Handbook NAT

Pierre-Yves GOUBIER - ***2013***

Table des Matières

La Translation d'adresses

Notion Inside et Outside d'un réseau d'entreprise :

Le coté **Inside** d'un routeur, correspond à un attachement *(une interface physique ou logique)*, à **l'intérieur** du réseau d'une entité.

Les sous-réseaux sont le plus souvent associés à des plages d'adresses privées, ou des adresses publiques administrées par elle.

Le coté **Outside** d'un routeur, correspond à un attachement *(une interface physique ou logique)*, à **l'extérieur** du réseau d'une entité.

Les sous-réseaux sont le plus souvent associés à des plages d'adresses publiques allouées par un fournisseur d'accès. Dans le cas d'une interconnexion privée vers une autre entité *(un fournisseur, par exemple)*, le sous réseau peut correspondre à une étendue privée, dont la gestion doit être coordonnée entre les deux entités.

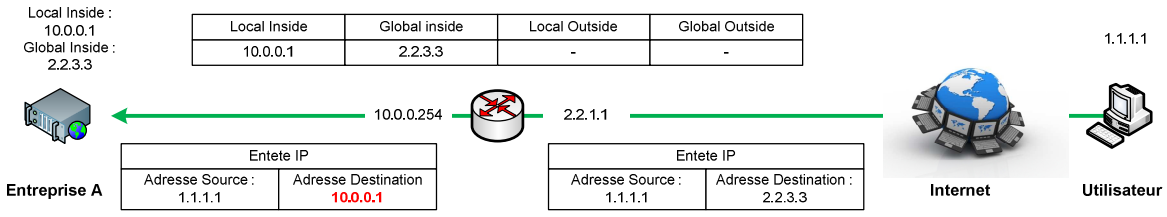
Les adresses Global Inside, Global Outside, Local Inside, Global Inside *(cf Cisco)* :

Les adresses circulant sur le LAN d'une entité peuvent être nommées différemment en fonction de la localisation de la ressource.

Elles peuvent être vues de manière **« Local »** *(au travers d'adresses ou de sous-réseaux appartenant au plan d'adressage de l'entité)*, ou de manière **« Global »** *(au travers d'adresses ou sous-réseaux n'appartenant pas au plan d'adressage de l'entité)*.

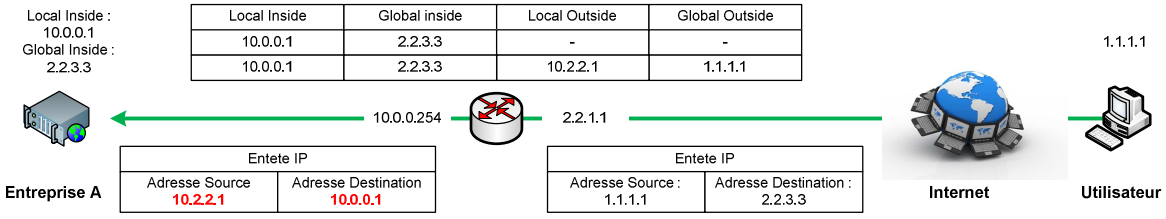
Prenons un exemple, pour une entreprise Alpha, qui possède un plan d'adressage privé de type 10.0.0.0/8, et qui met à disposition de l'internet une ressource de type serveur Web via une adresse publique fournie par un fournisseur d'accès :

- Alpha a un serveur Web dont l'adresse réelle est **10.0.0.1/24**.
- Elle met ce serveur à disposition de l'internet via une adresse publique allouée par un fournisseur d'accès : **2.2.3.3**.
- Quand un Internaute tentera d'accès à notre serveur Web, il le fera sur son Adresse **Global Inside** *(l'adresse du serveur interne, vue de l'extérieur, c'est-à-dire l'adresse de destination du paquet entrant)* **: 2.2.3.3.**
- Une ***translation*** installée sur le routeur d'Alpha, transformera cette adresse **Global Inside**, en adresse **Local Inside** *(c'est-à-dire l'adresse réelle du serveur Interne)* : **10.0.0.1**.



