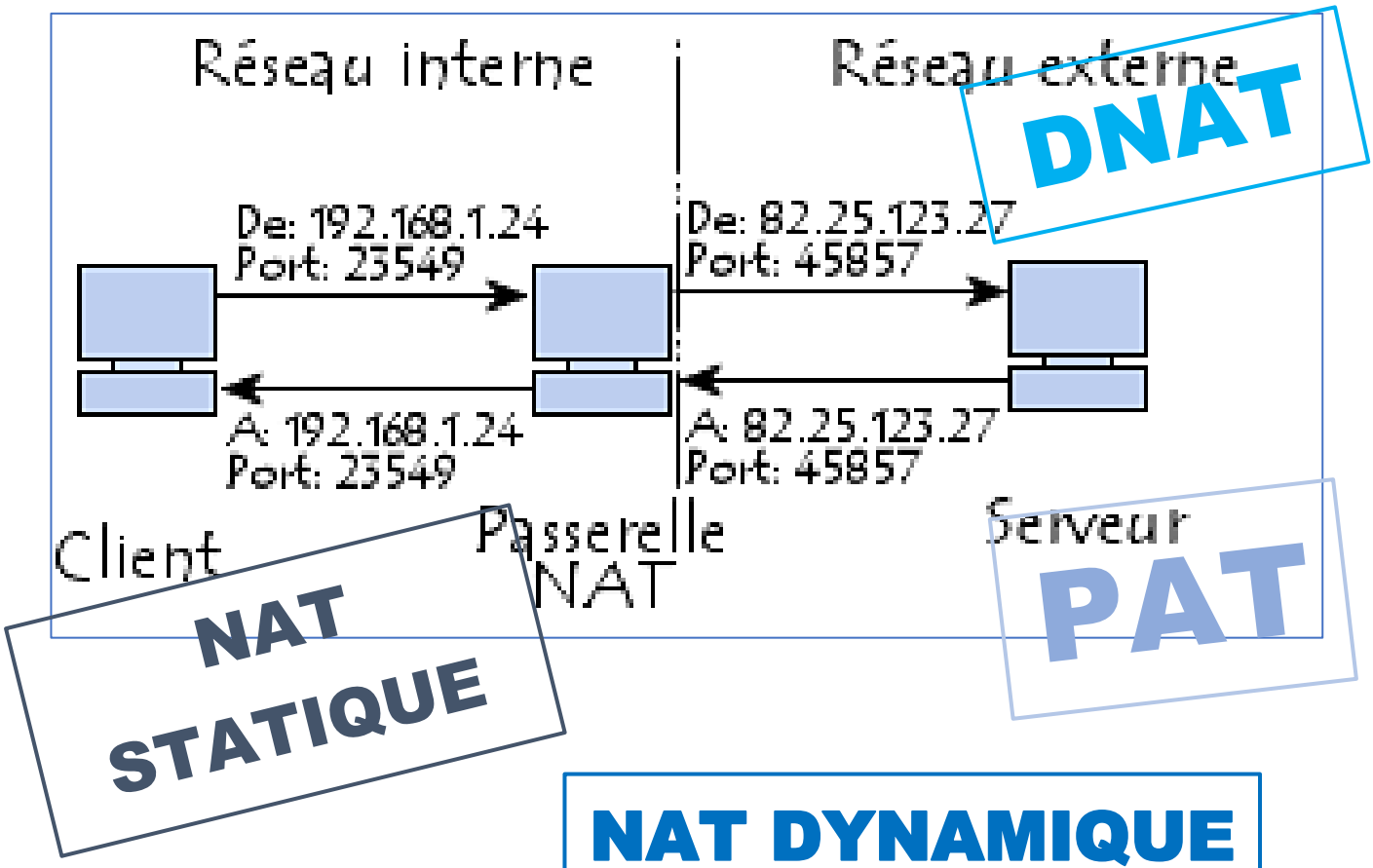
TUTOS-INFO
L'informatique par l'exemple

DOCUMENT

Comprendre les notions de NAT/DNAT/PAT



C'EST QUOI LE NAT ?

1 – POURQUOI LE NAT EST-IL APPARU ?

Le mécanisme de **translation d'adresses** (en anglais ***Network Address Translation*** noté **NAT**) a été mis au point afin de **répondre à la pénurie d'adresses IPv4**.

