

# 2012

## UD05 Practicas Proxy



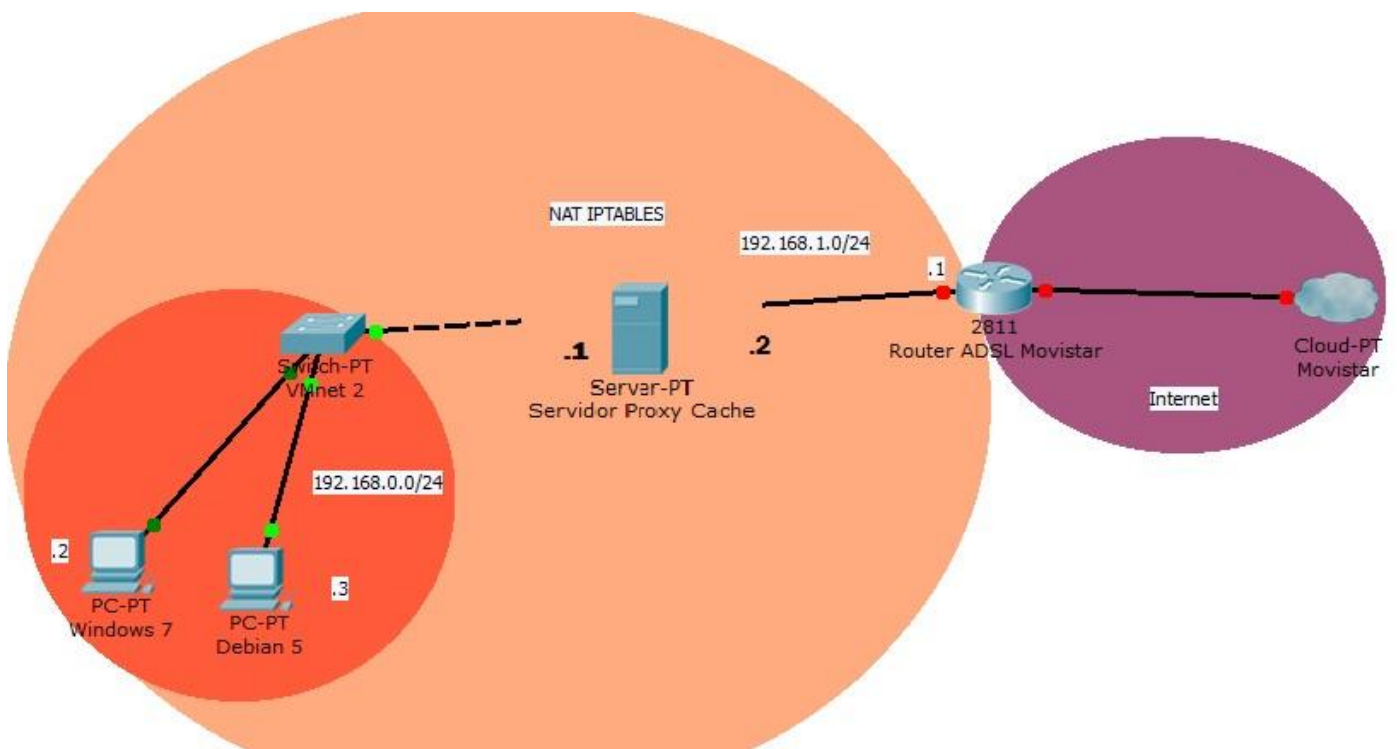
## Contenido

➤ Realiza en un documento PDF un planteamiento de escenario informático utilizando servidores proxy (servicios web y ftp). Debe utilizarse en las siguientes propuestas de prácticas	3
➤ Instalación y configuración del servidor Proxy “Squid” en GNU/Linux, realizando: .....	3
➤ Instalación y configuración del servidor Proxy “Squid” en GNU/Linux utilizando Webmin.	11
➤ Instalación y configuración del servidor Proxy “Zentyal” en GNU/Linux. ....	11
➤ Instalación y configuración del servidor Proxy “Wingate” en Windows. ....	15
Instalación y configuración del servidor Proxy “Squid” en GNU/Linux utilizando Webmin. ....	20
Descarga archivo de listas negras de sitios web y anexa las mismas a la configuración de Squid. <a href="http://urlblacklist.com/">http://urlblacklist.com/</a> . Prueba dichas listas negras. ....	25
Documenta la relación de productos que tiene y ha tenido Microsoft en relación a servidores “Proxy”. ¿Qué función tiene actualmente Microsoft Forefront TMG Treat Managment Gateway?. Describe su instalación y configuración. ....	30
Microsoft Forefront TMG Treat Managment Gateway.....	31
Información general .....	31
Requisitos del sistema .....	32
Instrucciones .....	32
Evaluación del producto .....	32
Introducción .....	32
Planeación y diseño .....	32
Implementación .....	33
Operaciones.....	33
Solucionar problemas.....	33
Referencia técnica .....	33

- **Realiza en un documento PDF un planteamiento de escenario informático utilizando servidores proxy (servicios web y ftp). Debe utilizarse en las siguientes propuestas de prácticas**

Lo primero que haremos será simular el escenario en el que trabajaremos, para ello tendremos que configurar un PC, con 2 tarjetas de red, de modo que mediante el enrutamiento NAT con iptables, podamos acceder a la red con equipos de distinta red.

Configuramos un servidor proxy Web, que revise las palabras que busquen los usuarios de la red 192.168.0.0/24, no permitiendo el acceso a paginas web, con contenido de sexo, drogas,etc...



- **Instalación y configuración del servidor Proxy "Squid" en GNU/Linux, realizando:**

Después de haber el enrutamiento por NAT, debemos tener algo parecido a esto:

```

root@primoguijarro-desktop: /usr/share/squid/errors/es
Archivo Editar Ver Terminal Ayuda
root@primoguijarro-desktop:/usr/share/squid/errors/es# ifconfig
eth0      Link encap:Ethernet direcciónHW 00:0c:29:6d:ef:29
         Direc. inet:192.168.1.2 Difus.:192.168.1.255 Másc:255.255.255.0
         Dirección inet6: fe80::20c:29ff:fe6d:ef29/64 Alcance:Enlace
         ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST MTU:1500 Métrica:1
         Paquetes RX:6826 errores:0 perdidos:0 overruns:0 frame:0
         Paquetes TX:4019 errores:0 perdidos:0 overruns:0 carrier:0
         colisiones:0 long.colatX:1000
         Bytes RX:7459257 (7.4 MB) TX bytes:501585 (501.5 KB)
         Interrupción:19 Dirección base: 0x2000

eth1      Link encap:Ethernet direcciónHW 00:0c:29:6d:ef:33
         Direc. inet:192.168.0.1 Difus.:192.168.0.255 Másc:255.255.255.0
         Dirección inet6: fe80::20c:29ff:fe6d:ef33/64 Alcance:Enlace
         ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST MTU:1500 Métrica:1
         Paquetes RX:886 errores:0 perdidos:0 overruns:0 frame:0
         Paquetes TX:926 errores:0 perdidos:0 overruns:0 carrier:0
         colisiones:0 long.colatX:1000
         Bytes RX:125756 (125.7 KB) TX bytes:799778 (799.7 KB)
         Interrupción:19 Dirección base: 0x2080

lo        Link encap:Bucle local
         Direc. inet:127.0.0.1 Másc:255.0.0.0
         Dirección inet6: ::1/128 Alcance:Anfitrión
         ACTIVO BUCLE FUNCIONANDO MTU:16436 Métrica:1

```

Realizamos la instalación del Servidor proxy Squid:

```

root@primoguijarro-desktop: /home/primoguijarro
Archivo Editar Ver Terminal Ayuda
PING www-cctld.l.google.com (74.125.230.88) 56(84) bytes of data.
64 bytes from par03s01-in-f24.1e100.net (74.125.230.88): icmp_seq=1 ttl=128 time
=381 ms
^C64 bytes from par03s01-in-f24.1e100.net (74.125.230.88): icmp_seq=2 ttl=128 ti
me=581 ms

--- www-cctld.l.google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 381.849/481.769/581.689/99.920 ms
root@primoguijarro-desktop:/home/primoguijarro# apt-get install squid
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes extras:
 squid-common squid-langpack
Paquetes sugeridos:
 squidclient squid-cgi logcheck-database resolvconf winbind
Se instalarán los siguientes paquetes NUEVOS:
 squid squid-common squid-langpack
0 actualizados, 3 se instalarán, 0 para eliminar y 0 no actualizados.
Necesito descargar 1347kB de archivos.
Se utilizarán 8503kB de espacio de disco adicional después de esta operación.
¿Desea continuar [S/n]? s
0% [Conectando a es.archive.ubuntu.com]

```

Abrimos el archivo de configuración así **nano /etc/squid/squid.conf**

Aceptamos conexiones por el puerto 3128

```
"
#      If you run Squid on a dual-homed machine with an internal
#      and an external interface we recommend you to specify the
#      internal address:port in http_port. This way Squid will only be
#      visible on the internal address.
#
# Squid normally listens to port 3128
|
http_port 3128
```

Le ponemos 1/3 de la memoria RAM que tengamos, es decir, si por ejemplo tenemos 512 Mb (Como en mi caso) le pondremos 192 MB, para la cache.

```
#      decreases, blocks will be freed until the high-water mark is
#      reached. Thereafter, blocks will be used to store hot
#      objects.
#
#Default:
cache mem 192 MB
```

Este parámetro asigna una zona de disco para squid, la ruta es donde estará los directorios de la cache, le pondremos 1000 MB, donde la esta cantidad no puede ser menor que la cache mem, el 16 quiere decir la cantidad de directorios que permitimos y el 256 los subdirectorios.

```
#
#      Note that for coss, max-size must be less than COSS_MEMBUF_SZ
#      (hard coded at 1 MB).
#
#Default:
|cache_dir ufs /var/spool/squid 1000 16 256
```

Nos creamos 2 acl donde en la primera permitimos que la red 192.168.0.0/24, acceda a través del proxy. La segunda línea quiere decir que buscare un fichero llamado "**noperm**", donde en su contenido pondremos las palabras que queremos que analice, para denegar o permitir su búsqueda.

```
acl purge method PURGE
acl CONNECT method CONNECT
acl asir20 src 192.168.0.0/24
acl noway url_regex "/etc/squid/noperm"
```

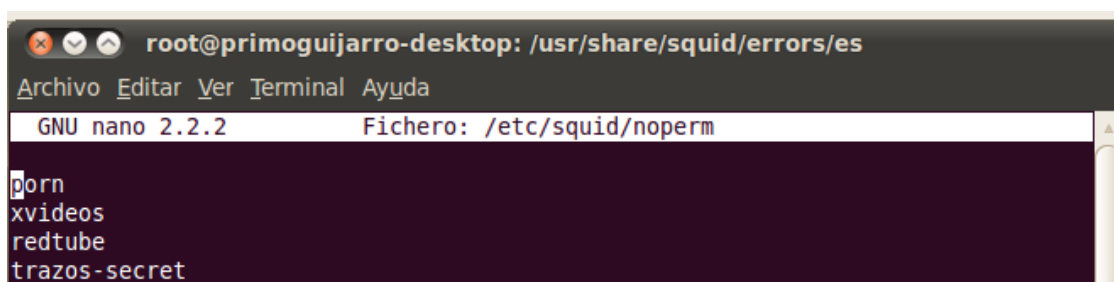
Añadimos 2 http\_access, donde en la primera denegamos la conexión aquellas peticiones que contengan las palabras que indicamos anteriormente.

