Linux IP Masquerade mini HOWTO

Ambrose Au, *ambrose@writeme.com*; David Ranch, *dranch@trinnet.net*
Version Française par Mathieu Arnold, *arn_mat@club-internet.fr* v1.50, 7 Février 1999

Ce document décrit la procédure pour mettre en place l'option IP masquerade sur un ordinateur Linux, permettant de connecter sur Internet des ordinateurs n'ayant pas d'adresses IP réservées, à travers votre ordinateur Linux.

Table des matières

1 Introduction

1.1 Introduction

Ce document décrit comment mettre en place l'option IP masquerade sous Linux, afin de permettre à des ordinateurs n'ayant pas d'adresse IP réservée de se connecter à Internet à travers votre ordinateur. Il est possible de connecter votre machine à l'hôte Linux grâce à de l'Ethernet, aussi bien que d'autres types de connexions comme un lien PPP. Ce document va se restreindre à une connexion Ethernet, puisque c'est l'hypothèse la plus probable.

> **Ce document suppose que vous utilisez les noyaux stables 2.2.x ou 2.0.x. Les anciennes versions telles 1.2.x ne sont PAS couvertes par ce document.**

1.2 Mise en garde, Feedback et Crédits

Je trouve que, en tant que débutant, il est très déroutant de mettre en place l'IP masquerade sur un noyau récent, comme sur un de la série des 2.x. Bien qu'il y ait une FAQ et une mailing list, il n'y a pas de documents spécifiques pour cela, et il y a des demandes sur la mailing list pour des documents tels qu'un HOWTO. J'ai donc décidé d'écrire ce document comme un point de départ pour un nouvel utilisateur, et peut-être comme un point de départ pour qu'un utilisateur expérimenté écrive une véritable documentation. Si vous pensez que ce document n'est pas parfait, n'hésitez pas à m'en faire part afin que je puisse l'améliorer.

Ce document est largement inspiré de la FAQ de Ken Eves, ainsi que de nombreux messages très utiles de la mailing list d'IP Masquerading. Je tiens à adresser des remerciements tout particuliers à M. Matthew Driver qui, par ses messages sur la mailing list, m'a donné envie de mettre en place l'IP Masquerading et d'écrire ce document.

N'hésitez pas à nous envoyer tout commentaire à *ambrose@writeme.com* et *dranch@trinnet.net* pour toute erreur ou tout oubli dans ce document. L'avenir de cet HOWTO sera fortement influencé par les réactions que j'aurais de votre part.

Ce HOWTO a été conçu pour être un guide pour que l'IP Masquerading fonctionne chez vous rapidement. Comme je ne suis pas un technicien, il se peut que vous trouviez les informations de ce document moins générales et moins objectives. Les dernières nouvelles et informations pourront être trouvées sur le site web de l'*IP Masquerading Ressource*, dont nous nous occupons. Si vous désirez poser des questions techniques à propos d'IP Masquerade, veuillez

souscrire à la mailing list IP Masquerade au lieu de m'envoyer des mails. J'ai peu de temps pour vous répondre, et les développeurs d'IP_Masq sont plus à même de répondre à vos questions.

La dernière version de ce document peut être obtenue à l'*IP Masquerade Ressource*, qui distribue également des versions HTML et PostScript de ce document :

- *http://ipmasq.cjb.net/*
- *http://ipmasq2.cjb.net/*
- Veuillez consulter la *liste des Sites Mirrors de l'IP Masquerade Ressource* pour contacter un site plus proche de chez vous.

1.3 Copyright & Dénégation

Toutes les informations contenues dans ce document sont l'état de mes connaissances. Cependant, l'IP Masquerading est *expérimental*, et il y a des chances que j'aie fait des erreurs ; c'est à vous de décider si vous voulez suivre les informations contenues dans ce document.

Personne n'est responsable pour un quelconque dommage sur vos ordinateurs ainsi qu'une quelconque autre perte due à l'utilisation des informations contenues dans ce document. C'est à dire :

> **L'AUTEUR ET LES MAINTENEURS NE SONT EN AUCUN CAS RESPONSABLES DES DOMMAGES OCCASIONNES PAR L'USAGE DES INFORMATIONS CONTENUES DANS CE DOCUMENT, QUELS QU'ILS SOIENT.**

2 Connaissances de base

2.1 Qu'est-ce que l'IP Masquerade?

L'IP Masquerade est une fonctionnalité réseau de Linux. Si un hôte Linux est connecté à Internet avec l'option IP Masquerade en place, alors les ordinateurs se connectant à celui-ci (que cela soit sur le réseau local ou par modem) peuvent atteindre Internet aussi, même *s'il n'ont pas d'adresse IP officielle*.

Cela permet à un ensemble de machines d'accéder de manière *invisible* à Internet, caché derrière une passerelle, qui apparaît comme étant le seul système utilisant la connexion Internet. Il devrait être énormément plus difficile de contourner un système basé sur le masquerade, s'il est bien configuré, que de passer outre un bon firewall effectuant du filtrage de paquets (en supposant qu'il n'y a de bogues chez aucun des deux).

2.2 Où cela en est ?

L'IP Masquerade est utilisé depuis quelques années et murit alors que Linux arrive dans les 2.2.x. Les noyaux, depuis la série 1.3.x, supportent en standard cette fonctionnalité. De nombreuses personnes, et même des entreprises l'utilisent, avec des résultats satisfaisants.

L'utilisation d'IP Masquerade pour parcourir le web, ou pour le telnet est tout à fait satisfaisante. FTP, IRC, et l'écoute de Real Audio fonctionnent en utilisant certains modules. D'autres technologies de flux audio par réseau, telles que True Speech et Internet Wave fonctionnent également. Certaines personnes, abonnées à la mailing list ont même essayé des logiciels de vidéo-conférence. `Ping` fonctionne à présent, avec le nouveau patch pour ICMP.

Veuillez consulter la section 4.3 pour une liste complète des logiciels supportés.

L'IP masquerade fonctionne convenablement avec des 'machines clientes' utilisant divers systèmes d'exploitation et différentes plate-formes. On a enregistré des succès pour des systèmes utilisant Unix, Windows 95, Windows NT, Windows pour Workgroups (avec l'extension TCP/IP), OS/2, MacOS avec Mac TCP, Mac Open Transport, DOS avec le package NCSA Telnet, VAX, Alpha sous Linux, et même Amiga avec AmiTCP ou la pile AS225. La liste continue à n'en plus finir, en réalité, si votre systeme d'exploitation parle TCP/IP, cela marcher avec l'IP Masquerade.

2.3 A qui peut être utile IP Masquerade?

- Si vous avez un hôte Linux connecté à Internet, et
- si vous avez un ou plusieurs ordinateurs utilisant TCP/IP, connecté à cet hôte Linux sur un réseau local, et/ou
- si votre hôte Linux a un ou plusieurs modems et joue le rôle de serveur PPP ou SLIP, et que
- ces **AUTRES** machines ne possèdent pas d'adresse IP officielle (ces machines seront désormais référencées sous le nom de **AUTRES**).
- et bien sûr, si vous désirez que ces **AUTRES** machines soient également connectées sur Internet sans débourser un centime de plus :-)

2.4 Qui n'a pas besoin d'IP Masquerade?

- Si votre machine est un hôte isolé, connecté sur Internet, alors c'est inutile de mettre en place l'IP Masquerading, ou
- si vous avez déjà obtenu des adresses officielles pour vos **AUTRES** machines, alors vous n'avez pas besoin d'IP Masquerade pour faire un firewall,
- et bien sûr, si vous n'aimez pas l'idée de connecter toutes les **AUTRES** machines gratuitement, de cette manière.

2.5 Comment fonctionne IP Masquerade?

D'après la FAQ IP Masquerade, de Ken Eves :

```
Voici un schéma du plus simple cas possible~:

   SLIP/PPP         +------------+                       +-------------+
vers le provider    |  Linux     |        SLIP/PPP       | Peu_importe |
  <---------- modem1|            |modem2 ----------- modem |             |
    111.222.333.444 |            |            192.168.1.100 |             |
                    +------------+                       +-------------+

  Dans le schéma ci-dessus, un ordinateur sous Linux, utilisant
  ip_masquerading est connecté à Internet par un lien SLIP ou PPP, utilisant
  modem1. Il possède l'adresse IP (officielle) 111.222.333.444. Il est
  configuré de telle façon que modem2 permet aux appelants de se connecter
  et d'initier une connexion PPP ou SLIP.

  Le second système (qui n'utilise par forcément Linux comme système
  d'exploitation) se connecte par modem sur l'hôte Linux et entame une
  liaison SLIP ou PPP. Il NE possède PAS d'adresse IP officielle donc il
```

```
    utilise 192.168.1.100 (voir ci-dessous).

    Avec l'option ip_masquerade et un routage configuré correctement, la
    machine Peu_importe peut interagir avec Internet comme si elle était
    réellement connectée (à quelques exceptions près).

Pour citer Pauline Middlelink~: N'oublie pas de rappeler que la machine
Peu_importe doit déclarer l'hôte Linux comme passerelle (que cela soit la
route par défaut ou juste un sous réseau importe peu). Si Peu_importe ne peut
pas le faire, l'hôte Linux devra faire du proxy arp pour toutes les adresses
routées, mais la mise en place du proxy arp est hors du domaine de ce
document.

Ce qui suit est l'extrait d'un article de comp.os.linux.networking qui a été
modifié pour utiliser les noms des machines de l'exemple ci-dessus~:
   o J'indique à la machine Peu_importe que le serveur Linux est sa
     passerelle.
   o Quand un paquet en provenance de Peu_importe arrive sur la machine Linux,
     elle va lui assigner un nouveau numéro de port, et indiquer sa propre
     adresse IP dans l'entête du paquet, tout en sauvegardant l'entête
     originale. Elle va alors envoyer le paquet modifié à travers son
     interface SLIP ou PPP, vers Internet.
   o Lorsqu'un paquet en provenance d'Internet arrive sur la machine Linux, si
     le numéro de port est un de ceux assignés à l'étape précédente, elle va
     modifier à nouveau l'entête pour y remettre les numéros de port et
     adresses IP originaux, et alors envoyer le paquet à la machine
     Peu_importe.
   o L'hôte qui a envoyé le paquet ne verra jamais la différence.
```

Un example d'IP Masquerading

Voici ci-dessous le schéma d'un exemple classique :

```
    +----------+
    |          |  Ethernet
    | Ordi A   |::::::
    |          |2   ~:192.168.1.x
    +----------+    ~:
                    ~:   +----------+   lien
    +----------+    ~:  1|  Linux   |   PPP
    |          |    ~::::| masq-gate|:::::::::// Internet
    | Ordi B   |::::::   |          |
    |          |3   ~:   +----------+
    +----------+    ~:
                    ~:
    +----------+    ~:
    |          |    ~:
    | Ordi C   |::::::
    |          |4
    +----------+
```

```
<-Réseau interne->
```

Il y a dans cet exemple 4 ordinateurs qui nous intéressent (il y a sûrement sur la droite quelque chose sur laquelle aboutit notre connexion, et encore plus à droite une autre machine avec laquelle nous échangeons des données). L'ordinateur sous Linux `masq-gate` est la passerelle qui effectue le masquerading pour le réseau interne des ordinateurs `A`, `B`, et `C`, afin de les relier à Internet. Le réseau interne utilise une des adresses assignées des réseaux privés, à savoir dans ce cas le réseau de classe C 192.168.1.0, l'ordinateur Linux ayant l'adresse 192.168.1.1 et les autres ordinateurs ayant d'autres adresses sur ce réseau.