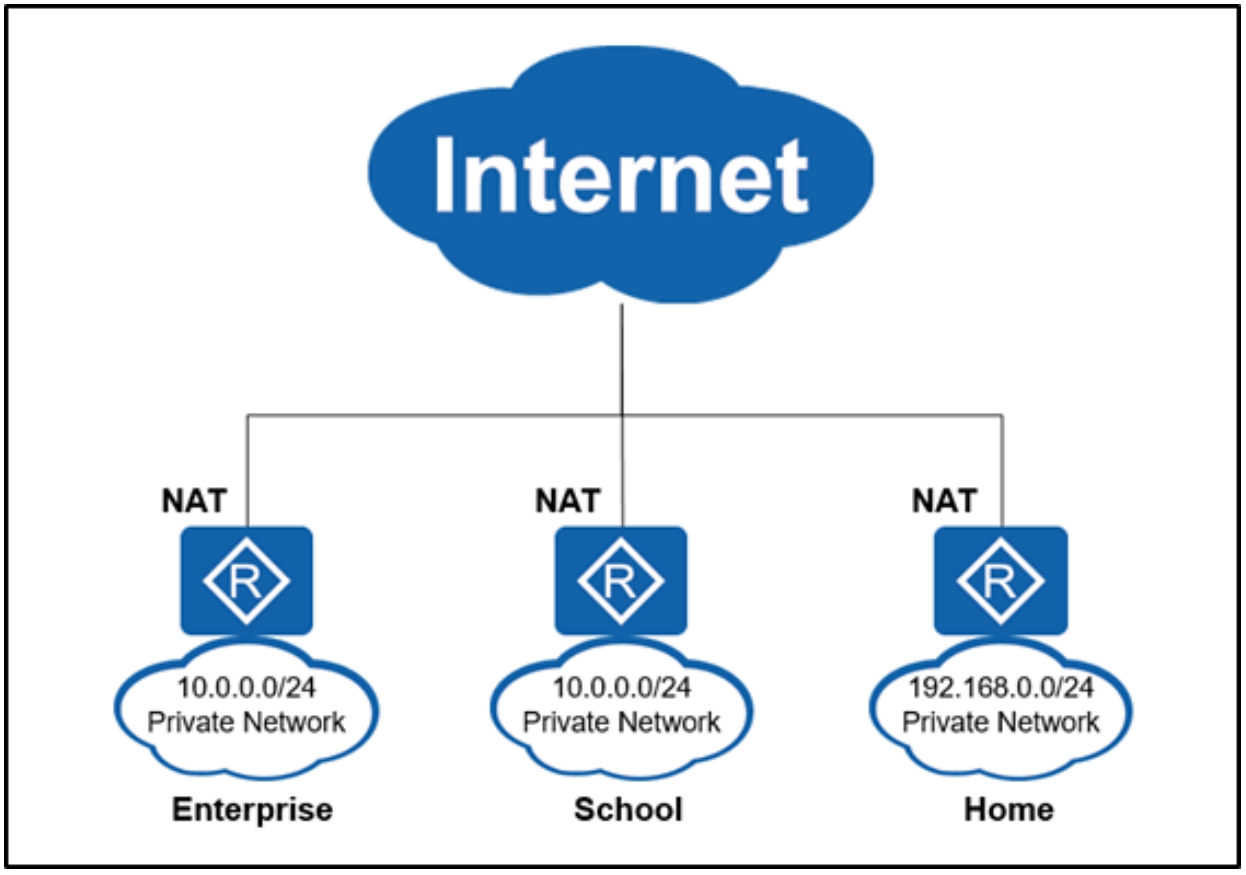
En effet, **en adressage IPv4 le nombre d'adresses IP routables (donc uniques sur la planète) n'est pas suffisant** pour permettre à toutes les machines nécessitant d'être connectées à internet de l'être.

Une **adresse IPv4** est codée sur 4 octets chacun représentant 8 bits ce qui fait un **total de plus de 4 200 000 000 adresses IPv4 disponibles pour la planète !**

Le principe du NAT consiste donc à utiliser une adresse IP routable (ou un nombre limité d'adresses IP) **pour connecter l'ensemble des machines du réseau en réalisant**, au niveau de la passerelle de connexion à internet, **une translation** (littéralement une « traduction ») **entre l'adresse interne (non routable)** de la machine souhaitant se connecter **et l'adresse IP de la passerelle**.

D'autre part, **le mécanisme de translation** d'adresses **permet de sécuriser le réseau interne** étant donné qu'il "**camoufle complètement l'adressage interne**".

En effet, pour un observateur externe au réseau, toutes les requêtes semblent provenir de la même adresse IP.



Cependant, le NAT peut également présenter des inconvénients. **Il peut limiter la capacité d'un ordinateur à recevoir des connexions entrantes**, ce qui peut rendre difficile l'hébergement de serveurs ou l'utilisation de certaines applications.

En conclusion, le NAT est un protocole important pour les réseaux domestiques et d'entreprise.

2 – LES TYPES DE NAT LES PLUS CONNUS

Le réseau public fait référence à Internet et l'**adresse IP publique** fait référence à l'adresse IP planifiée globalement sur Internet.

Les segments de réseau ne peuvent pas se chevaucher. **Les routeurs sur Internet peuvent transférer des paquets dont l'adresse de destination est une adresse de réseau public**.

