Guide pratique de l'IP masquerade simplifié

Nouvelles versions de ce document

Version française du *Masquerading made simple HOWTO*

John Tapsell

<tapselj0@cs.man.ac.uk>

Thomas Spellman

<thomasNO@SPAMresonancePLEASE.org>

Matthias Grimm

<DeadBull@gmx.net>

Version : 0.09.fr.1.0

10 octobre 2007

Revision History

Revision 0.09.fr.1.0	2007-10-07	Revised by: EM
Première traduction française		
Revision 0.09	2004-07-21	Revised by: TS
Revision 0.08	2002-07-11	Revised by: JPT
Revision 0.07	2002-02-27	Revised by: JPT
Revision 0.06	2001-09-08	Revised by: JPT
Revision 0.05	2001-09-07	Revised by: JPT
Revision 0.04	2001-09-01	Revised by: JPT
Revision 0.03	2001-07-06	Revised by: JPT

Ce guide pratique NE REMPLACE PAS le 'guide pratique de l'IP masquerade', mais le complète. Ces deux documents devraient être lus en parallèle. Je n'y ai inclu aucun élément déjà détaillé dans cet autre guide pratique, ni aucune explication sur leur fonctionnement et leur signification. Veuillez vous reporter à l'adresse http://ipmasq.webhop.net/ et lisez le 'guide pratique du masquerade standard', pour une bien meilleure aide.

Résumé

Ce document décrit l'activation du dispositif dIP Masquerading sur une machine hôte Linux. Le masquage d'adresse IP est une forme de traduction d'adresse réseau (Network Address Translation ou NAT en anglais),permettant aux ordinateurs d'un réseau privé n'ayant aucune adresse IP d'accéder à Internet via l'adresser IP unique d'une machine Linux.

Tous les auteurs sont joignables sur le canal #debian sur irc.opensource.net

John Tapsell (JohnFlux) est le responsable officiel.

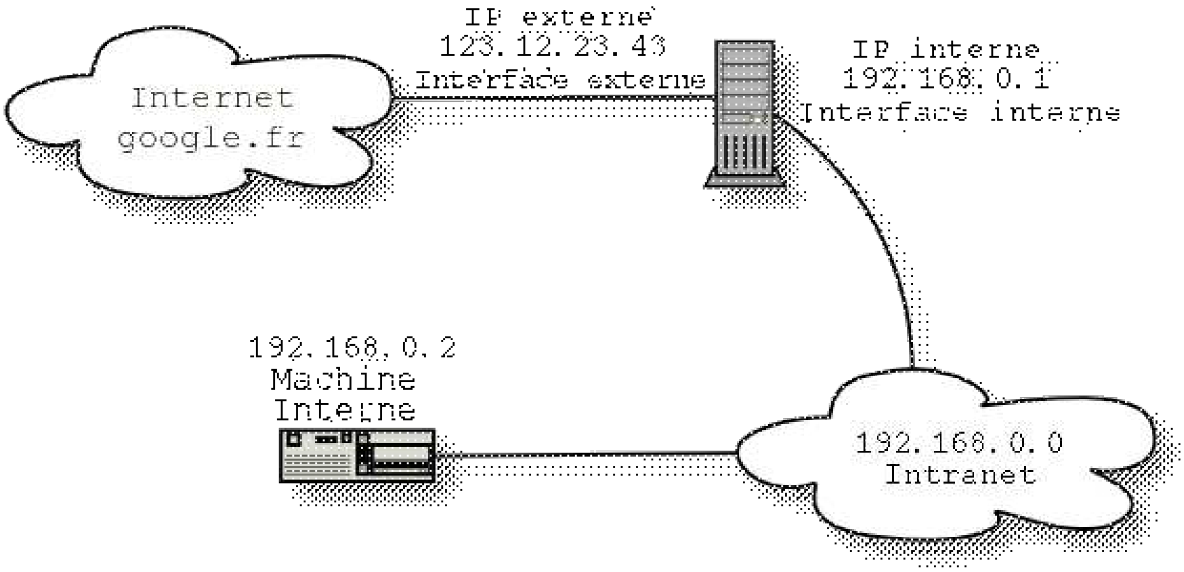
Contactez-moi (John Tapsell) pour toutes demandes, réactions, réclamations, rendez-vous, etc. !!!!!!!!!

Impudemment tiré du travail de David Ranch - <dranch@trinnet.net>

Introduction

Cette introduction est volontairement courte et ciblée.

Admettons que vous aviez un réseau que vous voulez raccorder à l'extérieur:



Sommaire (J'aime bien débuter par un sommaire!)

