

UFR de mathématique et d'informatique

Université de Strasbourg

Projet de recherche et de documentation scientifique

LES NAT SONT-ILS INFRANCHISSABLES ?

Carine WAKIM et Maxime ZINGRAFF

Etudiants en deuxième année de Coursus Master en Ingénierie : Informatique, Systèmes et Réseaux à l'UFR de Mathématique et Informatique de l'Université de Strasbourg

Encadrant : M. Julien MONTAVONT

Table des matières

I.	Introduction.....	3
II.	Méthodologie de recherche.....	3
III.	L'adressage sur Internet	4
A)	Les adresses IPv4.....	4
B)	Adresses IP privées, adresses IP publiques.....	4
IV.	Présentation générale des NAT.....	5
A)	Définition et fonctionnement des NAT	5
1.	Les NAT, des solutions palliatives	5
2.	Le fonctionnement des NAT	5
B)	Les différents types de NAT	6
1.	Endpoint-Independent Mapping	6
2.	Address-Dependent Mapping	6
3.	Address and Port-Dependent Mapping.....	6
C)	Les apports sécuritaires	6
V.	Les NAT, des entraves à la communication	8
A)	Les NAT et le modèle bout-en-bout	8
1.	Le modèle bout en bout : principe fondamental d'Internet.....	8
2.	Les NAT : des entraves au modèle bout en bout	8
B)	Les problèmes de connectivité engendrés par les NAT	8
VI.	Les méthodes de franchissement des NAT	9
A)	Le Relaying	9
B)	Le Hole Punching.....	10
VII.	Vers la disparition des NAT?	13
VIII.	Conclusion	15

Remerciements

Nous tenons à profondément remercier M. MONTAVONT pour nous avoir accompagnés et soutenus tout au long de ce projet, mais aussi pour nous avoir accordé la chance de découvrir les profondeurs du monde de la recherche.

Nous remercions également nos encadrants de CMI ainsi que tous les enseignants ayant participé à cette unité d'enseignement pour leurs précieux conseils et leur bienveillance.

Nous remercions enfin le personnel du laboratoire ICube pour avoir contribué à la création d'un environnement de travail sain, productif et convivial.

I. Introduction

La fin du XX^{ème} siècle est marquée par l'avènement et l'essor d'Internet. En quelques dizaines d'années, le réseau qui un jour ne reliait que quelques ordinateurs s'est transformé pour devenir le plus vaste réseau mondial de communication.

Cependant, l'essor fulgurant d'Internet dépasse largement les prévisions les plus ambitieuses de ses fondateurs. En effet, les 4,3 milliards d'adresses uniques proposées par le protocole IPv4 se révèlent rapidement insuffisantes face à l'explosion du nombre d'appareils connectés à Internet. L'on se trouve alors face à un problème prééminent : la pénurie des adresses IPv4. La solution évidente pour pallier un tel problème consiste à développer un autre protocole d'adressage proposant une plage d'adresses uniques plus large. Cependant, un tel projet est chronophage.

De peur de freiner l'expansion d'Internet, les organismes internationaux mettent alors en œuvre des solutions transitoires en attendant l'avènement de solutions plus pérennes. C'est ainsi qu'en 1994 un remède provisoire voit le jour : la réutilisation d'adresses IPv4 grâce aux NAT (Network Address Translators).

Les NAT ou Network Address Translators sont des traducteurs : ils traduisent les adresses IP privées en adresses IP publiques. Ainsi, ils réduisent le nombre d'adresses IPv4 allouées en permettant à plusieurs appareils différents d'utiliser la même adresse IP publique.

Bien qu'efficaces, ces solutions palliatives deviennent vite controversées. En effet, les NAT cassent le modèle de communication bout en bout qui est le pilier fondamental d'Internet.

Les NAT ne sont donc plus que de simples traducteurs : ils se transforment en de véritables barrières à la communication. Mais ces barrières sont-elles infranchissables ?

Au cours de ce rapport de recherche, nous nous attacherons à répondre à cette question centrale. Pour ce faire, nous commencerons par présenter les NAT et leur fonctionnement. Ensuite, nous examinerons les différents types de NAT ainsi que les éventuels avantages sécuritaires de chacun de ces types. Nous aborderons ensuite les problèmes posés par ces dispositifs de traduction, avant d'étudier les méthodes permettant de les traverser. Enfin, nous nous pencherons sur les perspectives d'avenir des NAT.

II. Méthodologie de recherche

Pour nos recherches, nous adoptons la dynamique suivante pour chaque cycle de recherches (en général un nouveau cycle toutes les deux semaines) :

- Divisions des sujets de recherches entre nous et recherches en autonomie
- Mise en commun des éléments les plus importants
- Clarification des incompréhensions et rédaction d'un résumé pour chaque sujet
- Adaptation du plan du sujet et mise à jour de la liste des sujets à traiter

Nous avons choisi de nous baser en priorité sur les *Requests For Comments (RFC)*. Ce sont des documents créés par l'*Internet Engineering Task Force* et qui standardisent de nombreux protocoles de communication de la couche « Transport [26] », « Réseau » et des couches supérieures. C'est donc une source que l'on peut considérer comme étant la plus fiable, en particulier pour les protocoles et le fonctionnement des NAT.

Nous nous sommes aussi appuyés sur des articles de recherche, qui évoquent le futur des NAT et de nouvelles déclinaisons des NAT. De même, nous avons utilisé des sources d'acteurs reconnus du monde d'Internet (comme Google) qui fournissent des données analytiques pertinentes. Enfin, certains ouvrages généralistes nous ont aidé à comprendre les notions élémentaires et à pouvoir construire un socle de connaissances.

III. L'adressage sur Internet

Les Network Address Translators sont des dispositifs de traduction d'adresses IP (protocole Internet) : ils convertissent une adresse IP privée en une adresse IP publique. Avant d'expliquer le principe des NAT, il est essentiel de comprendre, d'une part, ce qu'est une adresse IP et, d'autre part, de saisir la distinction entre une adresse IP privée et une adresse IP publique.

A) Les adresses IPv4

Pour échanger des données sur un réseau informatique, il est nécessaire de pouvoir identifier les différentes entités qui le composent. Les adresses IP, ou adresses de protocole Internet, remplissent cette fonction cruciale en fournissant à chaque appareil connecté une identification unique sur Internet.

La structure et le format des adresses IP sont déterminés par le protocole IP [2].

La première version du protocole IP sur Internet est le protocole IPv4 ou protocole Internet version 4. Ce protocole exige que l'adresse IP soit encodée sur 32 bits regroupés en quatre octets séparés par des points. Au total, le protocole IPv4 permet donc d'adresser 2^{32} machines soit environ 4,3 milliards de machines. Lors de l'avènement d'Internet, ce nombre paraît largement suffisant pour assigner une adresse IP à chaque appareil. Cependant, l'explosion du nombre d'appareils connectés à Internet entraîne rapidement un épuisement de l'espace d'adressage disponible. Les 4,3 milliards d'adresses IP proposées par le protocole IPv4 s'avèrent alors insuffisantes. Il faut donc développer un nouveau protocole IP qui propose un espace d'adressage plus large. En attendant l'avènement de ce nouveau protocole, des mesures d'urgences sont mises en place pour pallier le manque d'adresses IP. Parmi ces mesures d'urgence, l'on trouve les adresses IP privées et les NAT. Mais qu'est-ce qu'une adresse IP privée et en quoi diffère-t-elle d'une adresse IP publique ?