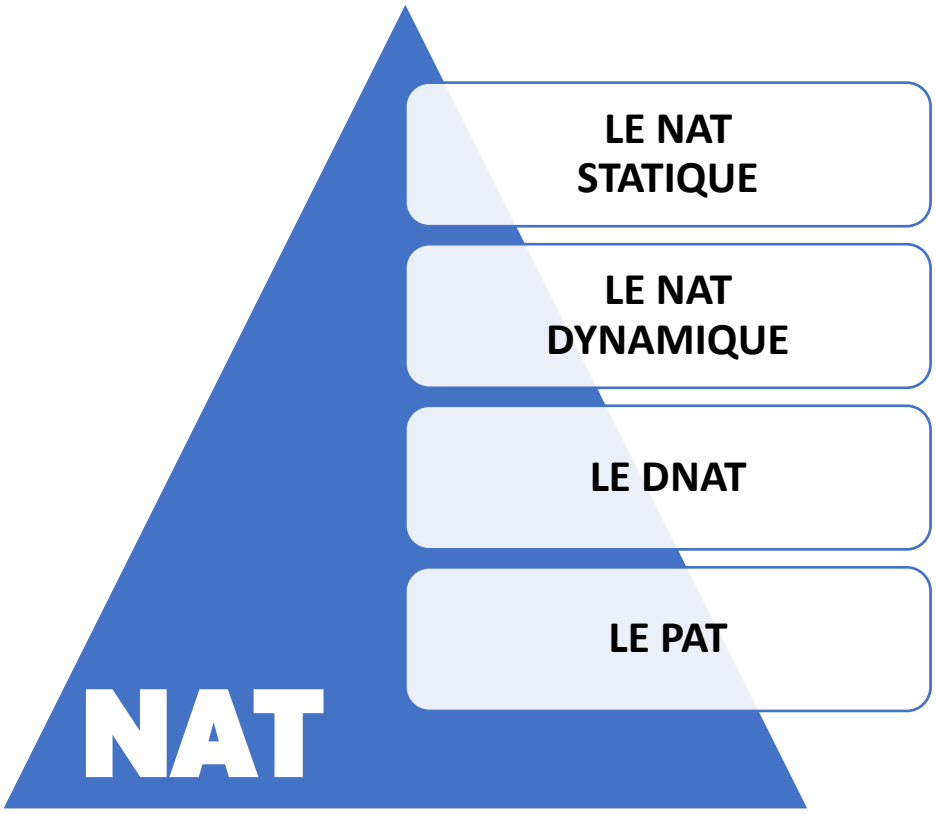
Dans l'espace d'adressage IP, **certaines adresses IP** de **classe A**, **classe B** et **classe C sont réservées en tant qu'adresses IP privées**.

Les adresses IP privées ne peuvent pas être utilisées sur le réseau public mais uniquement sur l'intranet. Les routeurs sur Internet n'ont pas de routes vers des adresses privées.

Les plages d'adresses privées réservées de classe A, classe B et classe C sont les suivantes :

- Adresse IP de **classe A** : 10.0.0.0 - 10.255.255.255
- Adresse IP de **classe B** : 172.16.0.0 – 172.31.255.255
- Adresse IP de **classe C** : 192.168.0.0 – 192.168.255.255

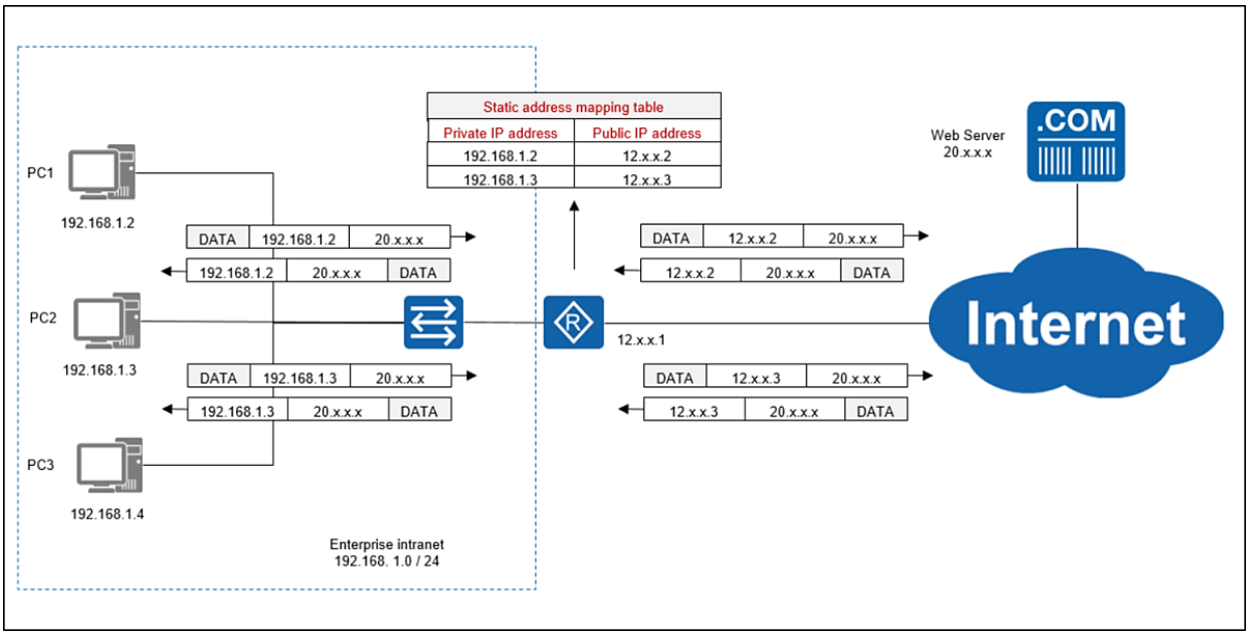
Il existe plusieurs types de NAT parmi lesquels :



