4.14. INSTALACIÓN Y CONFIGURACIÓN DEL PROXY.

4.14.1. CONFIGURACION DEL SQUID

Primero se verfica el squid y se prueba.

```
[root@www squid]# rpm -a -q|grep squid
squid-2.6.STABLE4-1.fc6
```

Se edita el archivo squid.conf y se crean las acls de ip, debajo de la ACL ALL:

```
acl all src 0.0.0.0/0.0.0.0
acl red src "/etc/squid/lista-ips-validas"
acl negados urlpath_regex "/etc/squid/sitios-negados"
acl listaextensiones urlpath_regex "/etc/squid/listaextensiones"
```

Más abajo se permite el acceso o uso del proxy a la red definida y se niega a las otras listas (de url y de extensiones):

```
http_access allow localhost
http_access deny negados
http_access deny listaextensiones
http_access allow red
http_access deny all
```

Se activa el log para tener rastro del uso de internet.

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

Se crea el archivo de lista de extensiones

```
[root@www squid]# cat listaextensiones
.mp3$
.mp4$
.mpg$
.mpeg$
.mov$
.ra$
.ram$
.rm$
.vob$
.wma$
.wmv$
.wav$
.mbd$
```

```
.pps$
.ace$
.bat$
.lnk$
.pif$
.scr$
.sys$
.zip$
.rar$
.exe$
```

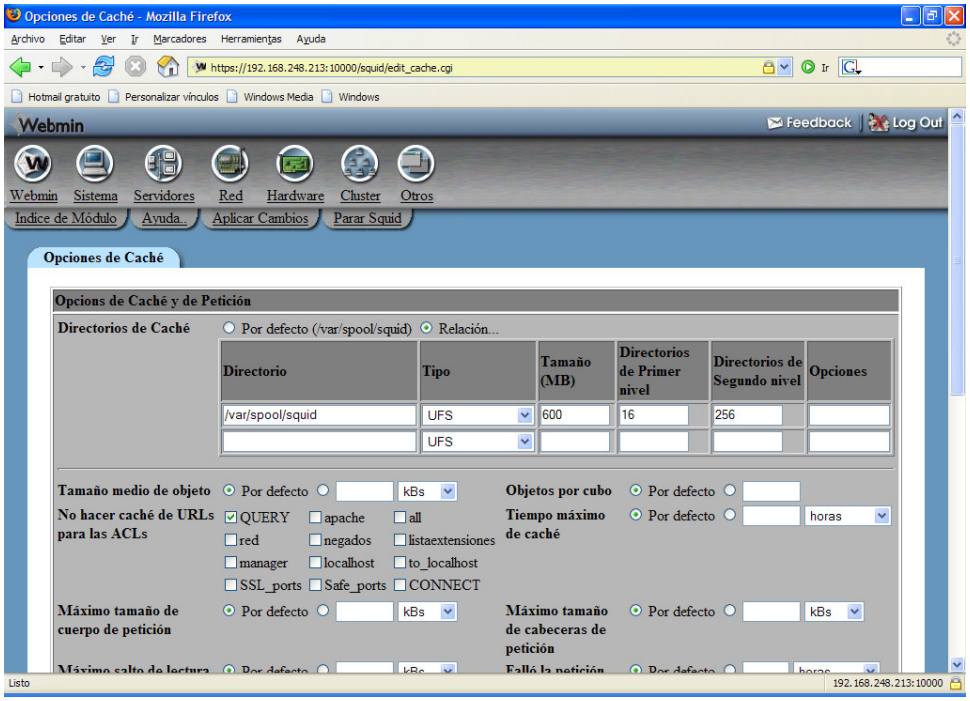
Se crea el archivo con la lista de sitios negados:

```
[root@www squid]# cat sitios-negados
http://www.playboy.com/
http://www.sexo.com/
sexo
xxx
orgia
venus
orgasmo
sex
porno
pornografia
porn
sexofree
violencia
armas
```

Se reinicia el servicio de squid.

```
[root@www squid]# service squid restart
Parando squid: .                                           [  OK  ]
Iniciando squid: .                                         [  OK  ]
[root@www squid]# service squid status
Se estÃ¡ ejecutando squid (pid 25903 25901)...
[root@www squid]#
```

Se define el cache de 600 Mb. Por webmin, servidores, squid:



Se cambia el link de los mensajes en ingles a español:

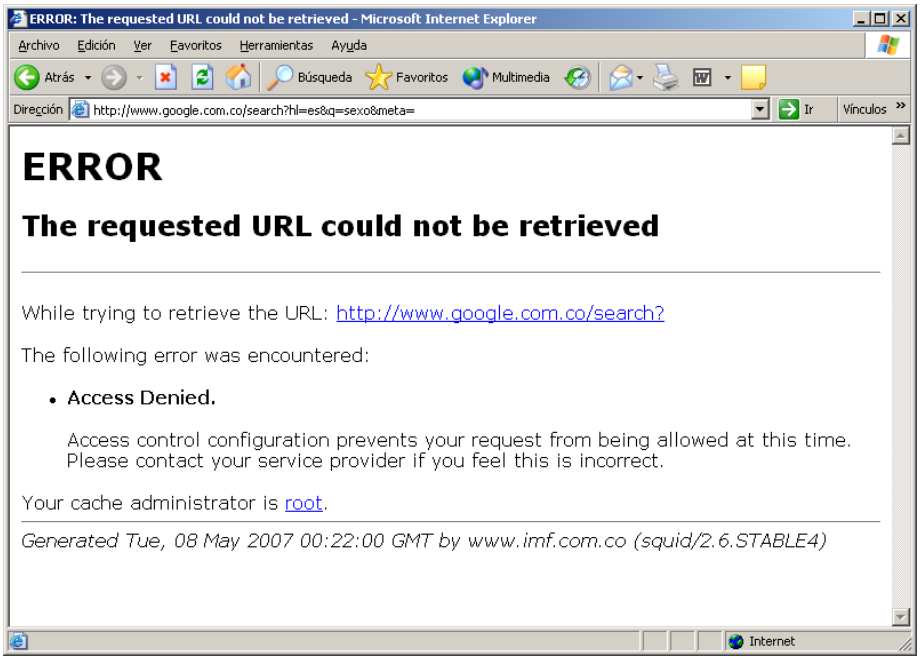
Estaba:

```
[root@www squid]# ls -l
total 464
-rw-r-----  1 root squid    367 may 16  2005 cachemgr.conf
lrwxrwxrwx  1 root root      31 ago 30 14:58 errors -> /usr/share/squid/errors/English
```

Y se cambia a:

```
[root@www squid]# unlink errors
[root@www squid]# ln -s /usr/share/squid/errors/Spanish errors
[root@www squid]# ls -l
total 404
-rw-r----- 1 root squid    419 oct  2  2006 cachemgr.conf
lrwxrwxrwx 1 root root      31 may  7 16:52 errors -> /usr/share/squid/errors/Spanish
lrwxrwxrwx 1 root root      22 abr 24 10:13 icons -> /usr/share/squid/icons
-rw-r--r-- 1 root root   27702 oct  2  2006 mib.txt
-rw-r--r-- 1 root root   11651 oct  2  2006 mime.conf
-rw-r--r-- 1 root root   11651 oct  2  2006 mime.conf.default
-rw-r--r-- 1 root root     421 oct  2  2006 msntauth.conf
-rw-r--r-- 1 root root     421 oct  2  2006 msntauth.conf.default
-rw-r----- 1 root squid 148027 oct  2  2006 squid.conf
-rw-r--r-- 1 root root  148027 oct  2  2006 squid.conf.default
[root@www squid]#
```

Se configura en el navegador el proxy y se prueba si se pueden visitar sitios prohibidos.

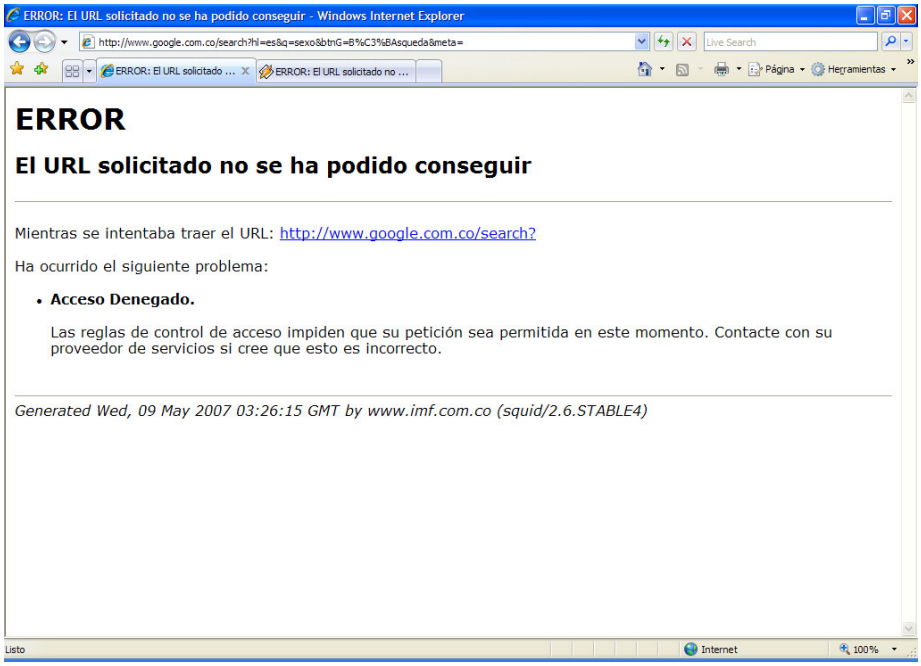


Como continuo mostrando las páginas en inglés, se creo una carpeta llamada errors, donde se copiaron los archivos con las páginas de errores en español, y se eliminó el link. Quedo:

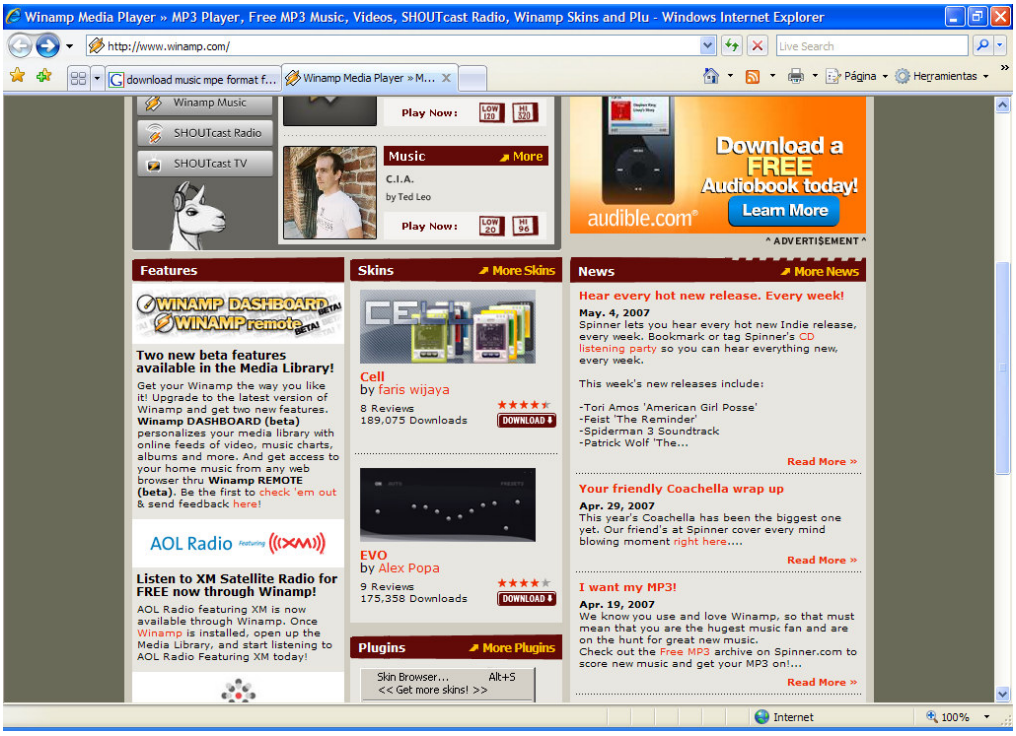
```
[root@www web]# cd /etc/squid
[root@www squid]# ls -l
```

```
total 488
-rw-r-----  1 root  squid    367 may 16  2005 cachemgr.conf
drwxr-xr-x  2 root  root    4096 abr 11 17:38 errors
lrwxrwxrwx  1 root  root      22 mar 29 15:54 icons -> /usr/share/squid/icons
-rw-r--r--  1 root  root      39 abr 10 18:09 ipvalidas
drwx------  4 squid squid   4096 abr 11 17:03 local
-rw-r--r--  1 root  root   26104 may 16  2005 mib.txt
-rw-r--r--  1 root  root   11651 may 16  2005 mime.conf
-rw-r--r--  1 root  root   11651 may 16  2005 mime.conf.default
-rw-r--r--  1 root  root     421 may 16  2005 msntauth.conf
-rw-r--r--  1 root  root     421 may 16  2005 msntauth.conf.default
-rw-r--r--  1 root  root      21 abr 10 18:11 sitiosnegados
-rw-r-----  1 root  squid 118542 abr 11 17:13 squid.conf
-rw-r--r--  1 root  root  118251 may 16  2005 squid.conf.default
-rw-r-----  1 root  root  118251 abr 10 17:48 squid.conf.ori
-rw-r--r--  1 squid squid   2904 may 31  2005 squidguard-blacklists.conf
-rw-r--r--  1 root  root    1225 abr 23  2006 squidguard.conf
-rw-r--r--  1 root  root    1515 abr 11 17:06 squidGuard.conf
-rw-r--r--  1 root  root    1225 abr 11 17:04 squidguard.conf.ori
[root@www squid]#
```