Les trois machines `A`, `B` et `C` (qui peuvent utiliser n'importe quel système d'exploitation, du moment qu'elles utilisent IP - comme par exemple **Windows 95**, **Macintosh MacTCP** ou même un autre Linux) peuvent se connecter à n'importe qu'elle machine sur Internet, mais `masq-gate` convertit toutes leurs connexions de façon à ce qu'elles semblent provenir de `masq-gate`, et s'arrange pour que toutes les données revenant d'Internet retournent au système qui en est à l'origine. Ainsi, les ordinateurs du réseau interne voient une route directe vers Internet et ne sont pas au courant du fait que leurs données ont été "masqueradées".

2.6 Ce qui est requis pour utiliser IP Masquerade sur un Linux 2.2.x

> **** Référez vous à *IP Masquerade Resource* `<http://ipmasq.cjb.net/>` pour les dernieres informations (en anglais). ****

- Les sources du noyau 2.2.x sont disponibles depuis *ftp://ftp.lip6.fr/pub/linux/kernel/sources/v2.2/*
  (La majorité des distributions de linux récentes telle la RedHat 5.2 - livrée avec un noyau 2.0.36 - ont le un noyau modulaire avec toutes les options nécessaires a l'IP Masquerading compilées. Dans ce genre de cas, il n'y a pas besoin de recompiler le noyau. Si vous mettez a jour votre noyau, alors vous devriez savoir ce dont vous avez besoin, nous y reviendrons un peu plus loin).
- Modules chargeables dynamiquement, de préférence avec un 2.1.121 ou plus récent.
- Ainsi qu'un réseau TCP/IP en bon état de marche
  tout ceci est décrit dans *Linux NET-3 HOWTO* `<http://www.freenix.org/unix/linux/HOWTO/NET-3-HOWTO.html>` et dans le *Guide de l'administrateur réseau* `<ftp://ftp.ibp.fr/pub/linux/french/books/nag.french.eoit-1.0.tar.gz>`
  Allez aussi faire un tour chez *Trinity OS Doc* `<http://www.ecst.csuchico.edu/~dranch/LINUX/TrinityOS.wri>`, une documentation tres simple sur Linux et le reseau.
- Connectivity to Internet for your Linux host
  Décrit dans *Linux ISP Hookup HOWTO* `<http://www.freenix.org/unix/linux/HOWTO/ISP-Hookup-HOWTO.html>`, *Linux PPP HOWTO* `<http://www.freenix.org/unix/linux/HOWTO/PPP-HOWTO.html>`, *Linux DHCP mini-HOWTO* `<http://www.freenix.org/unix/linux/HOWTO/mini/DHCP.html>` et *Linux Cable Modem mini-HOWTO* `<http://www.freenix.org/unix/linux/HOWTO/mini/Cable-Modem.html>`
- IP Chains 1.3.8 ou plus récent, disponible sur *http://www.rustcorp.com/linux/ipchains/*
  Plus d'informations sur les différentes versions, visitez *Linux IP Firewalling Chains page* `<http://www.rustcorp.com/linux/ipchains/>`
- Pour d'autres options, référez vous à *Linux IP Masquerade Resource* `<http://ipmasq.cjb.net/>`

2.7 Ce qui est requis pour utiliser IP Masquerade sur un Linux 2.0.x

> **** Veuillez s'il vous plaît consulter l'*IP Masquerade Resource* pour les dernières informations.****

- Les sources d'un noyau de la série 2.x, disponibles sur *ftp://ftp.ibp.fr/pub/linux/kernel/sources/v2.0/*
  (La majorité des distributions de linux récentes telle la RedHat 5.2 ont le un noyau modulaire avec

toutes les options nécessaires a l'IP Masquerading compilées. Dans ce genre de cas, il n'y a pas besoin de recompiler le noyau. Si vous mettez à jour votre noyau, alors, vous devriez savoir ce dont vous avez besoin, nous y reviendrons un peu plus loin).

- Les modules chargeables à la demande, de préférence la version 2.0.0 (ou ultérieure), disponible sur *ftp://ftp.ibp.fr/pub/linux/kernel/sources/v2.0/modules-2.0.0.tar.gz* (modules-1.3.57 étant le minimum)
- Un réseau TCP/IP fonctionnant convenablement
  (se référer à *Linux NET-3 HOWTO* `<http://www.freenix.org/unix/linux/HOWTO/NET-3-HOWTO.html>` (**en français**) et au *Network Administrator's Guide* `<ftp://ftp.ibp.fr/pub/linux/french/books/nag.french.eoit-1.0.tar.gz>`)
  Allez aussi faire un tour chez *Trinity OS Doc* `<http://www.ecst.csuchico.edu/~dranch/LINUX/TrinityOS.wri>`, une documentation très simple sur Linux et le réseau.
- Un accès Internet pour votre hôte Linux
  Se référer à *Linux ISP Hookup HOWTO* `<http://www.freenix.org/unix/linux/HOWTO/ISP-Hookup-HOWTO.html>` *Linux PPP HOWTO* `<http://www.freenix.org/unix/linux/HOWTO/PPP-HOWTO.html>`, *Linux DHCP mini-HOWTO* `<http://www.freenix.org/unix/linux/HOWTO/mini/DHCP.html>` et à *Linux Cable Modem mini-HOWTO* `<http://www.freenix.org/unix/linux/HOWTO/mini/Cable-Modem.html>`
- Ipfwadm 2.3, téléchargeable sur *ftp://ftp.xos.nl/pub/linux/ipfwadm/ipfwadm-2.3.tar.gz*
  Plus d'informations sur *Linux IPFWADM page* `<http://www.xos.nl/linux/ipfwadm/>`
- Vous pouvez, si vous le souhaitez, appliquer certains patches pour mettre en place certaines fonctionnalités. Vous trouverez plus d'informations sur la page des *IP Masquerade Resources* (ces patches s'appliquent à tout noyau de la série 2.0.x).

3 Mise en place d'IP Masquerade

Si votre réseau privé contient des informations vitales, repensez y à deux fois avant d'utiliser IP Masquerade. Cela constitue une passerelle pour vous, pour atteindre Internet, mais la réciproque est vraie et quelqu'un sur Internet pourrait pénétrer sur votre réseau privé.

3.1 Compiler le noyau pour le support d'IP Masquerade

Si votre distribution de Linux a déjà les fonctionnalités necessaires et les modules de compilés (la majorité des noyaux modulaires auront ce dont vous avez besoin) mentionnés ci-dessous, alors vous n'avez pas à recompiler le noyau. La lecture de cette section est quand meme largement recommandée car elle contient aussi d'autres informations très utiles.

3.1.1 Noyaus Linux 2.2.x

- Tout d'abord, Vous avez besoin des sources du noyau 2.2.x
- Si c'est la premiere fois que vous compilez un noyau, ne vous inquietez pas, en fait, c'est assez facile et tout est expliqué dans *Linux Kernel HOWTO* `<http://www.freenix.org/unix/linux/HOWTO/Kernel-HOWTO.html>`.
- Décompressez les sources du noyau dans `/usr/src/` avec la commande : `tar xvzf linux-2.2.x.tar.gz -C /usr/src`, ou x est la version du noyau.
  (Assurez vous qu'il existe un repertoire ou un lien symbolique appelé `linux`)

– Appliquez les patchs appropriés. Comme de nouveaux patch sortent régulierement, les détails ne sont pas décrits ici. Référez vous à *IP Masquerade Resources* `<http://ipmasq.cjb.net/>` pour des informations au jour le jour.
– Référez vous au Kernel HOWTO et au fichier README des sources du noyau pour plus d'informations sur la compilation d'un noyau.
– Voici les options que vous devez compiler :
  Dites *YES* aux options suivantes :

```
* Prompt for development and/or incomplete code/drivers
  CONFIG_EXPERIMENTAL
  - Ceci vous permettra de selectionner le code experimental IP Masquerade.

* Enable loadable module support
  CONFIG_MODULES
  - Vous permet de charger les modules ipmasq tel ip_masq_ftp.o

* Networking support
  CONFIG_NET

* Network firewalls
  CONFIG_FIREWALL

* TCP/IP networking
  CONFIG_INET

* IP: forwarding/gatewaying
  CONFIG_IP_FORWARD

* IP: firewalling
  CONFIG_IP_FIREWALL

* IP: masquerading
  CONFIG_IP_MASQUERADE

* IP: ipportfw masq support
  CONFIG_IP_MASQUERADE_IPPORTFW
  - Recommandé

* IP: ipautofw masquerade support
  CONFIG_IP_MASQUERADE_IPAUTOFW
  - Optionnel

* IP: ICMP masquerading
  CONFIG_IP_MASQUERADE_ICMP
  - Support pour masquerader les paquets ICMP, recommandé

* IP: always defragment
  CONFIG_IP_ALWAYS_DEFRAG
  - Chaudement recommandé

* Dummy net driver support
  CONFIG_DUMMY
  - Recommandé

* IP: ip fwmark masq-forwarding support
```

```
        CONFIG_IP_MASQUERADE_MFW
        - Optionnel
```

NOTE : Voici juste les composants qu'il faut pour que l'IP Masquerade marche, selectionnez les options spécifiques dont vous avez besoin pour votre systeme.

– Après avoir compilé le noyau, vous devriez compiler et installer les modules :

```
make modules; make modules_install
```

– Enfin, vous devriez ajouter quelques lignes dans votre `/etc/rc.d/rc.local` (ou le fichier que vous trouvez plus approprié) pour charger les modules résidants dans `/lib/modules/2.2.x/ipv4/` automatiquement à chaque redémarrage.

```
        .
        .
        .
/sbin/depmod -a
/sbin/modprobe ip_masq_ftp
/sbin/modprobe ip_masq_raudio
/sbin/modprobe ip_masq_irc
(Et d'autres modules tels ip_masq_cuseeme, ip_masq_vdolive
 Si vous avez appliqués les patchs)
        .
        .
        .
```

IMPORTANT: IP forwarding est désactivé par défaut pour les noyaux 2.2.x, alors, assurez vous de bien l'avoir activé en faisant :
`echo "1" > /proc/sys/net/ipv4/ip_forwarding`
Pour les utilisateurs de RedHat, vous pouvez essayer de changer `FORWARD_IPV4=false` en `FORWARD_IPV4=true` dans `/etc/sysconfig/network`

– Finalement, redémarrez votre machine.

