TEMA Y OBJETIVO GENERAL

FIREWALL CON BALANCEADOR DE DOS ENLACES DE INTERNET

Configurar un Firewall/Gateway, utilizando dos enlaces de Internet, para dar acceso a Internet a sus clientes dentro de una red LAN, y explicar de manera precisa su funcionamiento.

Instalación de aplicaciones

Apache2: Es un servidor Web HTTP de código abierto para plataformas libres y privadas.

Iproute:que sirve en el balanceo asignándole pasos a cada una de las placas existentes dentro de la computadora.

Iptables: Es una herramienta de cortafuego que permite no solamente filtrar paquetes sino también realizar traducción de direcciones de red.

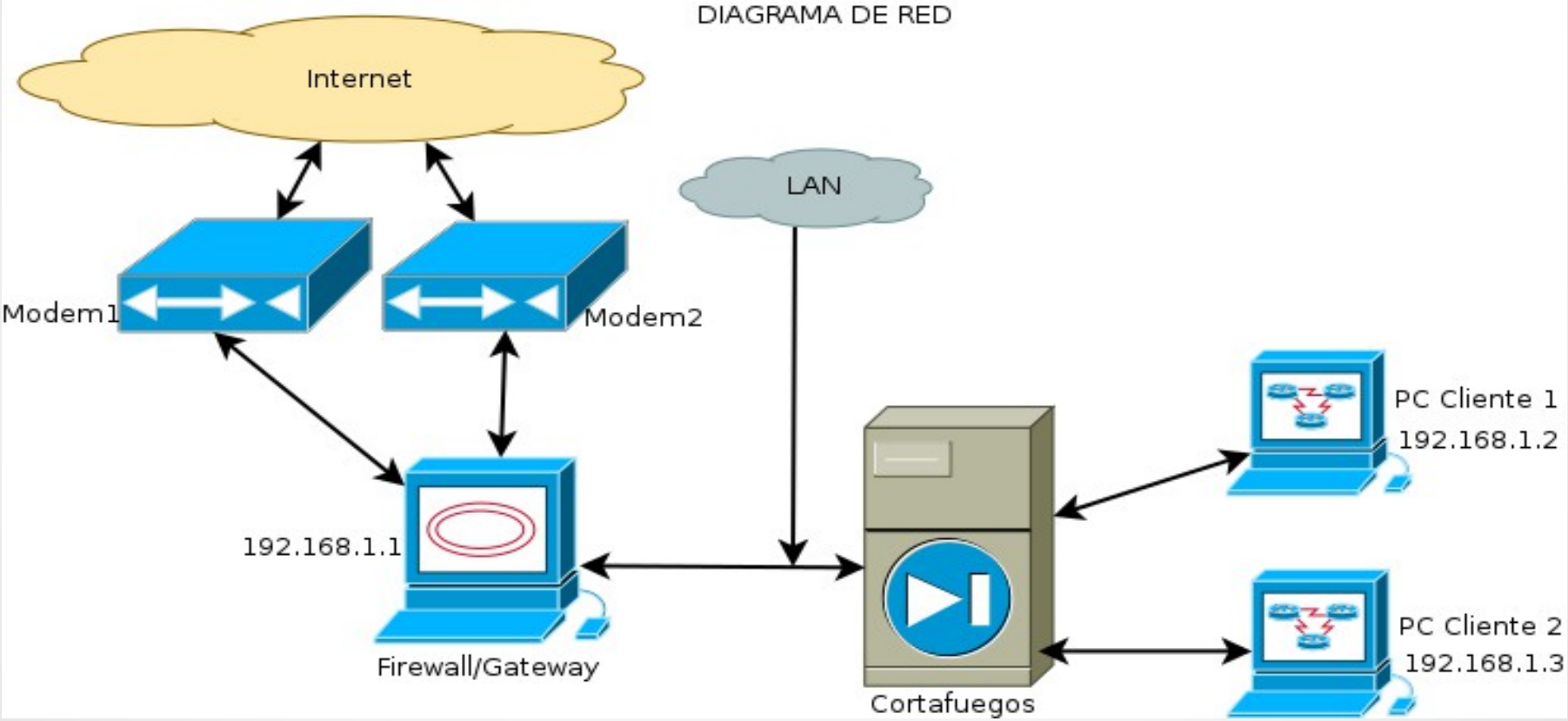
Munin: Es una herramienta escrita en Perl, de monitorización de sistema de red que nos muestra gráficos a través de una interfaz web.

