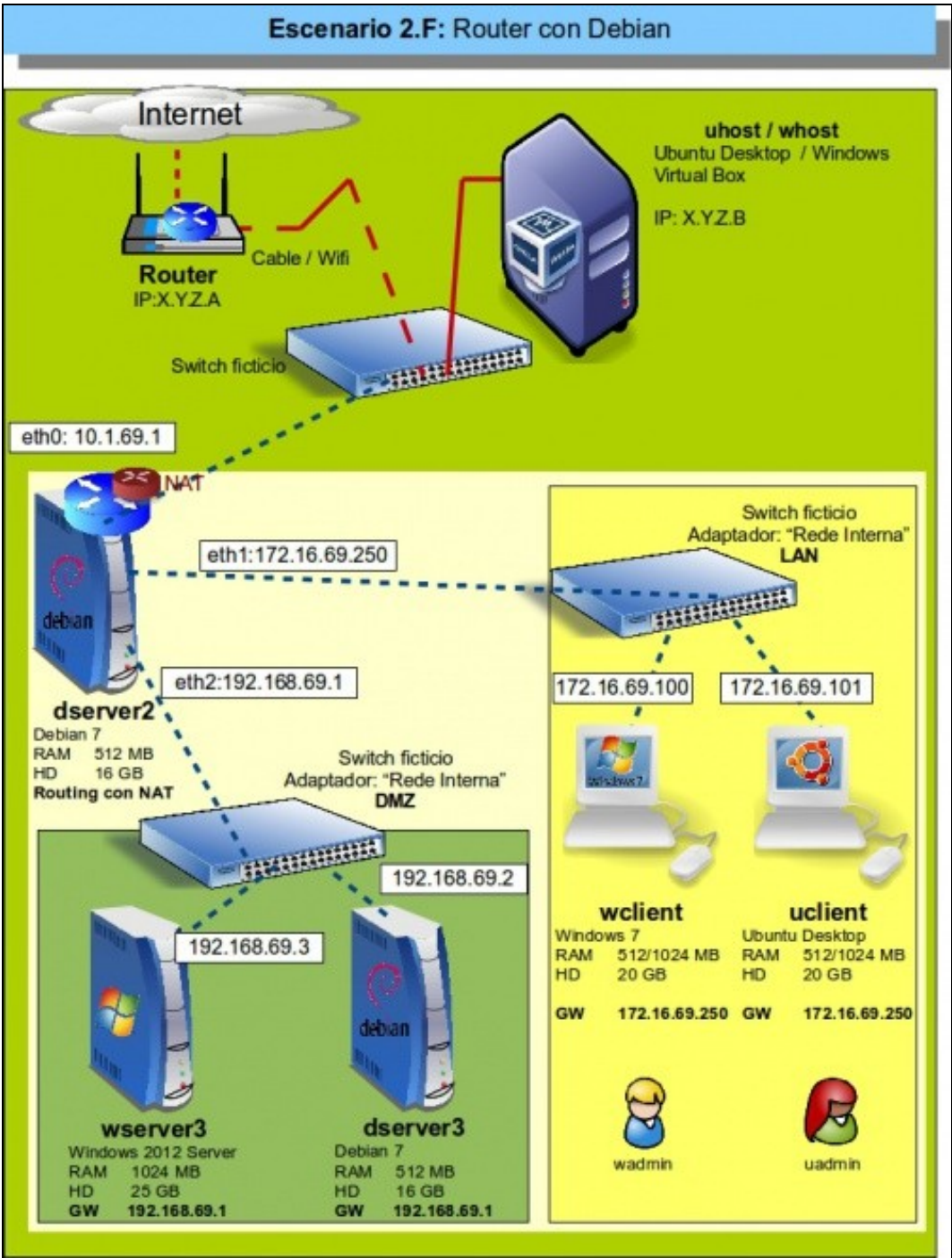
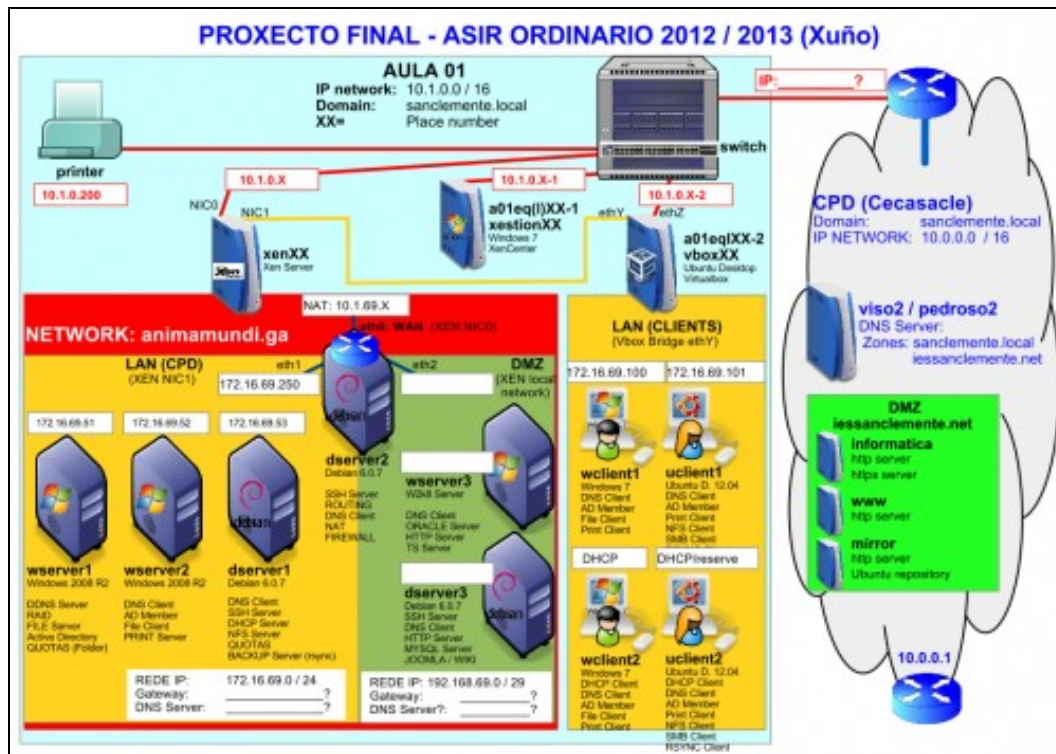


Escenario 2.F: Configuración dun router virtualizado con Debian



O que imos facer neste escenario é virtualizar o servidor *dserver2*, que realiza as funcións de router. Isto vainos permitir aplicar nun caso práctico e entender mellor o funcionamento dos modos de conexión en VirtualBox, xa que este servidor fai unha función similar á que realiza o propio VirtualBox cando nunha máquina conectamos unha tarxeta de rede en modo NAT ou rede NAT.

Este escenario está extraído do seguinte esquema de rede, no que se virtualiza este mesmo servidor sobre Xen Server:



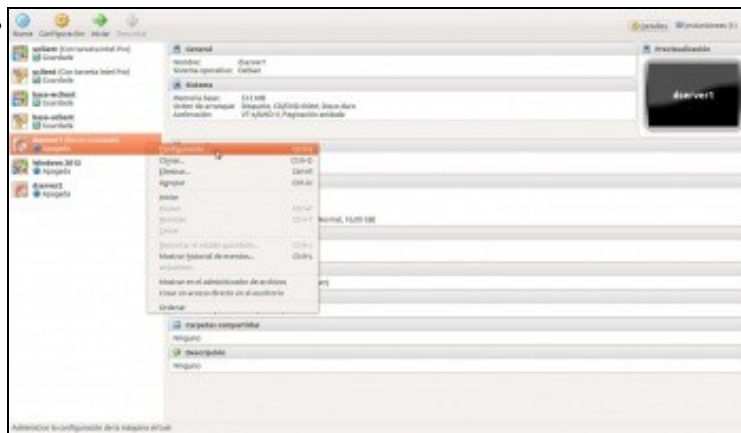
Sumario

- 1 Renomear e agrupar as máquinas do escenario
- 2 Configurar as tarxetas de rede das máquinas
- 3 Instalación de webmin e shorewall en *dserver2*
- 4 Configuración das interfaces de rede
- 5 Activación servizo de ruteo
- 6 Configuración da devasa e activación de NAT
- 7 Reenvío de portos

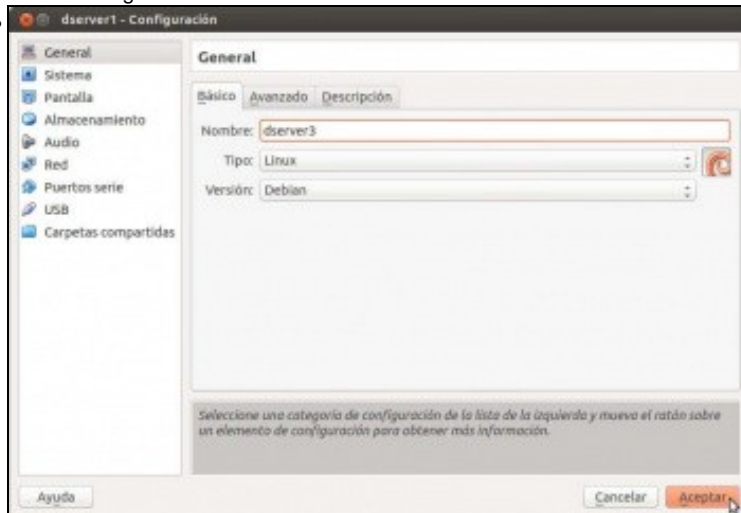
Renomear e agrupar as máquinas do escenario

Facendo uso da funcionalidade de VirtualBox de crear grupos de máquinas, imos agrupar todas as máquinas que van intervir neste escenario para facilitar o seu manexo.

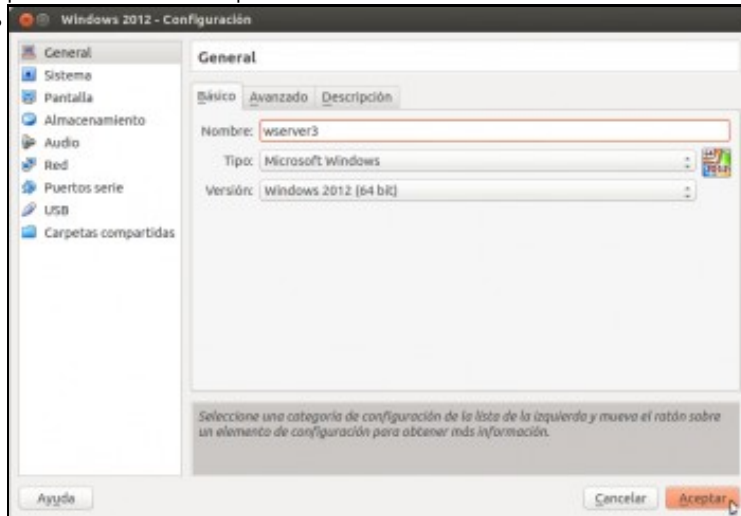
- Renomear e agrupar as máquinas do escenario



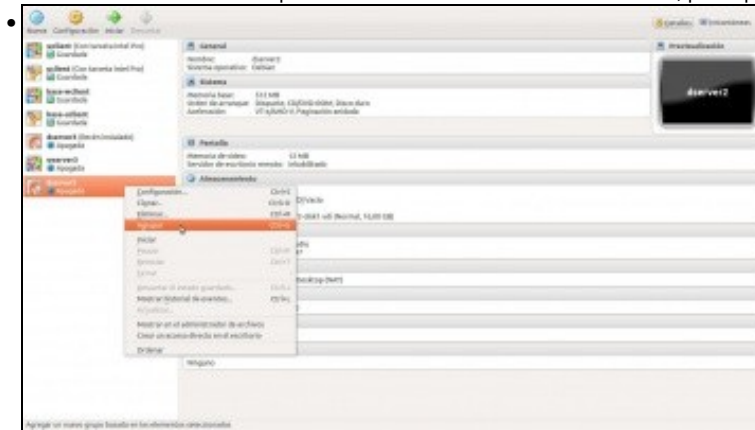
Imos á configuración de *dserver1*...



