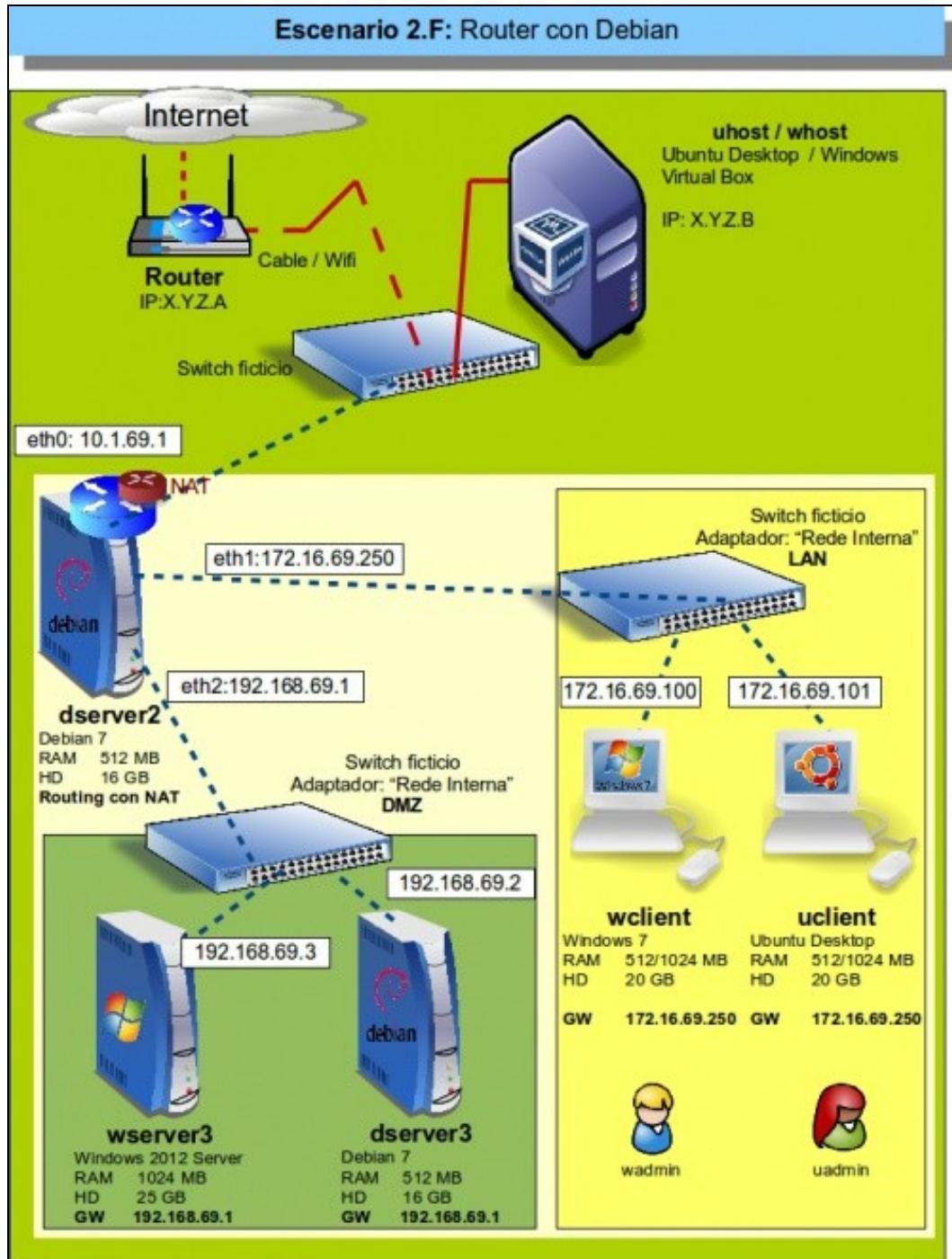
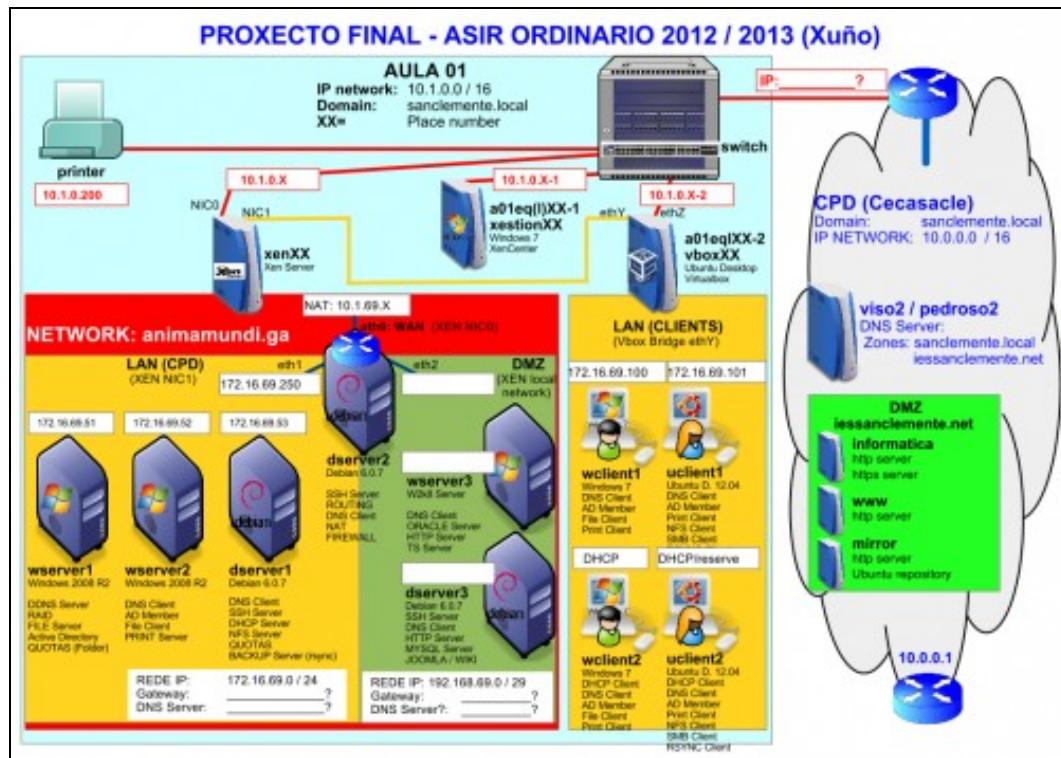


Escenario 2.F: Configuración dun router virtualizado con Debian



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:



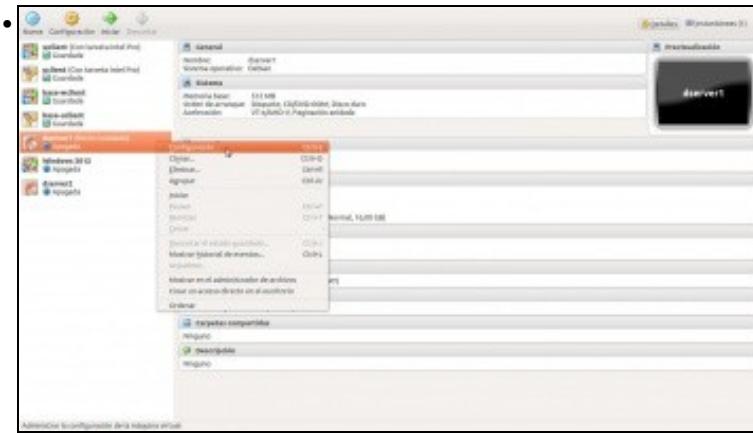
Sumario

- 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

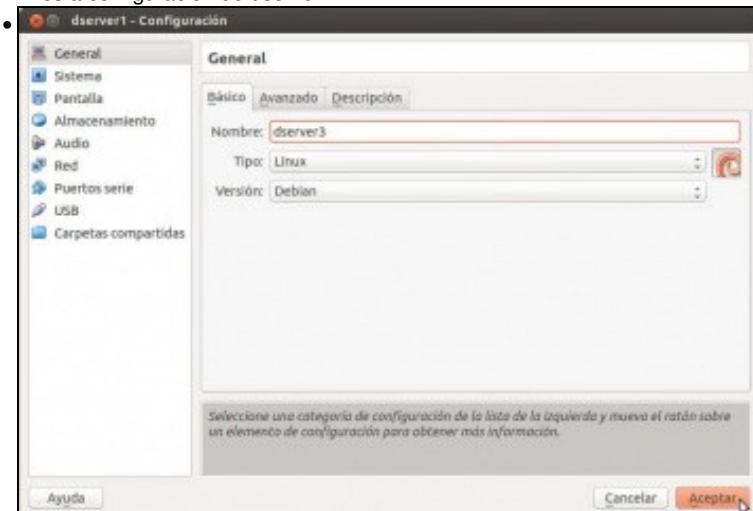
Renomear e agrupar as máquinas do escenario

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.

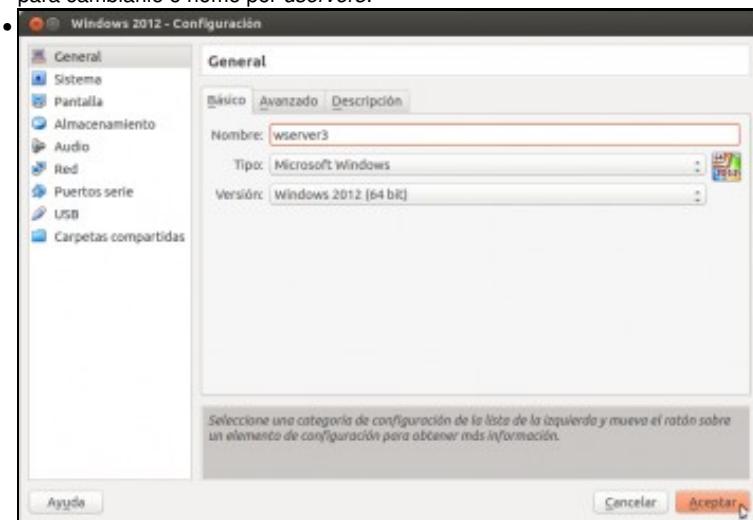
- Renomear e agrupar as máquinas do escenario



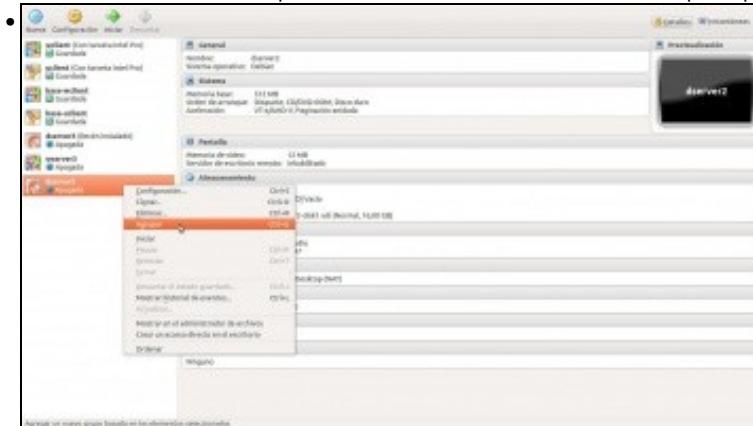
Imos á configuración de *dserver1*...



