Mini-COMO de Linux IP Masquerade, en ESPAÑOL.

Original de Ambrose Au, ambrose@writeme.com
Traducción de XosÉ Vázquez, xose@ctv.es
Original v1.2, 10 de noviembre de 1997; traducción, 20 de noviembre de 1997.

Este documento describe cómo activar la función IP Masquerade en un servidor Linux, permitiendo conectar a Internet, mediante su máquina Linux, ordenadores que no tienen registrada una dirección IP de Internet.

Índice General

1 Introducción.

1.1 Introducción.

Este documento describe cómo activar la función IP masquerade en un servidor Linux, permitiendo conectar a Internet, mediante su máquina Linux, ordenadores que no tengan registrada una dirección IP de Internet. Es posible conectar sus máquinas con el servidor Linux, tanto con ethernet como con otro tipo de conexiones, con un enlace ppp. Este documento hará énfasis en las conexiones ethernet, ya que este es el caso más usual.

Este documento está pensado para usuarios de núcleos 2.0.x. Los núcleos en desarrollo 2.1.x no son tratados.

1.2 Prólogo, retrospectiva y créditos.

Encuentro muy confuso, como nuevo usuario, configurar IP masquerade en los núcleos nuevos, esto es, `2.x`. Aunque hay *PUF*[1]s y listas de correo, no hay documentos dedicados a esto; y como hay algunas peticiones en las listas de correo solicitando un COMO que lo cubra, decidí escribirlo como punto de partida para

[1] **P**reguntas de **U**so **F**recuente

nuevos usuarios, y posiblemente como sección básica para que usuarios experimentados puedan crear más documentación. Si piensa que no estoy haciendo un buen trabajo, siéntase libre de decírmelo para que pueda hacerlo mejor.

Este documento está fuertemente basado en la *PUF* original de Ken Eves, y numerosos mensajes de ayuda de la lista de correo de `IP MASQUERADE`. Gracias especiales a Mr. Matthew Driver, cuyos mensajes a la lista de correo me inspiraron para configurar `ip_masq` y eventualmente para escribir esto.

Por favor siéntase libre de enviarme cualquier crítica o comentario a `ambrose@writeme.com` si algo de lo aquí explicado le parece erróneo, o si echa algo de menos. ¡Su inestimable comentario podrá influenciar el futuro de este COMO!

Este COMO está pensado para ser una guía rápida a fin conseguir que el IP Masquerade funcione en el plazo de tiempo más corto posible.

Podrá encontar las últimas novedades, así como mayor información en las páginas web de IP Masquerade Resource `http://ipmasq.home.ml.org/` que mantengo. Si tiene alguna pregunta técnica sobre IP Masquerade, por favor entre en la Lista de Correo de IP Masquerade en lugar de enviarme correo electrónico, mi tiempo es limitado, y los desarrolladores de `IP_Masq` están más capacitados para responder a sus preguntas.

La última versión de este documento se puede encontrar en *IP Masquerade Resource*, el cual también contiene las versiones HTML y PostScript:

- `http://ipmasq.home.ml.org/`
- Por favor consulte `http://ipmasq.home.ml.org/index.html#mirror`, réplica de estas páginas.

1.3 Copyright & Disclaimer.

** Nota del traductor ** : Aunque se traducen los términos de la licencia sólo se hace con carácter informativo. Se deja intacta la licencia original.

Nadie será responsable de daño alguno sufrido por sus ordenadores y cualesquiera otras pérdidas ocasionadas por el uso de la información contenida en este documento. Esto es:

> **EL AUTOR (y el TRADUCTOR) NO SE RESPONSABILIZA DE NINGÚN DAñO SUFRIDO DEBIDO A LAS ACCIONES REALIZADAS BASADAS EN ESTE DOCUMENTO.**

2 Conceptos básicos.

2.1 ¿Qué es IP Masquerade?

IP Masquerade es una capacidad de red de Linux en desarrollo. Si un servidor Linux está conectado a Internet con IP Masquerade habilitado, los ordenadores conectados a él (bien en la misma red local, bien por módem) también pueden conectarse a Internet, incluso aunque no tengan *una dirección IP oficial asignada*.

Esto permite a un conjunto de máquinas acceder *transparentemente* a Internet ocultas tras la máquina pasarela, la cual aparece como el único sistema que está usando Internet. Romper la seguridad de un sistema configurado de forma correcta con IP Masquerade es considerablemente más difícil que romper un buen filtro de paquetes basado en cortafuegos (suponiendo que no existan fallos en ninguno).

2.2 Estado actual

IP Masquerade está todavía en etapa experimental. De todas formas, los núcleos a partir del `1.3.x` tienen ya soporte interno incorporado. Muchos particulares y empresas lo están usando, con resultados satisfactorios.

Se ha comprobado que los Navegadores de páginas web y telnet funcionan bien sobre `ip_masq`. FTP, IRC y Real Audio funcionan con ciertos módulos cargados. Otras variedades de audio por red como True Speech e Internet Wave también funcionan. Algunos usuarios de la lista de correo incluso lo intentaron con software de vídeo-conferencia. Incluso `ping` funciona ahora, con el nuevo parche ICMP.

Por favor diríjase a la sección 4.3 para ver la lista completa de programas soportados.

IP Masquerade funciona bien con 'máquinas clientes' con diferentes sistemas operativos y plataformas. Ha habido éxito con sistemas usando Unix, Windows 95, Windows NT, Windows para Trabajo en Grupo (con el paquete TCP/IP), OS/2, Sistemas Macintosh OS con Mac TCP, Mac Open Transport, DOS con el paquete NCSA Telnet, VAX, Alpha con Linux, e incluso Amiga con AmiTCP o AS225-stack.

2.3 ¿Quién puede beneficiarse de IP Masquerade?

- Si tiene un servidor Linux conectado a Internet, y
- si tiene algunos ordenadores con TCP/IP conectados con esa máquina Linux en una subred local (LAN) , y/o
- si su servidor Linux tiene más de un módem y actúa como un servidor PPP o SLIP conectando a otros,
- los cuales no tienen asignada una dirección IP oficial. (Estas máquinas son representadas por **OTRAS** máquinas presentes).
- Y por supuesto, si quiere que esas **OTRAS** máquinas estén en Internet sin gastar dinero extra :)

2.4 ¿Quién NO necesita IP Masquerade?

- Si su máquina es un servidor Linux aislado conectado a Internet, entonces es inútil usar `ip_masq`, o
- si ya tiene direcciones asignadas a sus **OTRAS** máquinas, entonces no necesita IP Masquerade,
- y por supuesto, si no le gusta la idea de una salida gratuita a Internet.

2.5 ¿Cómo funciona IP Masquerade ?

De la *PUF* de IP Masquerade por Ken Eves:

Representación de la configuración más simple :

```
 SLIP/PPP        +------------+                        +------------+
 al proveedor    |  Linux     |       SLIP/PPP         | OTRA       |
<---------- modem1|            |modem2 <---------- modem |            |
  111.222.333.444 |            |          192.168.1.100 |            |
                 +------------+                        +------------+
```

En el dibujo de arriba un servidor Linux con ip_masquerading instalado y funcionando está conectado a Internet vía SLIP o PPP usando el `modem1`. Tiene asignada la dirección IP 111.222.333.444. En esta configuración ese `modem2` permite a las personas que llaman entrar e iniciar una conexión SLIP/PPP.

El segundo sistema (el cual no tiene porqué usar Linux) llama al servidor Linux e inicia una conexión SLIP o PPP. No tiene asignada una dirección IP en Internet así que usa 192.168.1.100 (ver abajo).

Con ip_masquerade y el rutado configurado adecuadamente la máquina OTRA puede interactuar con Internet como si estuviera realmente conectada (con unas pocas excepciones).

Citando a Pauline Middelink:

No olvide mencionar que OTRA debería tener al servidor Linux como su pasarela (si es la ruta por defecto o sólo una subred no importa). Si la OTRA no puede hacer esto, la máquina Linux debería hacer un proxy arp para todas las direcciones de rutado, pero la configuración del proxy arp va más allá del alcance del documento.

