

Documentación PROXY

Instalar PROXY Linux

- apt-get update
- apt-get install squid3

Configurar PROXY Linux

- Ir en /etc/squid3/squid.conf
 - acl aaron src 192.168.19.66
 - acl marca dstdomain www.marca.com
 - http_access deny marca
 - http_access allow aaron
- http_access allow/deny regla

Mozilla

IP Puerto 3128

Práctica 1

```
acl all src all
acl servidor src 192.168.19.203
acl subnet src 192.168.19.200-192.168.19.210
acl safe_ports port 80 443
acl post method POST
acl marca dstdomain www.marca.com
acl ip_sin_internet src 192.168.19.203-192.168.19.205

http_access deny post
http_access deny marca
http_access deny ip_sin_internet
http_access allow subnet safe_ports
http_access deny all
```

Práctica 2

Un client ens ha demanat que configurem el seu proxy per a que:

El cap i la seua filla puguem accedir a internet sense restriccions (IP's: 192.168.10.100 i 192.168.10.101)

Ara bé, la resta de personal que treballa a l'empresa només podrà accedir a Internet en l'horari de 14h a 16h, que és l'horari de dinar.

Durant tot l'horari de treball podran accedir a la pàgina web de l'empresa. (8-20h) i a més a més no podran descarregar-se cap contingut multimedia

Heu de treballar amb fitxers addicional sempre que siga possible

L'empresa treballa amb la xarxa 192.168.10.0/24

```
acl familia src 192.168.10.100 192.168.10.101
```

```
acl treballadors src 192.168.10.0/24
```

```
acl dinar time MTWHF 14:00-16:00
```

```
acl treball time MTWHF 8:00-20:00
```

```
acl descarregar urlpath_regex "/etc/squid3/regex"
```

```
acl paginaempresa dstdomain "/etc/squid3/dstdomain"
```

```
http_access allow familia
```

```
http_access allow treballadors dinar descarregar paginaempresa
```

```
http_access allow treballadors treball !descarregar paginaempresa
```

```
http_access deny treballadors
```

En el arxiu "/etc/squid3/regex" insertem:

```
.AVI$ .MPG$ .WAV$ .MP3$
```

En el arxiu "/etc/squid3/dstdomain" insertem:

```
www.miguel.com
```

Solució 2

```
acl redlocal src 192.168.10.0/24  
acl pare_filla src 192.168.10.100 192.168.10.101  
acl permeses dstdomain "/etc/squid3/dstdomain"  
acl horari_dinar time MTWHF 14:00-16:00  
acl horari time MTWHF 08:00-20:00  
acl extensions urlpath_regex "/etc/squid3/regex"
```

```
http_access allow pare_filla  
http_access allow horari_dinar  
http_access deny redlocal !permeses !horari  
extensions
```

En el arxiu "/etc/squid3/regex" insertem:

.AVI\$.MPG\$.WAV\$.MP3\$

En el arxiu "/etc/squid3/dstdomain" insertem:

www.miguel.com

Teoría

Un ACL es una definición de control de acceso, que en Squid se especifica mediante el parámetro acl según la siguiente sintaxis:

acl nombre_acl tipo_acl descripción ...

acl nombre_acl tipo_acl "fichero_de_descripciones" ...

Cuando usamos un "fichero_de_descripciones", cada descripción se corresponde con una línea del fichero.

Tipos de ACL

src

Especifica una dirección origen de una conexión en formato IP/máscara.

Por ejemplo, utilizaremos una acl de tipo src para especificar la red local:

acl red_local src 192.168.1.0/24

También podemos especificar rangos de direcciones mediante una acl de tipo src:

acl jefes src 192.168.1.10-192.168.1.25/32

dst

Especifica una dirección destino de una conexión en formato IP/máscara.

acl google_es dst 216.239.0.0/24

También podemos especificar hosts concretos mediante una acl de tipo dst:

acl google_es2 dst 216.239.59.104/32 216.239.39.104/32 216.239.57.104/32

Las definiciones son idénticas a las acl de tipo src salvo que se aplican al destino de las conexiones, no al origen.

srcdomain y dstdomain

Estos tipos de acl especifican un nombre de dominio.

