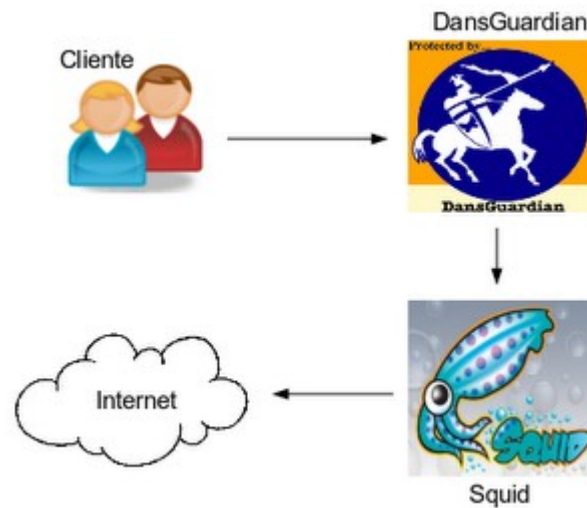


Servidor proxy-caché transparente





jamj2000 at gmail dot com

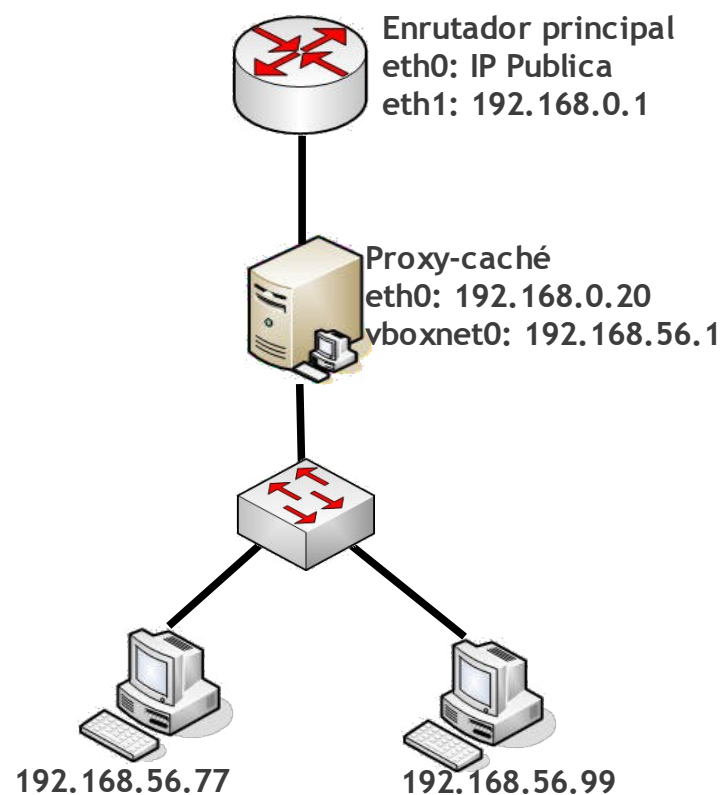
Índice de contenido

| | |
|--|----|
| Introducción..... | 3 |
| Objetivo..... | 4 |
| Recursos..... | 4 |
| Software..... | 5 |
| Montando la red local virtual..... | 6 |
| Configuración dinámica de red para clientes..... | 9 |
| Configuración de SQUID..... | 12 |
| Probando SQUID de forma no transparente..... | 14 |
| Configuración de DANSGUARDIAN..... | 16 |
| Configuración de SARG..... | 20 |
| Configuración del cortafuegos..... | 23 |
| Probando el resultado final | 26 |

INTRODUCCIÓN

Este documento pretende ser un mini-tutorial para el montaje de un proxy-caché transparente para una red local. No se pretende entrar en detalle en cada una de las opciones de configuración que pueden utilizarse, sino más bien servir de orientación en los pasos principales de su puesta en funcionamiento.

La red local quedará estructurada de la siguiente forma (Modelo simplificado):



El software utilizado ha sido el siguiente:

Ubuntu 10.10 Desktop

iptables 1.4.4

Squid 2.7.STABLE9

Dansguardian 2.10.1.1

Sarg 2.2.7.1

Webmin 1.530

dnsmasq 2.55

Para realizar las pruebas no es necesario disponer de una red local real. Para realizar esta documentación se ha hecho uso de una red simulada. Utilizando VirtualBox PUEL (Personal Use and Evaluation License) 3.2.10.

OBJETIVO

Cuando finalicemos este mini-tutorial deberías haber conseguido tener tu proxy-caché configurado bloqueando ciertos sitios indeseados y además dispondrás de un generador de informes que te permitirá comprobar que páginas visita cada usuario.

RECURSOS

Vamos a necesitar muy pocos recursos. Poquísimos. Antes de empezar necesitaras tener un equipo con **Ubuntu instalado** y cuenta de administrador. Otra distribución podría valer, pero deberas de realizar las modificaciones oportunas.

Ademas debes de tener **conexión a Internet**. Eso es todo.

SOFTWARE

Para ciertas operaciones utilizaremos un **terminal**. Puedes utilizar el que viene en Aplicaciones → Accesorios → Terminal. Dentro de él trabajaremos como administrador. Para ello escribe el comando **sudo su**, e introduce tu clave. En el indicador del sistema deberá aparecer el carácter almohadilla **#**. Si te aparece el dólar **\$** es que sigues como usuario sin privilegios.

Para establecer las reglas del cortafuegos necesitaremos el paquete **iptables**. Normalmente todas las distribuciones Linux vienen con él. Podemos comprobar si disponemos de él escribiendo dicho comando y pulsando intro. Si nos aparece un mensaje semejante a

```
iptables v1.4.4: no command specified
Try `iptables -h' or 'iptables --help' for more information.
```

entonces tenemos la versión 1.4.4.