La segunda es para permitir todas las peticiones de la red asir20.

```
# Only allow cachemgr access from localhost
http_access deny noway
http_access allow asir20
http_access allow manager localhost
http_access deny manager
```

Nos creamos el archivo **nano /etc/squid/noperm**

Añadimos las palabras que no queremos que nos busque en el navegador.



Con este parámetro le indicamos que la URL de acceso denegado será en español, en mi caso la he modificado por mi.

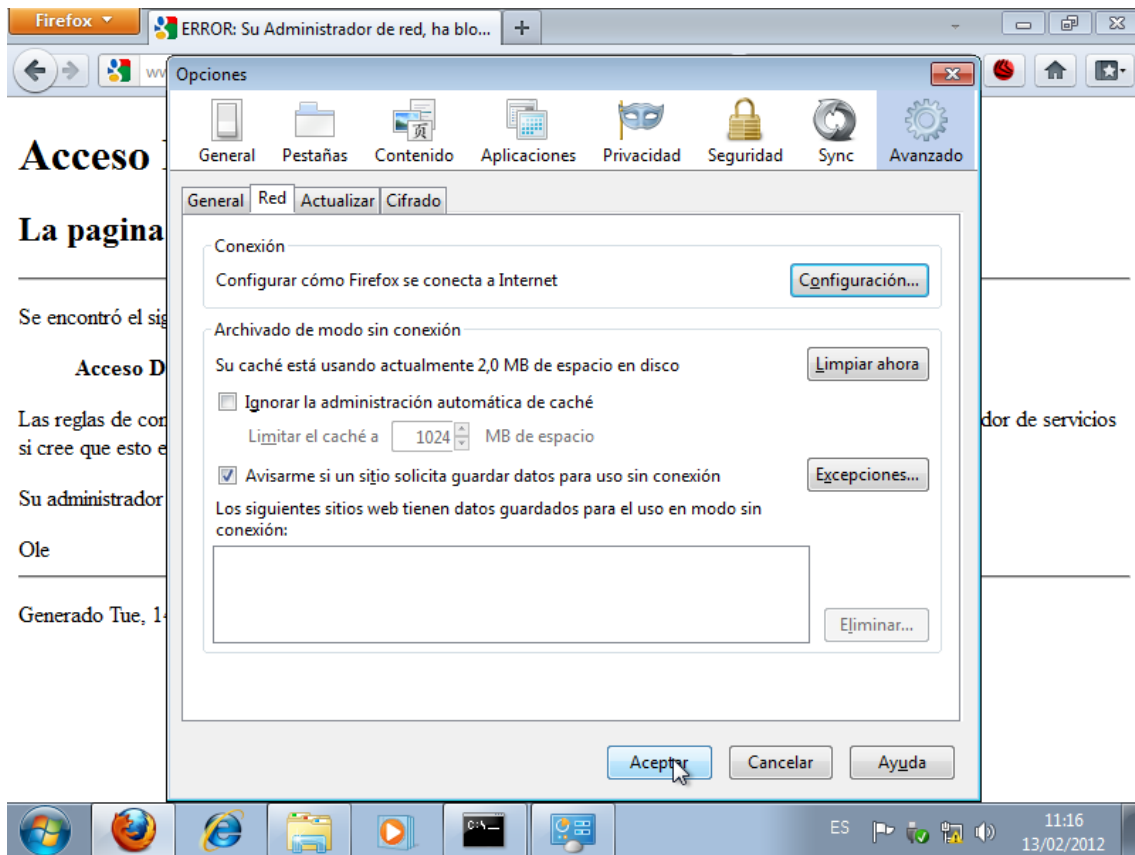
```
# The squid developers are interested in making squid available in
# a wide variety of languages. If you are making translations for a
# language that Squid does not currently provide please consider
# contributing your translation back to the project.
#
#Default:
error_directory /usr/share/squid/errors/es|
```

Reiniciamos los servicios de squid.

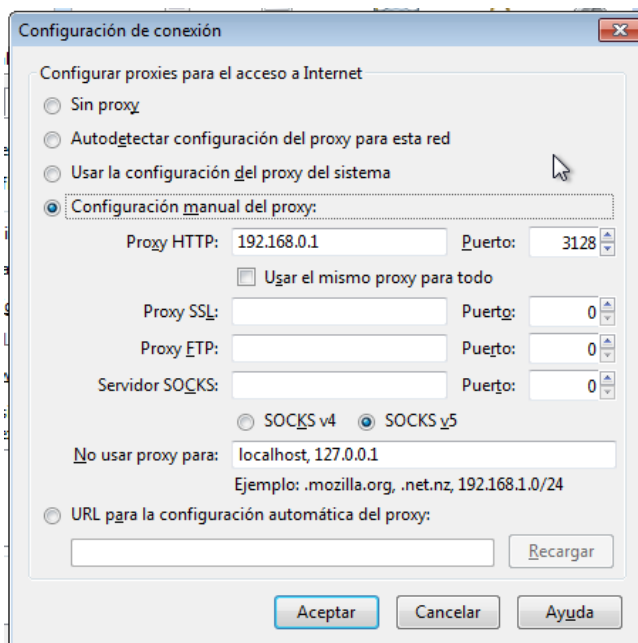
```
root@primoguijarro-desktop:/usr/share/squid/errors/es# /etc/init.d/squid restart
Rather than invoking init scripts through /etc/init.d, use the service(8)
utility, e.g. service squid restart

Since the script you are attempting to invoke has been converted to an
Upstart job, you may also use the restart(8) utility, e.g. restart squid
squid start/running, process 2646
root@primoguijarro-desktop:/usr/share/squid/errors/es#
```

Ahora en el navegador, toca configurarlo, le damos a Opciones, le damos a configurar una conexión a Internet.



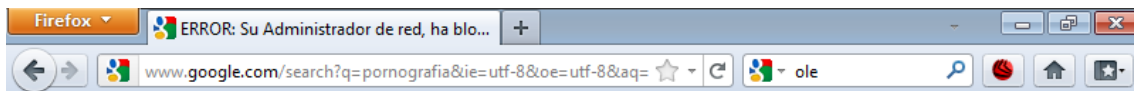
Asignamos la dirección IP del Servidor Proxy, y el puerto:



Aceptamos todo, y buscamos algo con contenido prohibido, por ejemplo:



Y como podemos ver salta el navegador, denegando el acceso.



## Acceso Denegado By PR1MO

### La pagina que solicita la he capado

Se encontró el siguiente error al intentar recuperar la dirección URL: <http://www.google.com/search?>

#### Acceso Denegado

Las reglas de control de acceso impiden que su petición sea permitida en este momento. Contacte con su proveedor de servicios si cree que esto es incorrecto.

Su administrador del caché es [webmaster](#).

Ole

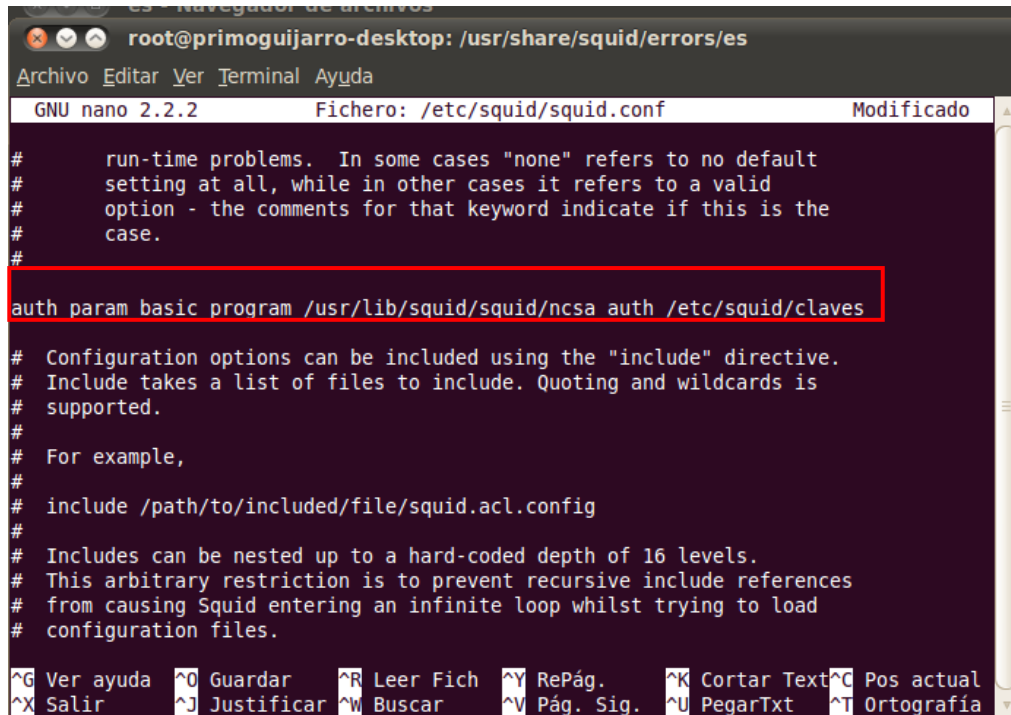
Generado Tue, 14 Feb 2012 19:24:03 GMT por primoguijarro-desktop (squid/2.7.STABLE7)





## AUTENTICACION

Descomentamos la siguiente línea, y al final ponemos la siguiente ruta donde será un archivo, donde asignaremos las claves de los usuarios:



```

root@primoguijarro-desktop: /usr/share/squid/errors/es
GNU nano 2.2.2      Fichero: /etc/squid/squid.conf      Modificado
#      run-time problems.  In some cases "none" refers to no default
#      setting at all, while in other cases it refers to a valid
#      option - the comments for that keyword indicate if this is the
#      case.
#
auth param basic program /usr/lib/squid/squid/ncsa_auth /etc/squid/claves
#
# Configuration options can be included using the "include" directive.
# Include takes a list of files to include. Quoting and wildcards is
# supported.
#
# For example,
#
# include /path/to/included/file/squid.acl.config
#
# Includes can be nested up to a hard-coded depth of 16 levels.
# This arbitrary restriction is to prevent recursive include references
# from causing Squid entering an infinite loop whilst trying to load
# configuration files.
^G Ver ayuda  ^O Guardar  ^R Leer Fich ^Y RePág.   ^K Cortar Text ^C Pos actual
^X Salir      ^J Justificar ^W Buscar    ^V Pág. Sig.  ^U PegarText  ^T Ortografía

```

Nos creamos el fichero claves, y le damos permisos.