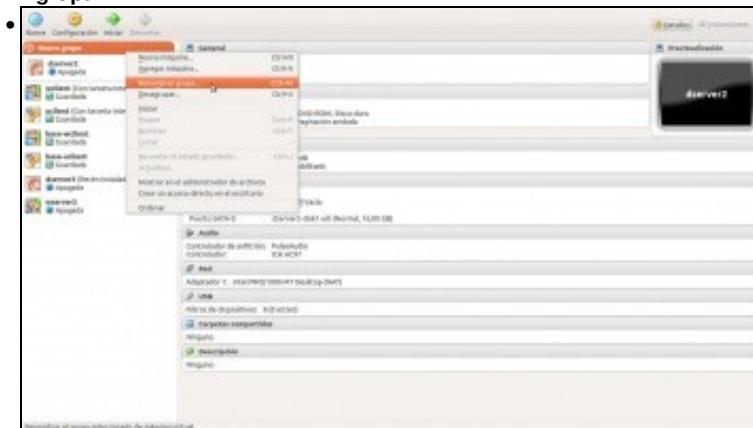
para cambiarle o nome por *dserver3*.



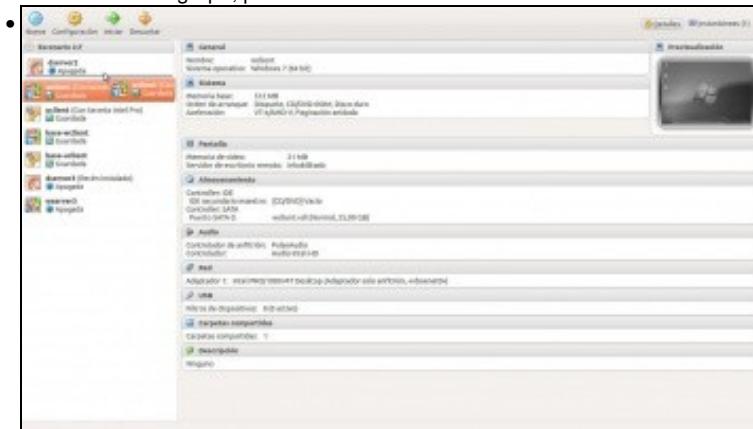
Tamén renomeamos a máquinas de Windows Server como `wserver3`, para que tamén coincida o seu nome co do escenario.



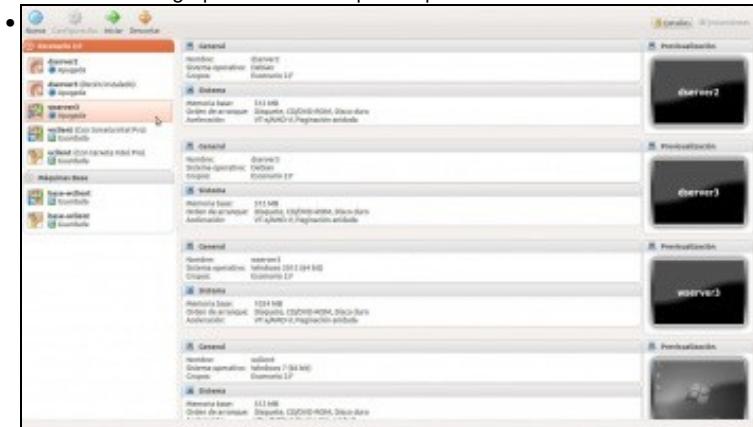
Agora imos agrupar as máquinas que van intervir no escenario. Picamos co botón dereito sobre unha delas e seleccionamos a opción de **Agrupar**.



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



Arrastramos ao grupo todas as máquinas que imos utilizar.



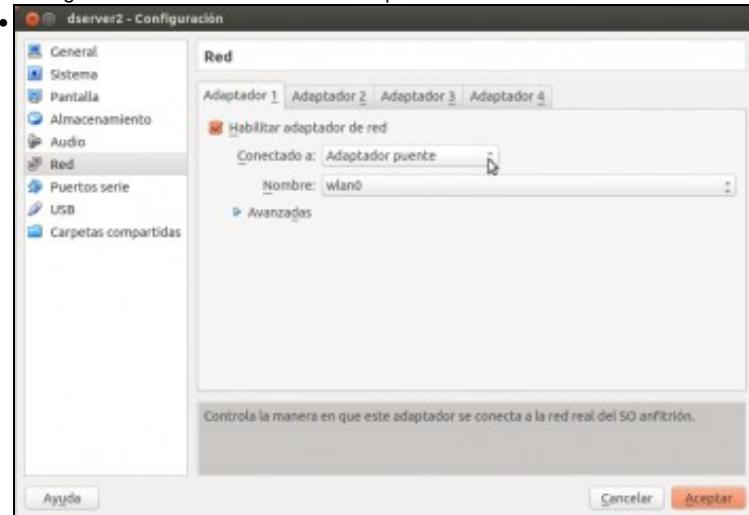
Vista do grupo coas máquinas xa incluídas.

Configurar as tarxetas de rede das máquinas

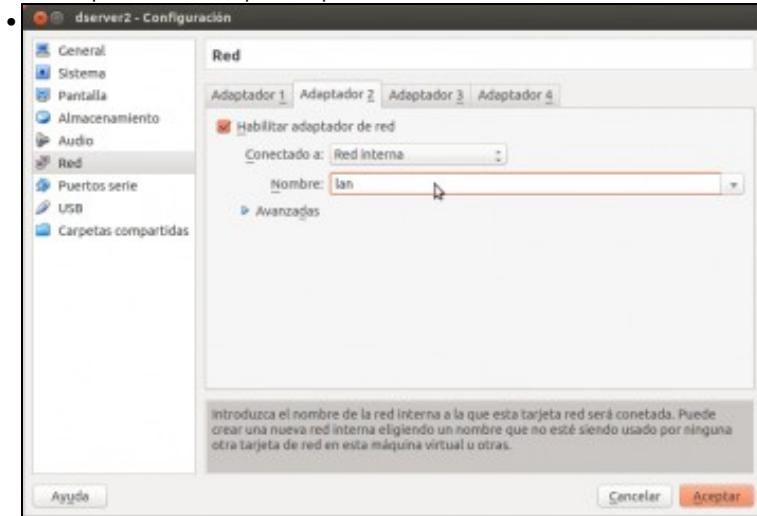
Como segundo paso, imos engadir nas máquinas os adaptadores necesarios e os modos de conexión de cada unha. Se revisamos o escenario, veremos que todos os adaptadores estarán en modo de rede interna excepto o adaptador 1 da máquina *dserver2* que estará en modo ponte.

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. Desa 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.

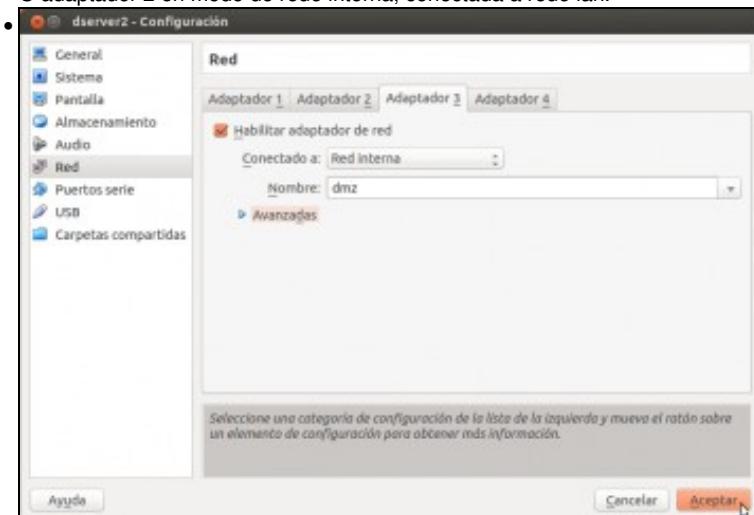
- Configurar as tarxetas de rede das máquinas



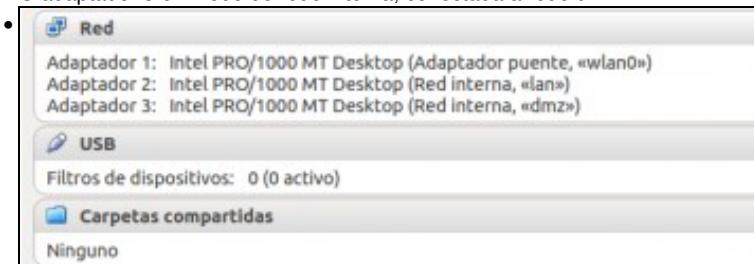
Na máquina *dserver2*, que é a que vai simular o router, habilitaremos tres tarxetas de rede. O adaptador 1 en modo ponte.



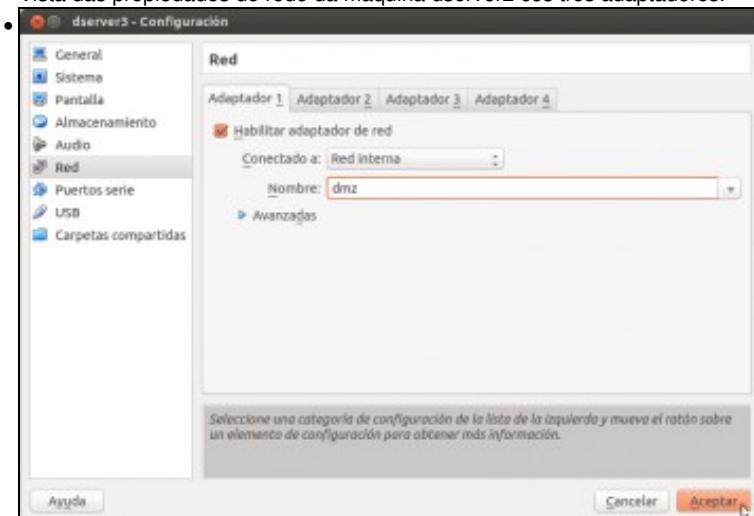
O adaptador 2 en modo de rede interna, conectada á rede *lan*.