Como software de proxy-caché utilizaremos **squid** y **dansguardian**. Este último trabaja sobre squid y proporciona control por contenido y posee extensas listas negras.

Por último necesitaremos el paquete **sarg** que nos permitirá generar informes de los accesos de los usuarios.

Para instalar estos paquetes escribimos en el terminal (como administrador):

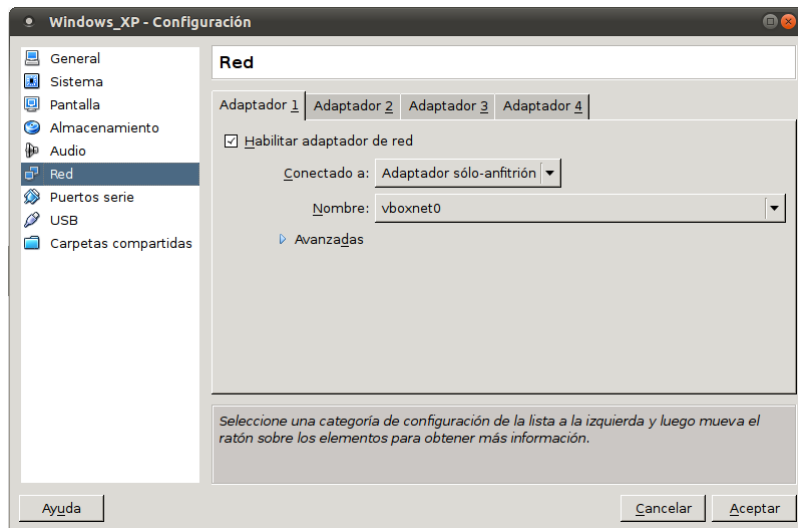
```
apt-get install iptables squid dansguardian sarg
```

Además necesitaremos los paquetes **VirtualBox** y **Webmin**. El primero nos permitirá crear una red local virtual con uno o varios equipos detrás de nuestro proxy-caché. El segundo nos permite administrar el proxy de forma cómoda a través de web.

Para la instalación de estos paquetes he recurrido a los sitios oficiales donde disponen de paquetes .deb adecuados para distribuciones basadas en Debian como Ubuntu.

MONTANDO LA RED LOCAL VIRTUAL

Una vez instalado todo el software anterior procederemos a configurar nuestra red virtual. Para ello bastará con ejecutar VirtualBox y instalar al menos una máquina virtual. En este caso he instalado Windows XP. La interfaz de red deberá configurarse como **Adaptador sólo-anfitrión**. Ello añadirá a nuestro Ubuntu una interfaz **vboxnet0** con la cual nos comunicaremos con las máquinas virtuales detrás del proxy.



Bueno, se supone que ya has instalado Windows XP y establecido el tipo de adaptador.

Antes de iniciar Windows XP deshabilitamos el servidor DHCP que proporciona VirtualBox. Esto es necesario puesto que puede interferir posteriormente con nuestro cortafuegos. No tenga muy claro porque es así, pero en mis prueba he tenido que deshabilitarlo.

Para ello escribimos en el terminal.

VBoxManage dhcpserver remove --ifname vboxnet0

Para hacer NAT por la interfaz externa:

```
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

o

```
iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to-source 192.168.0.20
```

NOTA: Este comando debemos ejecutarlo desde el mismo usuario con el cual ejecutamos VirtualBox.

Una vez iniciado Windows XP configuramos la conexión de red de forma manual. Por ejemplo:

IP: 192.168.56.77

Máscara: 255.255.255.0

Puerta de enlace: 192.168.56.1

CURIOSIDAD: Desde una ventana de MS-DOS podemos establecer la puerta de enlace por defecto con el comando

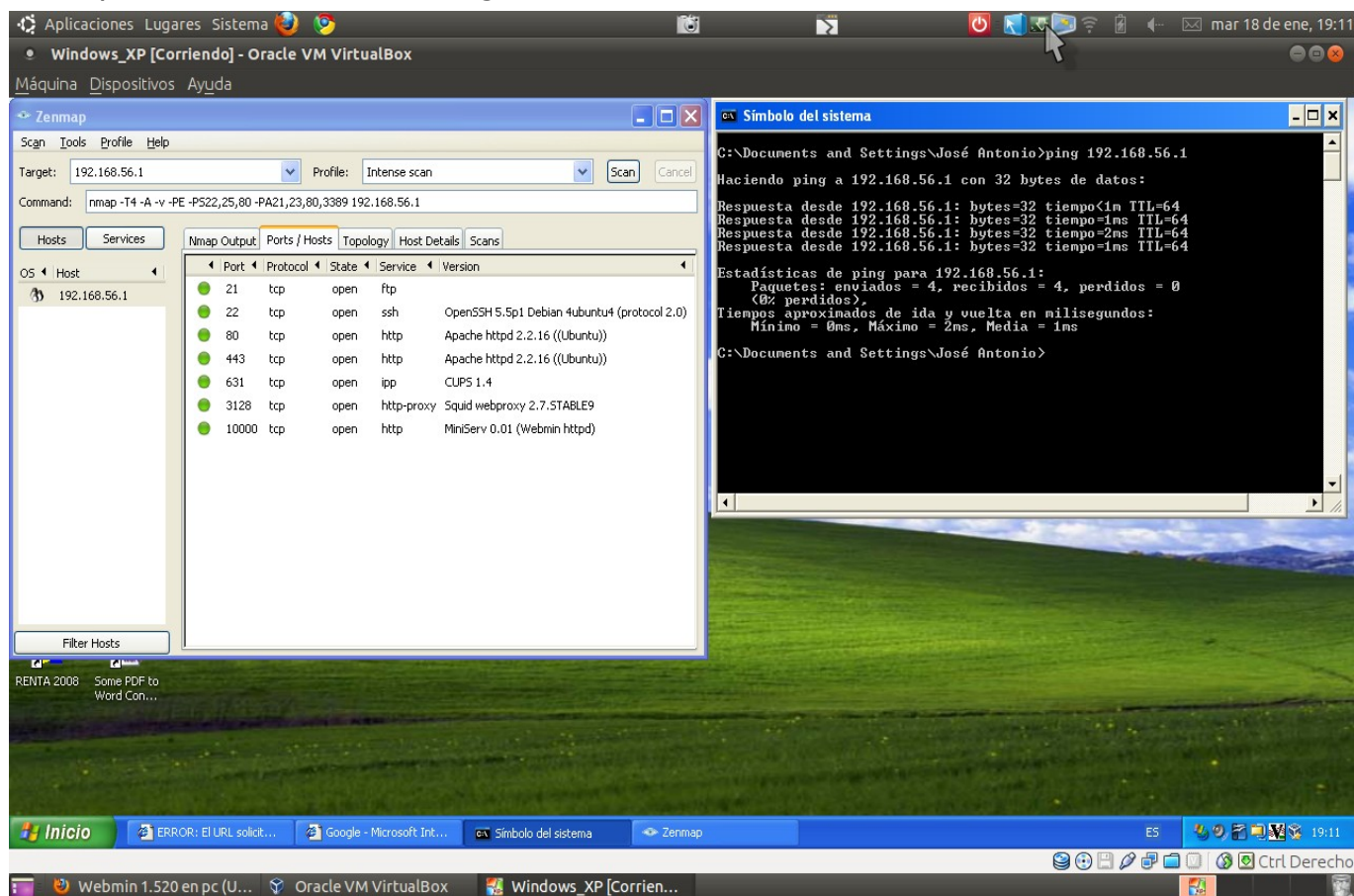
```
route add 0.0.0.0 mask 0.0.0.0 192.168.56.1 -p
```

Una vez hecho todo lo anterior comprobamos que tenemos conexión desde Windows XP a Ubuntu (nuestro proxy). Para ello bastará con escribir en el terminal de MS-DOS el comando