a) Le NAT STATIQUE

Avec le **NAT statique, le routeur** (ou le pare-feu) **traduit** une adresse IP privée en une seule adresse IP publique. Chaque adresse IP privée est mappée sur une seule adresse IP publique.

Le NAT statique **n'est pas souvent utilisé** car il **nécessite une adresse IP publique pour chaque adresse IP privée**.

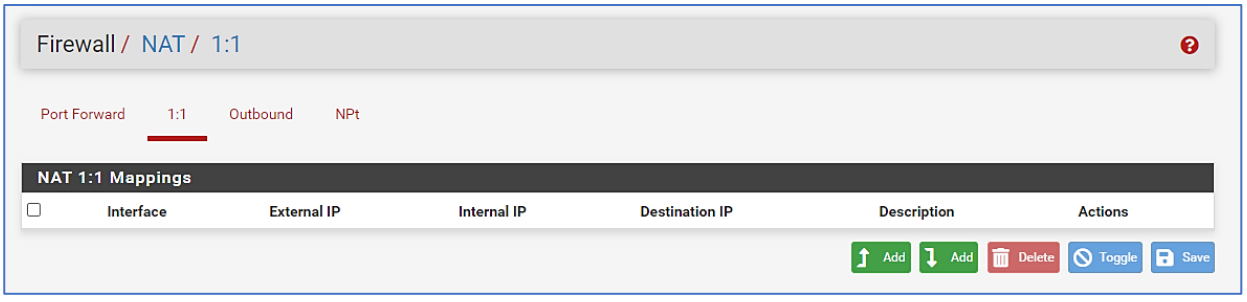


Comme le montre la figure ci-dessus, le FAI attribue trois adresses publiques 12.xx1, 12.xx2 et 12.xx3 à l'entreprise.

Le NAT statique est configuré sur le routeur de l'entreprise pour mapper l'adresse privée 192.168.1.2 de PC1 à l'adresse publique 12.x.x.2 et l'adresse privée 192.168.1.3 de PC2 à l'adresse publique 12.x.x.3

Une table de mappage d'adresses statiques est générée sur le routeur.

Le NAT statique mappe les adresses privées aux adresses publiques en mode un à un. Sur le routeur open source pfSENSE, ce type de NAT se paramètre dans le menu "**Firewall**" – "**NAT**" – "**1:1**"



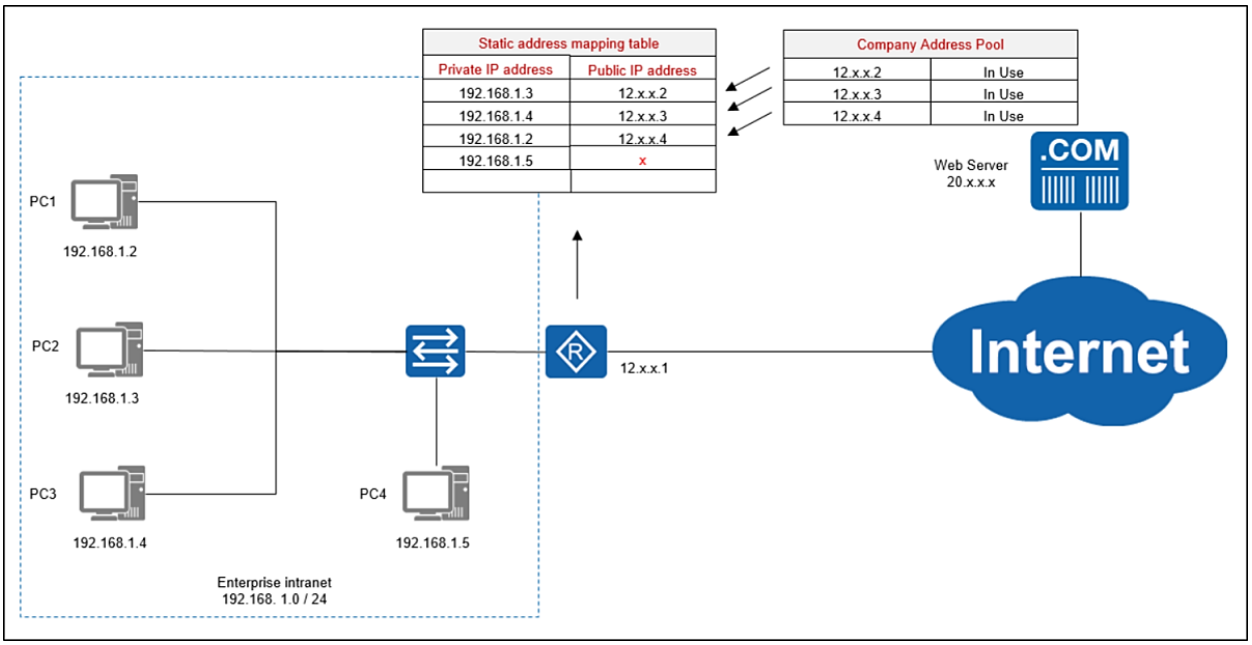
Avec le NAT statique, *les adresses publiques correspondantes sont toujours utilisées même si un hôte intranet est hors ligne pendant une longue période* ou n'envoie pas de données.