B) Adresses IP privées, adresses IP publiques

Pour temporairement remédier à la pénurie d'adresses IP, les plages d'adresses IP privées ont été introduites. Une adresse IP privée, non routable sur Internet, sert à identifier de manière unique une machine au sein d'un réseau local. Elle n'est accessible que par les autres appareils du même réseau local. Une adresse IP publique, quant à elle, est une adresse IP routable sur Internet : elle permet d'identifier de manière unique une machine sur Internet.

Dans un réseau local, comme celui d'un domicile ou d'une entreprise, certains appareils, comme par exemple les imprimantes, ne communiquent jamais sur Internet. Ainsi, ces appareils n'ont pas besoin d'être identifiables de manière unique sur Internet. Pour éviter de gaspiller des adresses IP uniques, il suffit donc pour de tels appareils de posséder une adresse IP privée, non routable sur Internet et non mondialement unique. Dans le protocole IPv4, les adresses IP privées sont celles appartenant aux plages suivantes [17] :

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

En utilisant des adresses IP privées pour les appareils qui n'ont pas besoin d'une connexion directe à Internet, on optimise l'utilisation des adresses IP disponibles en évitant ainsi le gaspillage des ressources d'adressage IP.

Maintenant que nous avons établi la distinction entre les adresses IP privées et publiques, nous pouvons nous pencher sur les NAT.

IV. Présentation générale des NAT

A) Définition et fonctionnement des NAT

1. Les NAT, des solutions palliatives

Les NAT ou Network Address Translators font partie des maintes solutions provisoires proposées pour pallier l'épuisement des adresses IPv4 [1]. Ces dispositifs, aujourd'hui implémentés dans la plupart des box Internet, réduisent considérablement le nombre d'adresses IPv4 consommées sur le réseau mondial [3].

En effet, en absence de NAT, chaque appareil d'un réseau possède une adresse IP publique. Cependant, certains appareils (par exemple, les imprimantes) ne communiquent jamais sur Internet. Ainsi, en leur attribuant une adresse routable, l'on gaspille des adresses IP.

Les NAT permettent d'éviter un tel gaspillage en n'attribuant une adresse IP publique qu'aux machines qui accèdent réellement à Internet.

2. Le fonctionnement des NAT

En pratique, ces dispositifs sont ancrés dans la couche « Réseaux » du modèle OSI. Lorsqu'une machine se trouvant sur un réseau local cherche à communiquer sur Internet, elle assemble un paquet IP contenant, dans le champ « Source », son adresse IP privée et dans le champ « Destination », l'adresse IP publique du destinataire. Ensuite, ce paquet est dirigé vers le routeur du réseau local qui implémente la fonctionnalité NAT. Le NAT accède alors à l'en-tête du paquet IP et modifie le champ « Source » : il remplace l'adresse IP privée de la machine émettrice par une adresse IP publique [6][7]. Pour se souvenir de cette conversion, le NAT stocke dans une table de traduction l'adresse IP privée de la machine émettrice et l'adresse IP routable qui lui a été attribuée. Enfin, le routeur envoie le paquet IP modifié à son destinataire [4].

Ce fonctionnement est explicité dans le schéma ci-dessous. La machine d'adresse IP privée "192.168.0.1" souhaite envoyer un paquet IP à la machine d'adresse IP publique "2.2.2.2". Elle constitue alors un paquet IP contenant, dans le champ « Source », son adresse IP privée "192.168.0.1". Puis, le paquet est transmis vers le routeur qui met en œuvre la fonctionnalité NAT. Le NAT modifie alors le champ « Source » du paquet IP en remplaçant l'adresse privée "192.168.0.1" par l'adresse publique "1.1.1.1". Il stocke également dans sa table de traduction la paire (adresse IP privée, adresse IP publique) qu'il vient de manipuler.

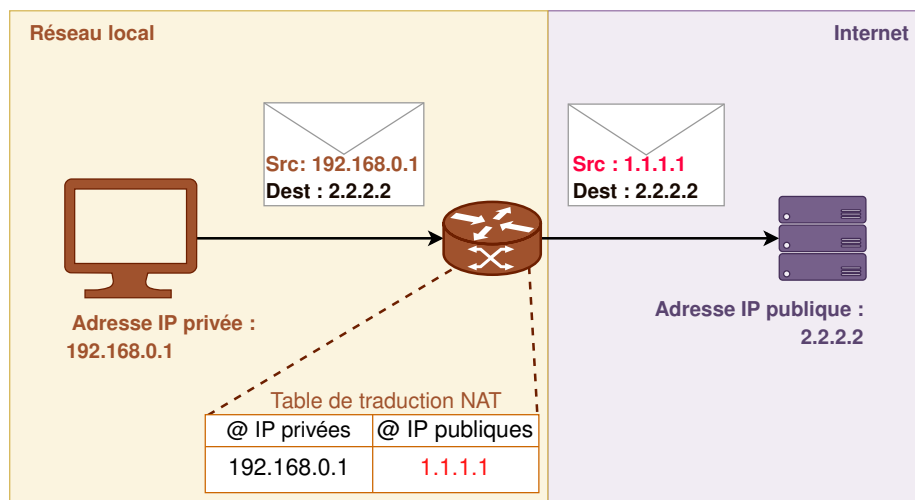


FIGURE 1 – Fonctionnement général des NAT

Mais si les NAT ne sont que de simples traducteurs d'adresses, alors pourquoi les qualifier de "barrières" ? Pour répondre à cette question, il est nécessaire d'examiner les différents types de NAT.

B) Les différents types de NAT

À la création des NAT, plusieurs nomenclatures non normalisées sont apparues, dont certaines sont encore utilisées aujourd'hui dans la littérature et dans l'industrie.

Le besoin pour une nomenclature unifiée est apparu : c'est donc pour cela que le *RFC 4787*[11][5] a été créé : il consacre de manière définitive une nomenclature standardisée, qui fait surtout la différence entre les manières de filtrer les connexions, plutôt qu'entre les manières d'attribuer les adresses.

On retrouve alors trois types de traductions (mappages) :

1. Endpoint-Independent Mapping

Ce type de traduction est indépendant du point de terminaison. Cela signifie qu'on attribue simplement une adresse publique à chaque couple <adresse :port> privé qui souhaite communiquer sur Internet. C'est une association simple entre les deux. En définitive, n'importe quel appareil qui connaît l'alias public peut donc contacter l'appareil sur le réseau local qui est lié à cet alias.

