Thème 12 : Traduction d'adresse sous Linux

A.PRINCIPE

Le NAT pour "Network Address Translation" (ou Traduction d'Adresse Réseau en français) permet d'utiliser des adresses IP privées sur le LAN et de translater ces adresses afin de les rendre accessible depuis un réseau public comme Internet. La machine faisant du NAT reçoit les paquets et les modifie pour offrir un accès au Net. Ainsi, les machines de l'ensemble du réseau local peuvent partager une seule et même connexion. Il existe deux sortes de NAT :

- Le DNAT (Destination NAT) permet de modifier l'adresse de destination des paquets réseaux. Ce type de NAT se fait avant le routage.
- Nous avons aussi le SNAT (Source NAT). A ce niveau, c'est l'adresse source des paquets réseau qui est modifiée. Ainsi, toutes les connexions qui sont faites depuis l'intérieur du réseau local semblent provenir de la même machine : la machine faisant le NAT. Le SNAT se fait après le routage.

B.CONFIGURATION DU NAT

1. Préliminaire : activer ip forwarding

Pour autoriser les paquets entrant sur une interface réseau à transiter sur une autre interface réseau, il faut activer l'ip forwarding. Cela peut se faire manuellement avec la commande suivante :

echo 1 > /proc/sys/net/ipv4/ip_forward

Mais dans ce cas, l'ip forwarding sera désactivé au prochain redémarrage de l'ordinateur. Pour l'activer en permanence, sous Debian, il existe au moins deux méthodes.

La première consiste à l'activer lors du démarrage d'une interface réseau (exemple : eth0) en modifiant le fichier "/**etc/network/interfaces**", ce qui donne :

iface eth0 inet loopback

up echo 1 > /proc/sys/net/ipv4/ip_forward

La deuxième méthode consiste à mettre "**ip_forward=yes**" à la place de "**ip_forward=no**" dans le fichier "**/etc/network/options**". Ce qui donne dans ce cas :

ip_forward=yes

spoofprotect=yes

syncookies=no

2. Netfilder

Netfilder est le module qui fournit à Linux les fonctions de pare-feu, de **traduction d'adresse** et d'historisation du trafic réseau. Netfilter fonctionne en mode noyau. Il intercepte et manipule les paquets IP avant et après le routage.

Iptables est la commande qui permet à un administrateur réseaux de configurer Netfilter en espace utilisateur. Nous pouvons installer iptables à partir des paquets Debian en tapant la commande : *apt-get install iptables* ou à l'aide du paquet : *dpkg –i iptables_1.2.6a-5_i386.deb.*

3. Traduction d'adresse

Nous distinguons de deux (2) types de chaînes (ou règles) pour le NAT : le PREROUTING (paquets entrants sur le firewall) et le POSTROUTING (paquets sortants du firewall).

✓ *MASQUERADE (uniquement POSTROUTING)*

La passerelle transforme les paquets sortants pour donner l'illusion qu'ils sortent de celle-ci par un port alloué dynamiquement ; lorsque la passerelle reçoit une réponse (d'Internet par exemple) sur ce port, elle utilise une table de correspondance entre le port et les machines du réseau local qu'elle gère pour lui faire suivre le paquet.

Exemple : *iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE ;*
/* Ce qui s'explique par :

-t nat	pour indiquer l'utilisation de la table NAT.
-A POSTROUTING	pour ajouter la règle sur les paquets sortant de l'interface.
-o eth1	pour indiquer l'interface (celle de l'extérieur).
-j MASQUERADE	pour indiquer l'échange de l'adresse IP avec celle du serveur*/

Ainsi, tous les paquets sortant par eth1 auront l'ip d'eth1.

✓ DNAT (uniquement PREROUTING)

Ceci est réalisé dans la chaîne PREROUTING, au moment où le paquet arrive. Le NAT de destination est spécifié en utilisant **"-j DNAT"', et l'option "--to-destination"** qui spécifie une adresse IP, une plage d'adresses IP, et éventuellement un port ou une plage de ports.

// Changer l'adresse de destination en 5.6.7.8

iptables -t nat -A PREROUTING -i eth0 -j DNAT --to 5.6.7.8

// Changer l'adresse de destination en 5.6.7.8, 5.6.7.9 ou 5.6.7.10

iptables -t nat -A PREROUTING -i eth0 -j DNAT --to 5.6.7.8-5.6.7.10

// Changer l'adresse de destination du trafic web en 5.6.7.8, port 8080

iptables -t nat -A PREROUTING -p tcp --dport 80 -i eth0 \ -j DNAT --to 5.6.7.8:8080

Redirection

Il y a un cas spécialisé de NAT de destination appelé redirection : c'est une simple facilité qui est exactement équivalente à faire du DNAT vers l'adresse de l'interface d'entrée.

// Envoyer le trafic web entrant du port 80 vers un mandataire transparent

iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 \ -j REDIRECT --to-port 3128

- ✓ SNAT (uniquement POSTOUTING)

Le NAT de source est spécifié en utilisant les options "**-j SNAT", et "--to-source**" qui spécifie une adresse IP, une plage d'adresses IP, et éventuellement un port ou une plage de ports.

// Changer l'adresse source en 1.2.3.4

iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 1.2.3.4

// Changer l'adresse source en 1.2.3.4, 1.2.3.5 ou 1.2.3.6

iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 1.2.3.4-1.2.3.6

// Changer l'adresse source en 1.2.3.4, port 1-1023

iptables -t nat -A POSTROUTING -p tcp -o eth0 -j SNAT --to 1.2.3.4:1-1023

Très important : Toutes ces lignes de commandes ci-dessus peuvent être sauvées dans un fichier pour éviter de les réinitialiser à chaque redémarrage. Le fichier pourra être créé dans **/etc ou /etc/rc.local** selon la distribution.

C. PROTOCOLES SUPPORTES

La syntaxe générale de iptables est :

iptables -A <nom_de_la_chaine> <condition>..<condition> -j <cible>

où parmi les conditions disponibles, nous avons l'option *"-p" qui* spécifie le protocole. Les protocoles supportés par iptables sont ***tcp***, ***udp*** et ***icmp***. Pour spécifier les trois protocoles à la fois, on utilise **all.** En dehors de ces trois protocoles, nous pouvons adapter d'autres protocoles comme le montre l'exemple de FTP suivant :

Pour accepter le trafic FTP, on met dans le fichier de configuration les deux lignes en italiques :

iptables -A INPUT -i eth0 -p tcp -sport 21 -m state --state ESTABLISHED -j ACCEPT

// Pour accepter les trames FTP qui rentrent sur l'interface eth0 seulement si c'est une connexion déjà établis.

iptables -A OUTPUT -o eth0 -p tcp -dport 21 -m state --state NEW,ESTABLISHED -j ACCEPT

// Pour accepter les trames FTP qui sortent si c'est une nouvelle connexion ou une connexion déjà établis.