Se repite la busqueda en google de la palabra sexo y muestra:



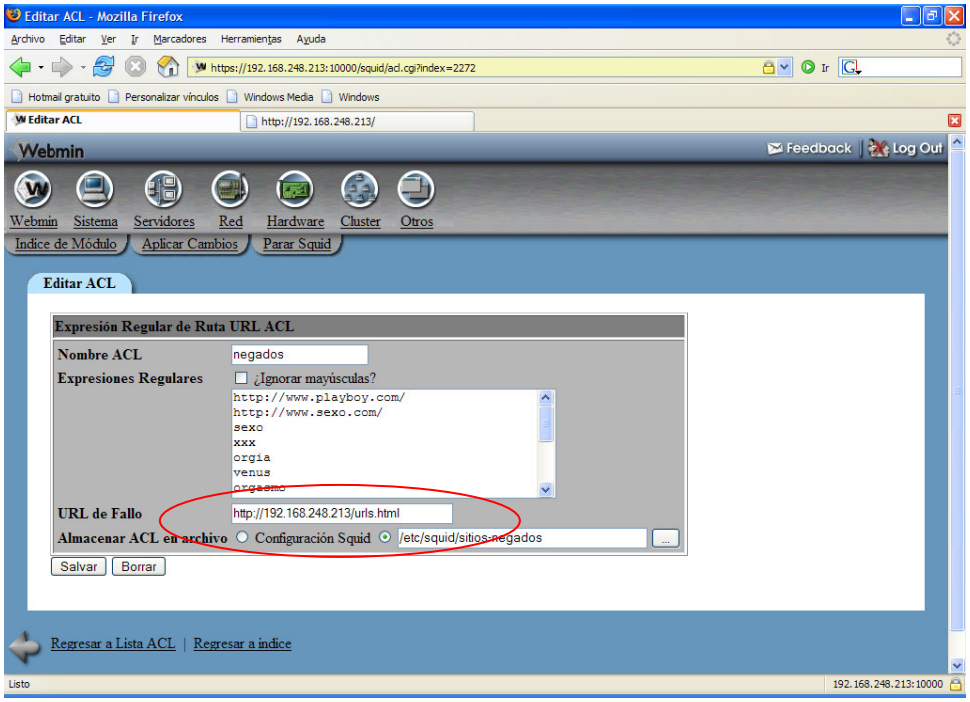
Este error de lista de acceso fue por encontrar la palabra sexo en el URL. Ahora si tratamos de descargar un archivo con extensión no permitida:

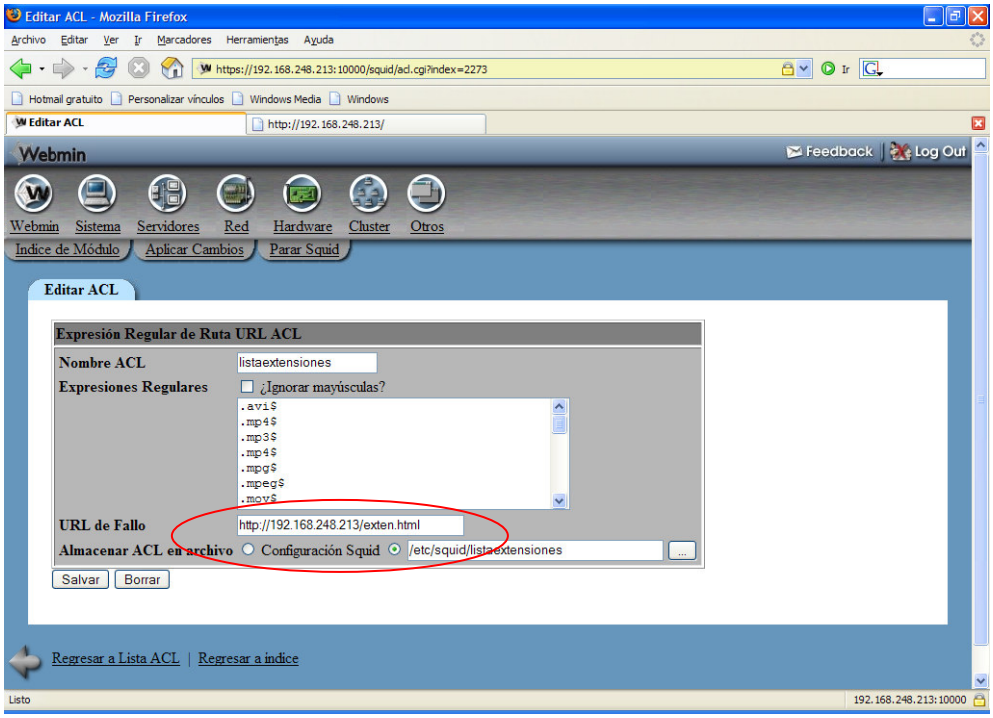


El Mensaje es el mismo, sobre una regla de acceso no permite acceder al sitio. Pero no se sabe que regla de acceso es la que nego el acceso.

4.14.2. PERSONALIZACION DE MENSAJES DE ERROR SEGÚN LA ACL

Se va a personalizar estos mensajes, definiendolos en la lista, indicándo el URL o página web a mostrar en el caso de que falle por una lista de acceso. Se prueba con la lista de URL y de extensiones:

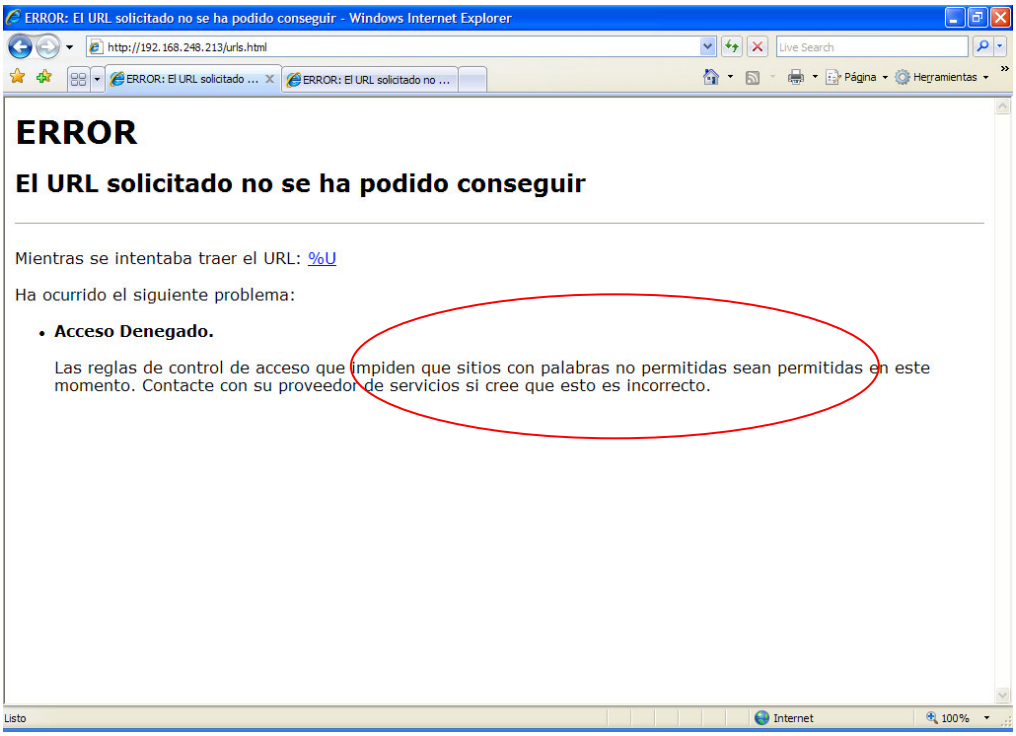


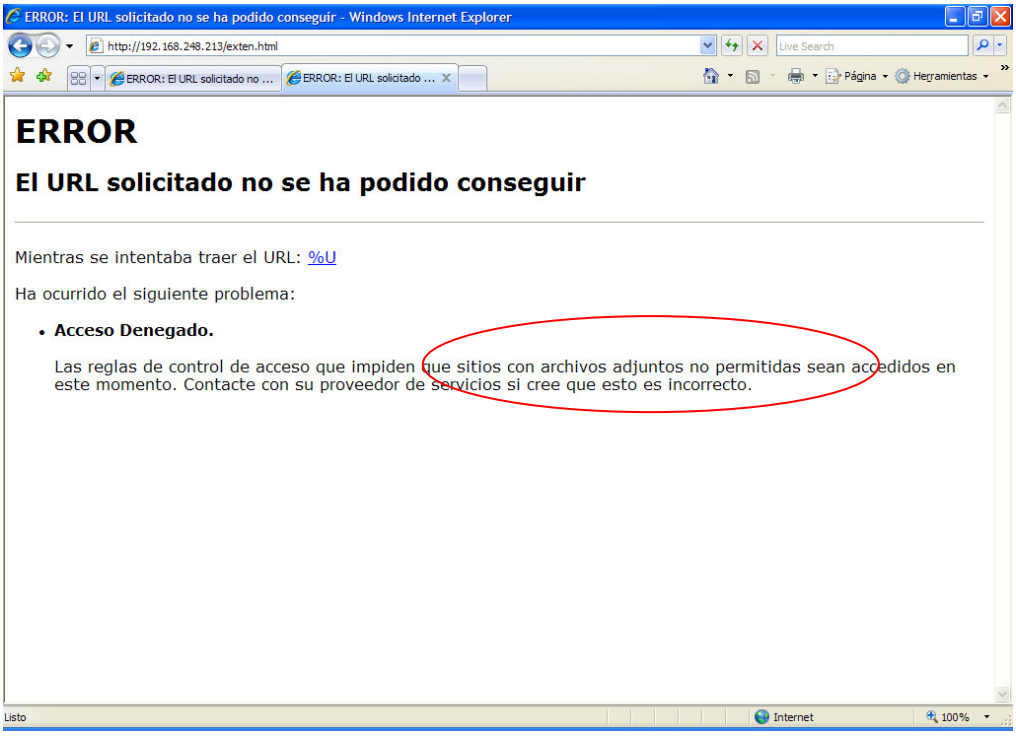


Se van a llamar a las páginas con los nombres urls.html y exten.html respectivamente en el caso de fallar por esas listas de acceso. Los archivos html se ubican en el directorio de las páginas web:

```
[root@www web]# pwd
/home/web
[root@www web]# ls
exten.html  index.html  prohibit.html  urls.html
[root@www web]#
```

Se prueba de nuevo con las páginas que no son permitidas y se observa:





Ya los mensajes no son el mismo, si no que para cada regla sale uno diferente.