Le NAT statique n'enregistre pas les adresses IP.

b) Le NAT DYNAMIQUE

Contrairement au NAT statique, où vous deviez définir manuellement un mappage statique entre une adresse privée et publique, **avec le NAT dynamique, le mappage d'une adresse locale à une adresse globale se produit de manière dynamique**.

Cela signifie que **le routeur sélectionne dynamiquement une adresse du pool d'adresses global qui n'est pas actuellement affectée**. Il peut s'agir de n'importe quelle adresse du pool d'adresses globales. L'entrée dynamique reste dans la table des traductions NAT tant que le trafic est échangé. **L'entrée expire après une période d'inactivité et l'adresse IP globale peut être utilisée pour de nouvelles traductions**.



Une fois le NAT dynamique configuré, le routeur périphérique de l'entreprise génère un pool d'adresses IP publiques en fonction des adresses IP publiques disponibles. Lorsque le PC de l'entreprise accède à Internet, le paquet de données passe par le routeur. Le routeur remplace l'adresse IP privée du PC par une adresse IP publique inactive, puis accède à Internet.

c) Le DNAT (ou "port forwarding")

La notion de "**Redirection de port**" appelée aussi "**port forwarding**" correspond au "**DNAT**" c'est-à-dire au "**Destination NAT**". En fait, on parle de "*Source NAT*" quand c'est l'adresse IP source du paquet qui est modifiée (par exemple : un PC du réseau local accède à un site Internet) et de "*Destination NAT*" quand c'est l'adresse IP de destination du paquet qui est modifiée (par exemple : un PC connecté à Internet accède à un NAS connecté à notre réseau local).

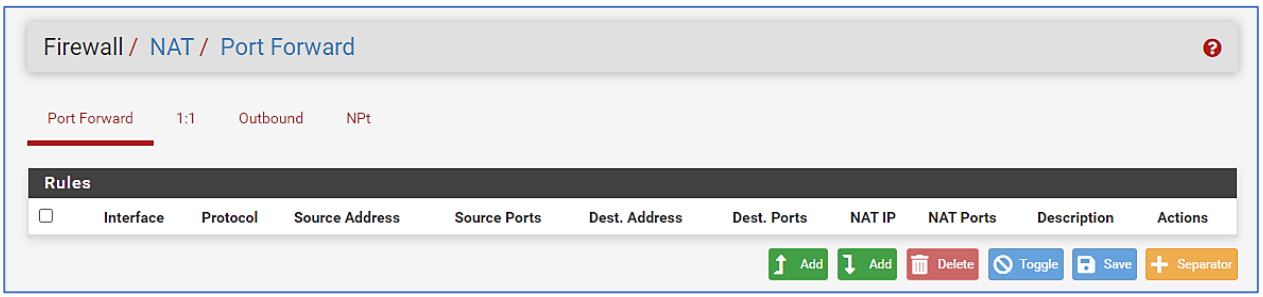
Grâce à une règle de redirection de port, **une machine connectée au réseau local et qui dispose d'une adresse IP privée pourra être accessible depuis l'extérieur**, c'est-à-dire depuis Internet, sur un ou plusieurs ports spécifiques, via l'adresse IP publique du routeur (box).

Par exemple :

- Un serveur Web connecté au réseau local pourra être joignable depuis l'extérieur sur le port TCP n° 443 qui correspond au HTTPS, en accédant à l'adresse IP publique de la box.

- Un serveur Linux connecté au réseau local pourra être joignable en SSH depuis l'extérieur sur le port TCP n° 22 (ou un autre port autre que celui par défaut), en accédant à l'adresse IP publique de la box.

Dans pfSENSE, la configuration du DNAT est accessible depuis le menu "**Firewall**" – "**NAT**" – "**Port forwarding**" :



Il faut savoir qu'il n'est pas obligatoire d'utiliser le même numéro de port pour la source et la destination.

Par exemple, un NAS sur le réseau local peut être accessible via le port 443 mais on peut décider de le rendre accessible depuis l'extérieur sur un autre port (par exemple 65001). Dans ce cas, on parle de "***port mapping***" : c'est le même principe que le "port forwarding" mais l'on utilise, ici, deux numéros de port différents.