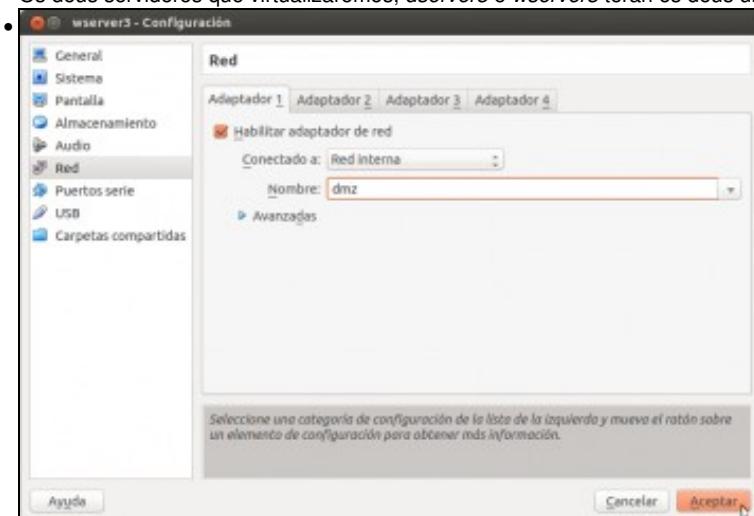
O adaptador 3 en modo de rede interna, conectada á rede *dmz*.



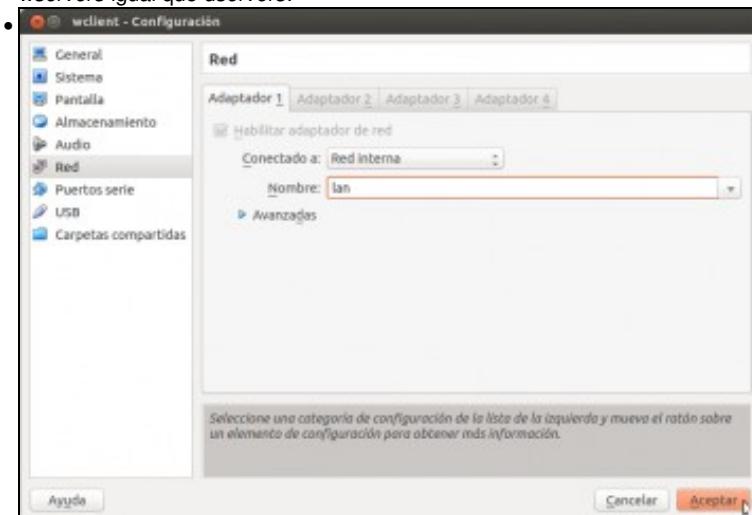
Vista das propiedades de rede da máquina *dserver2* cos tres adaptadores.



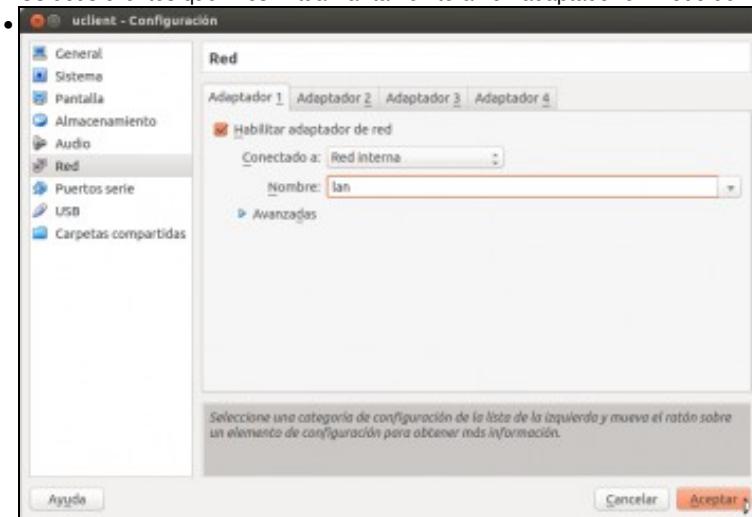
Os dous servidores que virtualizaremos, *dserver3* e *wserver3* terán os dous un adaptador en modo de rede interna, conectados á rede *dmz*.



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 más 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 ttym1
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*.)

```
• dserver2 [Corriendo] - Oracle VM VirtualBox
root@dserver:~# ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:52:cc:04
          inet addr:10.0.0.11 Bcast:10.255.255.255 Mask:255.0.0.0
            inet6 addr: fe80::a00:27ff:fe52:cc%eth0/64 Scope:Link
              UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
              RX packets:14654 errors:0 dropped:0 overruns:0 frame:0
              TX packets:18337 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 houbese 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@portatil17:~#
administrador@portatil17:~$ 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:d9:b7:c0:00:9b:ed:6e: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

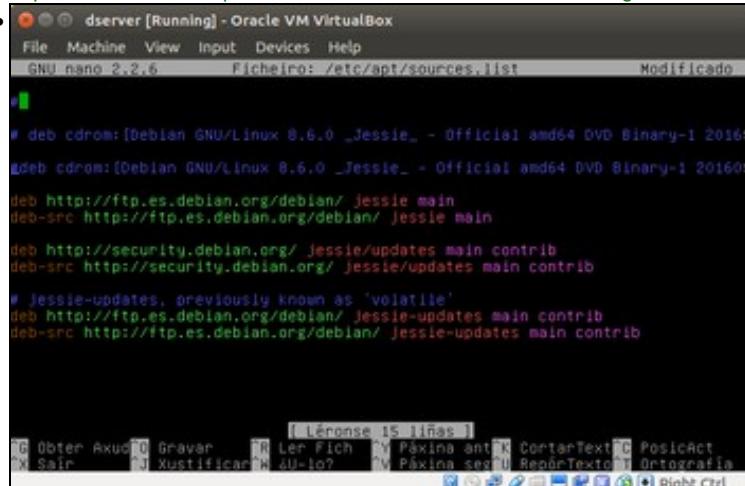
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

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).

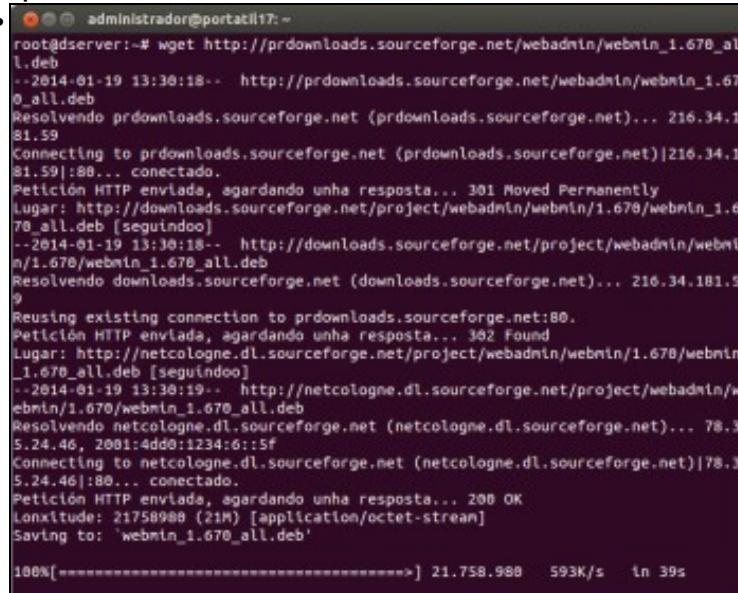
Olló que nas novas versións de ssh non deixa, por defecto, iniciar sesión co usuario root. Por tanto podemos iniciar sesión co usuario dadmin (abc123.) e unha vez no servidor pasarse a root con **su -**. Tamén se pode editar o ficheiro /etc/ssh/sshd-config tal como se indica en:

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



```
# deb cdrom:[Debian GNU/Linux 8.6.0 _Jessie_ - Official amd64 DVD Binary-1 2016-01-19] deb cdrom:[Debian GNU/Linux 8.6.0 _Jessie_ - Official amd64 DVD Binary-1 2016-01-19] 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
```

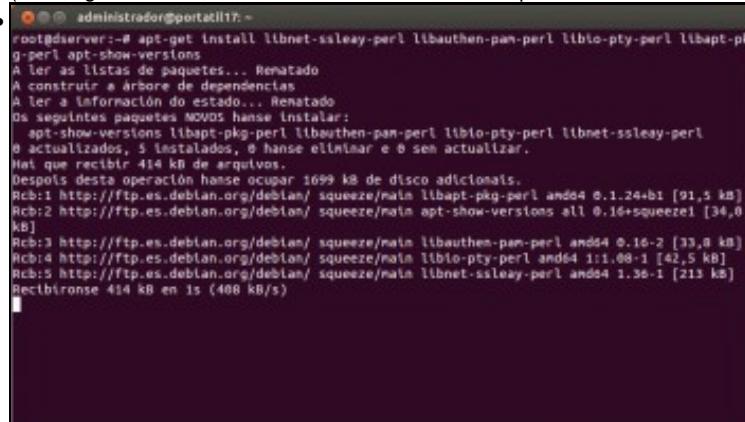
Asegurarse de que están comentadas as sources do CD-ROM (*nano /etc/apt/sources.list*). E actualizar a lista dos paquetes: **apt-get update**