```
ping 192.168.56.1
```

Servidor proxy-caché transparente 8 / 27

Se muestra en la parte derecha de la imagen.



En la parte izquierda he utilizado un escáner de puertos (Zenmap) para ver los puertos que tiene abiertos el proxy Ubuntu. Esto último no es necesario que lo hagas.

CONFIGURACIÓN DINÁMICA DE RED PARA CLIENTES

Si en lugar de disponer de un equipo cliente disponemos de muchos equipos, la configuración de los parámetros de red para los equipos de la red local se vuelve muy tediosa.

Para mejorar esta situación es altamente recomendable disponer en nuestro proxy de un servicio DHCP (y si además tenemos DNS mejor). Para este cometido lo mejor es utilizar el servidor DNSMASQ.

Instalamos dicho servidor:

```
apt-get install dnsmasq
```

Y copiamos el siguiente contenido en el archivo `/etc/dnsmasq.conf`:

```
domain=midominio.net
interface=vboxnet0

# Opciones para un mejor funcionamiento
#-----
domain-needed
# bogus-priv
# bogus-nxdomain=64.94.110.11
expand-hosts

# Otras opciones de DHCP
#-----
dhcp-authoritative
#dhcp-range=192.168.56.10,192.168.56.100,255.255.255.0,12h
dhcp-option=option:router,192.168.56.1
dhcp-option=option:dns-server,192.168.56.1
```

```
dhcp-range=192.168.56.0,static
dhcp-host=windows,192.168.56.11,12h
#dhcp-host=00:11:22:33:44:55,windows,192.168.3.11,12h

# Alias, Original
#-----
cname=cliente.midominio.net,windows.midominio.net
cname=win.midominio.net,windows.midominio.net
cname=servidor.midominio.net,pc.midominio.net
cname=ubuntu.midominio.net,pc.midominio.net
```

Esto indica que el servicio dnsmasq atenderá peticiones en la interfaz vboxnet0 y asignara el dominio “midominio.net” a los clientes. Establece la ruta por defecto y el servidor DNS para los clientes.

La línea

```
dhcp-host=windows,192.168.56.11,12h
```

es importante pues indica que al equipo cuyo nombre es “windows” le asignaremos la IP 192.168.56.11 por 12 horas. Previamente deberemos haber establecido el nombre de dicho equipo. Esto lo hacemos para dar siempre la mismas IP al mismo equipo y tener controlados a los clientes. Necesitamos una línea semejante a esta por cada equipo.

Podemos hacer lo mismo teniendo en cuenta la dirección MAC de la tarjeta de red:

```
dhcp-host=00:11:22:33:44:55,windows,192.168.3.11,12h
```

Si no nos importa qué IP recibe cada equipo entonces en lugar de

```
dhcp-range=192.168.56.0,static
```

escribimos

```
dhcp-range=192.168.56.10,192.168.56.100,255.255.255.0,12h
```

En este caso no necesitaríamos líneas “dhcp-host”

Además en el archivo **/etc/resolv.conf** del servidor deberemos poner las siguientes líneas:

```
domain midominio.net
```

```
search midominio.net
```

```
nameserver 127.0.0.1
```

```
nameserver 192.168.0.1
```

```
nameserver 80.58.0.33
```

Las 3 primeras líneas permiten al servidor resolver los nombres de la red local con su propio DNS. El resto de líneas son los DNS upstream.

CONFIGURACIÓN DE SQUID



SQUID es el proxy-caché propiamente dicho. Además nos proporciona una caché en disco donde va guardando todas las páginas visitadas para que así no tengan que volver a pedirse a Internet la próxima vez. Esto reduce el tráfico con el exterior y nos permite aprovechar mejor nuestro ancho de banda.

Aunque es posible configurarlo a través de Webmin, probablemente resulte más sencillo si abrimos el archivo de configuración y lo editamos a mano. Para ello te recomiendo copies y pegues las siguientes líneas dentro de

/etc/squid/squid.conf

