NAT

Différentes méthodes de translation d’adresse

Sommaire

De quoi s'agit-il ?

Introduction

Contexte

La problématique du NAT n'intervient que pour les adresses IPv4. Dans ce cours, la notation **IP** veut donc dire implicitement **IPv4**.

Le NAT est un mécanisme quasi-exclusif à l'IPv4.

En IPv6 il existe malgré tout le NPTv6.

Problématique des adresses IP privées

Un réseau interne utilise des **adresses IP privées** (RFC 1918) :

- 10.0.0.0/8 -> 10.0.0.0 à 10.255.255.255
- 172.16.0.0/12 -> 172.16.0.0 à 172.31.255.255
- 192.168.0.0/16 -> 192.168.0.0 à 192.168.255.255

=> Adresses non-routables sur Internet.

Problématique des adresses publiques

Il faut permettre :
- L'accès à Internet
- La publication de services

=> Adresses IP publiques
Attribution par l'**ICANN** -> **RIR** (RIPE NCC pour l'Europe) -> **LIR** etc.

Problématique des adresses publiques (suite)

IPv4 fournit environ $4{,}3.10^9$ adresses.

- Explosion du nombre d'équipements connectés
- Les adresses IPv4 publiques sont devenues "rares"

Le NAT apparaît comme une solution transitoire à la pénurie d'adresses IPv4 en attendant le déploiement d'IPv6.

Définition

Le **NAT** (*Network Address Translation*) permet de traduire une adresse IP.
Il fait la jonction entre :
- Un réseau privé LAN contenant des adresses IP privées
- Un réseau public WAN contenant des adresses IP publiques

Le NAT est généralement mis en place sur un routeur ou un pare-feu.

Définition (suite)

On qualifie parfois ce mécanisme de **masquage** (*masquerade*) d'adresse car il cache une adresse interne à un réseau externe.

NAT existe en plusieurs variantes et est défini notamment dans la RFC 3022.

Objectifs

Historiquement, NAT était utilisé pour cacher son plan d'adressage interne.

Aujourd'hui, il est massivement utilisé pour combler le manque d'adresses IPv4 publiques.
=> **Une seule adresse publique** utilisée par **des** machines clientes.

Masquer son plan d'adressage

Exemple avec 2 organisations qui ont chacune leur réseau.

- Chacune a un plan d'adressage IPv4 (probablement en RFC 1918)
- Elles décident d'interconnecter leurs réseaux
- Il est très probable que leurs plans d'adressage soient incompatibles => utilisation des mêmes plages d'adresses

Problématique :
Connecter les 2 réseaux des 2 entreprises.Solution 1 : Faire du routage

Masquer son plan d'adressage (suite)

Solution 1 : Faire du routage
Certaines plages réseaux se trouvent à plusieurs endroits => des adresses sont identiques des 2 côtés.
=> Impossibilité technique de connecter les 2 réseaux avec du routage.

Masquer son plan d'adressage (suite)

Solution 2 : Faire du routage avec du NAT
Mettre du NAT sur le routeur d'interconnexion permet donc de rendre les réseaux compatibles en masquant les adresses incompatibles.

Exemple sur un routeur

Les mécanismes de traduction d'adresses réseaux permettent à un routeur de modifier les paquets IP au moment de leur transmission.

Ils visent à remplacer une adresse IP (**source** ou **destination**) par une autre pour substituer à une adresse valable sur le réseau interne (**privée**) une autre adresse valable sur un autre réseau (par exemple **publique** sur Internet).

Principes de fonctionnement

Critères

Il existe 3 critères :

- Le sens de traduction -> Quelle adresse est modifiée ?
- Le mode d’association -> Comment la traduction est-elle établie ?
- Le niveau de traduction -> Qu’est-ce qui est traduit ?

Ils peuvent être combinés pour former différents types de NAT.

Sens de traduction - NAT source

NAT source :
- L’adresse source est traduite
- Typiquement lors d’une sortie vers Internet

Traduction de l’adresse (et éventuellement du port) du client.
Utilisé pour la sortie vers Internet.
Cas le plus classique (**PAT/NAPT**).

Sens de traduction - NAT destination

NAT destination :
- L’adresse de destination est traduite
- Typiquement pour publier un service

Traduction de l’adresse (et éventuellement du port) du serveur.
Utilisé pour la publication de services.
⇒ **DNAT/Port forwarding**

Mode d’association - Statique

Statique :
- Association fixe
- Connue à l’avance
- Ne change pas

Souvent pour des serveurs.

Mode d’association - Dynamique

Dynamique :
- Association temporaire
- Créée à la demande
- Expiration après délai

Souvent pour des clients.

