I- NAT ?

La version actuelle du protocole IP (IPV4) propose des adresses IP codées sur 32 bits. Ceci implique que dans le monde, il peut y avoir 2^32 soit environ 4 milliards d'adresse IP. Ce nombre d'adresses devient critique de nos jours, c'est pourquoi IPV6 devrait s'imposer dans les années à venir.

NAT (***Network Address Translation,*** en Français Translation d'Adresse Réseau) est un mécanisme destiné à faire correspondre un réseau entier (ou des réseaux) à une seule adresse IP. C'est un des bricolages trouvé pour résoudre le problème de pénurie d'adresse.

Le principe consiste à cacher tout son LAN privé, derrière une seule machine directement connectée à Internet. Il n'y à donc qu'une seule machine avec IP publique, qui s'arrangera pour faire passer toutes les requêtes provenant des machines internes, sous son adresse IP (figure 1).

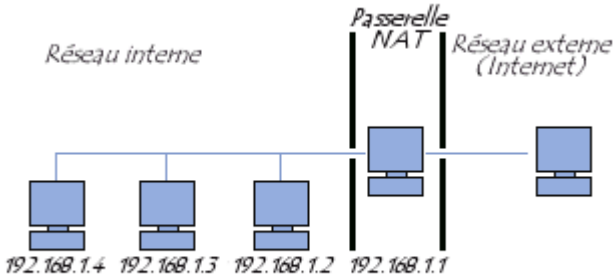

Figure 1

II- Fonctionnement de NAT

Lorsqu'un client du réseau interne entre en communication avec une machine sur Internet, il envoie des paquets IP à destination de cette machine. Ces paquets contiennent toutes les informations sur leur émetteur et leur destinataire nécessaires à leur bon acheminement. La NAT prend en compte les informations suivantes :

- l'adresse IP source (192.168.1.10 par exemple)
- le port TCP ou UDP source (2132 par exemple)

Lorsque les paquets passent à travers la machine-passerelle NAT, ils sont modifiés de telle façon à ce qu'ils semblent provenir de la passerelle NAT. Cette passerelle enregistrera les modifications effectuées dans sa table d'état afin de :

1. inverser les modifications pour les paquets de retour
2. s'assurer que les paquets de retour sont autorisés à traverser le pare-feu et ne sont pas bloqués

Par exemple, les modifications suivantes peuvent être effectuées :

- adresse IP source : remplacée par l'adresse externe de la passerelle (24.5.0.5 par exemple)
- port source : remplacé par un port non utilisé sur la passerelle et choisi de manière aléatoire (53136 par exemple)

Aucune des deux extrémités de la communication ne se rend compte de ces modifications. Pour la machine interne, le système qui effectue la NAT est simplement une passerelle Internet. Pour l'hôte

sur Internet, les paquets semblent provenir directement du système de NAT; il ne sait même pas que la machine interne existe.

Lorsque l'hôte sur Internet répond aux paquets de la machine interne, ils seront envoyés à l'adresse IP externe de la passerelle NAT (24.5.0.5) sur le port de traduction (53136). Dès réception de ces paquets, la passerelle NAT cherchera dans sa table d'état si ces paquets de retour correspondent à une connexion déjà établie.

Une correspondance unique sera trouvée, basée sur la combinaison IP/port qui permet à la passerelle de voir que les paquets appartiennent à une connexion initiée par la machine interne 192.168.1.10. La passerelle effectuera alors les modifications inverses à celles effectuées sur les paquets sortants puis enverra ces paquets à la machine interne.

III- Pré-requis pour la mise en œuvre de NAT sous OpenBSD 4.2

III.1- Interfaces réseau

La mise en œuvre de NAT sur une machine fonctionnant sous OpenBSD nécessitera au moins deux cartes réseau: une connectée à internet et l'autre connectée au réseau privé interne.

