécurité significatif à bloquer les paquets ICMP Destination injoignable. De plus, bloquer les paquets ICMP Destination injoignable peut interférer avec la reprise sur défaillance de l'application, la découverte de la MTU de chemin UDP (voir les [RFC1191] et [RFC1435]) et traceroute. Bloquer tout message ICMP est déconseillé, et bloquer le message ICMP Destination injoignable est fortement déconseillé.

REQ-12 : la réception d'aucune sorte de message ICMP NE DOIT terminer la transposition de NAT.

a) La configuration par défaut du NAT NE DEVRAIT PAS filtrer les messages ICMP sur la base de leur adresse IP de source.
b) Il est RECOMMANDÉ qu'un NAT prenne en charge les messages ICMP Destination injoignable.

Justification : c'est facile à faire et c'est utilisé pour de nombreuses choses incluant la découverte de la MTU et la détection rapide de conditions d'erreur, et n'a pas de conséquences négatives.

10. Fragmentation des paquets sortants

Quand la MTU de la liaison adjacente est trop petite, il peut survenir une fragmentation des paquets allant du côté interne au côté externe du NAT. Cela peut se produire si le NAT fait du point à point sur Ethernet, ou si le NAT a été configuré avec une petite MTU pour réduire le délai de mise en série lors de l'envoi de grands paquets et de petits paquets de priorité plus élevée, ou pour d'autres raisons.

On notera que de nombreuses piles IP n'utilisent pas la découverte de la MTU du chemin avec les paquets UDP.

Le paquet pourrait avoir son bit Ne pas fragmenter réglé à 1 (DF = 1) ou 0 (DF = 0).

REQ-13 : si le paquet reçu sur une adresse IP interne a le bit DF = 1, le NAT DOIT renvoyer un message ICMP "Fragmentation nécessaire et DF établi" à l'hôte, comme décrit dans la [RFC0792].
a) Si le paquet a DF = 0, le NAT DOIT fragmenter le paquet et DEVRAIT envoyer les fragments dans l'ordre.

Justification : c'est ce qui est conforme à la RFC 792.
a) C'est la même fonction qu'effectue un routeur dans une situation similaire [RFC1812].

11. Réception de paquets fragmentés

Pour diverses raisons, un NAT peut recevoir un paquet fragmenté. Le paquet IP qui contient l'en-tête pourrait arriver dans n'importe quel fragment, selon les conditions du réseau, l'ordre des paquets, et la mise en œuvre de la pile IP qui a généré les fragments.

Un NAT qui est capable seulement de recevoir des fragments dans l'ordre (c'est-à-dire, avec l'en-tête dans le premier paquet) et de transmettre chacun des fragments à l'hôte interne est décrit comme "fragments reçus dans l'ordre".

Un NAT qui est capable de recevoir les fragments dans l'ordre ou le désordre et de transmettre les fragments individuels (ou un paquet réassemblé) à l'hôte interne est décrit comme "reçoit les fragments en désordre". Voir la Section 13, Considérations sur la sécurité, pour une discussion de ce comportement.

Un NAT qui n'est ni l'un ni l'autre est décrit comme "ne reçoit pas de fragments".

REQ-14 : un NAT DOIT prendre en charge la réception de fragments dans l'ordre et de fragments déclassés, donc il DOIT avoir le comportement "reçoit les fragments en désordre".
a) Le mécanisme de traitement de fragments déclassés d'un NAT DOIT être conçu de telle façon que des attaques de déni de service fondées sur la fragmentation ne compromettent pas la capacité du NAT de traiter les paquets IP dans l'ordre et non fragmentés.

Justification : voir les considérations sur la sécurité.

12. Exigences

Les exigences de cette Section visent à minimiser les complications causées par les NAT aux applications comme les communications en temps réel et les jeux en ligne. Les exigences mentionnées plus tôt dans le présent document sont consolidées ici dans une seule section.

On devrait cependant comprendre que les applications ne savent normalement pas à l'avance si le NAT se conforme aux recommandations définies dans cette section. Les applications de supports d'homologue à homologue ont encore besoin d'utiliser les procédures normales, comme celles de ICE [RFC5245].