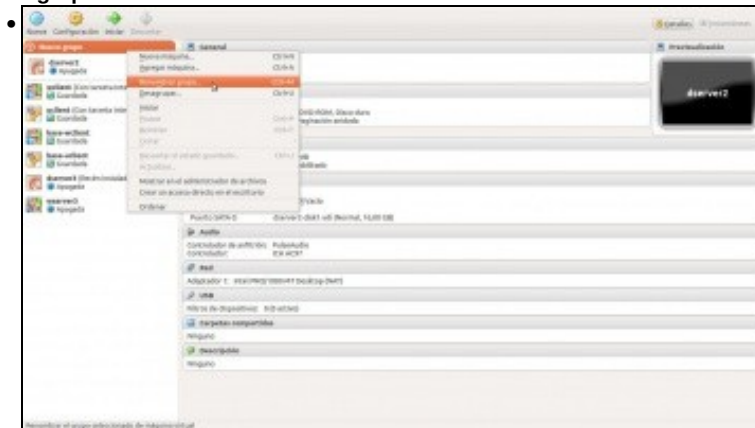
para cambiarle o nome por *dserver3*.



Tamén renomeamos a máquinas de Windows Server como `wserver3`, para que tamén coincida o seu nome co do escenario.



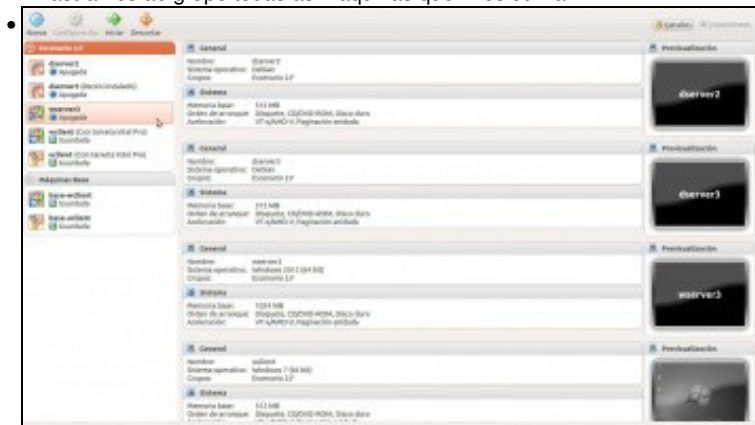
Agora imos agrupar as máquinas que van intervir no escenario. Picamos co botón dereito sobre unha delas e seleccionamos a opción de **Agrupar**.



Renomeamos o grupo, para chamalo **Escenario 2.F**.



Arrastramos ao grupo todas as máquinas que imos utilizar.



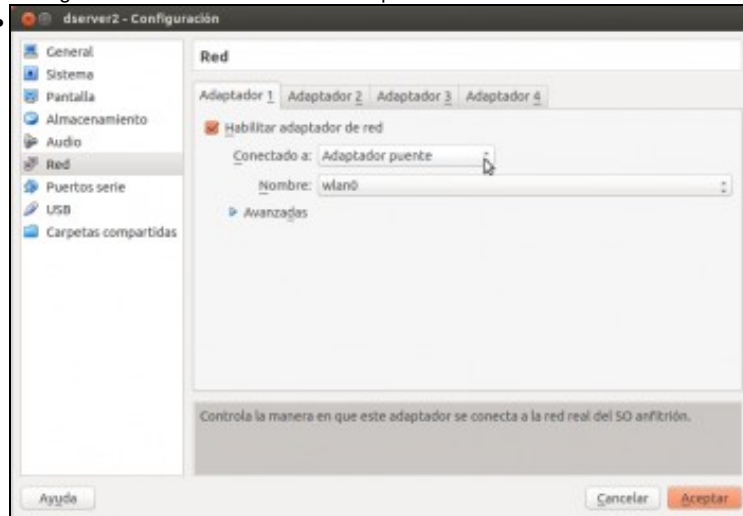
Vista do grupo coas máquinas xa incluídas.

Configurar as tarxetas de rede das máquinas

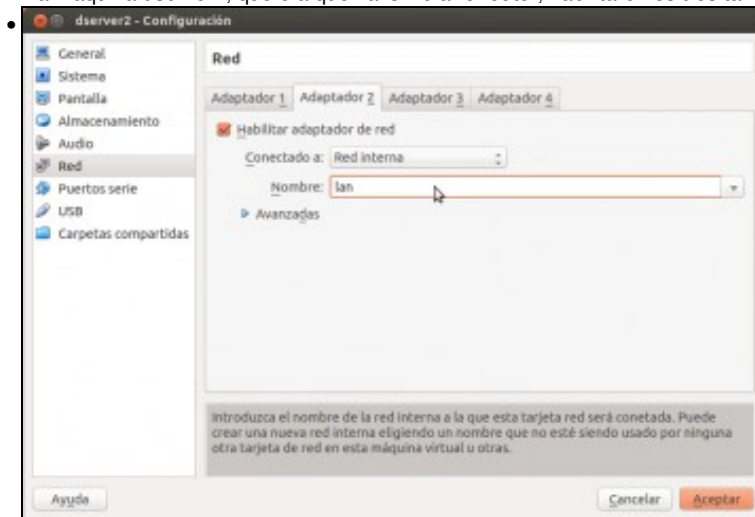
Como segundo paso, imos engadir nas máquinas os adaptadores necesarios e os modos de conexión de cada unha. Se revisamos o escenario, veremos que todos os adaptadores estarán en modo de rede interna excepto o adaptador 1 da máquina *dserver2* que estará en modo ponte.

Agora ben, non todos os adaptadores estarán na mesma rede interna. Dado que queremos simular dúas LANs distintas (a que leva por nome **LAN** e a que leva de nome **DMZ**), imos definir dúas redes internas diferentes, ás que lle poremos ese nome. Desá forma, os adaptadores que están conectados a unha rede interna teñen conexión entre si, pero non terán conexión cos que están conectados a outra rede interna.

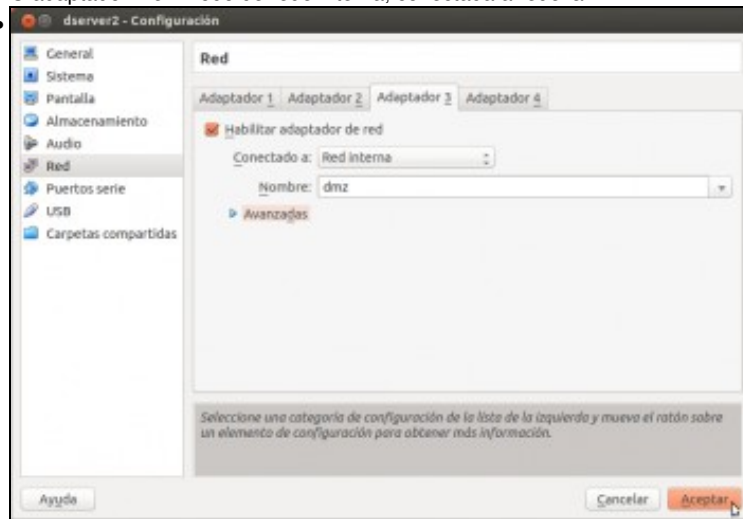
- Configurar as tarxetas de rede das máquinas



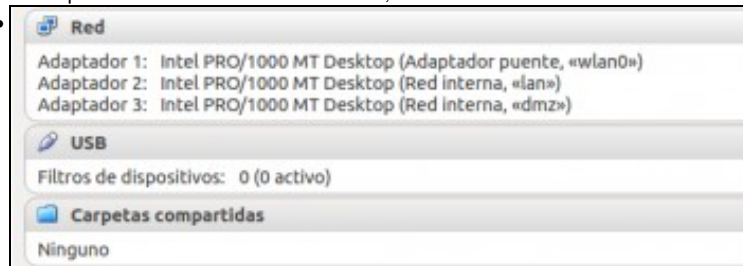
Na máquina *dserver2*, que é a que vai simular o router, habilitaremos tres tarxetas de rede. O adaptador 1 en modo ponte.



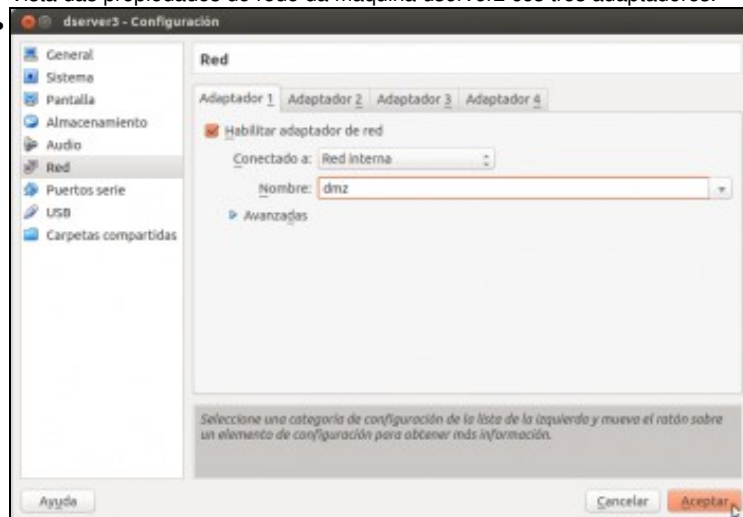
O adaptador 2 en modo de rede interna, conectada á rede *lan*.



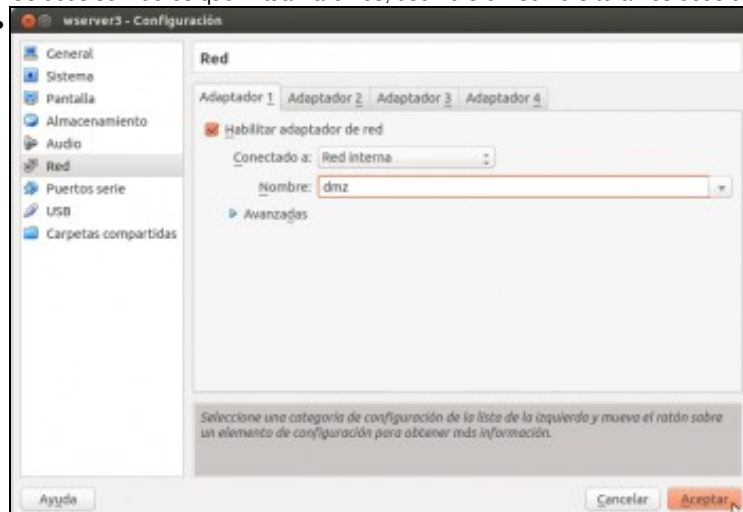
O adaptador 3 en modo de rede interna, conectada á rede *dmz*.