Lo siguiente es un extracto de un correo de `comp.os.linux.networking` que se ha editado para corresponder los nombres usados en el ejemplo de arriba:

- Le digo a la máquina OTRA que mi servidor Linux es su pasarela.
- Cuando un paquete llega a la máquina Linux desde OTRA, le asignará un nuevo número de puerto origen, y pega su propia dirección IP en la cabecera del paquete, guardando los originales. Entonces mandará el paquete modificado a Internet sobre el interfaz PPP/SLIP.
- Cuando un paquete viene desde Internet para la máquina Linux, si el número de puerto es uno de esos asignados arriba, obtendrá el puerto original y la dirección ip, repondrá la cabecera del paquete y lo enviará a OTRA.
- El servidor que envía el paquete nunca notará la diferencia.

Un ejemplo de IP Masquerading

el ejemplo típico se muestra en la siguiente figura:

```
+----------+
|          |  Ethernet
| ordenador|::::::
|    A     |2    :192.168.1.x
+----------+     :
                 :   +----------+   enlace
+----------+     :  1|  Linux   |   ppp
|          |     ::::| masq-gate|:::::::::// Internet
| ordenador|::::::   |          |
|    B     |3    :   +----------+
+----------+     :
                 :
+----------+     :
|          |     :
| ordenador|::::::
|    C     |4
+----------+

<- Red  Interna ->
```

En este ejemplo hay 4 ordenadores que centran este documento. También hay algo al otro lado de su conexión IP que le suministra la información de Internet y además otros sistemas con los que está interesado en intercambiar información.

El sistema Linux `masq-gate` es la pasarela enmascarada para la red interna de los ordenadores A, B y C que permite el acceso a Internet. La red interna usa una de las direcciones de red privadas, en este caso la red de clase C 192.168.1.0, donde la máquina Linux[2] tiene la dirección 192.168.1.1 y los demás tienen direcciones de esa misma red.

Las tres máquinas A, B y C (que pueden estar usando cualquier sistema operativo, siempre que pueda "hablar IP", como Windows 95, Macintosh MacTCP o incluso otro Linux) pueden conectarse a otras máquinas de Internet, ya que el sistema masquerade `masq-gate` enmascara todas sus conexiones de tal forma que parezcan originadas en `masq-gate`, y se encarga de que los datos que le devuelven en una conexión enmascarada sean retransmitidos al sistema original. Así los sistemas de la red interna ven una ruta directa a Internet y son incapaces de darse cuenta que sus datos están siendo enmascarados.

2.6 Requerimientos para usar IP Masquerade en Linux `2.x`

Por favor diríjase a `http://ipmasq.home.ml.org/` para información más actualizada, es difícil actualizar este COMO con frecuencia.

- Fuentes del núcleo `2.0.x`, disponibles en `ftp://ftp.kernel.org/pub/linux/kernel/v2.0/`

  (Sí, tendrá que compilar su núcleo con ciertos soportes... Se recomienda el último núcleo estable)

- Módulos cargables del núcleo, preferiblemente `2.0.0` o superior disponibles en `http://www.pi.se/blox/modules/modules-2.0.0.tar.gz`

  (`modules-1.3.57` es lo mínimo requerido)

[2] N. del T.
Mejor dicho, el interfaz ethernet de la máquina Linux

- Montar una red TCP/IP bien configurada, tema tratado en `http://www.caldera.com/LDP/HOWTO/NET-2-HOWTO.html` y en `http://linuxwww.db.erau.edu/NAG/`, disponible en castellano en `http://www.infor.es/LuCAS` como *GARL*, o *Guía del Administrador de Redes Linux*.
- Conexión a Internet para su servidor Linux.

  Tratado en `http://www.caldera.com/LDP/HOWTO/ISP-Hookup-HOWTO.html`, *PPP-Como*, disponible en `http://www.insflug.org` y `http://www.caldera.com/LDP/HOWTO/mini/PPP-over-ISDN`, así como para los que dispongan de Infovía, el *Infobia-Como*, `http://www.insflug.org`
- Ipfwadm 2.3 o más reciente, disponible en `ftp://ftp.xos.nl/pub/linux/ipfwadm/ipfwadm-2.3.tar.gz` más información sobre requerimientos de versiones en `http://www.xos.nl/linux/ipfwadm/`
- Puede opcionalmente aplicar parches de IP Masquerade para habilitar otras funcionalidades. Dispone de más información acerca de esto en `http://ipmasq.home.ml.org/` (estos parches aplicados a todos los núcleos `2.0.x`)

3 Configuración de IP Masquerade.

Si su red privada contiene información vital, piénselo dos veces antes de usar IP Masquerade. Esto puede ser una PASARELA para que salga a Internet, y viceversa, para que alguien de otra parte del mundo entre en su red.

3.1 Cómo compilar el núcleo para dar soporte IP Masquerade.

Por favor, diríjase a `http://ipmasq.home.ml.org/` para información más actualizada, es difícil actualizar este COMO frecuentemente.

- Lo primero de todo, necesita las fuentes del núcleo (preferiblemente la última versión estable, `2.0.0` o superior).
- Si es la primera vez que compila el núcleo, no se asuste. De hecho es bastante fácil y está perfectamente documentado en el *Kernel-Como* `http://www.insflug.org`.
- Descomprima las fuentes del núcleo en `/usr/src/` con el comando:

  ```
  tar xvzf linux-2.0.x.tar.gz -C /usr/src
  ```

  donde `x` es el nivel del parche sobre el núcleo `2.0.x` (asegúrese de que hay un directorio o un enlace simbólico llamado `linux`).
- Aplique los parches apropiados. Desde que están saliendo parches nuevos, los detalles no serán incluidos aquí. Por favor busque en `IP Masquerade Resources` para información más actualizada.
- Consulte el *Kernel-Como* y el fichero `README` de los fuentes del núcleo para más instrucciones sobre la compilación.
- Aquí están las opciones que necesita para compilar: Diga *SI* a lo siguiente:

  ```
  * Prompt for development and/or incomplete code/drivers
    CONFIG_EXPERIMENTAL
  ```

  esto permite seleccionar el código experimental `ip_masq` compilado en el núcleo.

```
* Enable loadable module support
  CONFIG_MODULES
```

le permitirá cargar módulos.

```
* 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
```

aunque es experimental, es *INDISPENSABLE*

```
* IP: ipautofw masquerade support (EXPERIMENTAL) [SOLO nucleos 2.0.30 y superiores]
  CONFIG_IP_MASQUERADE_IPAUTOFW
```

recomendado.

```
* IP: ICMP masquerading [SOLO nucleos 2.0.30 y superiores]
  CONFIG_IP_MASQUERADE_ICMP
```

soporte para enmascarar paquetes ICMP, opcional.

```
* IP: always defragment
  CONFIG_IP_ALWAYS_DEFRAG
```

altamente recomendado

```
* Dummy net driver support
  CONFIG_DUMMY
```

recomendado.

NOTA:

Estos son los componentes que necesita para `ip_masq`, seleccione cualquier otra opción que necesite para su configuración específica.

- Después de compilar el núcleo, debería de compilar e instalar los módulos:

```
make modules; make modules_install
```

- Luego debe añadir unas pocas líneas al fichero `/etc/rc.d/rc.local` (o en el apropiado) para cargar los módulos requeridos, que residen en `/lib/modules/2.0.x/ipv4/`, automáticamente durante el arranque:

```
              .
              .
              .
       /sbin/depmod -a
       /sbin/modprobe ip_masq_ftp
       /sbin/modprobe ip_masq_raudio
       /sbin/modprobe ip_masq_irc
```

(u otros módulos como `ip_masq_cuseeme`, o `ip_masq_vdolive` si ha aplicado parches)

Nota:

También puede cargar los módulos manualmente antes de usar `ip_masq`, pero no use `kerneld` para esto, NO funcionará.

3.2 Asignación de direcciones IP en la red privada

Como todas las OTRAS máquinas no tienen dirección oficial asignada, debe haber una forma correcta de adjudicar direcciones para esas máquinas.