Modems: Es un pequeño dispositivo electrónico que permite a un usuario acceder a internet a través de su PC portatil, cuando no dispone de una conexión a internet o cuando no se encuentra dentro de un zona WiFi.

Esquema de creación de un red LAN

DISPOSITIVO	***INTERFAZ***	***DIRECCIÓN IP***	***MASCARA DE SUBRED***	***PUERTA DE ENLACE***
FIREWALL/ GATEWAY	Eth0	192.168.1.1	255.255.255.0	Ips dinámicas
	ppp0	Ip dinámica	No asignada	No asignada
	ppp1	Ip dinámica	No asignada	No asignada
Pc1	Eth0	192.168.1.2	255.255.255.0	192.168.1.1
Pc2	Eth0	192.168.1.3	255.255.255.0	192.168.1.1

DIAGRAMA DE RED



Configuración de la pc router y pc cliente

nano /proc/sys/net/ipv4/conf/all/forwarding

el 0 se cambia por 1

nano /etc/sysctl.conf

descomentamos net.ipv4.ip_forward=1

/etc/init.d/network-manager stop

Para la interfaz eth0

Ifconfig eth0 192.168.1.1 netmask 255.255.255.0 up

Crea ip el linea de comandos

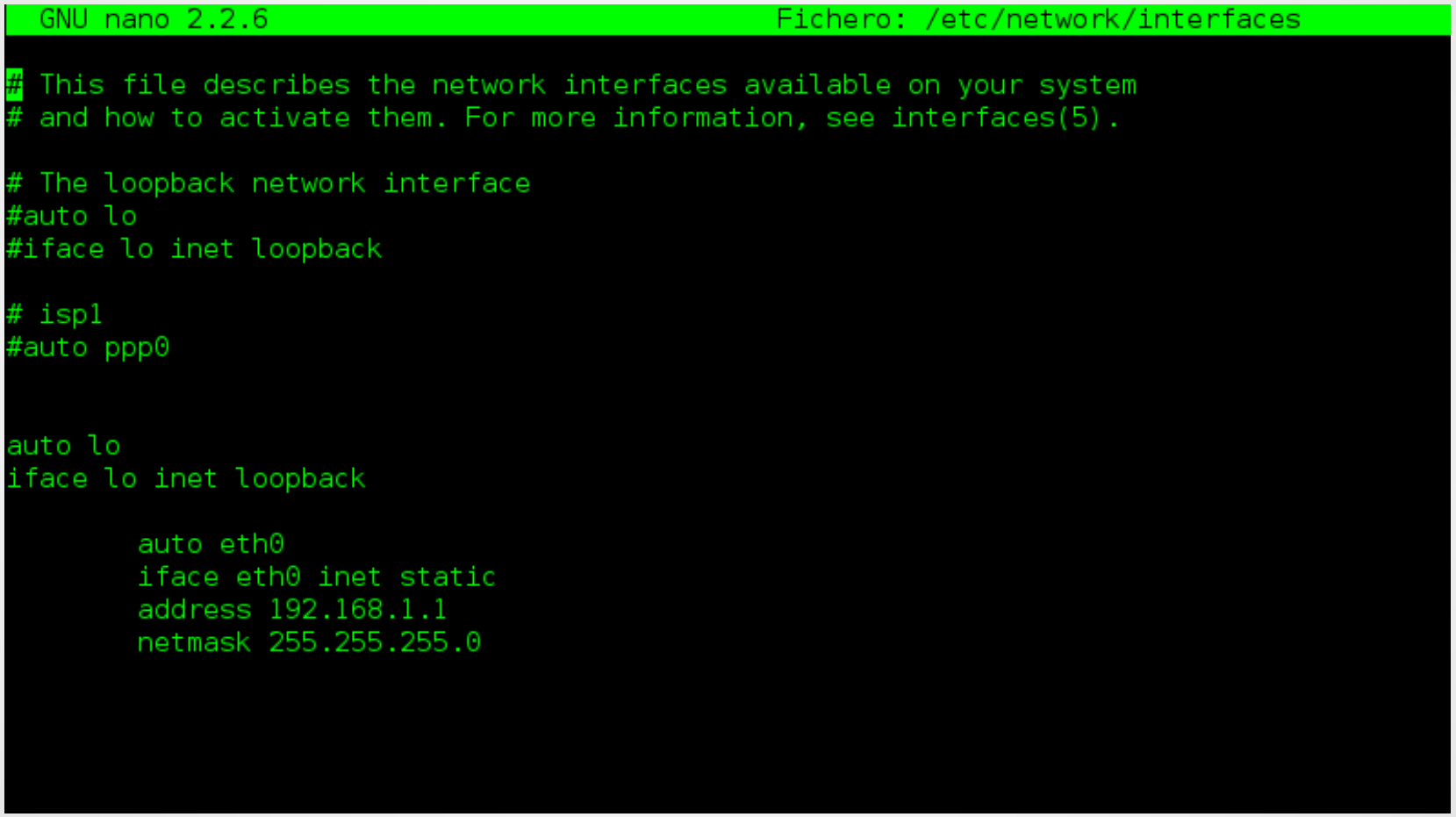
/etc/init.d/network-manager start

Reinicia la interfaza eth0 con la nueva io agregada

Route add default gw 192.168.1.1 eth0

Agrega la puerta de enlace a la ip de red

Crear una red en un fichero atraves de un editor



Interfaces del servidor

```
eth0      Link encap:Ethernet  HWaddr 18:67:b0:32:65:26
          inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::1a67:b0ff:fe32:6526/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:111573 errors:0 dropped:0 overruns:0 frame:0
          TX packets:114969 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:16230290 (15.4 MiB)  TX bytes:76896711 (73.3 MiB)
          Interrupt:40 Base address:0x8000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:26552 errors:0 dropped:0 overruns:0 frame:0