Un NAT qui prend en charge toutes les exigences obligatoires de la présente spécification (c'est-à-dire, marquées "DOIT") est "conforme à cette spécification". Un NAT qui prend en charge toutes les exigences de cette spécification (c'est-à-dire, incluant les "RECOMMANDÉ") est "pleinement conforme à toutes les exigences obligatoires et recommandées de cette spécification".

REQ-1 : un NAT DOIT avoir un comportement de "transposition indépendante du point d'extrémité".

REQ-2 : il est RECOMMANDÉ qu'un NAT ait un comportement de "réservoir d'adresses IP" de "apparié". Noter que cette exigence n'est pas applicable aux NAT qui ne prennent pas en charge le réservoir d'adresses IP.

REQ-3 : un NAT NE DOIT PAS avoir un comportement "d'allocation d'accès" de "surcharge d'accès".
a) Si l'accès de source d'un hôte était dans la gamme de 0 à 1023, il est RECOMMANDÉ que l'accès de source du NAT soit dans la même gamme. Si l'accès de source de l'hôte était dans la gamme 1024 à 65535, il est RECOMMANDÉ que l'accès de source du NAT soit dans cette gamme.

REQ-4 : il est RECOMMANDÉ qu'un NAT ait un comportement de "préservation de la parité d'accès" de "oui".

REQ-5 : un temporisateur de transposition UDP de NAT NE DOIT PAS expirer en moins de deux minutes, sauf si la REQ-5a s'applique.
a) Pour un accès de destination spécifique dans la gamme d'accès bien connue (accès de 0 à 1023) un NAT PEUT avoir des temporisateurs de transposition UDP plus courts que ceux spécifiques d'application enregistrée par l'IANA qui fonctionnent sur cet accès de destination spécifique.
b) La valeur du temporisateur de transposition UDP de NAT PEUT être configurable.
c) Une valeur par défaut de cinq minutes ou plus pour le temporisateur de transposition UDP de NAT est RECOMMANDÉE.

REQ-6 : La direction de rafraîchissement de transposition de NAT DOIT avoir un "comportement de rafraîchissement de NAT sortant" de "vrai".
a) La direction de rafraîchissement de transposition de NAT PEUT avoir un "comportement de rafraîchissement de NAT entrant" de "vrai".

REQ-7 : Un appareil de NAT dont l'interface IP externe peut être configurée dynamiquement DOIT soit (1) s'assurer automatiquement que son réseau interne utilise des adresses IP qui n'entrent pas en conflit avec celles de son réseau externe, soit (2) être capable de traduire et transmettre du trafic entre tous les nœuds internes et tous les nœuds externes dont les adresses IP entrent numériquement en conflit avec le réseau interne.

REQ-8 : Si la transparence d'application est de la plus grande importance, il est RECOMMANDÉ qu'un NAT ait un comportement de "filtrage indépendant du point d'extrémité". Si un comportement de filtrage plus contraignant est le plus important, il est RECOMMANDÉ qu'un NAT ait un comportement de "filtrage dépendant de l'adresse".
a) Le comportement de filtrage PEUT être une option configurable par l'administrateur du NAT.

REQ-9 : Un NAT DOIT prendre en charge le comportement "d'épingle à cheveux".
a) Un comportement de NAT d'épingle à cheveux DOIT être "adresse et accès IP de source externes".

REQ-10 : Pour éliminer les interférences avec les mécanismes UNSAF de traversée de NAT et permettre la protection de l'intégrité des communications UDP, les ALG de NAT pour les protocoles fondés sur UDP DEVRAIENT être désactivées. Les futures spécifications sur la voie de la normalisation qui définiront une ALG pourront mettre cela à jour pour recommander les ALG définies par défaut.
a) Si un NAT inclut des ALG, il est RECOMMANDÉ que le NAT permette à son administrateur d'activer ou désactiver chaque ALG séparément.