Niveau de traduction - Adresse IP

Adresse IP :

- Traduction simple
- 1 @IP interne ⟷ 1 @IP externe

Souvent appelé :

- **NAT simple**
- **NAT 1:1**

Niveau de traduction - Adresse IP & port

Adresse IP + port :
- Traduction plus fine
- Plusieurs flux via une même @IP publique

Souvent appelé **PAT** ou **NAPT** => NAT avec traduction de port.

PAT/NAPT

NAPT/PAT

NAPT (*Network Address and Port Translation*) :
➡ Traduction de l'adresse IP et du port (en sortie et au retour)

PAT (*Port address Translation*)
➡ C'est le port qui joue un rôle déterminant

Autres noms :
- **NAT overload**
- **NAT masquerade** (Linux / Netfilter / iptables / nftables)
- **SNAT avec ports (Source Network Address Translation)** (pfSense, Stormshield, Palo Alto)

Définition

Traduction dynamique de plusieurs flux internes (adresse IP et port) vers une seule IP publique - RFC 2663
Les ports servent à différencier les communications.

Le sens de traduction ➡ Source
Le mode d'association ➡ Dynamique
Le niveau de traduction ➡ @IP + port

Usage :
- Un des NAT les plus utilisés à cause de la pénurie d'@IP v4
- Fournir un accès Internet à des machines clientes

Exemple

Exemple : un routeur a une adresse publique 203.1.113.123 (IP WAN) :

- La machine interne (**10.1.1.11**) accède à Odyssey (**216.58.214.83**)
- Communication HTTPS, donc port Serveur = 443 et port client dynamique (ex : 52369)
- Requête de **10.1.1.11**:52369 (port) vers **216.58.214.83**:443

Le routeur note dans sa table PAT “interne ⇔ externe” :
10.1.1.11:52369 ⇔ 203.1.113.123:52369

Interne			Externe	
Adresse source	Port source	Routeur →	Adresse destination	Port destination
10.1.1.11	52369	203.1.113.123	**216.58.214.83**	443

Exemple (suite)

Traduction sortante :
Requête transmise par le routeur sur Internet :
203.1.113.123:52369 ➡ **216.58.214.83**:443

Le routeur remplace l'adresse source et le port source avant l'envoi vers Internet.

Interne			Externe	
Adresse source	Port source	Routeur →	Adresse destination	Port destination
10.1.1.11	52369	203.1.113.123	216.58.214.83	443

Exemple (suite)

Suite de l'exemple (retour) : Odyssey (**216.58.214.83**) reçoit une requête de 203.1.113.123 et réponds :

- Réponse de **216.58.214.83**:443 ➡ 203.1.113.123:52369
- Le routeur reçoit cette réponse pour lui MAIS il fait du NAT :
  - Le routeur cherche dans sa table une correspondance pour le port 52369 et trouve **10.1.1.11** ⇒ le routeur se base sur le port
  - Il transmet donc sur le réseau interne le paquet en remplaçant l'adresse de destination (la sienne) par **10.1.1.11**

Interne			Externe	
Adresse source	Port source	Routeur ←	Adresse destination	Port destination
10.1.1.11	52369	203.1.113.123	**216.58.214.83**	443

Remarque

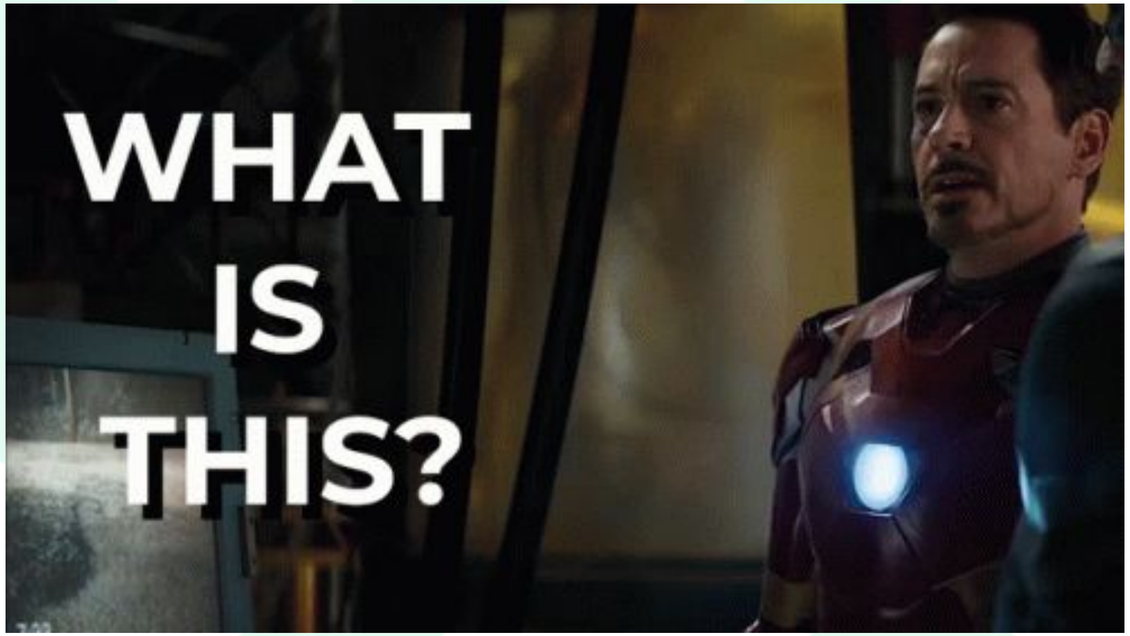
Si le port source était déjà utilisé dans la table de correspondance, par une autre machine interne par exemple (**collision de ports**) ?