4.14.3. INSTALACION Y CONFIGURACION DEL SQUIDGUARD

Se procede ahora con la instalación del squidguard y las listas de URL mas extensas:

```
[root@www opt]# pwd
/opt
[root@www opt]# ls -l
total 12612
drwxr-xr-x    2 root root      4096 nov  7  2005 MailScanner-4.47.4-2
drwxr-xr-x    6 3168 games     4096 oct 24 22:45 majordomo-1.94.5
-rw-r--r--    1 root root    312244 ene 27  2006 majordomo-1.94.5.tar.gz
-rw-r--r--    1 root root     88385 oct 25 00:12 squidguard-1.2.0-2.2.el4.rf.i386.rpm
-rw-r--r--    1 root root     85572 nov 29  2005 squidguard-1.2.0-2.2.fc4.rf.i386.rpm
-rw-r--r--         1  root  root    12381873  oct  25  00:01  squidguard-blacklists-20050528-
1.2.el4.rf.noarch.rpm
drwxr-xr-x  109 root bin       4096 ago 30 19:23 webmin-1.200
[root@www opt]#
```

Se instala el squidguard de fedora core 6.

```
[root@www instaladores]# rpm -ivh squidGuard-1.2.0-15.fc6.i386.rpm
```

```
warning: squidGuard-1.2.0-15.fc6.i386.rpm: Header V3 DSA signature: NOKEY, key ID
1ac70ce6
Preparing...                ########################################### [100%]
   1:squidGuard             ########################################### [100%]
/etc/squid/squidGuard.conf created as /etc/squid/squidGuard.conf.rpmnew
Loading new SELinux policy
/etc/selinux/targeted/src/policy /
```

Se tratan de instalar las listas de RedHat Enterprise 3, pues no hay para Fedora, pero pide una versión anterior de squidguard:

```
[root@www instaladores]# rpm -ivh squidguard-blacklists-20050528-
1.2.el4.rf.noarch.rpm
warning: squidguard-blacklists-20050528-1.2.el4.rf.noarch.rpm: Header V3 DSA signature:
NOKEY, key ID 6b8d79e6
error: Failed dependencies:
        squidguard = 1.2.0 is needed by squidguard-blacklists-20050528-1.2.el4.rf.noarch
```

Se va a realizar la instalación de forma manual de las listas.

En /etc/squid también estan los archivos del squidguard.

```
[root@www instaladores]# cd /etc/squid
[root@www squid]# ls
cachemgr.conf     mime.conf.default     squid.conf.default
errors            msntauth.conf         squid.conf.mayo8
icons             msntauth.conf.default  squidGuard.conf
listaextensiones  sitios-negados        squidguard.conf.ori
mib.txt           squid.conf            squidGuard.conf.rpmnew
mime.conf         squid.conf.antes
[root@www squid]#
```

Se saca una copia de los archivos originales de configuración.

```
[root@www squid]# cp squidguard.conf squidguard.conf.ori
```

Se cambia el nombre al archivo de configuración para que sea semejante al ejecutable del squidguard (con letra G):

```
[root@www squid]# mv squidguard.conf squidGuard.conf
```

Se edita el archivo de configuración y se hacen unos cambios. (El archivo final se adjunta en el CD).

Una sita del archivo de configuración es:

```
[root@www squid]# cat  squidGuard.conf
```

```
#------------------------------------------------------------------
# SquidGuard CONFIGURATION FILE
#------------------------------------------------------------------

# DIRECTORIOS DE CONFIGURACION
dbhome /var/lib/squidguard
logdir /var/log/squidguard
# GRUPOS DE DIRECCIONES
dest adult {
  domainlist adult/domains
  urllist adult/urls
  expressionlist adult/expressions
}
dest audio-video {
  domainlist audio-video/domains
  urllist audio-video/urls
}
dest hacking {
  domainlist hacking/domains
  urllist hacking/urls
}
dest warez {
  domainlist warez/domains
  urllist warez/urls
}
dest ads {
  domainlist ads/domains
  urllist ads/urls
  # la publicidad es reemplazada por una imagen vacia
  redirect http://127.0.0.1/nulbanner.png
}
dest aggressive {
  domainlist aggressive/domains
  urllist aggressive/urls
}
dest drugs {
  domainlist drugs/domains
  urllist drugs/urls
}
dest gambling {
  domainlist gambling/domains
  urllist gambling/urls
}
# permitimos los servidores gratuitos de correo
#dest mail {
#  domainlist mail/domains
#}
dest proxy {
  domainlist proxy/domains
  urllist proxy/urls
}
```

```
dest violence {
  domainlist violence/domains
  urllist violence/urls
  expressionlist violence/expressions
}

# CONTROL DE ACCESO
acl {
  # por defecto bloqueamos los grupos de direcciones creados
  default {
    pass !adult !audio-video !hacking !warez !ads !aggressive !drugs !gambling !proxy
!violence all
    # redireccionamos a una pagina web disuasoria
    redirect http://127.0.0.1/prohibit.html
  }
}
```

Se busca donde esta el ejecutable del squidGuard:

```
[root@www squid]# which squidGuard
/usr/bin/squidGuard
```

Se edita squid.conf y se incluye la línea para que se integre con el squidguard.

```
redirect_program /usr/bin/squidGuard -c /etc/squid/squidGuard.conf
```

Como no se instalaron las listas con los RPM, se procede a copiar manualmente las carpetas y archivos requeridos desde otra máquina. Ubicados en la otra máquina :

```
[root@www ~]# cd /var/lib
[root@www lib]# ls -ld squidguard/
drwx------  14 squid squid 4096 oct  6  2006 squidguard/
[root@www lib]# scp -r squidguard root@10.21.28.1:/var/lib/
root's password:
urls.db                                       100% 8192     8.0KB/s   00:00
expressions                                   100%    0     0.0KB/s   00:00
domains                                       100% 5359     5.2KB/s   00:00
urls                                          100% 1577     1.5KB/s   00:00
domains.db                                    100%   24KB  24.0KB/s   00:00
urls.db                                       100%   80KB  80.0KB/s   00:00
expressions                                   100%    0     0.0KB/s   00:00
domains                                       100% 9577     9.4KB/s   00:00
urls                                          100%   52KB  51.8KB/s   00:00
domains.db                                    100%   36KB  36.0KB/s   00:00
urls.db                                       100% 8192     8.0KB/s   00:00
expressions                                   100%    0     0.0KB/s   00:00
domains                                       100% 6055     5.9KB/s   00:00
urls                                          100%    0     0.0KB/s   00:00
```

```
domains.db                                    100%   24KB  24.0KB/s   00:00
urls.db                                     100% 8192     8.0KB/s   00:00
expressions                                   100%    0     0.0KB/s   00:00
domains                                     100% 5346     5.2KB/s   00:00
urls                                        100% 1677     1.6KB/s   00:00
domains.db                                    100%   20KB  20.0KB/s   00:00
urls.db                                     100% 8192     8.0KB/s   00:00
expressions                                   100%    0     0.0KB/s   00:00
domains                                     100% 3379     3.3KB/s   00:00
urls                                        100% 1533     1.5KB/s   00:00
domains.db                                    100%   16KB  16.0KB/s   00:00
urls.db                                     100% 8192     8.0KB/s   00:00
expressions                                   100%    0     0.0KB/s   00:00
domains                                     100% 1842     1.8KB/s   00:00
urls                                        100%  675     0.7KB/s   00:00
domains.db                                    100% 8192     8.0KB/s   00:00
urls.db                                     100% 4500KB   4.4MB/s   00:00
expressions                                   100%  799     0.8KB/s   00:00
domains                                     100% 9046KB   8.8MB/s   00:01
urls                                        100% 3174KB   3.1MB/s   00:01
domains.db                                    100%   22MB  11.1MB/s   00:02
domains                                     100%    0     0.0KB/s   00:00
expressions                                   100%   84     0.1KB/s   00:00
urls                                        100%    0     0.0KB/s   00:00
domains                                     100%   52     0.1KB/s   00:00
expressions                                   100%    0     0.0KB/s   00:00
urls                                        100%    0     0.0KB/s   00:00
urls.db                                     100% 8192     8.0KB/s   00:00
expressions                                   100%   55     0.1KB/s   00:00
domains                                     100% 1902     1.9KB/s   00:00
urls                                        100%  822     0.8KB/s   00:00
domains.db                                    100% 8192     8.0KB/s   00:00
urls.db                                     100%   24KB  24.0KB/s   00:00
expressions                                   100%   68     0.1KB/s   00:00
domains                                     100%   27KB  26.5KB/s   00:00
urls                                        100% 7445     7.3KB/s   00:00
domains.db                                    100%   76KB  76.0KB/s   00:00
urls.db                                     100% 8192     8.0KB/s   00:00
expressions                                   100%    0     0.0KB/s   00:00
domains                                     100%  432     0.4KB/s   00:00
urls                                        100%    0     0.0KB/s   00:00
domains.db                                    100% 8192     8.0KB/s   00:00
urls.db                                     100% 8192     8.0KB/s   00:00
expressions                                   100%    0     0.0KB/s   00:00
domains                                     100%  690     0.7KB/s   00:00
urls                                        100%  500     0.5KB/s   00:00
domains.db                                    100% 8192     8.0KB/s   00:00
urls.db                                     100%   16KB  16.0KB/s   00:00
expressions                                   100%    0     0.0KB/s   00:00
domains                                     100% 4632     4.5KB/s   00:00
urls                                        100% 6042     5.9KB/s   00:00
```

```
domains.db                                    100%   20KB  20.0KB/s   00:00
[root@www logrotate.d]# pwd
/etc/logrotate.d
[root@www logrotate.d]# scp -r squidguard-blacklists root@10.21.28.1:/etc/logrotate.d
root's password:
squidguard-blacklists                         100%   67     0.1KB/s   00:00
[root@www squid]# pwd
/etc/squid
[root@www squid]# scp -r local root@10.21.28.1:/etc/squid/
root's password:
domains                                       100%    0     0.0KB/s   00:00
expressions                                   100%   84     0.1KB/s   00:00
urls                                          100%    0     0.0KB/s   00:00
domains                                       100%   52     0.1KB/s   00:00
expressions                                   100%    0     0.0KB/s   00:00
urls                                          100%    0     0.0KB/s   00:00
```

Ubicados en la máquina nueva se cambian los permisos:

```
[root@www squid]# cd /var/lib
[root@www lib]# ls -ld squidguard/
drwx------ 15 root root 4096 may 17 09:36 squidguard/
[root@www lib]# chown -R squid:squid squidguard/
[root@www lib]# ls -ld squidguard/
drwx------ 15 squid squid 4096 may 17 09:36 squidguard/
[root@www lib]#cd /etc/logrotate.d
[root@www logrotate.d]# pwd
/etc/logrotate.d
[root@www logrotate.d]# ls -ld squid*
-rw-r--r-- 1 root root 543 oct  2  2006 squid
-rw-r--r-- 1 root root  87 sep  6  2005 squidGuard
-rw-r--r-- 1 root root  67 may 17 09:44 squidguard-blacklists
[root@www logrotate.d]# chown squid:squid squidguard-blacklists
[root@www squid]# cd /etc/squid
[root@www squid]# pwd
/etc/squid
[root@www squid]#
[root@www squid]# ls -ld local
drwx------ 4 root root 4096 may 17 09:57 local
[root@www squid]# chown squid:squid local
[root@www squid]# ls -ld local
drwx------ 4 squid squid 4096 may 17 09:57 local
```

Se crea la carpeta de LOG del squidguard y se dan permisos:

```
[root@www logrotate.d]# cd /var/log
[root@www log]# ls -ld squid*
drwxr-x--- 2 squid squid 4096 may 13 04:02 squid
[root@www log]# mkdir squidguard
[root@www log]# chown squid:squid squidguard
```

```
[root@www log]# ls -ld squid*
drwxr-x--- 2 squid squid 4096 may 13 04:02 squid
drwxr-xr-x 2 squid squid 4096 may 17 09:48 squidguard
```

El exito del uso del squidguard es contar con buenas listas negras de URLs, y estas se pueden consultar en:

http://www.squidguard.org/blacklists.html

Se reconfigurar el squid y se verifican los procesos de squidguard:

```
[root@www log]# squid -k reconfigure
[root@www log]# ps -ef | grep squid
root      2802     1  0 08:33 ?        00:00:00 squid -D
squid     2804  2802  0 08:33 ?        00:00:00 (squid) -D
squid     2811  2804  0 08:33 ?        00:00:00 (unlinkd)
squid     4772  2804  0 09:49 ?        00:00:00 (squidGuard) -c /etc/squid/squidGuard.conf
squid     4773  2804  0 09:49 ?        00:00:00 (squidGuard) -c /etc/squid/squidGuard.conf
squid     4774  2804  0 09:49 ?        00:00:00 (squidGuard) -c /etc/squid/squidGuard.conf
squid     4775  2804  0 09:49 ?        00:00:00 (squidGuard) -c /etc/squid/squidGuard.conf
squid     4776  2804  0 09:49 ?        00:00:00 (squidGuard) -c /etc/squid/squidGuard.conf
root      4778  3555  0 09:49 pts/1    00:00:00 grep squid
[root@www log]#
```