De la FAQ IP Masquerade:

Hay un RFC (#1597) en el cual están las direcciones IP para ser usadas en una red no conectada a Internet. Hay 3 bloques de números reservados específicamente para este fin. El que yo uso es una subred de clase C 255 desde 192.168.1.n hasta 192.168.255.n .

Del RFC 1597: Sección 3: Espacio para Direcciones Privadas

El *Internet Assigned Numbers Authority* (*IANA*) tiene reservado los siguientes 3 bloques de direcciones IP para redes privadas:

```
              10.0.0.0        -   10.255.255.255
              172.16.0.0      -   172.31.255.255
              192.168.0.0     -   192.168.255.255
```

Nos referiremos al primer bloque como "bloque de 24-bit", al segundo como "bloque de 20-bit", y al tercero como "bloque de 16-bit". Observe que el primer bloque no es más que un simple número de red de clase A, mientras que el segundo bloque es un conjunto de 16 números de red de clase B contiguos y el tercer bloque un conjunto de 255 números de red de clase C contiguos.

Así, si está usando una red de clase C, debería de nombrar a sus máquinas como 192.168.1.1, 1.92.168.1.2, 1.92.168.1.3, ..., 192.168.1.x

192.168.1.1 es normalmente la máquina pasarela, la cual es su servidor Linux conectado a Internet. Observe que 192.168.1.0 y 192.168.1.255 son las direcciones de RED (*Network*) y la dirección de EMISIÓN (*Broadcast*) respectivamente, las cuales están reservadas. Evite usar estas direcciones en sus máquinas.

3.3 Configuración de las OTRAS máquinas.

Además de asignar una dirección IP apropiada a las máquinas, también debería de poner la apropiada de la pasarela (*gateway*). En general, esto es coser y cantar. Simplemente introduzca la dirección de su servidor Linux (usualmente 192.168.1.1) como la dirección de la máquina pasarela.

Como Servidor de Nombres, puede añadir algún DNS disponible. El más obvio debería ser el que esté usando su máquina Linux. También puede añadir opcionalmente algún sufijo de dominio de búsqueda.

Después de que haya reconfigurado esas direcciones, recuerde reiniciar los servicios apropiados o reiniciar su sistema.

Las siguientes instrucciones de configuración suponen que está usando una red de clase C con 192.168.1.1 como dirección de su servidor Linux. Por favor, tenga en cuenta que 192.168.1.0 y 192.168.1.255 están reservadas.

3.3.1 Configuración de Windows 95.

1. Si no ha instalado todavía la tarjeta de red y el correspondiente controlador de dispositivo (*driver*), hágalo ahora.
2. Vaya a *'Panel de Control'/'Red'*.
3. Añada *'Protocolo'/'Microsoft'/'TCP/IP'* si no lo tiene.
4. En *'Propiedades'/'TCP/IP'*, vaya a *'Dirección IP'* y ponga la dirección IP 192.168.1.x, (1 < x < 255), y como máscara de subred 255.255.255.0.
5. Añada 192.168.1.1 como su pasarela en *'Puerta de enlace (Gateway)'*.
6. En *'Configuración DNS'/'Orden de búsqueda del servidor DNS'* añada el DNS que usa su servidor Linux (usualmente está en `/etc/resolv.conf`). Opcionalmente, puede añadir el apropiado sufijo de búsqueda de dominio.
7. Deje las otras opciones como están, salvo que sepa lo que está haciendo.
8. Pulse *'Aceptar'* en todas las cajas de diálogo y reinicialice el sistema.
9. Haga un `Ping` a la máquina Linux para comprobar la red: *'Inicio/Ejecutar'*, teclee : `ping 192.168.1.1`.

   (Esto sólo comprueba la conexión local, todavía no puede hacer `ping` al exterior.)
10. Opcionalmente puede crear un fichero `HOSTS` en el directorio de windows así puede usar los nombres de las máquinas de su red local. Hay un ejemplo llamado `HOSTS.SAM` en el directorio `c:\windows`.

3.3.2 Configuración de Windows para Trabajo en Grupo (3.11).

1. Si no ha instalado la tarjeta de red y el controlador, hágalo ahora.
2. Instale el paquete TCP/IP 32b si todavía no lo tiene.
3. En *'Principal'/'Configuración de Windows'/'Configuración de la Red'*, pulse en *'Controladores'*.
4. Marque *'Microsoft TCP/IP-32 3.11b'* en la sección *'Controladores de Red'*, pulse *'Setup'*.
5. Ponga la dirección IP 192.168.1.x (1 < x < 255), y la máscara de subred 255.255.255.0 y como Default Gateway 192.168.1.1
6. No habilite *'Automatic DHCP Configuration'* y no ponga nada en esas áreas de entrada *'WINS Server'* a menos que esté bajo un dominio de Windows NT y sepa lo que está haciendo.
7. Pulse *'DNS'*, añada la información mencionada en el PASO 6 de la sección 3.3.1, luego pulse *'Aceptar'* cuando esté listo.
8. Pulse *'Advanced'*, active *'Enable DNS for Windows Name Resolution'* y *'Enable LMHOSTS lookup'* si está usando un fichero de búsqueda de servidores, similar al mencionado en el PASO 10 de la sección 3.3.1
9. Pulse *'OK'* en todas las cuadros de diálogo y reinicialice el sistema.

10. Haga un `Ping` a la máquina Linux para comprobar la conexión de red: *'Archivo/Ejecutar'*, ponga: `ping 192.168.1.1`

    (Con esto sólo comprueba la conexión de la red local, todavía no puede hacer un `ping` al resto del mundo.)

3.3.3 Configuración de Windows NT.

1. Si no ha instalado su tarjeta de red y el controlador, hágalo ahora.
2. Vaya a *'Inicio'/'Panel de Control'/'Red'*
3. Añada *'Protocolo TCP/IP y Componentes Relacionados'* desde el menú *'Protocolos'* mediante el botón *'Agregar'* si no tiene todavía el servicio TCP/IP instalado.
4. En el área bajo *'Protocolos de red'*, seleccione *'Protocolo TCP/IP'*. Pinche en propiedades.
5. En *'Configuración TCP/IP'*, seleccione el adaptador de los instalados adecuado, por ejemplo: `[1]Novell NE2000 Adapter`. Luego ponga la Dirección IP 192.168.1.x (1 < x < 255), como Máscara de Subred 255.255.255.0 y como Pasarela 192.168.1.1.
6. No use la *'Configuración DHCP Automática'* y no ponga nada en *'WINS Server'* a menos que esté bajo un domino de Windows NT y sepa lo que está haciendo.
7. Pinche en *'DNS'*, y rellene con la información apropiada mencionada en el PASO 6 de la sección 3.3.1. Haga click en *'OK'* cuando esté listo.
8. Vaya a la sección *'Dirección WINS'*, y active las opciones *'Activar DNS para resolución de Windows'* y *'Activar la búsqueda de LMHOSTS'* si está usando un fichero de búsqueda de servidores, similar al mencionado en el PASO 10 de la sección 3.3.1
9. Pulse *'Aceptar'* en todos los cuadros de diálogo y reinicialice el sistema.
10. Haga un `Ping` a la máquina Linux para comprobar la conexión de red: (*'Inicio/Ejecutar'*), ponga: `ping 192.168.1.1`.

    (Esto sólo comprueba la conexión de la red local, todavía no puede hacer un `ping` al mundo exterior.)

3.3.4 Configuración de sistemas basados en UNIX.

1. Si no ha instalado la tarjeta de red y recompilado su núcleo con el controlador adecuado, hágalo ahora.
2. Instale la red TCP/IP, así como el paquete de herramientas de red, si no lo ha hecho todavía.
3. Ponga en la *DIRECCIÓN IP(IPADDR)* 192.168.1.x (1 < x < 255), y luego ponga 255.255.255.0 en *NETMASK*, *GATEWAY* 192.168.1.1, y en *BROADCAST* 192.168.1.255.

    Por ejemplo, puede editar el fichero `/etc/sysconfig/network-scripts/ifcfg-eth0` en sistemas Red Hat Linux, o simplemente hacerlo mediante el Control Panel.