En el caso de srcdomain es el dominio origen y se determina por resolución DNS inversa de la IP de la máquina, es decir, tendremos que tener bien configurado el DNS de la red local.

En el caso de dstdomain el nombre del dominio se comprueba con el dominio que se haya especificado en la petición de página web.

Por ejemplo:

acl google_com dstdomain google.com

srcdom_regex y dstdom_regex

Especifican una expresión regular que verifican los dominio origen o destino. La expresión regular hace distinción entre mayúsculas y minúsculas salvo que incluyamos la opción "-i" que evita dicha distinción.

Por ejemplo

acl google_todos dstdom_regex -i google\.*

Observamos como al incluir "-i" estamos indicando que no haga distinción entre mayúsculas y minúsculas.

time

Este tipo de acl permite especificar una franja horaria concreta dentro de una semana. La sintaxis es la siguientes

acl nombre_acl_horaria time [dias-abrev] [h1:m1-h2:m2]

Donde la abreviatura del día es:

S - Sunday (domingo)

M - Monday (lunes)

T - Tuesday (martes)

W - Wednesday (miércoles)

H - Thursday (jueves)

F - Friday (viernes)

A - Saturday (sábado)

además la primera hora especificada debe ser menor que la segunda, es decir h1:m1 tiene que ser menor que h2:m2

Por ejemplo

acl horario_laboral time M T W H F 8:00-15:00

Estaríamos especificando un horario de 8 a 15 y de lunes a viernes.

url_regex

Permite especificar expresiones regulares para comprobar una url completa, desde el http:// inicial.

Por ejemplo, vamos a establecer una acl que se verifique con todos los servidores cuyo nombre sea adserver:

url_regex serv_publicidad ^http://adserver.*

En otro ejemplo podemos ver una acl que verifique las peticiones de ficheros mp3:

url_regex ficheros_mp3 -i mp3\$

Nota: ver expresiones regulares

referer_regex

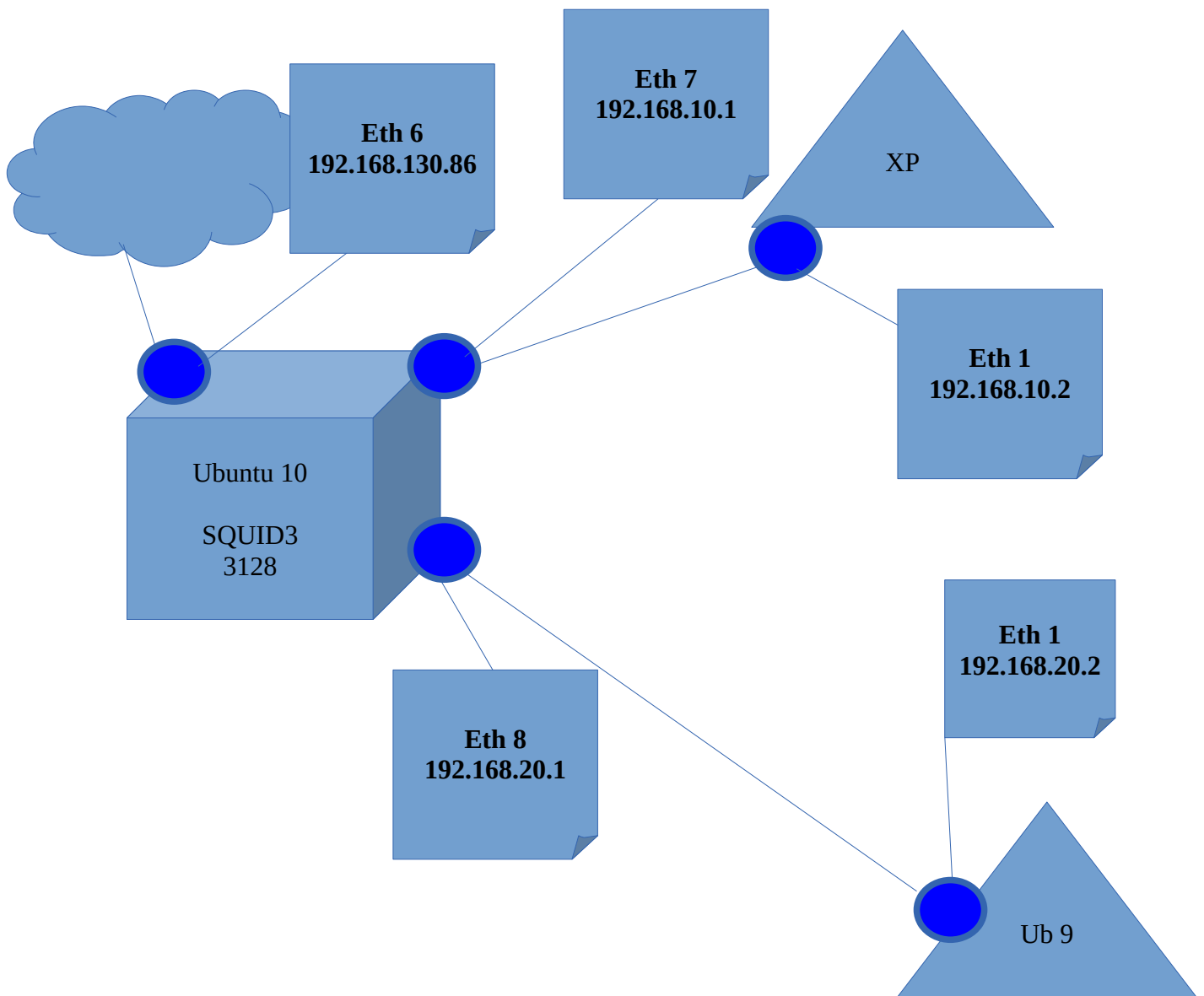
Define una acl que se comprueba con el enlace que se ha pulsado para acceder a una determinada página. Cada petición de una página web incluye la dirección donde se ha pulsado para acceder. Si escribimos la dirección en el navegador entonces estaremos haciendo una petición directa.

Por ejemplo vamos a establecer una acl para todas las páginas a las que hayamos accedido pulsando en una ventana de búsqueda de google:

acl pincha_google referer_regex http://www.google.*

Squid Proxy Transparente

http_port 3128 transparent [Línea 889]



#!/bin/bash

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

sudo iptables -t nat -A POSTROUTING -s 192.168.10.0/24 -o eth3 -j SNAT --to 192.168.19.200

sudo iptables -t nat -A PREROUTING -i eth5 -p tcp --dport 80 -j DNAT --to 192.168.19.200:3128

sudo iptables -t nat -A PREROUTING -i eth5 -p tcp --dport 80 -j REDIRECT --to-port 3128



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

```
sudo iptables -t nat -A POSTROUTING -s 192.168.10.0/24 -o eth7 -j SNAT --to 192.168.1.203
```

```
sudo iptables -t nat -A PREROUTING -i eth3 -p tcp --dport 80 -j DNAT --to 192.168.1.203:3128
```

```
sudo iptables -t nat -A PREROUTING -i eth3 -p tcp --dport 80 -j REDIRECT --to-port 3128
```

```
aaron@ChaseKID03:~$ ifconfig
eth3      Link encap:Ethernet  direcciónHW 08:00:27:46:f9:dc
          Direc. inet:192.168.10.1  Difus.:192.168.10.255  Másc:255.255.
          Dirección inet6: fe80::a00:27ff:fe46:f9dc/64 Alcance:Enlace
          ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST MTU:1500 Métrica:1
          Paquetes RX:314 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:120 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colatX:1000
          Bytes RX:34050 (34.0 KB)  TX bytes:32757 (32.7 KB)

eth7      Link encap:Ethernet  direcciónHW 08:00:27:f3:c3:ef
          Direc. inet:192.168.1.203  Difus.:192.168.1.255  Másc:255.255.
          Dirección inet6: fe80::a00:27ff:fef3:c3ef/64 Alcance:Enlace
          ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST MTU:1500 Métrica:1
          Paquetes RX:228 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:307 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colatX:1000
          Bytes RX:75948 (75.9 KB)  TX bytes:32757 (32.7 KB)
```

```
ubuntu@ubuntu:~$ nslookup google.es
Server:      192.168.10.1
Address:     192.168.10.1#53
```