```
root@dserver:~# wget http://prdownloads.sourceforge.net/webadmin/webmin_1.670_all.deb
--2014-01-19 13:30:18--  http://prdownloads.sourceforge.net/webadmin/webmin_1.670_all.deb
Resolving prdownloads.sourceforge.net (prdownloads.sourceforge.net)... 216.34.1.81
Connecting to prdownloads.sourceforge.net (prdownloads.sourceforge.net)|216.34.1.81|:80... conectado.
Petición HTTP enviada, aguardando unha resposta... 301 Moved Permanently
Lugar: http://downloads.sourceforge.net/project/webadmin/webmin/1.670/webmin_1.670_all.deb [segundo]
--2014-01-19 13:30:18--  http://downloads.sourceforge.net/project/webadmin/webmin/1.670/webmin_1.670_all.deb
Resolviendo downloads.sourceforge.net (downloads.sourceforge.net)... 216.34.181.5
Reusing existing connection to prdownloads.sourceforge.net:80.
Petición HTTP enviada, aguardando unha resposta... 302 Found
Lugar: http://netcologne.dl.sourceforge.net/project/webadmin/webmin/1.670/webmin_1.670_all.deb [segundo]
--2014-01-19 13:30:18--  http://netcologne.dl.sourceforge.net/project/webadmin/webmin/1.670/webmin_1.670_all.deb
Resolviendo netcologne.dl.sourceforge.net (netcologne.dl.sourceforge.net)... 78.3.5.24.46, 2001:4dd0:1234:6::5
Connecting to netcologne.dl.sourceforge.net (netcologne.dl.sourceforge.net)|78.3.5.24.46|:80... conectado.
Petición HTTP enviada, aguardando unha resposta... 200 OK
Longitud: 21758988 (21M) [application/octet-stream]
Saving to: 'webmin_1.670_all.deb'

100%[=====] 21.758.988  593K/s   in 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)



```
root@dserver:~# apt-get install libnet-ssleay-perl libauthen-pam-perl liblio-pty-perl libapt-pkg-perl
A ler as listas de paquetes... Renatado
A construir a árbore de dependencias
A ler a información do estado... Renatado
Os seguintes paquetes NOVOS hánse instalar:
  apt-show-versions libapt-pkg-perl libauthen-pam-perl liblio-pty-perl libnet-ssleay-perl
0 actualizados, 5 instalados, 0 hánse eliminar e 0 sem actualizar.
Notas: que recibir 414 kB de arquivos.
Despós desta operación hánse ocupar 1699 kB de disco adicional.
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 0.10-2 [33.8 kB]
Rcb:4 http://ftp.es.debian.org/debian/ squeeze/main liblio-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]
Recibiríonse 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 libauthen-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) ...
```

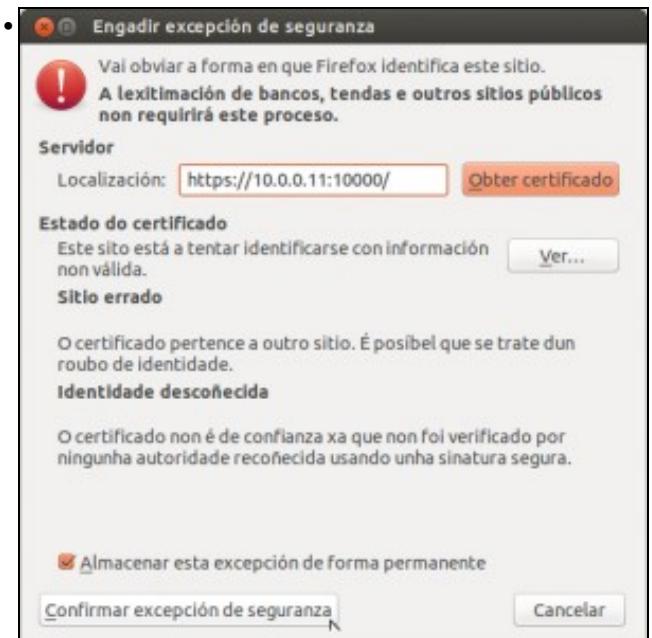
Instalamos o webmin, introducindo o comando `dpkg -i webmin_1.820_all.deb`

```
● 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 [678  
kB]  
Obtívérmonse 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 seguridad 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).

The screenshot shows the Webmin control panel interface. On the left, there's a sidebar with links like 'Logout', 'Webmin', 'Sistemas', 'Sistemas', 'Otros', and 'Red'. The main area displays system information: System hostname (dsvr01.comvmx.es), Operating system (Debian Linux 7), Webmin version (1.870), Time on system (Sat Jan 19 13:38:41 2014), Kernel and CPU (Linux 3.2.0-4-686-pae on x86_64). It also shows Processor information (Intel(R) Core(TM) i3 CPU M 380 @ 2.27GHz, 1 cores), System uptime (0 hours, 13 minutes), Running processes (65), GPU load averages (0.03 (1 min), 0.12 (5 min), 0.08 (15 min)), CPU usage (0% user, 0% kernel, 0% IO, 100% idle), Real memory (119.65 MB used, 498.97 MB total), Virtual memory (8 kB used, 714 MB total), Local disk space (1.75 GB used, 15.08 GB total), and Package updates (All installed packages are up to date). Below this, a message says 'The 1 following Webmin module updates are now available...'. A footer bar shows 'Module: Version: Fixes problems:' with 'Userspace de Webmin' (1.872) and 'Fix Perl error calling webmin::allow_factor_form_auth when enabling two-factor authentication'. There's also a 'Install Updates Now!' button.

Recargamos a páxina e xa temos disponible 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 das 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 das configurarémola co webmin (*dserver2*) e a outra manipulando directamente os ficheiros de configuración (*dserver3*).

- Configuración das interfaces de rede en *dserver2*

This screenshot is identical to the one above, showing the main Webmin dashboard in Spanish. The sidebar and main content area are the same, including the message about available module updates and the footer information.

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

The screenshot shows the 'Configuración de Red' (Network Configuration) screen. At the top, there are four icons: 'Configuración de Módulo', 'Configuración de Red' (which is selected), 'Búfer y Documentos', and 'Aplicación'. Below these are four buttons: 'Instancia de red', 'Nuevo y Editar', 'Nombre de redipula y cliente DNS', and 'Direcciones de Máquina'. A large button labeled 'Aplicar Configuración' is at the bottom. A note below it says: 'Prestione este botón para activar la interfaz de tiempo de arranque y la configuración de red actual, tal como se han después de un reinicio. Advertencia: esto podría dejar a su sistema inaccesible desde la red, y costar el acceso a fibraoptica.' The sidebar and footer are identical to the previous screenshots.

Entramos no apartado de Interfaces de Rede

Nombre	Tipo	Dirección IP	Máscara de red	IPv6 address	Activar al arrancar?
eth0	Ethernet	De DHCP	De DHCP	No	
lo	Loopback	No address configured	None	Si	

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 quien usará unha dirección IP que pertenza a rede que englobe ao *host*) e salvamos.

Nombre	Tipo	Dirección IP	Máscara de red	IPv6 address	Activar al arrancar?
eth0	Ethernet	10.1.69.1	255.0.0.0		Si
lo	Loopback	No address configured	None		Si

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**.

Índice de Módulo

Crear Interfaz de Arranque

Parámetros de interfaz de tiempo de arranque

Nombre:	eth1
Activate at boot?	<input checked="" type="radio"/> Sí <input type="radio"/> No
IPv4 address:	<input type="radio"/> No address configured <input type="radio"/> De DHCP <input type="radio"/> De BOOTP <input checked="" type="radio"/> Static configuration
Dirección IP:	172.16.69.250
Máscara de red:	255.255.255.0
Broadcast:	<input checked="" type="radio"/> Automático <input type="radio"/>
IPv6 addresses:	<input checked="" type="radio"/> IPv6 disabled <input type="radio"/> From IPv6 discovery <input type="radio"/> Static configuration
IPv6 address:	IPv6 address: [] Netmask: []
MTU:	<input checked="" type="radio"/> Defecto <input type="radio"/>
Interfaces virtuales:	0 (Añadir interfaz virtual)
Dirección de Hardware:	<input checked="" type="radio"/> Defecto <input type="radio"/>

Acciones: [Crear](#) [Crear y Aplicar](#) [Regresar a interfaces de red](#)

Poñemos como nome da interfaz **eth1**, marcamos que se active no inicio (**Activate at boot->Sí**), 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**.

Índice de Módulo

Interfaces de Red

Interfaces Activas Altonas | 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 arrancar?
eth0	Ethernet	10.1.69.1	255.0.0.0		<input type="radio"/> Sí
eth1	Ethernet	172.16.69.250	255.255.255.0		<input checked="" type="radio"/> Sí
lo	Loopback	No address configured	None		<input type="radio"/> Sí

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

[Delete Selected Interfaces](#) [Delete and Apply Selected Interfaces](#) [Apply Selected Interfaces](#)

[Regresar a configuración de red](#)

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

Índice de Módulo

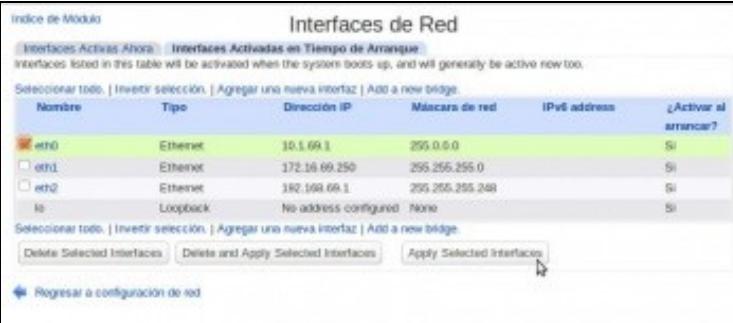
Crear Interfaz de Arranque

Parámetros de interfaz de tiempo de arranque

Nombre:	eth2
Activate at boot?	<input checked="" type="radio"/> Sí <input type="radio"/> No
IPv4 address:	<input type="radio"/> No address configured <input type="radio"/> De DHCP <input type="radio"/> De BOOTP <input checked="" type="radio"/> Static configuration
Dirección IP:	192.168.69.1
Máscara de red:	255.255.255.248
Broadcast:	<input checked="" type="radio"/> Automático <input type="radio"/>
IPv6 addresses:	<input checked="" type="radio"/> IPv6 disabled <input type="radio"/> From IPv6 discovery <input type="radio"/> Static configuration
IPv6 address:	IPv6 address: [] Netmask: []
MTU:	<input checked="" type="radio"/> Defecto <input type="radio"/>
Interfaces virtuales:	0 (Añadir interfaz virtual)
Dirección de Hardware:	<input checked="" type="radio"/> Defecto <input type="radio"/>

Acciones: [Crear](#) [Crear y Aplicar](#) [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**.

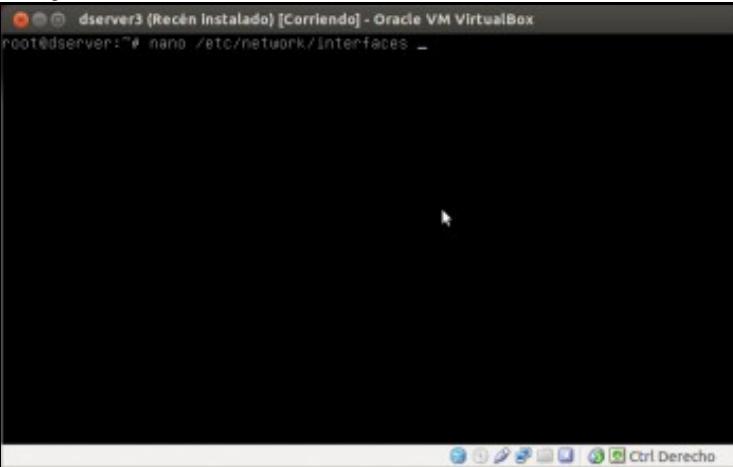
- 

Seleccionamos a interfaz **eth0**, que é o único cambio que ainda 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>

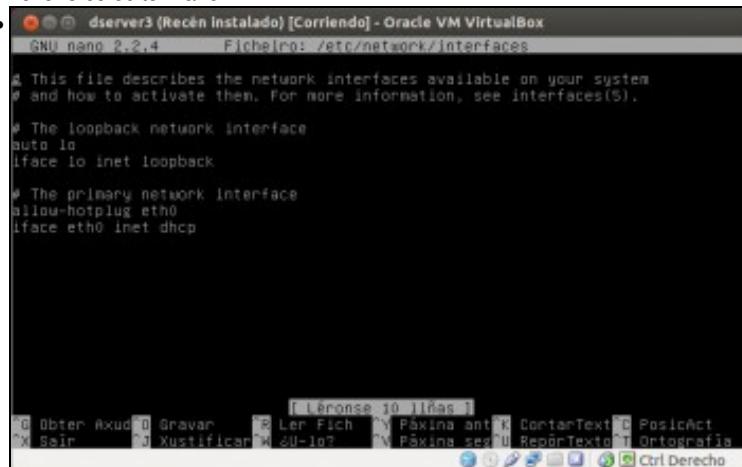
- 

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**.



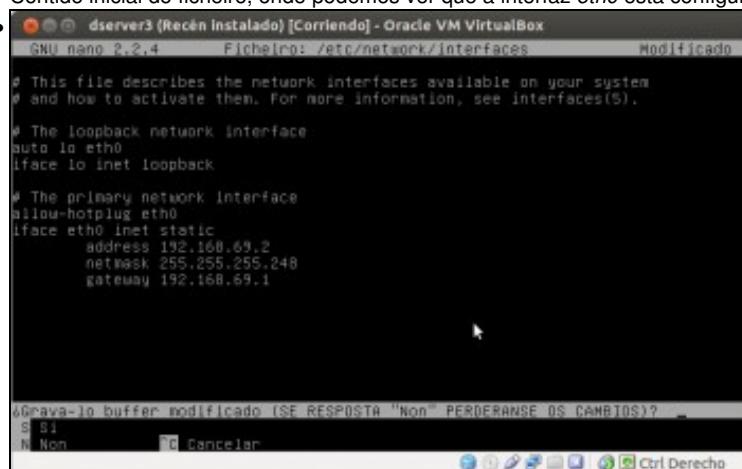
```
GNU nano 2.2.4      Ficheiro: /etc/network/interfaces