Ce type de traduction peut être utile pour un hébergeur de services sur Internet, comme un serveur Web, car n'importe quel utilisateur sera capable d'accéder au service sans condition préalable.

2. Address-Dependent Mapping

Dans cet type de traduction, la destination des paquets sortants revêt une importance capitale. En effet, le NAT ne va plus simplement associer un alias public à un couple <adresse :port> privé. Le routeur qui héberge le NAT va à présent attribuer un nouveau couple <adresse :port> public à chaque nouvelle adresse de destination.

En terme de filtrage, cela signifie qu'un appareil extérieur peut contacter l'appareil derrière le NAT si et seulement si l'appareil derrière le NAT a déjà initié une connexion avec l'appareil extérieur.

3. Address and Port-Dependent Mapping

Le principe de ce type de traduction reste le même que précédemment, sauf que le NAT attribue un nouveau couple <adresse :port> public à chaque nouveau couple <adresse :port> de destination. Par exemple, même si on a déjà communiqué avec un appareil, si un nouveau port est utilisé par le même appareil, alors une nouvelle association sera créée. Pour le type précédent (Address-Dependant), ce n'est pas le cas.

Il y a donc réellement deux familles de NAT, ceux dépendants et ceux indépendants du point de destination (filtrage sur les connexions entrantes ou non).

C) Les apports sécuritaires

De manière générale, les NAT apportent donc peu de sécurité quant au filtrage des connexions. Néanmoins, ils permettent au moins d'isoler certains appareils sensibles d'Internet, en ne leur attribuant aucun alias public. Les appareils isolés seront donc joignables par les autres appareils du réseau local uniquement, ce qui ne les protège pas d'une attaque par transitivité, où un autre appareil possédant un alias public serait infecté et contaminerait à son tour l'entièreté du réseau local.

Concernant les types Address (and Port)-Dependent Mapping, on peut considérer cela comme un apport sécuritaire. En effet, ces types permettent de filtrer les connexions d'appareils qui ne nous ont jamais contacté, ce qui évite de potentielles attaques provenant d'appareils inconnus.

Il est important de noter que ces apports sécuritaires sont tout de fois moins importants que ceux d'un pare-feu, car il n'y a aucune analyse du contenu des paquets ainsi qu'aucun filtrage sur les connexions sortantes [25].

Chaque type de NAT fournit donc, par effet de bord, un certain degré de sécurité [18]. Toutefois, ces apports sécuritaires s'accompagnent de problèmes de connectivité susceptibles de perturber le modèle de communication bout en bout d'Internet.

V. Les NAT, des entraves à la communication

A) Les NAT et le modèle bout-en-bout

1. Le modèle bout en bout : principe fondamental d'Internet

Le modèle bout en bout constitue l'un des piliers fondamentaux d'Internet [1]. Ce modèle repose sur l'idée que la majorité des fonctionnalités de traitement des données doit être située aux extrémités du réseau, c'est-à-dire au niveau des appareils des utilisateurs finaux, plutôt que dans les éléments intermédiaires du réseau. Ainsi, le modèle bout en bout consiste à concentrer "l'intelligence du réseau" non pas au cœur même du réseau mais au niveau de ses extrémités.

En ce sens, le modèle bout en bout renforce la robustesse et la résilience du réseau. En effet, si un élément intermédiaire tombe en panne, les dispositifs d'extrémité peuvent toujours effectuer le traitement nécessaire pour assurer la continuité des communications.

2. Les NAT : des entraves au modèle bout en bout

Le modèle bout en bout est pourtant compromis en présence de NAT. En effet, les NAT sont des éléments d'infrastructures intermédiaires qui jouent pourtant un rôle majeur dans la communication entre deux entités. La présence de NAT fragilise le principe fondamental du modèle bout en bout en dispersant l'intelligence du réseau au-delà de ses extrémités.

Sur ce, contrairement à d'autres composants du réseau tels que les routeurs, dont la panne peut être compensée par des chemins de contournement alternatifs, la défaillance d'un NAT interrompt complètement la communication à travers lui.

B) Les problèmes de connectivité engendrés par les NAT

En plus de casser le modèle bout en bout d'Internet, certains types de NAT engendrent des problèmes de connectivité. Ces problèmes ont notamment lieu lorsqu'un service (par exemple un serveur Web) est hébergé derrière un NAT.

Pour illustrer les effets perturbateurs des différents types de NAT, imaginons qu'une machine M diffuse continuellement du contenu vidéo (streaming vidéo) tout en étant placée derrière un NAT. Tout appareil souhaitant accéder au contenu diffusé doit contacter M sur son adresse IP publique. On distingue alors deux cas de figure :

1. La machine M est derrière un NAT de type *Endpoint-Independent*
2. La machine M se trouve derrière un NAT de type *non-Endpoint-Independent*

D'une part, si la machine M se trouve derrière un NAT de type *Endpoint-Independent*, le NAT lui assigne toujours la même adresse IP publique. Puisque l'adresse IP publique de M reste constante, toute machine peut facilement accéder au contenu en diffusion sans rencontrer de problèmes de connectivité. En d'autres termes, un NAT de type *Endpoint-Independent Mapping* n'engendre pas de problèmes de connectivité.

En revanche, les NAT de type *non-Endpoint-Independent Mapping* attribuent à une même machine plusieurs adresses IP publiques différentes. Ainsi, si la machine M se trouve derrière un NAT de type *non-Endpoint-Independent*, l'adresse IP publique qui lui est attribuée n'est pas fixe. Il est donc impossible pour un appareil de joindre M pour accéder aux services qu'elle propose.

Sur ce, les NAT de type *non-Endpoint-Independent Mapping* constituent des barrières entravantes à la communication. Mais ces barrières ne sont pas nécessairement infranchissables.

VI. Les méthodes de franchissement des NAT

Les problèmes de connectivité engendrés par les NAT ont stimulé l'élaboration de stratégies de franchissement. Les deux méthodes principales pour traverser les NAT sont le « Relaying » et le « Hole Punching » [5].

A) Le Relaying

La méthode du relais vise à franchir les NAT en acheminant toutes les communications entre deux entités à travers un serveur intermédiaire. Pour comprendre le fonctionnement du relaying, considérons le schéma ci-dessous. La machine **Y** est un fournisseur de services (par exemple, un serveur de streaming) se trouvant derrière un NAT. La machine **X**, quant à elle, souhaite accéder au service proposé par **Y**. Nous supposons que les machines **X** et **Y** se trouvent toutes deux derrière des NAT de type non-Endpoint Independent Mapping.