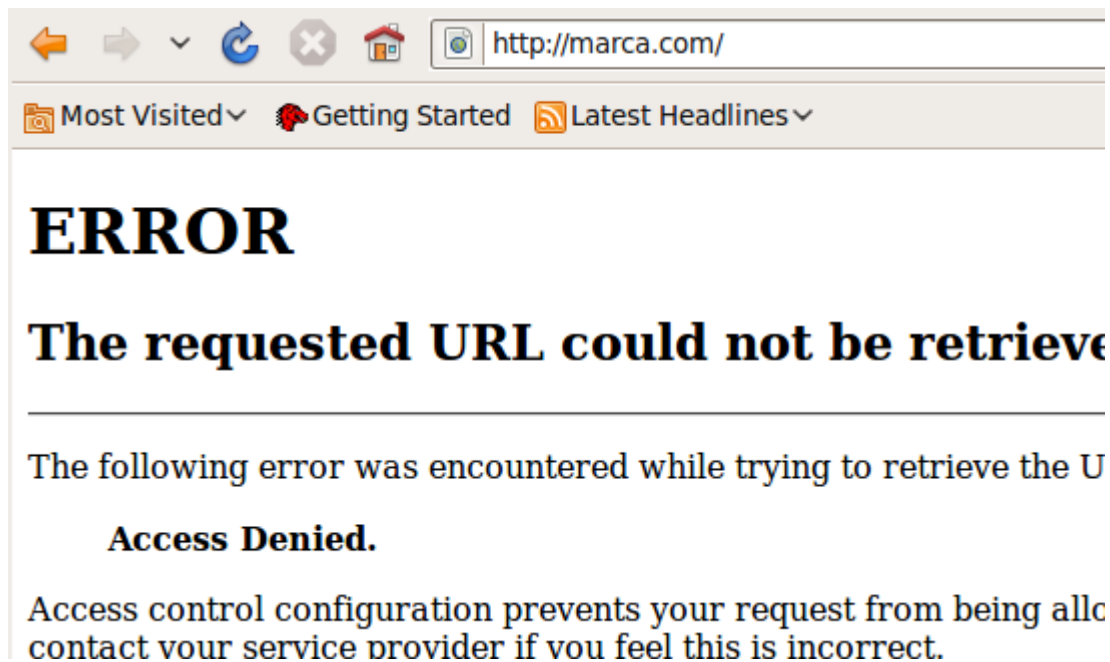
Non-authoritative answer:

```
Name:   google.es
Address: 173.194.41.31
Name:   google.es
Address: 173.194.41.23
Name:   google.es
Address: 173.194.41.24
```

```
ubuntu@ubuntu:~$ sudo service networking restart
* Reconfiguring network interfaces...
ubuntu@ubuntu:~$ ping www.google.es
PING www.google.es (173.194.41.23) 56(84) bytes of data.
64 bytes from mad01s14-in-f23.1e100.net (173.194.41.23): icmp_
35.3 ms
64 bytes from mad01s14-in-f23.1e100.net (173.194.41.23): icmp
```

```
# -----
acl localhost src 192.168.1.203
acl marca dst www.marca.com
acl inet1 src 192.168.10.0/24
#acl inet2 src 192.168.20.0/24

http_access deny marca
http_access allow inet1 !marca
#http_access
```



proxy_auth

<http://wiki.squid-cache.org/Features/Authentication>

<https://workaround.org/squid-acls>

Proxy Transparente X Autenticación = Incompatibles

Lista ACL

Autenticación =

<http://www.cyberciti.biz/tips/linux-unix-squid-proxy-server-authentication.html>