Dans cette autre exemple, on désire identifier les accès de l'extérieur *(les adresses publiques des internautes)* au travers d'un sous réseau IP particulier, issu du plan d'adressage privé de l'entité *(dans le but d'appliquer des règles de sécurité ou de Qos, par exemple…)*

- Alpha a un serveur Web dont l'adresse réelle est **10.0.0.1/24**.
- Elle met ce serveur à disposition de l'internet via une adresse publique allouée par un fournisseur d'accès : **2.2.3.3**.
- Quand un Internaute tentera d'accès à notre serveur Web, il le fera sur son Adresse **Global Inside** *(l'adresse du serveur interne, vue de l'extérieur, c'est-à-dire l'adresse de destination du paquet entrant)* **: 2.2.3.3.**
- Une ***première translation*** installée sur le routeur d'Alpha, transformera cette adresse **Global Inside**, en adresse **Local Inside** *(c'est-à-dire l'adresse réelle du serveur Interne)* : **10.0.0.1**.
- Une ***deuxième translation*** installée sur le routeur d'Alpha, transformera l'adresse source du client, **1.1.1.1**, son adresse **Global Outside**, en **10.2.2.1**, son adresse **Local Outside**.



-ooOoo-

Les types de Translation

Le NAT (Network Address Translation) Statique

La translation statique va consister à remplacer une adresses IP donnée par une autre adresse IP donnée, et cela pour une ou plusieurs instance. Il existe plusieurs types de translations statiques

Le NAT Statique Unidirectionnel et Bidirectionnel

L'initiateur de la connexion est important dans la définition de cette translation.

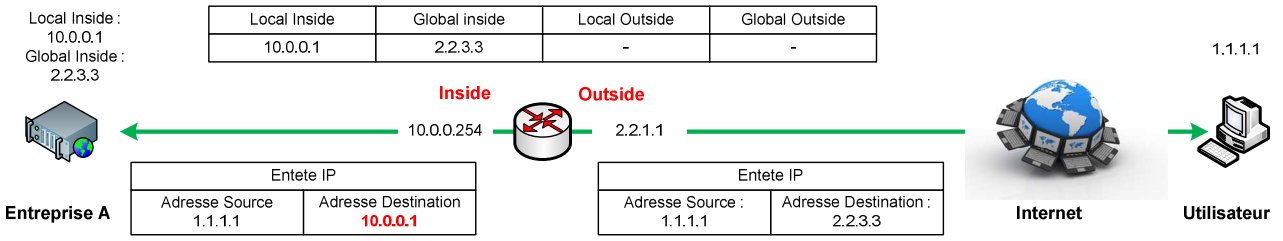
Si elle provient de l'utilisateur *(par une patte **Outside**)*, elle doit fonctionner
Par contre, elle ne fonctionne pas si c'est le serveur qui est à l'initiative de la tentative de connexion ; la translation est dite **unidirectionnelle**.

Si la translation fonctionne quel que soit l'initiateur de la connexion *(utilisateur externe en provenance de la patte **Outside**, ou serveur interne en provenance de la patte **Inside**)*, elle sera dite **bidirectionnelle**.

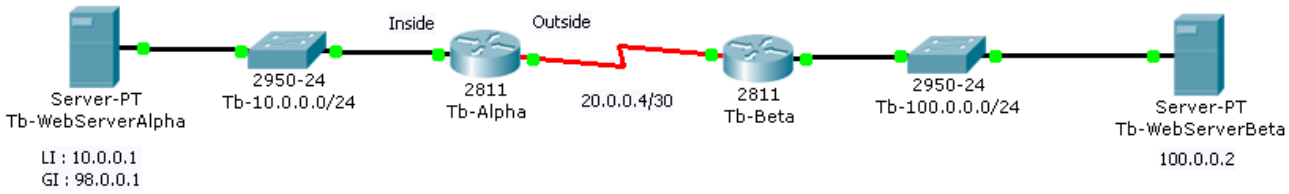
Sur la plupart des routeurs, la mise en place d'une translation statique est, par défaut, **bidirectionnelle**, la translation **unidirectionnelle** étant peut utilisée.

Par contre, certains types de nœud de sécurité *(Firewall)* peuvent utiliser systématiquement la translation **unidirectionnelle**, de manière à bloquer une tentative de connexion du serveur, suite à une prise de main malveillante.