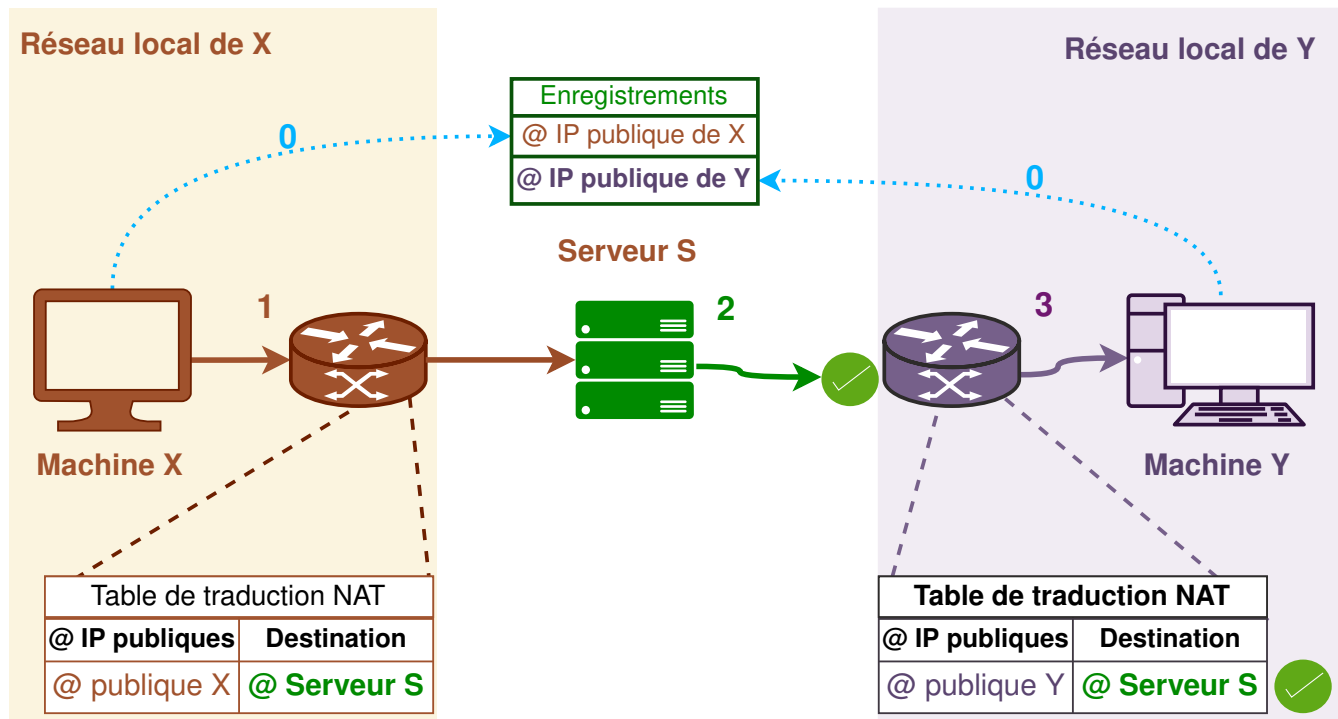


FIGURE 2 – Fonctionnement du relaying

En temps normal, la machine **X** ne peut aucunement joindre la machine **Y** car cette dernière ne possède pas d'adresse IP publique fixe. La méthode du relaying consiste alors à introduire un serveur intermédiaire **S** qui joue le rôle de relais entre **X** et **Y**.

Une précondition est pourtant nécessaire pour que le relaying fonctionne : il faut que les machines **X** et **Y** s'enregistrent préalablement auprès du serveur **S**. Dans le schéma, l'enregistrement est représenté par l'étape 0. Cette étape préliminaire possède deux objectifs : d'une part, permettre au serveur **S** de connaître les adresses IP publiques des machines **X** et **Y**, et d'autre part, de créer une entrée dans la table de NAT de chacune des machines **X** et **Y**.

Une fois cette étape accomplie, la communication peut être établie entre **X** et **Y**. Pour ce faire, la machine **X** envoie au serveur **S** le message qu'elle souhaite transmettre à **Y**. Or, grâce à l'étape préliminaire d'enregistrement, **S** connaît **Y**. Le serveur transmet alors le message envoyé par **X** à la machine **Y**. Enfin,

le NAT de **Y** autorise la communication entrante provenant du serveur car il possède déjà une entrée dans sa table lui correspondant (grâce à l'étape préliminaire d'enregistrement).

Le message de **X** parvient donc bien à **Y** : les NAT ont été traversés.

L'un des principaux avantages de la méthode du relais est qu'elle fonctionne avec tous les types de NAT. Cependant, le passage par un serveur intermédiaire est extrêmement consommateur en ressources matérielles et crée un point de défaillance unique : si le serveur intermédiaire tombe en panne, la communication entre les deux extrémités devient alors impossible.

En pratique, le relaying est implémenté par le protocole "Traversal Using Relays around NAT" ou "TURN" [21]. Toutefois, TURN est considéré comme une solution de dernier recours en raison de la latence qu'il peut introduire. Il existe donc une seconde méthode bien plus efficace qui permet de contourner les NAT : le Hole Punching.

B) Le Hole Punching

Le *Hole Punching* est une méthode de contournement plus sophistiquée que le Relaying, qui sert uniquement à établir la communication entre deux appareils, avant de les laisser communiquer entre eux sans intermédiaire. Néanmoins, elle demande un prérequis, à savoir un serveur intermédiaire qui servira à établir la connexion comme pour le *Relaying*. De même, la condition nécessaire à l'établissement de la connexion est l'acceptation de connexions entrantes venant du serveur **S**, du côté de **X** et de **Y**.

La différence majeure avec le *Relaying* est que le serveur va à présent être utilisé pour donner des instructions aux appareils **X** et **Y**, afin de créer des associations et de passer le filtrage dans le cas de NAT de types Address (and Port)-Dependant Mapping.

