Protocole NAT

Le `NAT` (Network Address Translation) est un mécanisme utilisé pour faire transiter des paquets IP entre réseaux avec des plages d’adresses différentes, en modifiant les adresses source ou destination.

SNAT et DNAT

Il existe deux types de NAT :

Type	Fonction	Usage
SNAT	Modifie l'adresse source d'un paquet.	Utilisé pour permettre aux hôte d'un LAN d'accéder à Internet.
DNAT	Modifie l'adresse de destination d'un paquet.	Utilisé pour rediriger le trafic entrant vers un hôte interne au réseau local.

SNAT

Le SNAT est automatiquement activé sur les box et modems, ce qui permet aux équipements du réseau local d'accéder à Internet sans configuration manuelle.

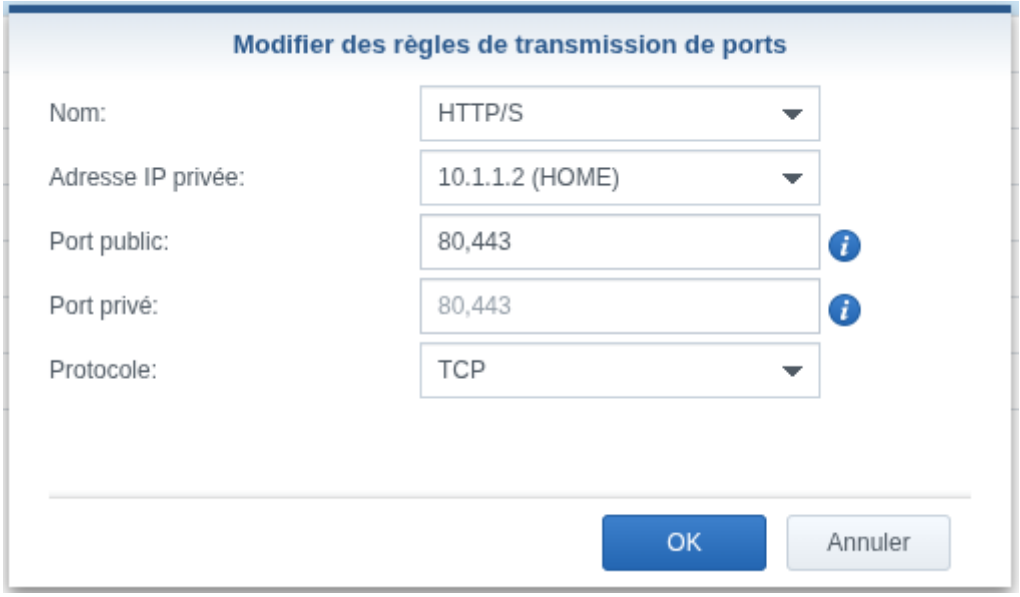
DNAT et Port Forwarding

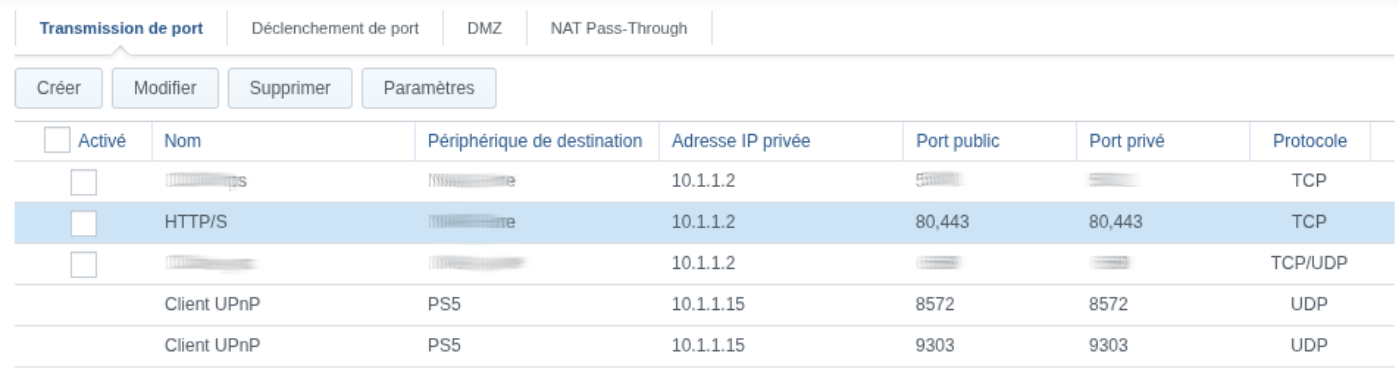
La redirection de port via DNAT est utilisée pour permettre l'accès à un service interne (hébergé sur une machine du réseau local) depuis l’extérieur du réseau.