Ahora agregamos un usuario Álvaro, con una contraseña con la siguiente forma:

```

root@primoguijarro-desktop:/etc/squid# touch claves
root@primoguijarro-desktop:/etc/squid# chmod 600 /etc/squid/claves
root@primoguijarro-desktop:/etc/squid# chown squid:squid /etc/squid/claves
chown: usuario inválido: «squid:squid»
root@primoguijarro-desktop:/etc/squid# htpasswd /etc/squid/claves alvaro
New password:
Re-type new password:
Adding password for user alvaro
root@primoguijarro-desktop:/etc/squid#

```

Guardamos y reiniciamos los servicios:

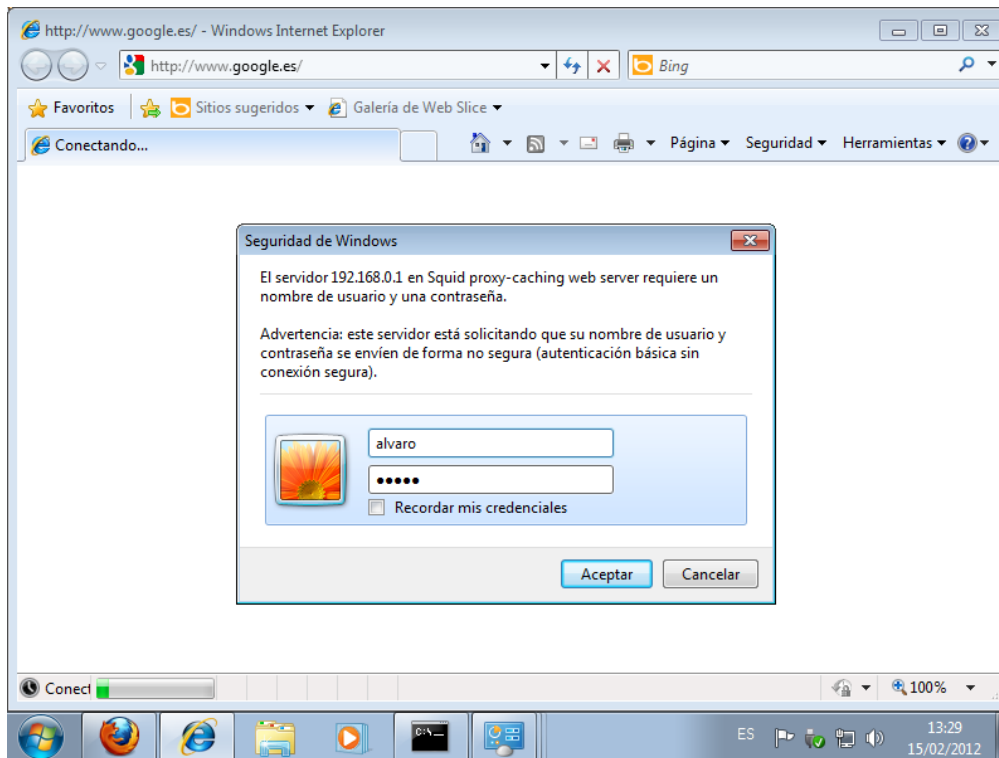
```

root@primoguijarro-desktop:/usr/share/squid/errors/es# /etc/init.d/squid restart
Rather than invoking init scripts through /etc/init.d, use the service(8)
utility, e.g. service squid restart

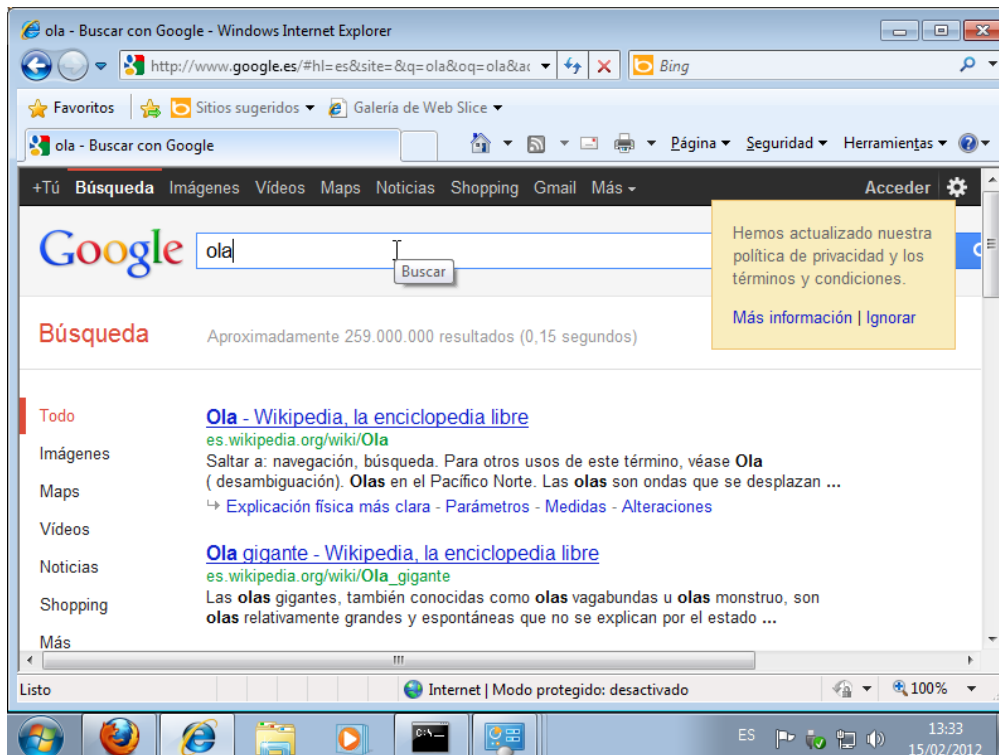
Since the script you are attempting to invoke has been converted to an
Upstart job, you may also use the restart(8) utility, e.g. restart squid
squid start/running, process 2646
root@primoguijarro-desktop:/usr/share/squid/errors/es#

```

Accedemos alguna pagina web, y nos pide la autenticación:



Comprobamos como podemos acceder correctamente y navegar a través del proxy web con autenticación:

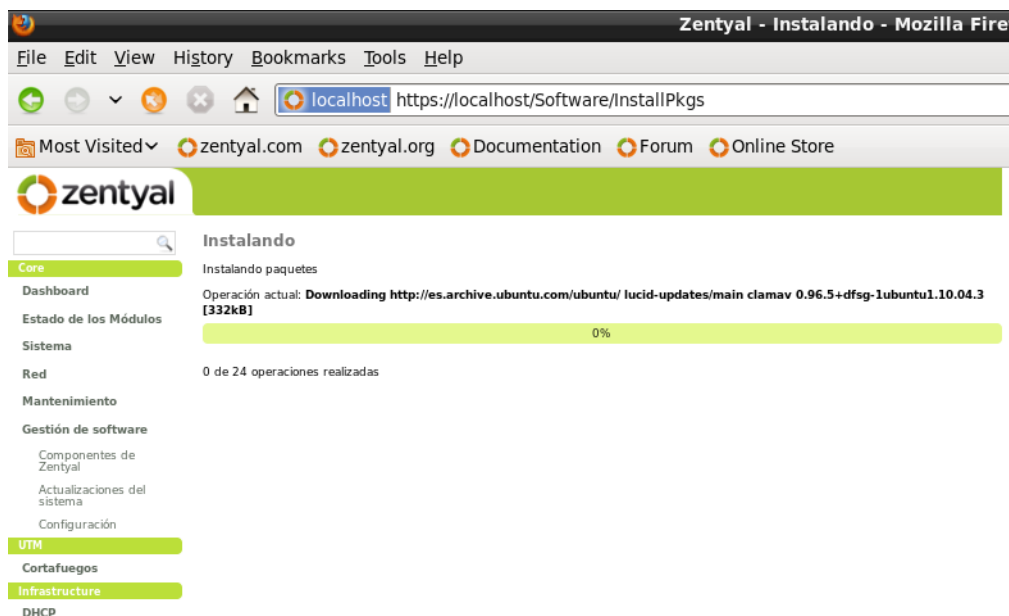


- **Instalación y configuración del servidor Proxy “Squid” en GNU/Linux utilizando Webmin.**
- **Instalación y configuración del servidor Proxy “Zentyal” en GNU/Linux.**

Instalamos el modulo HTTP Proxy en Zentyal.



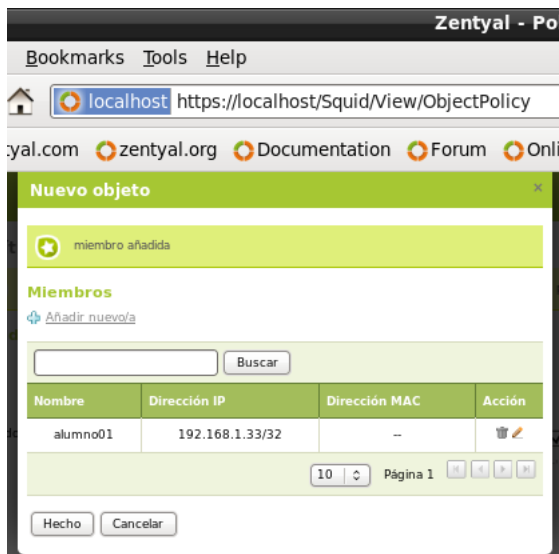
Esperamos a que se descargue:



Bloquemos la propaganda, le ponemos el puerto 3128:

Le asignamos una velocidad de descarga, y tamaño máximo de descarga, para limitar el tráfico de la red.

