2ème année 2014-2015

La traduction d'adresse

Décembre 2014

Objectifs

Traduction d'adresse : La traduction d'adresse (réseau) consiste à modifier des paquets IP afin de faire croire à une partie du réseau qu'ils ont été émis par (ou à destination de) une machine différente de celle qui en est réellement l'émetteur (ou le destinataire).

La traduction d'adresse (ou NAT pour *network address translation*) consiste à remplacer les adresses IP de certains paquets par d'autres adresses prédéterminées. La figure 1 donne un exemple de traduction d'adresse.

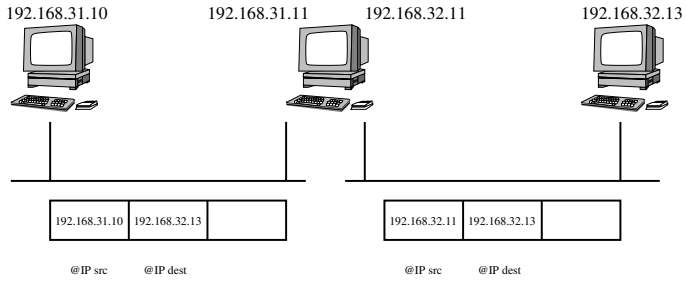

FIGURE 1 – La traduction d'adresse.

Le but est généralement de cacher des adresses ; ce qui peut-être utile notemment dans les cas suivants :

— ces adresses n'ont pas été obtenues officiellement, elles ne sont donc pas légitimes et ne peuvent pas être routées convenablement ;
— on souhaite ne rendre publique qu'un nombre limité d'adresses.

Linux permet de réaliser la traduction d'adresse. Ce mécanisme était auparavent nommé "masquerading". Dans la version 2.6 de Linux, la traduction d'adresse est réalisée par le biais d'une table intégrée dans le mécanisme de filtrage, que nous étudierons plus loin. Elle se manipule donc avec le même outil, la commande `iptables`.

Cette commande permet de manipuler des *tables*, ces tables étant composées de *chaînes*. La figure 2 montre les trois chaînes de la table `nat`.

Le principe est simple : lorsqu'un paquet arrive sur la machine, il passe par la chaîne `PREROUTING` avant de subir le verdict de la décision de l'algorithme de routage puis soit il passe par la chaîne `POSTROUTING` avant d'être émis, soit il est délivré localement. Lorsqu'un paquet est généré localement sur la machine, il passe par la chaîne `OUTPUT` puis il passe par la chaîne `POSTROUTING` avant d'être émis.

Sur chacune de ces chaînes, chaque paquet peut subir une traduction d'adresse. Il peut s'agir d'une traduction de l'adresse source `snat` ou de l'adresse destination `dnat`.

On utilise la commande `iptables` de la façon suivante

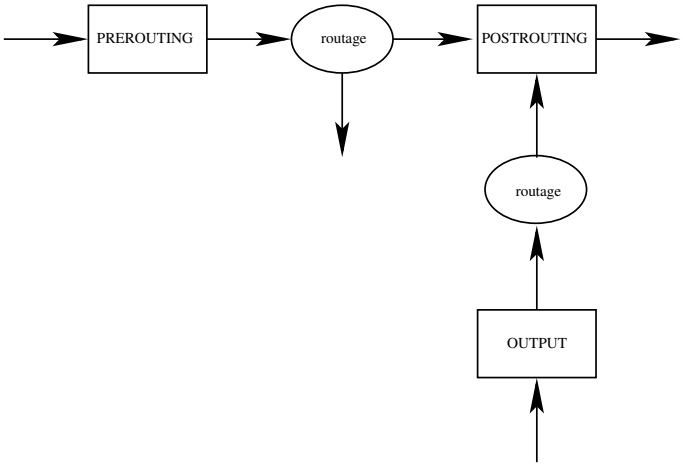

FIGURE 2 – Les chaînes du NAT.

— `iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 192.168.31.11` permet de changer l'adresse source (`SNAT` de paquets sortant par l'interface `eth0`
— `iptables -t nat -A POSTROUTING -p tcp --dport 80 -o eth0 -j SNAT --to 192.168.31.11` réalise la même chose mais pour le port 80 du protocole TCP uniquement
— `iptables -t nat -A PREROUTING -p tcp -d 147.127.0.0/16 -dport 80 -j DNAT --to 147.127.16.100:8080` permet de traduire l'adresse destination de tout paquet à destination du port 80 d'une machine du réseau 147.127.0.0 vers l'adresse 147.127.16.100, port 8080.

▷ **Exercice 1 : Mise en place de la traduction d'adresse**

Après avoir mis en place un réseau tel que celui de la figure 1, expérimentez la traduction d'adresse.

Utilisez `tcpdump` *(ou* `ethereal`*) pour constater l'effet sur les paquets qui circulent sur les réseaux.* ■