La redirection consiste à modifier l'adresse IP et le port de destination d'un paquet entrant afin de le rediriger vers une machine du réseau local.

> Cette méthode est couramment utilisée pour exposer des services comme des serveurs web, FTP, SSH, etc. derrière un routeur NAT.

Exemple sur un routeur Synology





DMZ

Une `DMZ` (Demilitarized Zone) est, à l'origine, une zone réseau intermédiaire destinée à héberger des services accessibles depuis Internet, tout en protégeant le réseau interne grâce à une séparation stricte.

En pratique, dans de nombreuses configurations, le terme désigne un **hôte placé en dehors du pare-feu via un port forwarding global**, exposant tous ses ports à Internet, ce qui revient à le connecter directement au réseau public.

Cas particuliers

NAT UPnP

L'`UPnP` (Universal Plug and Play) est un protocole qui permet aux équipements connectés d'un réseau de demander au routeur d'ouvrir automatiquement certains ports.
`UPnP` est souvent nécessaire pour le fonctionnement d'applications spécifiques à travers le NAT (P2P, jeux en ligne, visios, etc.).

>

> Dans l'exemple ci-dessus, la PS5 a ouvert des ports UPnP. Probablement pour une mise à jour distribuée en P2P.

Concrètement, au lieu de devoir ajouter manuellement des règles de redirection de ports sur le routeur, `UPnP` permet à ces applications de créer ou supprimer elles-mêmes des règles de façon dynamique et temporaire.

> `UPnP` peut représenter un risque de sécurité : des programmes malveillants peuvent exploiter cette fonctionnalité pour s'ouvrir un accès depuis l'extérieur.

Hairpinning

Le **hairpinning NAT** (ou loopback NAT) est une fonctionnalité qui permet à un appareil du réseau local d'accéder à un autre appareil du même LAN via l'adresse IP publique du routeur.

Exemple :
Un smartphone est connecté sur un réseau Wi-Fi domestique. L'utilisateur souhaite accéder au NAS en utilisant l'adresse IP publique du modem et le port redirigé en NAT

- **Sans hairpinning :** La requête sort vers l'IP publique mais le routeur ne la **reboucle** pas vers le NAS. Résultat : ça ne fonctionne pas, le routeur bloque ou ignore la redirection pour une requête qui vient du LAN vers le LAN via l'IP publique.

- **Avec hairpinning :** Le routeur reconnaît cette situation, reboucle la requête et la redirige correctement vers le NAS, comme si la connexion venait de l'extérieur.

> La plupart des box opérateurs ne supportent pas correctement le hairspinning.

CGNAT

Le **CGNAT** (Carrier-Grade NAT, ou NAT de niveau opérateur) est une technique utilisée par les fournisseurs d'accès à Internet (FAI) pour **partager une seule adresse IPv4 publique entre plusieurs abonnés**.
Cela permet de pallier la pénurie d'adresses IPv4.

Normalement, chaque box ou routeur chez un particulier reçoit une adresse IP publique unique.

À l'inverse, avec le CGNAT, le FAI attribue une **adresse IP privée** à chaque client (comme dans un réseau local).

Plusieurs clients **partagent la même IP publique** et le FAI utilise un routeur NAT à grande échelle pour faire la traduction entre les IP privées des clients et l'IP publique partagée.

Quelques exemples

- **Fibre Free** : Sur certaines offres, **une seule IP publique est partagée entre 4 abonnés**. Il est possible d'activer une option (gratuite) pour obtenir une IP fixe et dédiée.
- **Starlink** : Par défaut, les utilisateurs sont derrière un CGNAT.
  Pour obtenir une **IP publique dédiée**, il faut **payer une option supplémentaire**.

> Le CGNAT rend impossible la redirection de port.

Revision #17
Created 2 October 2025 21:09:31 by Thibaud FRICHET
Updated 22 October 2025 21:30:45 by Thibaud FRICHET