Considérons que l'interface réseau externe est eth0, l'adresse IP 123.12.23.43 et l'interface réseau interne est eth1 :

```
$> modprobe ipt_MASQUERADE # Si cela échoue, essayez tout-de-même de continuer
$> iptables -F; iptables -t nat -F; iptables -t mangle -F
$> iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 123.12.23.43
$> echo 1 > /proc/sys/net/ipv4/ip_forward
```

Ou pour une connexion par modem:

```
$> modprobe ipt_MASQUERADE # Si cela échoue, essayez tout-de-même de continuer
$> iptables -F; iptables -t nat -F; iptables -t mangle -F
$> iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE
$> echo 1 > /proc/sys/net/ipv4/ip_forward
```

Pour sécuriser cela:

```
$> iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

```
$> iptables -A INPUT -m state --state NEW -i ! eth0 -j ACCEPT
$> iptables -P INPUT DROP   #seulement si les deux commandes précédentes ont abouties
$> iptables -A FORWARD -i eth0 -o eth0 -j REJECT
```

Ou pour une connexion par modem (avec eth0 comme interface réseau interne):

```
$> iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
$> iptables -A INPUT -m state --state NEW -i ! ppp0 -j ACCEPT
$> iptables -P INPUT DROP   #seulement si les deux commandes précédentes ont abouties
$> iptables -A FORWARD -i ppp0 -o ppp0 -j REJECT
```

Et voilà! Pour visualiser les règles tapez "**iptables -t nat -L**"

Version un peu plus détaillée

Compilation du noyau: (Utilisez un noyau 2.4.x ou supérieur)

Le noyau doit inclure les supports suivants:

- Dans la section Networking Options
    - Network packet filtering (CONFIG_NETFILTER)
- Section Networking Options->Netfilter Configuration
    - Connection tracking (CONFIG_IP_NF_CONNTRACK)
    - FTP Protocol support (CONFIG_IP_NF_FTP)
    - IP tables support (CONFIG_IP_NF_IPTABLES)
    - Connection state match support (CONFIG_IP_NF_MATCH_STATE)
    - Packet filtering (CONFIG_IP_NF_FILTER)
        - REJECT target support (CONFIG_IP_NF_TARGET_REJECT)
    - Full NAT (CONFIG_IP_NF_NAT)
        - MASQUERADE target support (CONFIG_IP_NF_TARGET_MASQUERADE)
        - REDIRECT target support (CONFIG_IP_NF_TARGET_REDIRECT)
    - Packet mangling (CONFIG_IP_NF_MANGLE)
    - LOG target support (CONFIG_IP_NF_TARGET_LOG)

Tout d'abord, si les modules iptables et masq ne sont pas compilés dans le noyau ni installés, mais présents en tant que modules, il faut les installer. Si vous chargez le module ipt_MASQUERADE,les modules ip_tables, ip_conntrack et iptable_nat seront aussi chargés.

```
$> modprobe ipt_MASQUERADE
```

Que votre réseau interne soit vaste, ou bien que vous vouliez connecter deux ou trois machines sur Internet, cela ne fera aucune différence dans tous les cas.

Ok, je vais suppposer que vous n'avez aucune autre règle à rajouter, donc vous tapez:

```
$> iptables -F; iptables -t nat -F; iptables -t mangle -F
```

Si vous obtenez un message d'erreur indiquant "can't find iptables", téléchargez-le et installez-le. Si le message d'erreur indique "no such table 'nat'", recompilez le noyau avec le support nat. Si le message d'erreur indique "no such table as 'mangle'", ne vous inquiétez pas, cette table n'est pas nécessaire pour le Masquerading. Si le message d'erreur indique "iptables is incompatible with your kernel", téléchargez une version de noyau supérieure à 2.4 et compilez-le avec le support iptables.

Ensuite si vous avez une adresse IP statique(Par exemple une interface réseau n'utilisant pas le DHCP):

```
$> iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 123.12.23.43
```

ou pour une adresse dynamique (Par exemple un modem rtc - vous devez appelez un numéro tout d'abord):

```
$> iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE
```

Enfin, afin d'indiquer au noyau que vous voulez activer le routage de packets : (A faire après chaque redémarrage de la session - pas trop contraignant)

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

Une fois vérifié que tout fonctionne (voir section Post-install) vous n'allez autoriser l'IP masquerade que pour le réseau interne - vous ne souhaitez pas autoriser des personnes sur Internet à l'utiliser après tout :)

En premier lieu, autorisez toutes les connections existantes, ou les connections en dépendant (par exemple un serveur ftp vous renvoyant une réponse)

```
$> iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Si vous obtenez une erreur, vous n'avez probablement pas activé le marquage d'état sur les paquets dans le noyau - vous devrez le recompiler avec cette option. Nous allons ensuite n'autoriser que les nouvelles connections venant de notre réseau interne (réseau interne ou local). Remplacez ppp0 par eth0, ou par le nom de votre interface réseau *externe* (Le caractère ! signifie "tout sauf")

```
$> iptables -A INPUT -m state --state NEW -i ! ppp0 -j ACCEPT
```

Et bloquez maintenant tout le reste:

```
$> iptables -P INPUT DROP   #seulement si les deux commandes précédentes ont abouties
```

Si l'une des deux premières commandes échoue, cette règle empêchera le masquerading de fonctionner Pour annuler cette règle : "**iptables -P INPUT ACCEPT**".