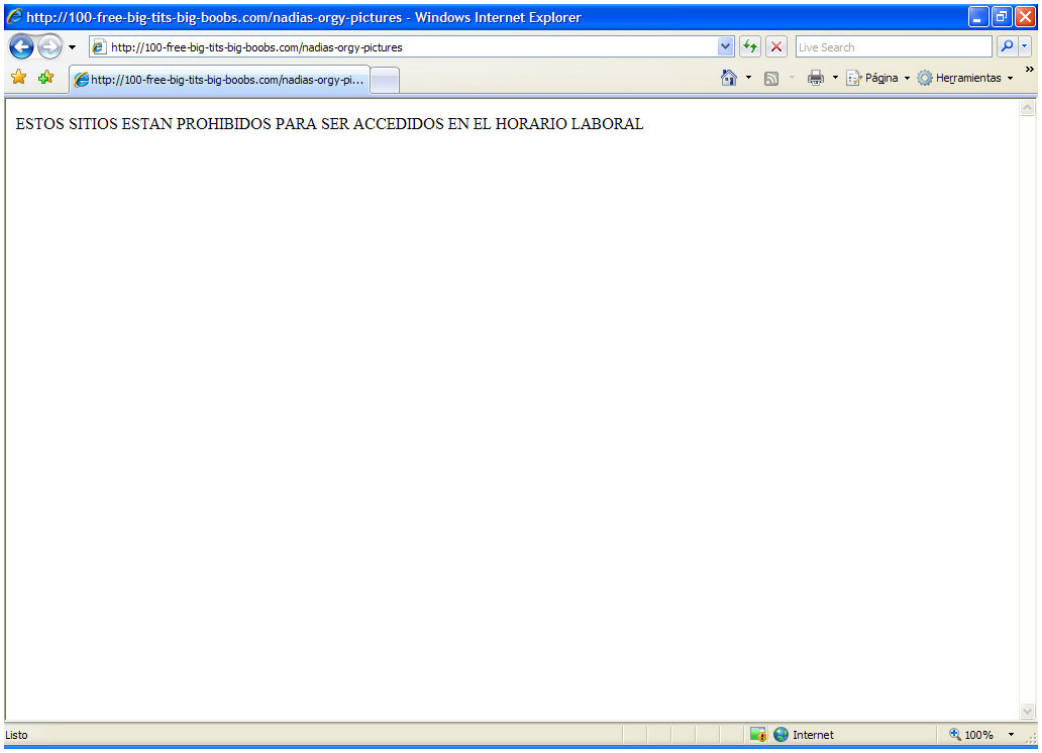
Se verifica que en el log aparezca el mensaje de que esta listo para recibir peticiones.

```
[root@www squid]# tail -5 /var/log/squid/squidGuard.log
2006-10-25 00:26:58 [31571] init urllist /var/lib/squidguard/violence/urls
2006-10-25 00:26:58 [31571] loading dbfile /var/lib/squidguard/violence/urls.db
2006-10-25 00:26:58 [31571] init expressionlist /var/lib/squidguard/violence/expressions
2006-10-25 00:26:58 [31571] squidGuard 1.2.0 started (1161754018.090)
2006-10-25 00:26:58 [31571] squidGuard ready for requests (1161754018.155)
[root@www squid]#
```

Se crea la página a la que se redireccionan los bloqueos:

```
[root@www squid]# cd /home/web
[root@www html]# ls
index.html  prohibit.html
 [root@www html]# cat prohibit.html
<html> ESTOS SITIOS ESTAN PROHIBIDOS PARA SER ACCEDIDOS EN EL HORARIO
LABORAL </html>
[root@www html]#
```

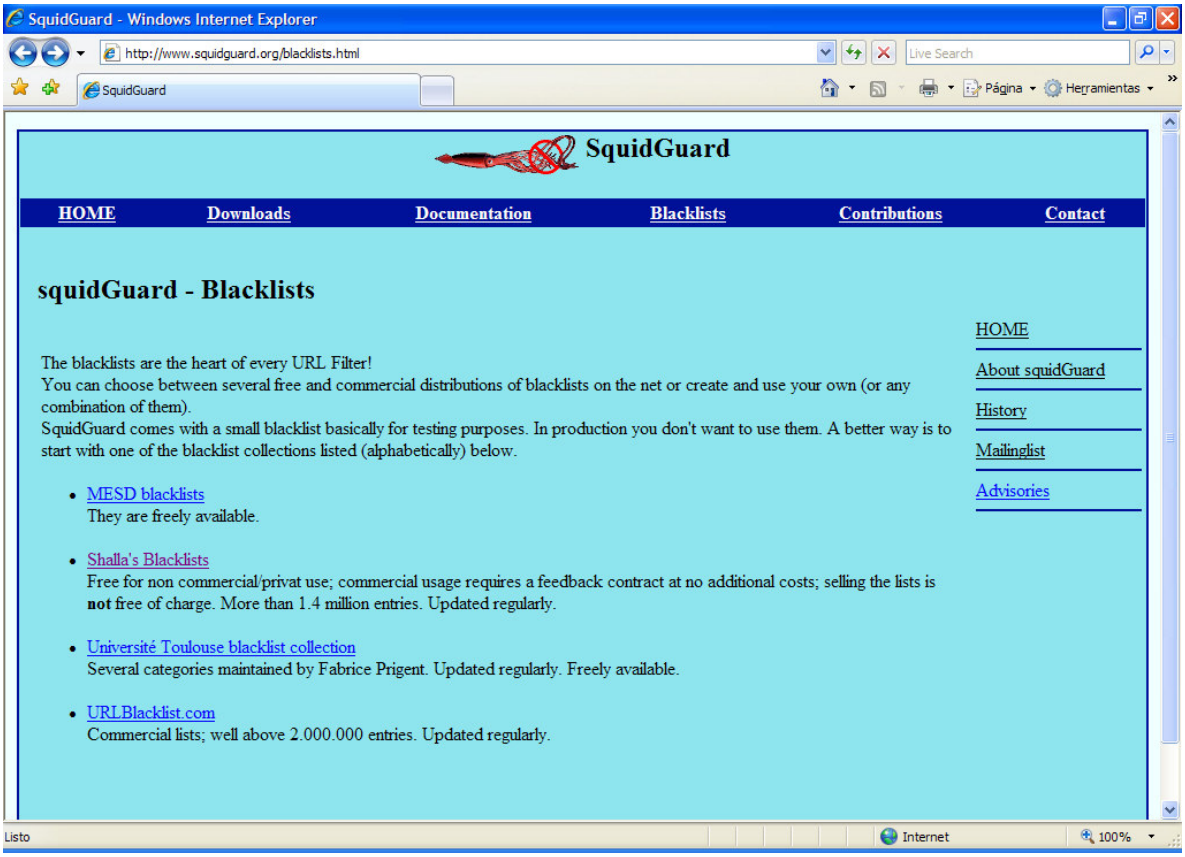
Se prueba con un sitio:



4.14.4. DESCARGA E INCLUSION DE OTRAS LISTAS PARA SQUIDGUARD

Como se mencionó anteriormente, el éxito del filtrado de contenido es contar con una buena base de datos de sitios clasificados en internet, para que sea mas sencillo su control. Productos comerciales como el Websense, son una de las mejores alternativas para esto, ya que practicamente proveen bases de datos con todos los sitios en internet clasificados y se actualizan diariamente. El usuario que compra la suscripción a ese producto, puede descargar diariamente esta base.

Como estamos trabajando con producto libres, descargaremos listas de uso gratuito, pero también las hay de uso comercial como se muestra en este sitio web:



Se descarga otro Blacklist y se deja en /opt/instaladores. Desde allí se descomprime:

```
[root@www instaladores]# ls *.tar
shallalist.tar.tar
[root@www instaladores]# tar xvf shallalist.tar.tar
BL/
BL/porn/
BL/porn/domains
BL/porn/urls
BL/gamble/
BL/gamble/domains
BL/gamble/urls
BL/chat/
BL/chat/domains
BL/chat/urls
BL/automobile/
BL/automobile/urls
BL/automobile/domains
BL/recreation/
BL/recreation/travel/
BL/recreation/travel/urls
BL/recreation/travel/domains
BL/recreation/wellness/
```

BL/recreation/wellness/domains
BL/recreation/wellness/urls
BL/recreation/humor/
BL/recreation/humor/domains
BL/recreation/humor/urls
BL/recreation/sports/
BL/recreation/sports/domains
BL/recreation/sports/urls
BL/webradio/
BL/webradio/domains
BL/webradio/urls
BL/webmail/
BL/webmail/domains
BL/webmail/urls
BL/warez/
BL/warez/urls
BL/warez/domains
BL/shopping/
BL/shopping/domains
BL/shopping/urls
BL/adv/
BL/adv/domains
BL/adv/urls
BL/movies/
BL/movies/urls
BL/movies/domains
BL/science/
BL/science/chemistry/
BL/science/chemistry/urls
BL/science/chemistry/domains
BL/science/astronomy/
BL/science/astronomy/domains
BL/science/astronomy/urls
BL/hobby/
BL/hobby/games/
BL/hobby/games/domains
BL/hobby/games/urls
BL/hobby/pets/
BL/hobby/pets/domains
BL/hobby/pets/urls
BL/hobby/cooking/
BL/hobby/cooking/domains
BL/hobby/cooking/urls
BL/violence/
BL/violence/domains
BL/violence/urls
BL/music/
BL/music/domains
BL/music/urls
BL/hacking/
BL/hacking/domains

BL/hacking/urls
BL/isp/
BL/isp/urls
BL/isp/domains
BL/drugs/
BL/drugs/domains
BL/drugs/urls
BL/aggressive/
BL/aggressive/domains
BL/aggressive/urls
BL/news/
BL/news/urls
BL/news/domains
BL/redirector/
BL/redirector/urls
BL/redirector/domains
BL/spyware/
BL/spyware/domains
BL/spyware/urls
BL/dating/
BL/dating/urls
BL/dating/domains
BL/finance/
BL/finance/banking/
BL/finance/banking/urls
BL/finance/banking/domains
BL/finance/other/
BL/finance/other/domains
BL/finance/other/urls
BL/finance/moneylending/
BL/finance/moneylending/domains
BL/finance/moneylending/urls
BL/dynamic/
BL/dynamic/urls
BL/dynamic/domains
BL/COPYRIGHT
BL/jobsearch/
BL/jobsearch/urls
BL/jobsearch/domains
BL/tracker/
BL/tracker/domains
BL/tracker/urls
BL/forum/
BL/forum/domains
BL/forum/urls
BL/webtv/
BL/webtv/urls
BL/webtv/domains
BL/downloads/
BL/downloads/urls
BL/downloads/domains

```
[root@www instaladores]# cd BL
[root@www BL]# ls
adv         COPYRIGHT  dynamic  hacking   movies  recreation  spyware   webmail
aggressive  dating     finance  hobby     music   redirector  tracker   webradio
automobile  downloads  forum    isp       news    science     violence  webtv
chat        drugs      gamble   jobsearch porn    shopping    warez
[root@www BL]#
```

Las diferentes categorias y sus archivos con listas residen en la carpeta BL (son 31 categorias). Debemos integrarlas con las listas actuales que residen en /var/lib/squidguard (son 14 categorias).