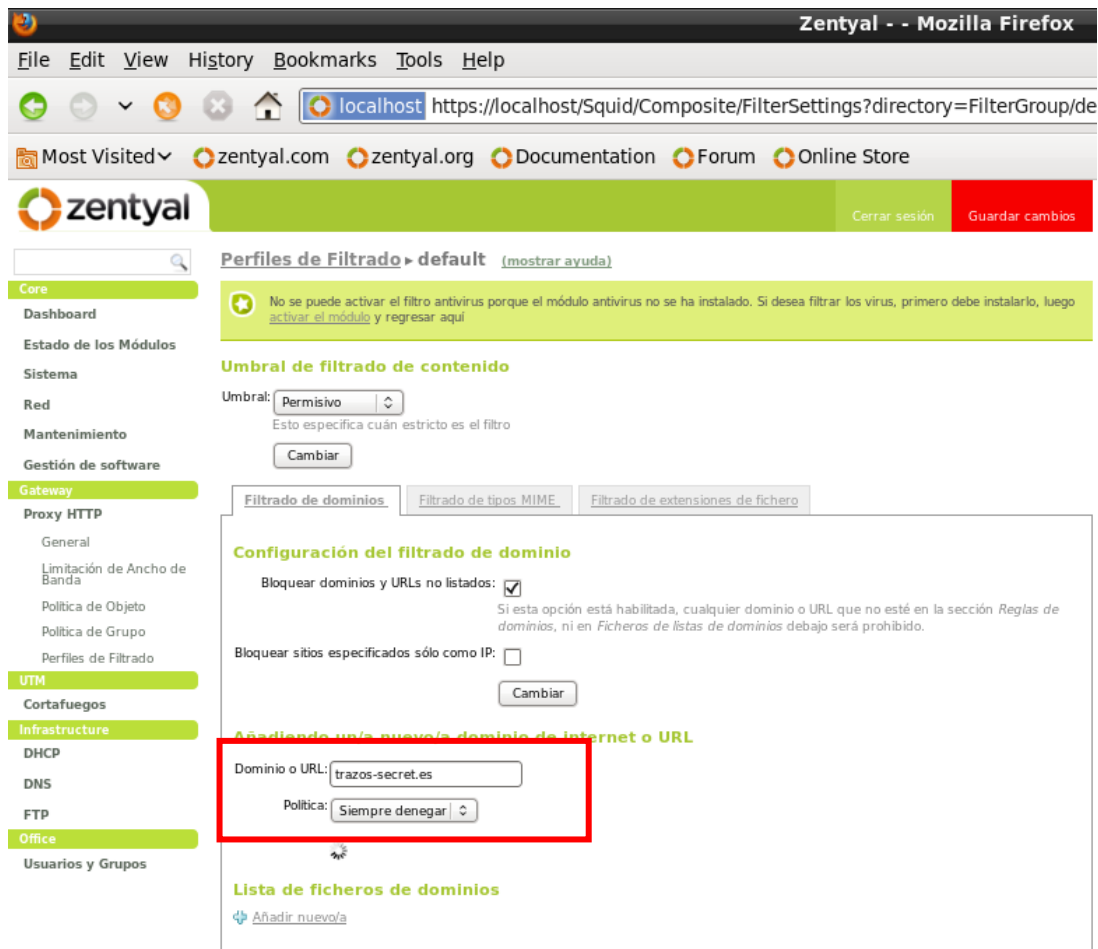
En política de Objeto añadimos un nuevo objeto, llamado alumno para la IP 192.168.1.33



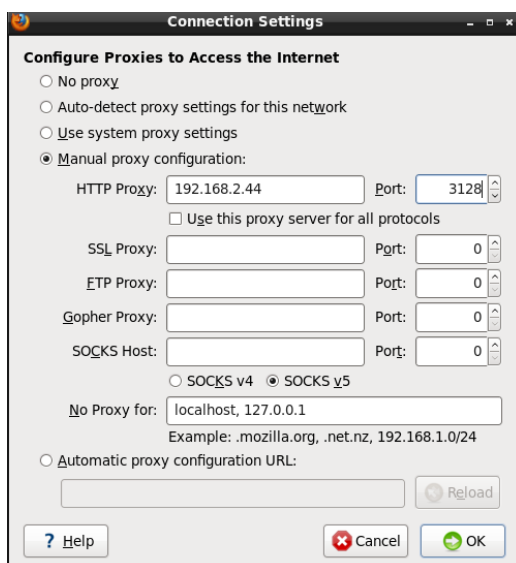
Le permitimos que solo acceda de 12:00-19:00. Los Lunes, Martes, Miércoles, Jueves y Viernes.



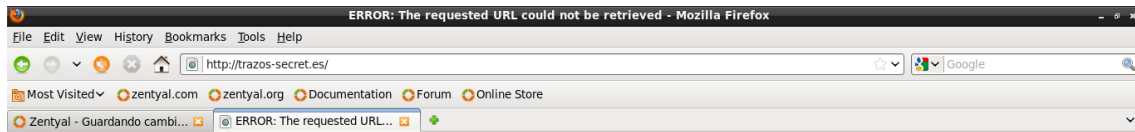
En la opción de Perfiles de filtrado, nos creamos uno para que no nos deje acceder a la pagina trazos-secret.es



Configuramos un cliente en el Navegador, con la dirección del servidor proxy.



Intentamos acceder a trazos-secret.es y comprobamos como nos da error.



## ERROR

### The requested URL could not be retrieved

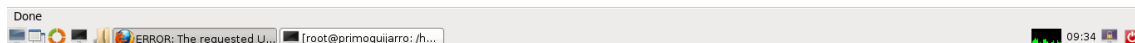
The following error was encountered while trying to retrieve the URL: <http://trazos-secret.es/>

#### Access Denied.

Access control configuration prevents your request from being allowed at this time. Please contact your service provider if you feel this is incorrect.

Your cache administrator is [webmaster](#).

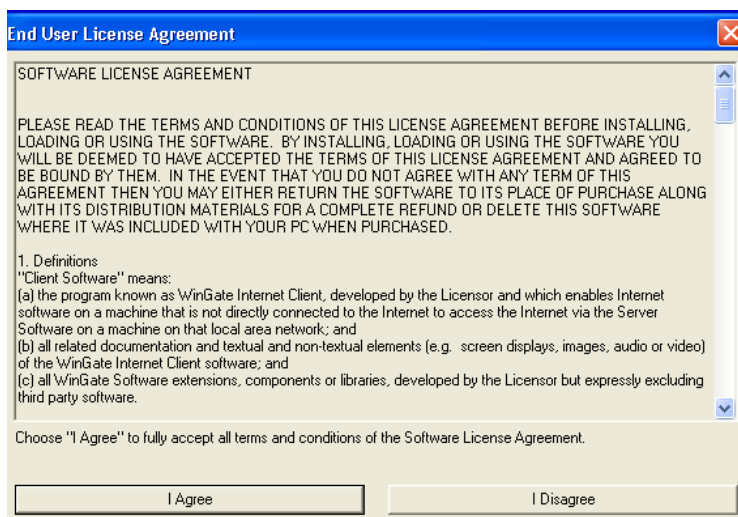
Generated Thu, 23 Feb 2012 08:34:30 GMT by primoguijarro.localdomain (squid/2.7.STABLE7)



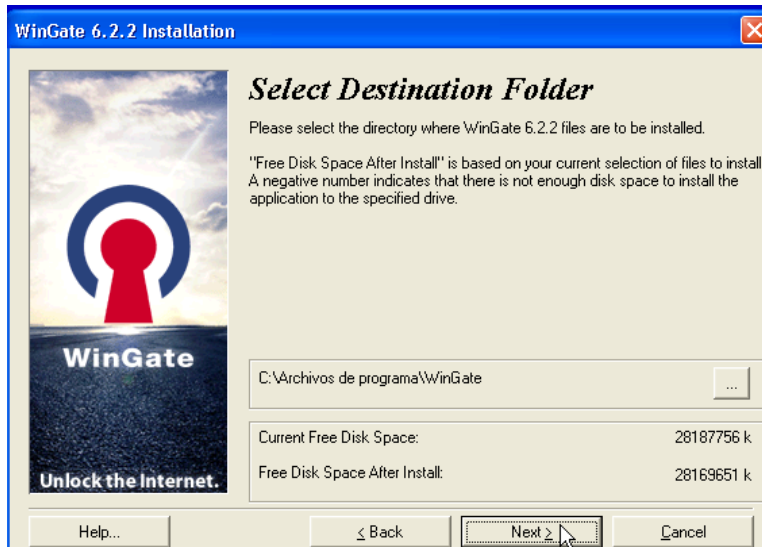
## ➤ Instalación y configuración del servidor Proxy “Wingate” en Windows.

Descargamos el software de la página oficial: <http://www.wingate.com>

Aceptamos las políticas...



Seleccionamos la ruta y le damos a siguiente.



Lo dejamos por defecto, y le damos a siguiente:

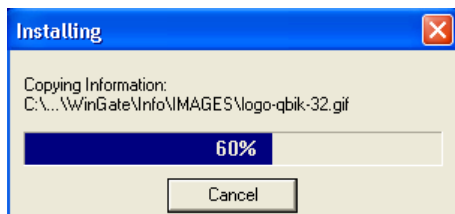




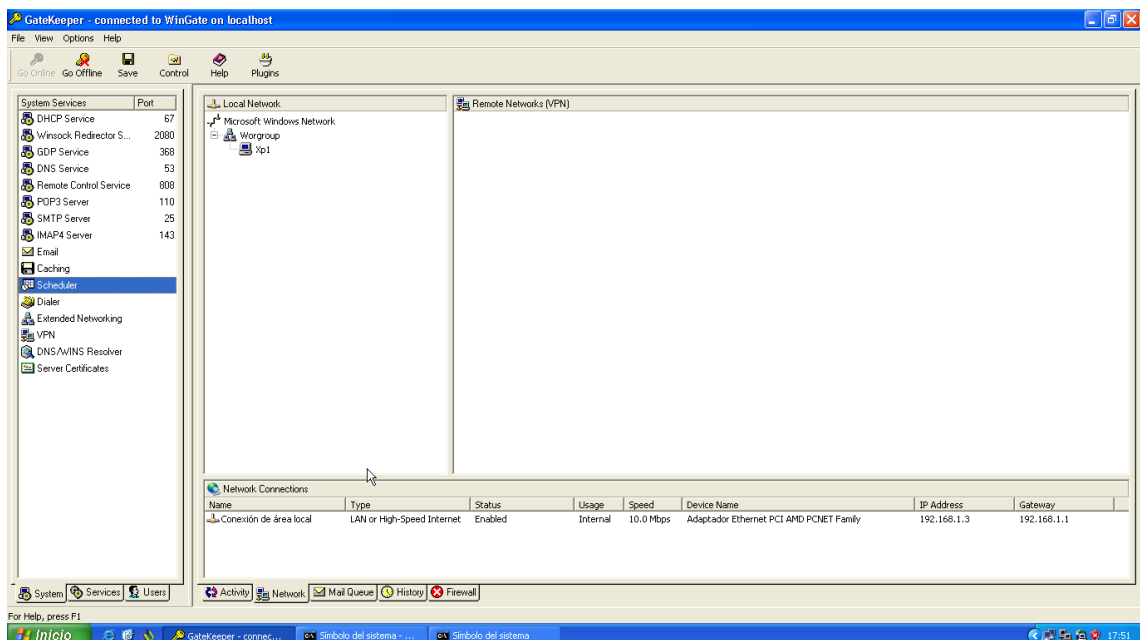
Marcamos la opción de Configurar Wingate Server.