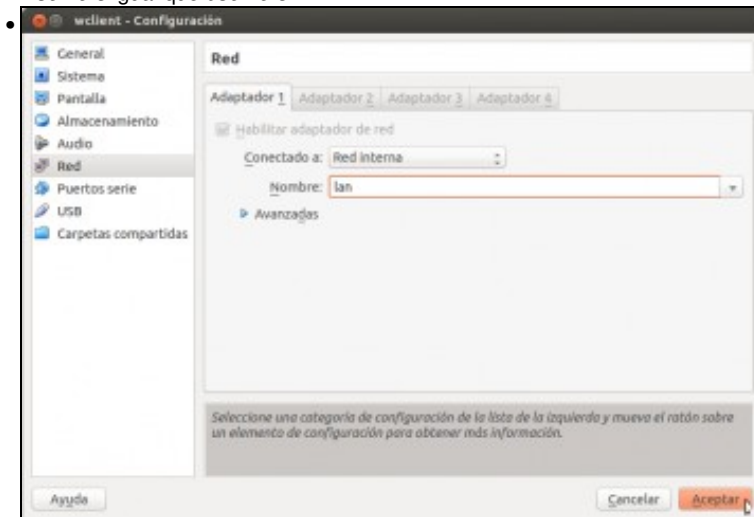
Vista das propiedades de rede da máquina *dserv2* cos tres adaptadores.



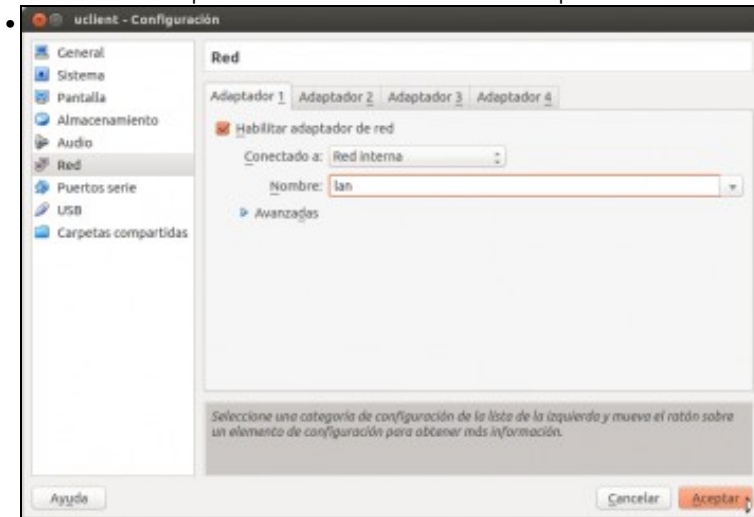
Os dous servidores que virtualizaremos, *dserv3* e *wserv3* terán os dous un adaptador en modo de rede interna, conectados á rede *dmz*.



wserver3 igual que *dserver3*.



Os dous clientes que imos virtualizar tamén terán un adaptador en modo de rede interna, pero neste caso conectados á rede *lan*.



uclient igual que *wclient*.

Instalación de webmin e shorewall en *dserver2*

Imos ver os pasos a seguir para configurar a máquina *dserver2* para que realice as funcións que se reflicten no escenario. O obxectivo deste curso non é afondar na configuración de servizos de rede en Debian, así que intentaremos propoñer unha configuración o máis sinxela posible. Utilizaremos a ferramenta de administración de sistemas GNU/Linux **webmin**, que nos permitirá configurar o servizo de ruteo e devasa da máquina sen ter que manipular directamente os ficheiros de configuración.

Por iso imos instalar en primeiro lugar esta ferramenta na máquina *dserver2*, xunto co módulo **shorewall** que nos permitirá configurar as regras da devasa de forma máis accesible.

- Instalación de webmin e shorewall en *dserver2*

```
dserver2 [Corriendo] - Oracle VM VirtualBox

Debian GNU/Linux 7 dserver tty1
dserver login: root
Password:
Last login: Sat Jan 18 18:01:38 CET 2014 on tty1
Linux dserver 3.2.0-4-amd64 #1 SMP Debian 3.2.51-1 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@dserver:~#
```

Arrancamos a máquina *dserver2* e iniciamos sesión co usuario *root* (contrasinal *abc123*.)

```
root@dserver:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:52:c0:54
          inet addr:10.0.0.11  Bcast:10.255.255.255  Mask:255.0.0.0
          inet6 addr: fe80::a00:27ff:fe52:c054/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:14654 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8337 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:22003999 (20.9 MiB)  TX bytes:559092 (545.9 KiB)

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:8 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:560 (560.0 B)  TX bytes:560 (560.0 B)

root@dserver:~#
```

Co comando **ifconfig** podemos ver a dirección IP que a máquina tomou automaticamente por DHCP na interface que ten conectada en modo ponte. Se non houbo un servidor DHCP na rede, habería que configurar a dirección IP de forma manual. Nun apartado posterior no que se explica a [configuración das interfaces de rede das distintas máquinas do escenario](#) pódense ver os pasos da configuración das interfaces en *dserver3* para ver como facelo.

```
administrador@portatl117:~$ ssh root@10.0.0.11
The authenticity of host '10.0.0.11 (10.0.0.11)' can't be established.
ECDSA key fingerprint is b0:89:c8:09:b7:c6:00:9b:ed:0e:e8:87:2a:87:fa:5a.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.0.11' (ECDSA) to the list of known hosts.
root@10.0.0.11's password:
Linux dserver 3.2.0-4-amd64 #1 SMP Debian 3.2.51-1 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Jan 19 13:25:57 2014
root@dserver:~#
```


Dado que a máquina *dserver2* ten instalado o servidor ssh, agora que sabemos a súa dirección IP podemos conectarnos con un cliente ssh dende o *host* ou outro equipo da rede, xa que isto nos facilitará copiar e pegar os comandos que vaimos introducindo (se o *host* é un equipo Windows podemos utilizar o programa *putty* como cliente ssh).

Olo que nas novas versións de ssh non deixa, por defecto, iniciar sesión co usuario root. Por tanto podemos iniciar sesión co usuario *dadmin* (abc123.) e unha vez no servidor pasarse a root con **su -**. Tamén se pode editar o ficheiro */etc/ssh/sshd-config* tal como se indica en:

<https://debiantalk.wordpress.com/2015/04/27/debian-8-no-root-login-via-ssh/>

```
• dserver [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
GNU nano 2.2.6 Ficheiro: /etc/apt/sources.list Modificado

# deb cdrom:[Debian GNU/Linux 8.6.0 _Jessie_ - Official amd64 DVD Binary-1 2016]
deb cdrom:[Debian GNU/Linux 8.6.0 _Jessie_ - Official amd64 DVD Binary-1 2016]

deb http://ftp.es.debian.org/debian/ jessie main
deb-src http://ftp.es.debian.org/debian/ jessie main

deb http://security.debian.org/ jessie/updates main contrib
deb-src http://security.debian.org/ jessie/updates main contrib

# jessie-updates, previously known as 'volatile'
deb http://ftp.es.debian.org/debian/ jessie-updates main contrib
deb-src http://ftp.es.debian.org/debian/ jessie-updates main contrib

Léronse 15 liñas
Obrir Arquivos Gravar Ler Ficheiro Páxina anterior Cortar Texto Posición
Saír Xustificar alí-lo? Páxina seguinte Reparar Texto Ortografía
Right Ctrl
```

Asegurarse de que están comentadas as sources do CD-ROM (**nano /etc/apt/sources.list**). E actualizar a lista dos paquetes: **apt-get update**

```
• administrador@portatil17: ~
root@dserver:~# wget http://prdownloads.sourceforge.net/webadmin/webmin_1.670_all
1.deb
--2014-01-19 13:30:18-- http://prdownloads.sourceforge.net/webadmin/webmin_1.67
0_all.deb
Resolvendo prdownloads.sourceforge.net (prdownloads.sourceforge.net)... 216.34.1
81.59
Connecting to prdownloads.sourceforge.net (prdownloads.sourceforge.net)[216.34.1
81.59]:80... conectado.
Petición HTTP enviada, agardando unha resposta... 301 Moved Permanently
Lugar: http://downloads.sourceforge.net/project/webadmin/webmin/1.670/webmin_1.6
70_all.deb [seguíndoo]
--2014-01-19 13:30:18-- http://downloads.sourceforge.net/project/webadmin/webmi
n/1.670/webmin_1.670_all.deb
Resolvendo downloads.sourceforge.net (downloads.sourceforge.net)... 216.34.181.5
9
Reusing existing connection to prdownloads.sourceforge.net:80.
Petición HTTP enviada, agardando unha resposta... 302 Found
Lugar: http://netcologne.dl.sourceforge.net/project/webadmin/webmin/1.670/webmin
_1.670_all.deb [seguíndoo]
--2014-01-19 13:30:19-- http://netcologne.dl.sourceforge.net/project/webadmin/w
ebmin/1.670/webmin_1.670_all.deb
Resolvendo netcologne.dl.sourceforge.net (netcologne.dl.sourceforge.net)... 78.3
5.24.46, 2001:4dd0:1234:6::5f
Connecting to netcologne.dl.sourceforge.net (netcologne.dl.sourceforge.net)[78.3
5.24.46]:80... conectado.
Petición HTTP enviada, agardando unha resposta... 200 OK
Longitude: 21758988 (21M) [application/octet-stream]
Saving to: 'webmin_1.670_all.deb'

100%[=====>] 21.758.988 593K/s 1n 39s
```

Descargamos o paquete do webmin para debian, co comando **wget http://prdownloads.sourceforge.net/webadmin/webmin_1.820_all.deb** (Descargaremos e instalaremos a última versión, independentemente da versión que aparece na imaxe)

```
• administrador@portatil17: ~
root@dserver:~# apt-get install libnet-ssleay-perl libauthen-pam-perl libio-pty-perl libapt-pk
g-perl apt-show-versions
A ler as listas de paquetes... Rematado
A construír a árbore de dependencias
A ler a información do estado... Rematado
Os seguintes paquetes NOVOS hanse instalar:
  apt-show-versions libapt-pkg-perl libauthen-pam-perl libio-pty-perl libnet-ssleay-perl
0 actualizados, 5 instalados, 0 hanse eliminar e 0 sen actualizar.
Hai que recibir 414 kB de arquivos.
Despois desta operación hanse ocupar 1699 kB de disco adicionais.
Rcb:1 http://ftp.es.debian.org/debian/ squeeze/main libapt-pkg-perl amd64 0.1.24+b1 [91,5 kB]
Rcb:2 http://ftp.es.debian.org/debian/ squeeze/main apt-show-versions all 0.16+squeeze1 [34,0
kB]
Rcb:3 http://ftp.es.debian.org/debian/ squeeze/main libauthen-pam-perl amd64 0.16-2 [33,0 kB]
Rcb:4 http://ftp.es.debian.org/debian/ squeeze/main libio-pty-perl amd64 1:1.08-1 [42,5 kB]
Rcb:5 http://ftp.es.debian.org/debian/ squeeze/main libnet-ssleay-perl amd64 1.36-1 [213 kB]
Recibíronse 414 kB en 1s (408 kB/s)
```

