

NAT & PAT

Le **NAT (Network Address Translation)** est un mécanisme permettant de modifier les adresses IP contenues dans les paquets IP lorsqu'ils traversent un équipement réseau (routeur, firewall).

Il est principalement utilisé pour permettre à des hôtes en **adresse privée (RFC 1918)** d'accéder à un réseau extérieur, généralement **Internet** en traduisant une **IP privée** en une **IP publique**.

Le **PAT (Port Address Translation)** est une variante du **NAT** dont le rôle est d'effectuer la traduction non seulement de l'adresse IP, mais également du numéro de port source.

C'est la forme de NAT la plus déployée aujourd'hui.

Objectifs du NAT/PAT

- Extension du plan d'adressage IPv4 : réduction de la consommation d'adresses publiques.
- Sécurisation : les adresses internes ne sont pas directement exposées.
- Simplification de l'architecture : centralisation de la communication externe sur une ou quelques adresses publiques.
- Contrôle des flux : permet d'ajouter des mécanismes de filtrage et de suivi des sessions.

Types de NAT

3.1 NAT statique

Association fixe 1:1 entre une adresse privée et une adresse publique.

Usage : exposition d'un serveur interne (web, mail, VoIP) vers l'extérieur.

Avantage : visibilité externe stable.

Limite : consomme une IP publique par hôte exposé.

3.2 NAT dynamique

Association 1:N permettant à plusieurs hôtes privés d'utiliser un pool d'adresses publiques.

L'adresse est allouée de manière temporaire lors de l'établissement de la session.

Avantage : permet de gérer plusieurs hôtes avec plusieurs IP publiques.

Limite : nécessite un pool suffisant.

3.3 PAT (NAT overload)

Toutes les machines privées partagent **une seule adresse publique**, différenciées grâce aux **ports source** modifiés dynamiquement.

Exemple simplifié :

- 192.168.1.10:40001 → 203.0.113.5:51010
- 192.168.1.11:50020 → 203.0.113.5:51011

Avantage : très économique en IP, très largement utilisé (routeurs domestiques, PME).

Limite : certaines applications complexes (VoIP, FTP actif) peuvent nécessiter des configurations spécifiques.

Fonctionnement interne

Le routeur ou firewall génère une entrée par session sortante, contenant :

- IP source interne
- Port source interne
- IP source publique assignée
- Port source public assigné
- Protocole (TCP/UDP)
- Durée de vie de l'entrée

Processus de traduction

1. Le paquet sortant arrive sur l'interface **inside**.
2. Le routeur vérifie s'il correspond à une règle NAT/PAT.
3. Le champ **IP source** (et éventuellement le **port source**) est remplacé.
4. Le checksum est recalculé.
5. Le paquet est envoyé vers l'interface **outside**.
6. À la réponse, le routeur utilise la table de traduction pour rétablir les valeurs internes.

Ce qui se passe VRAIMENT

Imaginons 3 PC en même temps :

- PC1 : 192.168.1.10:125
- PC2 : 192.168.1.11:125
- PC3 : 192.168.1.12:125

Ils peuvent tous utiliser le port 125, aucun souci.

Le routeur PAT fait ça :

Il a **UNE seule IP publique**, par exemple : **203.0.113.5**

Il transforme chaque flux comme ça :

- 192.168.1.10:125 → 203.0.113.5:51001
- 192.168.1.11:125 → 203.0.113.5:51002
- 192.168.1.12:125 → 203.0.113.5:51003

Table PAT :

- 51001 ↔ 192.168.1.10:125
- 51002 ↔ 192.168.1.11:125
- 51003 ↔ 192.168.1.12:125

LE DÉCLIC (très important)

À l'extérieur, on voit seulement :

- 203.0.113.5:51001
- 203.0.113.5:51002
- 203.0.113.5:51003

→ **Une seule IP publique**

→ **Des ports différents**

→ Donc le routeur sait à qui renvoyer chaque réponse

Résumé essentiel

- **NAT** = translation d'adresses entre un réseau interne et externe.
- **PAT** = translation d'adresses + de ports, permettant à plusieurs hôtes de partager une IP publique.
- **Très utilisé en IPv4**, rendu moins nécessaire en IPv6 mais toujours présent dans les infrastructures actuelles.