NAT Statique Bidirectionnel



Mise en œuvre sur Packet Tracer 5.3.3 (*Cf fichier « translations.pkt » à télécharger)*



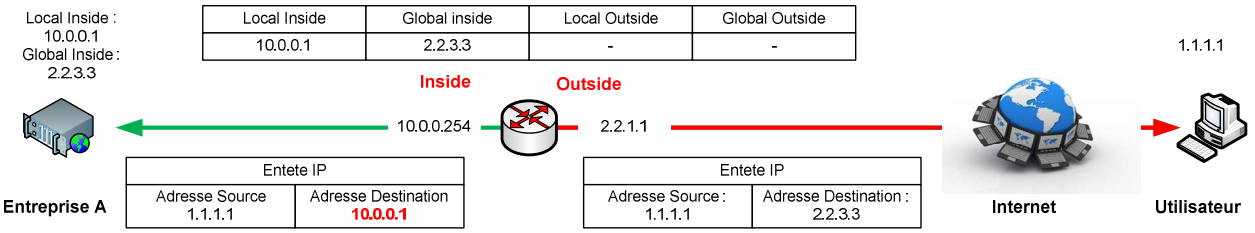
Pour valider le fonctionnement, on teste une connexion **TCP 80** ***(navigateur web du serveur Tb-WebServerBeta)*** vers le serveur **Tu-WebServerAlpha**, via son adresse **Global Inside** ***(98.0.0.1)***. La page d'accueil doit s'afficher.

Le test inverse doit également fonctionner *(affichage de la page d'accueil de* ***Tb-WebServerBeta****)* lorsque l'on accède au serveur Web de Beta via son adresse **Global inside : 100.0.0.2**.

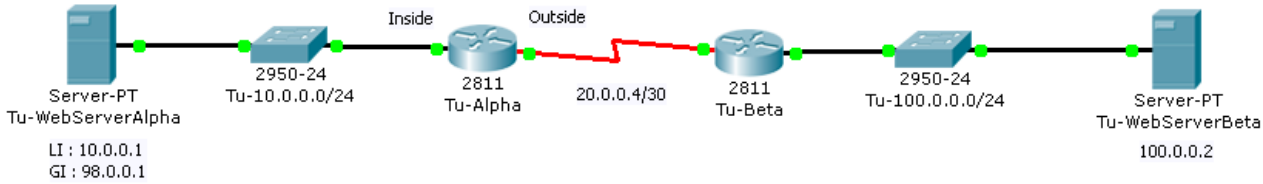
```
Tb-Alpha>sh ip nat trans
Pro  Inside global     Inside local       Outside local      Outside global
---  98.0.0.1          10.0.0.1           ---                ---
tcp 98.0.0.1:1025      10.0.0.1:1025      100.0.0.2:80       100.0.0.2:80
tcp 98.0.0.1:80        10.0.0.1:80        100.0.0.2:1025     100.0.0.2:1025
Tb-Alpha>
```

```
interface FastEthernet0/0
 ip address 10.0.0.254 255.255.255.0
 ip nat inside
 duplex auto
 speed auto
 (…)
interface Serial0/0/0
 ip address 20.0.0.6 255.255.255.252
 encapsulation ppp
 ip nat outside
 clock rate 4000000
 (…)
ip nat inside source static 10.0.0.1 98.0.0.1
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
```

NAT Statique Undirectionnel



Mise en œuvre sur Packet Tracer 5.3.3 (*Cf fichier « translations.pkt » à télécharger)*



Pour valider le fonctionnement, on teste une connexion **TCP 80** ***(navigateur web du serveur Tu-WebServerBeta)*** vers le serveur **Tu-WebServerAlpha**, via son adresse Global Inside ***(98.0.0.1)***. La page d'accueil doit s'afficher.La visualisation de la table de translation observable sur **Tu-Alpha** nous confirme le bon fonctionnement :