# 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.



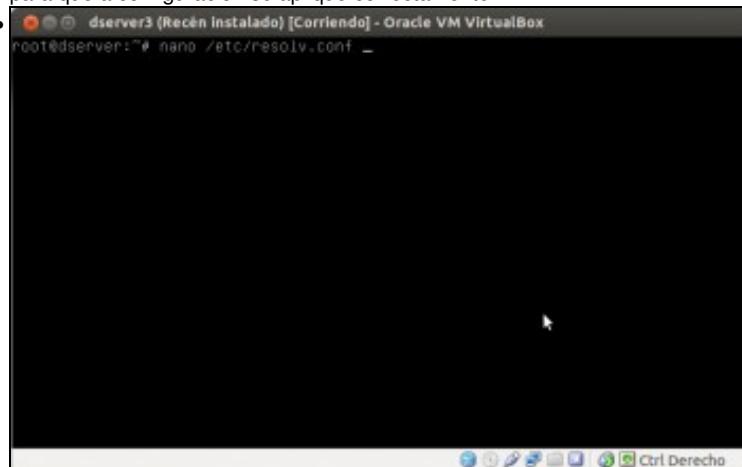
```
GNU nano 2.2.4      Ficheiro: /etc/network/interfaces      Modificado

# 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

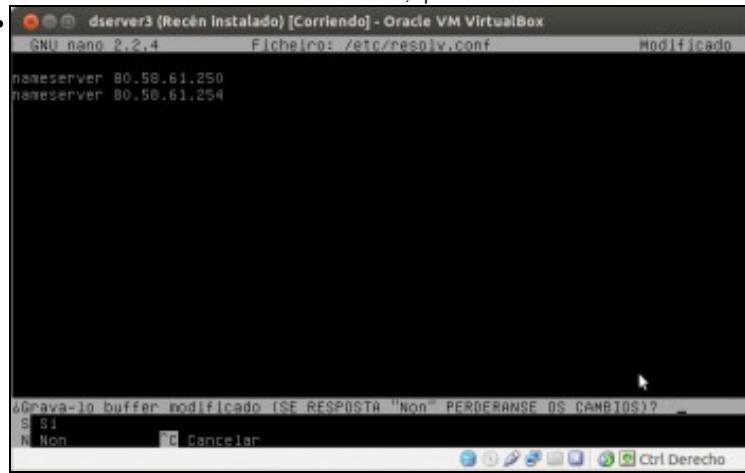
# The primary network interface
allow-hotplug eth0
iface eth0 inet static
    address 192.168.69.2
    netmask 255.255.255.248
    gateway 192.168.69.1
```

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.



```
root@dserver3:~# nano /etc/resolv.conf
```

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



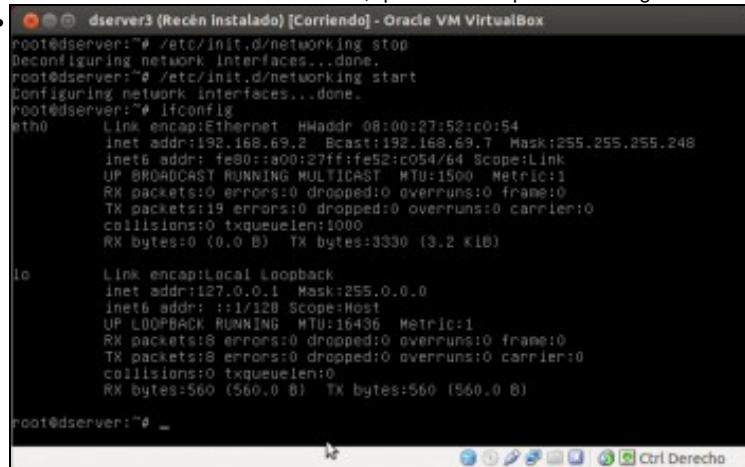
```
GNU nano 2.2.4           Ficheiro: /etc/resolv.conf          Modificado

nameserver 80.58.61.250
nameserver 80.58.61.254

Grava-la buffer modificado (SF, RESPONDA "Non" PERDERANSE OS CAMBIOS)?
```

S Si N Non [D] Cancelar Ctrl Derecho

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

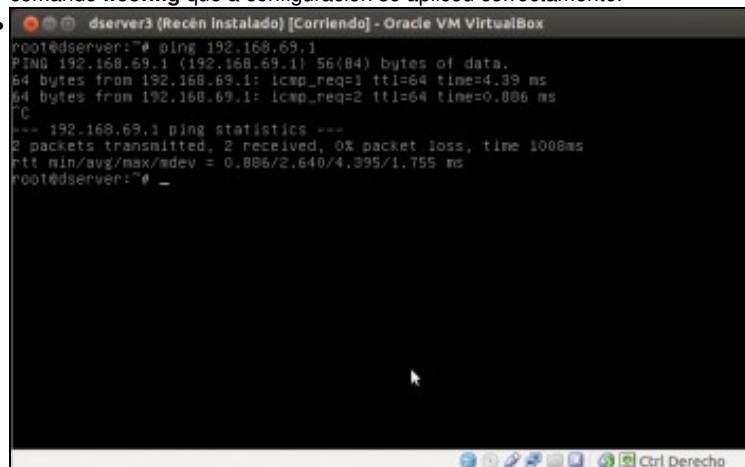


```
root@server3 [Recén Instalado] - Oracle VM VirtualBox
root@server3:~# /etc/init.d/networking stop
Decompressing network interfaces...done.
root@server3:~# /etc/init.d/networking start
Configuring network interfaces...done.
root@server3:~# ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:52:c0:54
          inet addr:192.168.69.2 Bcast:192.168.69.255 Mask:255.255.255.252
          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@server3:~#
```

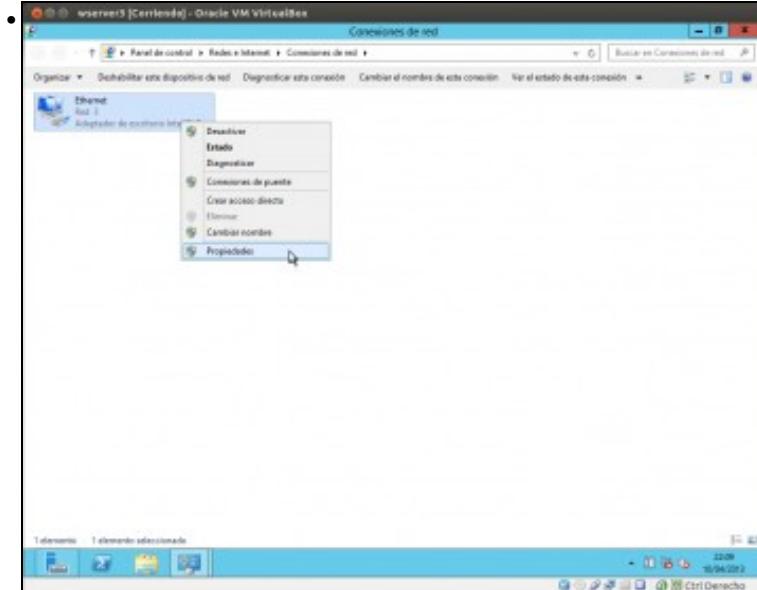
Detemos e iniciamos o servizo de rede cos comandos **/etc/init.d/networking stop** e **/etc/init.d/networking start**. Convén comprobar co comando **ifconfig** que a configuración se aplicou correctamente.