Si revisamos algunos directorios, su contenido difiere un poco. Por ejemplo las listas actuales de adultos:

```
[root@www squidguard]# ls -l adult
total 39412
-rw------- 1 squid squid  9263101 may 17 09:36 domains
-rw------- 1 squid squid 23166976 may 17 09:36 domains.db
-rw------- 1 squid squid      799 may 17 09:36 expressions
-rw------- 1 squid squid  3250614 may 17 09:36 urls
-rw------- 1 squid squid  4608000 may 17 09:36 urls.db
[root@www squidguard]# wc -l adult/urls
99237 adult/urls
```

Y las listas de adultos nuevas en BL:

```
[root@www BL]# ls -l porn
total 16212
-rw-r--r-- 1 1001 root 11380445 may  9 15:55 domains
-rw-r--r-- 1 1001 root  5186944 may  7 15:18 urls
[root@www BL]# wc -l porn/urls
141503 porn/urls
```

Con las listas actuales tenemos las categorias:

```
ads adult aggressive audio-video drugs forums gambling hacking local mail proxy violence warez
```

Se actualizan los archivos con los de las lista de BL, y los que no existian se copian con la carpeta:

```
[root@www BL]# cp porn/* /var/lib/squidguard/adult/
cp: Â¿sobreescribir Â«/var/lib/squidguard/adult/domainsÂ»? (s/n) s
cp: Â¿sobreescribir Â«/var/lib/squidguard/adult/urlsÂ»? (s/n) s
[root@www BL]# unalias cp
[root@www BL]# ls -l porn/
total 16212
-rw-r--r-- 1 1001 root 11380445 may  9 15:55 domains
```

```
-rw-r--r-- 1 1001 root  5186944 may  7 15:18 urls
[root@www BL]# cp adv/* /var/lib/squidguard/ads/
[root@www BL]# cp aggressive/* /var/lib/squidguard/aggressive/
[root@www BL]# cp -r movies /var/lib/squidguard/
[root@www BL]# cp -r webradio /var/lib/squidguard/
[root@www BL]# cp -r music  /var/lib/squidguard/
[root@www BL]# cp -r webtv/  /var/lib/squidguard/
[root@www BL]# cp drugs/* /var/lib/squidguard/drugs/
[root@www BL]# cp forum/* /var/lib/squidguard/forums/
[root@www BL]# cp gamble/* /var/lib/squidguard/gambling/
[root@www BL]# cp hacking/* /var/lib/squidguard/hacking/
[root@www BL]# cp webmail/* /var/lib/squidguard/mail/
[root@www BL]# cp violence/* /var/lib/squidguard/violence/
[root@www BL]# cp warez/* /var/lib/squidguard/warez/
[root@www BL]# cp -r automobile/  /var/lib/squidguard/
[root@www BL]# cp -r chat/  /var/lib/squidguard/
[root@www BL]# cp -r dating/  /var/lib/squidguard/
[root@www BL]# cp -r downloads/  /var/lib/squidguard/
[root@www BL]# cp -r dynamic  /var/lib/squidguard/
[root@www BL]# cp -r finance  /var/lib/squidguard/
[root@www BL]# cp -r hobby  /var/lib/squidguard/
[root@www BL]# cp -r isp  /var/lib/squidguard/
[root@www BL]# cp -r jobsearch  /var/lib/squidguard/
[root@www BL]# cp -r news  /var/lib/squidguard/
[root@www BL]# cp -r recreation  /var/lib/squidguard/
[root@www BL]# cp -r science  /var/lib/squidguard/
[root@www BL]# cp -r shopping  /var/lib/squidguard/
[root@www BL]# cp -r spyware  /var/lib/squidguard/
[root@www BL]# cp -r tracker  /var/lib/squidguard/
```

Hay algunas categorias que cambian de nombre, por ejemplo adultos, mail,ads, gamble, y se van a dejar con los nombres nuevos.

Se cambian los permisos a todas las carpetas y archivos:

```
[root@www squidguard]# chown -R squid:squid *
```

Algunos de las categorias traen adicional a las listas de URLs y Dominios, archivos con expresiones no permitidas (textos). Se debe de terner en cuenta esto en el archivo de configuración del squidguard, pues allí se deben de incuir todas las categorias .

Se copio uno de los archivos expression a todas las demás carpetas. El contenido del archivo es:

```
[root@www squidguard]# cat  webmail/expressions
(^|[-.\?+=/_0-
9])(all|big|cute|cyber|fake|firm|hard|huge|little|mega|mini|naughty|new|old|pure|real|small|s
```

```
erious|soft|super|tiny|young)(girl|virgin)s?(cafe|site|surf|surfing|web|website)?([-.\?+=/_0-
9]|$)
(^|[-.\?+=/_0-
9])(all|big|cute|cyber|fake|firm|hard|huge|little|mega|mini|naughty|new|old|pure|real|small|s
erious|soft|super|tiny|young)?(anal|babe|bharath|boob|breast|busen|busty|clit|cum|cunt|dic
k|fetish|fuck|hooter|lez|lust|naked|nude|oral|orgy|porno?|pupper|pussy|rotten|sex|shit|smut
pump|teen|tit|topp?les|vixen|xxx)s?(cafe|site|surf|surfing|web|website)?([-.\?+=/_0-9]|$)
(adultos|adultsight|adultsite|adultsonly|adultweb|blow-
?job|bondage|centerfold|cumshot|cyberlust|cybercore|hardcore|incest|masturbat|obscene|
pedophil|pedofil|playmate|pornstar|sexdream|showgirl|softcore|striptease)
```

Se cambiron los permisos de estos archivos:

```
[root@www squidguard]# chown -R squid:squid *
```

El archivo de configuración del squidguard de /etc/squid quedo:

```
[root@www squid]# cat    squidGuard.conf
#--------------------------------------------------------------------
# SquidGuard CONFIGURATION FILE
#--------------------------------------------------------------------

# DIRECTORIOS DE CONFIGURACION
dbhome /var/lib/squidguard
logdir /var/log/squidguard
# GRUPOS DE DIRECCIONES
dest porn {
  domainlist porn/domains
  urllist porn/urls
  expressionlist porn/expressions
}
dest audio-video {
  domainlist audio-video/domains
  urllist audio-video/urls
  expressionlist audio-video/expressions
}
dest hacking {
  domainlist hacking/domains
  urllist hacking/urls
  expressionlist hacking/expressions
}
dest warez {
  domainlist warez/domains
  urllist warez/urls
  expressionlist warez/expressions
}
dest adv {
  domainlist adv/domains
  urllist adv/urls
  expressionlist adv/expressions
```

```
  # la publicidad es reemplazada por una imagen vacia
  redirect http://127.0.0.1/nulbanner.png
}
dest aggressive {
  domainlist aggressive/domains
  urllist aggressive/urls
  expressionlist aggressive/expressions
}
dest drugs {
  domainlist drugs/domains
  urllist drugs/urls
  expressionlist drugs/expressions
}
dest gamble {
  domainlist gamble/domains
  urllist gamble/urls
  expressionlist gamble/expressions
}
# los servidores gratuitos de correo
dest webmail {
  domainlist webmail/domains
  urllist webmail/urls
  expressionlist webmail/expressions
}
dest proxy {
  domainlist proxy/domains
  urllist proxy/urls
  expressionlist proxy/expressions
}
dest violence {
  domainlist violence/domains
  urllist violence/urls
  expressionlist violence/expressions
}
dest automobile {
  domainlist automobile/domains
  urllist automobile/urls
  expressionlist automobile/expressions
}
dest chat {
  domainlist chat/domains
  urllist chat/urls
  expressionlist chat/expressions
}
dest dating {
  domainlist dating/domains
  urllist dating/urls
  expressionlist dating/expressions
}
dest downloads {
  domainlist downloads/domains
```

```
  urllist downloads/urls
  expressionlist downloads/expressions
}
dest dynamic {
  domainlist dynamic/domains
  urllist dynamic/urls
  expressionlist dynamic/expressions
}
dest finance {
  domainlist finance/domains
  urllist finance/urls
  expressionlist finance/expressions
}
dest hobby {
  domainlist hobby/domains
  urllist hobby/urls
  expressionlist hobby/expressions
}
dest isp {
  domainlist isp/domains
  urllist isp/urls
  expressionlist isp/expressions
}
dest jobsearch {
  domainlist jobsearch/domains
  urllist jobsearch/urls
  expressionlist jobsearch/expressions
}
dest movies {
  domainlist movies/domains
  urllist movies/urls
  expressionlist movies/expressions
}
dest music {
  domainlist music/domains
  urllist music/urls
  expressionlist music/expressions
}
dest news {
  domainlist news/domains
  urllist news/urls
  expressionlist news/expressions
}
dest recreation {
  domainlist recreation/domains
  urllist recreation/urls
  expressionlist recreation/expressions
}
dest science {
  domainlist science/domains
  urllist science/urls
```

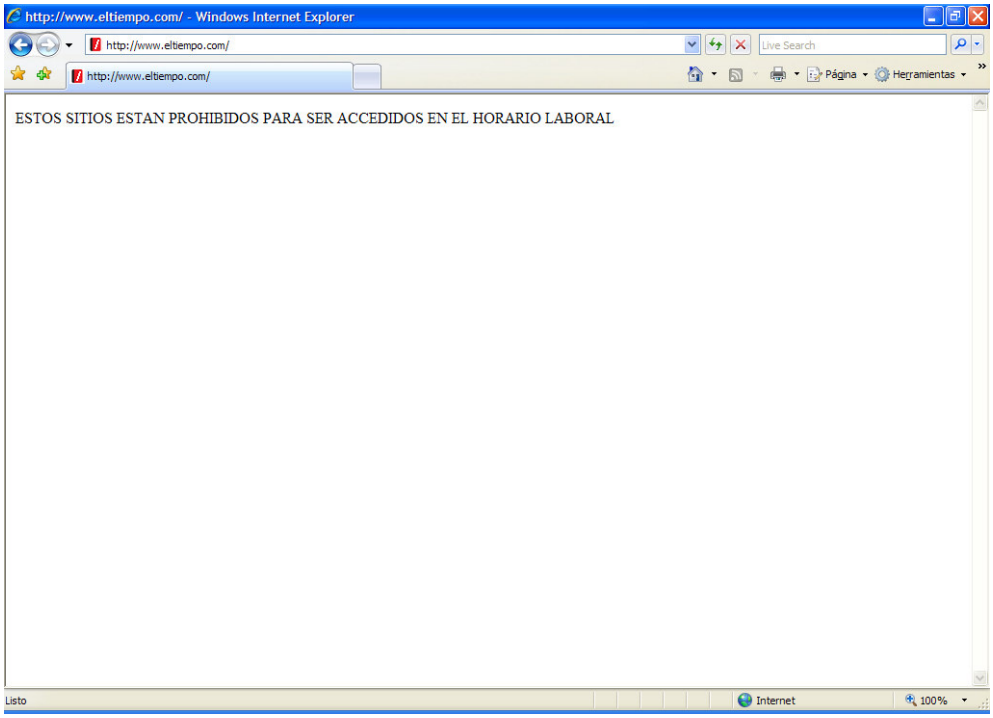
```
  expressionlist science/expressions
}
dest shopping {
  domainlist shopping/domains
  urllist shopping/urls
  expressionlist shopping/expressions
}
dest spyware {
  domainlist spyware/domains
  urllist spyware/urls
  expressionlist spyware/expressions
}
dest tracker {
  domainlist tracker/domains
  urllist tracker/urls
  expressionlist tracker/expressions
}
dest webradio {
  domainlist webradio/domains
  urllist webradio/urls
  expressionlist webradio/expressions
}
dest webtv {
  domainlist webtv/domains
  urllist webtv/urls
  expressionlist webtv/expressions
}
dest forums {
  domainlist forums/domains
  urllist forums/urls
  expressionlist forums/expressions
}

# CONTROL DE ACCESO
acl {
  # por defecto bloqueamos los grupos de direcciones creados
  default {
    pass !porn !aggressive !audio-video !automobile !chat !dating !downloads !dynamic
!finance !forums !gamble !hacking !hobby !isp !jobsearch !movies !music !news !proxy
!recreation !science !shopping !spyware !tracker !warez !adv !drugs !webradio !webtv
!violence all
    # redireccionamos a una pagina web disuasoria
    redirect http://127.0.0.1/prohibit.html
  }
}
```

