TP Firewall et Masquerading

Olivier AUBERT

28 février 2002

On va voir dans ce TP comment utiliser une machine linux pour effectuer du *masquerading* (ou `Network Address Translation` en mode *One-To-Many*). Ce mode permet à une machine de servir de passerelle de manière transparente à un réseau local. Les adresses privées du réseau local ne sont pas visibles de l'extérieur, seule l'adresse de la passerelle l'est.

Pour plus d'informations, reportez-vous au fichier `/usr/share/doc/HOWTO/en-txt/IP-Masquerading-HOWTO.gz` (consultable avec la commande `zless`).

1 Configuration réseau

On va simuler une telle configuration en utilisant deux machines : la première sera la passerelle, la seconde représentera le réseau local.

L'adresse de la machine du réseau local sera `192.168.1.2`. La passerelle disposera de deux adresses : une sur le réseau local `192.168.1.1` et une autre sur le réseau global, indiquée sur l'étiquette de la machine.

Effectuez une RAZ des machine (procédure `debpotato restore=...` au boot). Effectuez le câblage et la configuration réseau adéquats.

Sur les machines locales, indiquez `192.168.1.1` comme passerelle par défaut via la commande `route`.

Sur les passerelles, activez le transfert de paquets IP par la commande

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

Testez la connectivité entre les différentes machines passerelle. Essayez de faire de même depuis la machine locale : vers la passerelle, et vers d'autres machines passerelle. Pendant ces manipulations, il est intéressant d'utiliser `ethereal` ou `tcpdump` pour observer le trafic du réseau. Les paquets de la machine locale sont bien transmis sur le réseau global, mais ne donnent pas de résultat. Une explication ?

2 Initialisation

On utilise la commande `ipchains` pour manipuler les règles de filtrage de la passerelle. `man ipchains` en donne la syntaxe. Sur la machine passerelle, affichez les politiques par défaut par la commande `ipchains -L`. Pour supprimer toutes les politiques, utilisez la commande `ipchains -F` (*flush*).

Pour préciser une règle de filtrage, on précise plusieurs paramètres : le type de flux (`input`, `output` ou `forward`), l'interface concernée, le protocole traité, l'adresse source, l'adresse destination et l'action à entreprendre (`ACCEPT`, `REJECT`, `DENY`, `MASQ`).

Modifiez les politiques par défaut par les commandes

```
ipchains -P input REJECT
ipchains -P output REJECT
ipchains -P forward REJECT
```

Testez la connectivité dans diverses combinaisons (local/passerelle, de passerelle à passerelle).

3 Accepter un flux local

On va tout d'abord rétablir la connectivité du réseau local. Pour cela, il faut autoriser l'émission de paquets vers le réseau local :

```
ipchains -A output -d 192.168.1.0/24 -j ACCEPT
```

`ping 192.168.1.2` tente bien maintenant d'envoyer des paquets, mais ne reçoit rien. Pour régler cela, il faut autoriser la réception des paquets du réseau local :

```
ipchains -A input -s 192.168.1.0/24 -j ACCEPT
```

Le ping fonctionne à présent correctement entre la passerelle et le réseau local.

4 Activer les liaisons au réseau global

On veut sécuriser le site, donc on autorise les connexions sortantes en TCP seulement vers le réseau global, mais aucune connexion entrante depuis le réseau global. Pour identifier le réseau global, on précise l'identificateur de la carte réseau correspondante.

```
ipchains -A output -p tcp -i eth0 -j ACCEPT
ipchains -A input -p tcp -i eth0 ! -y -j ACCEPT
```

Depuis la passerelle, `telnet` fonctionne. `ping` ne fonctionne pas. Pourquoi ? Comment faire fonctionner le ping ?

La passerelle est à présent capable de communiquer avec son réseau local et avec son réseau global. Elle va pouvoir servir à faire la passerelle entre les deux.

5 Masquerading inconditionnel du réseau local

On va dans un premier temps effectuer une translation d'adresse inconditionnelle de tous les paquets originaires du réseau local :

```
ipchains -b -A forward -s 192.168.1.0/24  -j MASQ
```

Il est à présent possible, depuis la machine locale, de se connecter (`telnet`, `ping`) vers une machine du réseau global. Lancez `ethereal` sur la passerelle, observez les deux interfaces réseau (`eth0` et `eth1`) en parallèle pour voir quels sont les paquets qui transitent. Quelles observations pouvez vous effectuer, notamment sur les adresses de source et de destination indiquées dans les paquets ?

Pouvez-vous, depuis une machine du réseau global, vous connecter à votre machine locale ? Quelles sont les conséquences sur la sécurité de votre réseau local ?

6 Masquerading spécifique

On va effectuer un masquerading plus ciblé de certains services uniquement. Pour cela, on va commencer par annuler les règles de forward :

```
ipchains -F forward
```

On va ensuite activer le forwarding plus spécifique du service de `ping` :

```
ipchains -A forward -p icmp -s 192.168.1.0/24 -j MASQ
```

Testez l'efficacité de cette configuration.

On va a présent activer le protocole `telnet` vers l'extérieur. En français : on transmet les paquets TCP ayant pour source le réseau 192.168.1.0/24 avec un port supérieur à 1024, et à destination de n'importe quelle adresse (0/0) sur le port de telnet (vous devez savoir comment le trouver...). Pour ces paquets, on va effectuer le masquerading d'adresse.

Traduisez la règle ci-dessus en une ligne de commande `ipchains` permettant à une machine locale de se connecter via `telnet` à une machine du réseau global. Testez...

7 Gestion de protocoles spécifiques

Certains protocoles ont un fonctionnement particulier qui impose de les gérer spécialement, comme IRC, RealAudio, CU-SeeMe ou ftp. Pour cela, il faut activer un module particulier dans Linux afin que le protocole soit géré correctement. Nous allons voir l'exemple de ftp.

Configurez la translation d'adresses de manière à pouvoir vous connecter via ftp à un serveur (il peut être nécessaire de déclarer un utilisateur de test sur le serveur). Tentez une commande de type `ls` ou `get`.

Le protocole *ftp* utilise deux connexions : la première est une connexion de contrôle, permettant d'envoyer les commandes, initiée depuis la machine client. La seconde est une connexion de données, initiée par le serveur pour renvoyer les résultats des commandes. Cette initiation par le serveur d'une connexion impose la modification des règles d'accès au réseau extérieur (accepter les initiations de connexion depuis le réseau extérieur). Ceci permet d'effectuer du ftp depuis la passerelle.

Pour que la translation d'adresse fonctionne correctement depuis la machine locale, il faut que la passerelle adopte un comportement particulier pour les connexions ftp, de manière à pouvoir effectuer la connexion de données correctement. Pour cela, il faut activer le module noyau correspondant par la commande `modprobe ip_masq_ftp`.

Effectuez des tests en observant notamment les trafics réseau et les différents établissements de connexions TCP.