⇒ Modification aussi du port source (et donc traduction aussi du port).
En reprenant l'exemple, le routeur choisit un autre port source disponible (ex : 52370).
⇒ C'est aussi pour ça que l'on parle de **PAT** (*Port Address Translation*).

Inconvénients

- La table étant remplie lors de la requête de l'intérieur vers l'extérieur :
  - Le client doit être derrière le NAT
  - Impossible d'avoir un serveur interne (sans DNAT ou port forwarding)
- Le paquet IP (L3) et le protocole de niveau 4 (L4) sont modifiés :
  - Lourd: nécessite un recalcul des checksum
  - Pas possible avec tous les protocoles de couche 4
  - Incompatible avec certains protocoles, par ex. FTP actif (explications)
  - Incompatible avec certains contrôle d'intégrité
- Tord le Principe de bout en bout

DNAT



DNAT

DNAT (*Destination Network Address Translation*) :
➡ Traduction de l'adresse IP et du port (en sortie et au retour)

Autre nom :
- **Static DNAT** (sans changement de port)
- **Port forwarding** (avec changement de port)

Définition

Traduction statique de l'adresse IP de destination (et éventuellement du port destination) pour rediriger une communication entrante vers une machine interne.

Le sens de traduction ➡ Destination
Le mode d'association ➡ Statique
Le niveau de traduction ➡ @IP (+ éventuellement port)

Usage :
- Utilisé uniquement lorsque des services sont exposés
- Publication de services internes (HTTP, HTTPS, RDP, FTP, etc.)

Exemple

Exemple : un routeur a une adresse publique 203.1.113.123 (IP WAN) :

- Une machine externe (**204.1.97.10**) veut se connecter à un serveur sur un réseau interne (**172.16.1.15**)
- Communication HTTP :
  - Port Serveur (destination) = 80
  - Port client dynamique = par exemple 57221
- Requête entrante de **204.1.97.10**:57221 vers 203.1.113.123:**80**

Le routeur note dans sa table DNAT “interne ⇔ externe” :

172.16.1.15:80 ⇔ 203.1.113.123:**80**

Interne Externe

Adresse destination	Port destination	Routeur ←	Adresse source	Port source
172.16.1.15	80	203.1.113.123:**80**	**204.1.97.10**	57221

Exemple (suite)

Traduction entrante :

Requête reçue par le routeur : **204.1.97.10**:57221 ➡ 203.1.113.123:**80**

Le routeur effectue une traduction de destination :

- Adresse de destination : 203.1.113.123 ➡ **172.16.1.15**
- Port de destination : **80** ➡ 80

Requête transmise en interne : **204.1.97.10**:57221 ➡ **172.16.1.15**:80

Interne			Externe	
Adresse destination	Port destination	Routeur	Adresse source	Port source
172.16.1.15	80	203.1.113.123:**80**	**204.1.97.10**	57221

Exemple (suite)

Pour le retour, le serveur interne **172.16.1.15** répond :

- Réponse de **172.16.1.15**:80 ➡ **204.1.97.10**:57221

Le routeur reçoit la réponse et fait une traduction **inverse DNAT** :

- Adresse source remplacée : **172.16.1.15** → 203.1.113.123
- Port source conservé : 80

Réponse envoyée vers l'ext. : 203.1.113.123:**80** ➡ **204.1.97.10**:57221

Interne			Externe	
Adresse destination	Port destination	Routeur →	Adresse source	Port source
172.16.1.15	80	203.1.113.123:**80**	**204.1.97.10**	57221

Remarque

Le DNAT peut :
- Traduire uniquement l’adresse IP
- Ou traduire adresse IP + port

Plusieurs services peuvent être publiés sur une même IP publique à condition d’utiliser des ports différents.