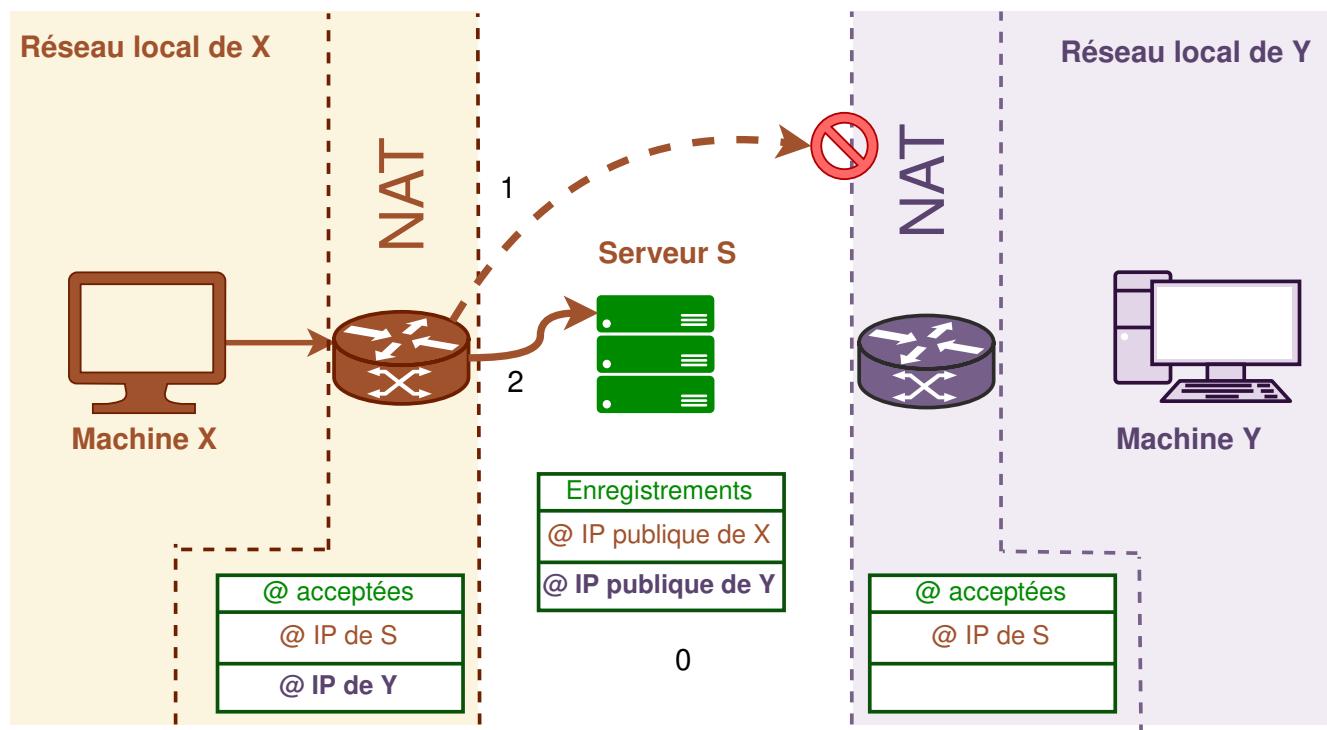


FIGURE 3 – La première étape du Hole Punching

Imaginons que **X** veuille initier la connexion. **X** va alors effectuer deux actions :

- Envoyer un premier paquet vers le serveur **S**, qui contient l’instruction suivante : « Demander à **Y** de contacter **X** »
- Envoyer un deuxième paquet vers la machine **Y**. Ce paquet va évidemment se voir refusé pour l’instant, car il n’y a à cette étape pas d’entrée de **Y** vers **X** dans la table de traduction du NAT derrière lequel se trouve **Y**. L’envoi de ce paquet permet néanmoins à **X** de pouvoir créer une entrée dans la table de son propre NAT. Cela signifie qu’un paquet provenant de **Y** à partir de ce moment serait accepté par **X**. Nous sommes donc pour l’instant dans une connexion asymétrique.

Ensuite, **S** va recevoir le premier paquet et l’instruction correspondante. Il va donc pouvoir contacter **Y**, et vu que le prérequis est qu’**Y** soit enregistré auprès de **S**, le paquet de **S** vers **Y** va être accepté par **Y**. [Figure 3]

Y va ensuite exécuter l’instruction, et donc envoyer un paquet directement vers **X**. Nous venons donc de créer une entrée dans la table de traduction de **Y**, et la connexion est devenue symétrique.

Vu que chacun des appareils possède une entrée dans la table de traduction du NAT opposé, ils peuvent surtout communiquer sans passer par le serveur **S**. Le nom de la méthode prend tout son sens : on crée de force des entrées dans les tables de traduction à l’aide de l’entrée de **S** (on passe par le trou de **S** dans les tables). [Figure 4]

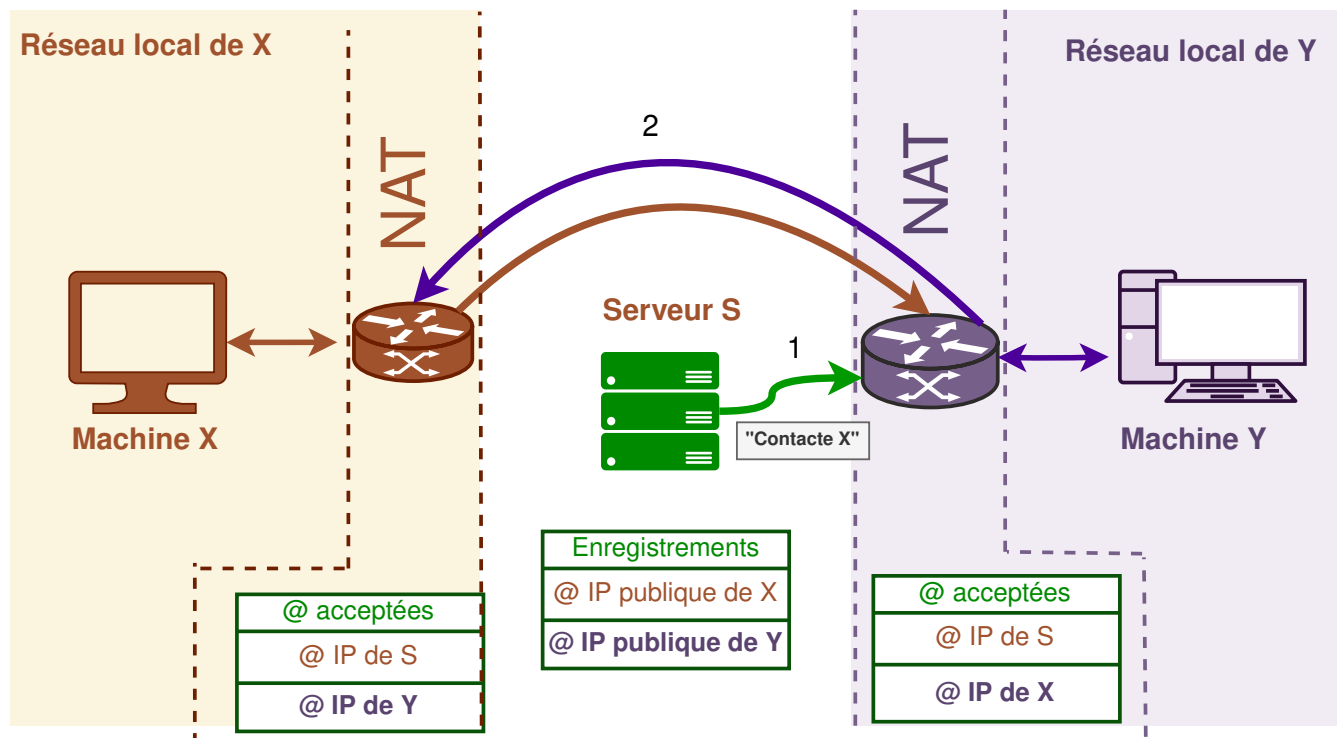


FIGURE 4 – État final du Hole Punching

Malheureusement, dans certains cas cette méthode ne fonctionne pas, ce qui explique donc la raison de l’existence du *Relaying*. C’est notamment le cas si le port et/ou l’adresse de destination de **X** ou de **Y** viennent à changer pendant une communication *Hole Punching*, car le processus doit être reproduit à nouveau. Alors que dans le cas du *Relaying*, il suffit au serveur **S** de réorienter les communications vers la nouvelle adresse.

