Le NAT et le PAT

Documentation rédigée par : GADONNAUD Ewen

Formation : BTS SIO 1ère année - Option SISR

Établissement : Lycée Paul-Louis Courier, Tours

Date : Mars 2026

1. Pourquoi le NAT ?

Les adresses IPv4 publiques sont une ressource limitée. Le NAT (Network Address Translation) a été conçu pour pallier cette pénurie en permettant à plusieurs équipements d'un réseau privé de partager une ou plusieurs adresses IP publiques pour accéder à Internet.

Sans NAT, chaque équipement aurait besoin de sa propre adresse IP publique — ce qui est impossible à l'échelle mondiale avec les ~4 milliards d'adresses IPv4 disponibles.

Avec le NAT, un routeur en bordure de réseau traduit les adresses privées (RFC 1918) en adresses publiques lors du passage vers Internet, et effectue l'opération inverse pour le trafic retour.

Plages d'adresses privées (RFC 1918) :

Plage	Masque	Utilisation courante
10.0.0.0 – 10.255.255.255	/8	Grandes entreprises
172.16.0.0 – 172.31.255.255	/12	Entreprises moyennes
192.168.0.0 – 192.168.255.255	/16	Réseaux domestiques / PME

2. Les types de NAT

Type	Description	Cas d'usage
NAT statique	1 IP privée ↔ 1 IP publique fixe	Serveur accessible depuis Internet
NAT dynamique	Pool d'IPs publiques partagé entre plusieurs hôtes	Rare en pratique
PAT (NAT overload)	N IPs privées → 1 IP publique (différenciées par les ports)	Cas le plus courant (box Internet, routeur d'entreprise)

3. Fonctionnement du PAT

Le PAT (Port Address Translation) est la forme la plus répandue du NAT. Il permet à des centaines d'équipements de partager une seule IP publique en différenciant les flux grâce aux **numéros de port source**.

Exemple de translation PAT :

```
Réseau interne                    Routeur (PAT)                Internet
                                  IP publique : 203.0.113.1

PC-A  192.168.10.10:52341  →→→   203.0.113.1:10001  →→→   Serveur Web
1.1.1.1:80
PC-B  192.168.10.20:48872  →→→   203.0.113.1:10002  →→→   Serveur Web
1.1.1.1:80
PC-C  192.168.20.10:61234  →→→   203.0.113.1:10003  →→→   Serveur Web
1.1.1.1:80
```

Les trois PC accèdent au même serveur web depuis la même IP publique. Le routeur maintient une **table de traduction** qui lui permet de renvoyer chaque réponse au bon équipement interne.

Table NAT du routeur :

IP privée	Port privé	IP publique	Port public	Destination
192.168.10.10	52341	203.0.113.1	10001	1.1.1.1:80
192.168.10.20	48872	203.0.113.1	10002	1.1.1.1:80
192.168.20.10	61234	203.0.113.1	10003	1.1.1.1:80

4. Vocabulaire inside / outside

Sur un routeur Cisco, les interfaces sont marquées selon leur position par rapport au NAT :

Terme	Signification	Interface typique
inside	Côté réseau privé interne	Interface LAN / sous-interfaces VLANs
outside	Côté réseau public / Internet	Interface WAN



Sans le marquage `ip nat inside` et `ip nat outside` sur les interfaces, le NAT ne fonctionnera pas, même si la règle de translation est correctement définie.

5. Maquette de référence

```
  [PC-A 192.168.10.10]  [PC-B 192.168.20.10]
           |                     |
    VLAN 10 (USERS)        VLAN 20 (IT)
           |                     |
```

```
     Gi0/0.10                Gi0/0.20
           \                    /
            \                  /
         +-------------------------+
         |        ROUTEUR          |
         |   Gi0/0 (inside)        |
         |   Gi0/1 (outside)       |
         +-------------------------+
                    |
              Gi0/1 — IP publique : 203.0.113.1
                    |
                Internet
```

6. Configuration NAT statique

Objectif : Rendre un serveur interne (192.168.30.10) accessible depuis Internet via une IP publique fixe (203.0.113.50).

```
! Définir la translation statique
ROUTEUR(config)# ip nat inside source static 192.168.30.10 203.0.113.50

! Marquer les interfaces
ROUTEUR(config)# interface GigabitEthernet0/0.30
ROUTEUR(config-subif)# ip nat inside

ROUTEUR(config)# interface GigabitEthernet0/1
ROUTEUR(config-if)# ip nat outside
```

Tout paquet arrivant sur l'IP publique 203.0.113.50 sera automatiquement redirigé vers 192.168.30.10.