    (Es diferente en SunOS, BSDi, Linux Slackware, etc...)
4. Añada su DNS y búsqueda de sufijo de dominio en `/etc/resolv.conf`
5. Puede querer actualizar su fichero `/etc/networks` dependiendo de sus configuraciones.
6. Reinicialice los servicios apropiados, o simplemente reinicialice el sistema.
7. Use un `ping` (comando: `ping 192.168.1.1`) para comprobar la conexión con la máquina pasarela.

    (Esto sólo comprueba la conexión de la red local, todavía no puede hacer un `ping` al mundo exterior.)

3.3.5 Configuración DOS usando el paquete NCSA Telnet.

1. Si no ha instalado la tarjeta de red, hágalo ahora.
2. Cargue el controlador adecuado. Para una tarjeta NE2000 , use `nwpd 0x60 10 0x300`, con su tarjeta de red en el IRQ 10 y la dirección hardware en 0x300 (Su configuración puede ser distinta).
3. Cree un nuevo directorio, y desempaquete el NCSA Telnet:

   ```
   pkunzip tel2308b.zip
   ```

4. Use un editor de texto para abrir el fichero `config.tel`
5. Ponga `myip=192.168.1.x` (1 < x < 255), y `netmask=255.255.255.0`
6. En este ejemplo, debería de poner `hardware=packet, interrupt=10, ioaddr=60`
7. Debería de tener al menos especificada una máquina individual como pasarela, por ejemplo, el servidor Linux :

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

8. Tiene otra especificación para el servicio de nombre de dominio:

   ```
   name=dns.dominio.com ; hostip=123.123.123.123; nameserver=1
   ```

   Nota: sustituya la información sobre el DNS por la que use en su servidor Linux.
9. Salve su fichero `config.tel`
10. Haga un telnet a la máquina Linux para comprobar la conexión de red: `telnet 192.168.1.1`

3.3.6 Configuración de sistemas basados en MacOS usando MacTCP

1. Si no ha instalado en controlador de su tarjeta ethernet, ahora podría ser un buen momento para hacerlo.
2. Abra el *MacTCP control panel*. Seleccione el controlador de red adecuado (Ethernet, NO EtherTalk) y pulse el botón *'More...'*.
3. Bajo *'Obtain Address:'*, pulse *'Manually'*.
4. Bajo *'IP Address:'*, seleccione *class C* del menú desplegable. Ignore el resto de esta sección de la caja de diálogo.
5. Rellene con la información adecuada, la *'Domain Name Server Information:'*.
6. Bajo *'Gateway Address:'*, introduzca 192.168.1.1
7. Pulse *'OK'* y sálvelo. En la ventana principal en *MacTCP control panel*, introduzca la dirección IP de su Mac (192.168.1.x, 1 < x < 255) en la caja *'IP Address:'*.
8. Cierre el *MacTCP control panel*. Si aparece un cuadro de diálogo indicando que reinicie el sistema, hágalo.
9. Puede hacer un ping a la máquina Linux para comprobar la conexión de red. Si tiene el programa freeware *MacTCP Watcher*, pulse en el botón *' Ping'*, e introduzca la dirección de su máquina Linux(192.168.1.1) en la caja de diálogo que se despliega. (Esto solamente comprueba la conexión de la red local, y todavía no puede hacer un ping al exterior.)

10. Opcionalmente puede crear un archivo `Hosts` en su *System Folder* de forma que pueda usar los nombres de la máquinas de su red local. Este archivo podría existir ya en su *System Folder*, y podría contener algunas entradas de ejemplo (comentadas) que puede modificar de acuerdo a sus necesidades.

3.3.7 Configuración de sistemas basados en MacOS usando Open Transport.

1. Si no ha instalado el controlador adecuado de la tarjeta ethernet, ahora sería un buen momento para hacerlo.
2. Abra el *TCP/IP Control Panel* y elija *'User Mode ...'* del menú *Edit*. Asegúrese que el modo de usuario es al menos *'Advanced '* y pulse el botón *'OK'*.
3. Elija *'Configurations...'* del menú *File*. Seleccione su configuración *'Default'* y pulse el botón *'Duplicate...'*. Introduzca 'IP Masq' (o algo para saber que está es una configuración especial) en el diálogo *'Duplicate Configuration'*, éste probablemente contendrá algo como *'Default copy'*. Luego pulse el botón *'OK'*, y el botón *'Make Active'*
4. Seleccione *'Ethernet'* del desplegable *'Connect via:'*.
5. Seleccione el elemento apropiado del desplegable *'Configure:'*. Si no sabe que opción elegir, probablemente debería de reselecionar su configuración *'Default'* y salir. Yo uso *'Manually'*.
6. Introduzca la dirección IP de su Mac (192.168.1.x, 1 < x < 255) en la caja *'IP Address:'*.
7. Ponga 255.255.255.0 en la caja de *'Subnet mask:'* .
8. Ponga 192.168.1.1 en la caja de *'Router address:'*.
9. Introduzca la dirección IP de su DNS en la caja *'Name server addr.: '*.
10. Introduzca el nombre de su dominio de Internet (por ejemplo: 'microsoft.com') en la caja *'Starting domain name'* bajo *'Implicit Search Path:'*.
11. Los siguientes procesos son opcionales. La introducción de valores incorrectos puede dar lugar a comportamientos erróneos. Si no está seguro, lo mejor es que los deje en blanco, sin marcar o sin seleccionar. Borre la información de esos campos, si es necesario. Hasta donde sé, no hay forma de decirle al sistema, a través de los diálogos TCP/IP, que no use un archivo de Hosts alternativo previamente seleccionado. Si Vd sabe cómo, me interesaría. Marque '802.3' si su red requiere tramas del tipo 802.3.
12. Pulse el botón *'Options...'* para estar seguro de que el TCP/IP está activo. Yo uso la opción '*Load only when needed*'. Si usa y quita aplicaciones TCP/IP con frecuencia sin reiniciar su máquina, puede que al deshabilitar esta última opción prevenga/reduzca los efectos de la administración de memoria. Con esta opción deshabilitada las pilas del protocolo TCP/IP están siempre cargadas y disponibles para su uso. Si está habilitada, las pilas TCP/IP se cargarán automáticamente cuando se necesiten y se descargarán cuando no. Estos procesos de carga y descarga hacen que la memoria de su máquina se fragmente.
13. Puede hacer un ping a su servidor Linux para comprobar la conexión de red. Si tiene el programa freeware *MacTCP Watcher*, pulse el botón *'Ping'* , e introduzca la dirección de su servidor Linux (192.168.1.1) en la caja de diálogo que aparece. (Esto sólo comprueba su conexión de la red local, todavía no puede hacer un ping al mundo exterior.)
14. Puede crear un fichero `Hosts` en *System Folder* y así podrá usar los nombres de las máquinas de su red local. Este fichero puede ya existir o no en la *System Folder*. Si es así, debería de contener alguna entrada (como comentario) de ejemplo, la cual puede modificar dependiendo de sus necesidades. Si no, puede obtener una copia del fichero de un sistema que use MacTCP, o crearlo Vd. mismo (sigue un subconjunto del formato de ficheros de Unix `/etc/hosts`, descrito en la página 33 de RFC 1035).

Una vez haya creado el fichero, abra el *TCP/IP control panel*, pulse el botón *'Select Hosts File...'*, y abra el archivo `Hosts`.

15. Pulse la caja cerrar o elija *'Close'* o *'Quit'* del menú *File*, y luego pulse el botón *'Save'* pasa salvar los cambios que ha hecho.