Il faut savoir que :

- **Le port externe impacte le client connecté à Internet**
- Si l'on met le port 65001 pour une interface Web, le visiteur devra saisir https://ip-publique:65001.
- **Le port interne impacte le serveur et la machine de destination**

d) Le PAT

Le **PAT** pour ***P**ort **A**ddress **T**ranslation* est une forme de NAT dynamique, que l'on appelle "**NAT overlay**" ou "**Masquerade NAT**", avec quelques différences très intéressantes, qui font du PAT le mode le plus couramment utilisé.

Ce type de NAT est également connu sous le nom de "surcharge NAT".

Comme le NAT dynamique, le PAT va effectuer une association dynamique et temporaire entre une adresse IP privée et une adresse IP publique, mais il va ajouter à cette association une autre information : **un numéro de port**, d'où le terme "PAT".

Le PAT fonctionne en créant un mappage NAT dynamique, dans lequel une adresse IP globale (publique) et un numéro de port unique sont sélectionnés.

Le routeur conserve une entrée de table NAT pour chaque combinaison unique de l'adresse IP et du port privés, avec traduction vers l'adresse globale et un numéro de port unique.

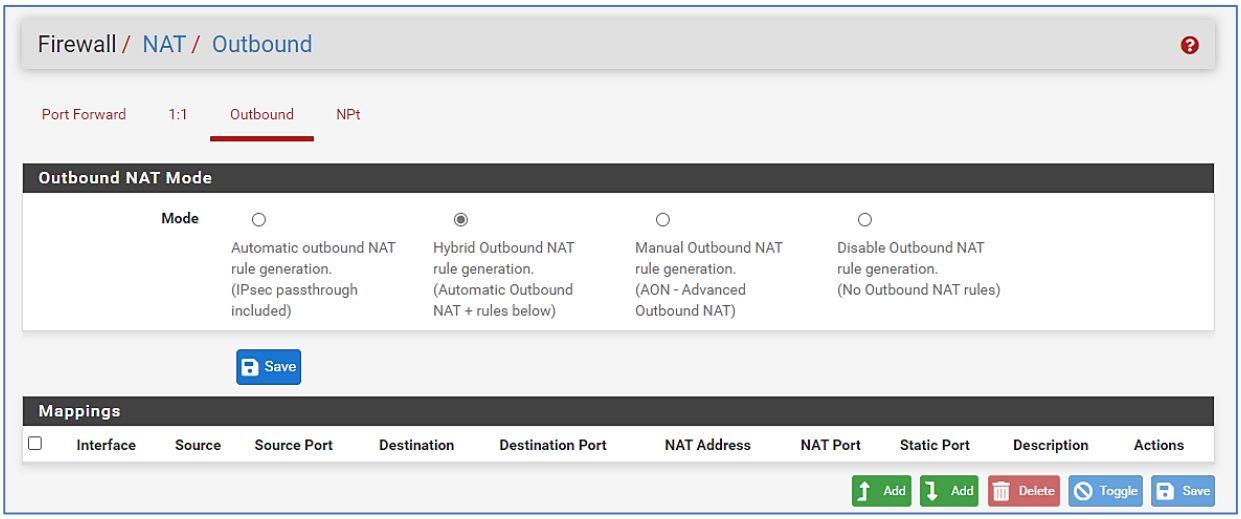
Grâce au PAT, une seule et même adresse IP publique peut être utilisée par X machines connectées sur le réseau local.

C'est exactement ce qu'il se passe à la maison : votre ordinateur, votre smartphone, votre tablette, etc. sont connectés à votre réseau local et utilisent tous **la même adresse IP publique pour accéder à Internet**.

A propos du "NAT SORTANT" dans pfSENSE :