          TX packets:26552 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:4229757 (4.0 MiB)  TX bytes:4229757 (4.0 MiB)

ppp0      Link encap:Point-to-Point Protocol
          inet addr:10.90.100.107  P-t-P:10.64.64.64  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:43 errors:0 dropped:0 overruns:0 frame:0
          TX packets:57 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:3
          RX bytes:9514 (9.2 KiB)  TX bytes:6216 (6.0 KiB)

ppp1      Link encap:Point-to-Point Protocol
          inet addr:10.135.144.174  P-t-P:10.64.64.65  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:8 errors:0 dropped:0 overruns:0 frame:0
          TX packets:9 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:3
          RX bytes:128 (128.0 B)  TX bytes:185 (185.0 B)

root@pablo:/home/pablo#
```

Conexión con la red LAN

```
root@pablo:/home/pablo# ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_req=1 ttl=64 time=0.261 ms
64 bytes from 192.168.1.2: icmp_req=2 ttl=64 time=0.336 ms
^C
--- 192.168.1.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.261/0.298/0.336/0.041 ms
root@pablo:/home/pablo# ping 192.168.1.3
PING 192.168.1.3 (192.168.1.3) 56(84) bytes of data.
64 bytes from 192.168.1.3: icmp_req=1 ttl=64 time=0.277 ms
64 bytes from 192.168.1.3: icmp_req=2 ttl=64 time=0.515 ms
^C
--- 192.168.1.3 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.277/0.396/0.515/0.119 ms
root@pablo:/home/pablo# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_req=1 ttl=64 time=0.114 ms
64 bytes from 192.168.1.1: icmp_req=2 ttl=64 time=0.070 ms
^C
--- 192.168.1.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 0.070/0.092/0.114/0.022 ms
root@pablo:/home/pablo#
```