16. Los cambios tendrán efecto inmediatamente, pero reinicializando el sistema no pierde nada.

3.3.8 Configuración de red Novell usando DNS.

1. Si no tiene instalado el controlador apropiado de su tarjeta ethernet, ahora sería un buen momento para hacerlo.

2. Descargue el fichero `tcpip16.exe` de `ftp.novell.com/pub/updates/unixconn/lwp5`

3. edite

   `c:\nwclient\startnet.bat`

   : (aquí tiene una copia del mío)

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

4. edite

   `c:\nwclient\net.cfg`

   : (cambie el enlace del controlador por el suyo; por ejemplo : NE2000)

```
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. finalmente, cree el

   `c:\bin\resolv.cfg`

   :

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

6. Espero que esto ayude a alguien para conseguir poner su red Novell en línea. Esto se puede hacer usando Netware 3.1x o 4.x

3.3.9 Configuración de OS/2 Warp.

1. Si no tiene instalado el controlador de su tarjeta Ethernet, ahora sería un buen momento para hacerlo.
2. Instale el protocolo TCP/IP, si todavía no lo tiene.
3. Diríjase a *Programms/ TCP/IP (LAN) / TCP/IP* Settings.
4. En *'Network'* añada su dirección TCP/IP y ponga como máscara de red (Netmask) 255.255.255.0
5. En *'Routing'* presione *'Add'*. Ponga el *Type* en *'default'* y teclee la dirección IP de su servidor Linux en el campo *'Router Address'*. (192.168.1.1).
6. Ponga la misma dirección DNS (Servidor de nombres) que usa su servidor Linux en *'Hosts'*.
7. Cierre el panel de control de TCP/IP. Y responda SI a la siguiente(s) pregunta(s).
8. Reinicialice la máquina.
9. Debe de hacer un ping al servidor Linux para comprobar la configuración de red. Teclee `'ping 192.168.1.1'` en una 'Ventana de comandos de OS/2'. Si los paquetes ping son recibidos es que todo está bien.

3.3.10 Configuración de otros sistemas.

Se deberían de seguir los mismos pasos para otras configuraciones. Lea las secciones anteriores. Si está interesado en escribir sobre alguno de estos sistemas, o algunas variantes de sistemas basados en UNIX, por favor mande las instrucciones detalladas de configuración a `ambrose@writeme.com`.

3.4 Configuración de la política de IP Forwarding.

Llegados a este punto ya debería de tener instalados el núcleo y demás paquetes requeridos, así como los módulos cargados. También, la dirección IP, la pasarela, y el DNS deberían estar configurados en todas las **OTRAS** máquinas.

Ahora, la única cosa que queda por hacer es usar `ipfwadm` para reenviar los paquetes apropiados a la máquina apropiada:

Esto puede ser de realizado de diferentes formas. Las siguientes sugerencias y ejemplos a mí me funcionan, pero usted puede tener diferentes ideas, por favor mire la sección 4.4 y las páginas `man` de `ipfwadm` para más detalles.

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

donde `x` es uno de los siguientes números dependiendo del tipo de su subred, e `yyy.yyy.yyy.yyy` es su dirección de red.

```
mascara de red  | x  | Subred
~~~~~~~~~~~~~~~~|~~~~|~~~~~~~~~~~~~~~
255.0.0.0       | 8  | Clase A
255.255.0.0     | 16 | Clase B
255.255.255.0   | 24 | Clase C
255.255.255.255 | 32 | Punto-a-punto
```

Por ejemplo, si estuviera en una subred de clase C , tendría que haber puesto:

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

Al segundo comando podría añadir bien `-V 192.168.1.1` o bien `-W eth0` para asegurar que los paquetes enmascarados vienen a través del interfaz del sistema apropiado. Si quiere estar seguro a conciencia (también conocido como paranoia justificable) entonces querrá hacer esto.

Puesto que `bootp` solicita paquetes que vienen sin una dirección IP válida el cliente no sabe nada sobre ello, para gente con un servidor `bootp` en la máquina masquerade/cortafuegos es necesario usar lo siguiente antes del comando `deny`:

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

También puede hacerlo máquina por máquina. Por ejemplo, si quiere que la 192.168.1.2 y la 192.168.1.8 tengan acceso a Internet, pero no las otras máquinas, debería de poner:

```
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
```

Alternativamente, puede poner la máscara de red en lugar del valor, por ejemplo: 192.168.1.0/255.255.255.0

Lo que parece ser un ERROR común es poner como primer comando :

```
ipfwadm -F -p masquerade
```

NO haga que su política por defecto sea masquerading de esta forma alguien puede manipular su ruta y será capaz de entrar a través su pasarela, ¡¡usándola para enmascarar su identidad!!

De nuevo, puede añadir estas líneas al fichero `/etc/rc.local`, o al fichero `rc` que prefiera, o hágalo manualmente cada vez que necesite `ip_masq`.

Por favor lea la sección 4.4 para una guía detallada de `ipfwadm`.

3.5 Comprobación de IP Masquerade.

Después de todo este duro trabajo, es la hora hacer un intento. Asegúrese de que la conexión a Internet del servidor Linux está bien.

Puede intentar navegar por algún sitio web de *'¡¡¡INTERNET!!!'* en sus **OTRAS** máquinas, y ver si lo consigue. En su primer intento le recomiendo usar una dirección IP en vez de un nombre de máquina, porque la configuración del DNS puede no ser correcta.

Por ejemplo, puede acceder al servidor *Linux Documentation Project* `http://sunsite.unc.edu/mdw/linux.html` con el valor de `http://152.2.254.81/mdw/linux.html`.

Si ve la página del LDP, ¡felicidades!, ¡funciona! Luego puede intentarlo con el nombre del servidor, y luego un telnet, ftp, Real Audio, True Speech, ... o todo aquello soportado por IP Masquerade.....

Hasta ahora no he tenido problemas con las configuraciones anteriores, y están totalmente acreditadas por la gente que invierte su tiempo en hacer que esta maravillosa prestación funcione.

4 Otras características de IP Masquerade y soporte de programas.

4.1 Problemas con IP Masquerade.

Algunos protocolos no funcionarán adecuadamente con masquerading porque presuponen cosas sobre números de puerto; –o lo impiden datos cifrados en sus cadenas de información sobre direcciones y puertos– estos últimos protocolos necesitan un proxy específico en el código masquerading para que funcionen.

4.2 Servicios de entrada.

El Masquerading no puede manejar todos los servicios de entrada. Existen formas de permitirlos, pero son completamente independientes de masquerading, y son realmente parte de la práctica estándar de cortafuegos.

Si no requiere altos niveles de seguridad simplemente puede redireccionar los puertos. Hay varias formas para hacer esto –Yo uso un programa modificado llamado `redir` (espero que este disponible en sunsite y réplicas)–. Si desea tener algún nivel de autorización en conexiones entrantes puede usar TCP wrappers o Xinetd sobre `redir` (0.7 o superior) para permitir sólo direcciones IP específicas, o usar alguna otra herramienta. *El TIS Firewall Toolkit* es un buen lugar para buscar herramientas e información.

Se puede encontrar más detalles en `http://ipmasq.home.ml.org`.

4.3 Programas cliente soportados y otras notas de configuración.

La siguiente lista no será mantenida durante más tiempo.
Por favor, remítase a `http://masqapps.home.ml.org` para saber qué aplicaciones funcionan a través de un servidor Linux con IP masquerading y a `http://ipmasq.home.ml.org/` para más detalles.

Generalmente, las aplicaciones que usan TCP y UDP deberían de funcionar. Si tiene alguna sugerencia sobre aplicaciones que no son compatibles con IP Masquerade, por favor envíeme correo electrónico con el nombre del cliente y una breve descripción.

4.3.1 Clientes que funcionan

Clientes Generales

HTTP

todas las plataformas soportadas, navegadores web.

POP & SMTP

todas las plataformas soportadas, clientes de correo electrónico.

Telnet

todas las plataformas soportadas, sesión remota.

FTP

todas las plataformas soportadas, con el módulo `ip_masq_ftp.o` (no todos los servidores funcionan con ciertos clientes; por ejemplo algún sitio puede no ser alcanzado usando `ws_ftp32`, pero sí con Netscape)

Archie

todas las plataformas soportadas, buscador de archivos (no todos los clientes archie son soportados).

NNTP (USENET)

todas las plataformas soportadas, cliente de noticias USENET.