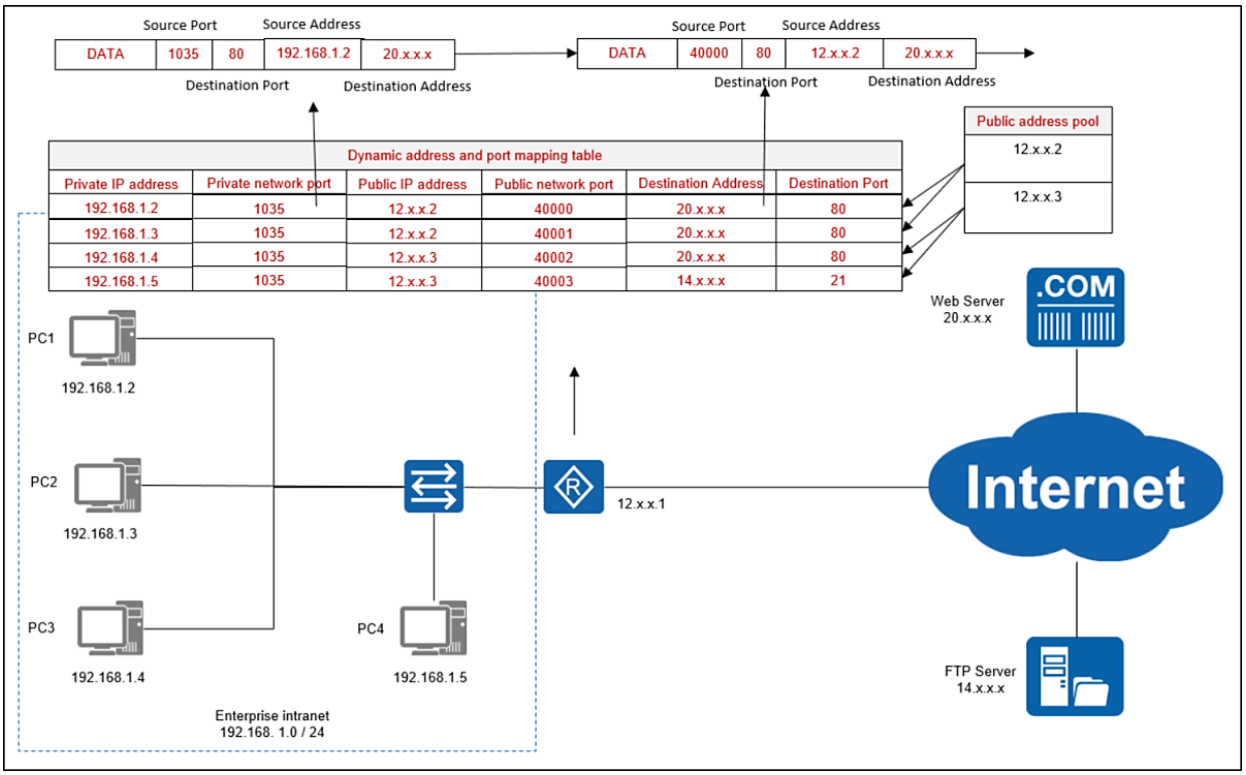
Dans pfSENSE, vous pouvez configurer un "NAT SORTANT" ou "Outbound". Le NAT sortant, également connu sous le nom *de **"NAT source"***, contrôle la façon dont le logiciel pfSENSE traduit l'adresse source et les ports de trafic quittant une interface.

Le NAT SORTANT se configure dans le menu "**Firewall**" – "**NAT**" – "**Outbound**" :



3 – LE NAPT

La traduction d'adresses réseau et de ports (NAPT) traduit non seulement les adresses IP, mais également les numéros de port lors de la sélection d'adresses dans le pool d'adresses. De cette manière, un mappage un à plusieurs entre les adresses publiques et les adresses privées est mis en œuvre, ce qui améliore efficacement l'utilisation des adresses publiques.



Comme illustré dans la figure précédente, après l'activation de NAPT, le routeur génère une adresse dynamique et une table de mappage de port.

Le pool d'adresses IP publiques du routeur de périphérie n'a que deux adresses IP publiques. Lorsque PC1 accède au serveur Web sur Internet, le paquet de données transporte les paramètres du port source, du port de destination, de l'adresse source et de l'adresse de destination vers le routeur.

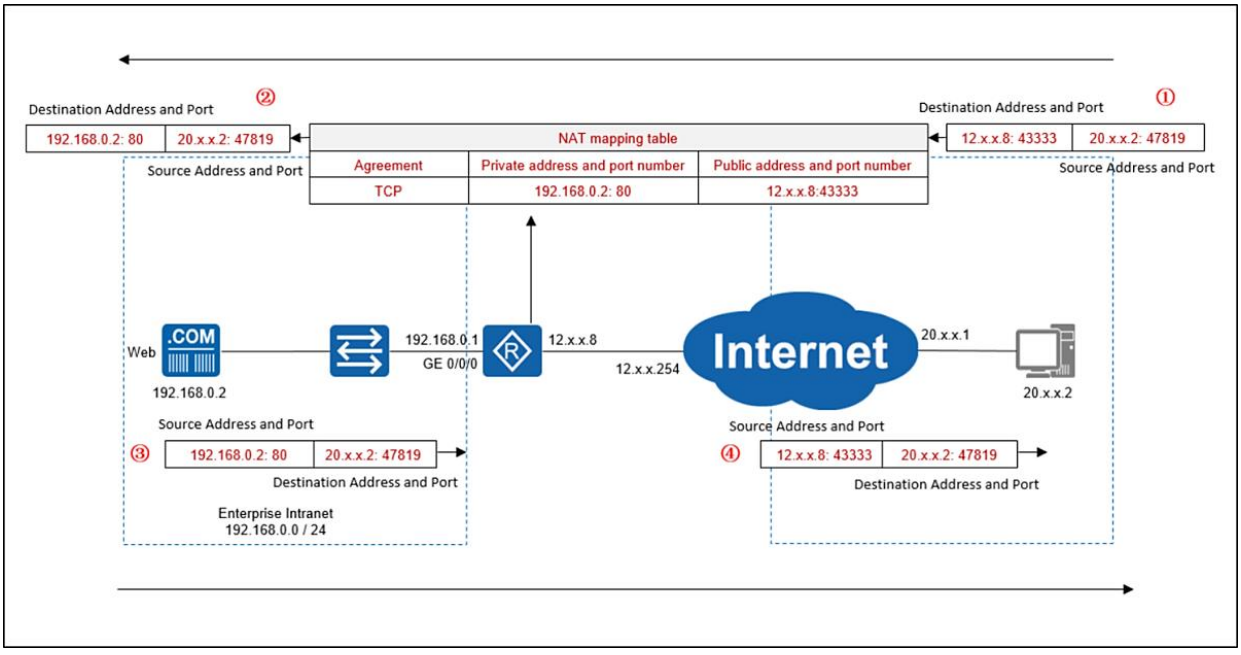
Ensuite, le routeur effectue une traduction d'adresse publique et une traduction de port source. De plus, le numéro de port traduit et l'adresse IP publique sont enregistrés dans la table de mappage d'adresses et de ports dynamiques. Enfin, PC1 accède à Internet.