Conexión con internet

```
root@pablo:/home/pablo# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_req=1 ttl=39 time=131 ms
64 bytes from 8.8.8.8: icmp_req=2 ttl=39 time=200 ms
64 bytes from 8.8.8.8: icmp_req=3 ttl=39 time=2104 ms
64 bytes from 8.8.8.8: icmp_req=4 ttl=39 time=1104 ms
64 bytes from 8.8.8.8: icmp_req=5 ttl=39 time=141 ms
64 bytes from 8.8.8.8: icmp_req=6 ttl=39 time=120 ms
^C
--- 8.8.8.8 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5002ms
rtt min/avg/max/mdev = 120.109/633.858/2104.141/744.943 ms, pipe 3
root@pablo:/home/pablo# ping www.youtube.com
PING youtube-ui.l.google.com (173.194.125.73) 56(84) bytes of data.
64 bytes from mia07s27-in-f9.1e100.net (173.194.125.73): icmp_req=1 ttl=49 time=399 ms
64 bytes from mia07s27-in-f9.1e100.net (173.194.125.73): icmp_req=2 ttl=49 time=399 ms
64 bytes from mia07s27-in-f9.1e100.net (173.194.125.73): icmp_req=3 ttl=49 time=419 ms
^C64 bytes from mia07s27-in-f9.1e100.net (173.194.125.73): icmp_req=4 ttl=49 time=410 ms

--- youtube-ui.l.google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 399.602/407.349/419.625/8.360 ms
```

Protocolos de enrrutamiento

- 1. BGP (Border Gateway Protocol)

  de una sesión de comunicación basada en TCP en el puerto número 179
- 2. IS-IS (Intermediate System - Sistema Intermedio)

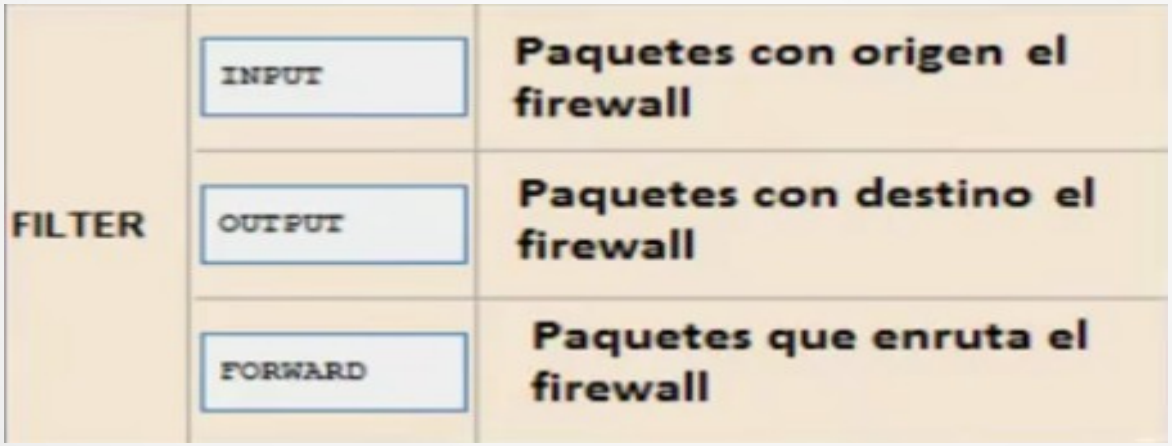
  Protocolo de intercambio enrutador de sistema intermedio a sistema intermedio protocolo 1142
- 3. OSPF (Open Shortest Path First)

  El camino más corto primero
- 4. RIP (Protocolo de Información de Enrutamiento)