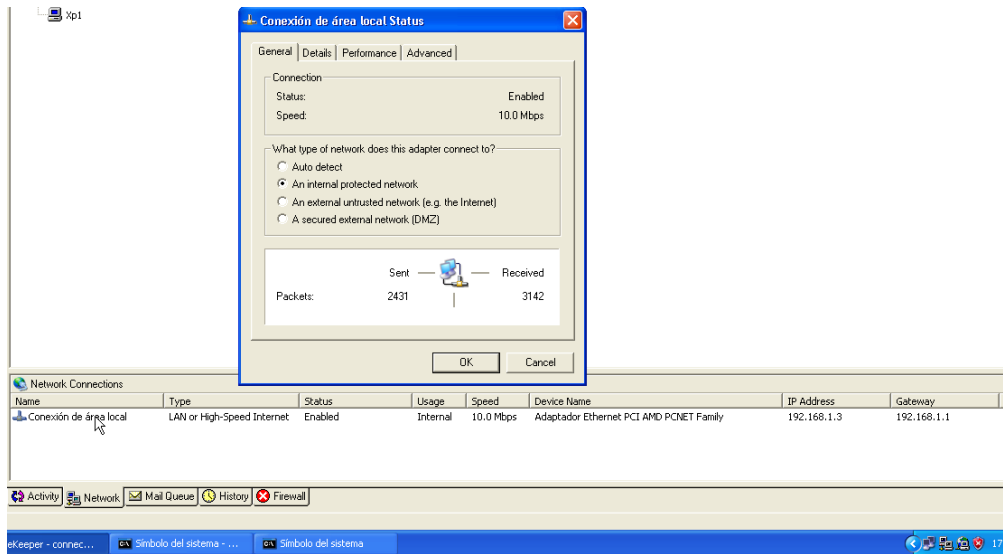
Comienza la instalación esperamos unos segundos.



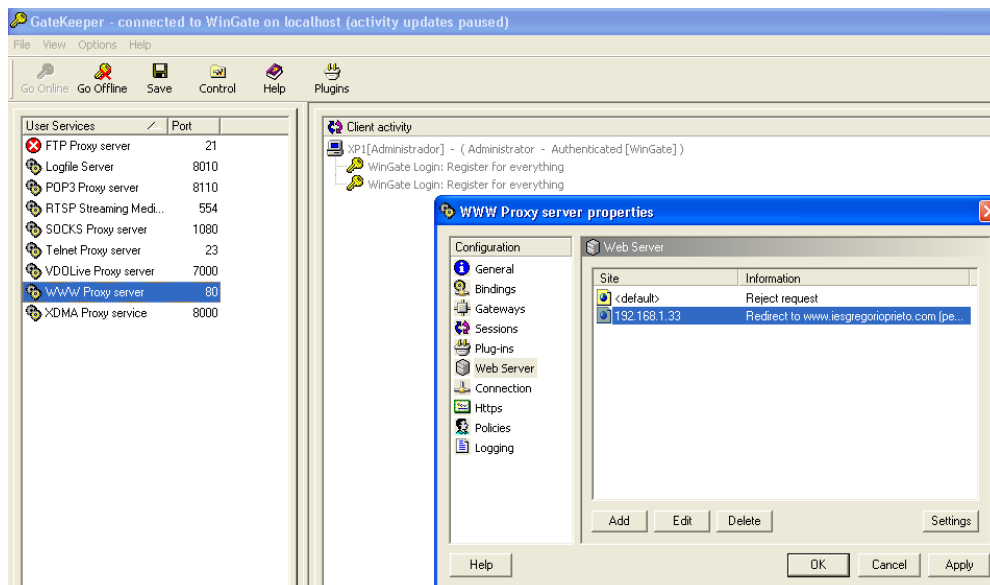
Aquí podemos ver la interfaz grafica de Wingate:



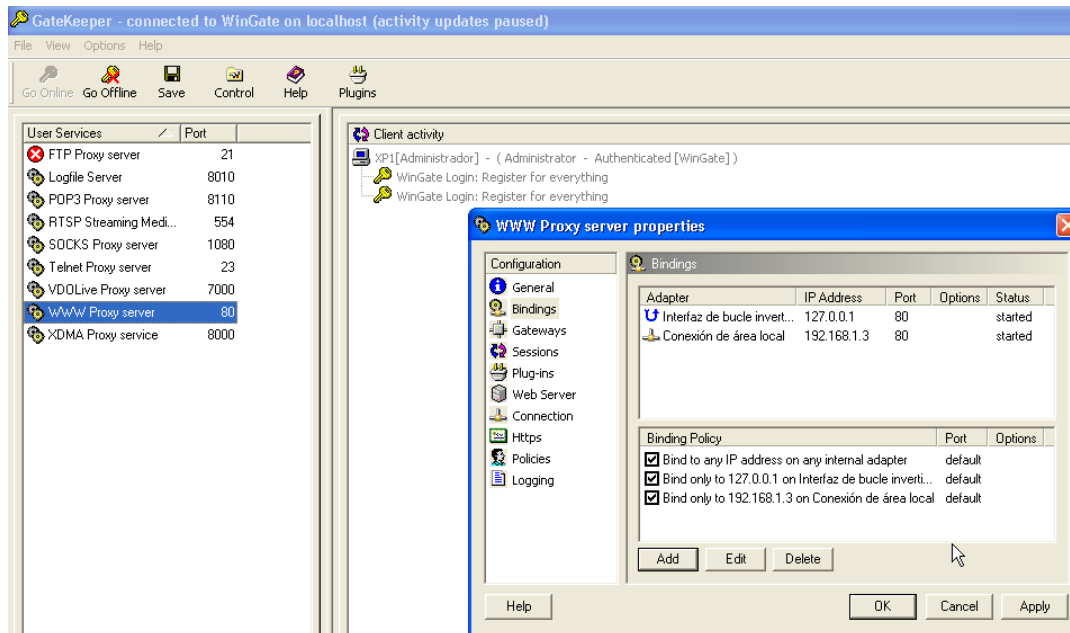
Abajo pinchamos en Conexión de área local y seleccionamos An internal protected network, esto quiere decir que este servidor proxy protejera una red interna.



En WWW Proxy Server, le vamos añadir una política que redirija a la pagina del instituto, solamente a la dirección ip 192.168.1.33

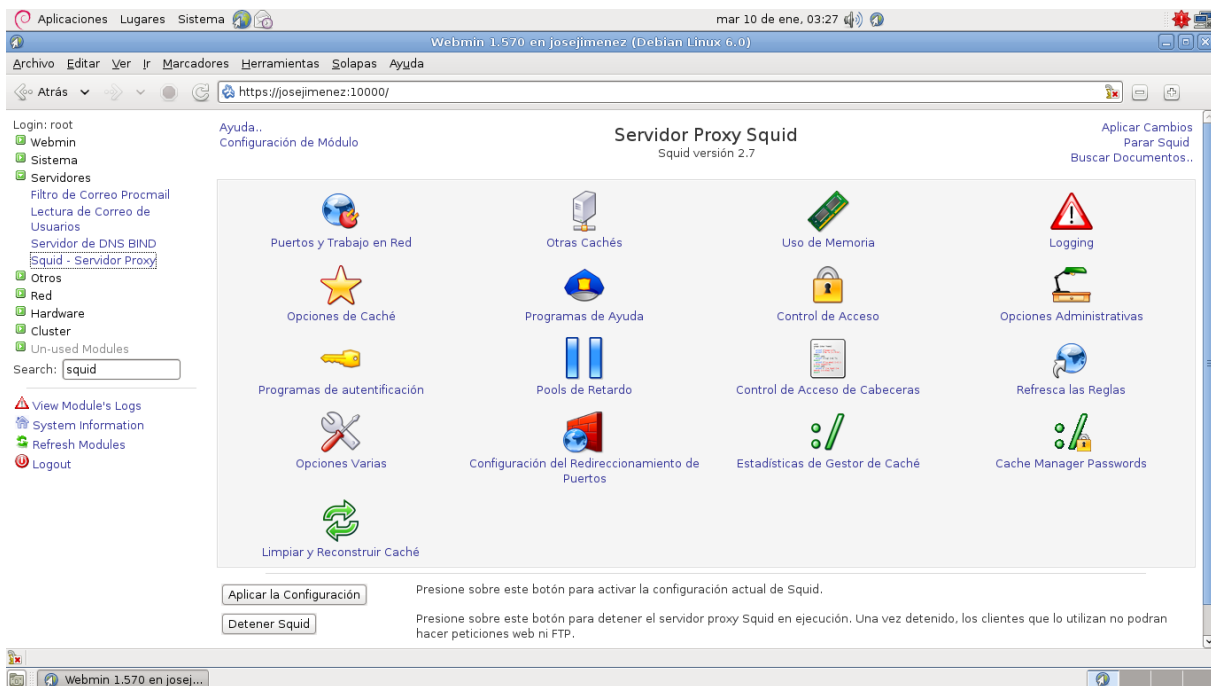


Para que funcione correctamente, añadimos la dirección ip del servidor Proxy.



## Instalación y configuración del servidor Proxy "Squid" en GNU/Linux utilizando Webmin.

Instalamos **squid**, para ello debemos tener conexión a internet, y Webmin instalado correctamente. Una vez instalado la interfaz grafica es parecido a esto:



Le damos a Puertos y trabajo de red. Configuramos la ip del servidor en nuestro caso realizamos un ifconfig, es la 192.168.1.163.