3.1.2 Noyaux Linux 2.0.x

– Vous devez tout d'abord disposer des sources du noyau (de préférence la derniere version 2.0.36 ou plus récente).
– Si c'est la première fois que vous compilez votre noyau, ne soyez pas effrayé. En fait, c'est plûtot simple, et tout est expliqué dans le *Kernel HOWTO* `<http://www.freenix.org/unix/linux/HOWTO/Kernel-HOWTO.html>`
– Décompressez les sources du noyau dans `/usr/src/` avec la commande `tar xvzf linux-2.0.x.tar.gz -C /usr/src`, où x est le numéro de révision du noyau.
(vérifiez qu'il y a un répertoire ou un lien symbolique nommé `linux`)
– Appliquez les patches appropriés. Comme de nouveaux patches sortent souvent, aucun détail ne sera inclus ici. Référez vous à l'*IP Masquerade Resources* pour une information récente.
– Veuillez consulter le Kernel HOWTO et le fichier README dans le répertoire des sources du noyau pour plus d'informations sur la compilation d'un noyau.
– Voici les options que vous devrez utiliser :
Répondre *YES* à :

```
      * Prompt for development and/or incomplete code/drivers
        CONFIG_EXPERIMENTAL
        - Cela vous permettra de pouvoir sélectionner IP Masquerade,
```

```
    qui est expérimental.

  * Enable loadable module support
    CONFIG_MODULES
    - Permet le chargement des modules.

  * Networking support
    CONFIG_NET

  * Network firewalls
    CONFIG_FIREWALL

  * TCP/IP networking
    CONFIG_INET

  * IP: forwarding/gatewaying
    CONFIG_IP_FORWARD

  * IP: firewalling
    CONFIG_IP_FIREWALL

  * IP: masquerading (EXPERIMENTAL)
    CONFIG_IP_MASQUERADE
    - bien que cela soit expérimental, il *FAUT* l'intégrer

  * IP: ipautofw masquerade support (EXPERIMENTAL)
    CONFIG_IP_MASQUERADE_IPAUTOFW
    -recommended

  * IP: ICMP masquerading
    CONFIG_IP_MASQUERADE_ICMP
    - support for masquerading ICMP packets, optionnel.

  * IP: always defragment
    CONFIG_IP_ALWAYS_DEFRAG
    - très recommendé

  * Dummy net driver support
    CONFIG_DUMMY
    - recommendé
```

NB : Ce sont juste les composants dont vous avez besoin pour l'IP Masquerade. Ajoutez toute autre option nécessaire pour votre configuration personnelle.

- Une fois le noyau compilé, compilez et installez les modules :

```
make modules; make modules_install
```

- Ajoutez alors quelques lignes dans votre fichier `/etc/rc.d/rc.local` (ou dans le fichier approprié), pour charger automatiquement les modules nécessaires dans `/lib/modules/2.0.x/ipv4/`, après chaque reboot :

```
        .
        .
        .
/sbin/depmod -a
/sbin/modprobe ip_masq_ftp.o
```

```
/sbin/modprobe ip_masq_raudio.o
/sbin/modprobe ip_masq_irc.o
(et tout autre module, comme ip_masq_cuseeme, ip_masq_vdolive si vous avez appliqué les patches)
        .
        .
        .
```

IMPORTANT: IP forwarding est désactivé par défaut depuis le noyau 2.0.34 alors, assurez vous de bien l'avoir activé en faisant :

`echo "1" > /proc/sys/net/ipv4/ip_forwarding`

Pour les utilisateurs de RedHat, vous pouvez essayer de changer `FORWARD_IPV4=false` en `FORWARD_IPV4=true` dans `/etc/sysconfig/network`

- Finalement, redémarrez votre machine.

3.2 Assignation d'adresse IP pour le réseau local

Puisque toutes les **AUTRES** machines n'ont pas d'adresse IP officielle, il faut leur en allouer de manière intelligente.

Selon la FAQ d'IP Masquerade :

Il existe un RFC (#1597, qui doit etre obsolete maintenant) qui indique quelles adresses IP assigner à un réseau non connecté. Il existe 3 plages réservées spécialement à cet effet. Une de celles que j'utilise est un sous réseau de classe C, faisant partie de la plage allant de 192.168.1.n à 192.168.255.n.

```
Selon le RFC 1597~:

Section 3~: Adressage de réseaux privés

L' "Internet Assigned Numbers Authority" (IANA) a réservé les 3 plages
suivantes pour leur utilisation par des réseaux privés~:

              10.0.0.0        -   10.255.255.255
              172.16.0.0      -   172.31.255.255
              192.168.0.0     -   192.168.255.255

Nous ferons référence à la première en tant que la "plage de 24 bits", la
deuxième comme "plage de 20 bits" et la troisième comme "plage de 16 bits".
Notez que la première plage n'est rien d'autre qu'un réseau de classe A, la
deuxième un ensemble de 16 réseaux de classe B contigus, et la troisième un
ensemble de 255 réseaux de classe C contigus.
```

Ainsi, si vous utilisez un réseau de classe C, vous devrez utiliser les adresses IP 192.168.1.1, 1.92.168.1.2, 1.92.168.1.3, ..., 192.168.1.x

192.168.1.1 est habituellement la machine passerelle, qui est ici votre machine Linux se connectant à Internet. Remarquez que 192.168.1.0 et 192.168.1.255 sont respectivement les adresses de réseau et de broadcast, qui sont réservées. Evitez d'utiliser ces adresses sur vos machines.

3.3 Configurer les AUTRES machines

En plus d'affecter les adresses IP pour chaque machine, vous devrez indiquer la bonne passerelle. En général, c'est plutôt simple. Vous entrez juste l'adresse de votre machine Linux (généralement 192.168.1.1) en tant qu'adresse de passerelle.

Pour le DNS, vous pouvez utiliser n'importe quel DNS utilisable. Le plus simple est d'utiliser celui qu'utilise votre machine Linux. Vous pouvez aussi, si vous le désirez, ajouter des suffixes d'ordre de recherche DNS.

Une fois configurées ces adresses IP, n'oubliez pas de relancer les programmes concernés, ou de rebooter vos machines.

Les instructions de configuration qui suivent supposent que vous utilisez un réseau de classe C, et que votre machine Linux a pour adresse 192.168.1.1. Notez que 192.168.1.0 et 192.168.1.255 sont réservées.

3.3.1 Configurer Windows 95

1. Si vous n'avez pas installé votre carte réseau et son driver, faites le maintenant.
2. Allez dans *Panneau de configuration / Réseau* .
3. Ajoutez le *protocole TCP/TP* si ce n'est pas déjà fait.
4. Dans les *propriétés de TCP/IP*, allez dans *Adresse IP* et entrez votre adresse IP, 192.168.1.x (1 < x < 255). Fixez le *Masque de sous réseau* à 255.255.255.0
5. Ajoutez 192.168.1.1 dans *Passerelle*.
6. Dans *Configuration / Ordre de recherche DNS*, ajoutez le DNS qu'utilise votre machine Linux (que l'on peut trouver dans `/etc/resolv.conf`). Vous pouvez éventuellement ajouter les suffixes de domaine adéquats.
7. Laissez les autres paramètres tels quels, à moins que vous sachiez ce que vous faites.
8. Cliquez sur *OK* dans toutes les boîtes de dialogue et relancez le système.
9. `Ping`uez la machine Linux pour tester la connexion réseau : *Démarrer / Executer*, tapez: `ping 192.168.1.1` (C'est seulement un test de connexion locale, vous ne pouvez pas encore `ping`uer l'extérieur).
10. Vous pouvez éventuellement créér un fichier `HOSTS` dans le répertoire de Windows, pour que vous puissiez utiliser les noms d'hôtes des autres machines de votre réseau local. Il y a un exemple nommé `HOSTS.SAM` dans le répertoire Windows.

3.3.2 Configurer Windows pour Workgroup 3.11

1. Si vous n'avez pas encore installé votre carte réseau et son driver, faites le maintenant.
2. Installez le package TCP/IP 32b si ce n'est pas déjà fait.
3. Dans *Groupe Principal / Installation / Configuration réseau*, cliquez sur *Drivers*.
4. Séléctionnez *Microsoft TCP/IP-32 3.11b* dans la section *Drivers Réseaux*. Choisissez *Configuration*.
5. Saisissez l'adresse IP 192.168.1.x (1 < x < 255), et positionnez le masque de sous réseau à 255.255.255.0 et la passerelle par défaut à 192.168.1.1.
6. Ne sélectionnez pas *Configuration automatique DHCP* et mettez n'importe quoi dans la case *Server WINS*, à moins que vous ne fassiez partie d'un domaine Windows NT et que vous sachiez ce que vous faites.
7. Cliquez sur *DNS*, et remplissez les informations appropriés, mentionnées à l'étape 6 de la section 3.3.1. Cliquez sur *OK* une fois que c'est fini.
8. Cliquez sur *Configuration avancée*, cochez *Utiliser le DNS pour la résolution de noms*, et *Utiliser LMHOSTS* si vous utilisez un fichier de résolution, comme celui mentionné à l'étape 10 de la section 3.3.1.
9. Cliquez alors sur *OK* sur toutes les boites de dialogue, et redémarrez le système.
10. `Ping`ez la machine Linux pour tester la connexion réseau : *Fichier / Exécuter*, taper : `ping 192.168.1.1` (C'est juste un test de connexion locale, vous ne pouvez pas encore `ping`er le monde extérieur.

3.3.3 Configurer Windows NT

1. Si vous n'avez pas encore installé votre carte réseau et son driver, faites le maintenant.
2. Allez dans *Groupe Principal / Panneau de configuration / Réseau*.
3. Ajoutez le protocole TCP/IP et les composants qui s'y rattachent depuis le menu *Ajout de logiciels* si vous n'avez pas encore installé le service TCP/IP.
4. Dans la section *Logiciel et carte réseau*, sélectionnez *Protocole TCP/IP* dans la boite de choix *Logiciels réseaux installés*.
5. Dans *Configuration TCP/IP*, sélectionnez l'adaptateur réseau appropriées, par exemple `[1]Novell NE2000 Adapter`. Entrez l'adresse IP 192.168.1.x ($1 < x < 255$), positionnez le masque de sous réseau sur 255.255.255.0 et la passerelle par défaut à 192.168.1.1.
6. Ne sélectionnez pas *Configuration automatique DHCP* et mettez n'importe quoi dans la case *Server WINS*, à moins que vous ne fassiez partie d'un domaine Windows NT et que vous sachiez ce que vous faites.
7. Cliquez sur *DNS*, et remplissez les informations appropriés, mentionnées à l'étape 6 de la section 3.3.1. Cliquez sur *OK* une fois que c'est fini.
8. Cliquez sur *Configuration avancée*, cochez *Utiliser le DNS pour la résolution de noms*, et *Utiliser LMHOSTS* si vous utilisez un fichier de résolution, comme celui mentionné à l'étape 10 de la section 3.3.1.
9. Cliquez alors sur *OK* sur toutes les boites de dialogue, et redémarrez le système.
10. `Ping`ez la machine Linux pour tester la connexion réseau : *Fichier / Exécuter*, taper : `ping 192.168.1.1` (C'est juste un test de connexion locale, vous ne pouvez pas encore `ping`er le monde extérieur).

3.3.4 Configurer les systèmes UNIX

1. Si vous n'avez pas encore installé votre carte réseau et recompilé votre noyau avec le driver adéquat, faites le maintenant.
2. Installez des outils TCP/IP, comme par exemple le package nettools, si ce n'est déjà fait.
3. Affectez *IPADDR* à 192.168.1.x ($1 < x < 255$), puis *NETMASK* à 255.255.255.0, *GATEWAY* à 192.168.1.1 et *BROADCAST* à 192.168.1.255.
   Par exemple, sur les systèmes Red Hat Linux, vous pouvez éditer le fichier `/etc/sysconfig/network-scripts/ifcfg-eth0`, ou simplement le faire par l'intermédiaire du *Control Panel*.
   (c'est différent sur SunOS, BSDi, Slackware Linux, etc...)
4. Ajoutez l'adresse IP de votre DNS et votre ordre de recherche DNS dans `/etc/resolv.conf`.
5. Il sera éventuellement nécessaire de mettre à jout le fichier `/etc/networks`, selon votre configuration.
6. Redémarrez les services adéquats, ou, plus simplement, redémarrez votre système.
7. Testez votre connexion avec la passerelle en utilisant la commande `ping` : `ping 192.168.1.1`.
   (ceci est juste un test sur votre réseau local, vous ne pouvez pas encore `ping`er l'extérieur.