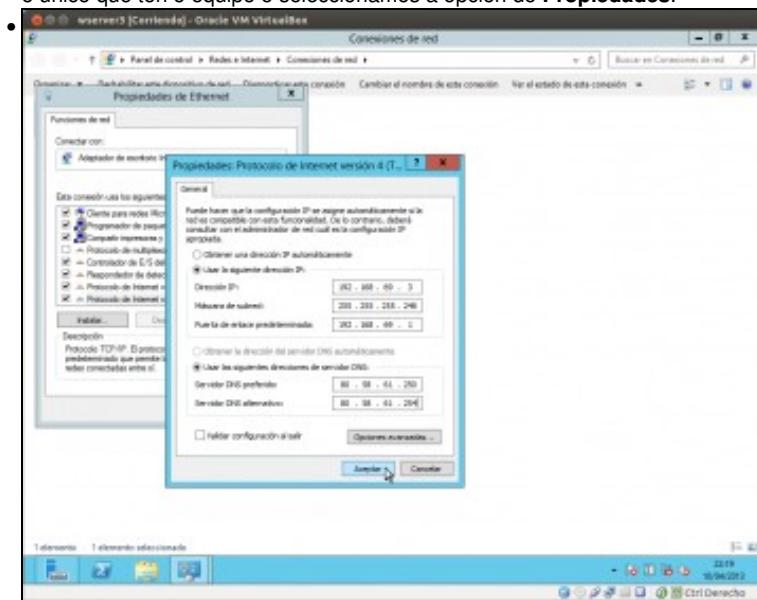
```
root@server3 [Recén Instalado] - Oracle VM VirtualBox
root@server3:~# ping 192.168.69.1
PING 192.168.69.1 (192.168.69.1) 56(84) bytes of data.
64 bytes from 192.168.69.1: icmp_seq=1 ttl=64 time=4.39 ms
64 bytes from 192.168.69.1: icmp_seq=2 ttl=64 time=0.006 ms
```
-- 192.168.69.1 ping statistics --
2 packets transmitted, 2 received, 0% packet loss, time 1008ms
rtt min/avg/max/mdev = 0.006/2.640/4.395/1.755 ms
root@server3:~#
```

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.

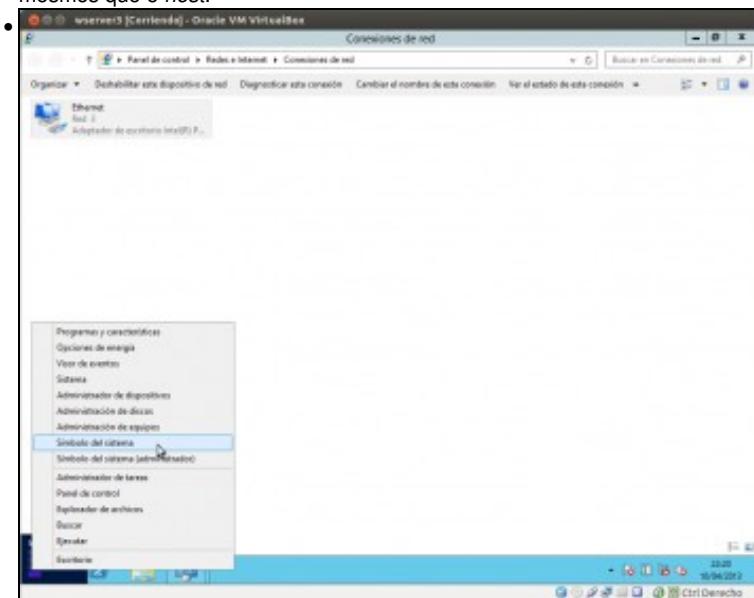
- Configuración das interfaces de rede en *wserver3*



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 **Procolo 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*.

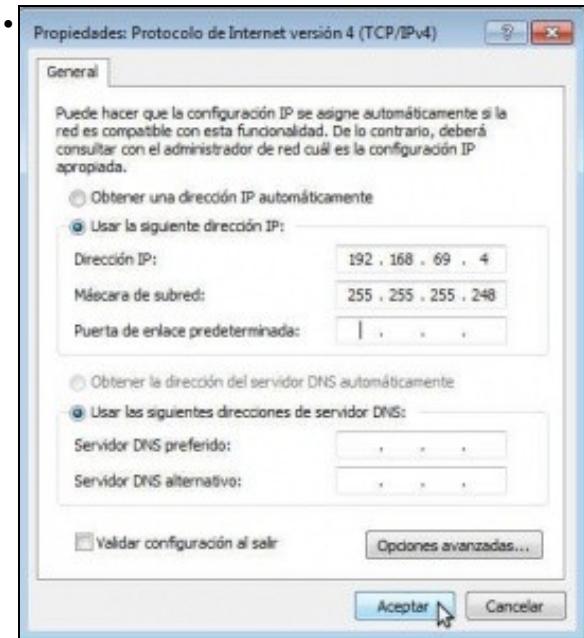


Abrimos unha ventá de **Símbolo do sistema** para facer un *ping* e comprobar a conectividade con *dserver2* e *dserver3*

```
Administrador: Símbolo del sistema
C:\Users\Administrador>ping 192.168.69.1
Haciendo ping a 192.168.69.1 con 32 bytes de datos:
Respuesta desde 192.168.69.1: bytes=32 tiempo<1ms TTL=64
Respuesta desde 192.168.69.1: bytes=32 tiempo<1ms TTL=64
Estadísticas de ping para 192.168.69.1:
 Paquetes: enviados = 2, recibidos = 2, perdidos = 0
 (0% perdidos)
Tiempo aproximado de ida y vuelta en milisegundos:
 Mínimo = 0ms, Máximo = 0ms, Media = 0ms
Control-C
C:\Users\Administrador>ping 192.168.69.2
Haciendo ping a 192.168.69.2 con 32 bytes de datos:
Respuesta desde 192.168.69.2: bytes=32 tiempo=1ms TTL=64
Respuesta desde 192.168.69.2: bytes=32 tiempo=3ms TTL=64
Estadísticas de ping para 192.168.69.2:
 Paquetes: enviados = 2, recibidos = 2, perdidos = 0
 (0% perdidos)
Tiempo aproximado de ida y vuelta en milisegundos:
 Mínimo = 1ms, Máximo = 3ms, Media = 2ms
Control-C
C:\Users\Administrador>
```

Perfecto!!

- Configuración das interfaces de rede en *wclient*



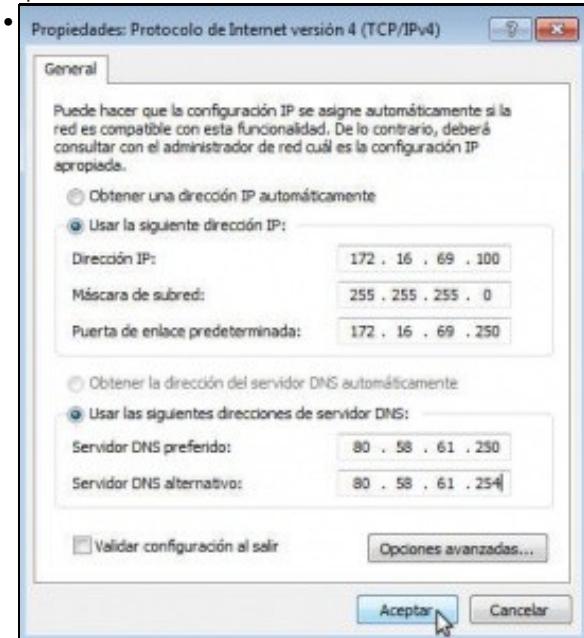
Neste caso, para comprender mellor o funcionamento da rede interna en VirtualBox, imos poñerlle á interfaz antes unha dirección IP dentro da mesma LAN que *dserver2* e *wserver3*. ¿Teremos conectividade entre elas???

```
C:\Windows\system32\cmd.exe
C:\Users\wadmin>ping 192.168.69.2
Haciendo ping a 192.168.69.2 con 32 bytes de datos:
Respueta desde 192.168.69.4: Host de destino inaccesible.

Estadisticas de ping para 192.168.69.2:
Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0x perdidos).

C:\Users\wadmin>
```

A resposta é que non, porque áinda 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 e *switchs ficticios* distintos e que non teñen conexión física entre si, como se refire no escenario.



Agora si poñemos os datos que se corresponden co escenario,

```
• C:\Windows\system32\cmd.exe
Microsoft Windows (Versión 6.1.7601)
Copyright © 2009 Microsoft Corporation. Reservados todos los derechos.
C:\Users\wadmin>ping 172.16.69.258

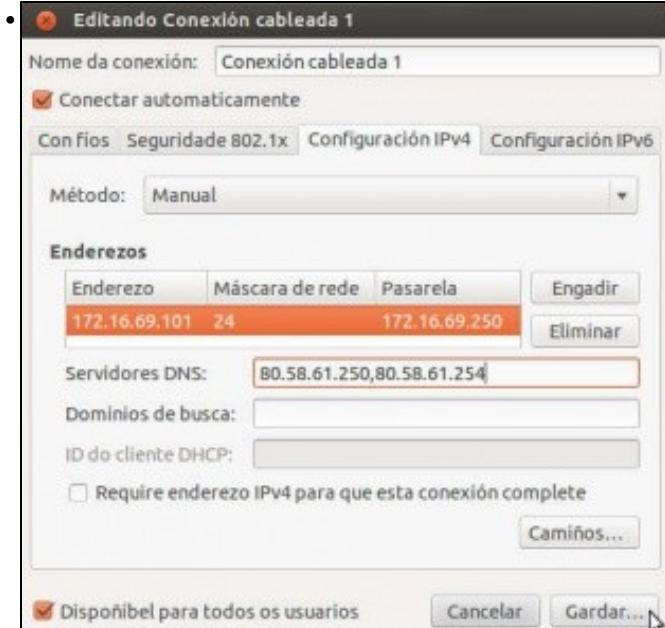
Haciendo ping a 172.16.69.258 con 32 bytes de datos:
Respueta desde 172.16.69.258: bytes=32 tiempo<1ms TTL=64

Estadísticas de ping para 172.16.69.258:
 Paquetes: enviados = 4, recibidos = 4, perdidos = 0
 (%) perdidos.
Tiempo aproximado de ida y vuelta en milisegundos:
 Minimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\wadmin>
```

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 último 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 172.16.69.258
PING 172.16.69.258 (172.16.69.258) 56(84) bytes of data.
64 bytes from 172.16.69.258: icmp_req=1 ttl=64 time=0.556 ms
64 bytes from 172.16.69.258: icmp_req=2 ttl=64 time=0.985 ms
^C
--- 172.16.69.258 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@uclient:~
administrador@uclient:~$ 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@uclient:~$
```

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**.