Ahora le damos a Control de acceso y abajo seleccionamos Expresion Regular de Ruta URL, porque denegaremos el acceso al tuenti.

Le asignamos un nombre razonable de acl, y le agregamos la dirección URL.

**Expresión Regular de Ruta URL ACL**

Nombre ACL:

Expresiones Regulares: ☐ ¿Ignorar mayúsculas?

URL de Fallo:

Almacenar ACL en archivo: ☒ Configuración Squid ☐ Separate file

☐ ¿Usar sólo contenidos existentes del archivo?

Aceptamos y le damos a la pestaña Restricciones Proxy, Añadir restricción proxy.

Webmin 1.570 en josejimenez (Debian Linux 6.0)

https://josejimenez:10000/

Login: root

Webmin

Sistema

Servidores

Filtro de Correo Procmail

Lectura de Correo de Usuarios

Servidor de DNS BIND

Squid - Servidor Proxy

Otros

Red

Hardware

Cluster

Un-used Modules

Search: squid

View Module's Logs

System Information

Refresh Modules

Logout

Índice de Módulo

Ayuda..

Control de Acceso

Restricciones Proxy

Restricciones ICP

Programas externos ACL

Reply proxy restrictions

Añadir restricción proxy

Acción	ACLs	Mover
<input type="checkbox"/> Denegar	denegar_tuenti	↓
<input type="checkbox"/> Permitir	permitir_clientes	↓↑
<input type="checkbox"/> Permitir	manager localhost	↓↑
<input type="checkbox"/> Permitir	purge localhost	↓↑
<input type="checkbox"/> Denegar	manager	↓↑
<input type="checkbox"/> Denegar	purge	↓↑
<input type="checkbox"/> Denegar	!Safe_ports	↓↑
<input type="checkbox"/> Denegar	CONNECT !SSL_ports	↓↑
<input type="checkbox"/> Denegar	denegar_tuenti	↓↑
<input type="checkbox"/> Permitir	localhost	↓↑
<input type="checkbox"/> Denegar	all	↑

Añadir restricción proxy

Delete Selected Restrictions

Regresar a índice squid

https://josejimenez:10000/squid/http\_access.cgi?new=1

Webmin 1.570 en josej...

La seleccionamos y le damos a Denegar. Aceptamos .

**Restricción de Proxy**

Acción: ☐ Permitir ☒ Denegar

Coincidir con ACLs:

No coincidir con ACLs:

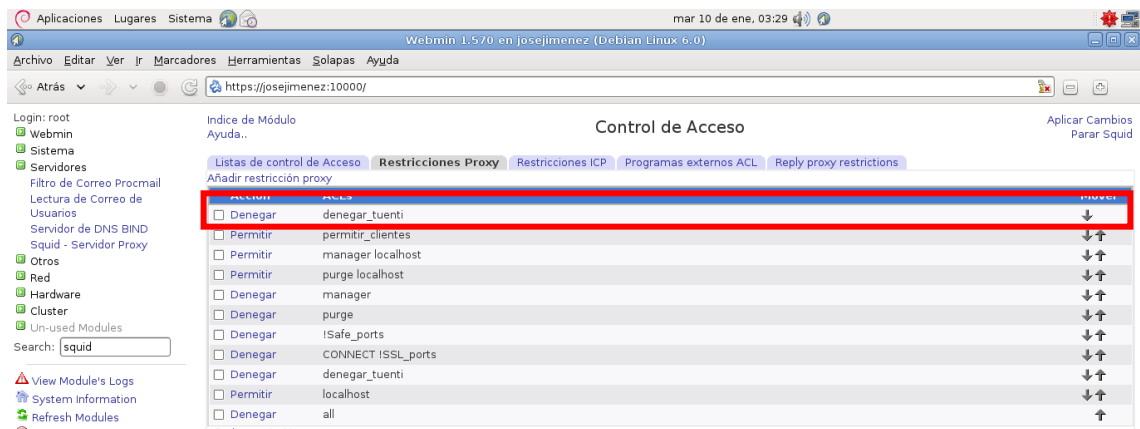
ACLs:

- SSL\_ports
- Safe\_ports
- purge
- CONNECT
- shoutcast
- apache
- permitir\_windows
- denegar\_tuenti
- permitir\_clientes
- horarios\_den

ACLs:

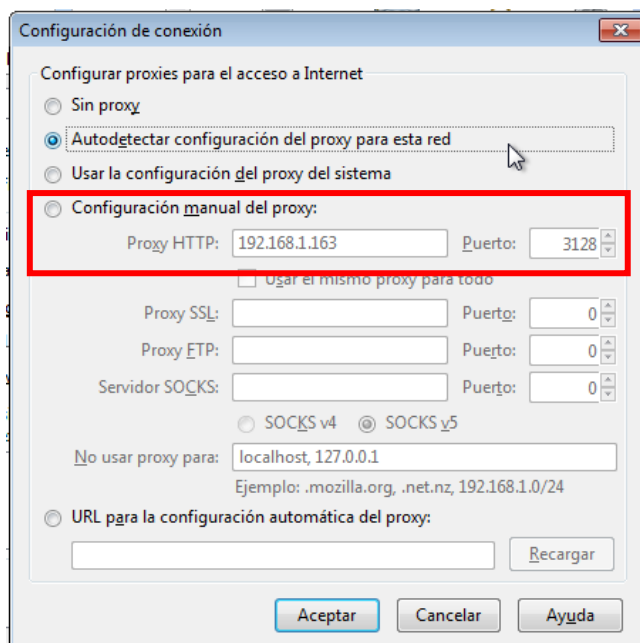
- all
- manager
- localhost
- to\_localhost
- localnet
- SSL\_ports
- Safe\_ports
- purge
- CONNECT
- shoutcast

Ahora lo que haremos será subirla la primera, con las flechitas.

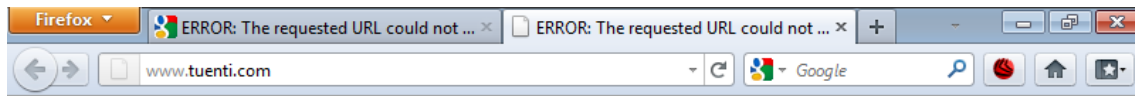


Ahora configuramos un cliente navegador de la red, con la dirección ip 192.168.1.163 y el puerto 3128.

Y marcamos la opción Configuración manual del proxy.



Intentamos acceder a [www.tuenti.com](http://www.tuenti.com) , y no nos deja.



## ERROR BY PR1MO

### The requested URL could not be retrieved

The following error was encountered while trying to retrieve the URL: <http://tuenti.com>

#### Access Denied.

Access control configuration prevents your request from being allowed at this time. Please contact your service provider if you feel this is incorrect.

Your cache administrator is [webmaster](#).

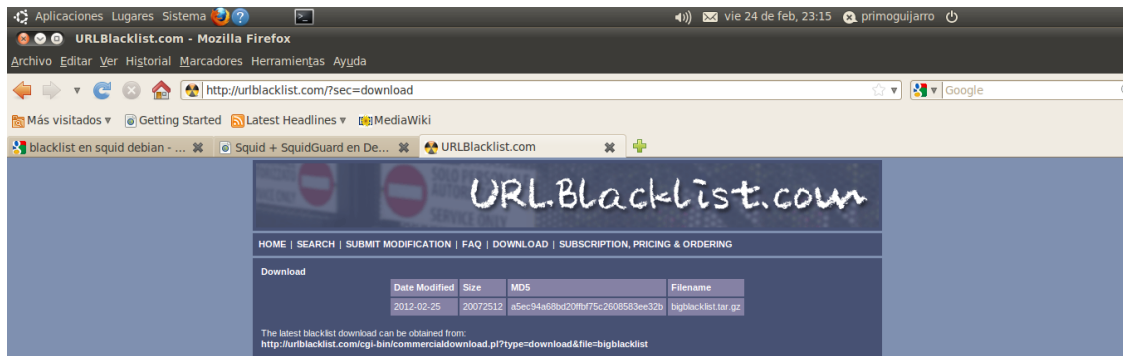
Generated Tue, 10 Jan 2012 02:17:54 GMT by PR1MO (squid/2.7.STABLE9)



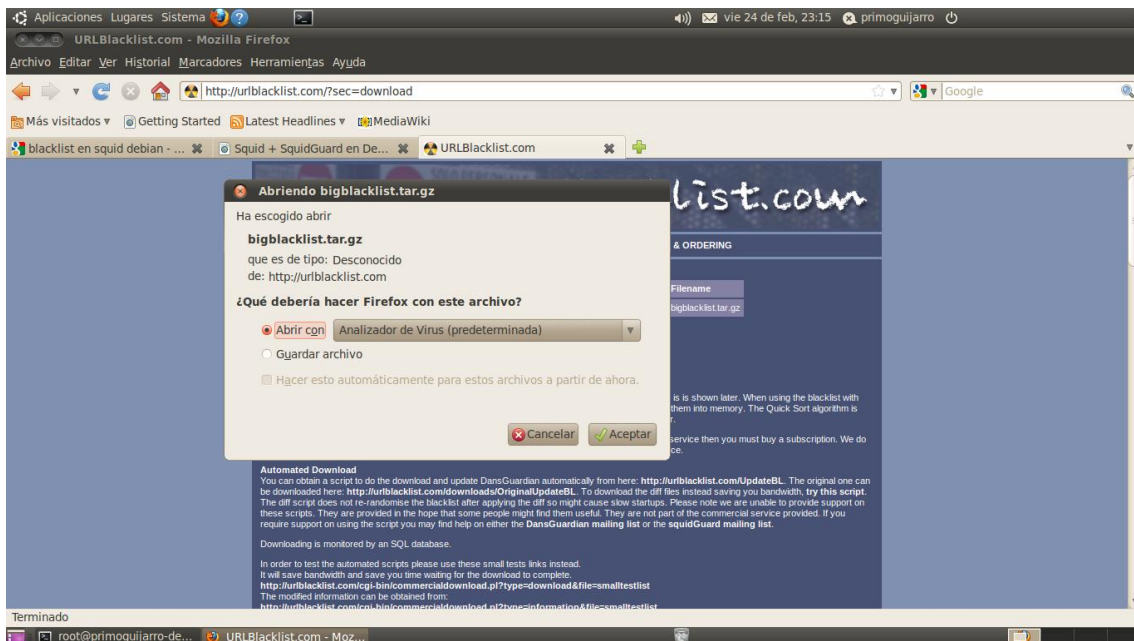


Descarga archivo de listas negras de sitios web y anexa las mismas a la configuración de Squid. <http://urlblacklist.com/>. Prueba dichas listas negras.