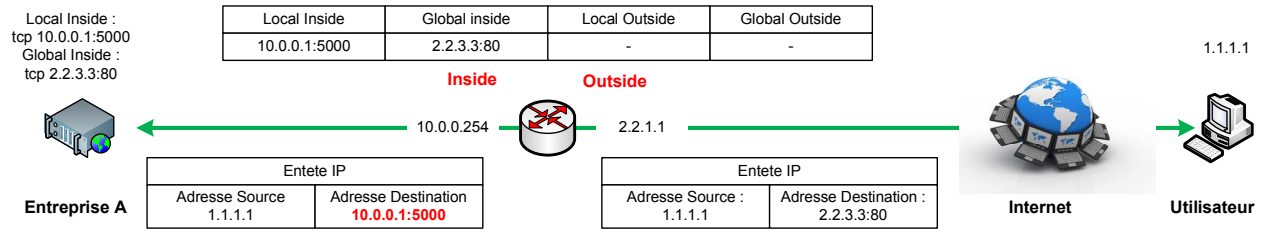
```
Tu-Alpha>sh ip nat trans
Pro  Inside global     Inside local       Outside local      Outside global
---  98.0.0.1          10.0.0.1           ---                ---
tcp 98.0.0.1:80        10.0.0.1:80        100.0.0.2:1025     100.0.0.2:1025

Tu-Alpha#sh ip access-lists
Extended IP access list BlocPourUni
    permit tcp host 98.0.0.1 any established (3 match(es))
    deny ip any any
Tu-Alpha#
```

Pour réaliser en simulation une translation unidirectionnelle, nous avons fait usage d'une ACL qui filtre les paquets, autorisant le retour d' Alpha vers Beta, seulement quand la connexion est à l'initiative de Beta. Les paquets seront droppés dans le cas d'une tentative de connexion d'Alpha vers Beta.

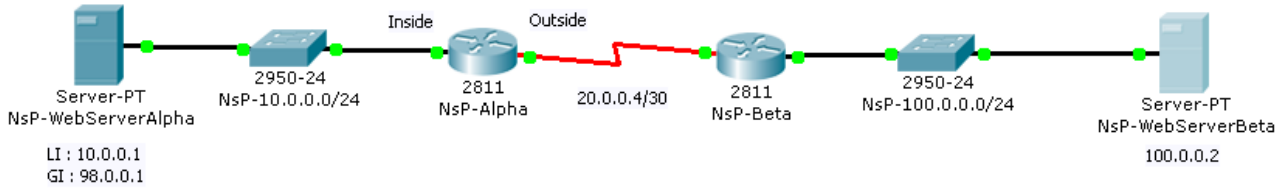
```
interface FastEthernet0/0
 ip address 10.0.0.254 255.255.255.0
 ip nat inside
 duplex auto
 speed auto
(…)
interface Serial0/0/0
 ip address 20.0.0.6 255.255.255.252
 encapsulation ppp
 ip access-group BlocPourUni out
 ip nat outside
 clock rate 4000000
(…)
ip nat inside source static 10.0.0.1 98.0.0.1
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
!
ip access-list extended BlocPourUni
 permit tcp host 98.0.0.1 any established
```

Ce type de translation associe une translation d'adresse statique unidirectionnelle ou bidirectionnelle, ainsi qu'une translation sur le port.

NAT Statique PAT



Mise en œuvre sur Packet Tracer 5.3.3 (*Cf fichier « translations.pkt » à télécharger)*



Pour valider le fonctionnement, on teste une connexion **TCP 5000** ***(navigateur web du serveur NsP-WebServerBeta)*** vers le serveur **Nsp-WebServerAlpha**, via son adresse **Global Inside** ***(98.0.0.1)*** **en précisant le port 5000, c'est-à-dire : 98.0.0.1 :5000**. La page d'accueil doit s'afficher.

```
NsP-Alpha>sh ip nat trans
Pro  Inside global     Inside local       Outside local      Outside global
tcp 98.0.0.1:5000      10.0.0.1:80        ---                ---
tcp 98.0.0.1:5000      10.0.0.1:80        100.0.0.2:1026     100.0.0.2:1026
NsP-Alpha>

interface FastEthernet0/0
 ip address 10.0.0.254 255.255.255.0
 ip nat inside
 duplex auto
 speed auto
(…)
interface Serial0/0/0
 ip address 20.0.0.6 255.255.255.252
 encapsulation ppp
 ip nat outside
 clock rate 4000000
(…)
ip nat inside source static tcp 10.0.0.1 80 98.0.0.1 5000
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
```

-ooOoo-

Le NAT (Network Address Translation) Dynamique

Les translations d'adresses dynamiques ne sont pas précisément prédéfinies pour une adresse donnée, mais sont effectuées au moment de la connexion.