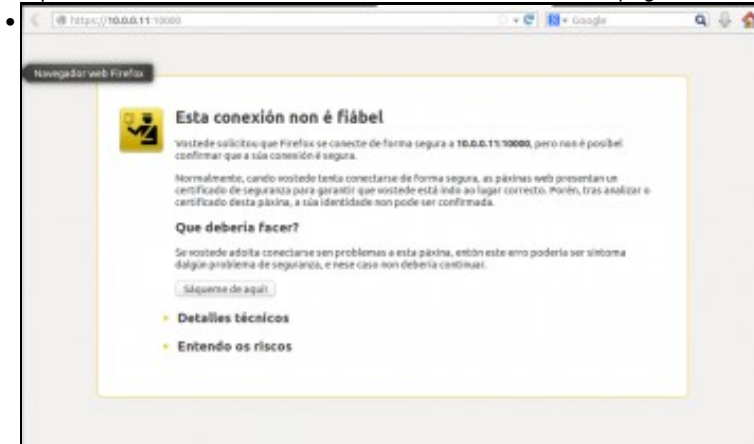
Instalamos unha serie de paquetes necesarios para poder instalar o webmin. Introducimos o comando: `apt-get install libnet-ssleay-perl libauthn-pam-perl libio-pty-perl libapt-pkg-perl apt-show-versions`

```
administrador@portatil17: ~$
root@dserver:~# dpkg -i webmin_1.670_all.deb
Selecting previously unselected package webmin.
(A ler a base de datos ... 25414 files and directories currently installed.)
A desempaquetar webmin (de webmin_1.670_all.deb) ...
```

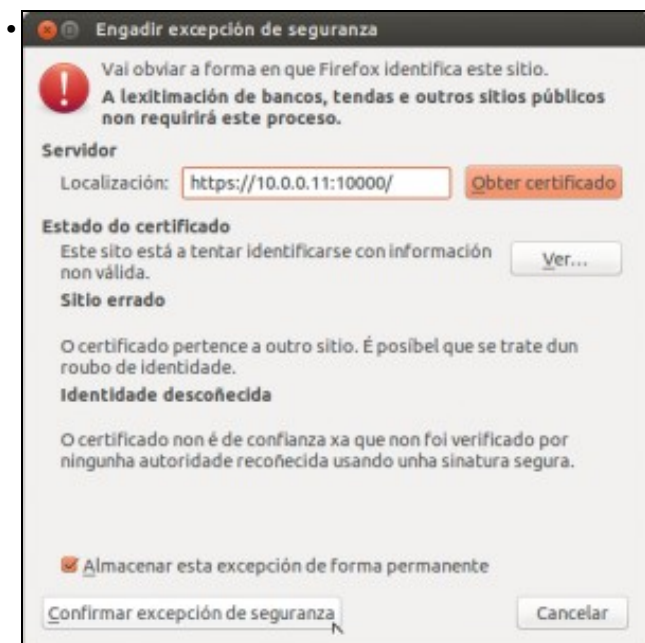
Instalamos o webmin, introducindo o comando `dpkg -i webmin_1.820_all.deb`

```
administrador@portatil17: ~$
root@dserver:~# apt-get install shorewall
Lendo as listas de paquetes... Feito
Construindo a árbore de dependencias
Lendo a información do estado... Feito
Instalaranse os seguintes paquetes extra:
  shorewall-core
Paquetes suxeridos:
  shorewall-doc
Os seguintes paquetes NOVOS hanse instalar:
  shorewall shorewall-core
0 anovados, 2 instalados, Vanse retirar 0 e deixar 0 sen anovar.
Ten que recibir 726 kB de arquivos.
Despois desta operación ocuparanse 1887 kB de disco adicionais.
Quere continuar [S/n]? S
Rcb:1 http://ftp.es.debian.org/debian/ wheezy/main shorewall-core all 4.5.5.3-3 [48,4 kB]
Rcb:2 http://ftp.es.debian.org/debian/ wheezy/main shorewall all 4.5.5.3-3 [670 kB]
Obtivéronse 726 kB en 1s (453 kB/s)
Preconfigurando paquetes ...
Selecting previously unselected package shorewall-core.
(A ler a base de datos ... 49646 files and directories currently installed.)
A desempaquetar shorewall-core (de .../shorewall-core_4.5.5.3-3_all.deb) ...
Selecting previously unselected package shorewall.
A desempaquetar shorewall (de .../shorewall_4.5.5.3-3_all.deb) ...
A procesar os disparadores de man-db ...
A configurar shorewall-core (4.5.5.3-3) ...
A configurar shorewall (4.5.5.3-3) ...
root@dserver:~#
```

E por último, instalamos o shorewall, introducindo o comando `apt-get install shorewall`



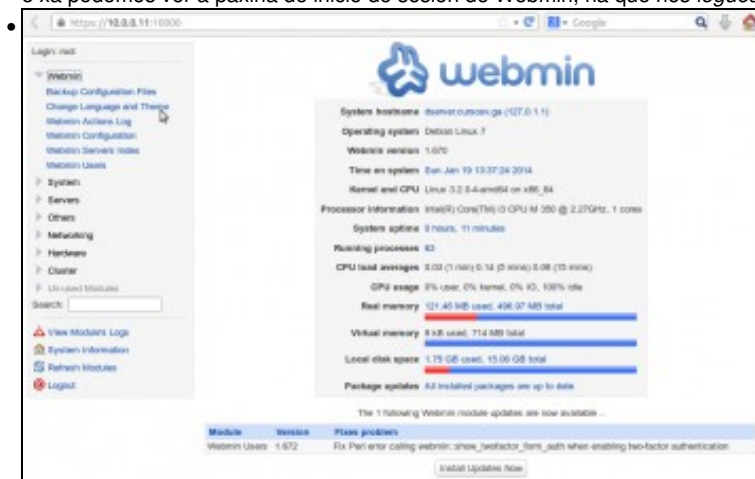
Xa podemos conectarnos ao webmin instalado en *dserver2*. Webmin é un servizo de administración remota que *corre* no porto 10000 e ao que pode accederse con un navegador usando unha conexión segura (*https*). Así que no *host* ou en calquera equipo da rede abrimos un navegador e introducimos como dirección `https://IP_dserver2:10000`. Aparecerá o aviso do navegador debido a que o certificado de seguridade non é fiable, cousa totalmente normal. Engadimos unha excepción...



Confirmamos a excepción...



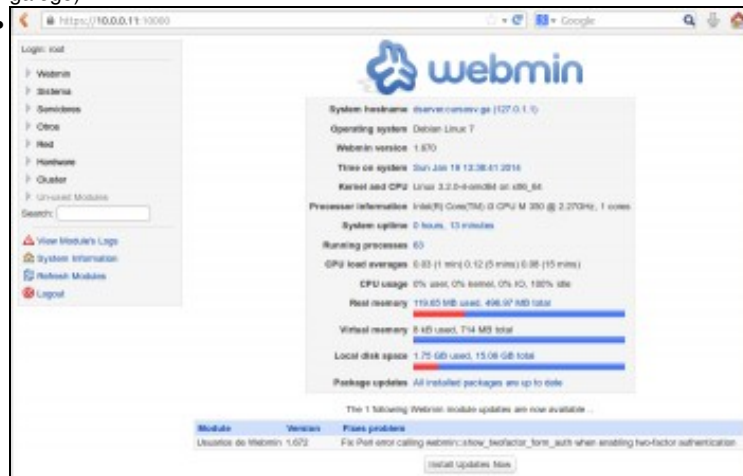
e xa podemos ver a páxina de inicio de sesión de Webmin, na que nos *loguearemos* co usuario *root* e contrasinal *abc123*.



Xa estamos na páxina de inicio de Webmin, e o que podemos facer para deixar a ferramenta personalizada é cambiar o idioma, xa que por defecto ven en Inglés. Picamos dentro da categoría **Webmin** en **Change Language and Theme**.



En **Webmin UI language** activamos **Personal choice** e seleccionamos **Spanish** (desafortunadamente, non contamos con tradución ao galego).



Recargamos a páxina e xa temos dispoñible toda a interface en castelán.

Configuración das interfaces de rede

Neste apartado imos abordar a configuración IP de todas as máquinas virtuais que forman o escenario. Cada unha delas será diferente xa que contamos con unha máquina Windows 7 (*wclient*), unha máquina Ubuntu (*uclient*), unha máquina Windows 2012 Server (*wserver3*) e dúas máquinas debian pero unha delas configuráremola co webmin (*dserver2*) e a outra manipulando directamente os ficheiros de configuración (*dserver3*).

- Configuración das interfaces de rede en *dserver2*



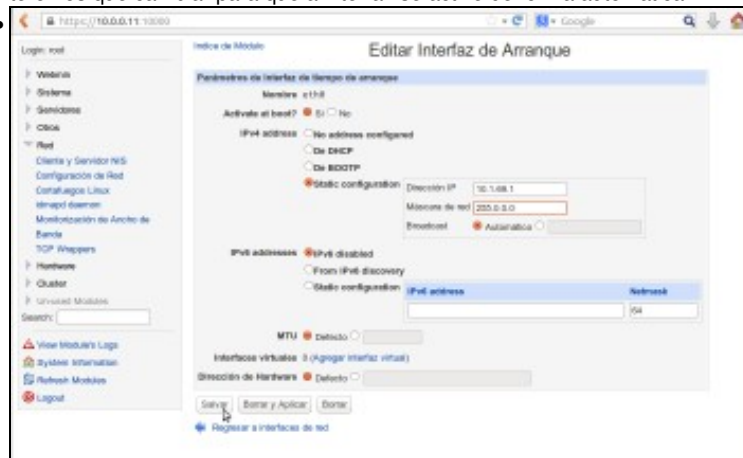
Neste caso imos facer a configuración IP deste equipo mediante o webmin. Dentro do apartado de **Rede**, picamos en **Configuración de Rede**.



Entramos no apartado de **Interfaces de Rede**



É moi importante prestar atención a que esta páxina se divide en dúas pestanas: **Interfaces Activas Agora** e **Interfaces Activadas en Tempo de Arranque**, e sempre teremos que facer os cambios nesta última (que é a que vemos por defecto), xa que senón os cambios non perdurarán cando se reinicie a máquina virtual. Veremos que só hai unha interfaz configurada, *eth0*, por DHCP. Picamos sobre ela para poñerlle a dirección que lle corresponde no escenario. Fixarse antes en que na columna de **Activar ao inicio** pon que non, parámetro que teremos que cambiar para que a interfaz se active de forma automática.



No parámetro **Activate at boot** marcamos que **Si**, e en **IPv4 address** marcamos **Static configuration**. Introducimos a dirección IP e máscara que corresponde segundo o escenario (pero cada quen usará unha dirección IP que pertenza a rede que englobe ao *host*) e salvamos.



Agora imos engadir outra interfaz de rede, xa que no equipo xa existen dúas interfaces máis (pódense ver co comando **ifconfig -a**) que son *eth1* e *eth2*, pero non están configurados. Picamos en **Agregar unha nova interfaz**.