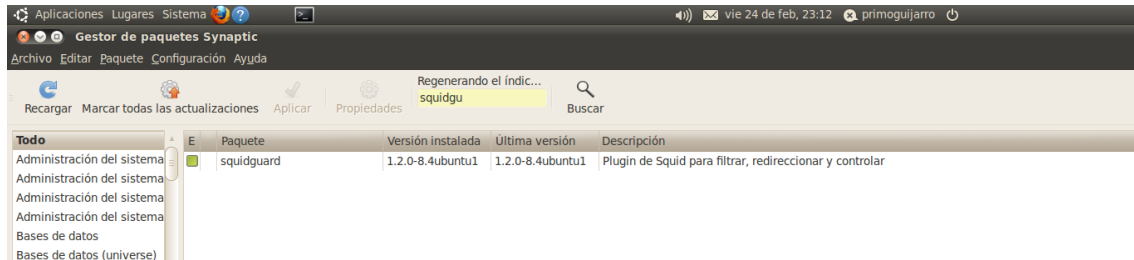
Nos vamos a <http://urlblacklist.com/>. Y descargamos las listas negras.



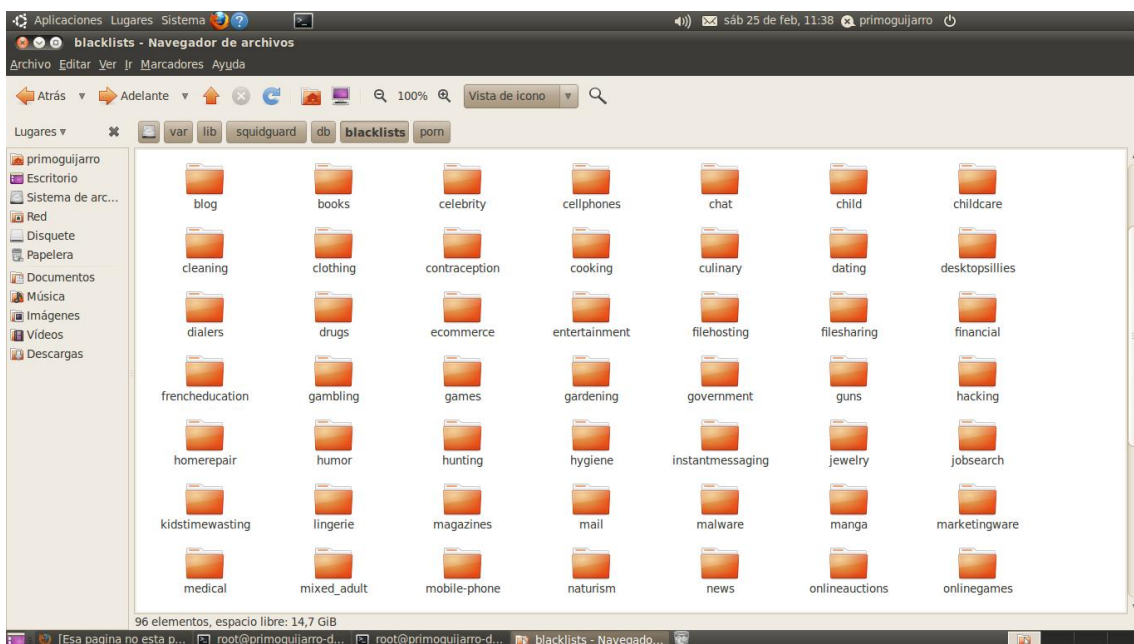
Lo guardamos.



Instalamos squidguard, será el encargado de utilizar las blacklists.



Se descomprime el archivo blacklist en la carpeta /var/lib/squidguard/db, de modo que tienen que quedar una estructura de directorios parecida a esto:



Editamos el archivo de configuración de squid, para añadir las siguientes líneas:

```

root@primoguijarro-desktop: /var/lib/squidguard/db
Archivo Editar Ver Terminal Ayuda
GNU nano 2.2.2 Fichero: /etc/squid/squid.conf Modificado
#
#       tcpkeepalive[=idle,interval,timeout]
#       Enable TCP keepalive probes of idle connections
#       idle is the initial time before TCP starts probing
#       the connection, interval how often to probe, and
#       timeout the time before giving up.
#
#       If you run Squid on a dual-homed machine with an internal
#       and an external interface we recommend you to specify the
#       internal address:port in http_port. This way Squid will only be
#       visible on the internal address.
#
# Squid normally listens to port 3128
http_port 3128 transparent
url_rewrite_program /usr/bin/squidGuard -c /etc/squid/squidGuard.conf
# TAG: https_port
# Note: This option is only available if Squid is rebuilt with the
^G Ver ayuda ^O Guardar ^R Leer Fich ^Y RePág. ^K Cortar Tex ^C Pos actual
^X Salir ^J Justificar ^W Buscar ^V Pág. Sig. ^U PegarTxt ^T Ortografía

```

Reiniciamos squid, ahora vamos al archivo de configuración de squiguard.

Estas líneas son importantes porque dicen donde están las blacklists

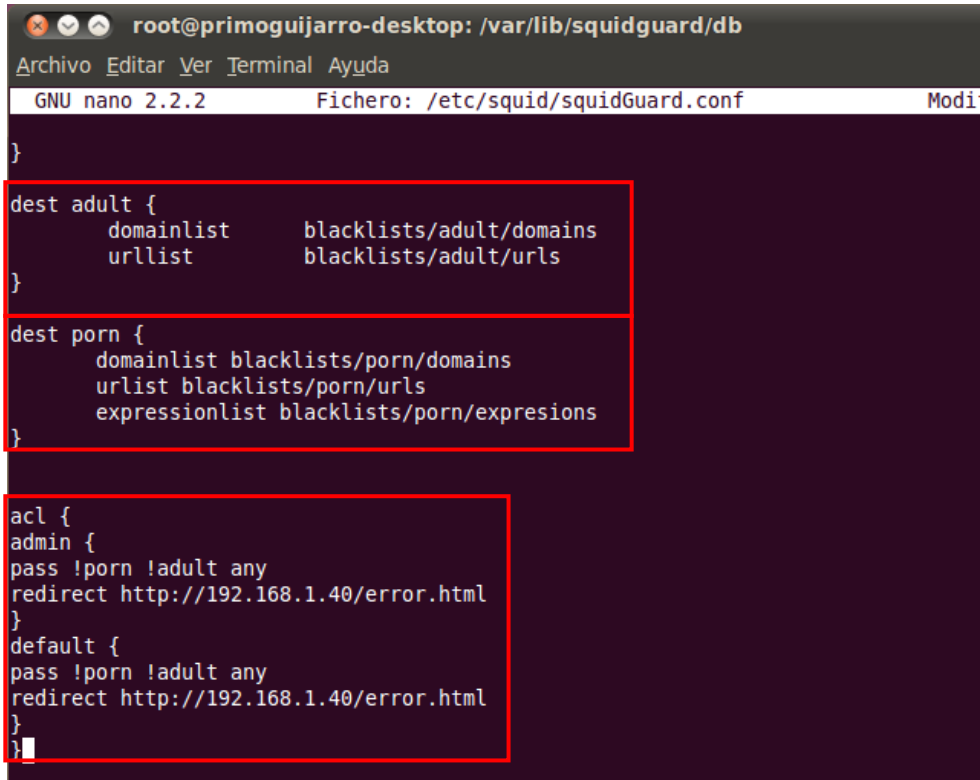
```

root@primoguijarro-desktop: /var/lib/squidguard/db
Archivo Editar Ver Terminal Ayuda
GNU nano 2.2.2 Fichero: /etc/squid/squidGuard.conf Modi
#
# CONFIG FILE FOR SQUIDGUARD
#
dbhome /var/lib/squidguard/db
logdir /var/log/squid
#
# TIME RULES:
# abbrev for weekdays:
# s = sun, m = mon, t = tue, w = wed, h = thu, f = fri, a = sat
time workhours {
    weekly mtwhf 08:00 - 16:30
    date *-*-01 08:00 - 16:30
}
#
# REWRITE RULES:
#
#rew dmz {
#   s@://admin/@://admin.foo.bar.no/@i
#   s@://foo.bar.no/@://www.foo.bar.no/@i

```

Mas abajo configuramos lo siguiente:

Le indicamos que no queremos que se vean las paginas con el contenido para adult y porn, además le indicamos una pagina de error, que crearemos posteriormente.



```
root@primoguijarro-desktop: /var/lib/squidguard/db
Archivo Editar Ver Terminal Ayuda
GNU nano 2.2.2 Fichero: /etc/squid/squidGuard.conf Modi
}
dest adult {
    domainlist blacklists/adult/domains
    urlist blacklists/adult/urls
}
dest porn {
    domainlist blacklists/porn/domains
    urlist blacklists/porn/urls
    expressionlist blacklists/porn/expresions
}

acl {
    admin {
    pass !porn !adult any
    redirect http://192.168.1.40/error.html
    }
    default {
    pass !porn !adult any
    redirect http://192.168.1.40/error.html
    }
}
```

Para que se guarden los cambios tendremos que hacer lo siguiente:

```
root@primoguijarro-desktop:/var/lib/squidguard/db# update-squidguard
Double checking directory and file permissions...done!
Re-building SquidGuard db files...done!
Reloading Squid...done!
root@primoguijarro-desktop:/var/lib/squidguard/db#
```