Remarque (suite)

Exemple un serveur qui a 2 rôles RDP (3389) et HTTP (80) :

Interne			Externe	
Adresse destination	Port destination	Routeur ←	Adresse source	Port source
172.16.1.15	80	203.1.113.123:**80**	204.1.97.10	51456
172.16.1.15	3389	203.1.113.123:**3389**	227.7.6.182	54816

Inconvénients

- Expose des services internes vers l’extérieur. Nécessite :
  - Règles de pare-feu strictes
  - Durcissement des serveurs
- Rupture du principe de bout en bout
- Peut poser des problèmes avec certains protocoles applicatifs

NAT 1:1

NAT 1:1

NAT 1:1 (*One-to-One Network Address Translation*) :
➡ Traduction statique d'une adresse IP privée vers une adresse IP publique dédiée, dans les deux sens (aller et retour).

Autre nom :
- **Static NAT**

Définition

Permet d'attribuer une adresse IP publique dédiée à un serveur interne.

Le sens de traduction ➡ Source et Destination
Le mode d'association ➡ Statique
Le niveau de traduction ➡ @IP

Usage : Rendre un serveur joignable sur Internet.
Concrètement : serveur en DMZ.

Exemple

Exemple :
- @IP serveur interne : **172.16.1.20**
- @IP publique attribuée : **203.1.113.50** (IP WAN)
- Services hebergés : HTTP (80), HTTPS (443), RDP (3389)

NAT 1:1 configuré sur le routeur : **172.16.1.20** ⇔ **203.1.113.50**

Interne	Externe
172.16.1.20	**203.1.113.50**

Exemple (suite)

Traduction sortante :

Requête transmise vers le routeur :

172.16.1.20:443 ➡ 203.1.113.123:443

Les ports ne changent pas.

L'adresse source est remplacée : 172.16.1.20 ➡ **203.1.113.50**

Requête transmise par le routeur sur Internet :

203.1.113.50:443 ➡ 216.58.214.83:443

Interne			Externe		
Adresse source	Port source	Routeur →	Adresse publique dédiée	Adresse destination	Port destination
172.16.1.20	443	203.1.113.123	**203.1.113.50**	216.58.214.83	443

Exemple (suite)

Traduction entrante :

Réponse reçue sur le routeur :

216.58.214.83:443 ➡ **203.1.113.50**:443

Les ports ne changent pas.

Traduction inverse : **203.1.113.50** ➡ **172.16.1.20**

Requête transmise vers le serveur interne :

216.58.214.83:443 ➡ **172.16.1.20**:443

Interne			Externe		
Adresse source	Port source	Routeur ←	Adresse publique dédiée	Adresse destination	Port destination
172.16.1.20	443	203.1.113.123	**203.1.113.50**	216.58.214.83	443

Particularité

Tous les ports sont accessibles :
- HTTP (80)
- HTTPS (443)
- RDP (3389), etc.

Le port forwarding n’est pas nécessaire.
Pas de multiplexage de ports.

Inconvénients

- Consommation d’une @IP publique par machine
- Expose directement les serveurs :
  - Nécessite un pare-feu strict
- Rupture du principe de bout en bout

Aller plus loin

Serveur derrière NAT

Pour héberger un serveur derrière un NAT, il faut mettre en place une correspondance statique.
Ce genre de correspondance est un **port forwarding**.
Elle consiste à déclarer un port sur le routeur NAT et à lui associer une adresse interne (et éventuellement un port).

Serveur derrière NAT (suite)

Ex : Un serveur web - les ports 80 (TCP) et 443 (TCP) doivent être rediriger vers l'adresse interne du serveur.

Limite : dans le cas de plusieurs serveurs pour le même service, seul un d'entre eux pourra utiliser le port standard.

Depuis l'extérieur

L'utilisation de NAT implique qu'une adresse IP est utilisée par plusieurs interfaces de manière transparente.

Dans le cas ou un serveur (ou un équipement réseau) considère qu'un trafic réseau est abusif (Surconsommation, spam, comportement suspect).
Il est fréquent qu'il réagisse en bloquant l'adresse.

Problème : plusieurs utilisateurs viennent d'être bloqué d'un coup, y compris ceux qui était légitime.

Traverser des NAT

Pour permettre la traversée de NAT à certains protocoles incompatibles ou éviter d'exiger des configurations réseaux aux particuliers, plusieurs techniques ont été mise au point pour pouvoir traverser des NAT

Une première approche de ces techniques peut être consulter sur la page NAT traversal sur Wikipedia (🇬🇧).

En résumé

A retenir

NAT est indispensable pour permettre de continuer à utiliser IPv4.
Il est notamment utiliser sur les box des particuliers.
Mais il est souvent déployé à plus large échelle, par exemple directement sur le réseau d'un opérateur (voir Carrier-grade NAT).

Mais NAT introduit beaucoup de problème.

Avec IPv6, NAT existe encore, mais n'est plus indispensable.

Une autre raison pour accélérer son déploiement ?

MERCI

pour votre participation.

C’est à vous maintenant.
Des questions ?
Des remarques ?