3.3.5 Configuration sous DOS avec le package NCSA

1. Si vous n'avez pas encore installé votre carte réseau, faites le maintenant.
2. Chargez le driver adéquat. Pour une carte NE2000, tapez `nwpd 0x60 10 0x300`, si votre carte utilise l'IRQ 10 et l'adresse d'entrée/sortie 0x300.
3. Créez un nouveau répertoire, et décompressez-y l'archive NCSA Telnet : `pkunzip tel2308b.zip`
4. Utilisez un éditeur de texte pour ouvrir le fichier `config.tel`.
5. Affectez `myip=192.168.1.x` ($1 < x < 255$), et `netmask=255.255.255.0`.
6. Dans cet exemple, vous auriez à régler `hardware=packet, interrupt=10, ioaddr=60`.

7. Vous devriez avoir au moins une seule machine déclarée comme passerelle, à savoir la machine sous Linux :

   ```
   name=default
   host=le_nom_de_votre_hote_linux hostip=192.168.1.1 gateway=1
   ```

8. Pour mettre en place le DNS :

   ```
   name=dns.domain.com~; hostip=123.123.123.123; nameserver=1
   ```

   NB: remplacez les champs par les informations qu'utilise votre machine Linux.

9. Sauvegardez votre nouveau fichier `config.tel`.
10. Lancez un telnet vers la machine Linux pour tester la connexion réseau : `telnet 192.168.1.1`.

3.3.6 Configuration des systèmes MacOS utilisant MacTCP

1. Si vous n'avez pas encore installé le driver pour votre carte Ethernet, ça serait une excellente idée de le faire maintenant.
2. Ouvrez le *Tableau de bord MacTCP*. Selectionnez le driver réseau adapté (Ethernet, PAS EtherTalk) et cliquez sur le bouton.
3. Dans la section *Obtenir l'adresse*, sélectionnez *Manuellement*.
4. Dans *Adresse IP*, choisissez *class C* dans le menu déroulant. Vous pouvez ignorer le reste de cette boite de dialogue.
5. Remplissez la section *Information DNS* avec les informations qui conviennent.
6. Dans *Adresse de la passerelle*, entrez 192.168.1.1.
7. Cliquez sur *OK* pour sauvegarder les changements. Dans la fenêtre principale du *Tableau de bord MacTCP*, entrez l'adresse IP de votre Mac (192.168.1.x, $1 < x < 255$) dans la zone *Adresse IP*.
8. Refermez le *Tableau de bord MacTCP*. Si une boite de dialogue vous demande de redémarrer le système, faites le.
9. Vous pouvez si vous le désirez `ping`er l'hôte Linux pour tester la connexion réseau. Si vous avez le programme freeware *MacTCP Watcher*, cliquez sur le bouton *Ping* et entrez l'adresse de votre hôte Linux (192.168.1.1) dans la boîte de dialogue qui apparait. (C'est uniquement une connexion locale, vous ne pouvez pas encore `ping`er l'extérieur).
10. Vous pouvez, si vous le désirez, créer un fichier `Hosts` dans votre dossier système, pour pouvoir utiliser les noms d'hôte des machines de votre réseau local. Le fichier devrait déjà exister dans votre dossier système, et contenir quelques exemples commentés, que vous n'avez qu'à modifier pour correspondre à vos besoins.

3.3.7 Configuration des systèmes MacOS utilisant Open Transport

1. Si vous n'avez pas encore installé le driver pour votre carte Ethernet, ça serait une excellente idée de le faire maintenant.
2. Ouvrez le *Tableau de bord TCP/IP* et choisissez *Mode utilisateur...* dans le menu *Edition*. Assurez nous que le mode utilisateur est mis au niveau *Avancé* et cliquez sur le bouton *OK*.
3. Choisissez *Configurations...* depuis le menu *Fichier*. Sélectionnez la configuration *Par défaut* et cliquez sur le bouton *Recopier*. Entrez 'IP Masq' (ou quelque chose d'autre du moment que vous puissiez etre sur qu'il s'agit d'une configuration spéciale) dans la boite de dialogue *Configuration de copie*. Cliquez sur le bouton *OK* puis sur *Rendre active*.
4. Sélectionnez *Ethernet* depuis le menu *Se connecter via...*.
5. Sélectionnez l'option qui convient dans le menu *Configuration*. Si vous ne savez pas quelle option choisir, vous devriez sans doute resélectionner la configuration par défaut et quitter. Je choisis *Manuellement*.
6. Saisissez l'adresse IP de votre Mac (192.168.1.x, $1 < x < 255$) dans la zone *Adresse IP*.

7. Mettez le *Masque de sous réseau* à 255.255.255.0.
8. L'*Adresse de routeur* est 192.168.1.1.
9. Remplissez la case *Adresse du DNS* en y mettant votre adresse IP.
10. Entrez le nom de votre domaine Internet (par exemple 'microsoft.com') dans la boite de dialogue *Ordre de recherche DNS*.
11. La procédure suivante est optionnelle. L'utilisation de valeurs incorrectes peut entrainer des comportements inattendus. Si vous ne savez pas ce que vous faites, il vaut mieux ne pas y toucher, et si nécessaire vider les cases et zones de sélection. Pour ce que j'en sais, il n'est pas possible, par l'intermédiaire des boites de dialogue, de demander au système de ne pas utiliser un fichier "Hosts" sélectionné précédemment. Si vous saviez comment faire, je serais très intéressé.
    Sélectionnez l'option *802.3* si votre réseau nécessite des paquets de type 802.3.
12. Cliquez sur le bouton *Options...* pour vous assurer que le TCP/IP est activé. J'utilise l'option *Charger uniquement si besoin*. Si vous lancez et quittez des applications utilisant TCP/IP assez souvent, sans relancer votre machine, vous pourrez sans doute désélectionner *Charger uniquement si besoin* pour diminuer les effets sur le gestionnaire mémoire de votre machine. Lorsque l'option est désélectionnée, les piles du protocole TCP/IP sont toujours en mémoire et prêtes à l'emploi. Si l'option est cochée, la pile TCP/IP est automatiquement chargée lorsqu'elle est nécessaire, et déchargée sinon. Le processus de la charger et la décharger en mémoire peut fragmenter la mémoire de votre ordinateur.
13. `Ping`ez la machine Linux pour tester la connexion réseau. Si vous avez le programme freeware *MacTCP Watcher*, cliquez sur le bouton *Ping*, et entrez l'adresse de votre machine Linux (192.168.1.1) dnas la boite de dialogue qui apparait. (C'est une connexion locale, vous ne pouvez pas encore `ping`er l'extérieur).
14. Vous pouvez créer un fichier `Hosts` dans votre dossier Système, pour pouvoir utiliser les noms d'hotes de votre réseau local. Le fichier peut exister ou non dans votre dossier Système. Si c'est le cas, il devrait contenir des exemples (en commentaires) que vous pouvez modifier selon vos souhaits. Sinon, vous pouvez obtenir une copie d'un système utilisant MacTCP, ou juste créer le votre (cela ressemble fortement au fichier `/etc/hosts` sur un système Unix, qui est décrit dans la RFC 952). Une fois le fichier créé, ouvrez le *Tableau de bord TCP/IP*, cliquez sur le bouton *Sélectionner le fichier Hosts...*, et ouvrez le fichier `Hosts`.
15. Cliquez sur *Fermer* ou choisissez *Fermer* ou *Quitter* depuis le menu *Fichier*, et cliquez alors sur le bouton *Enregistrer* pour enregistrer vos changements.
16. Les changements prennent effet immédiatement, mais cela ne fera pas de mal de rebouter le système.

3.3.8 Configurer un réseau Novell utilisant le DNS

1. Si vous n'avez pas encore installé le gestionnaire de périphérique de votre adaptateur Ethernet, faites le dès maintenant.
2. Téléchargez tcpip16.exe depuis (NdT ???)
3. Editez `c:\nwclient\startnet.bat` (voici une copie du mien) :

```
SET NWLANGUAGE=ENGLISH
LH LSL.COM
LH KTC2000.COM
LH IPXODI.COM
LH tcpip
LH VLM.EXE
F:
```

4. Editez `c:\nwclient\net.cfg` (changez le `Link drivers`, NE2000 dans mon cas) :

```
Link Driver KTC2000
```

```
        Protocol IPX 0 ETHERNET_802.3
        Frame ETHERNET_802.3
        Frame Ethernet_II
        FRAME Ethernet_802.2

NetWare DOS Requester
           FIRST NETWORK DRIVE = F
           USE DEFAULTS = OFF
           VLM = CONN.VLM
           VLM = IPXNCP.VLM
           VLM = TRAN.VLM
           VLM = SECURITY.VLM
           VLM = NDS.VLM
           VLM = BIND.VLM
           VLM = NWP.VLM
           VLM = FIO.VLM
           VLM = GENERAL.VLM
           VLM = REDIR.VLM
           VLM = PRINT.VLM
           VLM = NETX.VLM

Link Support
        Buffers 8 1500
        MemPool 4096

Protocol TCPIP
        PATH SCRIPT     C:\NET\SCRIPT
        PATH PROFILE    C:\NET\PROFILE
        PATH LWP_CFG    C:\NET\HSTACC
        PATH TCP_CFG    C:\NET\TCP
        ip_address      xxx.xxx.xxx.xxx
        ip_router       xxx.xxx.xxx.xxx
```

5. et finalement, créez `c:\bin\resolv.cfg` :

```
SEARCH DNS HOSTS SEQUENTIAL
NAMESERVER 207.103.0.2
NAMESERVER 207.103.11.9
```

6. J'espère que cela vous aura aidé à configurer vos réseaux Novell, mais cela ne fonctionne que pour Netware 3.1x ou 4.x.

3.3.9 Configurer OS/2 Warp

1. Si vous n'avez toujours pas configuré votre adaptateur réseau Ethernet, c'est le moment de le faire.
2. Installez le protocole TCP/IP s'il n'est pas déjà présent.
3. Allez dans les paramètres *Programs/TCP/IP(LAN)/TCP/IP*
4. Dans *'Network'*, ajoutez votre adresse TCP/IP et configurez votre masque de sous réseau (255.255.255.0)
5. Dans *"Routing"* cliquez sur *"Ajouter"*. Sélectionnez *"default"* pour le *Type* and entrez l'adresse de votre machine Linux dans le champs *"Router Address"* (192.168.1.1).
6. Utilisez la même adresse DNS (Serveur de noms) que celle de votre machine Linux.

7. Fermez le panneau de contrôle de TCP/IP. Répondez oui au (à la) question(s) suivante(s).
8. Rebootez votre système.
9. Vous devriez être en mesure de `ping`er votre hôte Linux pour tester la configuration réseau. Taper `'ping 192.168.1.1"` dans une boîte de commande OS/2. Si vous recevez les paquets IP, tout fonctionne correctement.

3.3.10 Configurer les autres systèmes

Ces systèmes devraient suivre la meme logique d'installation. Lisez les sections précédentes. Si vous êtes intéressés par l'écriture de la documentation sur n'importe quel système, comme OS/2, ou une variété quelconque de système Unix, envoyez s'il vous plait des instructions détaillées à *ambrose@writeme.com* (Note du traducteur : en anglais bien sûr).

3.4 Configurer les règles d'IP Forwarding

A ce point du document, vous devriez avoir votre noyau et les autres packages installés, ainsi que les modules nécessaires chargés. De plus, les adresses IP, la passerelle, et le DNS devraient être installés sur les **AUTRES** ordinateurs.