Ainsi, sur un groupe d'adresses internes privées, par exemple, une translation pourra être effectuée sur la base d'un pool d'adresses publiques.

Il est probable que le nombre d'adresses publiques disponibles pour la translation ne sera jamais suffisant au regard de centaines d'adresses privées voulant accéder à des ressources publiques.

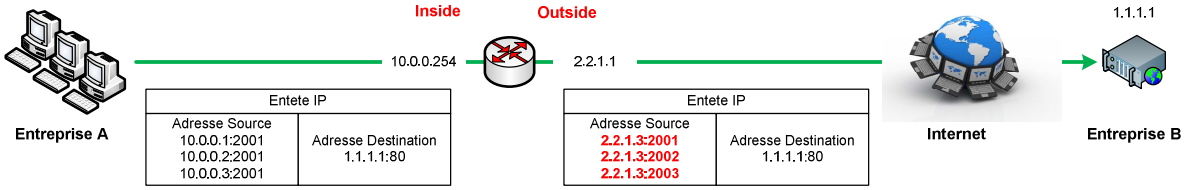
Dans un tel cas, on utilisera conjointement à la translation d'adresses, une technique de multiplexage largement éprouvée dans le monde IP : L'utilisation d'une technique de niveau L4, à savoir Tcp, en effectuant une translation de port.

Comme pour la translation statique, il existe également plusieurs types de translation dynamiques.

Dans l'exemple suivant, plusieurs postes de travail veulent accéder à une ressource publique.ne Ils ne disposent cependant que d'une seule adresse publique pouvant se présenter comme la source de la demande de connexion. On effectuera alors une translation d'adresse sur la source en utilisant cette dernière, et on multiplexera l'information à l'aide d'une translation dynamique de ports.

NAT Dynamique PAT

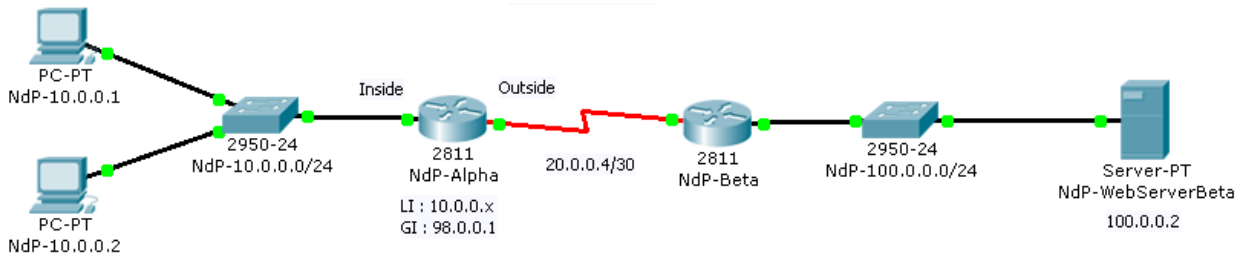
Local Inside	Global inside	Local Outside	Global Outside
10.0.0.1:2001	2.2.1.3:2001	1.1.1.1:80	1.1.1.1:80
10.0.0.2:2001	2.2.1.3:2002	1.1.1.1:80	1.1.1.1:80
10.0.0.3:2001	2.2.1.3:2003	1.1.1.1:80	1.1.1.1:80



Entete IP	
Adresse Source 10.0.0.1:2001 10.0.0.2:2001 10.0.0.3:2001	Adresse Destination 1.1.1.1:80

Entete IP	
Adresse Source 2.2.1.3:2001 2.2.1.3:2002 2.2.1.3:2003	Adresse Destination 1.1.1.1:80

Mise en œuvre sur Packet Tracer 5.3.3 (*Cf fichier « translations.pkt » à télécharger)*