De plus, le *Hole Punching* nécessite la prise en charge des messages d’instructions provenant de **S**. Ces fonctionnalités sont matérialisées par le protocole « Session Traversal Utilities for NAT » ou « STUN ».

Il est intéressant de noter qu’un protocole regroupant les deux méthodes de *Relaying* et de *Hole Punching* a été créé : il s’agit du « Interactive Connectivity Establishment » ou « ICE » [13][24], qui, concrète-

ment, regroupe *TURN* [21] et *STUN* [23]. Il implémente des fonctionnalités d'identification des adresses candidates pour la transmission des données. On appelle adresses candidates les adresses potentiellement utilisables pour la transmission des données, avec une adresse distincte pour chaque flux de données. Elles sont proposées par chaque machine, ainsi que par le serveur S selon un algorithme explicité dans la norme. *ICE* classe donc ces adresses candidates pour maximiser les chances d'établir une communication [8]. Le protocole *ICE* applique *STUN* en priorité avant de passer à *TURN* si nécessaire.

Ainsi, le Relaying et le Hole Punching permettent de contourner les effets perturbateurs des NAT dans la communication bout-en-bout. Cependant, ces méthodes ne seront éventuellement plus nécessaires car les NAT sont voués à disparaître.

VII. Vers la disparition des NAT ?

On peut distinguer trois scénarios possibles pour le futur des NAT. Tout d’abord, le maintien dans le *statu quo* actuel. Concrètement, cela signifie accorder une place importante à IPv4 et donc continuer vers un épuisement généralisé de ce type d’adresse IP. En effet, rien que dans le Registre Internet Régional Européen (*RIPE NCC*), on observe qu’il n’y a plus d’adresses IPv4 disponibles pour d’éventuels nouveaux fournisseurs d’accès à Internet depuis quelques années [22]. Les seules adresses disponibles sont des adresses réservées. Actuellement, un fournisseur d’accès à Internet a pour unique solution de s’inscrire sur une liste d’attente avec une attente moyenne supérieure à un an, et permettant d’obtenir un maximum de 4 096 adresses seulement.

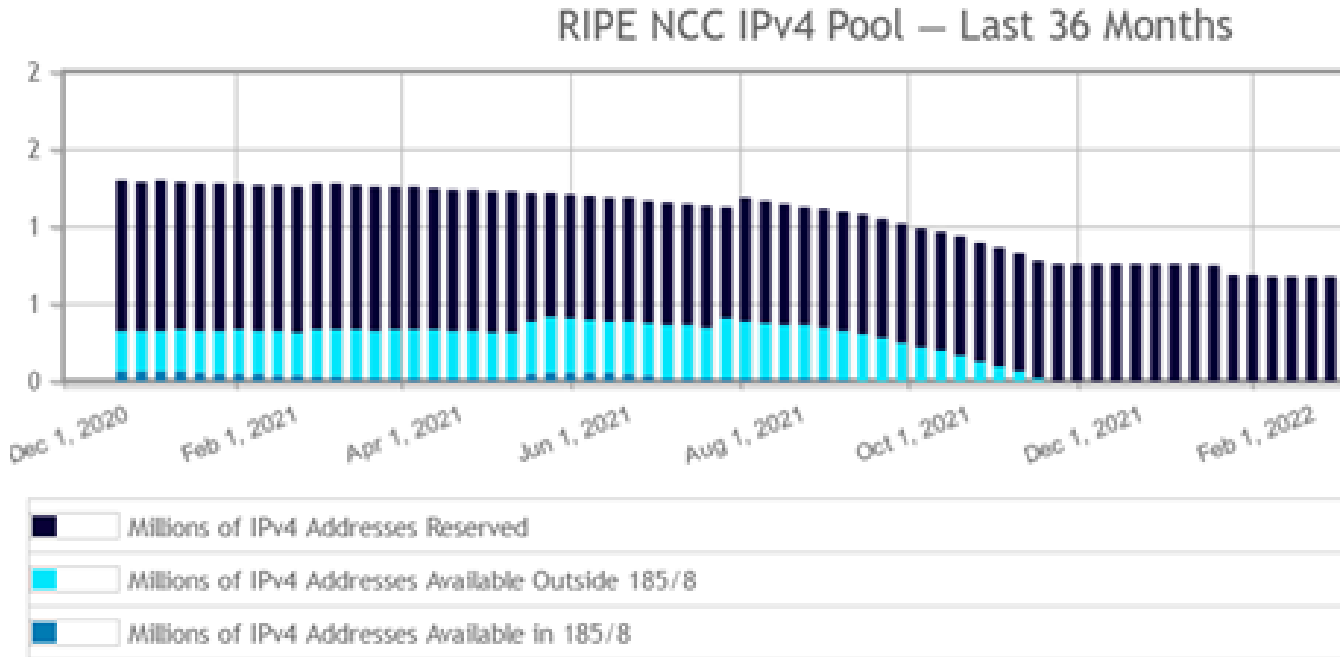


FIGURE 5 – Adresses IPv4 disponibles au sein du registre européen RIPE NCC [22]

C’est une situation qu’on retrouve dans les autres registres régionaux. Dans cette configuration, les NAT sont évidemment indispensables car ils permettent de démultiplier artificiellement le nombre d’adresses IP disponibles. Mais même en ayant chaque client derrière un NAT, les fournisseurs risquent de manquer d’adresses et pourraient recourir à d’autres solutions, comme des NAT au niveau du réseau de l’opérateur (appelés « Carrier-grade NAT ») [14][12].

Une autre piste envisageable serait la migration totale vers IPv6. Etant donné le nombre largement suffisant d’adresses disponibles en IPv6, il n’y aurait aucunement besoin de démultiplier les adresses avec des NAT. De plus, les apports sécuritaires des NAT peuvent totalement être remplacés par les apports d’un pare-feu. D’autant plus qu’un pare-feu peut effectuer un filtrage sur le contenu des paquets, et est un dispositif de sécurité bien plus pertinent que les NAT. On se rend alors compte que, en IPv6, les NAT n’ont plus aucun intérêt et seraient donc amenés à disparaître. Il existe bien des spécifications de NAT en IPv6, mais les cas où il est utile de les implémenter sont faibles.

Il reste enfin l’entre deux : la cohabitation de réseaux IPv4 et IPv6, et l’utilisation de méthodes d’interconnexions entre ces deux versions, à travers des protocoles dédiés et à travers des NAT qui peuvent faire la traduction d’adresses IPv4 vers IPv6 ou inversement.

La trajectoire qui se réalisera dépend évidemment de l'adoption ou non d'IPv6 par le grand public, les entreprises et les fournisseurs d'accès à Internet. D'après Google, la connexion aux services de l'entreprise via IPv6 est grandissante, avec néanmoins de grandes disparités entre les pays.

