Rapport Thème Réseau: Translation d'adresse (NAT) sous FreeBSD.

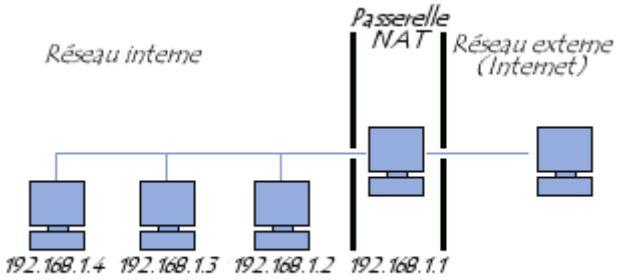
I) Principe :

1) Principe du NAT :

*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 IP avec le protocole IPv4 (le protocole IPv6 répondra à terme à ce problème).*

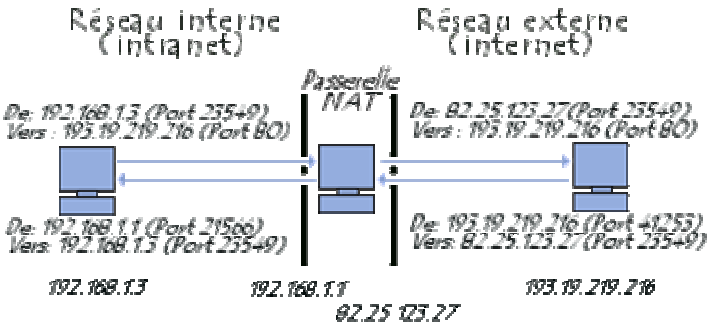
En effet, en adressage IPv4 le nombre d'adresses IP routables (donc uniques sur la planète) n'est pas suffisant pour permettre à toutes les machines le nécessitant d'être connectées à internet.

Le principe du NAT consiste donc à utiliser une passerelle de connexion à internet, possédant au moins une interface réseau connectée sur le réseau interne et au moins une interface réseau connectée à Internet (possédant une adresse IP routable), pour connecter l'ensemble des machines du réseau.



Il s'agit de réaliser, au niveau de la passerelle, une translation (littéralement une « traduction ») des paquets provenant du réseau interne vers le réseau externe.

Ainsi, chaque machine du réseau nécessitant d'accéder à internet est configurée pour utiliser la passerelle NAT (en précisant l'adresse IP de la passerelle dans le champ « Gateway » de ses paramètres TCP/IP). Lorsqu'une machine du réseau effectue une requête vers Internet, la passerelle effectue la requête à sa place, reçoit la réponse, puis la transmet à la machine ayant fait la demande.



Étant donné que la passerelle camoufle complètement l'adressage interne d'un réseau, le mécanisme de translation d'adresses permet d'assurer une fonction de ***sécurisation****. En effet, pour un observateur externe au réseau, toutes les requêtes semblent provenir de l'adresse IP de la passerelle.*

2) Espace d'adressage :

*L'organisme gérant l'espace d'adressage public (adresses IP routables) est l'Internet Assigned Number Authority (****IANA****). La RFC 1918 définit un espace d'adressage privé permettant à toute organisation d'attribuer des adresses IP aux machines de son réseau interne sans risque d'entrer en conflit avec une adresse IP publique allouée par l'IANA. Ces adresses dites non-routables correspondent aux plages d'adresses suivantes :*

- *Classe A : plage de 10.0.0.0 à 10.255.255.255 ;*
- *Classe B : plage de 172.16.0.0 à 172.31.255.255 ;*
- *Classe C : plage de 192.168.0.0 à 192.168.255.55 ;*

Toutes les machines d'un réseau interne, connectées à internet par l'intermédiaire d'un routeur et ne possédant pas d'adresse IP publique doivent utiliser une adresse contenue dans l'une de ces plages. Pour les petits réseaux domestiques, la plage d'adresses de 192.168.0.1 à 192.168.0.255 est généralement utilisée.

3) Translation statique :

Le principe du ***NAT statique*** *consiste à associer une adresse IP publique à une adresse IP privée interne au réseau. Le routeur (ou plus exactement la passerelle) permet donc d'associer à une adresse IP privée (par exemple 192.168.0.1) une adresse IP publique routable sur Internet et de faire la traduction, dans un sens comme dans l'autre, en modifiant l'adresse dans le paquet IP.*

La translation d'adresse statique permet ainsi de connecter des machines du réseau interne à internet de manière transparente mais ne résout pas le problème de la pénurie d'adresse dans la mesure où n adresses IP routables sont nécessaires pour connecter n machines du réseau interne.