VRML

Windows (posiblemente soportado en todas las plataformas), navegación con realidad virtual.

traceroute

principalmente las plataformas basadas en UNIX, algunas variantes pueden no funcionar.

ping

todas las plataformas, con el parche ICMP.

todo lo basado en IRC

todas las plataformas soportadas, con el módulo `ip_masq_irc.o`

Clientes Gopher

todas las plataformas soportadas.

clientes WAIS

todas las plataformas soportadas.

Clientes Multimedia

Real Audio Player

Windows, envío de audio por red, con el módulo `ip_masq_raudio` cargado.

True Speech Player 1.1b

Windows, envío de audio por red.

Internet Wave Player

Windows, envío de audio por red.

Worlds Chat 0.9a

Windows, programa Cliente-Servidor 3D de conversación.

Alpha Worlds

Windows, programa Cliente-Servidor 3D de conversación.

Internet Phone 3.2

Windows, comunicaciones de audio de Igual-a-igual (*Peer-to-peer*), la gente puede ponerse en contacto con Vd. si inicia Vd. la conexión, pero no le pueden llamar.

Powwow

Windows, comunicaciones tipo *pizarra* de audio texto de Igual-a-igual, la gente puede ponerse en contacto con Vd. si Vd. inicia la llamada, pero ellos no pueden llamarle.

CU-SeeMe

todas las plataformas soportadas, con el módulo `cuseeme` cargado, por favor mire en `http://ipmasq.home.ml.org/` para los detalles.

VDOLive

Windows, con el parche `vdolive`.

Nota: Algunos clientes como IPhone y Powwow pueden funcionar incluso si Vd. no es el que inicia la llamada, si usa el paquete `ipautofw` (mire la sección 4.6)

Otros Clientes

NCSA Telnet 2.3.08

DOS, un paquete que contiene telnet, ftp, ping, etc.

PC-anywhere para windows 2.0

MS-Windows, control remoto de PCs sobre TCP/IP, sólo funciona si es cliente pero no servidor.

Socket Watch

usa ntp - protocolo de tiempo por red.

Linux net-acct package

Linux, paquete de administración de cuentas de red.

4.3.2 Clientes que NO funcionan

Intel Internet Phone Beta 2

Conecta pero la voz viaja en una dirección (sale) sólo.

Intel Streaming Media Viewer Beta 1

No puede conectar con el servidor.

Netscape CoolTalk

No puede conectar con el lado opuesto.

talk, ntalk

no funcionarán - requieren que sea escrito un proxy en el núcleo.

WebPhone

No puede funcionar por el momento (asume direcciones no válidas).

X

Sin probar, pero creo que no podrá funcionar a menos que alguien construya un X proxy, el cual probablemente es un programa externo al código de masquerading. Una forma de hacer que esto funcione es usar un **ssh** como el enlace y usar un X proxy interno ¡que haga funcionar las cosas!

4.3.3 Plataformas/SO testeados como las OTRAS máquinas.

- Linux
- Solaris
- Windows 95
- Windows NT (ambos, workstation y server)
- Windows para Trabajo En Grupo 3.11 (con el paquete TCP/IP)
- Windows 3.1 (con el paquete Chameleon)
- Novel 4.01 Server
- OS/2 (incluido Warp v3)
- Macintosh OS (con MacTCP u Open Transport)
- DOS (con el paquete NCSA Telnet, el DOS Trumpet trabaja parcialmente)
- Amiga (con AmiTCP o AS225-stack)
- VAX Stations 3520 y 3100 con UCX (TCP/IP stack para VMS)
- Alpha/AXP con Linux/Redhat
- SCO Openserver (v3.2.4.2 y 5)
- IBM RS/6000 con AIX
- (¿Alguien lo ha intentado con otras plataformas?)

4.4 Administración de cortafuegos IP con `ipfwadm`.

Esta sección proporciona una guía más exhaustiva del uso de **ipfwadm**.

Esta es una configuración para un sistema de cortafuegos/masquerade detrás de un enlace PPP con la siguiente dirección PPP estática. El interfaz de confianza es 192.168.255.1, el interfaz PPP ha sido cambiado para proteger al culpable :). Listé cada interfaz de entrada y salida individualmente para capturar IP spoofing también como ruta relleno y/o masquerading. ¡Todo aquello no explícitamente permitido esta prohibido!

```
#!/bin/sh
#
# /etc/rc.d/rc.firewall, define la configuracion del cortafuegos, invocado
# desde rc.local.
#

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

```
# comprobacion, espera un bit luego limpia toda norma del cortafuegos.
# descomente las siguientes lineas si quiere que el cortafuegos se
# desconecte automaticamente pasados 10 minutos
#
# (sleep 600; \
# ipfwadm -I -f; \
# ipfwadm -I -p accept; \
# ipfwadm -O -f; \
# ipfwadm -O -p accept; \
# ipfwadm -F -f; \
# ipfwadm -F -p accept; \
# ) &

# Entrante, purga y establece la politica por defecto de denegar. La
# verdad es que la politica por defecto es irrelevante porque hay un
# cierre de  toda norma con denegar y anotar

ipfwadm -I -f
ipfwadm -I -p deny

# interfaz local, maquinas locales, van a cualquier sitio valido
ipfwadm -I -a accept -V 192.168.255.1 -S 192.168.0.0/16 -D 0.0.0.0/0

# interfaz remota, reclamando ser maquinas locales, IP spoofing, perdido
ipfwadm -I -a deny -V su.direccion.ppp.estatica -S 192.168.0.0/16 -D 0.0.0.0/0 -o

# interfaz remota, cualquier origen, es valido ir a direcciones PPP permanentes
ipfwadm -I -a accept -V su.direccion.PPP.estatica -S 0.0.0.0/0 -D su.direccion.PPP.estatica/32

# el interfaz loopback es valido.
ipfwadm -I -a accept -V 127.0.0.1 -S 0.0.0.0/0 -D 0.0.0.0/0

# cierra toda norma, todas las otras entradas son denegadas y registradas.
# Lastima que no haya una opcion de registro, aunque esto hace el trabajo
# en su lugar

ipfwadm -I -a deny -S 0.0.0.0/0 -D 0.0.0.0/0 -o

# Saliente, purga y pone la politica por defecto de denegar. La verdad es
# que la politica por defecto es irrelevante porque hay un cierre de toda
# norma con  denegar y anotar

ipfwadm -O -f
ipfwadm -O -p deny

# interfaz local, cualquier origen con destino a la red local es valido
ipfwadm -O -a accept -V 192.168.255.1 -S 0.0.0.0/0 -D 192.168.0.0/16

# saliente para la red local sobre el interfaz remoto , stuffed routing,
# denegado

ipfwadm -O -a deny -V su.direccion.PPP.estatica -S 0.0.0.0/0 -D 192.168.0.0/16 -o

# saliente desde la red local sobre el interfaz remoto, stuffed masquerading,
# denegado
```

```
ipfwadm -O -a deny -V su.direccion.PPP.estatica -S 192.168.0.0/16 -D 0.0.0.0/0 -o

# saliente desde la red local sobre el interfaz remoto, stuffed masquerading,
# denegado

ipfwadm -O -a deny -V su.direccion.PPP.estatica -S 0.0.0.0/0 -D 192.168.0.0/16 -o

# algo mas saliente sobre la interfaz remota es valido.

ipfwadm -O -a accept -V su.direccion.PPP.estatica -S su.direccion.PPP.estatica/32 -D 0.0.0.0/0

# el interfaz loopback es valido.

ipfwadm -O -a accept -V 127.0.0.1 -S 0.0.0.0/0 -D 0.0.0.0/0

# norma de capturar todo, todo lo otro saliente es denegado y anotado.
# Lastima que no hay una opcion de registro en la politica pero esto
# hace  el trabajo en su lugar.

ipfwadm -O -a deny -S 0.0.0.0/0 -D 0.0.0.0/0 -o

# Envios, purga y pone la politica por defecto de denegar. La verdad es
# que la politica por defecto es irrelevante porque hay una cierre de toda
# norma con  denegar y anotar.

ipfwadm -F -f
ipfwadm -F -p deny

# Enmascaramiento (Masquerade) desde la red local sobre el interfaz local
# hacia cualquier sitio.

ipfwadm -F -a masquerade -W ppp0 -S 192.168.0.0/16 -D 0.0.0.0/0

# norma de capturar todo, el resto de envios son denegados y anotados.
# Lastima que no hay una opcion de registro en la politica, pero esto hace
# el trabajo en su lugar.

ipfwadm -F -a deny -S 0.0.0.0/0 -D 0.0.0.0/0 -o
```

Puede bloquear el tráfico para un sitio en particular usando `-I`, `-O` o `-F`. Recuerde que el conjunto de las normas son examinadas desde arriba hacia abajo y `-a` significa ªñadir" a los valores existententes de la norma, así cualquier restricción necesita venir antes de las normas generales. Por ejemplo (sin probar):

Usando normas `-I`. Probablemente es la más rápida pero sólo detiene las máquinas locales, el cortafuegos puede todavía acceder a sitios "prohibidos". Por supuesto le puede interesar permitir esa combinación.