  Protocolo de Información de Enrutamiento

Reglas de configuracion de firewall y balanceo de internet

NAT	PREROUTING	DNAT Antes del enrrutamiento
	POSTROUTING	SNAT Posterior al enrrutamiento



Opciones para agregar una nueva regla en terminal o ficheros linux

-A	-append	Agrega una regla a una cadena
-D	-delete	Borra una regla de una cadena espesificada
-R	-replace	Reemplaza una regla
-I	-incert	Incerta una regla en lugar de una cadena
-L	-list	Muestra las reglas que le pasamos como argumento
-F	-flush	Borra todas las reglas de una cadena
-Z	-zero	Pone a cero todos los contadores de una cadena
-N	-new-chain	Permite al usuario crear su propia cadena
-X	-delete-chain	Borra la cadena espesificada
-P	-policy	Explica al kernel que hacer con los paquetesque no coinsidan con una regla
-E	-rename-chain	Cambia el orden de una cadena

Condiciones principales para iptables

-i	Interfaz de entrada (eth0,eth1,eth2...)
-o	Interfaz de salida (eth0,eth1,eth2...)
--sport	Puerto de origen
--dport	Puerto destino
-p	El protocolo del paquete a comprobar, tcp, udp, icmp o all. Por defecto es all
-j	Esto especifica una acción
-s	IP origen
-d	IP destino

Acciones que se dan con la condición -j

ACCEPT	Paquete aceptado
REJECT	Paquete rechazado. Se envía notificación
DROP	Paquete rechazado. Sin notificación
DNAT	Enmascaramiento de la dirección destino
SNAT	Enmascaramiento de la IP origen
MASQUERADE	Enmascaramiento de la dirección IP origen

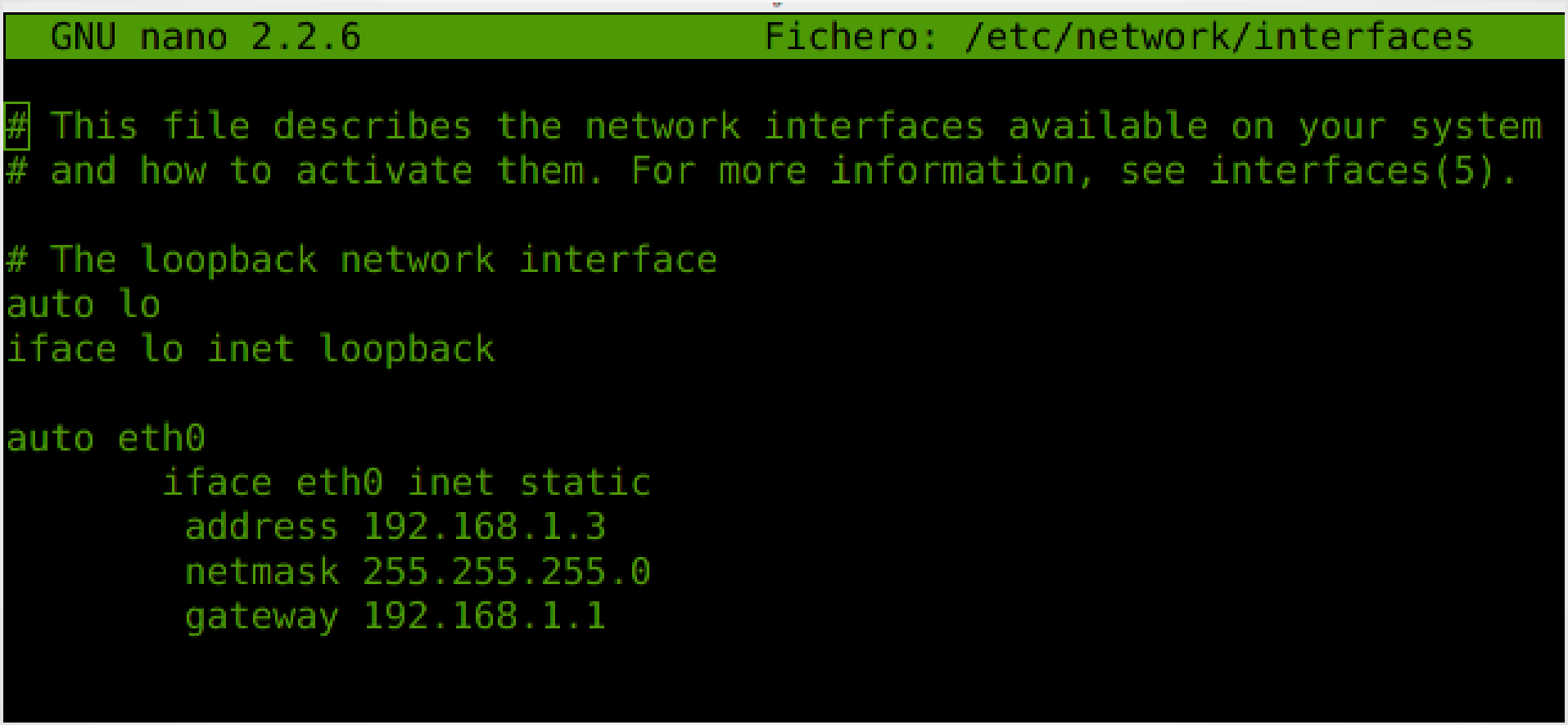
Comandos ejecutables para compartir internet a las pc clientes

```
root@pablo:/home/pablo# iptables --flush
root@pablo:/home/pablo# iptables --table nat --flush
root@pablo:/home/pablo# iptables --table nat --append POSTROUTING --out-interface ppp0 -j MASQUERADE
root@pablo:/home/pablo# iptables --table nat --append POSTROUTING --out-interface ppp1 -j MASQUERADE
root@pablo:/home/pablo# iptables --append FORWARD --in-interface eth0 -j ACCEPT
root@pablo:/home/pablo# ip route del default
root@pablo:/home/pablo#
```