Indice de Módulo

Crear Interfaz de Arranque

Parámetros de interfaz de tiempo de arranque

Nombre

Activar al boot? ☒ Si ☐ No

IPv4 address ☐ No address configured
☐ De DHCP
☐ De BOOTP
☒ Static configuration

Dirección IP
Máscara de red
Broadcast ☒ Automático ☐

IPv6 addresses ☒ IPv6 disabled
☐ From IPv6 discovery
☐ Static configuration

IPv6 address
Netmask

MTU ☒ Defecto ☐

Interfaces virtuales 0 (Agregar interfaz virtual)

Dirección de Hardware ☒ Defecto ☐

[Regresar a interfaces de red](#)

Poñemos como nome da interfaz *eth1*, marcamos que se active no inicio (*Activate at boot->Si*), e marcamos **Static configuration** en **IPv4 address** para introducir a dirección IP e máscara que se indican no escenario (fixarse que estamos usando unha dirección IP de clase B con máscara de clase C xa que estamos definindo subredes). Picamos en **Crear e Aplicar**.

Indice de Módulo

Interfaces de Red

Interfaces Activas Ahora: Interfaces Activadas en Tiempo de Arranque

Interfaces listed in this table will be activated when the system boots up, and will generally be active now too.

Seleccionar todo | Invertir selección | Agregar una nueva interfaz | Add a new bridge

| Nombre | Tipo | Dirección IP | Máscara de red | IPv6 address | ¿Activar al arranque? |
|-------------------------------|----------|-----------------------|----------------|--------------|-----------------------|
| <input type="checkbox"/> eth0 | Ethernet | 10.1.69.1 | 255.0.0.0 | | Si |
| <input type="checkbox"/> eth1 | Ethernet | 172.16.68.250 | 255.255.255.0 | | Si |
| <input type="checkbox"/> lo | Loopback | No address configured | None | | Si |

Seleccionar todo | Invertir selección | Agregar una nueva interfaz | Add a new bridge

[Regresar a configuración de red](#)

E o mesmo imos facer con *eth2*. Picamos en **Agregar unha interfaz**.

Indice de Módulo

Crear Interfaz de Arranque

Parámetros de interfaz de tiempo de arranque

Nombre

Activar al boot? ☒ Si ☐ No

IPv4 address ☐ No address configured
☐ De DHCP
☐ De BOOTP
☒ Static configuration

Dirección IP
Máscara de red
Broadcast ☒ Automático ☐

IPv6 addresses ☒ IPv6 disabled
☐ From IPv6 discovery
☐ Static configuration

IPv6 address
Netmask


MTU ☒ Defecto ☐

Interfaces virtuales 0 (Agregar interfaz virtual)

Dirección de Hardware ☒ Defecto ☐

[Regresar a interfaces de red](#)

Introducimos os datos da interfaz segundo o escenario (de novo estamos facendo subredes na rede de clase C). Picamos en **Crear y Aplicar**.

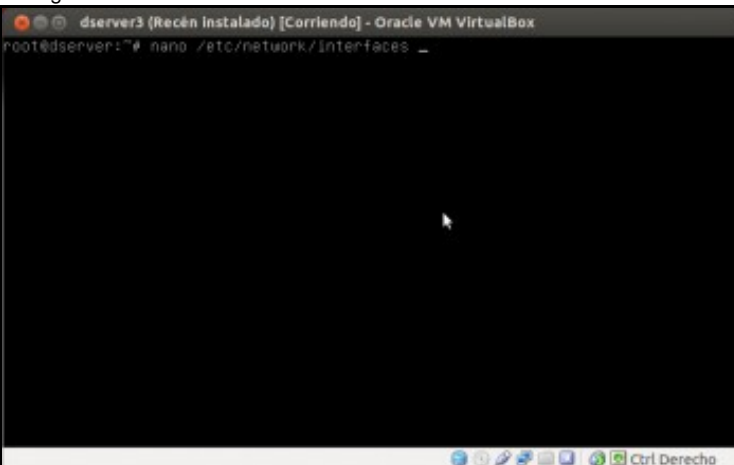
- 

Seleccionamos a interfaz *eth0*, que é o único cambio que aínda non está aplicado, e picamos no botón de **Apply Selected Interfaces**. Neste momento o webmin deixará de responder, xa que acabamos de cambiar a dirección IP da interfaz pola que nós nos estabamos conectado co navegador (era 10.0.0.11 e pasa a ser 10.1.69.1). Así que teremos que cambiar a dirección do navegador para poñer <https://10.1.69.1:10000>

- 

E xa debemos ter acceso ao webmin.

- Configuración das interfaces de rede en *dserver3*

- 

Neste caso, na máquina non temos o webmin instalado, así que imos facer a configuración IP da súa interfaz directamente nos ficheiros de configuración. O ficheiro de configuración básico das interfaces de rede en Debian é `/etc/network/interfaces`, así que imos editar este ficheiro co editor *nano*.

```
dserver3 (Recén instalado) [Corriendo] - Oracle VM VirtualBox
GNU nano 2.2.4 Ficheiro: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug eth0
iface eth0 inet dhcp
```

Contido inicial do ficheiro, onde podemos ver que a interfaz `eth0` está configurada por DHCP.

```
dserver3 (Recén instalado) [Corriendo] - Oracle VM VirtualBox
GNU nano 2.2.4 Ficheiro: /etc/network/interfaces Modificado

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug eth0
iface eth0 inet static
    address 192.168.69.2
    netmask 255.255.255.248
    gateway 192.168.69.1
```

Na imaxe vese o contido que imos deixar no ficheiro, engadindo a interfaz na liña **auto...** para que se active automaticamente e establecendo unha configuración IP estática, cos datos de dirección e máscara indicados no escenario. A porta de enlace predeterminada (*gateway*) para este equipo será a dirección IP da interfaz `eth2` de *dserver2*. É moi importante revisar ben a sintaxe de todo o que se introduciu no ficheiro para que a configuración se aplique correctamente.

```
dserver3 (Recén instalado) [Corriendo] - Oracle VM VirtualBox
root@dserver:~# nano /etc/resolv.conf
```

Só nos falta indicar os servidores de DNS, que se introducen no ficheiro `/etc/resolv.conf`. Editamos este ficheiro....

```
dserver3 (Recén instalado) [Corriendo] - Oracle VM VirtualBox
GNU nano 2.2.4      Ficheiro: /etc/resolv.conf      Modificado

nameserver 80.50.61.250
nameserver 80.50.61.254

root@dserver3:~#

$Glibc-2.10 buffer modificado (SE RESPONDA "Non" PERDERANSE OS CAMBIOS)?
S: Si
N: Non
Ctrl Derecho
```

E introducimos os servidores de DNS, que serán os que teña configurado o equipo *host*. Cada quen debe introducir os do seu equipo.

```
dserver3 (Recén instalado) [Corriendo] - Oracle VM VirtualBox
root@dserver3:~# /etc/init.d/networking stop
Deconfiguring network interfaces...done.
root@dserver3:~# /etc/init.d/networking start
Configuring network interfaces...done.
root@dserver3:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:52:c0:54
          inet addr:192.168.69.2  Bcast:192.168.69.7  Mask:255.255.255.248
          inet6 addr: fe80::a00:27ff:fe52:c054/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:19 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:3330 (3.2 KiB)

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:8 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:560 (560.0 B)  TX bytes:560 (560.0 B)

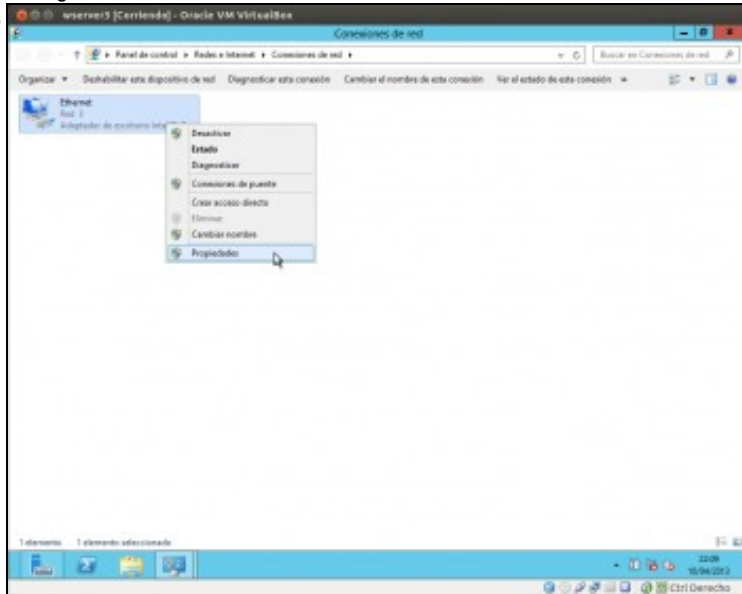
root@dserver3:~#
```

Detemos e iniciamos o servizo de rede cos comandos `/etc/init.d/networking stop` e `/etc/init.d/networking start`. Convén comprobar co comando `ifconfig` que a configuración se aplicou correctamente.

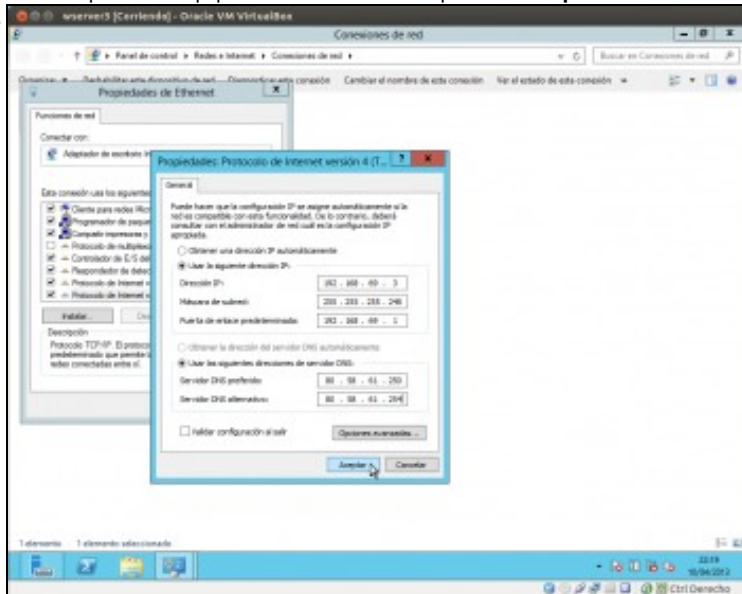
```
dserver3 (Recén instalado) [Corriendo] - Oracle VM VirtualBox
root@dserver3:~# ping 192.168.69.1
PING 192.168.69.1 (192.168.69.1) 56(84) bytes of data:
64 bytes from 192.168.69.1: icmp_req=1 ttl=64 time=4.39 ms
64 bytes from 192.168.69.1: icmp_req=2 ttl=64 time=0.886 ms
^C
--- 192.168.69.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1008ms
rtt min/avg/max/mdev = 0.886/2.640/4.395/1.755 ms
root@dserver3:~#
```

Tamén imos comprobar que temos conectividade co equipo *dserver2*. É normal que non teñamos conexión co *host* nin a Internet, xa que *dserver2* non está facendo as funcións de ruteo e NAT.