REQ-11 : Un NAT DOIT avoir un comportement déterministe, c'est-à-dire, il NE DOIT changer le comportement de traduction de NAT (Section 4) ou de filtrage (Section 5) à aucun moment, ni dans aucune condition particulière.

REQ-12 : La réception d'aucune sorte de message ICMP NE DOIT terminer la transposition de NAT.
a) La configuration de NAT par défaut NE DEVRAIT PAS filtrer les messages ICMP sur la base de leur adresse IP de source.
b) Il est RECOMMANDÉ qu'un NAT prenne en charge les messages ICMP Destination injoignable.

REQ-13 : Si le paquet reçu sur une adresse IP interne a le bit DF = 1, le NAT DOIT renvoyer un message ICMP

"Fragmentation nécessaire et bit DF établi" à l'hôte, comme décrit dans la [RFC0792].
a) Si le paquet a le bit DF = 0, le NAT DOIT fragmenter le paquet et DEVRAIT envoyer les fragments dans l'ordre.

REQ-14 : Un NAT DOIT prendre en charge la réception des fragments dans l'ordre et déclassés, donc il DOIT avoir le comportement "Fragments reçus déclassés".
a) Un mécanisme de traitement de fragment déclassé pour le NAT DOIT être conçu de telle façon que les attaques de déni de service fondées sur la fragmentation ne compromettent pas la capacité du NAT de traiter les paquets en ordre et non fragmentés.

13. Considérations sur la sécurité

Les NAT sont souvent déployés pour réaliser des buts de sécurité. La plupart des recommandations et exigences du présent document n'affectent pas les propriétés de sécurité de ces appareils, mais quelques unes ont des implications pour la sécurité et elles sont discutés dans cette section.

Le présent document recommande que les temporisateurs pour la transposition soient rafraîchis sur les paquets sortants (voir la REQ-6) et ne fait pas de recommandation sur si les paquets entrants devraient ou non mettre à jour les temporisateurs. Si les paquets entrants mettent à jour les temporisateurs, un attaquant externe pourrait garder la transposition en vie pour toujours et attaquer de futurs appareils qui peuvent finir avec la même adresse interne. Un appareil qui a aussi été le serveur DHCP pour l'espace d'adresses privé pourrait atténuer cela en purgeant toutes les transpositions à l'expiration d'un prêt DHCP. Pour le trafic UDP en envoi individuel (qui est le domaine d'application du présent document) il peut sembler non pertinent de prendre en charge le rafraîchissement du temporisateur d'entrée ; cependant, pour UDP en diffusion groupée, la question est plus difficile. Il est prévu que de futurs documents discutant du comportement de NAT avec le trafic en diffusion groupée affinent les exigences sur le traitement du temporisateur de rafraîchissement en entrée. Certains appareils d'aujourd'hui mettent à jour les temporisateurs sur les paquets entrants.

Le présent document recommande que les filtres de NAT soient spécifiques seulement de l'adresse IP externe (voir la REQ-8) et non de l'adresse IP¨et accès UDP externes. On peut objecter que ceci est moins sûr que d'utiliser l'adresse et accès IP. Les appareils qui souhaitent filtrer sur l’adresse et l'accès IP sont quand même conformes à ces exigences.

Les NAT non déterministes présentent un risque du point de vue de la sécurité. Ils sont très difficiles à vérifier à cause de leur caractère non déterministe. L'essai par une personne qui en configure un peut avoir pour résultat que la personne pense qu'il se comporte comme désiré, alors que dans des conditions différentes, que peut créer un attaquant, le NAT peut se comporter différemment. Ces exigences recommandent que les appareils soient déterministes.

Le présent document exige que les NAT aient un comportement de "transposition externe de NAT indépendante du point d'extrémité". Cela ne réduit pas la sécurité des appareils. Quels paquets sont autorisé à s'écouler à travers l'appareil est déterminé par le comportement de filtrage externe, qui est indépendant du comportement de transposition.