Instructions post-installation

Cela devrait fonctionner maintenant. N'oubliez pas de :

- Configurer toutes les machines du réseau interne afin d'indiquer comme passerelle l'adresse réseau unique de la machine Linux. (Sous Windows, clic droit sur le voisinage réseau ->propriétés->connexion au réseau local -> propriétés -> Protocol Internet (TCP/IP) -> passerelle, et remplacez-la par l'adresse IP interne de la machine Linux.)
- Configurer tous vos clients afin d'utiliser le serveur proxy http de votre fournisseur d'accès si vos clients en ont un, et utiliser un proxy en mode transparent (ATTENTION - Certains rapports font état de proxy en mode transparent engendrant un ralentissement très important sur les très grands réseaux), ou activez le squid sur votre passerelle Linux (ceci est facultatif mais préférable pour les grands réseaux)
- Spécifier un serveur de DNS sur les machines clientes. Sinon vous obtiendrez un message d'erreur indiquant 'cannot resolve address' etc. Si la résolution d'adresse DNS fonctionnait (adresse URL fonctionnelle) avant d'avoir configuré le MASQUERADING, cela signifie que le serveur DHCP de votre fournisseur d'accès n'arrive plus à vous indiquer quelle est l'adresse DNS.

[Aparté] Je me demande si vous ne pourriez pas simplement envoyer un broadcast DHCP qui sera acheminé vers le serveur dns (et vers le proxy http pendant qu'on y est) sans avoir à configurer un serveur DHCP (ou même si vous le faites). Quelqu'un pourrait-il me renseigner à ce sujet? :)

Merci à Richard Atcheson pour me l'avoir fait remarquer

- A présent, vous devriez commencer à sécuriser un peu tout cela! Premièrement, désactivez le routage : "**iptables -P FORWARD DROP**", puis apprenez à utiliser les règles de filtrage iptables, `/etc/hosts.allow` et `/etc/hosts.deny` afin de sécuriser votre système. ATTENTION - N'essayez pas d'appliquer ces règles iptables avant d'avoir un masquerading opérationnel. Vous devez explicitement autoriser chaque transfert de paquet si vous paramétrez la dernière règle avec l'option DENY. (Annulez avec "**iptables -P FORWARD ACCEPT**")
- Autorisez les accès provenant d'Internet pour chaque service.

  Par exemple, pour autoriser l'accès au serveur web, vous faites:

  ```
  $> iptables -A INPUT --protocol tcp --dport 80 -j ACCEPT
  $> iptables -A INPUT --protocol tcp --dport 443 -j ACCEPT
  ```

  Pour autoriser l'authentification (Se connecter sur les channels IRC etc...), faites

  ```
  $> iptables -A INPUT --protocol tcp --dport 113 -j ACCEPT
  ```

Pour le tester:

- Essayez de vous connecter sur Internet depuis une machine cliente en utilisant une adresse IP. L'adresse IP de Google est 64.233.183.103 (enfin, l'une d'entre elles) et vous devriez obtenir une réponse en retour Par exemple "**ping 64.233.183.103**" "**lynx 64.233.183.103**".
- Essazyez une connexion par nom, par exemple "**ping google.fr**" "**lynx google.fr**" ou depuis Internet Explorer / netscape.

Où eth0 est l'interface réseau externe, et 123.12.23.43 est l'adresse ip de ce client.

FAQ - Foire aux réclama**** Questions

- Comment lister les règles appliquées?

  - Essayez

  ```
  $> iptables -L
  $> iptables -t nat -L
  ```
- Je ne peux résoudre les adresses IP! Je tape 'www.microsoft.com' et cela m'indique qu'il ne le trouve pas!

  - Assurez-vous d'avoir ajouté l'adresse IP du serveur dns sur les machines clientes
- Cela ne fonctionne pas! Il ne supporte pas iptables / NAT / SNAT / MASQ

  - Téléchargez le dernier noyau et compilez-le avec le support iptables et full NAT.
- Cela ne marche pas! Le masquerading ne fonctionne pas du tout! Meurs pourriture!

  - Essayez **echo 1 > /proc/sys/net/ipv4/ip_forward**
- Cela ne fonctionne pas! Je ne peux plus utiliser le réseau et je vous hais!