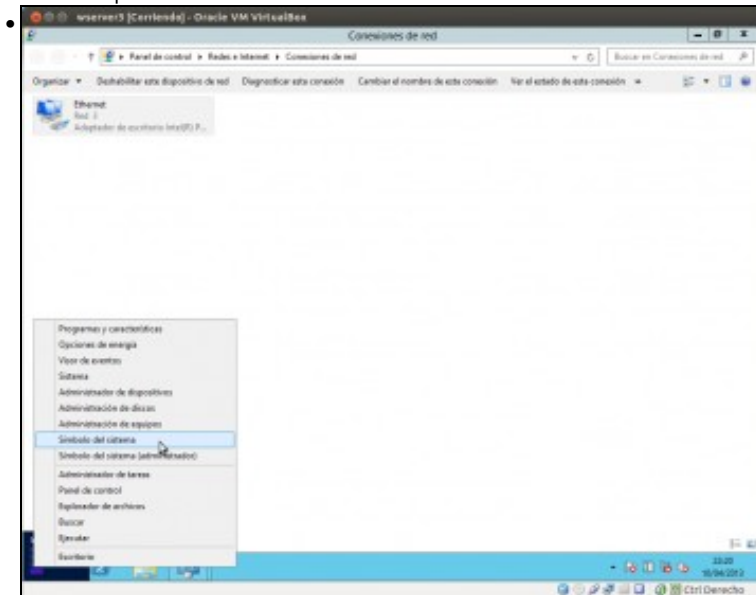
- Configuración das interfaces de rede en *wserver3*



Neste caso a configuración é similar a que temos feito en apartados anteriores sobre *wclient*. Na lista de adaptadores de rede, picamos sobre o único que ten o equipo e seleccionamos a opción de **Propiedades**.



Facemos dobre clic sobre o **Protocolo de Internet (TCP/IP) versión 4** e introducimos na ventá os datos de dirección IP e máscara que se indican no escenario. A porta de enlace predeterminada será de novo a dirección IP da interfaz *eth2* de *dserver2*, e os servidores DNS os mesmos que o *host*.

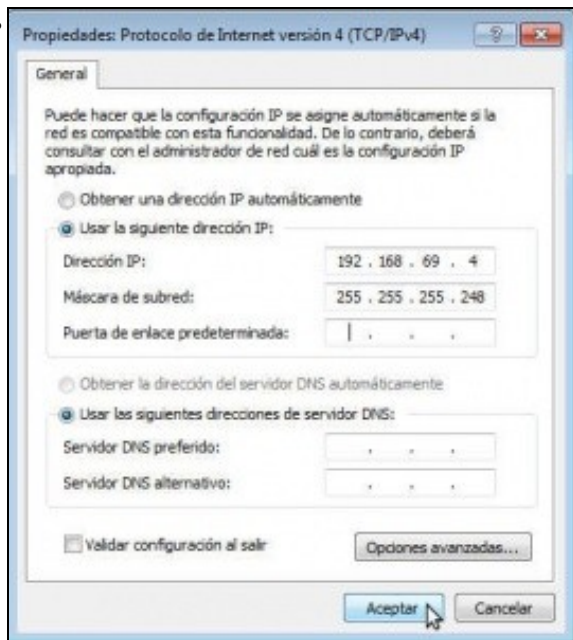


Abrimos unha ventá de **Símbolo do sistema** para facer un *ping* e comprobar a conectividade con *dserver2* e *dserver3*

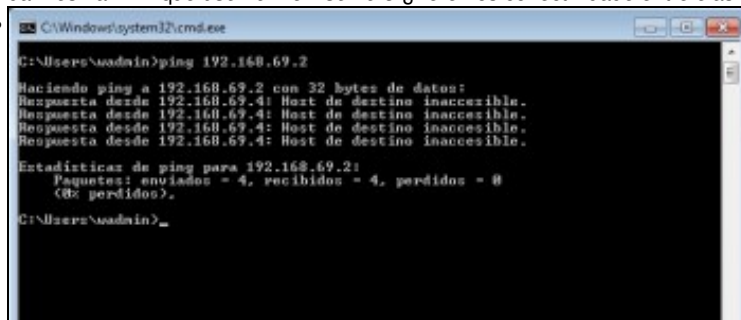


Perfecto!!

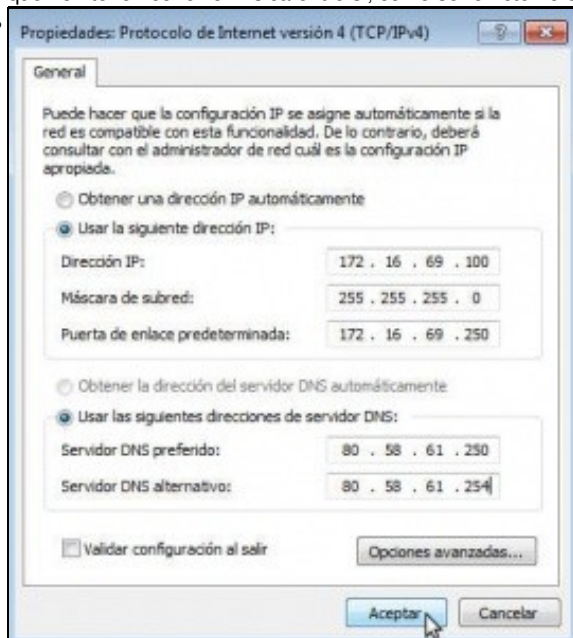
- Configuración das interfaces de rede en *wclient*



Neste caso, para comprender mellor o funcionamento da rede interna en VirtualBox, imos poñerlle á interfaz antes unha dirección IP dentro da mesma LAN que *dserver2* e *wserver3* ¿Teremos conectividade entre elas???



A resposta é que non, porque aínda que todas as interfaces destas máquinas están en modo de rede interna, están conectadas a redes internas diferentes (a de esta máquina á rede *lan* e as das outras dúas á rede *dmz*), así que están conectados a *switchs ficticios* distintos e que non teñen conexión física entre si, como se reflicte no escenario.



Agora si poñemos os datos que se corresponden co escenario,

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\vaadin>ping 172.16.69.250

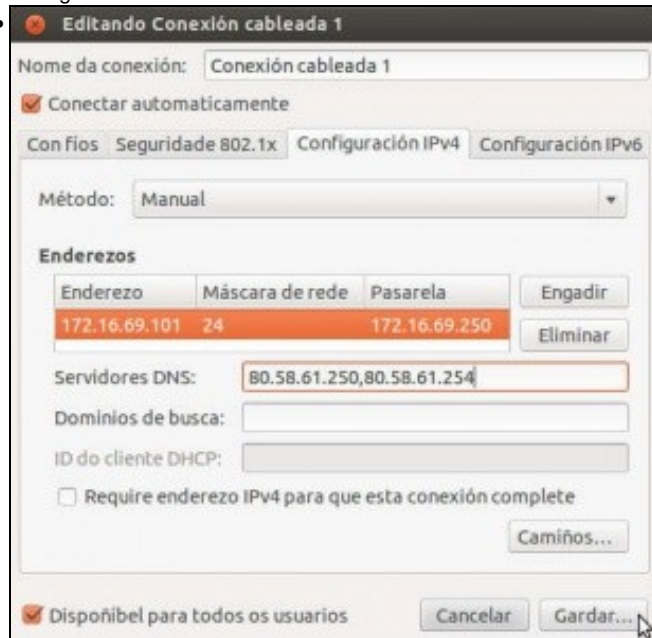
Haciendo ping a 172.16.69.250 con 32 bytes de datos:
Respuesta desde 172.16.69.250: bytes=32 tiempo<1m TTL=64
Respuesta desde 172.16.69.250: bytes=32 tiempo<1m TTL=64
Respuesta desde 172.16.69.250: bytes=32 tiempo<1m TTL=64
Respuesta desde 172.16.69.250: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 172.16.69.250:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
            (0% perdidos):
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 3ms, Media = 0ms

C:\Users\vaadin>_
```

e temos conexión coa interfaz *eth1* de *dserver2*, xa que esa interfaz si que está en modo de rede interna e conectada á rede *lan*.

- Configuración das interfaces de rede en *uclient*



E por últimao introducimos a configuración IP para este equipo segundo os datos do escenario. Gardamos os cambios,

```
administrador@uclient: ~
administrador@uclient:~$ ping 172.16.69.100
PING 172.16.69.100 (172.16.69.100) 56(84) bytes of data:
64 bytes from 172.16.69.100: icmp_req=1 ttl=128 time=0.718 ms
64 bytes from 172.16.69.100: icmp_req=2 ttl=128 time=1.86 ms
^C
--- 172.16.69.100 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.718/1.293/1.868/0.575 ms
administrador@uclient:~$ ping 172.16.69.250
PING 172.16.69.250 (172.16.69.250) 56(84) bytes of data:
64 bytes from 172.16.69.250: icmp_req=1 ttl=64 time=0.556 ms
64 bytes from 172.16.69.250: icmp_req=2 ttl=64 time=0.985 ms
^C
--- 172.16.69.250 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.556/0.770/0.985/0.216 ms
administrador@uclient:~$
```

e podemos comprobar que temos conectividade co equipo *wclient* e *dserver2*. Perfecto!!

```
administrador@wclient: ~
administrador@wclient:~$ ping 192.168.69.2
PING 192.168.69.2 (192.168.69.2) 56(84) bytes of data:
^C
--- 192.168.69.2 ping statistics ---
13 packets transmitted, 0 received, 100% packet loss, time 11999ms
administrador@wclient:~$
```

Pero non temos conectividade cos equipos que están na rede *dmz*, xa que *dserver2* non ten activado o servizo de ruteo e polo tanto non reenvía os paquetes que esta máquina lle está mandando ao seu destino. Imos ver como podemos solucionalo...

Activación servizo de ruteo

Utilizando o webmin, imos activar o servizo de enrutamento na máquina *dserver2* para poder ter conexión entre as máquinas que están nas dúas redes (*lan* e *dmz*):

- Activar o servizo de ruteo na MV Debian



Dentro da ferramenta de **Configuración de Rede**, picamos na opción de **Ruteo e gateways**.



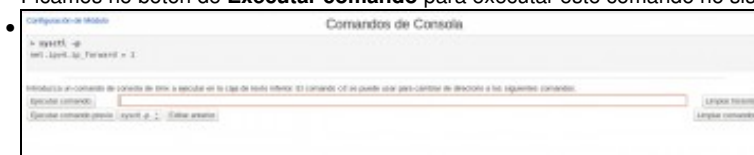
Establecemos como porta de enlace predeterminada (*Router por defecto*) para este equipo a mesma que estea usando o equipo *host* para conectarse a Internet. Neste caso, 10.0.0.1. Na opción de **¿Actuar como router?** indicamos que si.



Picamos no botón de **Aplicar configuración**, pero neste caso (bug do webmin) con isto non conseguimos realmente activar xa o servizo de ruteo na máquina. Se reiniciásemos a máquina virtual xa se activaría, pero imos ver como podemos activar o cambio sen ter que reiniciar.



No propio webmin, imos á ferramenta de **Comandos de consola** (dentro do apartado de **Otros**) e introducimos o comando: **sysctl -p**. Picamos no botón de **Executar comando** para executar este comando no sistema.



Vemos o resultado do comando, que xa activa o enrutamento.