Quand un paquet fragmenté est reçu du côté externe, et que les paquets sont en désordre de telle sorte que le fragment initial n'arrive pas en premier, de nombreux systèmes éliminent simplement les paquets déclassés. De plus, comme certains réseaux livrent les petits paquets avant les grands, il peut y avoir de nombreux fragments déclassés. Les NAT qui sont capables de livrer ces paquets déclassés sont possibles, mais ils ont besoin de mémoriser les fragments déclassés, ce qui peut ouvrir une opportunité de déni de service, si c'est fait de façon incorrecte. La fragmentation a été un outil utilisé dans de nombreuses attaques, certaines impliquant de passer des paquets fragmentés à travers les NAT, et d'autres impliquant des attaques de déni de service fondées sur l'état nécessaire pour réassembler les fragments. Les mises en œuvre de NAT devraient tenir compte des [RFC3128] et [RFC1858].

14. Considérations de l'IAB

L'IAB a étudié le problème de "l'auto réparation unilatérale d'adresse", qui est le processus général par lequel un client tente de déterminer son adresse dans un autre domaine de l'autre côté d'un NAT par un mécanisme de réflexion de protocole collaboratif [RFC3424].

La présente spécification ne constitue pas par elle-même une application UNSAF. Elle consiste en une série d'exigences pour les NAT visant à minimiser l'impact négatif que ces appareils ont pour les applications de supports d'homologues à

homologues, en particulier quand ces applications utilisent des méthodes UNSAF.

La Section 3 de UNSAF fait une liste de plusieurs problèmes pratiques avec des solutions aux problèmes des NAT. Le présent document fait des recommandations pour réduire l'incertitude et les problèmes introduits par ces questions pratiques des NAT. De plus, UNSAF énumère cinq considérations architecturales. Bien que ce ne soit pas une proposition UNSAF, il est intéressant de considérer l'impact de ce travail sur ces considérations architecturales.

Arch-1 : La portée de ceci est limitée aux paquets UDP dans les NAT comme ceux largement déployés aujourd'hui. La "réparation" aide à restreindre la variabilité des NAT aux vraies solutions UNSAF telles que STUN.

Arch-2 : Cela va sortir au même taux que les NAT sortent. Cela n'implique aucune machinerie de protocole qui continuerait de vivre après le départ des NAT, ou qui rendrait leur retrait plus difficile.

Arch-3 : Cela ne réduit pas la fragilité globale des NAT, mais va peut-être réduire certains des comportements de NAT les plus dommageables et rendre plus facile de discuter et prédire les comportement de NAT dans des situations données.

Arch-4 : Ceci fonctionne et les résultats [RESULTS] de divers NAT représentent le travail le plus complet de l'IETF sur ce que sont les problèmes réels avec les NAT pour des applications comme VoIP. Ce travail et STUN ont mis en évidence, plus que toute autre chose, la fragilité que les NAT introduisent et les difficultés du traitement de ces questions.

Arch-5 : Ce travail et les résultat des essais [RESULTS] fournissent un modèle de référence pour ce que toute proposition UNSAF pourrait rencontrer dans les NAT déployés.

15. Remerciements

L'éditeur tient à remercier Bryan Ford, Pyda Srisuresh, et Dan Kegel de leurs nombreuses contributions sur les communications d'homologue à homologue à travers un NAT. Dan Wing a contribué substantiellement au texte sur la fragmentation IP et le comportement de ICMP. Merci à Rohan Mahy, Jonathan Rosenberg, Mary Barnes, Melinda Shore, Lyndsay Campbell, Geoff Huston, Jiri Kuthan, Harald Welte, Steve Casner, Robert Sanders, Spencer Dawkins, Saikat Guha, Christian Huitema, Yutaka Takeda, Paul Hoffman, Lisa Dusseault, Pekka Savola, Peter Koch, Jari Arkko, et Alfred Hoenes de leurs contributions.

16. Références

16.1 Références normatives

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

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

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

16.2 Références pour information

[RESULTS] Jennings, C., "NAT Classification Test Results", Travail en cours, octobre 2006.

[RFC0792] J. Postel, "Protocole du message de contrôle Internet – Spécification du protocole du programme Internet DARPA", STD 5, septembre 1981. *(MàJ par la* RFC6633)

[RFC1191] J. Mogul et S. Deering, "Découverte de la MTU de chemin", novembre 1990.