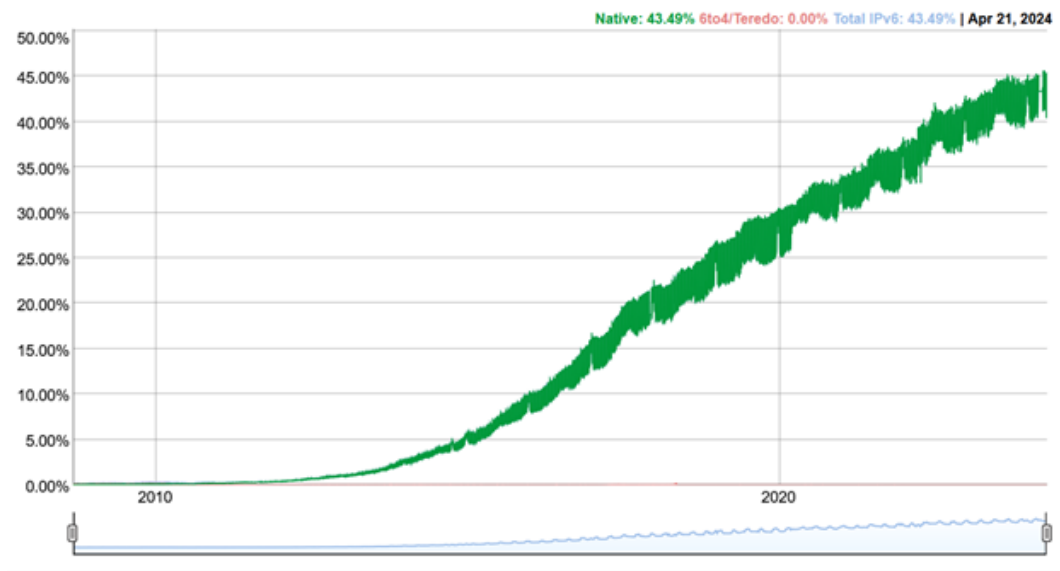


FIGURE 6 – Schéma représentant l'adoption d'IPv6 parmi les utilisateurs des services de Google [9]

Si on suit la trajectoire actuelle, on peut se projeter à moyen terme sur une cohabitation entre IPv4 et IPv6 et l'utilisation de méthodes d'interconnexions, et à long terme sur une marginalisation d'IPv4 (voire une disparition) et une domination d'IPv6. Cela acterait donc probablement la fin de l'utilisation des NAT à grande échelle.

VIII. Conclusion

En conclusion, les NAT sont des dispositifs de traduction conçus pour provisoirement pallier le manque d'adresses IPv4. Il existe trois types de NAT qui engendrent des apports sécuritaires mais aussi des problèmes de connectivité différents. Ce comportement dual transforme les NAT en des barrières à la fois protectrices mais surtout entravantes.

Les apports sécuritaires des NAT sont pourtant à relativiser. En effet, les NAT sont avant tout des traducteurs d'adresses dont l'objectif principal est de pallier l'épuisement des adresses IPv4 et non de protéger un réseau : ils ne remplacent donc aucunement des dispositifs sécuritaires tels les pare-feux.

Par ailleurs, le mécanisme des NAT de type non-Endpoint-Independent engendre des problèmes de connectivité non négligeables. Il existe pourtant des moyens pour contourner ces barrières entravantes : les NAT ne sont donc pas infranchissables. Les deux méthodes de contournement principales sont, d'une part le Relaying, et d'autre part, le Hole Punching.

Cependant, ces méthodes de contournement ne seront éventuellement plus nécessaires car les NAT semblent voués à disparaître. En effet, les NAT constituent avant tout des solutions provisoires qui combleront le manque d'adresses IPv4 en attendant l'essor de solutions durables. Or, une solution pérenne est aujourd'hui déjà disponible : le protocole IPv6. Si le réseau mondial migre entièrement vers IPv6, les barrières traductrices s'écrouleront et l'on ne bénéficiera plus des apports sécuritaires minimaux des NAT.

Ce projet a non seulement élargi nos connaissances au niveau académique, mais a également favorisé notre développement personnel. En effet, cette unité d'enseignement a mis en lumière l'importance du travail d'équipe, de la synthèse et surtout de l'organisation.

Nous avons appris à collaborer efficacement, à partager nos idées et à intégrer les perspectives de chacun pour mener à bien nos recherches. Nous avons également appris l'importance de sélectionner soigneusement les informations pertinentes tout en écartant celles qui peuvent sembler déroutantes. En effet, nous avons dû faire preuve de discernement en écartant certains livres qui présentaient les NAT comme des dispositifs de sécurité à part entière. De même, nous avons traversé des moments de remise en question, et avons appris à prendre de la hauteur et observer le problème d'un autre angle. Cette capacité à évaluer de manière critique les sources d'information nous a permis de garantir la fiabilité et la pertinence de nos recherches, renforçant ainsi la crédibilité de notre travail.

Enfin, cette expérience nous a permis de développer notre esprit critique, de nourrir notre curiosité intellectuelle tout en survolant le monde passionnant de la recherche.

Bibliographie

- [1] Brian E. CARPENTER. *Internet Transparency*. Request for Comments RFC 2775. Num Pages : 18. Internet Engineering Task Force, fév. 2000. DOI : 10.17487/RFC2775. URL : <https://datatracker.ietf.org/doc/rfc2775> (visité le 19/05/2024).
- [2] José DORDOIGNE. *Réseaux informatiques Notions fondamentales (9e édition) - (Protocoles, Architectures, Réseaux sans fil...)* Editions ENI, 2022. 804 pages. ISBN : 978-2-409-03517-3.
- [3] Kjeld Borch EGEVANG et Paul FRANCIS. *The IP Network Address Translator (NAT)*. Request for Comments RFC 1631. Num Pages : 10. Internet Engineering Task Force, mai 1994. DOI : 10.17487/RFC1631. URL : <https://datatracker.ietf.org/doc/rfc1631> (visité le 29/03/2024).
- [4] Kjeld Borch EGEVANG et Pyda SRISURESH. *Traditional IP Network Address Translator (Traditional NAT)*. Request for Comments RFC 3022. Num Pages : 16. Internet Engineering Task Force, jan. 2001. DOI : 10.17487/RFC3022. URL : <https://datatracker.ietf.org/doc/rfc3022> (visité le 29/03/2024).
- [5] Bryan FORD, Dan KEGEL et Pyda SRISURESH. *State of Peer-to-Peer (P2P) Communication across Network Address Translators (NATs)*. Request for Comments RFC 5128. Num Pages : 32. Internet Engineering Task Force, mars 2008. DOI : 10.17487/RFC5128. URL : <https://datatracker.ietf.org/doc/rfc5128> (visité le 29/03/2024).
- [6] Bryan FORD et al. *NAT Behavioral Requirements for TCP*. Request for Comments RFC 5382. Num Pages : 31. Internet Engineering Task Force, oct. 2008. DOI : 10.17487/RFC5382. URL : <https://datatracker.ietf.org/doc/rfc5382> (visité le 29/03/2024).
- [7] Saikat GUHA et al. *NAT Behavioral Requirements for ICMP*. Request for Comments RFC 5508. Num Pages : 29. Internet Engineering Task Force, avr. 2009. DOI : 10.17487/RFC5508. URL : <https://datatracker.ietf.org/doc/rfc5508> (visité le 29/03/2024).
- [8] Christer HOLMBERG et Justin UBERTI. *Interactive Connectivity Establishment Patiently Awaiting Connectivity (ICE PAC)*. Request for Comments RFC 8863. Num Pages : 6. Internet Engineering Task Force, jan. 2021. DOI : 10.17487/RFC8863. URL : <https://datatracker.ietf.org/doc/rfc8863> (visité le 03/04/2024).
- [9] *IPv6 – Google*. URL : <https://www.google.fr/ipv6/statistics.html#tab=ipv6-adoption> (visité le 23/04/2024).
- [10] *IPv6 – Google*. IPv6 – Google. URL : <https://www.google.fr/ipv6/statistics.html#tab=ipv6-adoption> (visité le 23/04/2024).