1. `cd /etc/squid3`
2. `htpasswd -c /etc/squid3/claves aaron`
3. `chmod 600 claves`
4. `gedit /etc/squid3/squid.conf`

1. Deshabilitar el PROXY TRANSPARENTE (Ya que no funciona)

```
acl localhost src 192.168.19.0/24
acl cliente1 src 192.168.10.0/24
acl cliente2 src 192.168.20.0/24
acl ncsa_users proxy_auth REQUIRED
acl ncsa_users1 proxy_auth aaron

http_access allow ncsa_users
http_access allow ncsa_users1
http_access allow localhost
http_access allow cliente1
http_access allow cliente2
```

2. Añadir esas ACL.

3. Descomentar estas líneas

`auth_param basic program /usr/lib/squid/ncsa_auth /etc/squid3/claves`

`auth_param basic children 5`

`auth_param basic realm Squid proxy-caching web server`

`auth_param basic credentialsttl 2 hours`

`auth_param basic casesensitive off`

4. Reiniciar

Exercici 3 ACL

Una empresa que té en total 64 ip assignades, sempre s'assignen les més baixes, i vol que els seus treballadors no puguin connectar-se a les pàgines amb contingut pornogràfics, d'esports, de descàrregues i de jocs.

També vol que es bloquegen els arxius .exe .mp3 .mpg .wav .iso .zip .rar.

La navegació només es podrà fer de de 8 a 12 am y de 1 a 4:30 pm. els treballadors

Hem de tindre en compte que existeix un usuari X.X.X.248 que no té cap restricció (el gerent de l'empresa).

A més a més, ens diuen que ls treballadors podran accedir a les pàgines de correu electrònic gratuït només de 12,00 a 13,00h.

Per últim ens han comentat que el proxy dels treballadors funcionarà com proxy-transparent.

Heu de fer una configuració per a que es complisquen aquestes restriccions.

Acl all src all

acl red-empresa src 192.168.10.2-192.168.10.64

acl jefe src 192.168.10.248

acl pags url_regex "/etc/squid3/archivo"

#Pongo "juegos" "gratis".

acl arxius urlpath_regex "/etc/squid3/arxius"

#En el archivo arxius poner \.jpg\$ \.mp3\$ \.exe\$ \.wav\$ \.iso\$ \.zip\$ \.rar\$

acl horari1 time MTWHF 08:00-12:00

acl horari2 time MTWHF 13:00-16:30

acl horari3 time MTWHF 12:00-13:00

acl correu port 25 465 443 [PuertoCorreo]

acl correu dstdomain "/etc/squid3/pagcorreu"

#En el archivo correu poner www.gmail.com www.hotmail.com www.yahoo.com

http_access allow red-empresa horari1 horari2 !pags !arxius

http_access allow jefe

http_access allow red-empresa horari3

http_access deny all

SQUIDGUARD

SquidGuard. Sistema de filtrado combinado de redireccionamiento web, y el plugin del controlador de acceso para Squid. Utiliza una lista negra "Blacklists" como base de datos para denegar o permitir sitios web al usuario. Su mayor utilidad es la prevención de dominios o URLs que contengan informaciones no deseadas o nada productivas en horario laboral.

Lista negra

Una lista negra "blacklists" en la computación, es una lista de dominios, URLs o direcciones de IP que deben ser restringidas por contener informaciones no adecuadas, en muchos casos por proveer Spam, Spyware, Hacking, Porn, etc.

squidGuard

Agafem una maquina nova i instal·lem el squid i el squidGuard

apt-get install squid3

apt-get install squidguard

Canviem el propietari de la carpeta db (és on tindrem els llocs prohibits)

chown -R proxy:proxy /var/lib/squidguard/db

Hem d'editar l'arxiu de configuració del squidGuard.

gedit /etc/squid/squidGuard.conf

Esborrem el contingut i posem:

dbhome /var/lib/squidguard/db

logdir /var/log/squid

dest adv {

domainlist adv/domains

urllist adv/urls

}

dest porn {

domainlist porn/domains

urllist porn/urls

}

dest warez {

domainlist warez/domains

urllist warez/urls

}

acl {

default {

pass !adv !porn !warez all

redirect http://X.X.X.X/blocked.html

}

}

Hem d'instal·lar l'Apache

Dins de **/var/www/**

hem de crear un arxiu anomenat blocked.html amb el text que volem que
isca.