4) Translation dynamique :

Le ***NAT dynamique*** *permet de partager une adresse IP routable (ou un nombre réduit d'adresses IP routables) entre plusieurs machines en adressage privé. Ainsi, toutes les machines du réseau interne possèdent virtuellement, vu de l'extérieur, la même adresse IP. C'est la raison pour laquelle le terme de «* ***mascarade IP*** *» (en anglais IP masquerading) est parfois utilisé pour désigner le mécanisme de translation d'adresse dynamique.*

*Afin de pouvoir « multiplexer » (partager) les différentes adresses IP sur une ou plusieurs adresses IP routables le NAT dynamique utilise le mécanisme de translation de port (****PAT*** *- Port Address Translation), c'est-à-dire l'affectation d'un port source différent à chaque requête de telle manière à pouvoir maintenir une correspondance entre les requêtes*

provenant du réseau interne et les réponses des machines sur Internet, toutes adressées à l'adresse IP du routeur.

Port Forwarding :

La translation d'adresse ne permet de relayer que des requêtes provenant du réseau interne vers le réseau externe, ce qu'il signifie qu'il est impossible en tant que tel pour une machine externe d'envoyer un paquet vers une machine du réseau interne. En d'autres termes, les machines du réseau interne ne peuvent pas fonctionner en tant que serveur vis-à-vis de l'extérieur.

*Pour cette raison, il existe une extension du NAT appelée « **redirection de port** » (en anglais Port Forwarding ou Port mapping) consistant à configurer la passerelle pour transmettre à une machine spécifique du réseau interne, tous les paquets réçus sur un port particulier. Ainsi, si l'on souhaite pouvoir accéder de l'extérieur à un serveur web (port 80) fonctionnant sur la machine 192.168.1.2, il sera nécessaire de définir une règle de redirection de port sur la passerelle, redirigeant tous les paquets TCP reçus sur son port 80 vers la machine 192.168.1.2.*

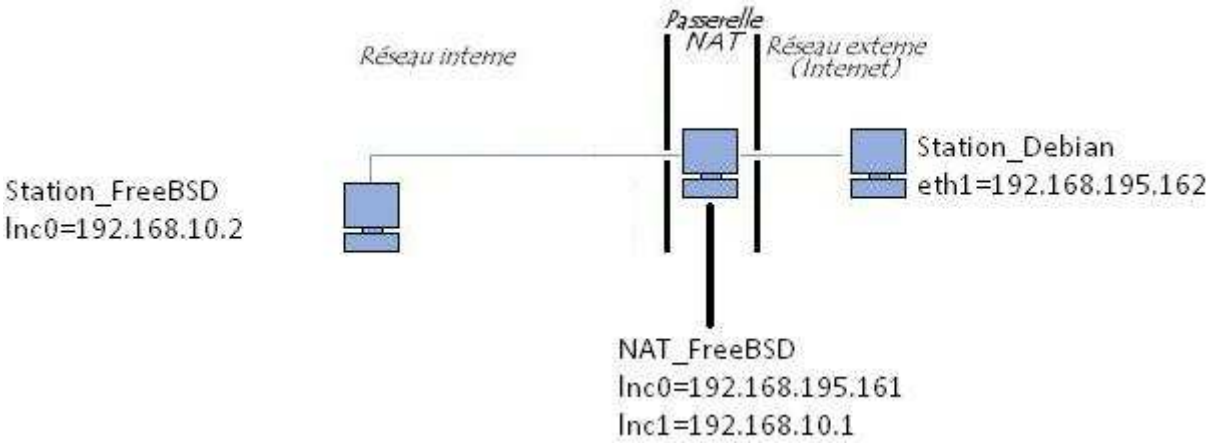
II) Configuartion :

Je vais créer trois machines sous vmware:

Une machine sous FreeBSD qui va jouer le rôle de '' Routeur '' (elle sera nommée NAT_FreeBSD), on lui intégrera 2 cartes réseaux, une carte réseau en mode Bridged pour qu'elle puisse accéder au monde exterieur et une carte réseau sur le réseau interne (sur vmnet5) avec comme adresse IP 192.168.10.1 et comme masque de sous-réseau 255.255.255.0.

Une deuxième machine sous FreeBSD qui va jouer le rôle de '' machine interne '' (elle sera nommée Station_FreeBSD), on lui mettra 1 carte réseau, cette carte réseau sera sur le réseau interne (sur vmnet5) avec comme adresse IP 192.168.10.2 et comme masque de sous-réseau 255.255.255.0. Sa passerelle par défaut sera 192.168.10.1.

Une troisième machine sous Debian (elle sera nommée Station_Debian) qui va jouer le rôle de machine exterieur (machine externe=machine sur Internet), on lui associera une carte réseau qui sera en mode Bridged.