```
http_port 3128 transparent
cache_mem 256 MB
cache_dir ufs /var/spool/squid 10000 16 256
maximum_object_size 800000 KB

visible_hostname proxy

cache_access_log /var/log/squid/access.log

offline_mode on
ie_refresh on

error_directory /usr/share/squid/errors/es

acl all src 0.0.0.0/0.0.0.0
acl localhost src 127.0.0.1/255.255.255.255
acl localnet src 192.168.56.0/255.255.255.0
acl multimedia url_regex youtube.com video.google tu.tv
acl juegos url_regex minijuegos juegos.com juegosjuegos.com
acl mensajerias url_regex ebuddy.com meebo.com tuenti e-messenger
acl pornografia url_regex sextv pornotube putas mocrosoftx
acl varios url_regex sexyono votamicuerpo forocoches meristation.com

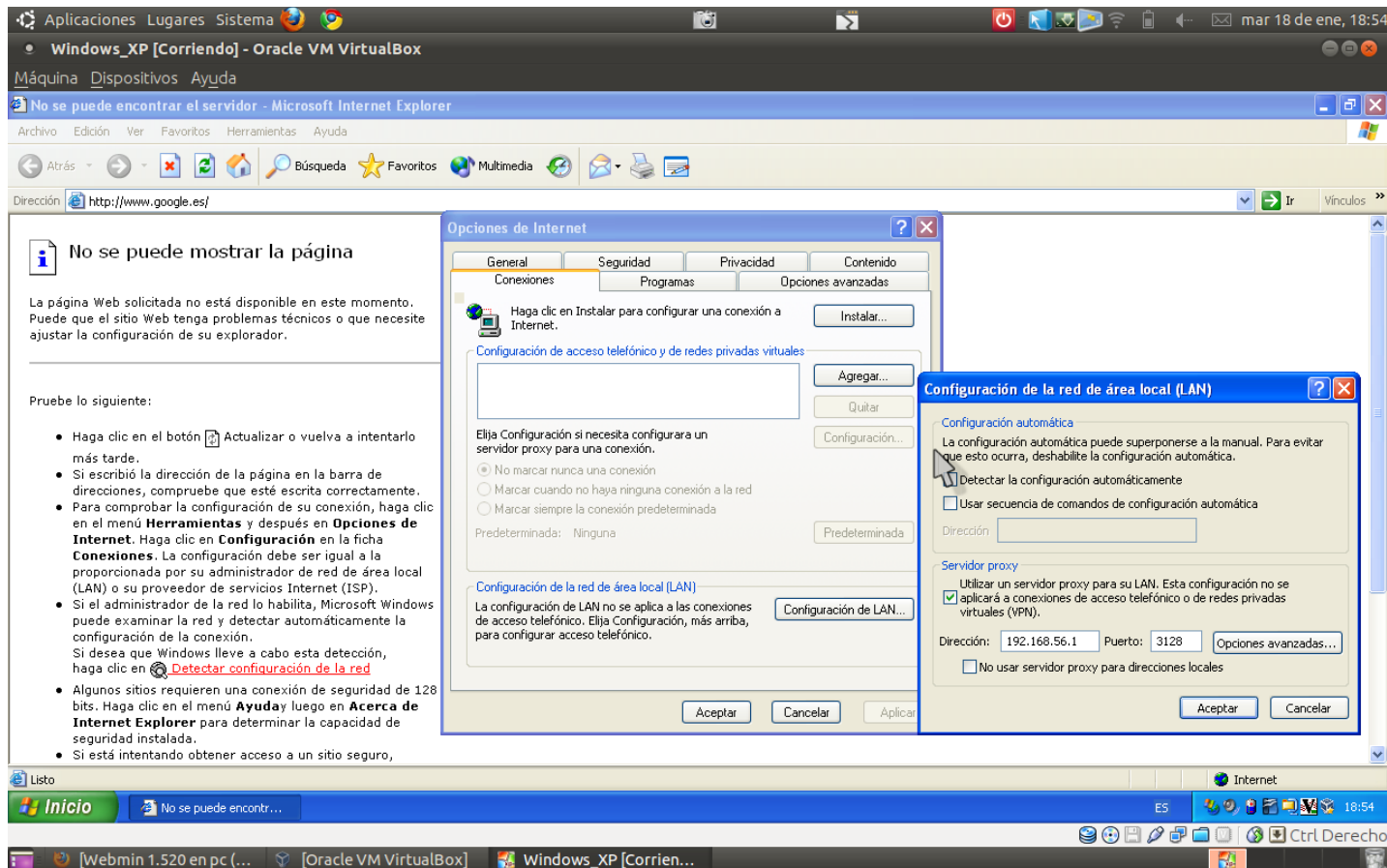
http_access deny multimedia
http_access deny juegos
http_access deny pornografia
http_access deny mensajerias
http_access deny varios
http_access allow localhost
http_access allow localnet
http_access allow all
```

Mediante Webmin podemos iniciar y parar de forma sencilla el proxy-caché.

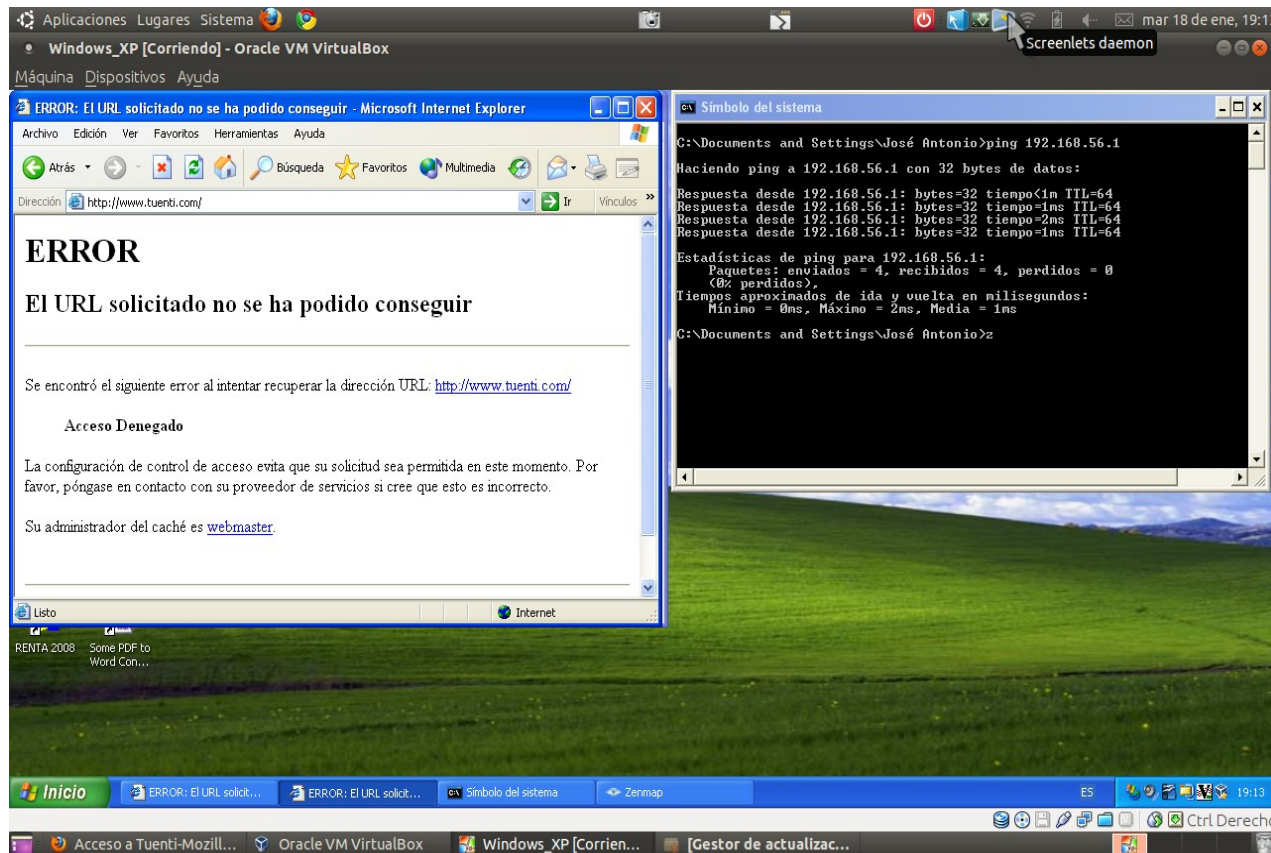
NOTA: SQUID no iniciará si no dispones de una conexión a Internet.

PROBANDO SQUID DE FORMA NO TRANSPARENTE

Si SQUID ha iniciado de forma correcta, podemos probar a navegar desde Windows XP. Si intentamos acceder a internet en este momento comprobaremos que no podemos. Esto es debido a que SQUID atiende las peticiones en el puerto 3128 y los navegadores hacen peticiones de páginas web al puerto 80.