Maintenant, la seule chose à faire est d'utiliser l'outil de firewalling IP (ipfwadm) pour faire suivre les paquets appropriés à la machine qui convient :

> ** Ceci peut être fait de diverses façons. Les suggestions et exemples suivants fonctionnent pour moi, mais il se peut que vous ayez d'autres idées. Je vous renvoie à la section 4.4 et aux pages de manuel de ipchains(2.2.x) / ipfwadm(2.0.x) pour plus de détails. **
>
> **** Cette section fournis UNIQUEMENT le minimum de règles pour avoir un l'IP Masquerade opérationnel, les problemes de sécurités ne sont pas considérés. Il est fortement recommandé que vous passiez quelque temps pour appliquer quelques règles de firewalling appropriées pour augmenter la sécurité. ****

3.4.1 Noyaux Linux 2.2.x

ipfwadm n'est plus l'outil à utiliser pour manipuler les règles ipmasq pour les noyaux 2.2.x, utilisez ipchains.

```
ipchains -P forward DENY
ipchains -A forward -s yyy.yyy.yyy.yyy/x -j MASQ
```

Où x est le nombre correspondant a la classe de votre sous réseau, et yyy.yyy.yyy.yyy est l'adresse de votre réseau.

```
netmask         | x  | Subnet
~~~~~~~~~~~~~~~~|~~~~|~~~~~~~~~~~~~~~
255.0.0.0       | 8  | Class A
255.255.0.0     | 16 | Class B
255.255.255.0   | 24 | Class C
255.255.255.255 | 32 | Point-to-point
```

Vous pouvez aussi utiliser le format yyy.yyy.yyy.yyy/xxx.xxx.xxx.xxx, où xxx.xxx.xxx.xxx spécifie votre masque de sous réseau tel 255.255.255.0

Par exemple dans mon réseau de classe C, j'entrais ;

```
ipchains -P forward DENY
ipchains -A forward -s 192.168.1.0/24 -j MASQ
```

ou

```
ipchains -P forward DENY
ipchains -A forward -s 192.168.1.0/255.255.255.0 -j MASQ
```

Vous pouvez aussi le faire machine par machine. Par exemple, si je veux que 192.168.1.2 et 192.168.1.8 aient accès à Internet, mais pas les autres machines, j'aurais mis :

```
ipchains -P forward DENY
ipchains -A forward -s 192.168.1.2/32 -j MASQ
ipchains -A forward -s 192.168.1.8/32 -j MASQ
```

Il ne faut **jamais** que votre règle par défaut soit le masquerading, sinon n'importe qui pouvant manipuler ses tables de routage pourra utiliser votre machine Linux pour masquer son identité !

De même, vous pouvez ajouter ces lignes a votre `/etc/rc.local`, ou au fichier rc que vous préférez, ou le faire manuellement à chaque fois que vous en avez besoin.

Pour plus de détails sur ipchain, référez vous au *Linux IPCHAINS HOWTO* `<http://www.freenix.org/unix/linux/HOWTO-vo/IPCHAINS-HOWTO.html>`

3.4.2 Noyaux Linux 2.0.x

```
ipfwadm -F -p deny
ipfwadm -F -a m -S yyy.yyy.yyy.yyy/x -D 0.0.0.0/0
```

ou

```
ipfwadm -F -p deny
ipfwadm -F -a masquerade -S yyy.yyy.yyy.yyy/x -D 0.0.0.0/0
```

Où x est le nombre correspondant à la classe de votre sous reseau, et yyy.yyy.yyy.yyy est l'adresse de votre réseau.

```
Masque de sous réseau | x  | Sous réseau
~~~~~~~~~~~~~~~~~~~~~|~~~~|~~~~~~~~~~~~~~~
255.0.0.0            | 8  | Classe A
255.255.0.0          | 16 | Classe B
255.255.255.0        | 24 | Classe C
255.255.255.255      | 32 | Point-to-point (PPP)
```

Vous pouvez aussi utiliser le format yyy.yyy.yyy.yyy/xxx.xxx.xxx.xxx, où xxx.xxx.xxx.xxx spécifie votre masque de sous réseau tel 255.255.255.0

Par exemple dans mon réseau de classe C, j'entrais ;

```
ipfwadm -F -p deny
ipfwadm -F -a m -S 192.168.1.0/24 -D 0.0.0.0/0
```

Puisque les paquets de demande de bootp arrivent sans adresse IP valide alors que le client ne connait rien de lui, les personnes utilisant un serveur bootp comme machine de masquerading/firewall devront utiliser la commande suivante avant la commande deny :

```
ipfwadm -I -a accept -S 0/0 68 -D 0/0 67 -W bootp_clients_net_if_name -P udp
```

Vous pouvez également faire cela machine par machine. Par exemple, si je veux que 192.168.1.2 et 192.168.1.8 aient accès à Internet, mais pas les autres machines, j'utiliserai :

```
ipfwadm -F -p deny
ipfwadm -F -a m -S 192.168.1.2/32 -D 0.0.0.0/0
ipfwadm -F -a m -S 192.168.1.8/32 -D 0.0.0.0/0
```

Une erreur fréquente est d'utiliser comme première règle la commande :

`ipfwadm -F -p masquerade`

Il ne faut **jamais** que votre règle par défaut soit le masquerading, sinon n'importe qui pouvant manipuler ses tables de routage pourra utiliser votre machine Linux pour masquer son identité !

Une fois encore, vous pouvez ajouter ces lignes à vos fichiers `/etc/rc.local`, ou le faire manuellement à chaque fois que vous avez besoin de l'IP Masquerading.

Veuillez lire la section 4.4 pour des instructions détaillées sur Ipfwadm.

3.5 Tester IP Masquerade

Il est maintenant temps de tester notre travail. Assurez vous que la connexion de votre hôte Linux à Internet est correcte.

Vous pouvez par exemple essayer de parcourir quelques sites Web (sur *Internet* !!!) depuis vos **AUTRES** machines, et voir ce que vous obtenez. Je recommande d'utiliser une adresse IP plutôt qu'un nom DNS lors de votre premier essai, puisque votre réglage pour le DNS peut être incorrect.

Par exemple, vous pouvez accéder au site Web du Linux Documentation Project à http://metalab.unc.edu/mdw/linux.html en entrant *http://152.19.254.81/mdw/linux.html*

Si vous voyez la page du LDP, félicitations ! Ca marche ! Vous pouvez alors essayer avec un autre hôte, puis ping, telnet, ssh, ftp, Real Audio, True Speech, etc...

Pour l'instant je n'ai eu aucun problème avec ces réglages, et c'est totalement grâce aux personnes qui ont passé du temps à faire fonctionner cette superbe fonctionnalité de Linux.

4 Autres sujets relatifs à IP Masquerade et au support logiciel

4.1 Problèmes avec IP Masquerade

Certains protocoles ne marcheront pas avec l'IP masquerading, parce que soit ils supposent des choses sur les numéros de port ou soit qu'ils encodent les données sur le port et les adresses dans leurs paquets. Ces protocoles ont besoin de *proxy* intégrés dans le code du masquerading pour fonctionner.

4.2 Services entrants

Le masquerading ne peut pas du tout prendre en charge les services entrants. Il y a plusieurs façons de les autoriser, mais ces méthodes sont complètement en dehors du thème du masquerading et se rapprochent plutôt de la technique des firewalls.

Si vous n'avez pas besoin d'une grande sécurité, vous pouvez simplement rediriger les ports. Il y a de nombreuses façons de faire cela - personnellement j'utilise une version modifiée du programme redir (qui, je l'espère, sera disponible sur sunsite et ses mirrors prochainement). Si vous désirez avoir des niveaux d'autorisation sur les connexions entrantes, vous pouvez alors utiliser les `TCP Wrappers` ou `Xinetd` par dessus redir (version 0.7 ou supérieure) pour autoriser seulement des adresses IP données, ou utiliser d'autre outils. La boîte à outils pour firewall TIS (TIS Firewall Toolkit) est un bon produit pour ceux qui cherchent des outils et des informations.

Une section en disant plus long sur le forwarding sera bientot ajoutée.

4.3 Programmes clients supportés et autres remarques pour la configuration

> **** La liste suivante n'est plus maintenue. Voyez *cette page* sur les applications fonctionnant au travers d'IP Masquerading et la page *IP Masquerade Resource* pour plus de détails. ****

En général, les applications qui utilisent TCP et/ou UDP devraient fonctionner. Si vous avez une quelconque suggestion ou question à propos des applications compatibles avec IP masquerade, visitez la page sur les *applications fonctionnant avec IP Masquerading* par Lee Nevo.

4.3.1 Les clients qui fonctionnent

Clients génériques

HTTP
: toutes les plateformes, naviguer sur le web ;

POP & SMTP
: toutes les plateformes, clients de courrier électronique ;

Telnet
: toutes les plateformes, sessions distantes ;

FTP
: toutes les plateformes, avec le module `ip_masq_ftp.o` (tous les sites ne fonctionnent pas avec certains clients ; par exemple, certains sites ne peuvent pas être atteints en utilisant ws_ftp32 mais fonctionnent avec Netscape) ;

Archie
: toutes les plateformes, client de recherche de fichiers (tous les clients ne fonctionnent pas) ;

NNTP (USENET)
: toutes les plateformes, client news USENET ;

VRML
: Windows (peut être toutes les plateformes), réalité virtuelle ;

traceroute
: surtout les plateformes UNIX, certaines variantes ne devraient pas fonctionner ;

ping
: toutes plateformes, avec le patch ICMP

quoique ce soit, basé sur IRC
toutes les plateformes, avec le module `ip_masq_irc.o` ;

Client Gopher
toutes les plateformes ;

Client WAIS
toutes les plateformes.

Clients Multimédia

Real Audio Player 2.0
Windows, flux audio par réseau, avec le module `ip_masq_raudio`

True Speech Player 1.1b
Windows, flux audio par réseau

Internet Wave Player
Windows, flux audio par réseau

Worlds Chat 0.9a
Windows, programme client-serveur de discussion 3D

Alpha Worlds
Windows, programme client-serveur de discussion 3D

Internet Phone 3.2
Windows, communications audio. Vous ne pouvez être contacté que si vous initiez la connexion, mais on ne peut pas vous appeler.

Powwow
Windows, communication audio. Vous ne pouvez être contacté que si vous initiez la connexion, mais on ne peut pas vous appeler.

CU-SeeMe
toutes les plateformes, avec le module cuseeme, voir sur *IP Masquerade Resource* `<http://ipmasq.cjb.net>` pour les détails.

VDOLive
Windows, avec le patch vdolive

NB : Certains clients tels IPhone et Powwow peuvent fonctionner même si vous n'êtes pas la personne qui initie la connexion, en utilisant le *package ipautofw* (voir la section 4.6).

Autres clients

NCSA Telnet 2.3.08
DOS, une suite de logiciels contenant telnet, ftp, ping, etc...

PC-anywhere pour Windows 2.0
MS-Windows, controle d'un PC à distance avec TCP/IP, fonctionne uniquement si la machine est un client et non un hôte.

Socket Watch
utilise ntp - network time protocol

Linux net-acct package
Linux, package d'administration par réseau

4.3.2 Clients qui ne fonctionnent pas

Intel Internet Phone Beta 2
Connexion ok, mais la voix ne peut que sortir de votre réseau.

Intel Streaming Media Viewer Beta 1
Connexion impossible au serveur.

Netscape CoolTalk
Connexion à l'hôte distant impossible.

talk,ntalk
ne fonctionnera pas - nécessite l'écriture d'un proxy noyau.