The screenshot shows the 'Ruteo y Gateways' configuration screen. It has sections for 'Booting time configuration' (with 'Active configuration' selected), 'Configuración de ruteo activada en tiempo de arranque' (with 'Router por defecto' set to 'Gateway 10.0.0.1'), and 'Actuar como router?' (with 'Si' checked). There are also tabs for 'Rutas estáticas' and 'Rutas locales'. At the bottom are 'Guardar' and 'Regresar a configuración de red' buttons.

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*.

```
● root@dserver3 [Recién Instalado] [Corriendo] - Oracle VM VirtualBox
root@dserver3:~# 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@dserver3:~#
```

E áinda 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 [bastiões](#)). 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.



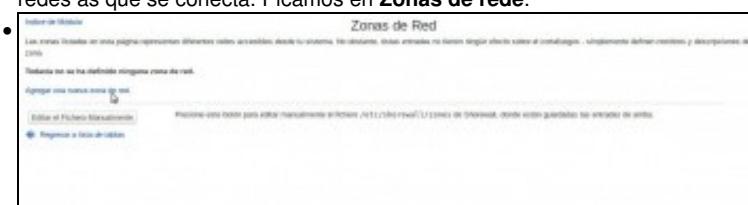
De momento o módulo de *Shorewall* non aparece en ningunha das categorías do webmin, xa que foi instalado despois. Picamos na opción de **Refresh Modules** para que webmin busque se ten novos módulos instalados e os engada na categoría correspondente.



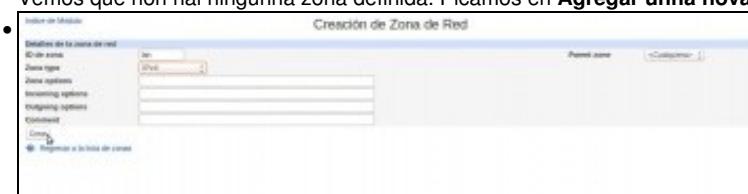
Atoparemos agora dentro da categoría de *Rede* o módulo de **Cortafuegos Shoreline**. Entramos nel. De momento o módulo está parado (fixarse en que temos o botón de *Iniciar el Cortafuegos*), pero se intentamos inicialo veremos que nos da un erro, debido a que é necesario establecer unha configuración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



En primeiro lugar, teremos que definir as zonas de rede que vai xestionar a devasa, que non son más 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.

• [Índice de Módulo](#)

**Zonas de Red**

En esta página, debes crear zonas y crear una de las interfaces de red del sistema que quieras que Shorewall proteja, asociadas con la zona en la que estén conectadas. La interfaz de Shorewall 1 no ha de aparecer.

| Nombre de la zona | Nombre interno | Tipo            | Estado   | Depósito | Acción |
|-------------------|----------------|-----------------|----------|----------|--------|
| ds2               | ds2            | Firewall system | Activo   | +        | +      |
| wan               | wan            | IPFW            | Inactivo | +        | +      |
| dmz               | dmz            | IPFW            | Inactivo | +        | +      |
| lan               | lan            | IPFW            | Inactivo | +        | +      |

[Configurar IPFW](#) | [Inventar interfaces](#) | [Añadir una nueva zona de red](#)

[Borrar selección](#)

[Volver al menú principal](#)

[Regresar a lista de zonas](#)

Presione este botón para editar masivamente el fichero /etc/shorewall/1/zones de Shorewall, donde están guardados los cambios de zona.

• [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**. Recoméndase seguir estes nomes xa que teñen que ser nomes curtos e hai moitos caracteres inválidos.

• [Configuración de Módulo](#)

**Cortafuegos Shorewall**

Shorewall versión 4.12.0

[Borrar Documento](#)

[Configurar IPFW](#) | [Inventar interfaces](#) | [Añadir una nueva zona de red](#)

Presione este botón para iniciar Shorewall con la configuración actual como orden shorewall1 -t & net.

Presione este botón para borrar que Shorewall utilice la configuración con la orden shorewall1 -t & clean.

Click this button to view Shorewall tracing information from the shorewall1 -dmpg command.

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

• [Índice de Módulo](#)

**Interfaces de Red**

En esta página, debes crear interfaces y crear una de las interfaces de red del sistema que quieras que Shorewall proteja, asociadas con la zona en la que estén conectadas. La interfaz de Shorewall 1 no ha de aparecer.

No se han definido ninguna interfaz de red.

[Añadir una nueva interfaz de red](#)

[Configurar IPFW](#) | [Comprobar el funcionamiento](#) | [Borrar limpia](#)

Presione este botón para editar masivamente el fichero /etc/shorewall/1/interfaces de Shorewall, donde están guardados los cambios de interfaz.

Click this button to view Shorewall tracing information from the shorewall1 -dmpg command.

Non hai ningunha interface. Agregamos...

• [Índice de Módulo](#)

**Crear Interfaz de Red**

Datos de la interfaz de red

|           |      |                  |     |
|-----------|------|------------------|-----|
| Interfaz: | eth0 | Miembro de zona: | wan |
|-----------|------|------------------|-----|

Definición de la interfaz de red

Opiones:

- Ninguna
- Autobridging
- Interface tiene MAC
- Interface tiene IP
- Enable anti-spoofing traffic filtering
- Report packets on broadcast
- Report packets on linklocal
- Only respond to ARP requests
- Only respond to ARP responses
- Skip interface if it has no broadcast address
- Skip interface if it has no linklayer address

Presione este botón para borrar la interfaz de red.

[Borrar](#)

[Añadir otra interfaz](#)

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**.

• [Índice de Módulo](#)

**Interfaces de Red**

En esta página, debes crear interfaces y crear una de las interfaces de red del sistema que quieras que Shorewall proteja, asociadas con la zona en la que estén conectadas. La interfaz de Shorewall 1 no ha de aparecer.

Eliminación de interfaz | Invertir ordenadas | [Añadir una nueva interfaz de red](#)

| Interfaz | Miembro de zona | Dirección de la interfaz | Opciones | Depósito | Acción |
|----------|-----------------|--------------------------|----------|----------|--------|
| eth0     | wan             | 192.168.1.10             | Ninguna  | +        | +      |
| eth1     | lan             | 192.168.1.11             | Ninguna  | +        | +      |
| eth2     | dmz             | 192.168.1.12             | Ninguna  | +        | +      |

[Borrar selección](#)

[Volver al menú principal](#)

[Regresar a lista de interfaces](#)

Presione este botón para editar masivamente el fichero /etc/shorewall/1/interfaces de Shorewall, donde están guardados los cambios de interfaz.

Click this button to view Shorewall tracing information from the shorewall1 -dmpg command.

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

• [Configuración de Módulo](#)

**Cortafuegos Shorewall**

Shorewall versión 4.12.0

[Borrar Documento](#)

[Configurar IPFW](#) | [Inventar interfaces](#) | [Añadir una nueva interfaz de red](#)

Presione este botón para iniciar Shorewall con la configuración actual como orden shorewall1 -t & net.

Presione este botón para borrar que Shorewall utilice la configuración con la orden shorewall1 -t & clean.

Click this button to view Shorewall tracing information from the shorewall1 -dmpg 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 cuestiós: 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 nalgúnha 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.

- Índice de contenido
 

### Políticas por Defecto

Esta páxina permite configurar las acciones para devolver pa el tráfico entre zonas diferentes del cortafuegos. Pueden ser prioritarias para controlar tráfico en tipos de tráfico en la página de reglas del Cortafuegos.

También nos se ha definido ninguna política por defecto.

Añadir una nueva política por defecto

[Editar el Fichero de Manuscritos](#)

[Añadir otra política por defecto](#)

[Regresar a la lista de políticas](#)

Non hai políticas definidas. Agregamos unha.

- Índice de contenido
 

### Creación de Política por Defecto

Detalles de la política por defecto

Zona origen:

Zona destino:

Nivel de syring:

Límite de tráfico:

[Añadir otra política por defecto](#)

[Regresar a la lista de políticas](#)

As políticas simplemente teñen unha zona orixe, unha zona de destino e unha acción a tomar. Por exemplo, neste caso estamos dicindolle 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.

- Índice de contenido
 

### Políticas por Defecto

Esta páxina permite configurar las acciones para el tráfico entre zonas diferentes del cortafuegos. Pueden ser prioritarias para controlar tráfico en tipos de tráfico en la página de reglas del Cortafuegos.

| Zona origen | Zona destino | Política | Nivel de syring | Límite de tráfico | Desplazar | Altida |
|-------------|--------------|----------|-----------------|-------------------|-----------|--------|
| Outras      | wan          | ACEPT    | Ninguna         | Ninguna           | 4         | T_A    |
| Outras      | Exterior     | RECH     | Ninguna         | Ninguna           | 9         | F_A    |

[Añadir otra política por defecto](#)

[Regresar a la lista de políticas](#)

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 rexítase. 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 abaxo. Por exemplo, se neste caso situásemos a segunda regra como primeira, executaríase sempre, xa que encaixa con calquera tráfico.



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

- Índice de contenido
 

### Reglas del Cortafuegos

Este tablo lista las excepciones de las políticas por defecto para cierto tipo de tráfico, reglos, o directorios. La acción tomada se aplica a los paquetes que coinciden con los criterios establecidos en cada una de las políticas por defecto.

Añadir una nueva regla del cortafuegos

[Añadir otra política por defecto](#)

[Regresar a la lista de políticas](#)

Agregamos unha nova regra.