Le bon fonctionnement de cette maquette s'effectue en accédant à partir **des deux postes d'Alpha**, au **NdP-WebServerBeta**, via son adresse 100.0.0.2.

```
NdP-Alpha>sh ip nat trans
Pro  Inside global     Inside local       Outside local      Outside global
tcp 98.0.0.1:1025      10.0.0.1:1025      100.0.0.2:80       100.0.0.2:80
tcp 98.0.0.1:1024      10.0.0.2:1025      100.0.0.2:80       100.0.0.2:80
NdP-Alpha>
```

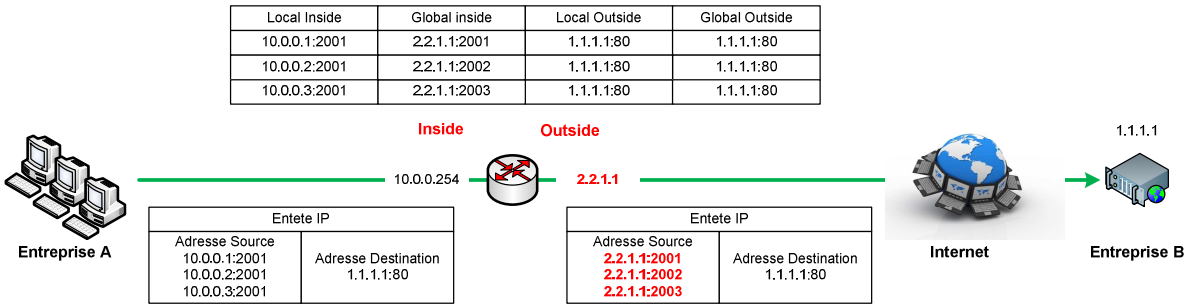
```
NdP-Alpha#sh ip access-lists
Extended IP access list TransInOut
    permit ip 10.0.0.0 0.0.0.255 any (4 match(es))
NdP-Alpha#
```

```
NdP-Alpha#sh run
interface FastEthernet0/0
 ip address 10.0.0.254 255.255.255.0
 ip nat inside
 duplex auto
 speed auto
!
(…)
!
interface Serial0/0/0
 ip address 20.0.0.6 255.255.255.252
```

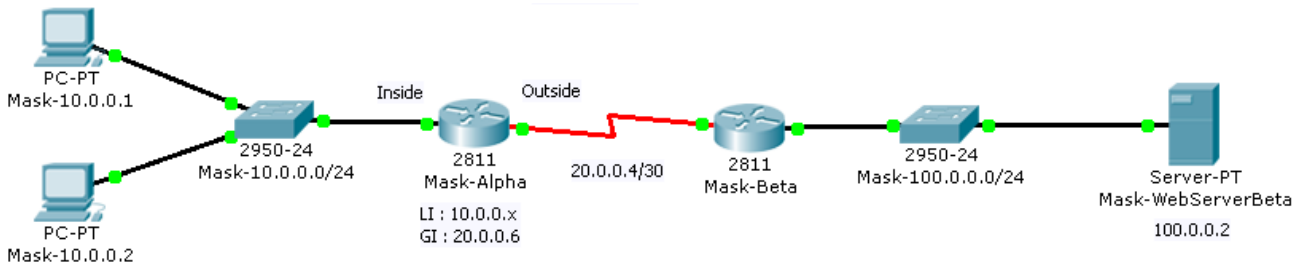
```
 encapsulation ppp
 ip nat outside
 clock rate 4000000
!
(…)
!
ip nat pool PoolInOut 98.0.0.1 98.0.0.1 netmask 255.255.255.0
ip nat inside source list TransInOut pool PoolInOut overload
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
!
!
ip access-list extended TransInOut
 permit ip 10.0.0.0 0.0.0.255 any
!
```

Dans des conditions encore plus restreintes ou, par exemple, la seule adresse publique disponible est déjà affectée à l'interface du routeur, coté **Outside**, on utilisera directement celle-ci, en lui associant une translation dynamique de ports.