WebPhone
Ne peut pas fonctionner (il fait des suppositions
invalides sur les adresses).

X
Non testé, mais je pense que cela ne peut pas fonctionner à moins que quelqu'un écrive un proxy X, qui est sans doute un programme externe au code de masquerading. Une façon de le faire fonctionner est d'utiliser **ssh** comme lien, et X comme proxy.

4.3.3 Plateformes/Systèmes d'exploitations testés sur des machines clientes

- Linux
- Solaris
- Windows 95
- Windows NT (workstation et serveur)
- Windows pour Workgroup 3.11 (avec le package TCP/IP)
- Windows 3.1 (avec le package Chameleon)
- Novel 4.01 Serveur
- OS/2 (y compris Warp v3)
- Macintosh OS (avec MacTCP ou Open Transport)
- DOS (avec le package NCSA Telnet, DOS Trumpet fonctionne partiellement)
- Amiga (avec AmiTCP ou AS225-stack)
- Stations VAX 3520 et 3100 avec UCX (pile TCP/IP pour VMS)
- Alpha/AXP avec Linux/Redhat
- SCO Openserver (v3.2.4.2 et 5)
- IBM RS/6000 sous AIX

Normalement, tous les OS disposant d'une couche TCP/IP et permettant de specifier un firewall/gateway devraient marcher avec l'IP masquerading

4.4 Administration du firewall IP (ipfwadm)

Cette section constitue un guide plus précis sur l'utilisation d'ipfwadm.

Voici un script d'initialisation pour un système qui fait office de firewall et de masquerading. L'interface à laquelle on fait confiance est 192.168.255.1 (celle du réseau local) et l'interface PPP a été changée pour des raisons de sécurité. Toutes les interfaces sont listées individuellement pour intercepter l'IP spoofing et les routages inexacts. Tout ce qui n'est pas explicitement autorisé est interdit !

```
#!/bin/sh
#
# /etc/rc.d/rc.firewall, définit la configuration du firewall.
# appelé depuis rc.local.
```

```
#

PATH=/sbin:/bin:/usr/sbin:/usr/bin

# pour les tests, attend un moment puis efface toutes les règles du
# firewall. Décommentez les lignes suivantes si vous voulez que le firewall
# soit désactivé automatiquement après 10 minutes.
# (sleep 600; \
# ipfwadm -I -f; \
# ipfwadm -I -p accept; \
# ipfwadm -O -f; \
# ipfwadm -O -p accept; \
# ipfwadm -F -f; \
# ipfwadm -F -p accept; \
# ) &

# Connexions entrantes, efface tout et positionne le comportement par défaut à
# deny (refus). En fait, le comportement par défaut est inadéquat puisqu'il y
# a une règle pour tout intercepter, avec refus et logging.
ipfwadm -I -f
ipfwadm -I -p deny
# interface locale, machines locales. Aller n'importe où est autorisé.
ipfwadm -I -a accept -V 192.168.255.1 -S 192.168.0.0/16 -D 0.0.0.0/0
# interface distante, prétendant être une machine locale. C'est de l'IP
# spoofing, on refuse.
ipfwadm -I -a deny -V votre.adresse.PPP.statique -S 192.168.0.0/16 -D 0.0.0.0/0 -o
# interface distante, n'importe qu'elle source, l'accès à notre adresse PPP
# est valide
ipfwadm -I -a accept -V votre.adresse.PPP.statique -S 0.0.0.0/0 -D votre.adresse.PPP.statique/32
# l'interface loopback est valide.
ipfwadm -I -a accept -V 127.0.0.1 -S 0.0.0.0/0 -D 0.0.0.0/0
# une fois toutes les règles faites, toutes les autres connexions entrantes
# sont refusées et logguées.
ipfwadm -I -a deny -S 0.0.0.0/0 -D 0.0.0.0/0 -o

# Connexions sortantes,efface tout et positionne le comportement par défaut à
# deny (refus).En fait, le comportement par défaut est inadéquat puisqu'il y a
# une règle pour tout intercepter, avec refus et logging.
ipfwadm -O -f
ipfwadm -O -p deny
# interface locale, machines locales. N'importe quelle source allant vers le
# réseau local est valide.
ipfwadm -O -a accept -V 192.168.255.1 -S 0.0.0.0/0 -D 192.168.0.0/16
# destination vers le réseau local à partir de l'interface sortante. C'est du
# routage piraté, tout refuser.
ipfwadm -O -a deny -V votre.adresse.PPP.statique -S 0.0.0.0/0 -D 192.168.0.0/16 -o
# sortante depuis le réseau local sur l'interface sortante. C'est du
# masquerading pirate, tout refuser.
ipfwadm -O -a deny -V  votre.adresse.PPP.statique -S 192.168.0.0/16 -D 0.0.0.0/0 -o
# sortante depuis le réseau local sur l'interface sortante. C'est du
```

```
# masquerading pirate, tout refuser.
ipfwadm -O -a deny -V votre.adresse.PPP.statique -S 0.0.0.0/0 -D 192.168.0.0/16 -o
# l'interface loopback est valide.
ipfwadm -O -a accept -V 127.0.0.1 -S 0.0.0.0/0 -D 0.0.0.0/0
# une fois toutes les règles faites, toutes les autres connexions sortantes
# sont refusées et logguées.
ipfwadm -O -a deny -S 0.0.0.0/0 -D 0.0.0.0/0 -o


# Connexions à faire suivre (forwarding), efface tout et positionne le
# comportement par défaut à deny (refus). En fait, le comportement par défaut
# est inadéquat puisqu'il y a une règle pour tout intercepter, avec refus et
# logging.
ipfwadm -F -f
ipfwadm -F -p deny
# Masquerade depuis le réseau local sur l'interface locale vers n'importe où
ipfwadm -F -a masquerade -W ppp0 -S 192.168.0.0/16 -D 0.0.0.0/0
# une fois toutes les règles faites, toutes les autres connexions à faire
# suivre sont refusées et logguées.
ipfwadm -F -a deny -S 0.0.0.0/0 -D 0.0.0.0/0 -o
```

Vous pouvez bloquer le trafic vers ou depuis un site particulier en utilisant -I, -O ou -F. Souvenez vous que les règles sont analysées de haut en bas, et -a signifie ajoute (*append*) à l'ensemble des règles existantes. Par exemple (non testé) :

En utilisant les règles -I. Probablement le plus rapide mais stoppe uniquement les machines locales, le firewall peut encore accéder au site "interdit". C'est peut être d'ailleurs le comportement que vous désirez.

```
... début des règles -I ...
# rejette et loggue l'interface locale et la machine locale allant sur
# 204.50.10.13
ipfwadm -I -a reject -V 192.168.255.1 -S 192.168.0.0/16 -D 204.50.10.13/32 -o
# interface locale, machines locales. Aller n'importe où est autorisé.
ipfwadm -I -a accept -V 192.168.255.1 -S 192.168.0.0/16 -D 0.0.0.0/0
... fin des règles -I ...
```

En utilisant les règles -O. C'est le plus lent puisque les paquets passent d'abord à travers le masquerading, mais cette règle empèche même au firewall d'accéder au site interdit.

```
... début des règles -O ...
# rejette et loggue les connexions sortantes vers 204.50.10.13
ipfwadm -O -a reject -V votre.adresse.PPP.statique -S votre.adresse.PPP.statique/32 -D 204.50.10.13/32 -o
# tout le reste, sortant vers l'interface distante est valide
ipfwadm -O -a accept -V votre.adresse.PPP.statique -S votre.adresse.PPP.statique/32 -D 0.0.0.0/0
... fin des règles -O ...
```

En utilisant les règles -F. Probablement plus lent qu'en utilisant les règles -I, et cela stoppe uniquement les machines pour lesquelles on effetue du masquerading (c'est à dire les machines internes). Le firewall peut encore accéder au site interdit.

```
... début des règles -F ...
```

```
# Rejette et loggue les connexions depuis le réseau local sur l'interface PPP
# vers 204.50.10.13.
ipfwadm -F -a reject -W ppp0 -S 192.168.0.0/16 -D 204.50.10.13/32 -o
# Masquerade depuis le réseau local sur l'interface locale vers n'importe où
ipfwadm -F -a masquerade -W ppp0 -S 192.168.0.0/16 -D 0.0.0.0/0
... fin des règles -F ...
```

Il n'y a pas besoin d'une règle spéciale pour autoriser 192.168.0.0/16 à se connecter sur 204.50.11.0, ce comportement est inclus dans les règles globales.

Il y a plus d'une façon d'écrire les règles précédentes. Par exemple, au lieu de -V 192.168.255.1, vous pouvez utiliser -W eth0, au lieu de -V votre.adresse.PPP.statique, vous pouvez utiliser -W ppp0. C'est une question de goût personnel.

4.5 Chaines IP Firewalling (ipchains)

Voici l'outil de manipulation de règles de firewalling créé pour les noyaux 2.2.x (il y a un patch qui permettra de l'utiliser avec le 2.0.x).

Nous mettrons à jour cette section pour donner plein d'exemples sur l'utilisation d'ipchains très bientôt.

Référez vous à *Linux IP Firewalling Chains page* <http://www.rustcorp.com/linux/ipchains/> et *Linux IPCHAINS HOWTO* <http://www.freenix.org/unix/linux/HOWTO-vo/IPCHAINS-HOWTO.html> pour plus de détails.

4.6 L'IP Masquerade et la numérotation à la demande.

1. Si vous voulez que votre réseau se connecte automatiquement à Internet, le package *diald* de numérotation à la demande sera une grande aide.
2. Pour mettre en place *diald*, veuillez vous référer à la page (en anglais) *Setting Up Diald for Linux Page* <http://home.pacific.net.sg/~harish/diald.config.html>
3. Une fois que diald et IP masq auront été installés, vous pouvez aller sur n'importe laquelle des machines clients et initier une connexion web, telnet ou ftp.
4. *diald* va détecter une demande, appeler votre provider Internet et établir la connexion.
5. Un *timeout* (délai d'attente dépassé) sera inévitable sur la première connexion, mais c'est le lot des modems analogiques. Le temps mis à établir la connexion va provoquer un timeout de votre programme client. Ceci peut être évité si vous utilisez une connexion ISDN. Tout ce que vous devez faire est relancer le client qui a fait le timeout.

4.7 Faire suivre les paquets avec IPautofw

IPautofw est un module générique pour faire suivre les paquets TCP et UDP pour le Masquerading de Linux. Généralement, pour utiliser un client utilisant UDP, un module spécifique doit être chargé. Ipautofw agit de manière plus générique, puisqu'il fait suivre tout type de trafic, y compris ceux pour lesquels les modules spécifiques ne feront rien suivre. Cela peut créer un trou de sécurité, si ce n'est pas administré correctement.

4.8 CU-SeeMe et le mini-HOWTO Linux IP-Masquerade

Fournis par *Michael Owings* <mailto:mikey@swampgas.com>.

4.8.1 Introduction

Cette section explique les étapes nécessaires pour faire en sorte que Cu-SeeMe (Les deux versions : Cornell ou White Pine) marche bien avec l'IP-Masquerade de Linux.

Cu-SeeMe est un paquetage de vidéoconférence disponible pour Windows et Macintosh. Une version gratuite est disponible à *Cornell University* `<http://cu-seeme.cornell.edu>`. Une version commerciale largement améliorée peut etre obtenue à *White Pine Software* `<http://www.wpine.com>`.