A estas alturas aún no disponemos de un proxy transparente. Por tanto para probar deberemos configurar el navegador de los equipos que se hallan detrás del proxy. Como comprenderás esto no es una muy buena técnica, sobre todo si disponemos de muchos equipos. No obstante nosotros lo probaremos para mostrar con se configuran los clientes cuando disponemos de un proxy no transparente. En Internet Explorer, vamos al menú Herramientas → Opciones de Internet. Luego pulsamos en la pestaña Conexiones y después en el botón Configuración de LAN... Marcamos la casilla del Servidor proxy tal como aparece en la imagen.



Una vez realizados los pasos anteriores, si todo ha ido bien, podremos navegar. Algunos sitios serán denegados por SQUID. En la configuración que presentamos en el apartado anterior estaban denegadas URLs como youtube.com, minijuegos o tuenti.com. Por tanto estos sitios no podremos verlos.

Una vez probado el proxy no transparente dejamos el navegador como estaba al principio y seguimos con este tutorial.

CONFIGURACIÓN DE DANSGUARDIAN



Antes de configurar el cortafuegos para tener un proxy transparente, configuraremos DANSGUARDIAN y SARG y dejaremos para el final la configuración del cortafuegos.

DANSGUARDIAN nos añade funcionalidad y sobre todo una gestión de las listas negras más cómoda.

DANSGUARDIAN atiende peticiones en el puerto 8080 y funciona sobre SQUID.

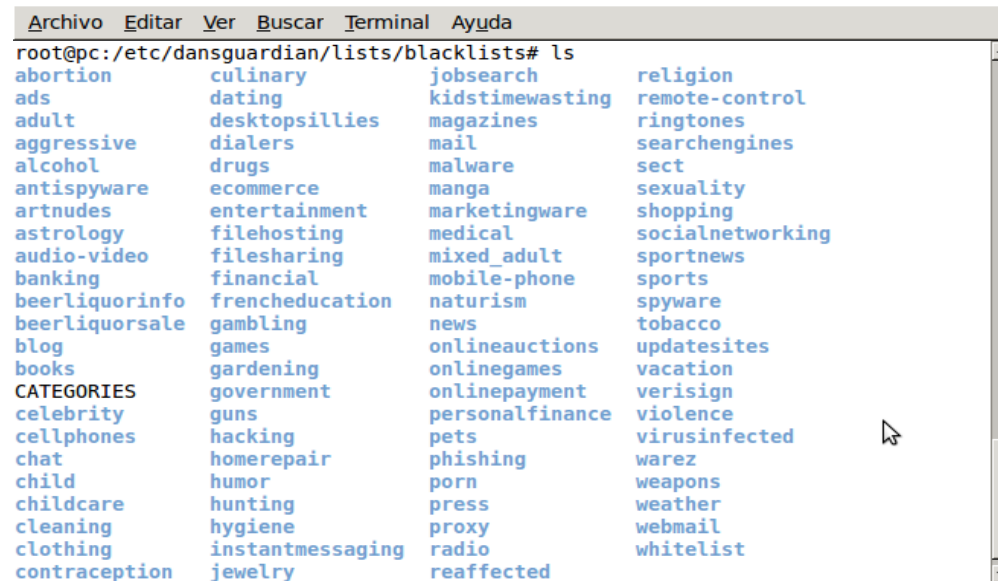
Cuando instalamos dansguardian apenas tenemos listas negras.

Podemos descargar una muy completa (`bigblacklist.tar.gz`) desde <http://urlblacklist.com/?sec=download>

Una vez descargada la guardamos en el directorio adecuado. Para ello ejecutamos en un terminal como administrador:

```
cp bigblacklist.tar.gz /etc/dansguardian/lists
cd /etc/dansguardian/lists
tar zxvf bigblacklist.tar.gz
```


Esto descomprimirá dentro de /etc/dansguardian/lists/blacklists un mogollón de listas clasificadas por temática. Ten en cuenta que, aunque el directorio se llame blacklists, no todas las listas que aparecen aquí son negras.



```
root@pc:/etc/dansguardian/lists/blacklists# ls
abortion      culinary      jobsearch    religion
ads           dating       kidstimestwasting  remote-control
adult         desktopsillies  magazines    ringtones
aggressive    dialers       mail         searchengines
alcohol       drugs         malware      sect
antispymware  ecommerce    manga        sexuality
artnudes      entertainment  marketingware shopping
astrology     filehosting   medical      socialnetworking
audio-video   filesharing   mixed_adult  sportnews
banking        financial     mobile-phone sports
beerliquorinfo  frencheducation naturism     spyware
beerliquorsale  gambling      news         tobacco
blog           games         onlineauctions updatesites
books          gardening     onlinergames vacation
CATEGORIES     government    onlinepayment verisign
celebrity      guns          personalfinance violence
cellphones     hacking       pets          virusinfected
chat           homerepair    phishing      warez
child          humor         porn          weapons
childcare      hunting       press         weather
cleaning       hygiene       proxy         webmail
clothing       instantmessaging radio         whitelist
contraception  jewelry       reaffected
```

A continuación editamos el archivo /etc/dansguardian/list/bannedsitelist para bloquear el acceso a ciertos sitios.

Descomentamos o añadimos las siguientes líneas para bloquear el acceso a redes sociales y sitios de mensajería instantánea:

```
.Include</etc/dansguardian/lists/blacklists/socialnetworking/domains>
```

```
.Include</etc/dansguardian/lists/blacklists/instantmessaging/domains>
```

NOTA: Es posible hacer lo mismo con las URLs mediante el archivo /etc/dansguardian/list/bannedurllist y con otros tipos de listas.

Si deseamos comprobar el contenido que se encuentra dentro de las páginas, es decir el tipo de palabras que aparecen y las veces que aparecen, podemos bloquear aquellas páginas que posean gran cantidad de palabras ofensivas.

Podemos descargar una muy completa lista de frases ofensivas (phraselistsoct23.tar.gz) desde <http://contentfilter.futuragts.com/phraselists/>

Una vez descargada la guardamos en el directorio adecuado. Para ello ejecutamos en un terminal como administrador:

```
cp phraselistsoct23.tar.gz /etc/dansguardian/lists
cd /etc/dansguardian/lists
tar zxvf phraselistsoct23.tar.gz
rm -r phraselists
mv "_current phraselists" phraselists
```

Editamos el archivo /etc/dansguardian/lists/weightedphraselist y comentamos las líneas donde aparece polish y swedish.

Al igual que hicimos con el archivo anterior, configuramos éste a nuestro gusto.

Por último para terminar con DANSGUARDIAN, instalaremos su módulo para administrador desde Webmin.

Podemos descargar el modulo para webmin (dgwebmin-0.7.1.wbm) desde <http://sourceforge.net/projects/dgwebminmodule/files/dgwebmin-stable/0.7/dgwebmin-0.7.1.wbm>

Este módulo posee una configuración de caminos no adecuada para Ubuntu. Para arreglar este problema pulsa en la parte izquierda en DansGuardian Filtro de Contenido y a continuación en el cuadro de la derecha en la esquina superior izquierda en Configuración de Modulo.

Establece los caminos tal como aparecen en la imagen inferior.

Configuración

Para el módulo DansGuardian Filtro de Contenido Web

Opciones configurables para DansGuardian Filtro de Contenido Web

| | |
|---|---------------------------|
| Full camino a la DG de configuración (etc) directorio | /etc/dansguardian |
| Full camino a la DG archivo pid | /var/run/dansguardian.pid |
| Full camino a la DG binario | /usr/sbin/dansguardian |
| Full camino a la DG de registro de directorio | /var/log/dansguardian |
| Full camino a la DG de mensajes de archivo (o literal "followDansGuardian") | followDansGuardian |

Format de la Dirección General de 'log'

☒ followDansGuardian
☐ DG vigor nativo
☐ CSV vigor
☐ Calamar vigor nativo (no de análisis de registro)
☐ fuerza delimitada por tabuladores

Command para reiniciar la Dirección General (si se permite)

☐ módulo incorporado en el sistema
☒ /etc/init.d/dansguardian rest

Auto reiniciar la Dirección General según sea necesario (si lo permite)

☒ explícito manual de reiniciar sólo
☐ reinicie automáticamente
☐ módulo incorporado en el sistema
☐ /etc/init.d/dansguardian star

Command para iniciar la DG (si se permite)

/etc/init.d/dansguardian star

Command para poner fin a la Dirección General (si se permite)

☐ módulo incorporado en el sistema
☒ /etc/init.d/dansguardian stop

Auto recargar la DG grupos

1 1-recarga automáticamente

Include "fijos" listas (blacklists/phraselists/etc.) muestra en

☒ excluir "fijos" listas de pantalla
☐ pantalla "fijos" listas

Salvar

[Regresar a índice](#)

CONFIGURACIÓN DE SARG

SARG (Squid Analysis Report Generator) es un generador de informes para SQUID. Pero nosotros lo vamos a adaptar para generar informes para DANSGUARDIAN, puesto que trabajaremos principalmente con este último.

Para ello debemos de editar el archivo **/etc/sarg/sarg.conf** debes cambiar la línea