```
... inicio de la norma -I ...
# rechaza y anota el interfaz local, las maquinas locales van a 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
# interfaz local, maquinas locales, ir a cualquier sitio es valido
ipfwadm -I -a accept -V 192.168.255.1 -S 192.168.0.0/16 -D 0.0.0.0/0
... fin de la norma -I ...
```

Usando la norma `-O`. Más lento porque los paquetes van primero a través de masquerading pero esta norma incluso detiene los accesos del cortafuegos a los sitios prohibidos.

```
... inicio de la norma -O  ...
```

```
# deniega y anota las salidas a 204.50.10.13
ipfwadm -O -a reject -V su.direccion.PPP.estatica -S su.direccion.PPP.estatica/32 -D 204.50.10.13/32 -o
# cualquier otra salida sobre el interfaz remoto es valida
ipfwadm -O -a accept -V su.direccion.PPP.estatica -S su.direccion.PPP.estatica/32 -D 0.0.0.0/0
... fin de la norma -O  ...
```

Usando la norma `-F`. Probablemente más lento que `-I` y esto todavía solo detiene a las máquinas enmascaradas (por ejemplo: las internas), el cortafuegos puede todavía acceder a sitios prohibidos

```
... inicio de  la norma -F  ...
# deniega y anota desde la red local sobre el interfaz PPP hacia 204.50.10.13.
ipfwadm -F -a reject -W ppp0 -S 192.168.0.0/16 -D 204.50.10.13/32 -o
# Enmascara (Masquerade) desde la red local sobre interfaces locales hacia
# cualquier sitio.
ipfwadm -F -a masquerade -W ppp0 -S 192.168.0.0/16 -D 0.0.0.0/0
... fin de la norma -F ...
```

No es necesario una norma especial para permitir a 192.168.0.0/16 para ir a 204.50.11.0, está cubierto por la norma global.

Hay más de una forma de codificar el interfaz en las normas de arriba. Por ejemplo en lugar de `-V 192.168.255.1` puede poner `-W eth0`, en lugar de `-V su.direccion.PPP.estatica` y puede usar `-W ppp0`. La elección es más que otra cosa personal y de documentación.

4.5 IP Masquerade y llamada bajo demanda (*Dial On Demand*).

1. Si le gustaría activar su red automáticamente para llamar a Internet, el paquete de llamada bajo demanda `diald` le será de gran utilidad.
2. Para configurar `diald`, por favor mire en `http://home.pacific.net.sg/~harish/diald.config.html`
3. Una vez que `diald` e `ip_masq` hayan sido configurados, puede ir a alguna de las máquinas clientes e iniciar una sesión web, telnet o ftp.
4. `diald` detectará peticiones entrantes, luego llamará a su ISP y establecerá la conexión.
5. Hay un tiempo de espera que ocurrirá con la primera conexión. Esto es inevitable si esta usando un módem analógico. El tiempo dado para establecer el enlace entre el módem y la conexión PPP causará que su programa cliente termine. Esto puede ser evitado si esta usando un conexión RDSI. Todo lo que necesita hacer es terminar el proceso actual en el cliente y reiniciarlo.

4.6 Reenvío de paquetes `ipautofw`.

`ftp://ftp.netis.com/pub/members/rlynch/ipautofw.tar.gz` es un transportador genérico de TCP y UDP para masquerading de Linux. Generalmente para utilizar un paquete que requiera UDP necesitará cargar un módulo específico de `ip_masq`; `ip_masq_raudio`, `ip_masq_cuseeme`, ... `ipautofw` actúa de una forma más genérica, enviará cualquier tipo de tráfico incluído aquel que los módulos específicos no envían. Esto puede crear un agujero de seguridad si no se administra correctamente.

5 Varios.

5.1 Obtención de ayuda.

Por favor NO INTENTE enviarme correo electrónico para consultas o problemas de IP Masquerade. Debido a mi intensa carga de trabajo personal, no prometo responder a todas las cuestiones que no se encuentren en la página web. En su lugar, para enviar sus dudas diríjase a `http://ipmasq.home.ml.org/index.html#mailinglist` (creo que es la mejor forma si no quiere recibir una respuesta pasadas semanas).

- `http://ipmasq.home.ml.org/` debería de tener suficiente información para montar IP Masquerade.
- Unirse a la lista de correo de IP masquerade (recomendado)

  Para suscribirse, envíe un mensaje electrónico con el tema "`subscribe`" (sin comillas) a `masq-request@indyramp.com`

  Para desubscribirse, envíe un correo electrónico con tema "`unsubscribe`" (sin comillas) a `masq-request@indyramp.com`

  Para obtener ayuda en el uso de la lista de correo, mande un mensaje con tema "`archive help`" o "`archive dir`" (sin comillas) a `masq-request@indyramp.com`
- `http://www.indyramp.com/masq/list/` contiene todos los mensajes pasados enviados a la lista.
- Este documento: `http://ipmasq.home.ml.org/ipmasq-HOWTO.html` para núcleos 2.x (si está usando un núcleo `1.3.x` ó `2.x`)
- `http://ipmasq.home.ml.org/ipmasq-HOWTO-1.2.x.txt` si está usando un núcleo antiguo.
- `http://www.indyramp.com/masq/ip_masquerade.txt` contiene algo de información general.
- `http://www.xos.nl/linux/ipfwadm/` contiene las fuentes, binarios, documentación, y otra información sobre el paquete `ipfwadm`.
- Una pagina sobre `http://masqapps.home.ml.org` por Lee Nevo proporciona trucos y consejos para que las aplicaciones funcionen con IP Masquerade.
- `http://linuxwww.db.erau.edu/NAG/` (*Network Administrator Guide*)[3] indispensable para principiantes que intentan instalar una red.
- `http://www.caldera.com/LDP/HOWTO/NET-2-HOWTO.html` también tiene mucha información útil sobre las redes en Linux.
- `http://www.caldera.com/LDP/HOWTO/ISP-Hookup-HOWTO.html`[4] y `http://www.caldera.com/LDP/HOWTO/PPP-HOWTO.html`[5] información de como conectar su servidor Linux a Internet.
- `http://www.caldera.com/LDP/HOWTO/Ethernet-HOWTO.html` es una buena fuente de información sobre montar una LAN con ethernet.
- También debe de estar interesado en `http://www.caldera.com/LDP/HOWTO/Firewall-HOWTO.html`[6]

[3] N del T:
Disponible en castellano, ver sección 6.5

[4] N del T:
disponible documento análogo en castellano, ver sección 6.5

[5] N del T:
Disponible en castellano ver sección 6.5

[6] N del T:
Disponible en castellano ver sección 6.5

- `http://www.caldera.com/LDP/HOWTO/Kernel-HOWTO.html`[7] le guiará para el proceso de compilar el núcleo.
- Otros `http://www.caldera.com/LDP/HOWTO/HOWTO-INDEX-3.html`
- Envíe correo al grupo de noticias de USENET: `comp.os.linux.networking`

5.2 Agradecimientos.

- Gabriel Beitler, `gbeitler@aciscorp.com` contribuyó en la sección 3.3.8 (Configuración de Novell)
- Ed Doolittle, `dolittle@math.toronto.edu` sugirió la opción `-V` en el comando `ipfwadm` para mejorar la seguridad.
- Matthew Driver, `mdriver@cfmeu.asn.au` por la extensa ayuda en este HOWTO, y mejora de la sección 3.3.1 (Configuración de Windows 95).
- Ken Eves, `ken@eves.com` por la PUF que proporcionó información incalculable para este COMO.
- Ed. Lott, `edlott@neosoft.com` por un larga lista de sistemas comprobados y programas.