Masquerading



Mise en œuvre sur Packet Tracer 5.3.3 (*Cf fichier « translations.pkt » à télécharger)*



Le bon fonctionnement se teste de la même manière que pour le Nat Dynamique Pat. On valide celui-ci par la consultation de la table de translation

```
Mask-Alpha>sh ip nat trans
Pro  Inside global     Inside local       Outside local      Outside global
tcp 20.0.0.6:1025      10.0.0.1:1025      100.0.0.2:80       100.0.0.2:80
tcp 20.0.0.6:1024      10.0.0.2:1025      100.0.0.2:80       100.0.0.2:80
Mask-Alpha>
```

```
Mask-Alpha#sh ip access-lists
Extended IP access list TransInOut
    permit ip 10.0.0.0 0.0.0.255 any (4 match(es))
Mask-Alpha#
```

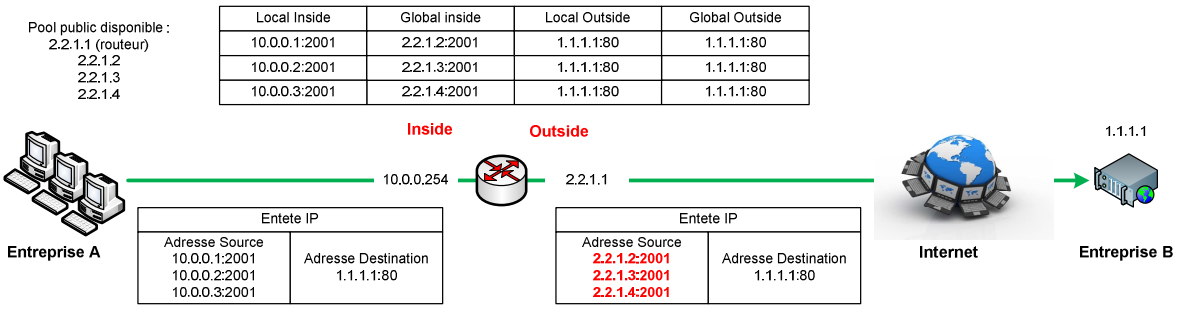
```
interface FastEthernet0/0
 ip address 10.0.0.254 255.255.255.0
 ip nat inside
 duplex auto
 speed auto
!
(…)
!
interface Serial0/0/0
 ip address 20.0.0.6 255.255.255.252
 encapsulation ppp
 ip nat outside
 clock rate 4000000
```

```
(…)
!
ip nat pool PoolInOut 98.0.0.1 98.0.0.1 netmask 255.255.255.0
ip nat inside source list TransInOut interface Serial0/0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
!
ip access-list extended TransInOut
 permit ip 10.0.0.0 0.0.0.255 any
```

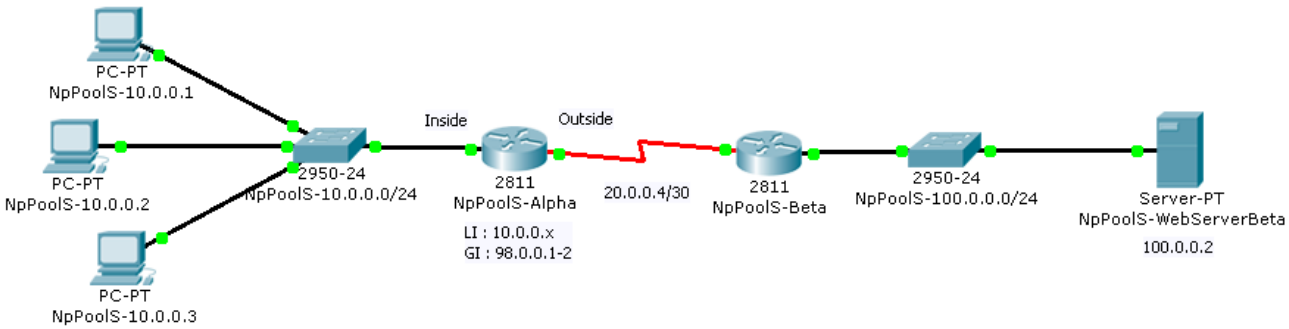
Cette technique repose sur la disponibilité d'un pool d'adresses publiques disponibles important, puisqu'il suppose une affectation privée/publique de **un pour un** *(une adresse publique pour chaque adresse privée)*.

Le port n'est pas modifié. Le fonctionnement de ce type de translation est limité au nombre d'adresses publiques disponibles. Elle n'est plus utilisée.