```
administrador@uclient: ~
administrador@uclient:~$ ping 192.168.69.2
PING 192.168.69.2 (192.168.69.2) 56(84) bytes of data.
64 bytes from 192.168.69.2: icmp_req=1 ttl=63 time=14.3 ms
64 bytes from 192.168.69.2: icmp_req=2 ttl=63 time=8.99 ms
64 bytes from 192.168.69.2: icmp_req=3 ttl=63 time=6.54 ms
^C
--- 192.168.69.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 6.542/9.975/14.390/3.280 ms
administrador@uclient:~$
```

Agora podemos comprobar que dende *uclient* podemos acceder a *dserver3*. Ben!!

```
administrador@uclient: ~
administrador@uclient:~$ ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
^C
--- 10.0.0.1 ping statistics ---
23 packets transmitted, 0 received, 100% packet loss, time 22126ms

administrador@uclient:~$
```

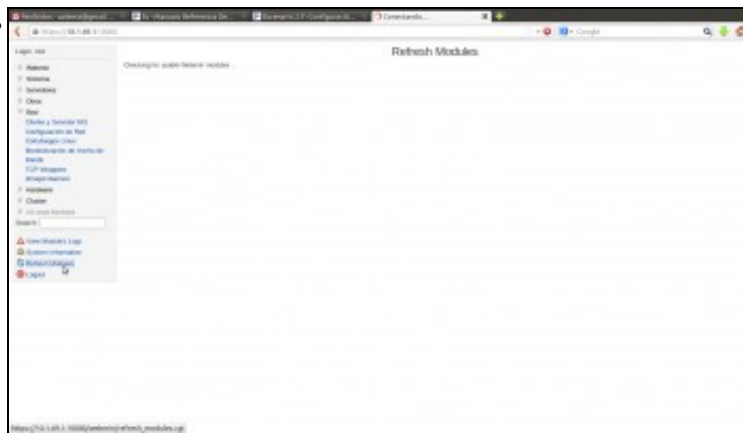
Pero... ¿podemos acceder a un equipo da rede real (o router de saída a Internet, por exemplo)?... Non... ¿Por que? Porque *dserver2* non está facendo a función de NAT, e polo tanto un equipo como *uclient* que ten unha dirección IP privada non pode acceder a unha rede pública (aínda que a rede 10 sexa unha rede privada, neste caso para os equipos que están nas redes *lan* e *dmz*, é como se fose pública. Revisar a teoría sobre NAT). O mesmo pasará co resto das máquinas que están nas redes *lan* e *dmz*.

```
dserver3 (Recén instalado) [Corriendo] - Oracle VM VirtualBox
root@dserver:~# ping 172.16.69.101
PING 172.16.69.101 (172.16.69.101) 56(84) bytes of data.
64 bytes from 172.16.69.101: icmp_req=1 ttl=63 time=2.67 ms
64 bytes from 172.16.69.101: icmp_req=2 ttl=63 time=1.37 ms
64 bytes from 172.16.69.101: icmp_req=3 ttl=63 time=1.25 ms
64 bytes from 172.16.69.101: icmp_req=4 ttl=63 time=1.40 ms
^C
--- 172.16.69.101 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.257/1.678/2.677/0.579 ms
root@dserver:~#
```

E aínda temos outro problema... Dende o equipo *dserver3* podemos acceder ao equipo *uclient* ¿Debe ser así? Seguindo as regras da devasa, suponse que non se deberían permitir conexións que intenten entrar na rede interna, xa que é a rede que queremos protexer do exterior. A única rede accesible dende o exterior debería ser en todo caso a *zona desmilitarizada* ou *dmz*, que é na que se atopan equipos que prestan servizos accesibles dende Internet (chamados comunmente *bastións*). Imos agora a resolver todo isto...

Configuración da devasa e activación de NAT

Para resolver as dúas problemáticas que acabamos de detectar no apartado anterior, imos configurar a devasa no equipo *dserver2* e activar a función de NAT. Utilizaremos para iso o módulo de *shorewall* de webmin, que nos facilitará a configuración de *iptables*, que é o módulo de Linux que xestiona as regras da devasa.



De momento o módulo de *Shorewall* non aparece en ningunha das categorías do webmin, xa que foi instalado despois. Picamos na opción de **Refresh Modules** para que webmin busque se ten novos módulos instalados e os engada na categoría correspondente.



Atoparemos agora dentro da categoría de *Rede* o módulo de **Cortafuegos Shoreline**. Entramos nel. De momento o módulo está parado (fixarse en que temos o botón de *Iniciar el Cortafuegos*), pero se intentamos inicialo veremos que nos da un erro, debido a que é necesario establecer unha configuración básica para poderlo facer.



En primeiro lugar, teremos que definir as zonas de rede que vai xestionar a devasa, que non son máis que nomes lóxicos para as distintas redes ás que se conecta. Picamos en **Zonas de rede**.



Vemos que non hai ningunha zona definida. Picamos en **Agregar unha nova zona de rede**.



Poñemos un ID da zona (*lan*), seleccionamos como tipo *IPv4* e picamos no botón de **Crear**. Esta zona representa a conexión coa rede *lan* do escenario.

Zonas de Red

Las zonas listadas en esta página representan diferentes redes asociadas desde la consola. Los elementos, estas entradas se deben configurar sobre el cortafuegos, simplemente definen nombres y descripciones de ellas.

Seleccionar todo | Insertar selección | Agregar una nueva zona de red

| Nombre de zona | Descripción de zona | Zona tipo | Comentario | Organizar | Estado |
|-------------------------------|---------------------|-----------------|------------|-----------|--------|
| <input type="checkbox"/> eth0 | | Firewall system | | ↓ | Y ↓ |
| <input type="checkbox"/> wan | | eth0 | | ↑ ↓ | Y ↓ |
| <input type="checkbox"/> dmz | | eth0 | | ↑ ↓ | Y ↓ |
| <input type="checkbox"/> lan | | eth0 | | ↑ | Y ↓ |

Seleccionar todo | Insertar selección | Agregar una nueva zona de red

Editar en Configuración de Cortafuegos | Presione este botón para editar manualmente el archivo /etc/shorewall/zones de Shorewall, donde están guardadas las entradas de zonas.

Regresar a lista de zonas

Así teremos que definir as zonas *wan* (que representa a rede pública) e *dmz* (que representa a rede *dmz* do escenario). Tamén teremos que definir unha zona de tipo *Firewall system*, que representa ao propio equipo. Neste caso chamámoslle *ds2*. Recomendase seguir estes nomes xa que teñen que ser nomes curtos e hai moitos caracteres inválidos.

Configuración de Módulos

Cortafuegos Shorewall
Shorewall versión 4.4.12.0

Buscar Documentación

Zona de Red (Zones)

Tipo de Servicio (net)

Cuando Esta Operando (whenoperating)

Additional Working Privileges (privileges)

Interfaz de Red (Interfaces)

Enmascaramiento (mask)

Tamaño MTU (mtu)

Routing Rules (rules_rules)

Módulo por Defecto (Default)

MTU máxima (mt)

Modo de Zona (zone)

Custom generated (generated)

Reglas de Configuración (Rules)

IPV4 I. 2.345 (IPV4 I. 2.345)

Proxy ARP (proxyarp)

Revisión de la zona segura (checkzone)

Modo configuración file (shorewall.conf)

Inicio de Configuración | Comprobar la Configuración | Borrar Configuración

Presione este botón para iniciar Shorewall con la configuración actual como orden shorewall[1] -t start.
Presione este botón para hacer que Shorewall utilice la configuración con la orden shorewall[1] -t check.
Click this button to view Shorewall tracing information from the shorewall[1] debug command.

Agora temos que asociar as interfaces de rede do equipo ás zonas. Picamos en **Interfaces de rede**.

Interfaces de Red

En esta página, deben estar todas y cada una de las interfaces de red del sistema que quiere que Shorewall gestione, asociadas con la entrada a la que están conectadas. La interfaz de red que se no ha de aparecer. No se ha definido ninguna interfaz de red.

Agregar una nueva interfaz de red

Editar en Configuración de Cortafuegos | Presione este botón para editar manualmente el archivo /etc/shorewall/interfaces de Shorewall, donde están guardadas las entradas de zonas.

Regresar a lista de zonas

Non hai ningunha interface. Agregamos...

Crear Interfaz de Red

Seleccione de la interfaz de red

Interfaz: Nombre de zona:

Descripción de interfaz:

Opciones:

☐ ninguno ☐ Autodiscover ☐ ninguno ☐ Autodiscover ☐ ninguno ☐ Autodiscover

Crear | Regresar a lista de interfaces

Introducimos o nome dunha interface de rede do equipo, neste caso *eth0*. Esta interface é a que se conecta á rede pública, así que seleccionamos como zona asociada **wan**. Deixamos o resto das opcións por defecto e picamos en **Crear**.

Interfaces de Red

En esta página, deben estar todas y cada una de las interfaces de red del sistema que quiere que Shorewall gestione, asociadas con la zona a la que están conectadas. La interfaz de red que se no ha de aparecer.

Seleccionar todo | Insertar selección | Agregar una nueva interfaz de red

| Interfaz | Nombre de zona | Descripción de interfaz | Opciones | Organizar | Estado |
|-------------------------------|----------------|-------------------------|----------|-----------|--------|
| <input type="checkbox"/> eth0 | wan | Interfaz de red de wan | Ninguno | ↓ | Y ↓ |
| <input type="checkbox"/> eth1 | lan | Interfaz de red de lan | Ninguno | ↑ ↓ | Y ↓ |
| <input type="checkbox"/> eth2 | dmz | Interfaz de red de dmz | Ninguno | ↑ | Y ↓ |

Seleccionar todo | Insertar selección | Agregar una nueva interfaz de red

Editar en Configuración de Cortafuegos | Presione este botón para editar manualmente el archivo /etc/shorewall/interfaces de Shorewall, donde están guardadas las entradas de zonas.

Regresar a lista de zonas

Ao final temos que ter asociadas as tres interfaces *eth0*, *eth1* e *eth2* ás zonas *wan*, *lan* e *dmz* respectivamente.

Configuración de Módulos

Cortafuegos Shorewall
Shorewall versión 4.4.12.0

Buscar Documentación

Zona de Red (Zones)

Tipo de Servicio (net)

Cuando Esta Operando (whenoperating)

Additional Working Privileges (privileges)

Interfaz de Red (Interfaces)

Enmascaramiento (mask)

Tamaño MTU (mtu)

Routing Rules (rules_rules)

Módulo por Defecto (Default)

MTU máxima (mt)

Modo de Zona (zone)

Custom generated (generated)

Reglas de Configuración (Rules)

IPV4 I. 2.345 (IPV4 I. 2.345)

Proxy ARP (proxyarp)

Revisión de la zona segura (checkzone)

Modo configuración file (shorewall.conf)

Inicio de Configuración | Comprobar la Configuración | Borrar Configuración

Presione este botón para iniciar Shorewall con la configuración actual como orden shorewall[1] -t start.
Presione este botón para hacer que Shorewall utilice la configuración con la orden shorewall[1] -t check.
Click this button to view Shorewall tracing information from the shorewall[1] debug command.

O terceiro paso é definir a política por defecto da devasa; é dicir, como se vai comportar a nivel xeral. Aquí haberá que ter en conta dúas cuestións: primeiro que todo posible tráfico que poida manexar o equipo (da rede *lan* á rede *wan*, da rede *wan* á rede *dmz*, etc.) debe estar incluído nalgũa política, xa que se non a devasa non sabería que facer con el. E segundo que as políticas son as pautas básicas que rexen o comportamento da devasa, que logo afinaremos máis concretamente coas regras. As regras teñen prioridade sobre as políticas, así que a devasa mirará primeiro se ao paquete se lle pode aplicar unha regra, e se non é así, aplicaralle unha das políticas por defecto que teña definidas.



Non hai políticas definidas. Agregamos unha.



As políticas simplemente teñen unha zona orixe, unha zona de destino e unha acción a tomar. Por exemplo, neste caso estamos dicíndolle á devasa que todo o que vaia de calquera sitio á zona *wan* (recórdese que a devasa ten asociada a zona *wan* á interface *eth0*) o acepte.



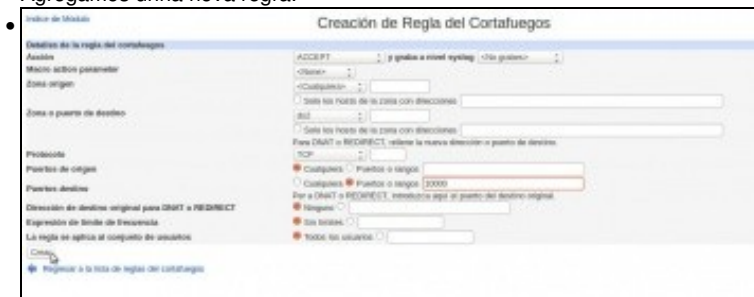
A configuración da devasa é unha decisión moi delicada e dependerá moito do nivel de seguridade e restricións que queiramos aplicar na nosa rede, pero unha opción para este caso podería ser deixar estas dúas políticas. Acéptase todo o que vaia á *wan*, e o resto rexéitase. Nótese que a orde na que se definen as políticas son moi importantes (por iso hai botóns para subilas e baixalas), xa que se aplican se arriba a abaixo. Por exemplo, se neste caso situásemos a segunda regra como primeira, executaríase sempre, xa que encaixa con calquera tráfico.



Por último, imos introducir algunhas regras para afinar o comportamento da devasa antes de iniciala (Olo!! Non se debe iniciar a devasa neste momento xa que deixaremos de ter acceso ao webmin dende o host... Pénsese por que).



Agregamos unha nova regra.



Reglas del Contingentes

Esta tabla lista las excepciones de los permisos por defecto por cada tipo de tráfico, origen, o destino. La acción seleccionada se aplica a los paquetes que coincidan con las opciones seleccionadas en contra de la política por defecto.

Seleccionar todo | Insertar selección | Agregar una nueva regla del contingente | Añadir una nueva...

| Acción | Origen | Destino | Protocolo | Paquetes de origen | Paquetes destino | Ingresar | Salir |
|---------|------------|--------------------------------------|-----------|--------------------|------------------|----------|-------|
| ICIDEST | Zona 1-6 | Zona 6-7 | TCP | Frankfurt | | + | 7 ↓ |
| ICIDEST | Zona 1-6 | Redes 192.168.0/24, 2 de la zona 6-7 | TCP | Costa Rica | | + | 7 ↓ |
| ICIDEST | Costa Rica | Zona 6-7 | TCP | Costa Rica | | + | 7 ↓ |

Seleccionar todo | Insertar selección | Agregar una nueva regla del contingente | Añadir una nueva...

[Detalles de la regla](#)

Configuración de Módulos

Cortadouegos Shorewall
Shorewall versión 4.6.11.0

Buscar Documentos

Zonas de Fiel (zones)

TOS

Tipos de Servicios (net)

STOP

Cuentas (red, Servicios (parameters))

Additional Logging (providers)

Horarios por Fiel (policies)

Zonas de destino (chains)

Tarjetas IP4 (networks)

Scripts (scripts)

Políticas por Fiel (policies)

NAT realice (nat)

Revisión de Datos (tables)

?

Custom parameters (parameters)

Reglas de firewall (rules)

IPV1.1
2.34

Proxy ARP (parameters)

Procesos de la Red (rules)

IPV1.1
2.34

Monitor configuración de (parameters)

Inicio de Cortadouegos

Comando de Configuración

Inicio (help)

Presione este botón para iniciar Shorewall con la configuración actual con el orden shorewall[1] -s -a -t.

Presione este botón para iniciar que Shorewall utilice la configuración con el orden shorewall[1] -check.

Click this button to load Shorewall using information from the shorewall[1] -load command.



TOS
Tape of Tapes
TOS
Cuando todo comienza (posterlogos)



Tape of Tapes
Tape of Tapes
Tape of Tapes
Cuando todo comienza (posterlogos)



Tape of Tapes
Tape of Tapes
Tape of Tapes
Cuando todo comienza (posterlogos)



Tape of Tapes
Tape of Tapes
Tape of Tapes
Cuando todo comienza (posterlogos)



Tape of Tapes
Tape of Tapes
Tape of Tapes
Cuando todo comienza (posterlogos)



Tape of Tapes
Tape of Tapes
Tape of Tapes
Cuando todo comienza (posterlogos)



Tape of Tapes
Tape of Tapes
Tape of Tapes
Cuando todo comienza (posterlogos)



Tape of Tapes
Tape of Tapes
Tape of Tapes
Cuando todo comienza (posterlogos)