- Índice de contenido
 

### Creación de Regla del Cortafuegos

Detalles de la regla del cortafuegos

Acción:

Zona origen:

Zona destino:

Sobre las rules de la zona con:

Protocolo:

Puertos de origen:

Puertos destino:

Para el DNAT o REDIRECT, seleccione la ruleta desinversa en puertos de destino:

Para el DNAT o REDIRECT, seleccione la ruleta desinversa en puertos de destino:

[Añadir otra regla del cortafuegos](#)

Como podemos ver, as regras ofrecen criterios moi más específicos para poder indicar á devasa que tipo de tráfico se debe aceptar e cal non (protocolo, IP de orixe e destino, porto de orixe e destino, etc.). Con este regra indicámoslle que acepte o tráfico que vaia ao propio equipo con protocolo TCP ao porto 10000 (que é o porto no que corre o webmin).

| Acción | Origen   | Destino           | Protocolo | Prioridad del origen | Puertos destino | Regras | Acción |
|--------|----------|-------------------|-----------|----------------------|-----------------|--------|--------|
| ACCEPT | Zona lan | Zona dmz          | TCP       | Coste 1              | 10000           | +      | Y ↴    |
| ACCEPT | Zona lan | Rest 251.168.0/24 | TCP       | Coste 1              | 22              | +      | Y ↴    |
| ACCEPT | Coste 1  | Zona dmz          | TCP       | Coste 1              |                 | +      | Y ↴    |
| DENY   | Todos    | Todos             | Todos     | Coste 10000          |                 |        |        |

Podemos deixar estas regras: Permitimos o acceso ao webmin, os *pings* dende a *lan* á *dmz* e acceder dende a *lan* ao porto 22 da máquina *dserver3*. En función dos servizos que quixésemos ter accesibles nos servizos da *DMZ* dende a *lan* ou dende Internet iríamos engadindo máis regras. A orde nas regras tamén é moi importante, áinda que neste caso non se solapan unhas coas outras.

Por fin!! Xa podemos iniciar a devasa (Agora se se cometeu algún erro na configuración a devasa non arrancará, neste caso revisese as zonas, interfaces, políticas e regras definidas).

Aplica la Configuración: Presione este botón para activar la configuración actual de Shorewall con la orden shorewall11 restart.  
Reiniciar Shorewall: Presione este botón para activar los cambios de Shorewall con la orden shorewall11 refresh.  
Configuración completa: Presione este botón para limpiar el entabullado Shorewall con la orden shorewall11 clear. Esto permitirá el acceso desde todos los hosts sin ningún tipo de restricción.  
Opciones de Consultas: Presione este botón para usar Shorewall con la orden shorewall11 vifstat.  
PROVISIÓN DE RED: Presione este botón para usar Shorewall con la orden shorewall11 statif.  
Comprobación de Consultas: Presione este botón para hacer que Shorewall valide la configuración con la orden shorewall11 check.  
Estado Cambio: Clique en este botón para ver Shorewall having information from the shorewall11 dump command.

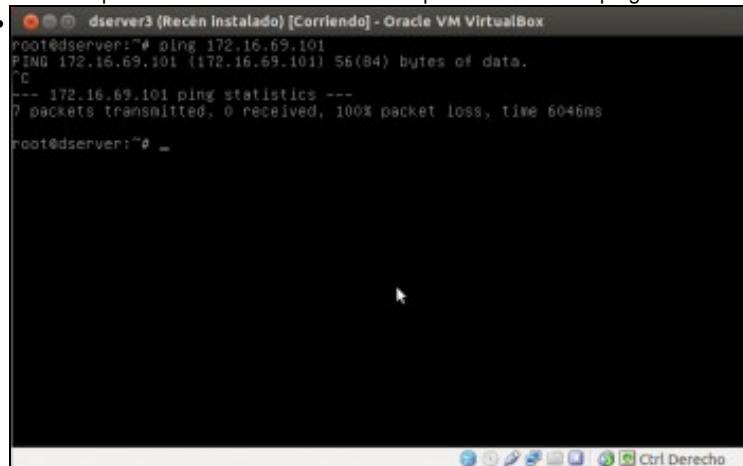
As opcións que aparecen agora de manexo da devasa indican que está iniciado.

```
● 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=1.00 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 = 0.854/1.227/1.681/0.375 ms
administrador@uclient:~$ 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.

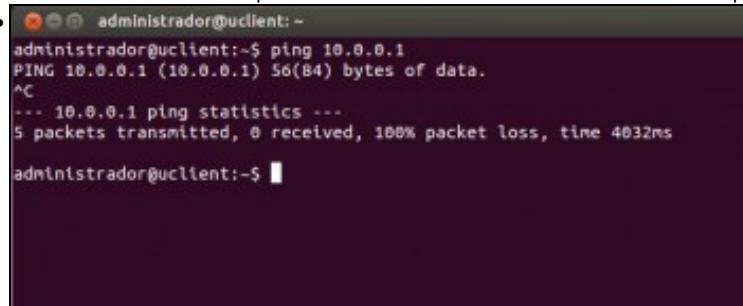
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Apr 12 00:21:06 2013 from 172.16.69.101
root@dserver:~#
```

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

- 

```
root@dserver:~# 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@dserver:~#
```

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

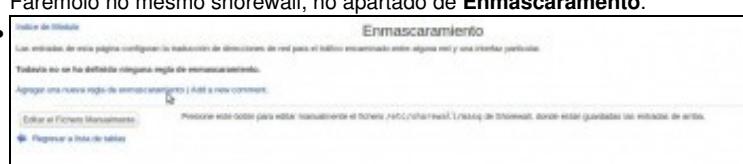
- 

```
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*.



Farémoslo no mesmo shorewall, no apartado de Enmascaramento.

- 

| Regla de destino | Red a enmascarar | Dirección SNAT | Restricciones | Restricciones de porta | Opciones |
|------------------|------------------|----------------|---------------|------------------------|----------|
| eth0 en destino  |                  |                |               |                        |          |

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

- 

**Crear de Regla de Enmascaramiento**

Datos de la regla de enmascaramiento

Interfaz de salida:  Sobre para el destino:  eth0  Sobre en la interfaz:  eth1 Excepción:  las redes:

Dirección SNAT:  Ninguna  Any protocol  TCP  All ports  Defecto

Restricciones:  Restricciones de porta:

Opciones:  Repetir la lista de enmascaramiento

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.

- 

| Regla de destino | Red a enmascarar | Dirección SNAT | Restricciones | Restricciones de porta | Opciones |
|------------------|------------------|----------------|---------------|------------------------|----------|
| eth0 en destino  |                  |                |               |                        |          |
| eth1 en destino  |                  |                |               |                        |          |

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/mdev = 2.42/11.493/28.565/9.072 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/mdev = 72.628/74.452/76.155/1.476 ms
administrador@uclient:~$
```

Agora si!! Xa temos os dous problemas resoltos.

- 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 dunha máquina da *DMZ*. Imos coller o servizo de ssh de *dserver3*:

- Reenvío de portos coa MV Debian

• [Índice de Módulos](#)

**Detalles de la regla del cortafuegos**

Servicio: **ACCEPT** y **gratuito a nivel synseq <No gratuito>**

Zona origen: **lan**

Zona destino: **dmz**

Protocolo: **TCP**

Puertos de origen: **22222**

Puertos destino: **22**

Dirección de destino original para DNAT o REDIRECT:

Espacios de dirección de trascendencia:

La regla se aplica al conjunto de usuarios:

**Guardar**

[Regresar a la lista de reglas del cortafuegos.](#)

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

• [Índice de Módulos](#)

**Creación de Regla del Cortafuegos**

**Detalles de la regla del cortafuegos**

Servicio: **ACCEPT** y **gratuito a nivel synseq <No gratuito>**

Zona origen: **lan**

Zona destino: **dmz**

Protocolo: **TCP**

Puertos de origen: **22222**

Puertos destino: **22**

Dirección de destino original para DNAT o REDIRECT:

Espacios de dirección de trascendencia:

La regla se aplica al conjunto de usuarios:

**Crear**

[Regresar a la lista de reglas del cortafuegos.](#)

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 do *dserver2* que será redirixido ao servidor ssh de *dserver3*).

• [Índice de Módulos](#)

**Reglas del Cortafuegos**

Este tablón lista las excepciones de las políticas por destino para cierto tipo de tráfico, origen, o destino. La acción correspondiente se aplicará a los paquetes que coincidan con las condiciones establecidas en cada fila de la política por orden:

Dar clic sobre cada fila para editar manualmente el filtro /etc/shorewall/rules de Shorewall, donde están guardados los entradas de filtro.

| Acción  | origen   | destino                             | Protocolo | Puertos de origen | Espacios destino | Destino | Adición |
|---------|----------|-------------------------------------|-----------|-------------------|------------------|---------|---------|
| Denegar | Zona wan | Host 192.168.69.2-31 de la zona dmz | TCP       | Calquera          | 22222            | +       | Y L     |
| ACCEPT  | Calquera | Host 192.168.69.2 de la zona dmz    | TCP       | Calquera          | 22               | +       | Y L     |
| ACCEPT  | Zona lan | Zona dmz                            | ICMP      | Calquera          | +                | +       | Y L     |
| ACCEPT  | Calquera | Zona dmz                            | TCP       | Calquera          | 60000            | +       | Y L     |

**Desactivar todo | Iniciar selección | Agrega una nueva regla del cortafuegos | Añadir a lista de cambios**

**Editar en Filtros Manualmente**

Posicione este botón para editar manualmente el filtro /etc/shorewall/rules de Shorewall, donde están guardados los entradas de filtro.

[Regresar a la lista de tablas](#)

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

```
• administrador@portatil17: ~
administrador@portatil17:~$ ssh -p 22222 root@10.1.69.1
root@10.1.69.1'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 00:35:35 2013 from 10.0.0.2
root@dserver:~# ifconfig eth0
eth0 Link encap:Ethernet HWaddr 08:00:27:52:c0:54
 inet addr:192.168.69.2 Bcast:192.168.69.255 Mask:255.255.255.252
 inet6 addr: fe80::a00:27ff:fe52:c054/64 Scope:Link
 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
 RX packets:337 errors:0 dropped:0 overruns:0 frame:0
 TX packets:420 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:1000
 RX bytes:38038 (37.1 Kib) TX bytes:82602 (80.6 Kib)

root@dserver:~#
```

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 --