NAT Pool Source



Mise en œuvre sur Packet Tracer 5.3.3 (*Cf fichier « translations.pkt » à télécharger)*



Le test s'effectue en contactant **NpPoolS-WebServerBeta** à partir des **trois postes** clients d' Alpha. Cela fonctionnera pour deux des postes **mais pas pour le troisième**, le pool d'adresses disponibles n'étant que de deux ***(98.0.0.1 et 98.0.0.2)***.

```
NpPoolS-Alpha>sh ip nat trans
Pro  Inside global     Inside local       Outside local      Outside global
tcp 98.0.0.1:1025      10.0.0.1:1025      100.0.0.2:80       100.0.0.2:80
tcp 98.0.0.2:1025      10.0.0.2:1025      100.0.0.2:80       100.0.0.2:80

NpPoolS-Alpha#sh ip access-lists
Extended IP access list TransInOut
    permit ip 10.0.0.0 0.0.0.255 any (28 match(es))


interface FastEthernet0/0
 ip address 10.0.0.254 255.255.255.0
 ip nat inside
 duplex auto
 speed auto
!
(…)
!
```

```
interface Serial0/0/0
 ip address 20.0.0.6 255.255.255.252
 encapsulation ppp
 ip nat outside
 clock rate 4000000
!
(…)
!
ip nat pool PoolSource 98.0.0.1 98.0.0.2 netmask 255.255.255.0
ip nat inside source list TransInOut pool PoolSource
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
!
!
ip access-list extended TransInOut
 permit ip 10.0.0.0 0.0.0.255 any

NpPoolS-Alpha#
```

NAT Pool Destination

Cette technique consiste à faire une translation d'une adresse de destination vers plusieurs adresses réelles de serveurs.

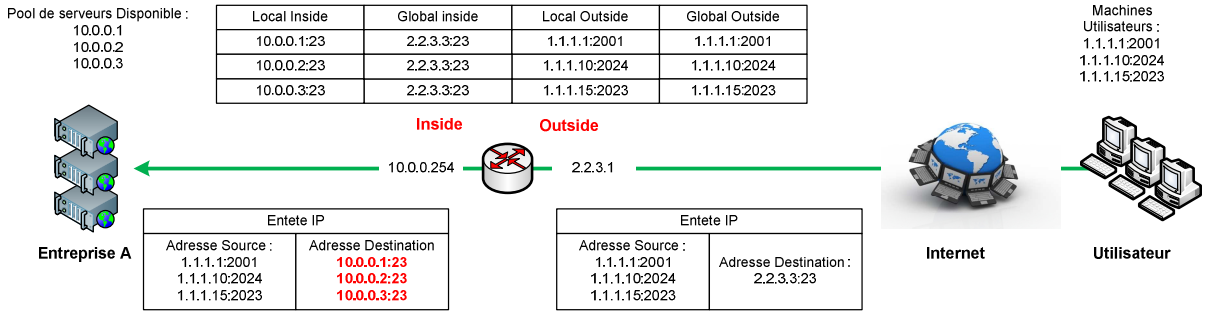
Typiquement, cela revient à faire de la répartition de charge d'une application entre plusieurs serveurs.

Dans l'exemple ci-dessous, on observe les tentatives de connexions de trois postes utilisateurs, vers une même ressource publique, en Telnet ***(2.2.3.3 :23)***.

La translation permet à chacun des trois postes, de se connecter sur un des trois serveurs.

Si un quatrième poste se présentait pour une connexion Telnet, le routeur effectuerait une translation en repartant du début du pool disponible *(10.0.0.1 :23 dans notre exemple)*.

NAT Pool Destination



Mise en œuvre sur Packet Tracer 5.3.3

Ce fonctionnement n'est pas simulable sur Packet Tracer, car il nécessite la mise en place de fonctions particulières de distribution sur le routeur, en frontal de l'entité hébergeant le ressource Web.

L'approvisionnement de la table de translation est, en effet, assuré par le sens des paquets arrivant sur des interfaces internes ou externes…. Il n'est donc pas possible d'effectuer :

- Soit **trois** translations statiques GI pour **une** adresse LI,
- Soit utiliser un pool dynamique, **car le client web est l'initiateur de la connexion**, et par conséquence, n'approvisionne pas la table de translation du routeur frontal au serveur.

-ooOoo-