L'IP masquerade permet à une ou plusieurs machines d'un LAN de se cacher derriere une seule machine Linux connectée à Internet. Les stations du LAN accedent à Internet d'une maniere presque transparente meme sans adresse IP valide. La machine Linux réécrit les paquets sortant du LAN pour aller vers Internet de telle sort qu'ils semblent venir de cette meme machine. Les paquets revenants sont réécrits et reroutés vers la bonne machine sur le LAN. Cet arrangement permet à la majorité des applications Internet de marcher de façon transparente depuis les stations du LAN. Pour quelques applications (comme CU-SeeME), néanmoins, le code de routage masquerading de Linux a besoin d'un peu d'aide pour router les paquets proprement. Cette aide vient de modules spéciaux du noyau. Pour plus d'informations sur l'IP Masquerading, référez vous à *The Linux IP Masquerading Website* `<http://www.indyramp.com/masq/>`.

4.8.2 Le faire marcher...

Tout d'avord, vous avec besoin d'un noyau proprement configuré. Vous devriez avoir un support complet de compilé pour IP-Masquerading et IP-AutoForwarding. IP AutoForwarding est disponible depuis la version 2.0.30 du noyau - vous aurez a patcher des noyaux plus anciens. Référez vous à *Linux IP Masquerade Resource* `<http://ipmasq.cjb.net>` pour des liens vers l'IP-AutoForwarding.

Ensuite, vous aurez besoin de la derniere version de ip_masq_cuseeme.c. La derniere version est disponible via FTP depuis *ftp://ftp.swampgas.com/pub/cuseeme/ip_ masq_ cuseeme.c*. Ce nouveau module sera inclut dans la version 2.0.31 du noyau. Vous devriez remplacer le votre par celui là. ip_masq_cuseeme.c réside normalement dans le repertoire net/ipv4 des sources de linux. Vous devriez compiler et installer ce module.

Maintenant, vous devriez mettre en place de l'ip autoforwarding pour les ports udp 7648 et 7649 comme il suit :

```
ipautofw -A -r udp 7648 7649 -c udp 7648 -u
```

Ou

```
ipautofw -A -r udp 7648 7649 -h www.xxx.yyy.zzz
```

La premiere forme autorisera les appels de/vers la derniere station à avoir utilisé le port 7648 (le port Cu-SeeMe principal). Je préfere la premiere invocation car elle est plus flexible car il n'y a pas besoin de specifier une IP fixe. Bien sur, cela implique que la station aura eu à faire un appel sortant pour pouvoir recevoir un appel...

Notez que que les deux lignes laissent les ports 7648 et 7649 des machines clients ouvertes au monde exterieur - et bien que cela ne pose pas un trop gros trou de sécurité, vous devriez etre précautionneux.

Finalement, chargez le nouveau modules ip_masq_cuseeme comme ça :

```
modprobe ip_masq_cuseeme
```

Vous devriez maintenant être capable de lancer CU-SeeMe depuis une machine cachée sur votre LAN et de vous connecter à un réflecteur distant, ou à un autre utilisateur de CU-SeeMe. Vous devriez aussi etre capable de recevoir des appels. Notez que les appelant de l'exterieur devront appeler l'IP de votre gateway, PAS la station cachée.

4.8.3 Restrictions/Mise en garde

Reflecteurs protégé par mot de passe Ce n'est même pas la peine d'y songer. White Pine utilise l'IP source (comme cela est fait par le client) pour encrypter le mot de passe avant la transmission. Comme nous avons à réécrire l'adresse le réflecteur utilise une mauvaise IP pour pour le decrypter, ce qui donne un mot de passe invalide... Cela ne sera réparé que si White Pine change sa facon d'encryter (comme je leur ait suggéré), ou si ils decident de rendre leurs routines d'encryption publique de telle sorte que l'on puisse réparrer ip_masq_cuseeme. Alors que les chances de voir la deuxieme solution s'envolent, j'encourage tous ceux qui lisent ça à contacter White Pine et leur suggérer la premiere approche. Comme le trafic sur cette page est relativement gros, je suppose que nous pouvons générer suffisament d'email pour faire avancer ce probleme dans la liste de priorités de White Pine.

Merci à Thomas Griwenka d'avoir porté cela à mon attention.

Lancer un Réflecteur Vous ne devez pas essayer de lancer un réflecteur sur la même machine où vous avez un ip_masq_cuseeme et un ipautoforwarding sur le port 7648 de chargé. Cela ne marcherais pas, car les deux requièrent le port 7648. Donc, lancez le réflecteur soit sur une machine accessible depuis l'Internet, ou déchargez le support pour le client Cu-SeeMe avant de lancer le réflecteur.

Plusieurs utilisateurs de CU-SeeMe Vous ne pouvez pas avoir plusieurs utilisateurs simultanés de CU-SeeMe sur le LAN au même instant. Ceci est du au fait que CU-SeeMe se borne à toujours utiliser le port 7648, qui ne peut être redirigé (facilement) qu'à une seule station en même temps.

En utilisant du -c (port controleur) en lancant ipautofw ci-dessus, vous pouvez eviter de spécifier une adresse de station fixe autorisée a utiliser CU-SeeMe. La première station qui envoie quelque chose sur le port 7648 sera désignée pour recevoir le trafic sur les ports 7648 et 7649. A peu pres 5 minutes après que cette station soit devenue inactive sur le port 7648, une autre station pourra utiliser CU-SeeMe.

Besoin d'aide pour CU-SeeMe? N'hésitez pas à envoyer un email avec vos commentaires ou vos questions à *mikey@swampgas.com*. Ou si vous préférez, vous pouvez m'*appeler via CU-SeeMe* `<http://www.swampgas.com/vc/vc.htm>`.

4.9 Autres outils en relation

Nous mettrons à jour cette section très prochainement pour traiter d'autres outils en relation avec ipmasq tels ipportfw ou masqadmin.

5 Foire Aux Questions

Si vous trouvez une FAQ intéressante, envoyez la à *ambrose@writeme.com* et *dranch@trinnet.net* (NdT: en anglais :-)). S'il vous plait, poser clairement la question et la réponse appropriée. Merci !

5.1 Est-ce que IP Masquerade marche avec une IP dynamique?

Oui, bien sur que cela marche avec une adresse IP dynamique assignée par votre FAI, d'habitude, via un serveur DHCP. Aussi longtemps que vous avez une adresse Internet valide, cela devrait marcher. Bien entendu, les IP statiques conviennent aussi.

5.2 Puis-je utiliser des modems cable, DSL, liaison satellite, etc pour me connecter à Internet en utilisant IP masquerading ?

Bien sûr, tant que Linux supporte l'interface réseau, cela marchera.

5.3 Quels sont les programmes qui fonctionnent avec l'IP Masquerade ?

Il est très difficile d'avoir une liste exhaustive des "programmes qui marchent". Toutefois, la majorité des applications internet sont supportées, telles que surfer sur Internet (Netscape, MSIE, etc.), ftp (comme WS_FTP), Real Audio, telnet, SSH, POP3 (courrier entrant - pine, Outlook), SMTP (courrier sortant), etc.

Les programmes qui impliquent des protocoles plus compliqués ou des méthodes de connexion spéciales necessitent des outils d'aide spéciaux.

Pour plus de détails, référez vous à cette page : *programmes qui marchent avec le Linux IP masquerading* `<http://dijon.nais.com/~nevo/masq/>` par Lee Nevo.

5.4 Comment puis-je faire marcher l'IP Masquerading sur une RedHat, une Debian, une Slackware, etc ?

La distribution de Linux que vous avez, les procédures pour mettre en place l'IP masquerading mentionnées dans ce HOWTO devraient suffire. Certaines distributions auront peut être des programmes graphiques ou des fichiers de configuration spéciaux pour rendre les réglages plus simples. Nous faisons en sorte de rendre ce HowTo aussi simple que possible.

5.5 Je viens de passer au noyau 2.2.x et ça ne marche plus !

Il y a plusieurs raisons qui peuvent faire que cela ne marche plus, en supposant que vous avez une bonne connection à Internet et à votre LAN :

- Assurez vous que vous avez les fonctionnalités et les modules nécessaires compilés et chargés. Référez vous aux sections précedentes pour cela.
- Vérifiez `/usr/src/linux/Documentation/Changes` et assurez vous que vous avez les bonnes versions des outils réseau installés.
- Assurez vous d'avoir bien activé l'IP forwarding. Essayez de lancer `echo "1" > /proc/sys/net/ipv4/ip_forwarding`.
- Vous devez utiliser *ipchains* `<http://www.rustcorp.com/linux/ipchains/>` pour manipuler les regles ipmasq et firewal.
- Refaites toute la préparation et la configuration encore ! La plupart du temps, c'est juste une erreur de typo ou une erreur stupide que vous verrez facilement.

5.6 Je viens de mettre à jour mon noyau avec un 2.0.30 ou plus récent et ça ne marche plus !

Il y a plusieurs chose que vous devriez vérifier, en supposant que vous avez une bonne connection à Internet et à votre LAN :

- Assurez vous que vous avez bien toutes les fonctionnalités et modules de compilés et chargés. Référez vous aux sections précédentes pour plus de détails.

– Verifiez dans `/usr/src/linux/Documentation/Changes` que vous avez bien mis a jour le minimum pour survivre.
– Assurez vous de bien avoir activé l'IP forwardinf. Essayez `echo "1" > /proc/sys/net/ipv4/ip_forward`.
– Vous devriez utiliser *ipfwadm* `<http://www.xos.nl/>` pour manipuler les regles ipmasq et firewall. Vous aurez a patcher les noyaux 2.0.x pour utiliser ipchains.
– Refaites toute la préparation et la configuration encore ! La plupart du temps, c'est juste une erreur de typo ou une erreur stupide que vous verrez facilement.

5.7 Je n'arrive pas à faire marcher l'IP Masquerade ! Quelles sont les possibilités pour le faire avec Windows ?

Laisser tomber une solution gratuite, fiable, performante qui fonctionne sur un matériel minimal pour payer une fortune pour quelque chose qui nécessite plus de matériel, est moins performant et moins fiable ? (IMHO : Et oui, j'ai une expérience de ces choses ;-)

Ok, c'est vous qui voyez, faites une recherche sur le web sur MS Proxy Server, Wingate, ou aller sur www.winfiles.com. Mais ne dites pas que c'est moi qui vous y envoie !

5.8 J'ai tout vérifié, et ça ne marche toujours pas. Que dois-je faire ?

– Restez calme. Allez vous faire un thé, et prenez une pose. Ensuite, essayez les suggestions ci-dessous.
– Faites une recherche dans l'*Archive de la mailing list* `<http://home.indyramp.com/lists/masq/>`, votre réponse vous y attend très certainement.
– Posez la question dans la mailing list IP Masquerade, voyez ci-dessous pour plus de détails. S'il vous plait, n'essayez cela que si vous ne trouvez pas la réponse dans les archives de la liste.
– Posez votre question dans les newsgroups parlant de réseau et de Linux.
– Envoyez un email à *ambrose@writeme.com* et *dranch@trinnet.net*. Vous avez plus de chance de recevoir une réponse si vous nous l'envoyez à nous deux. David est plutôt rapide a répondre, et je ne commenterais pas ma vitesse de réponse.
– Revérifiez votre configuration :-)

5.9 Comment je m'inscris à la liste IP Masquerade ?

Pour s'inscrire à la liste IP Masquerading envoyez un mail à *masq-subscribe@indyramp.com*.