- [11] Cullen Fluffy JENNINGS et Francois AUDET. *Network Address Translation (NAT) Behavioral Requirements for Unicast UDP*. Request for Comments RFC 4787. Num Pages : 29. Internet Engineering Task Force, jan. 2007. DOI : 10.17487/RFC4787. URL : <https://datatracker.ietf.org/doc/rfc4787> (visité le 29/03/2024).
- [12] Orestis KANARIS et Johan POUWELSE. *Mass Adoption of NATs : Survey and experiments on carrier-grade NATs*. 15 nov. 2023. arXiv : 2311.04658[cs]. URL : <http://arxiv.org/abs/2311.04658> (visité le 29/03/2024).
- [13] Ari KERÄNEN, Christer HOLMBERG et Jonathan ROSENBERG. *Interactive Connectivity Establishment (ICE) : A Protocol for Network Address Translator (NAT) Traversal*. Request for Comments RFC 8445. Num Pages : 100. Internet Engineering Task Force, juill. 2018. DOI : 10.17487/RFC8445. URL : <https://datatracker.ietf.org/doc/rfc8445> (visité le 03/04/2024).
- [14] Ioana LIVADARIU et al. "Inferring Carrier-Grade NAT Deployment in the Wild". In : *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications*. IEEE INFOCOM 2018 - IEEE Conference on Computer Communications. Avr. 2018, p. 2249-2257. DOI : 10.1109/INFOCOM.2018.8486223. URL : <https://ieeexplore.ieee.org/document/8486223> (visité le 29/03/2024).
- [15] Philip MATTHEWS, Jonathan ROSENBERG et Rohan MAHY. *Traversal Using Relays around NAT (TURN) : Relay Extensions to Session Traversal Utilities for NAT (STUN)*. Request for Comments RFC 5766. Num Pages : 67. Internet Engineering Task Force, avr. 2010. DOI : 10.17487/RFC5766. URL : <https://datatracker.ietf.org/doc/rfc5766> (visité le 03/04/2024).
- [16] Christian JACQUENET MOHAMED BOUCADAI. *Contrôle dynamique de ressources Internet*. Techniques de l'Ingénieur. 10 nov. 2014. URL : <https://www-techniques-ingenieur-fr.scd-rproxy.u-strasbg.fr/base-documentaire/technologies-de-l-information-th9/administration-de-reseaux-applications-et-mise-en-oeuvre-42481210/controle-dynamique-de-ressources-internet-te7612/> (visité le 29/03/2024).
- [17] Robert MOSKOWITZ et al. *Address Allocation for Private Internets*. Request for Comments RFC 1918. Num Pages : 9. Internet Engineering Task Force, fév. 1996. DOI : 10.17487/RFC1918. URL : <https://datatracker.ietf.org/doc/rfc1918> (visité le 29/03/2024).
- [18] *Notice détaillée norme*. Sécurité de l'information, cybersécurité et protection de la vie privée - Systèmes de management de la sécurité de l'information - Exigences. Juill. 2023. URL : <https://cobaz-afnor-org.scd-rproxy.u-strasbg.fr/notice/norme/nf-en-iso-iec-27001/FA206487?rechercheID=22800293&searchIndex=1&activeTab=all> (visité le 17/04/2024).
- [19] Reinaldo PENNO et al. *Updates to Network Address Translation (NAT) Behavioral Requirements*. Request for Comments RFC 7857. Num Pages : 14. Internet Engineering Task Force, avr. 2016. DOI : 10.17487/RFC7857. URL : <https://datatracker.ietf.org/doc/rfc7857> (visité le 29/03/2024).
- [20] Simon PERREAULT et al. *Common Requirements for Carrier-Grade NATs (CGNs)*. Request for Comments RFC 6888. Num Pages : 15. Internet Engineering Task Force, avr. 2013. DOI : 10.17487/RFC6888. URL : <https://datatracker.ietf.org/doc/rfc6888> (visité le 29/03/2024).

- [21] Tirumaleswar REDDY.K et al. *Traversal Using Relays around NAT (TURN) : Relay Extensions to Session Traversal Utilities for NAT (STUN)*. Request for Comments RFC 8656. Num Pages : 79. Internet Engineering Task Force, fév. 2020. DOI : 10.17487/RFC8656. URL : <https://datatracker.ietf.org/doc/rfc8656> (visité le 19/05/2024).
- [22] *RIPE NCC IPv4 Pool*. RIPE NCC IPv4 Pool. URL : <https://www.ripe.net/manage-ips-and-asns/ipv4/ipv4-pool/> (visité le 23/04/2024).
- [23] Jonathan ROSENBERG et al. *STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)*. Request for Comments RFC 3489. Num Pages : 47. Internet Engineering Task Force, mars 2003. DOI : 10.17487/RFC3489. URL : <https://datatracker.ietf.org/doc/rfc3489> (visité le 03/04/2024).
- [24] Jonathan ROSENBERG et al. *TCP Candidates with Interactive Connectivity Establishment (ICE)*. Request for Comments RFC 6544. Num Pages : 29. Internet Engineering Task Force, mars 2012. DOI : 10.17487/RFC6544. URL : <https://datatracker.ietf.org/doc/rfc6544> (visité le 03/04/2024).
- [25] Claude SERVIN. *Réseaux & télécoms*. 4^e éd. DUNOD. 800 p. ISBN : 978-2-10-059258-6.
- [26] *Transmission Control Protocol*. Request for Comments RFC 793. Num Pages : 91. Internet Engineering Task Force, sept. 1981. DOI : 10.17487/RFC0793. URL : <https://datatracker.ietf.org/doc/rfc793> (visité le 29/03/2024).