Configuración de maquinas clientes

```
root@arias:/home/arias# /etc/init.d/network-manager stop
[ ok ] Stopping network connection manager: NetworkManager already stopped.
root@arias:/home/arias#  ifconfig eth0 192.168.1.2 netmask 255.255.255.0 up
root@arias:/home/arias# route add default gw 192.168.1.1 eth0
SIOCADDRT: El fichero ya existe
root@arias:/home/arias# /etc/init.d/network-manager start
[ ok ] Starting network connection manager: NetworkManager.
root@arias:/home/arias#
```

Crear interfaz desde fichero linux



Ping a las maquinas dela red LAN

```
root@arias:/home/arias# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_req=1 ttl=64 time=0.462 ms
64 bytes from 192.168.1.1: icmp_req=2 ttl=64 time=0.549 ms
^C
--- 192.168.1.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.462/0.505/0.549/0.048 ms
root@arias:/home/arias# ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_req=1 ttl=64 time=0.841 ms
64 bytes from 192.168.1.2: icmp_req=2 ttl=64 time=0.496 ms
^C
--- 192.168.1.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.496/0.668/0.841/0.174 ms
root@arias:/home/arias#
root@arias:/home/arias# ping 192.168.1.3
PING 192.168.1.3 (192.168.1.3) 56(84) bytes of data.
64 bytes from 192.168.1.3: icmp_req=1 ttl=64 time=0.189 ms
64 bytes from 192.168.1.3: icmp_req=2 ttl=64 time=0.106 ms
64 bytes from 192.168.1.3: icmp_req=3 ttl=64 time=0.127 ms
^C
--- 192.168.1.3 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.106/0.140/0.189/0.037 ms
root@arias:/home/arias#
```