```
access_log /var/log/squid/access.log
```

por

```
access_log /var/log/dansguardian/access.log
```

Esto indica que haremos uso del registro de accesos de dansguardian en lugar del de squid como viene por defecto.

Además deberemos modificar el archivo **/etc/dansguardian/dansguardian.conf** y cambiar la línea

```
logfileformat = 0
```

por

```
logfileformat = 3
```

Esto indica que debemos registrar los accesos siguiendo el formato que emplea squid.

Para no mezclar datos de distintos formatos borramos el contenido del registro de accesos:

```
echo "" > /var/log/dansguardian/access.log
```

y borramos archivos anteriores

```
rm /var/log/dansguardian/access.log.*
```

Por último para terminar con SARG, instalaremos su módulo para administrarlo desde Webmin.

Podemos descargar el modulo para webmin (sarg.wbm.gz) desde <http://download.webmin.com/download/modules/>

Este módulo posee una configuración de caminos no adecuada para Ubuntu. Para arreglar este problema pulsa en la parte izquierda en Generador de Informes de Análisis de Squid y a continuación en el cuadro de la derecha en la esquina superior izquierda en Configuración de Modulo.

Establece los caminos tal como aparecen en la imagen inferior.

Configuración
Para el módulo Generador de Informes de Análisis de Squid

| Opciones configurables para Generador de Informes de Análisis de Squid | |
|--|---|
| Ruta completa al ejecutable sarg | <input type="text" value="/usr/bin/sarg"/> |
| Ruta complete al archivo de configuración de Sarg | <input type="text" value="/etc/sarg/sarg.conf"/> |
| Add Webmin header and footer to SARG report? | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| <input type="button" value="Salvar"/> | |

A continuación se muestra un informe de los sitios visitados por el equipo 192.168.56.11 el día 22 de Enero de 2011.

[Índice de Módulo](#)

Informe Sarg



Squid Analysis Report Generator

Squid User Access Reports

Período: 2011Jan22-2011Jan22

Usuario: 192.168.56.11

Clasificado por: BYTES, reverse

Usuario Reporte

| SITIO ACCEDIDO | CONEXION | BYTES | %BYTES | ENTRADA-CACHE-SALIDA | TIEMPO UTILIZADO | MILISEC | %HORA | |
|-------------------------------|-----------|----------------|----------------|----------------------|------------------|--------------|----------------|----------|
| googleads.g.doubleclick.net | 7 | 83.91K | 61.58% | 47.90% 52.10% | 00:00:02 | 2,115 | 31.09% | |
| iesjacs.mdl.gnomio.com | 17 | 31.95K | 23.45% | 0.73% 99.27% | 00:00:02 | 2,555 | 37.56% | |
| www.google.es | 3 | 16.24K | 11.92% | 7.58% 92.42% | 00:00:00 | 580 | 8.53% | DENEGADO |
| adblockdetector.com | 2 | 2.39K | 1.75% | 50.00% 50.00% | 00:00:00 | 891 | 13.10% | |
| tuenti.com | 1 | 1.21K | 0.89% | 100.00% 0.00% | 00:00:00 | 9 | 0.13% | DENEGADO |
| clients1.google.es | 4 | 557 | 0.41% | 0.00% 100.00% | 00:00:00 | 533 | 7.83% | |
| pagead2.googlesyndication.com | 14 | 0 | 0.00% | 0.00% 0.00% | 00:00:00 | 26 | 0.38% | |
| www.google-analytics.com | 3 | 0 | 0.00% | 0.00% 0.00% | 00:00:00 | 83 | 1.22% | DENEGADO |
| skype.com | 1 | 0 | 0.00% | 0.00% 0.00% | 00:00:00 | 2 | 0.03% | DENEGADO |
| facebook.com | 1 | 0 | 0.00% | 0.00% 0.00% | 00:00:00 | 9 | 0.13% | DENEGADO |
| TOTAL | 53 | 136.27K | 100.00% | 32.34% 67.66% | 00:00:06 | 6,803 | 100.00% | |
| PROMEDIO | 53 | 136.27K | | | 00:00:06 | 6,803 | 100.00% | |

Generado por [sarg-2.2.7.1](#) Feb-12-2010 el Jan/24/2011 20:08

CONFIGURACIÓN DEL CORTAFUEGOS

Para el correcto funcionamiento del **proxy-caché transparente** deberemos redirigir las peticiones hechas al puerto 80 hacia el puerto 8080. Por si algún cliente despistado tiene configurado el navegador para hacer peticiones al puerto 3128 deberemos redirigir también las peticiones hechas al puerto 3128 hacia el puerto 8080.

De esta forma todas las peticiones HTTP pasarán por DANSGUARDIAN. Este a su vez hará uso de SQUID, quien finalmente hará las peticiones de las páginas web.