III.2- Activation du routage IP

L'activation du routage IP est nécessaire pour permettre aux paquets de traverser les interfaces réseau du système OpenBSD. L'activation du routage IP se fait par l'exécution des commandes suivantes:

```
sysctl net.inet.ip.forwarding=1
sysctl net.inet6.ip6.forwarding=1    (si ipv6 est utilisé)
```

Pour rendre cette modification permanente lors de chaque démarrage du système, les lignes suivantes doivent être ajoutées au fichier **/etc/sysctl.conf** :

```
net.inet.ip.forwarding=1
net.inet6.ip6.forwarding=1
```

Remarque: ces lignes sont déjà présentes dans l'installation par défaut mais sont commentées (préfixées avec un caractère #). Supprimez le # et sauvegardez le fichier.

III.3- Activation de Packet Filter

Packet Filter (PF) est le pare-feu logiciel officiel d'OpenBSD. Ce pare-feu contient un ensemble de règles de filtrages contenues dans le fichier /etc/pf.conf. Il est essentiel de bien configurer PF pour faire de la translation d'adresse sous OpenBSD.

Pour activer PF, il faut éditer le fichier /etc/rc.conf afin qu'il contienne la ligne suivante :

```
PF= « YES »  ;
```

Pour activer/désactiver manuellement Packet filter, on utilisera les commandes :

```
Pfctl –e (activation)
Pfctl –d (désactivation)
```

IV- Configuration de NAT sous OpenBSD 4.2

IV.1- Utilisation générale

La configuration du NAT sous OpenBSD se fait par l'utilisation de l'instruction ***nat*** dans le fichier de configuration des règles de Packet Filter se trouvant à l'emplacement /etc/pf.conf.

L'instruction NAT permet de "cacher" une machine ou un réseau derrière la passerelle NAT. Elle possède de nombreux paramètres détaillés dans le man. Une syntaxe d'utilisation "standard" pourrait être la suivante :

```
nat on [interface externe] from [debut poule d'adresse source] to [debut
       poule d'adresse source] -> [adresse/interface destination]
```

Voici un exemple d'utilisation :

```
nat on pcn0 from 192.168.1.0/24 to any -> 24.5.0.5
```

Cette règle permet d'effectuer une translation d'adresse sur l'interface pcn0 sur tout paquet provenant du réseau 192.168.1.0/24 et remplace l'adresse IP source par 24.5.0.5. On rappelle que pcn0 est l'interface interne. On rappelle que cette règle a été écrite à la fin du fichier pf.conf.

IV.2- Utilisation « statique »

Le principe du NAT statique consiste à associer une adresse IP externe à une adresse IP interne au réseau. Ce type de NAT permet ainsi de connecter des machines du réseau interne à internet de manière transparente.

Ceci peut être pratique par exemple pour permettre à un serveur web interne d'avoir sa propre adresse de traduction externe. Les connexions en provenance d'Internet à destination de cette adresse externe seront acheminées vers l'adresse interne du serveur web.

Quant aux requêtes émanant du serveur web (telles que les requêtes DNS), elles seront traduites de telle façon à remplacer l'adresse interne par l'adresse externe de traduction attribuée au serveur web.

Une mise en correspondance bidirectionnelle (traduction 1 à 1) sous OpenBSD peut être établie en utilisant l'instruction ***binat***. Binat s'utilise de la même façon que la commande nat.

Il suffit maintenant désactiver puis d'activer PF afin que les modifications NAT soient prises en compte.

IV.3- Vérification de l'état de NAT

Pour voir les traductions actives, il faut utiliser pfctl avec l'option -s state. Cette option affichera une liste de toutes les sessions NAT en cours. Voici un exemple de son utilisation

```
# pfctl -s state
pcn0 TCP 192.168.1.35:2132 -> 24.5.0.5:53136 -> 65.42.33.245:22
TIME_WAIT:TIME_WAIT
```

Dans cet exemple, on peut voir qu'une translation d'adresse est active sur l'interface externe pcn0.

- Le protocole utilisé par cette connexion est TCP
- La machine interne mise en en a pour adresse IP privée 192.168.1.35 utilisant le port 2132

- L'adresse Ip externe utilisée est 24.5.0.5 via le port 53136
- La machine interne est connectée à une machine sur Internet ayant pour adresse IP 65.42.33.245, et cette connexion se fait via son port 22

Liens externes

http://fr.wikipedia.org/wiki/Network_address_translation
http://www.openbsd.org/faq/pf/fr/nat.html
http://www.commentcamarche.net/internet/nat.php3
man pf.conf