  - Essayez

  ```
  $> iptables -F
  ```

```
$> iptables -t nat -F
$> iptables -t mangle -F
```

(Toutes les règles sont effacées) puis redémarrez les autres règles iptables.

- Essayez**iptables -P FORWARD ACCEPT**

• Cela ne marche toujours pas!

- Hmm, la commande "**dmesg | tail**" vous renvoie-t'elle des erreurs? ou bien "**cat /var/log/messages | tail**" ? Comme je le crains...

• Cela ne renvoit rien. Et cela ne fonctionne toujours pas!

- Je ne sais pas... mais vous devriez est capable de :

```
      1) pinguer l'extérieur depuis la passerelle
       2) pinguer les machines locales depuis la passerelle
       3) pinguer la passerelle depuis les machines locales
```

Et cela *avant* que vous n'appliquiez le masquerading

• Où dois-placer ces trucs?

- Dans le fichier `/etc/network/interfaces`, ou firewall.rc. Si vous le placez dans le fichier interfaces, mettez le avant l'activation de l'interface réseau externe, et placez "**iptables -t nat -F**" après la désactivation de celle-ci.

• How do I get it to only bring the ppp up on demand?

- Considérant que l'adresse IP de votre passerelle FAI est 23.43.12.43 pour le bien-fondé de l'argument, then rajoutez une ligne comme celle-ci:

:23.43.12.43

à la fin du fichier`/etc/ppp/peers/provider`. (Pour une adresse IP dynamique). Pour une adresse IP statique : **external.ip.number:23.43.12.43**)

A la fin de ce fichier, rajoutez une nouvelle ligne:

demand

Le démon pppd restera en arrière-plan pour relancer la connection si elle est désactivée, jusqu'à ce que vous faites un "**ifdown ppp0**" ou un "**poff**", à moins que vous n'ajoutiez une option "**nopersist**" , dans chaque cas pppd s'arrêtera une fois la connection activée. Vous pouvez également ajouter une ligne "**idle 600**" pour déconnecter après 10 minutes d'inactivité.

• La connection reste inactive!

- Tout d'abord, avez-vous effectué la procédure de connection? Est-ce que cela fonctionne comme cela est supposé? Vérifiez le fichier`/etc/ppp/peers/provider`, et assurez-vous que votre connection marche bien avant d'essayer le masquerading.

- Deuxièmement, si cela ne marche pas (cela m'est arrivé), cela devient peut-être étrange, et vous devrez revenir à un noyau 2.4.3 et voir si cela marche à la place.. je ne sais pas pourquoi.

• Je n'aime pas faire cela moi-même! Je voudrais un script tout fait, une interface graphique.

- Bien sûr: http://shorewall.sourceforge.net/

A déguster sans restrictions!

* Dois-je considérer les modems comme ayant une adresse IP statique ou dynamique?

  - Bonne question.. Vous devriez la placer en dynamique.
* Dois-je considérer les cartes réseaux DHCP comme ayant des adresses IP statiques ou dynamiques?

  - Elles sont dynamiques.
* Comment traiter les services entrants?

  - Essayez de laisser passer ou de rediriger les requêtes en provenance de ces ports IP - encore une fois, assurez-vous de les bloquer si nécessaire.
* Depuis les machines clientes, je peux pinguer l'adresse IP externe de la passerelle Linux, mais je ne peux accéder à internet.

  - Okay, essayez un "**rmmod iptable_filter**" - Plus d'info lorsque je les recevrai.

  - Assurez-vous de ne pas avoir activé le *routage* ou la *passerelle* - pour vérifier l'activation : "**ps aux | grep -e routed -e gated**".

  - Reportez-vous au site http://ipmasq.webhop.net/
* Comment visualiser les connections établies? Avec netstat...

  - Essayez la commande cat /proc/net/ip_conntrack
* Je désire plus d'information sur le filtrage, le routage et autres trucs!

  - Lisez le Guide Pratique du routage avancé http://ftp.traduc.org/doc-vf/HOWTO/telechargement/html-1page/Adv-Routing-HOWTO.html
* Ce guide pratique est une foutaise! Comment puis-je engueler le gars qui l'a écrit?

  - Allez sur le canal #debian sur irc.opensource.net, et dénichez JohnFlux. - Envoyez-moi un email (JohnFlux) à tapselj0@cs.man.ac.uk
* Cet How-To est nul! Comment puis-je obtenir de meilleurs versions?

  - Essayez http://ipmasq.cjb.net

  - Consultez la LDP Masq-HOWTO.
* Sur quoi d'autres travaillez-vous?

  Actuellement j'écris un guide simplifié pour Linux sur des missiles anti-missile. Il n'existe pas de bons guides pour débutants concernant la protection de votre système en cas d'attaque nucléaire Les gens semblent penser que c'est une science armée ou autre..