Le sujet et le corps de ce message sont **ignorés**. Ceci vous permet de recevoir tous les messages de la liste alors qu'ils arrivent. Vous avez la possibilité de recevoir les messages sous cette forme, mais si vous pouviez plutot vous abonner au condensé (digest), choisissez le plutôt. Le digest charge moins les machines qui servent les listes. Notez aussi qu'il n'est possible de poster qu'à partir de l'adresse où vous êtes enregistrés.

Pour plus de commandes, envoyez un email à *masq-help@tori.indyramp.com*.

5.10 Je veux aider au développement de l'IP Masquerading. Comment faire ?

Abonnez vous à la liste de développement de l'IP Masquerading, et contactez les grands développeurs là-bas, en envoyant un email à *masq-dev-subscribe@tori.indyramp.com* (ou pour le digest *masq-dev-digest-subscribe@tori.indyramp.com*).

NE posez pas de questions n'ayant pas de rapport avec le développement sur cette liste !!

5.11 Où puis-je trouver plus d'informations sur l'IP Masquerading ?

Vous pouvez trouver plus d'informations sur l'IP Masquerading à *Linux IP Masquerade Resource* `<http://ipmasq.cjb.net/>` que David et moi maintenons. référez vous a la section 6.2 pour la disponibilité.

Vous pouvez aussi trouver plus d'informations à *The Semi-Original Linux IP Masquerading Web Site* `<http://www.indyramp.com/masq/>` maintenu par Indyramp Consulting, qui fournissent aussi les listes ipmasq.

5.12 Je veux traduire ce HOWTO dans une autre langue. Comment faire ?

Assurez vous que le langage dans lequel vous voulez traduire n'est pas déjà couvert par quelqu'un d'autre; une liste des traductions faites est disponible sur *Linux IP Masquerade Resource* `<http://ipmasq.cjb.net/>`.

Envoyez un email à *ambrose@writeme.com* et je vous enverrais la derniere version du SGML de ce HOWTO.

5.13 Ce HOWTO semble à l'abandon, vous vous en occupez toujours ? Pouvez vous inclure plus d'informations sur ... ? Comptez vous l'améliorer ?

Oui, ce HOWTO est toujours maintenu. Je suis coupable d'être trop occupé à travailler sur deux boulots et je n'ai pas beaucoup de temps pour travailler dessus, toutes mes excuses. Toutefois, avec l'arrivée de David Ranch et tant que mainteneur, les choses devraient bouger un peu.

Si vous pensez à un sujet qui devrais être inclus dans ce HOWTO, envoyez nous un email. Cela serais encore mieux si vous pouviez nous fournir cette information. David et moi inclurons cette information dans le HOWTO si elle nous semble appropriée. Et merci pour votre contribution.

Nous avons beaucoup de nouvelles idées et de plans pour mettre à jour ce HOWTO, comme des études de cas, qui couvreraient differentes configurations réseau mettant en jeu l'IP Masquerading, plus de choses sur la sécurité, l'utilisation d'ipchains, des exemples sur ipfwadm/ipchains, plus de FAQ, plus de choses sur les utilitaires de forwarding de port et de protocoles tels masqasmin, etc. Si vous pensez que vous pouvez aider, faites le. Merci.

5.14 J'ai reussi à faire marcher l'IP Masquerade, c'est génial ! Qu'est ce que je pourrais faire pour vous remercier ?

Remerciez les developpeurs, et appréciez le temps et les efforts qu'ils ont passés dessus. Envoyez nous un email pour nous faire savoir que vous êtes contents. Faites connaitre Linux autour de vous, et aidez les gens qui ont des problèmes.

6 Divers

6.1 Ressources utiles

Note du Traducteur : Tous les documents cités dans cette section sont en anglais, à moins d'une mention spéciale de ma part.

- *IP Masquerade Resource page* `<http://ipmasq.cjb.net/>` devrait contenir assez d'information pour l'installation d'IP Masquerade
- L'*archive de la mailing list IP Masquerade* `<http://www.indyramp.com/masq/list/>` contient certains des messages envoyés récement sur la liste.

- Ce document, en anglais : *Linux IP Masquerade mini HOWTO* `<http://ipmasq.cjb.net/ipmasq-HOWTO.html>` pour les noyaux 2.2.x et 2.0.x.
- Le *IP Masquerade HOWTO pour les noyaux 1.2.x* `<http://ipmasq.cjb.net/ipmasq-HOWTO-1.2.x.txt>` si vous utilisez un vieux noyau
- La *FAQ IP Masquerade* `<http://www.indyramp.com/masq/ip_masquerade.txt>` contient des informations générales
- *Linux IPCHAINS HOWTO* `<http://www.freenix.org/unix/linux/HOWTO-vo/IPCHAINS-HOWTO.html>` et *http://www.rustcorp.com/linux/ipchains/* contiennent plein d'informations sur l'utilisation d'ipchains, ainsi que les sources et les binaires pour ipchains.
- La page *X/OS Ipfwadm page* `<http://www.xos.nl/linux/ipfwadm/>` contient les sources, binaires, de la documentation et d'autres informations sur le package `ipfwadm`.
- Une page sur les *applications qui marchent avec l'IP Masquerading de Linux* `<http://dijon.nais.com/~nevo/masq/>` par Lee Nevo fournis des trucs et astuces pour faire marcher tout ça avec l'IP Masquerading.
- Le *LDP Network Administrator's Guide* `<http://metalab.unc.edu/mdw/LDP/nag/nag.html>` est incontournable pour les débutants essayant d'installer un réseau.
- *Trinity OS Doc* `<http://www.ecst.csuchico.edu/~dranch/LINUX/TrinityOS.wri>`, Une documentation très complete sur l'utilisation de Linux en réseau.
- Le *Linux NET-3 HOWTO* `<http://www.freenix.org/unix/linux/HOWTO/NET-3-HOWTO.html>` (**en français**) contient aussi beaucoup d'informations utiles sur l'utilisation du réseau sous Linux.
- Le *Linux ISP Hookup HOWTO* `<http://www.freenix.org/unix/linux/HOWTO/ISP-Hookup-HOWTO.html>` (**en français**) et le *PPP HOWTO* `<http://www.freenix.org/unix/linux/HOWTO/PPP-HOWTO.html>` (**en français**) vous donnent des informations pour connecter votre hôte Linux sur Internet.
- Le *Linux Ethernet-Howto* `<http://www.freenix.org/unix/linux/HOWTO/Ethernet-HOWTO.html>` (**en français**) est une bonne source d'informations sur la mise un place d'un réseau local utilisant Ethernet.
- Vous pouvez également être intéressé par le *Linux Firewalling and Proxy Server HOWTO* `<http://www.freenix.org/unix/linux/HOWTO/Firewall-HOWTO.html>` (**en français**)
- Le *Linux Kernel HOWTO* `<http://www.freenix.org/unix/linux/HOWTO/Kernel-HOWTO.html>` (**en français**) vous guidera pour pour la recompilation de votre noyau.
- D'autres HOWTOs, en *français* `<http://www.freenix.org/unix/linux/HOWTO/>`, ou en *anglais* `<http://www.caldera.com/LDP/HOWTO/HOWTO-INDEX-3.html>`.
- Poster dans les newsgroups USENET : *comp.os.linux.networking*, ou, en français, *fr.comp.os.linux.configuration* ou *fr.comp.os.linux.moderated*

6.2 Ressources sur l'IP Masquerade

Le site *Linux IP Masquerade Resource* `<http://ipmasq.cjb.net/>` est dédié à l'IP Masquerading, aussi maintenu par David Ranch et moi. Les dernieres informations y sont toujours disponibles, et il peut y avoir des choses non disponibles dans ce HOWTO.

Vous trouverez les ressources sur l'IP Masquerading aux endroits suivants :

- *http://ipmasq.cjb.net/*, site primaire, redirigé sur *http://www.tor.shaw.wave.ca/~ambrose/*
- *http://ipmasq2.cjb.net/*, site secondaire, redirigé sur *http://www.geocities.com/SiliconValley/Heights/2288/*

6.3 Remerciements

- David Ranch, dranch@trinnet.net
  Aide à maintenir ce HOWTO, et la page de l'IP Masquerading, ..., trop de choses pour tout mettre ici :)

- Michael Owings, mikey@swampgas.com
  Pour avoir fournis la section sur CU-SeeMe et le Linux IP-Masquerade mini How-To
- Gabriel Beitler, gbeitler@aciscorp.com
  section 3.3.8 sur Novell.
- Ed Doolittle, dolittle@math.toronto.edu
  suggestion de l'option `-V` dans la commande `ipfwadm` pour une sécurité améliorée
- Matthew Driver, mdriver@cfmeu.asn.au
  aide active pour cet HOWTO, et écriture de la section section 3.3.1 (configuration de Windows 95)
- Ken Eves, ken@eves.com
  pour la FAQ qui m'a servi à écrire cet HOWTO
- Ed. Lott, edlott@neosoft.com
  pour une longue liste de logiciels et de systèmes testés
- Nigel Metheringham, Nigel.Metheringham@theplanet.net
  pour sa contribution au IP Packet Filtering et IP Masquerading HOWTO, ce qui fait de ce HOWTO un meilleur document plus technique
  section 4.1, 4.2, et autres
- Keith Owens, kaos@ocs.com.au
  pour l'excellent guide d'ipfwadm de la section 4.2
  pour la correction de l'option `ipfwadm -deny` qui évite un trou de sécurité et a clarifié le statut de `ping` sous IP Masquerade
- Rob Pelkey, rpelkey@abacus.bates.edu
  pour les sections 3.3.6 et 3.3.7 (configuration de MacTCP et Open Transport)
- Harish Pillay, h.pillay@ieee.org
  pour la section 4.5 (numérotation à la demande avec diald)
- Mark Purcell, purcell@rmcs.cranfield.ac.uk
  pour la section 4.6 sur IPautofw
- Ueli Rutishauser, rutish@ibm.net
  pour la section 3.3.9 sur OS/2 Warp
- John B. (Brent) Williams, forerunner@mercury.net
  pour la section 3.3.7 (configuration d'Open Transport)
- Enrique Pessoa Xavier, enrique@labma.ufrj.br
  pour la suggestion de la configuration de bootp
- Les développeurs d'IP Masquerade pour cet excellent produit
  - Delian Delchev, delian@wfpa.acad.bg
  - Nigel Metheringham, Nigel.Metheringham@theplanet.net
  - Keith Owens, kaos@ocs.com.au
  - Jeanette Pauline Middelink, middelin@polyware.iaf.nl
  - David A. Ranch, trinity@value.net
  - Miquel van Smoorenburg, miquels@q.cistron.nl
  - Jos Vos, jos@xos.nl
  - Paul Russell, Paul.Russell@rustcorp.com.au
  - Et tous ceux que j'ai pu oublier (faites-le moi savoir !)
- tous les utilisateurs envoyant des suggestions et des critiques à la mailing list, et plus particulièrement ceux qui m'ont fait part d'erreurs dans ce document et les clients supportés ou non.
- Je vous demande pardon si je n'ai pas inclus les informations que certains utilisateurs m'ont envoyées. De nombreuses idées et suggestions me sont envoyées, mais je n'ai pas le temps de les vérifier, ou je les égare. J'essaie de faire de mon mieux pour incorporer toutes les informations qu'on m'envoye pour rédiger ce HOWTO. Je vous remercie pour votre effort, et j'espère que vous comprenez ma situation.

6.4 Réference

- IP masquerade FAQ de Ken Eves
- Archive de la mailing list IP Masquerade de Indyramp Consulting
- La page sur Ipfwadm par X/OS
- Divers HOWTOs liés au réseau sous Linux