```

administrador@uc1ient:~$ ping 192.168.69.2
PING 192.168.69.2 (192.168.69.2) 56(84) bytes of data:
64 bytes from 192.168.69.2: icmp_req=1 ttl=63 time=1.60 ms
64 bytes from 192.168.69.2: icmp_req=2 ttl=63 time=0.854 ms
^C
--- 192.168.69.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.854/1.227/1.601/0.375 ms
administrador@uc1ient:~$ ssh root@192.168.69.2
root@192.168.69.2's password:
Linux dserver 2.6.32-5-amd64 #1 SMP Mon Feb 25 00:26:11 UTC 2013 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Apr 12 00:21:06 2013 from 172.16.69.101
root@dserver:~#
```

Imos comprobar o resultado. Dende *uclient* podemos facer un ping e conectarnos por ssh a *dserver3*.

```
root@dserver3:~# ping 172.16.69.101
PING 172.16.69.101 (172.16.69.101) 56(84) bytes of data.
^C
--- 172.16.69.101 ping statistics ---
7 packets transmitted, 0 received, 100% packet loss, time 6046ms
root@dserver3:~#
```

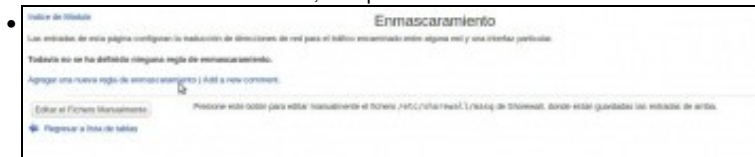
Pero dende *dserver3* non podemos acceder a *uclient*... Perfecto!! A *lan* está protexida pola devasa.

```
administrador@uclient:~$ ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
^C
--- 10.0.0.1 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4032ms
administrador@uclient:~$
```

Aínda temos un problema por solucionar, xa que *uclient* non pode conectarse á rede pública; falta activar NAT no router *dserver2*.



Farémolo no mesmo shorewall, no apartado de **Enmascaramiento**.



Agregamos unha nova regra de enmascaramento (xa que o imos facer é *enmascarar* unha rede privada sobre unha interface pública que ten o router).



Como interface de saída seleccionamos *eth0*, que é a interface pública do router. Como rede a enmascarar, seleccionamos a subrede na interface *eth1*, que é a rede *lan*. O resto das opcións deixámolas como están.



Engadimos outra regra igual pero para enmascarar a subrede na interface *eth2*, que é a rede *dmz* (esta rede tamén é privada e se non non terá acceso á rede pública).



Aplicamos a configuración, e....

```

administrador@uclient:~$ ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
64 bytes from 10.0.0.1: icmp_req=1 ttl=63 time=20.5 ms
64 bytes from 10.0.0.1: icmp_req=2 ttl=63 time=2.42 ms
^C
--- 10.0.0.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/ndev = 2.421/11.493/20.565/9.072 ms
administrador@uclient:~$ ping www.google.es
PING www.google.es (173.194.45.63) 56(84) bytes of data.
64 bytes from par03s12-in-f31.1e100.net (173.194.45.63): icmp_req=1 ttl=53 time
72.6 ms
64 bytes from par03s12-in-f31.1e100.net (173.194.45.63): icmp_req=2 ttl=53 time
74.5 ms
64 bytes from par03s12-in-f31.1e100.net (173.194.45.63): icmp_req=3 ttl=53 time
76.1 ms
^C
--- www.google.es ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/ndev = 72.628/74.452/76.155/1.476 ms
administrador@uclient:~$

```

Agora si!! Xa temos os dous problemas resolto.

- Pero.... ¿todo isto non se sae un chisco do obxecto do curso? Ademais de xogar de forma máis profunda cos modos das interfaces de rede en VirtualBox, o router que acabamos de simular é precisamente o que VirtualBox implementa cando configuramos unha interfaz de rede dunha máquina virtual por NAT ou rede NAT. Nese caso, é VirtualBox o que fai de router, con NAT, pero ademais tamén implementa o servidor DHCP e DNS (nós ímonos quedar aquí). Con isto preténdese así que quede máis claro todo este proceso, e entender a virtualización da rede que implementa VirtualBox.

Reenvío de portos

Para rematar, imos facer co noso router virtualizado a mesma función que VirtualBox permite coas tarxetas en modo NAT e rede NAT co reenvío de portos. Recórdese que isto permite acceder a un porto da máquina virtual mediante o reenvío dun porto da máquina *host*.

O equivalente neste caso sería redirixir un porto libre de *dserver2* a un servizo por exemplo duha máquina da *DMZ*. Imos coller o servizo de ssh de *dserver3*:

- Reenvío de portos coa MV Debian

Primeiro teremos que modificar a regra que só permitía acceder a este servizo dende a zona *lan*, para poñer como zona orixe *calquera*.

Creamos unha regra de tipo *DNAT* (Destination NAT), que redirixe o tráfico que veña da zona *wan* e vaia á zona *dmz*, concretamente ao porto 22 do equipo 192.168.69.2, co protocolo TCP os paquetes que reciba para o porto 22222 (este será o porto de *dserver2* que será redirixido ao servidor ssh de *dserver3*).

Vista de como quedan as dúas regras. Aplicamos os cambios no shorewall.

E xa podemos acceder dende un equipo da rede pública (por exemplo dende o *host*) por ssh ao porto 22222 da máquina *dserver2* usando a súa dirección IP pública. Unha vez dentro executamos o comando **ifconfig** para saber en que máquina estamos realmente; a dirección IP indica que estamos en *dserver3*.

-- Antonio de Andrés Lema e Carlos Carrión Álvarez --