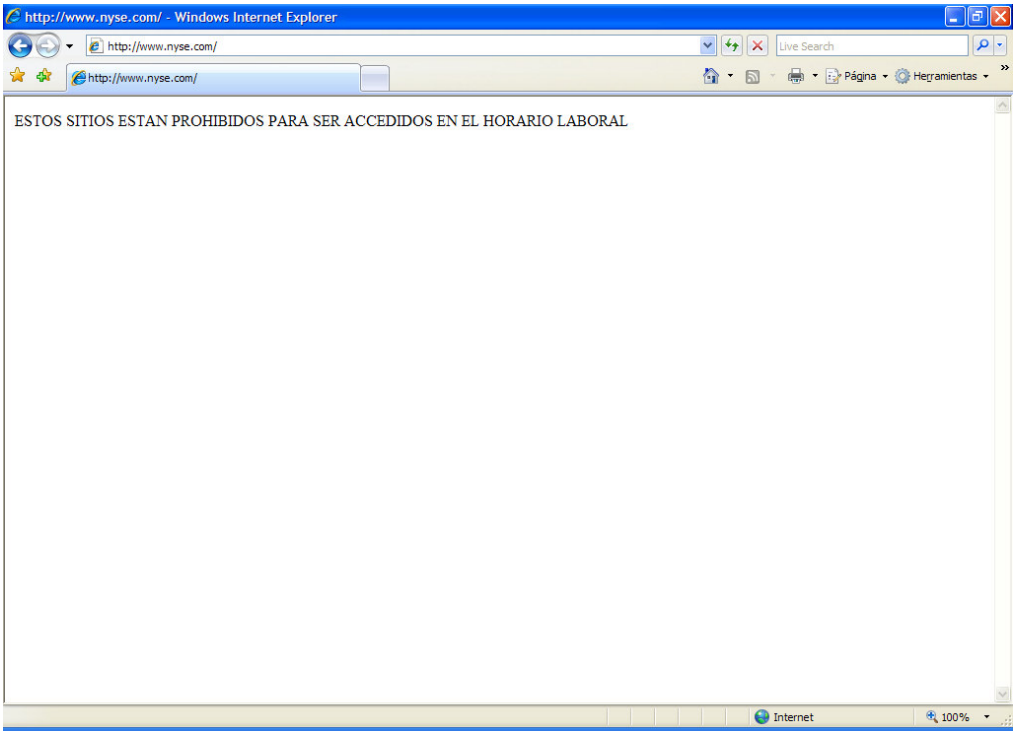
Se verifica que todas las categorias y carpetas tengan los archivos de domains y urls, y en las que no existen se crean con algún contenido (hobbies, recreation, science).

Se reconfigura el squid y se verifican los procesos:

```
[root@www squid]# squid -k reconfigure
[root@www squid]# service squid stop
Parando squid: .....                       [  OK  ]
[root@www squid]# service squid start
Iniciando squid: .                         [  OK  ]
[root@www squid]# ps -ef | grep squid
root      5954     1  0 11:37 ?        00:00:00 squid -D
squid     5956  5954  1 11:37 ?        00:00:00 (squid) -D
squid     5958  5956  4 11:37 ?        00:00:00 (squidGuard) -c /etc/squid/squidGuard.conf
squid     5959  5956  4 11:37 ?        00:00:00 (squidGuard) -c /etc/squid/squidGuard.conf
squid     5960  5956  4 11:37 ?        00:00:00 (squidGuard) -c /etc/squid/squidGuard.conf
squid     5961  5956  4 11:37 ?        00:00:00 (squidGuard) -c /etc/squid/squidGuard.conf
squid     5962  5956  4 11:37 ?        00:00:00 (squidGuard) -c /etc/squid/squidGuard.conf
squid     5963  5956  0 11:37 ?        00:00:00 (unlinkd)
root      5966  3555  0 11:37 pts/1    00:00:00 grep squid
[root@www squid]#
```

Se prueba accediendo a algunos sitios que están en las listas prohibidas:





4.14.5. GENERACION DE ESTADISTICAS SOBRE NAVEGACION EN INTERNET

Para tener un visión de lo que los usuarios hacen en internet, a través del proxy, se puede configurar el sarg, para que nos presente de forma gráfica los LOGs de acceso a internet.

Se instalara una nueva versión, para fedora core 6, ubicada en /opt/instaladores:

```
[root@proxyudi squid]# cd /opt/instaladores/
[root@proxyudi instaladores]# ls -l sar*
-rw-r--r-- 1 root root 316208 may  9 21:09 sarg-2.2.1-1.fc6.rf.i386.rpm
[root@proxyudi instaladores]#
[root@proxyudi instaladores]# rpm -ivh sarg-2.2.1-1.fc6.rf.i386.rpm
warning: sarg-2.2.1-1.fc6.rf.i386.rpm: Header V3 DSA signature: NOKEY, key ID
1aa78495
Preparing...                ########################################### [100%]
   1:sarg                   ########################################### [100%]
[root@proxyudi instaladores]#
```

Se edita el archivo de configuracion (/etc/sarg/sarg.conf):

Descomentamos y se arreglan las siguientes lineas :

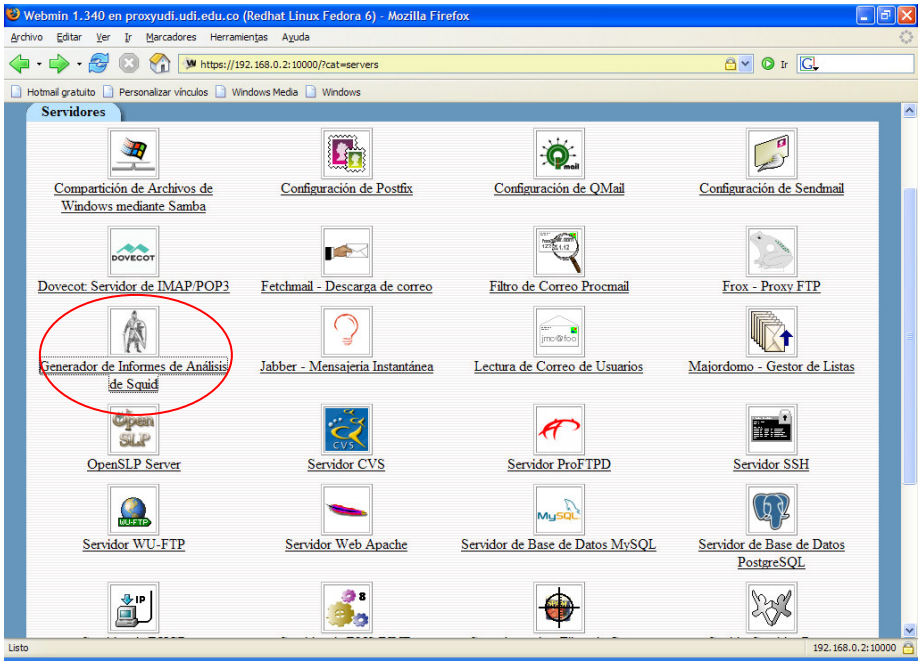
```
access_log /var/log/squid/access.log
```

```
output_dir /home/paginas/reportes
```

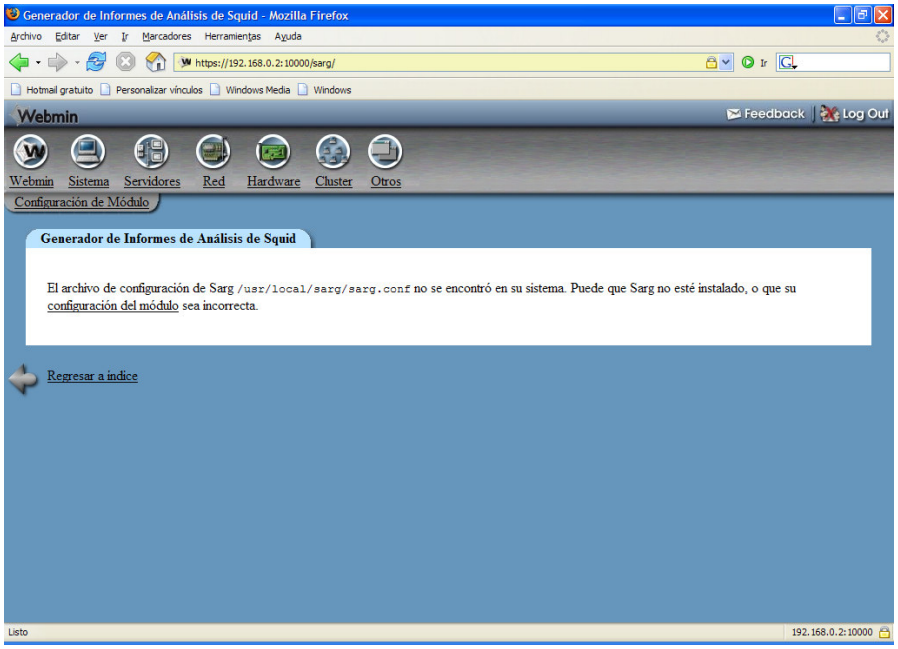
Se crea la carpeta donde residirán los reportes y se dan permisos:

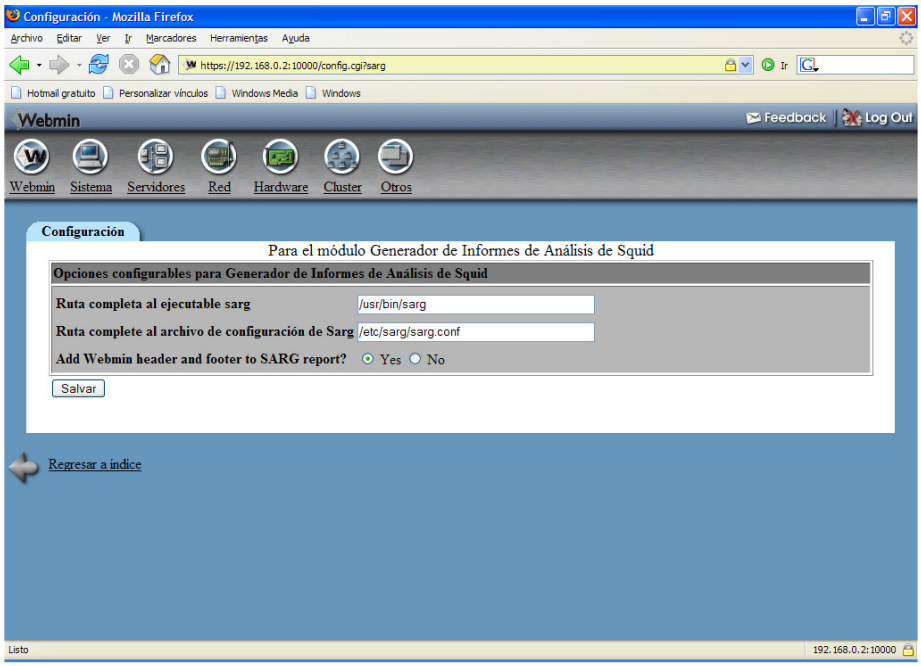
```
[root@www sarg]# mkdir /home/web/reportes
[root@www sarg]# chown apache:apache /home/web/reportes
```

En el webmin, por servidores, hay un icono para configuración del sarg:

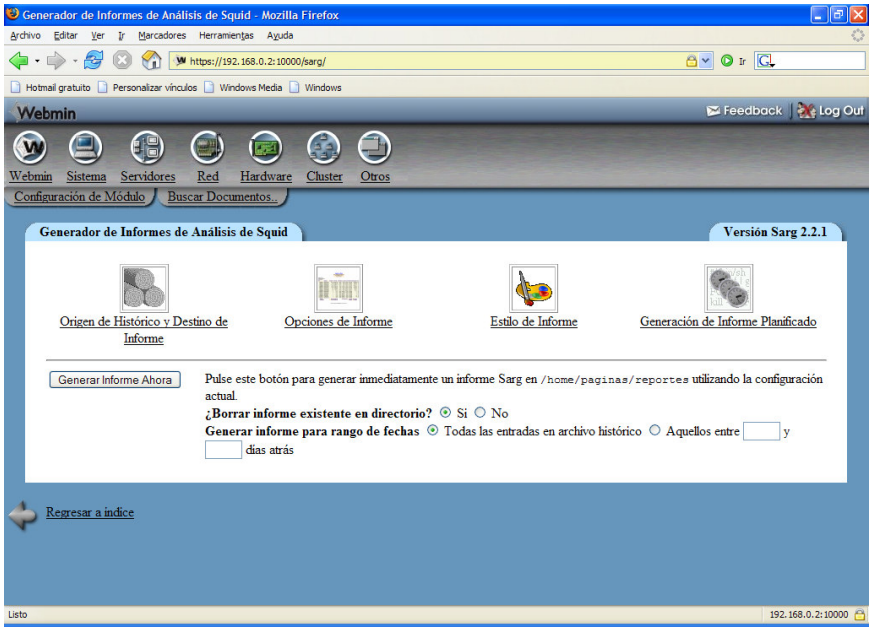


Se escoge, para configurarlo, pues el usa otro archivo de configuración:





Al salvar muestra:

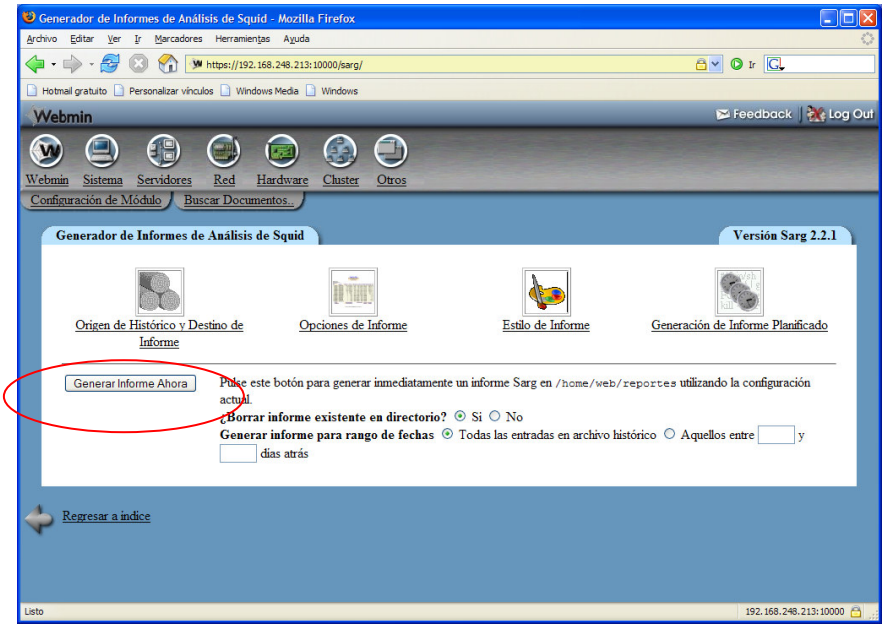


Se crea la carpeta de los reportes, debajo del directorio web:

Reiniciamos el servicio de apache:

```
[root@www reportes]# service httpd restart
Parando httpd:                                             [  OK  ]
Iniciando httpd:                                           [  OK  ]
```

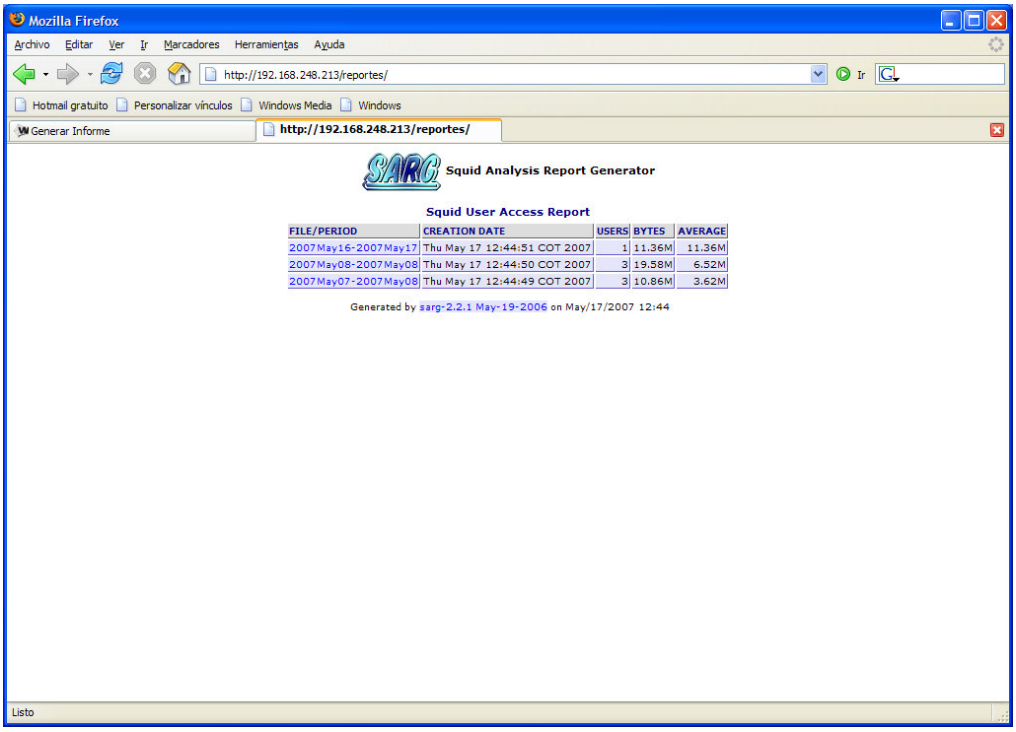
En la opción del webmin, dentro del sarg, se escoge generar informe:



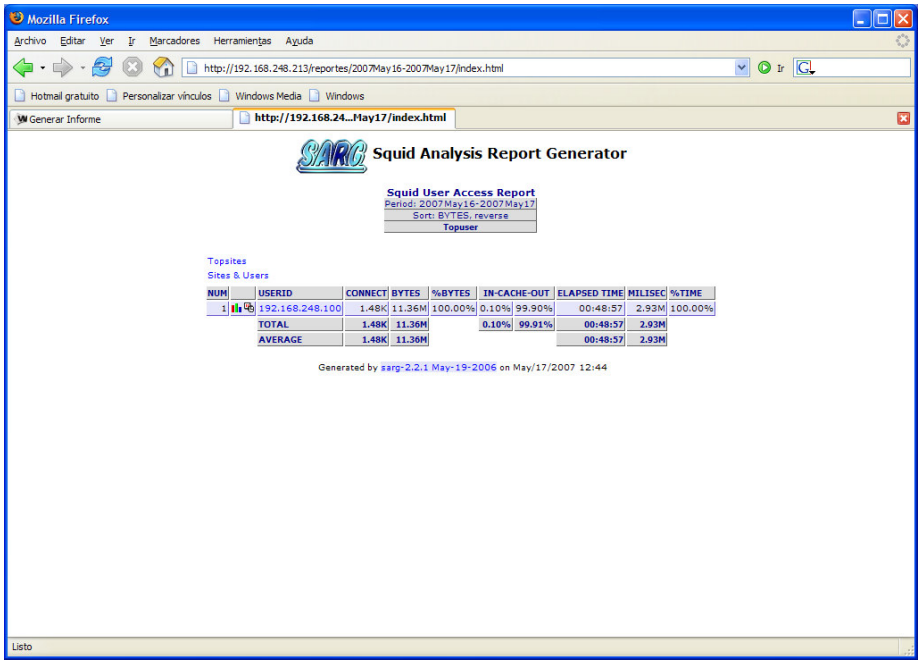
Ese informe debe ser ubicado en /home/web/reportes.

```
[root@www conf.d]# cd /home/web
[root@www web]# ls
exten.html  index.html  prohibit.html  reportes  urls.html
[root@www web]# cd reportes/
[root@www reportes]# pwd
/home/web/reportes
[root@www reportes]# ls
2007May07-2007May08    2007May08-2007May08    2007May16-2007May17    images
index.html
```

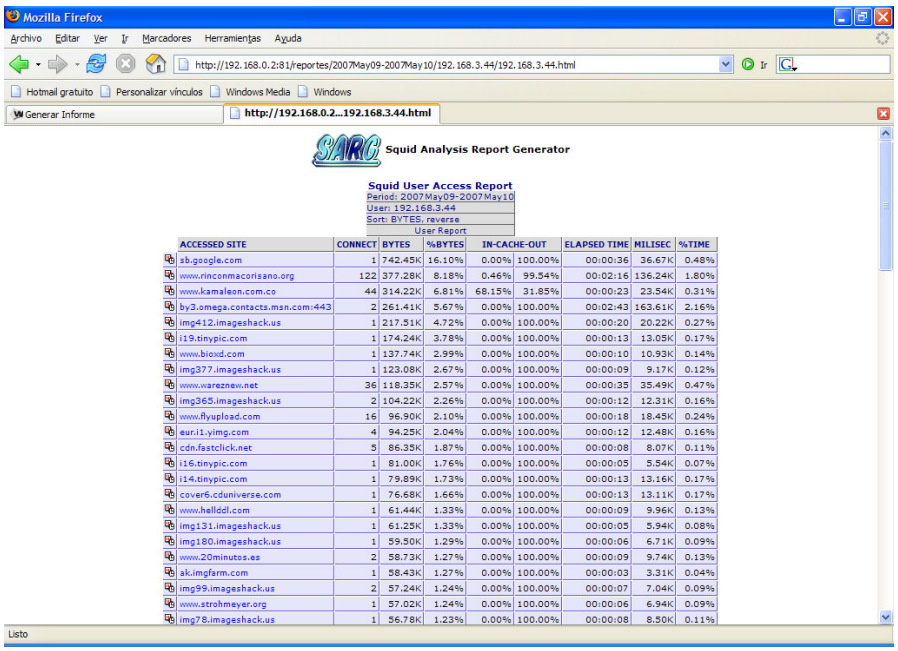
Vamos al navegador y verificamos si podemos ingresar a ver los reportes del sarg



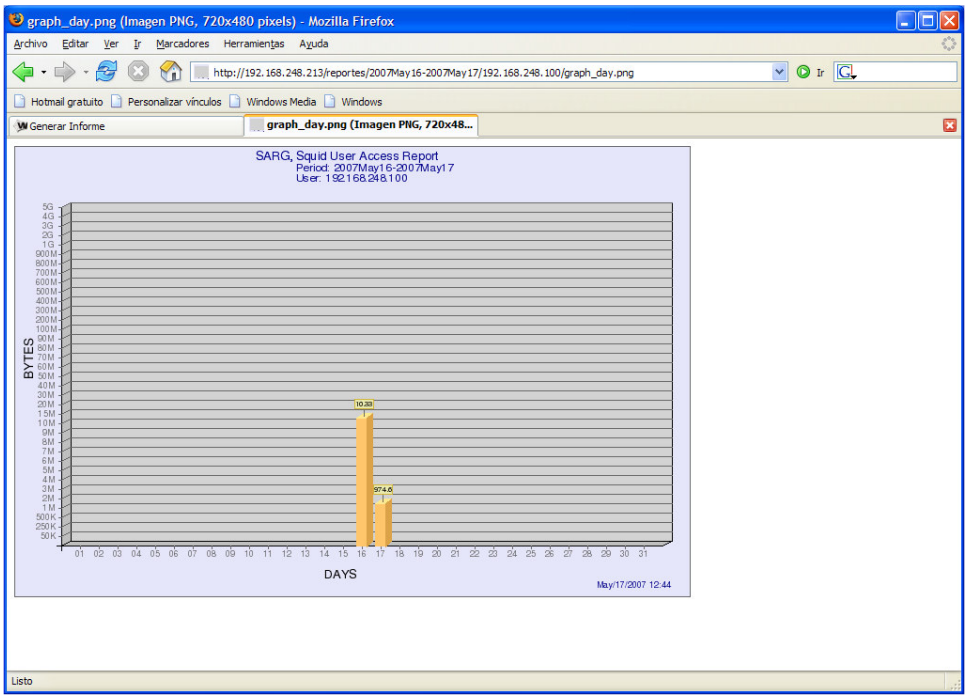
Se escoge la fecha del informe:



Se puede empezar a ver el detalle por usuario:

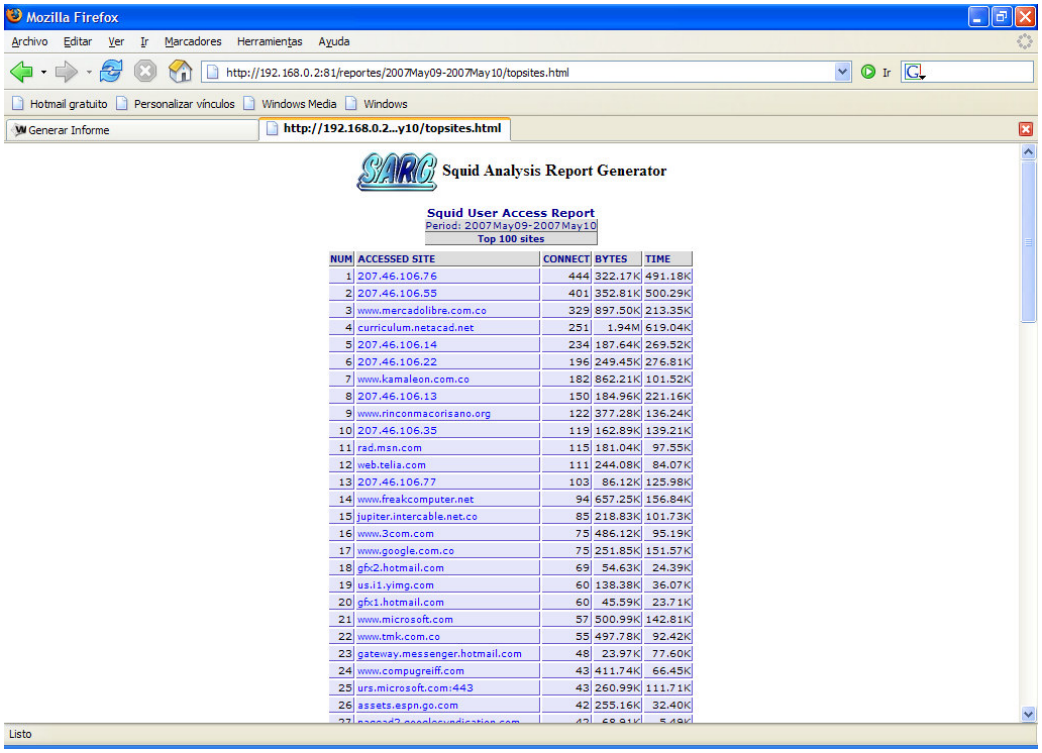


Se puede pedir graficar el consumo de un usuario, por ejemplo del equipo: 192.168.248.100:

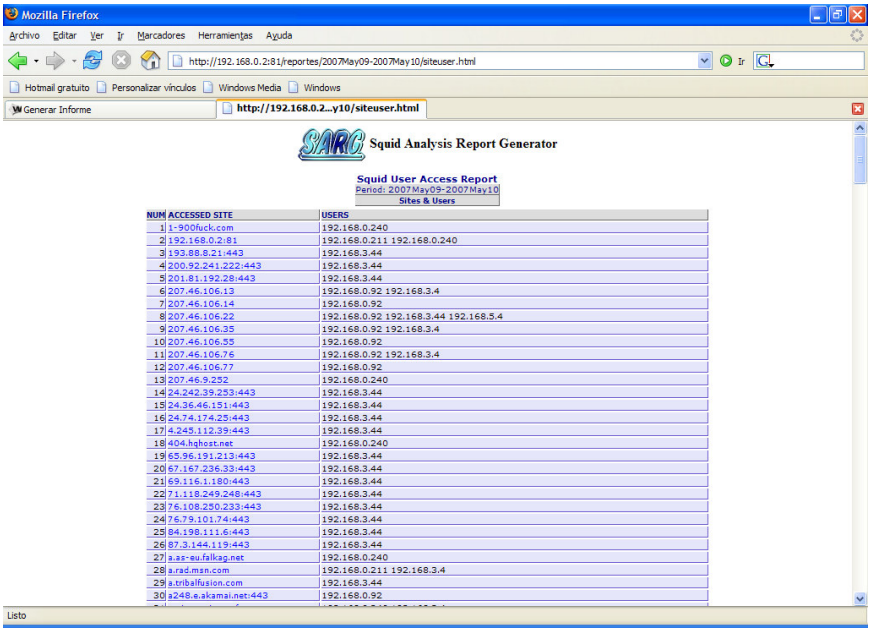


A continuación, veremos un breve vistazo al funcionamiento del sarg y los reportes que genera.

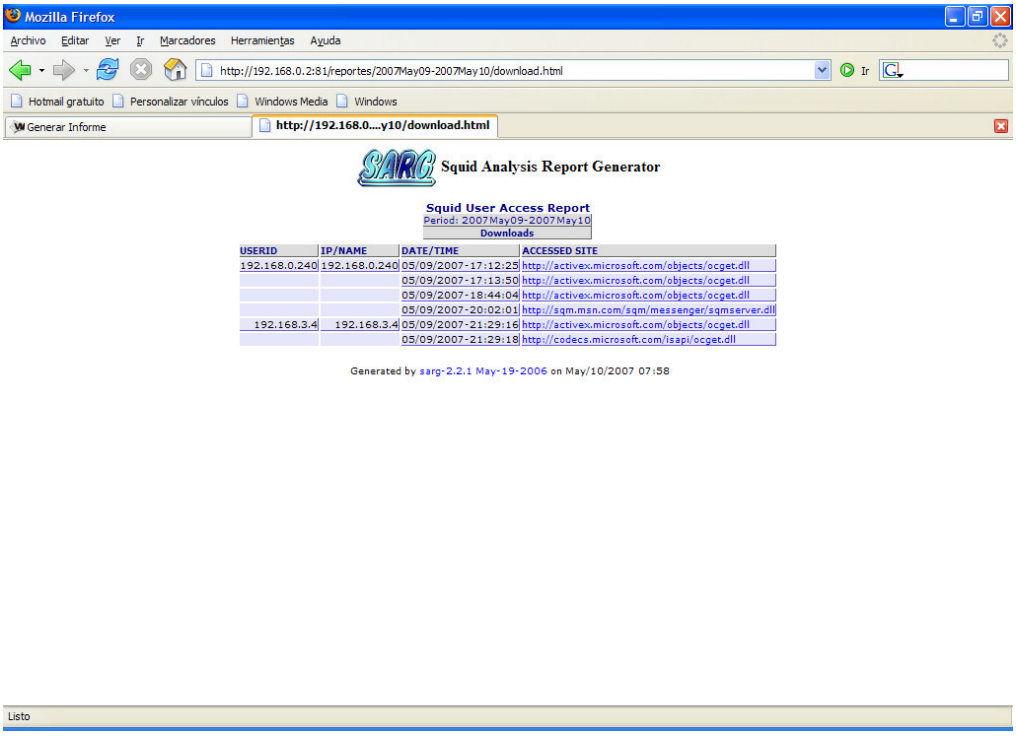
Top sities: en este caso por defecto muestra 100 sitios mas visitados



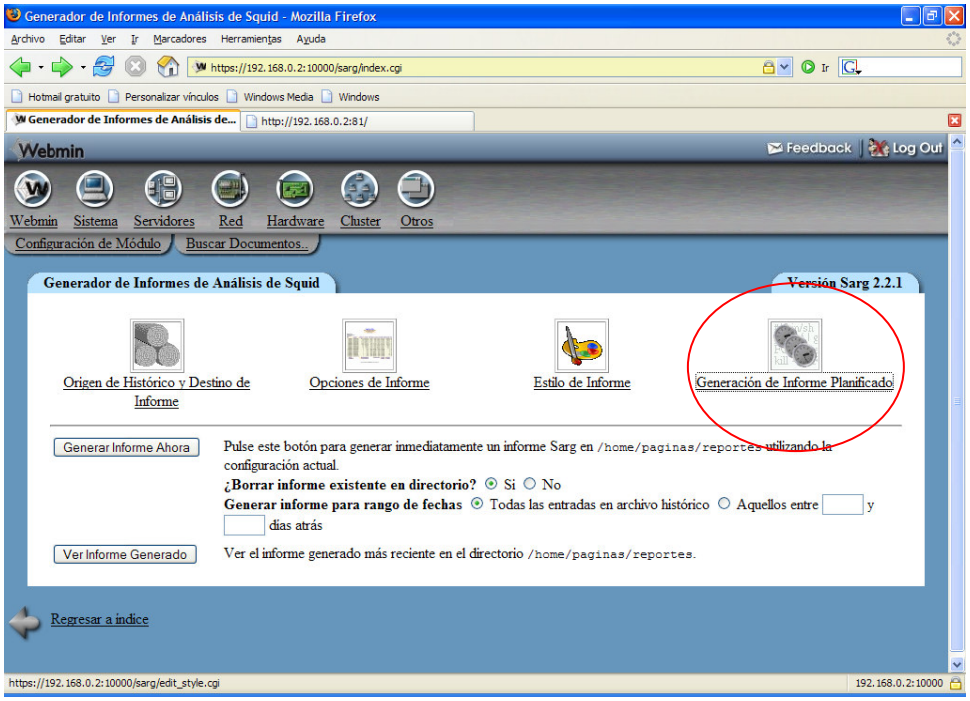
Sitios y usuarios:



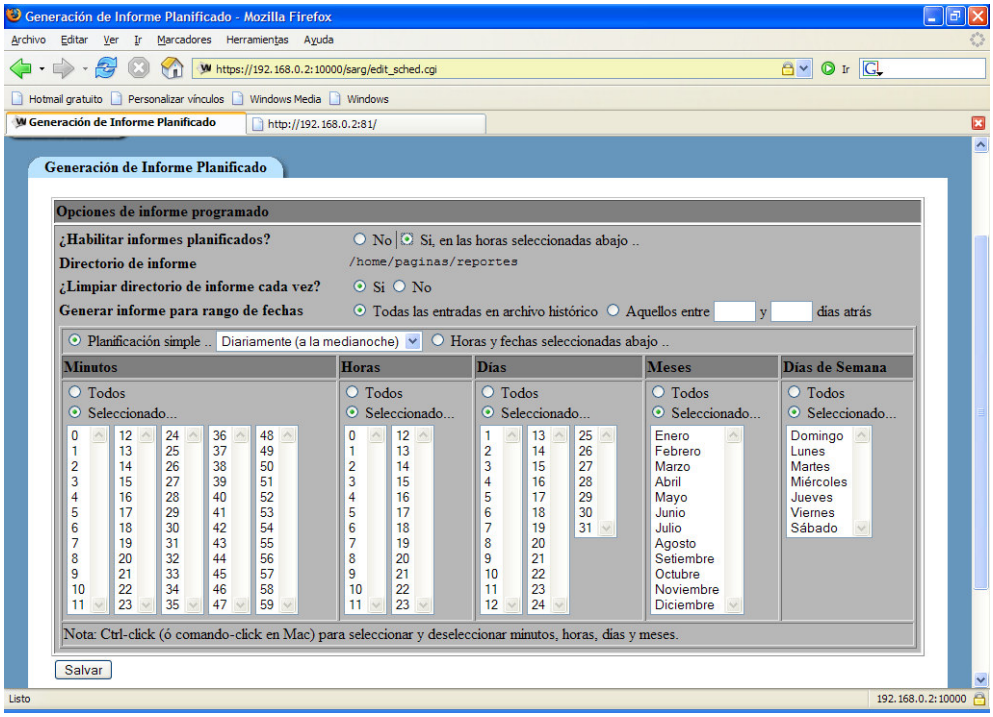
Bajados:



Por la opción del webmin de planificar reportes se puede pedir la generación de estos a determinadas horas y de los dias escogidos:



Por defecto se activo para que genere diario a la medianoche.


Generación de Informe Planificado - Mozilla Firefox
Archivo Editar Ver Ir Marcadores Herramientas Ayuda
https://192.168.0.2:10000/sarg/edit_sched.cgi
Hotmail gratuito Personalizar vínculos Windows Media Windows
Generación de Informe Planificado
http://192.168.0.2:81/
Generación de Informe Planificado
Opciones de informe programado
¿Habilitar informes planificados?
No
Si, en las horas seleccionadas abajo ..
Directorio de informe
/home/paginas/reportes
¿Limpiar directorio de informe cada vez?
Si
No
Generar informe para rango de fechas
Todas las entradas en archivo histórico
Aquellos entre
y
días atrás
Planificación simple ..
Diariamente (a la medianoche)
Horas y fechas seleccionadas abajo ..
Minutos
Horas
Días
Meses
Días de Semana
Todos
Seleccionado...
Enero
Febrero
Marzo
Abril
Mayo
Junio
Julio
Agosto
Setiembre
Octubre
Noviembre
Diciembre
Domingo
Lunes
Martes
Miércoles
Jueves
Viernes
Sábado
Nota: Ctrl-click (ó comando-click en Mac) para seleccionar y deseleccionar minutos, horas, días y meses.
Salvar
Listo
192.168.0.2:10000