- Nigel Metheringham, `Nigel.Metheringham@theplanet.net` contribuyó con su versión de IP Packet Filtering e IP Masquerading HOWTO, el cual hace de este HOWTO un documento mejor y con más profundidad técnica en las secciones 4.1, 4.2, y otras.
- Keith Owens, `kaos@ocs.com.au` proporcionó una excelente guía de `ipfwadm` en la sección 4.2 corrigió la opción `ipfwadm -deny` que evita un agujero de seguridad, y aclaró el estado de `ping` sobre `ip_masq`.
- Rob Pelkey, `rpelkey@abacus.bates.edu` proporcionó las secciones 3.3.6 y 3.3.7 (configurción de MacTCP y Open Transport).
- Harish Pillay, `h.pillay@ieee.org` proporcionó la sección 4.5 (llamada bajo demanda usando `diald`).
- Mark Purcell, `purcell@rmcs.cranfield.ac.uk` proporcionó la sección 4.6 (`ipautofw`)
- John B. (Brent) Williams, `forerunner@mercury.net` proporcionó la sección 3.3.7 (configuración Open Transport)
- Enrique Pessoa Xavier, `enrique@labma.ufrj.br` en la sugerencia de configuración de `bootp`.
- A los desarrolladores de Masquerade por esta gran prestación:
  - 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`
  - Y a quien haya olvidado mencionar aquí (por favor, hágamelo saber)
- A todos los usuarios que enviaron críticas y sugerencias a la lista de correo, especialmente a los que informaron de errores en la documentación y los clientes que son soportados y los que no.
- Pido disculpas si no he incluido información que algún usuario me haya enviado. Hay muchas sugerencias e ideas que me son enviadas, pero no tengo suficiente tiempo para verificarlas o pierdo la pista de ellas. Estoy intentando incorporar toda la información que me envían en el COMO. Le agradezco su esfuerzo, y espero que comprenda mi situación.

[7] N del T:
Disponible en castellano ver sección 6.5

5.3 Referencias.

- PUF de IP masquerade por Ken Eves.
- Archivos de la lista de correo de IP masquerade por *Indyramp Consulting*.
- Página de `ipfwadm` de X/OS.
- Diversos COMOs de Linux sobre redes.

6 Anexo de la traducción.

6.1 Traducción.

La traducción ha sido realizada por `XosÉ Vázquez`, en el grupo INSFLUG. Agradezco a Pablo Fábrega `pfabrega@arrakis.es` el repaso que le ha dado a este documento en busca de errores. Le agradecería que me enviase las imperfecciones que contenga este documento. Críticas no constructivas a > dev/null :-)

6.2 Anexo: El INSFLUG

El *INSFLUG* forma parte del grupo internacional *Linux Documentation Project*, encargándose de las traducciones al castellano de los Howtos (Comos), así como la producción de documentos originales en aquellos casos en los que no existe análogo en inglés.

En el **INSFLUG** se orienta preferentemente a la traducción de documentos breves, como los *COMOs* y *PUFs* (**P**reguntas de **U**so **F**recuente, las *FAQs*. `:)`), etc.

Diríjase a la sede del INSFLUG para más información al respecto.

En la sede del INSFLUG encontrará siempre las **últimas** versiones de las traducciones: `www.insflug.org`. Asegúrese de comprobar cuál es la última versión disponible en el Insflug antes de bajar un documento de un servidor réplica.

Se proporciona también una lista de los servidores réplica (*mirror*) del Insflug más cercanos a Vd., e información relativa a otros recursos en castellano.

Francisco José Montilla, `pacopepe@insflug.org`.

6.3 Fuentes de información en español

- `http://slug.ctv.es/`SLUG, grupo de usuarios de Linux.
- `http://www.infor.es/LuCAS` LuCAS, las *guides* y otros documentos en español.
- `http://mercury.chem.pitt.edu/~angel/LinuxFocus/Castellano/` Revista Linux Focus en castellano.
- Linux en México: `http://www.linux.org.mx/`
- Linux en Argentina: `http://www.linux.org.ar/`
- Linux en Uruguay: `Linux en Uruguay`
- `http://wagner.princeton.edu/~juan/manpages/`, páginas del manual (`man`) en español.
- `es.comp.os.linux`, grupo de noticias de linux en español.
- Área R34.Linux de Fido.
- Multiples `http://www.arrakis.es/~barreiro/menu_lista_es.shtml` listas de correo.

6.4 Recursos de Linux y distribuciones.

- Distribución Debian: `http://www.es.debian.org`

  `ftp://ftp.de.debian.org/debian`

- Distribución RedHat `http://www.redhat.com`

  `ftp://ftp.redhat.com/pub/redhat`

- Distribución Caldera, `http://www.caldera.com`

  `ftp://ftp.caldera.com/pub/`

- Distribución Slackware `http://www.slackware.org`

  Walnut Creek CDROM `http://www.cdrom.com`

  `ftp://ftp.cdrom.com/pub/linux`

- El hogar del núcleo, Kernel Org `http://www.kernel.org` y LinuxHQ `http://www.linuxhq.com` (información de actualizaciones y parches).

  `ftp://ftp.kernel.org/pub/linux/kernel`

- `http://www.linux.org`
- Linux Journal & Linux Gazette `http://www.ssc.com`
- Linux Documentation Project `http://sunsite.unc.edu/LDP`
- Sunsite `http://sunsite.unc.edu/pub/Linux/welcome.html`

  `ftp://sunsite.unc.edu/pub/Linux/`

- GNU, `http://www.gnu.org`, GNUstep `http://www.gnustep.org`

  `ftp://prep.ai.mit.edu/pub/gnu` y `ftp://ftp.gnustep.org/pub/gnustep`

- `ftp://tsx-11.mit.edu/pub/linux/`

6.5 Cómo colaborar

Existen diferentes proyectos de hispanohablantes relativos a la traducción de documentación y programas.

Si quiere colaborar en algún proyecto es *IMPRESCINDIBLE* que se ponga en contacto, con su coordinador :

- INSFLUG, `www.insflug.org`, traducción de COMOs coordinado por Francisco José Montilla, `pacopepe@insflug.org`.
- LuCAS, traducción de libros coordinado por Juan José Amor `jjamor@ls.fi.upm.es` o en fido `2:341/12.19`
- Páginas man, traducción de páginas del manual coordinado por Miguel Angel Sepúlveda `sepulved+@pitt.edu`
- GÑU en español, `http://slug.ctv.es/~emelero/`, españolización de los paquetes de GNU coordinado por Enrique Melero.

  `b182@mail.fh-wuerzburg.de`

- Grupo de hispanización de Debian, traducción de documentación y programas, se organiza en la lista `debian-l10n-spanish@lists.debian.org`

7 Anexo: El INSFLUG

El *INSFLUG* forma parte del grupo internacional *Linux Documentation Project*, encargándose de las traducciones al castellano de los Howtos (Comos), así como la producción de documentos originales en aquellos casos en los que no existe análogo en inglés.

En el **INSFLUG** se orienta preferentemente a la traducción de documentos breves, como los *COMOs* y *PUFs* (**P**reguntas de **U**so **F**recuente, las *FAQs*. `:)`), etc.

Diríjase a la sede del INSFLUG para más información al respecto.

En la sede del INSFLUG encontrará siempre las **últimas** versiones de las traducciones: `www.insflug.org`. Asegúrese de comprobar cuál es la última versión disponible en el Insflug antes de bajar un documento de un servidor réplica.

Se proporciona también una lista de los servidores réplica (*mirror*) del Insflug más cercanos a Vd., e información relativa a otros recursos en castellano.

Francisco José Montilla, `pacopepe@insflug.org`.