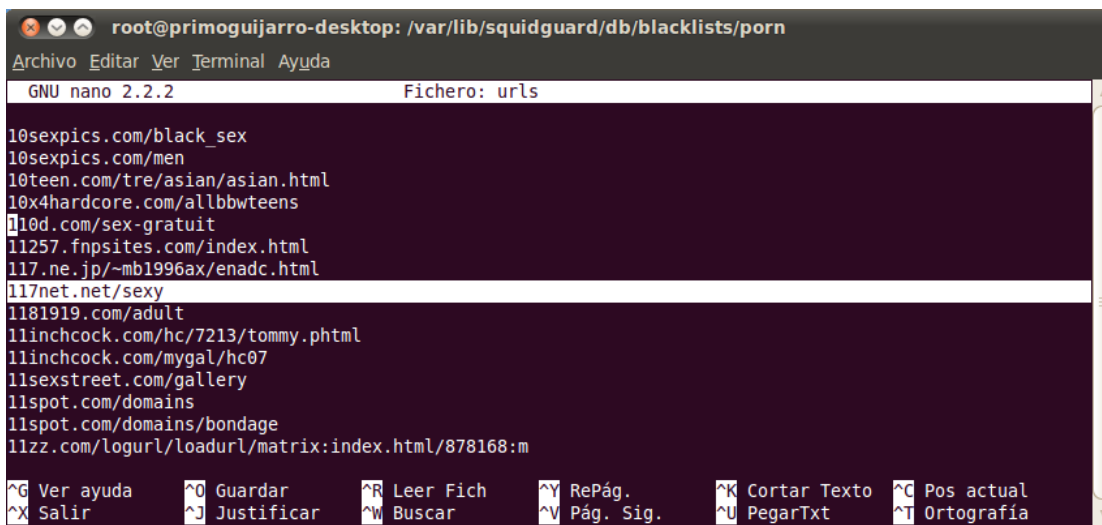
Creamos el archivo `/var/www/error.html`



```
root@primoguijarro-desktop: /home/primoguijarro
primoguijarro@primoguijarro-desktop: ~
GNU nano 2.2.2 Fichero: /var/www/error.html
<html>
<head><title>Esa pagina no esta permitida en esta organizacion</title></head>
<body><h1>Esa pagina no esta permitida en la organizacion de PRIMO</h1></body>
</html>
[ 4 líneas leídas ]
^G Ver ayuda  ^O Guardar  ^R Leer Fich  ^Y RePág.  ^K Cortar Texto  ^C Pos actual
^X Salir      ^J Justificar  ^W Buscar    ^V Pág. Sig.  ^U PegarTxt    ^T Ortografía
```

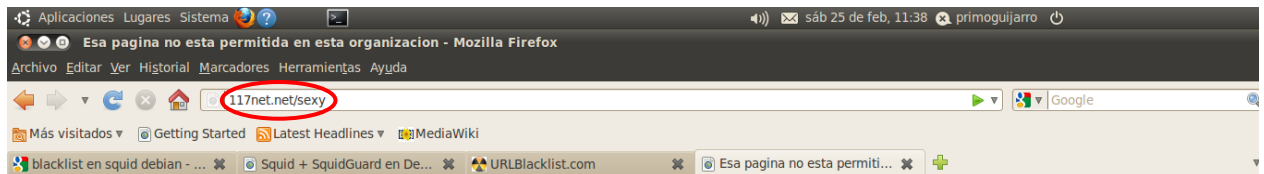
Guardamos y abrimos el fichero `urls`, de la carpeta `porn` en `blacklists`.

Probaremos con la dirección siguiente.



```
root@primoguijarro-desktop: /var/lib/squidguard/db/blacklists/porn
GNU nano 2.2.2 Fichero: urls
10sexpics.com/black_sex
10sexpics.com/men
10teen.com/tre/asian/asian.html
10x4hardcore.com/allbbwteens
110d.com/sex-gratuit
11257.fnpsites.com/index.html
117.ne.jp/~mb1996ax/enadc.html
117net.net/sexy
1181919.com/adult
11inchcock.com/hc/7213/tommy.phtml
11inchcock.com/mygal/hc07
11sexstreet.com/gallery
11spot.com/domains
11spot.com/domains/bondage
11zz.com/logurl/loadurl/matrix:index.html/878168:m
^G Ver ayuda  ^O Guardar  ^R Leer Fich  ^Y RePág.  ^K Cortar Texto  ^C Pos actual
^X Salir      ^J Justificar  ^W Buscar    ^V Pág. Sig.  ^U PegarTxt    ^T Ortografía
```

Introducimos la url y nos sale la pagina denegada.



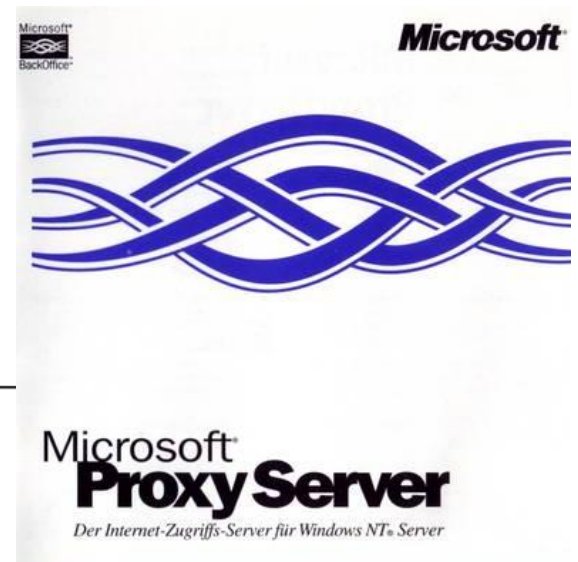
**Esa pagina no esta permitida en la organizacion de PR1MO**

**Documenta la relación de productos que tiene y ha tenido Microsoft en relación a servidores “Proxy”. ¿Qué función tiene actualmente Microsoft Forefront TMG Treat Managment Gateway?. Describe su instalación y configuración.**

ADEMAS DE MICROSOFT TMG, MICROSOFT TAMBIEN TIENE [PROXY SERVER](#)

Proxy Server actúa como un gateway o pasarela segura para conectar su red local LAN a Internet. Gateway se refiere un software u ordenador ejecutando software que permite la comunicación entre dos redes.

Usando un gateway Proxy Server, usted será capaz de proteger su red contra intrusos. El Gateway actúa como una barrera que le permitirá



hacer peticiones a Internet y recibir información, pero no permitirá el acceso a su red de usuarios no autorizados.

Usted puede configurar Proxy Server para permitir la comunicación de sus estaciones de trabajo con servicios remotos en Internet. Cuando seleccione el hardware apropiado para un ordenador ejerciendo funciones de Gateway o pasarela, asegúrese de que tiene el adecuado ancho de banda para la conexión a Internet y planifique con cuidado la seguridad para proteger su LAN.

Para ejecutar Proxy Server, el ordenador debe estar ejecutando Windows NT 4.0 o posterior. El ordenador debe también tener dos adaptadores o tarjetas de red. Una de ellas conectará su servidor Proxy a su red local, y la otra le conectará a Internet.

Proxy Server consta de dos servicios: Web Proxy y WinSock Proxy (WSP).

- Web Proxy. Soporta HTTP, lectura FTP y gopher para ordenadores de la intranet ejecutando TCP/IP.

- WinSock Proxy. Soporta protocolos Windows Sockets como Telnet y RealAudio para ordenadores en intranet ejecutando TCP/IP o Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX).

## Microsoft Forefront TMG Threat Management Gateway



### Información general

El Service Pack incluye nueva funcionalidad y mejoras de características:

#### Nuevos informes

- El nuevo informe de actividad de sitio muestra la transferencia de datos entre los usuarios y sitios web específicos.

#### Páginas de error

- Las páginas de error tienen una nueva apariencia.
- Ahora es más fácil personalizar las páginas de error e incluir objetos incrustados.

#### Autenticación Kerberos

- Ahora puede utilizar autenticación Kerberos al implementar una matriz con equilibrio de carga de red (NLB).

Para leer las notas de la versión, vea Forefront TMG Release Notes (SP2) [Notas de la versión de Forefront TMG (SP2)].

Principio de página

## Requisitos del sistema

- **Sistemas operativos compatibles:** Windows Server 2008; Windows Server 2008 R2

- Forefront TMG 2010 Standard Edition SP1 con la Actualización 1
- Forefront TMG 2010 Enterprise Edition SP1 con la Actualización 1

### Nota importante sobre la instalación del SP2

Antes de instalar este Service Pack, es muy recomendable que lea el artículo de TechNet Installing Forefront TMG Service Packs (Instalación de Service Packs de Forefront TMG). No se ofrece soporte para la instalación del Service Pack en los equipos de Forefront TMG en un orden distinto al descrito en este artículo.

Principio de página

## Instrucciones

1. Haga clic en el botón **Descargar** de esta página.
2. Haga clic en **Guardar** para descargar en el equipo.
3. Lea el artículo de TechNet Installing Forefront TMG Service Packs (Instalación de Service Packs de Forefront TMG) como orientación para la implementación.

## Evaluación del producto

En la sección Evaluación del producto Forefront TMG se ofrece un resumen de las novedades de la versión más reciente, una comparación entre Forefront TMG Standard Edition y Enterprise Edition, y la información sobre cómo adquirir una versión de software de evaluación del producto.

## Introducción

En la sección Introducción a Forefront TMG se ofrece la información y las notas de la versión acerca del uso de los métodos abreviados de teclado para seleccionar comandos y para navegar en los paneles de consola y entre ellos.

## Planeación y diseño

Use la sección Planeación y diseño de Forefront TMG para comenzar a implementar Forefront TMG. Las guías de planeación y diseño le permiten identificar estrategias de diseño y hacerlas coincidir con sus requisitos de implementación. Las guías de diseño se proporcionan para cada fase de implementación y operaciones de Forefront TMG, incluyendo la planeación para alta disponibilidad y escalabilidad, asegurando el acceso a la web y a los recursos corporativos internos, protegiendo los equipos y servidores de la red extendida y administrando su implementación de Forefront TMG.



## **Implementación**

Use la guía Implementación de Forefront TMG conforme instala Forefront TMG y configure las redes y enrutamiento, la configuración del cliente y el servidor de Forefront TMG, las matrices de Forefront TMG y la Protección de acceso a redes. En Implementación de Forefront TMG también encontrará guías de soluciones descentralizadas para interoperabilidad con BranchCache, y para planeación, implementación y configuración de una puerta de enlace web segura de Forefront TMG.

## **Operaciones**

La guía Operaciones de Forefront TMG ofrece información para ayudarle a configurar el acceso seguro a Internet y a los recursos corporativos, a configurar la protección de los equipos y los servidores de la red extendida, y a administrar las operaciones diarias para sus servidores de Forefront TMG.

## **Solucionar problemas**

En la sección Forefront TMG Troubleshooting se ofrece información que puede ayudarle a solucionar problemas de Forefront TMG, incluyendo cómo usar el registro de diagnóstico, las instrucciones de solución de problemas para la instalación y configuración de Forefront TMG, y la solución de problemas para la protección del acceso web.

En Unsupported configurations se resumen las configuraciones no admitidas habituales y los escenarios que puede encontrar al implementar y mantener Forefront TMG.

## **Referencia técnica**

En la sección Forefront TMG Technical Reference se incluyen temas de referencia detallados acerca de Forefront TMG, incluyendo la documentación para herramientas de administración, aplicaciones de seguridad y otros componentes que se integran con la plataforma de Forefront TMG y se compilan en ella.