Conexión a internet en PC cliente

```
root@arias:/home/arias# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_req=1 ttl=38 time=1779 ms
64 bytes from 8.8.8.8: icmp_req=3 ttl=38 time=458 ms
64 bytes from 8.8.8.8: icmp_req=4 ttl=38 time=376 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 3 received, 25% packet loss, time 3010ms
rtt min/avg/max/mdev = 376.794/871.521/1779.272/642.742 ms, pipe 2
root@arias:/home/arias# ping www.youtube.com
PING youtube-ui.l.google.com (190.212.166.45) 56(84) bytes of data.
64 bytes from 190.212.166.45: icmp_req=1 ttl=54 time=228 ms
64 bytes from 190.212.166.45: icmp_req=3 ttl=54 time=341 ms
64 bytes from 190.212.166.45: icmp_req=4 ttl=54 time=313 ms
^C^C64 bytes from 190.212.166.45: icmp_req=5 ttl=54 time=332 ms

--- youtube-ui.l.google.com ping statistics ---
5 packets transmitted, 4 received, 20% packet loss, time 26381ms
rtt min/avg/max/mdev = 228.763/304.092/341.036/44.616 ms
root@arias:/home/arias#
```

Balanceo de carga con dos accesos a internet

```
 GNU nano 2.2.6                                  Fichero: enrutamiento.sh

#!/bin/bash
IF1=ppp0
IF2=ppp1
IP1=10.135.98.101
IP2=0.15.5.208
P1=10.64.64.64
P2=10.64.64.65
P1_NET=10.135.98.101
P2_NET=0.15.5.208



echo "ip route add $P1_NET dev $IF1 src $IP1 table 1"
ip route add $P1_NET dev $IF1 src $IP1 table 1
echo "ip route add default via $P1 table 1"
ip route add default via $P1 table 1


echo "ip route add $P2_NET dev $IF2 src $IP2 table 2"
ip route add $P2_NET dev $IF2 src $IP2 table 2
echo "ip route add defaul via $P2 table 2"
ip route add dafaul via $P2 table 2

echo "ip route add $P1_NET dev $IF1 src $IP1"
ip route add $P1_NET dev $IF1 src $IP1

echo "ip route add $P2_NET dev $IF2 src $IP2"
ip route add $P2_NET dev $IF2 src $IP2

echo "ip rule add from $IP1 table T1"
ip rule add from $IP1 table 1

echo "ip rule add from $IP2 table T2" ip rule add from $IP2 table 2


echo "ip route add default scope global nexthop via $P1 dev $IF1 weight 1 nexthop via $P2 dev $IF2 weight 1"
ip route add default scope global nexthop via $IP1 dev $IF1 weight 1 nexthop via $IP2 dev $IF2 weight 1
```

Firewall con iptables para proteger una red LAN de posibles amenazas que vengan de internet y controlar el trafico interno y el tafico a l exterior

```
root@pablo:/media# iptables -F
root@pablo:/media# iptables -A OUTPUT -d 173.252.100.27 -j DROP
root@pablo:/media# iptables -A OUTPUT -o eth0 -d 192.168.1.0/24 -j DROP
root@pablo:/media# iptables -A OUTPUT -d 192.168.1.0/24 -j DROP
root@pablo:/media# clear
```

```
root@pablo:/home/pablo# iptables -F
root@pablo:/home/pablo# iptables -t filter -A OUTPUT -p icmp --icmp-type echo-reply -j DROP
root@pablo:/home/pablo#
```