[RFC1435] S. Knowles, "Avis de l'IESG d'une expérience avec découverte de la MTU de chemin", mars 1993. *(Info)*

[RFC1812] F. Baker, "Exigences pour les routeurs IP version 4", juin 1995. *(MàJ par les* RFC2644, RFC6633)

[RFC1858] G. Ziemba, D. Reed, P. Traina, "Considérations sur la sécurité pour le filtrage de fragment IP", octobre 1995. *(Mise à jour par la* RFC3128*) (Information)*

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

[RFC2460] S. Deering et R. Hinden, "Spécification du protocole Internet, version 6 (IPv6)", décembre 1998. *(MàJ par* 5095, 6564 *; D.S ; Remplacée par* RFC8200, STD 86*)*

[RFC2623] M. Eisler, "Questions de sécurité de NFS versions 2 et 3 et utilisation de RPCSEC_GSS et Kerberos v5 par le protocole NFS", juin 1999. *(P.S.)*

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

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

[RFC3027] M. Holdrege, P. Srisuresh, "Complications de protocole avec le traducteur d'adresse réseau IP", janvier 2001. *(Info.)*

[RFC3128] I. Miller, "Protection contre une variante de l'attaque de petit fragment (RFC1858)", juin 2001. *(Info.)*

[RFC3261] J. Rosenberg et autres, "SIP : Protocole d'initialisation de session", juin 2002. (*Mise à jour par* 3265, 3853, 4320, 4916, 5393, 6665, 8217, 8760)

[RFC3424] L. Daigle, éd., IAB, "Considérations de l'IAB sur l'auto correction d'adressage unilatérale (UNSAF) à travers la traduction d'adresse réseau", novembre 2002. *(Information)*

[RFC3489] J. Rosenberg et autres, "STUN - Simple traversée par le protocole de datagramme d'utilisateur (UDP) des traducteurs d'adresse réseau (NAT)", mars 2003. (*Obsolète, voir* RFC5389) *(P.S.)*

[RFC3550] H. Schulzrinne, S. Casner, R. Frederick et V. Jacobson, "RTP : un protocole de transport pour les applications en temps réel", STD 64, juillet 2003. *(MàJ par* RFC7164, RFC7160, RFC8083, RFC8108, RFC8860)

[RFC3605] C. Huitema, "Attribut du protocole de contrôle en temps réel (RTCP) dans le protocole de description de session (SDP)", octobre 2003. *(P.S.)*

[RFC4380] C. Huitema, "Teredo : Tunnelage IPv6 sur UDP à travers des traducteurs d'adresse réseau (NAT)", février 2006. *(P.S.)*

[RFC5245] J. Rosenberg,"Établissement de connexité interactive (ICE) : Protocole pour la traversée de traducteur d'adresse réseau (NAT) pour les protocoles d'offre/réponse", avril 2010. (*Remplace* RFC4091, 4092) (*P. S. ; remplacée par* 8445)

[RFC5389] J. Rosenberg et autres, "Utilitaires de traversée de session pour les NAT (STUN)", octobre 2008. (*Remplace* RFC3489) *(P.S.)*

[RFC5766] R. Mahy, P. Matthews, J. Rosenberg, "Traversée de NAT au moyen d'un relais (TURN) : Extensions de relais aux utilitaires de traversée de session pour les NAT (STUN)", avril 2010. *(P. S. ; MàJ par* RFC8155 ; Remplacée par RFC8656

[H.323] Recommandation UIT-T H.323v3, "Systèmes de communication multimédia fondés sur le paquet", Genève, septembre 1999.

Adresse des auteurs

François Audet (éditeur)
Nortel Networks
4655 Great America Parkway
Santa Clara, CA 95054
US
mél : audet@nortel.com

Cullen Jennings
Cisco Systems
170 West Tasman Drive
MS: SJC-21/2
San Jose, CA 95134
mél : fluffy@cisco.com

Déclaration complète de droits de reproduction

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