Lorsque le serveur WEB renvoie des données, le paquet de données transmet également ces paramètres au routeur. Ensuite, le routeur interroge la table de mappage d'adresses et de ports dynamiques et envoie le paquet de données à PC1.

NAPT traduit les numéros de port de la couche de transport pour différencier les terminaux sur l'intranet et permet à plusieurs adresses IP privées de partager une adresse IP publique, économisant ainsi les adresses IP.

4 – SERVEUR NAT

Le serveur NAT fait référence au mappage de port. Lorsque le serveur du réseau privé doit fournir des services pour le réseau public, vous devez configurer le serveur NAT sur le routeur et spécifier le mappage un à un entre [adresse IP publique : port] et [adresse IP privée : port] pour mapper le serveur intranet au réseau public. L'hôte du réseau public accède à [adresse IP publique : port] pour accéder au serveur intranet.



Comme illustré dans la figure précédente, le serveur Web sur l'intranet de l'entreprise doit être accessible par des ordinateurs sur Internet. Pour implémenter cela, vous devez configurer le serveur NAT sur le routeur périphérique de l'entreprise.

1. Mappage de l'adresse IP et du numéro de port de service du serveur Web (192.168.0.2:80) à l'adresse IP publique et au numéro de port du routeur périphérique (12.x.x.8:43333).

2. Lorsqu'un ordinateur sur Internet accède au service Web sur l'intranet, l'adresse IP de destination et le numéro de port du paquet de données sont l'adresse IP et le numéro de port (12.x.x.8:43333) mappés sur le serveur NAT.

3. Après avoir reçu le paquet, le routeur périphérique de l'entreprise consulte la table de mappage NAT et traduit l'adresse IP de destination et le numéro de port en adresse IP et numéro de port du serveur Web (192.168.0.2:80).

4. De cette manière, les services du réseau privé sont accessibles via le réseau public.

5 – LES AVANTAGES ET INCONVENIENTS DU NAT

Avantages du NAT

1. L'intranet de l'entreprise utilise des adresses IP privées, ce qui réduit l'occupation des adresses IP publiques. Le NAT est généralement appliqué aux routeurs frontaliers comme les routeurs connectés à Internet.

En utilisant la technologie NAPT, les entreprises peuvent utiliser des adresses IP publiques pour accéder à Internet à partir de réseaux privés, en enregistrant les adresses IP publiques.

- Si différentes entreprises ou écoles n'ont pas besoin de communiquer entre elles, leurs adresses privées peuvent se chevaucher.

- Si les intranets de différentes écoles ou entreprises communiquent entre eux via des VPN ou des lignes louées, les adresses privées utilisées par différentes écoles ou entreprises ne peuvent pas se chevaucher.

2. Le réseau privé n'est pas directement accessible sur Internet pour renforcer la sécurité de l'intranet.

Inconvénients du NAT

1. Lorsque NAT ou NAPT est exécuté sur un routeur, la couche réseau et la couche transport des paquets de données doivent être modifiées et le mappage entre le port et la traduction d'adresse doit être conservé et enregistré dans le routeur. Le routage des paquets de données entraîne un délai de commutation important et consomme un grand nombre de ressources sur le routeur.

2. Une adresse IP privée est utilisée pour accéder à Internet. L'adresse IP source est remplacée par une adresse IP publique. Si un étudiant d'une école publie un message sur le forum, le forum ne peut enregistrer que l'adresse IP publique de l'éditeur et ne peut pas tracer l'adresse IP intranet. Autrement dit, le traçage IP de bout en bout ne peut pas être effectué.

3. Le réseau public ne peut pas accéder au réseau privé. Pour accéder au réseau privé, vous devez effectuer le mappage des ports.

4. Certaines applications ne peuvent pas s'exécuter sur le réseau NAT.