```
iptables -t nat -A PREROUTING -i vboxnet0 -p tcp -j REDIRECT --dport 80 --to-ports 8080
iptables -t nat -A PREROUTING -i vboxnet0 -p tcp -j REDIRECT --dport 3128 --to-ports 8080
iptables-save > /etc/iptables.up.rules
```

Las 2 primeras líneas establecen el redireccionamiento de puertos en la entrada de la interfaz vboxnet0.

La última línea salva las reglas en el archivo /etc/iptables.up.rules

Para comprobar si las reglas están aplicándose hacemos un listado:

```
iptables -t nat -L
```

Y deberá aparecer una salida igual a la siguiente:

```
Chain PREROUTING (policy ACCEPT)
```

| target | prot | opt | source | destination | |
|----------|------|-----|----------|-------------|-------------------------------|
| REDIRECT | tcp | -- | anywhere | anywhere | tcp dpt:www redir ports 8080 |
| REDIRECT | tcp | -- | anywhere | anywhere | tcp dpt:3128 redir ports 8080 |

Chain OUTPUT (policy ACCEPT)

```
target    prot opt source                destination
```

Chain POSTROUTING (policy ACCEPT)

```
target    prot opt source                destination
```

Para cargar estas reglas en el inicio del sistema podemos indicarlo en el archivo **/etc/network/interfaces**

```
auto lo
iface lo inet loopback
pre-up iptables-restore < /etc/iptables.up.rules
```

IMPORTANTE:

Es necesario activar el enrutamiento interno para que los paquetes puedan viajar de una interfaz a otra. Para ello ejecutamos en el terminal:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Esto funcionará mientras esté el equipo encendido.

Para hacer este cambio permanente debe haber la siguiente línea en el archivo **/etc/sysctl.conf**:

```
net.ipv4.ip_forward=1
```


IMPORTANTE:

Es altamente recomendable configurar las interfaces de red del servidor de forma estática para no llevarnos sorpresas. Esto puede hacerse modificando el archivo **/etc/network/interfaces** de la siguiente forma:

```
auto lo
iface lo inet loopback
pre-up iptables-restore < /etc/iptables.up.rules
```

```
auto eth0
iface eth0 inet static
address 192.168.0.20
netmask 255.255.252.0
gateway 192.168.0.1
```

```
auto vboxnet0
iface vboxnet0 inet static
address 192.168.56.1
netmask 255.255.255.0
```

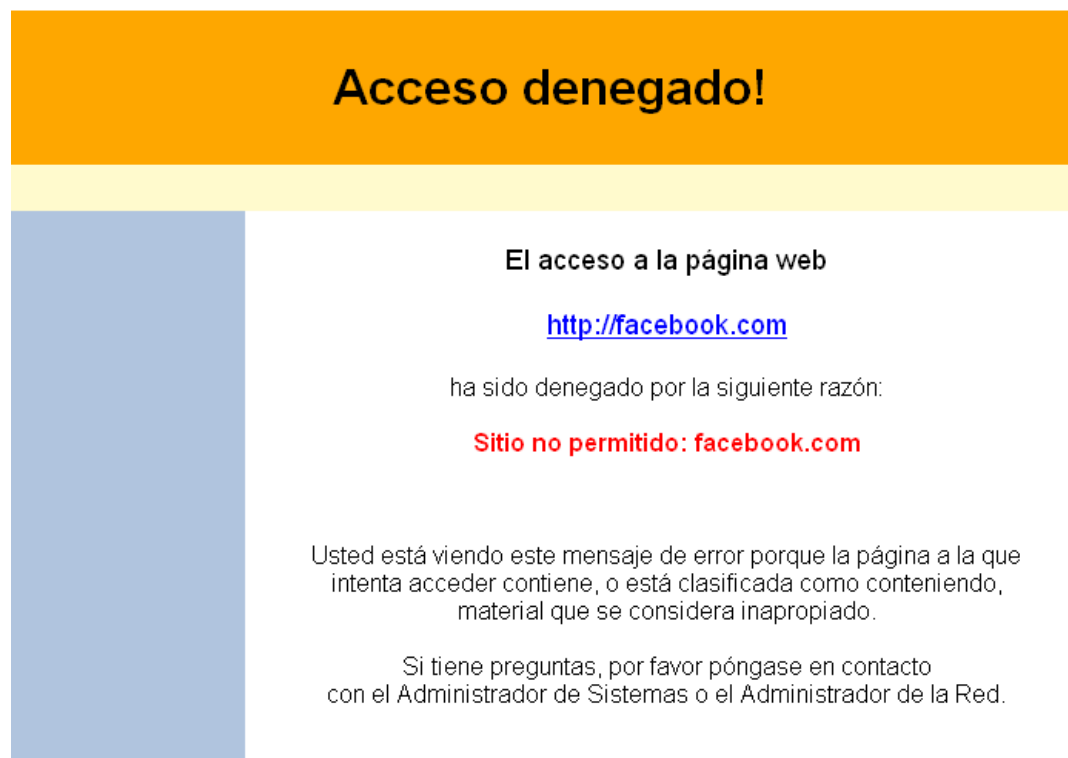
CURIOSIDAD:

Si utilizamos como cortafuegos a firestarter debemos añadir al archivo **/etc/firestarter/user-post** las siguientes reglas:

```
$IPT -t nat -A PREROUTING -i vboxnet0 -p tcp -j REDIRECT --dport 80 --to-ports 8080
$IPT -t nat -A PREROUTING -i vboxnet0 -p tcp -j REDIRECT --dport 3128 --to-ports 8080
```

PROBANDO EL RESULTADO FINAL

Página mostrada (Sitio no permitido) cuando accedemos a facebook.com desde un equipo cliente:



Y cuando accedemos a 18soon.com (Límite de ponderación de frases permitidas)