1) <u>Configuration de la machine NAT FreeBSD :</u>

La configuration réseau se fait dans le fichier /etc/rc.conf, on ouvre ce fichier avec vi ou emacs et on tape les lignes suivante :

ifconfig_lnc0=''DHCP''
ifconfig_lnc1=''inet 192.168.10.1 netmask 255.255.255.0''
sshd_enable=''YES''
gateway_enable=''YES''
ipfilter_enable=''YES''
ipnat_enable=''YES''
ipnat_rules=''/etc/ipnat.rules''

Puis dans le fichier /etc/ipf.rules, on doit taper les lignes suivantes :

pass in quick on lnc0 all
pass out quick on lnc0 all

Et pour finir, dans le fichier /etc/ipnat.rules, on doit taper la lignes suivante :

map lnc0 192.168.10.0/24 -> 192.168.195.161

Pour que ces modifications soient prises en comptes, on doit taper en ligne de commande, sur un terminal, ''/etc/rc.conf/netif restart'' puis ''ipf -Fa -f /etc/ipf.rules'' et pour finir ''ipnat -CF -f /etc/ipnat.rules''.

2) <u>Configuration de la machine Station_FreeBSD :</u>

Dans le cas de Station_FreeBSD, on aura seulement à entrer les deux lignes suivantes dans le fichier '' /etc/rc.conf'' :

ifconfig_lnc0=''inet 192.168.10.2 netmask 255.255.255.0''
default_router=''192.168.10.2''

Pour le routeur par défaut (la passerelle), on peut le taper la ligne de commande suivante : route add default 192.168.10.1.

3) <u>Configuration de la machine Debian :</u>

On aura juste à lui indiquer qu'il faut qu'elle obtienne son adresse IP via un serveur DHCP.

<u>Vérifications :</u>

On vérifie que la machine Station1_FreeBSD peut atteindre l'interface 192.168.10.1 (interface réseau sur vmnet5 de la machine NAT_FreeBSD), grâce à la commande ''ping'', puis on vérifie qu'elle puisse atteindre l'interface réseau en mode Bridged de la machine NAT_FreeBSD qui a pour adresse 192.168.195.161.

On vérifie maintenant que 192.168.195.161 (NAT_FreeBSD) peut atteindre l'interface réseau de la machine Station_Debian (Station_Debian a pour adresse 192.168.195.162).

Pour finir, on vérifie que la station qui se trouve dans le réseau interne (Station_FreeBSD) puisse pinger la machine qui se trouve sur le réseau externe (Station_Debian).

On constate que la machine qui se trouve sur le réseau externe (Station_Debian) n'arrive pas à pinger la machine qui se trouve sur le réseau interne (Station_FreeBSD).

<u>Remarque:</u>

On constate que la machine NAT_FreeBSD joue bien le rôle de ''Routeur'' entre le réseau interne et le réseau externe. On peut conclure que la machine NAT_FreeBSD fait de la traduction d'adresse (NAT).

Maintenant on va essayer de configurer la machine NAT_FreeBSD de façon à ce qu'elle fasse des redirections de ports vers la machine Station_FreeBSD. Lorsqu'une machine exterieur (ex: Station_Debian) fera une requête sur le port 22 (ssh) de la machine NAT_FreeBSD, la machine NAT_FreeBSD fera une redirection de cette requête sur le port 22 de la machine Station_FreeBSD (Station qui se trouve sur le réseau interne) cf. 5)Port Forwarding*.*

Pour faire une redirection de port, soyez sûr d'avoir installer un serveur ssh sur la machine interne (Station_FreeBSD) et sur la machine externe (Station_Debian). La machine qui fait le rôle de ''Routeur'' (NAT_FreeBSD) n'a pas besoin d'être équipé d'un serveur ssh. Sur les machines Free_BSD, un serveur ssh est déjà installé.

En ce qui concerne la configuration pour la redirection de port , on aura seulement à ajouter une ligne dans le fichier ''/etc/ipnat.rules''de la machine NAT_FreeBSD, la ligne est la suivante :

rdr lnc0 192.168.195.161/32 port 22 -> 192.168.10.2 port 22

Ne pas oublier de taper la commande ''ipnat -CF -f /etc/ipnat.rules'' pour que la ligne qui a été ajouter dans le fichier ''/etc/ipnat.rules'' soit prise en compte.

Commande à taper sur la station qui se trouve sur le réseau externe (Station_Debian):

ssh root@192.168.195.161

Remarque:

L'identifiant doit être celui de la machine NAT_FreeBSD.
L'adresse IP doit être celle de la machine qui fait le rôle de NAT (NAT_FreeBSD); la machine qui se trouve dans le réseau interne (Station_FreeBSD) est invisible pour les machines qui se trouve sur Internet (monde externe). Lorsque l'on vous demande le password, mettre le password de la machine interne (Station_Debian).