7. Configuration PAT (cas le plus courant)

Objectif : Permettre à tous les équipements des VLANs 10 et 20 d'accéder à Internet via l'unique IP publique du routeur.

Étape 1 — Définir les hôtes concernés par le NAT

```
ROUTEUR(config)# ip access-list standard ACL-NAT
ROUTEUR(config-std-nacl)# permit 192.168.10.0 0.0.0.255
ROUTEUR(config-std-nacl)# permit 192.168.20.0 0.0.0.255
```

Étape 2 — Activer le PAT sur l'interface WAN

```
ROUTEUR(config)# ip nat inside source list ACL-NAT interface
GigabitEthernet0/1 overload
```

Le mot-clé `overload` active le PAT (plusieurs IPs privées → une IP publique via les ports).

Étape 3 — Marquer les interfaces

```
ROUTEUR(config)# interface GigabitEthernet0/0.10
ROUTEUR(config-subif)# ip nat inside

ROUTEUR(config)# interface GigabitEthernet0/0.20
ROUTEUR(config-subif)# ip nat inside

ROUTEUR(config)# interface GigabitEthernet0/1
ROUTEUR(config-if)# ip nat outside
```



Si le routeur a plusieurs sous-interfaces `inside`, chacune doit être marquée individuellement avec `ip nat inside`.

8. NAT statique + PAT simultanés

Il est possible de combiner les deux : PAT pour les postes clients, NAT statique pour un serveur exposé.

```
! NAT statique pour le serveur
ROUTEUR(config)# ip nat inside source static 192.168.30.10 203.0.113.50

! PAT pour les postes clients (VLANs 10 et 20)
ROUTEUR(config)# ip access-list standard ACL-NAT
ROUTEUR(config-std-nacl)# permit 192.168.10.0 0.0.0.255
ROUTEUR(config-std-nacl)# permit 192.168.20.0 0.0.0.255

ROUTEUR(config)# ip nat inside source list ACL-NAT interface
GigabitEthernet0/1 overload
```

9. Vérification

```
show ip nat translations          ! Table de traduction active
show ip nat translations verbose  ! Détail complet de chaque entrée
show ip nat statistics            ! Compteurs (hits, misses, translations
actives)
clear ip nat translation *        ! Vide toute la table NAT
```

Exemple de sortie `show ip nat translations` :

```
Pro  Inside global     Inside local       Outside local      Outside global
tcp  203.0.113.1:10001 192.168.10.10:52341 1.1.1.1:80        1.1.1.1:80
tcp  203.0.113.1:10002 192.168.20.10:48872 1.1.1.1:80        1.1.1.1:80
```

```
---  203.0.113.50      192.168.30.10      ---                ---
```

Colonne	Signification
Inside local	IP/port de l'équipement interne (privé)
Inside global	IP/port vue depuis Internet (publique)
Outside local	IP destination vue depuis le réseau interne
Outside global	IP destination réelle sur Internet

10. Points clés à retenir

- Le NAT traduit des adresses IP — le PAT traduit des adresses **et des ports**
- Le PAT permet à **N équipements** de partager **1 seule IP publique** grâce aux ports
- Les interfaces doivent obligatoirement être marquées `inside` / `outside`
- Le NAT statique est utilisé pour les **serveurs exposés** sur Internet
- Le PAT (`overload`) est le cas le plus courant dans les réseaux d'entreprise et domestiques
- `show ip nat translations` est la commande de référence pour déboguer

— Ewen 2026/03/10

11. Publication de services et recette

SNAT traduit la source ; **DNAT** traduit la destination. La traduction et le filtrage sont deux décisions distinctes : publier une adresse ne garantit ni l'autorisation du flux ni le fonctionnement du service.

1. Vérifier le service depuis une zone autorisée.
2. Décrire adresses et ports avant et après traduction.
3. Tester depuis un client réellement externe.
4. Contrôler les compteurs, les journaux et le chemin retour.
5. Vérifier qu'un port non autorisé reste inaccessible.

Un test depuis le LAN vers l'adresse publique peut dépendre du NAT de rebouclage. Pour FTP, contrôler aussi les connexions de données, pas seulement TCP 21.

La configuration produit est présentée dans Stormshield.

From:
https://wiki.ewengadonnaud.xyz/ - **Base de savoir réseaux/cyber/devops**

Permanent link:
https://wiki.ewengadonnaud.xyz/doku.php?id=reseau:cisco:cours:cours_nat

Last update: **2026/10/18 01:23**