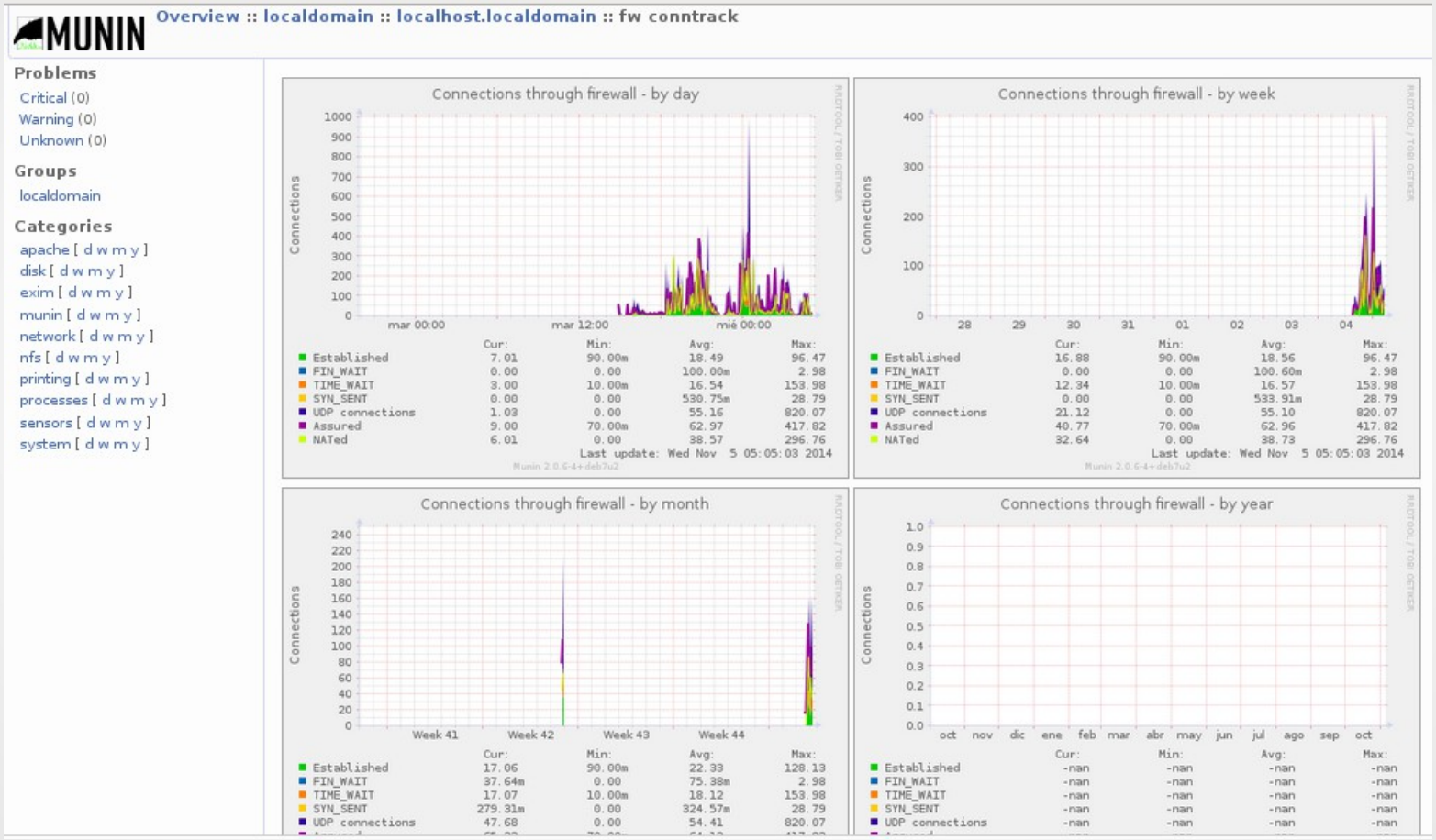
Control de traficos de datos de entrada y salidas

```
root@pablo:/media# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  192.168.1.0/24       anywhere             tcp dpt:https
ACCEPT     tcp  --  anywhere             192.168.1.0/24       tcp spt:https
ACCEPT     udp  --  192.168.1.0/24       anywhere             udp dpt:domain
ACCEPT     udp  --  anywhere             192.168.1.0/24       udp spt:domain
ACCEPT     tcp  --  192.168.1.0/24       anywhere             tcp dpt:domain
ACCEPT     tcp  --  192.168.1.0/24       anywhere             tcp dpts:ftp-data:ftp
ACCEPT     tcp  --  anywhere             192.168.1.0/24       tcp spts:ftp-data:ftp

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@pablo:/media#
```

Control de datos de firewall en munin



GRACIAS POR SU AMABLE ATENCIÓN