Dins de **/etc/squid3/squid.conf**

Hem de posar:

url_rewrite_program /usr/bin/squidGuard -c /etc/squid/squidGuard.conf

Fem

squid3 -k reconfigure

Fem

wget http://www.shallalist.de/Downloads/shalla_update.sh

Editem el script i substituïm

squidGuardpath="/usr/bin/squidGuard"

squidpath="/usr/sbin/squid3"

httpget="/usr/bin/wget"

tarpath="/bin/tar"

chownpath="/bin/chown"

dbhome="/var/lib/squidguard/db"

squidGuardowner="proxy:proxy"

ejecutamos script

sh shalla_update.sh

ahora compilamos:

squidGuard -u -C all -d

reiniciamos squid3

/etc/init.d/squid3 restart

Creamos un nuevo elemento blacklist llamado "futbol" donde prohibiremos las páginas relacionadas con el Real Madrid.

Mkdir /var/lib/squidGuard/db/futbol

cd /var/lib/squidGuard/db/futbol

touch domains urls

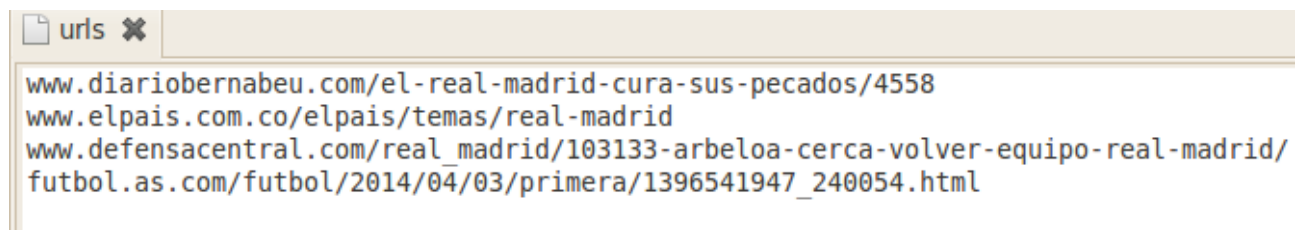
gedit domains



domains ✕

marca.com
as.com
diariobernabeu.com
defensacentral.com
diario-digital-madridista.blogspot.com.es
elpais.com.co
diariobernabeu.com

gedit urls



urls ✕

www.diariobernabeu.com/el-real-madrid-cura-sus-pecados/4558
www.elpais.com.co/elpais/temas/real-madrid
www.defensacentral.com/real_madrid/103133-arbeloa-cerca-volver-equipo-real-madrid/
futbol.as.com/futbol/2014/04/03/primera/1396541947_240054.html

En /etc/squid/squidGuard.conf añadimos

```

dest futbol {

    domainlist futbol/domains

    urllist futbol/urls

}

acl {

    default {

        pass !adv !porn !warez !futbol !drugs all

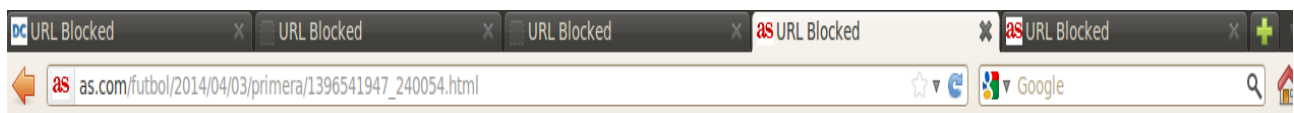
        redirect http://192.168.19.203/blocked.html

    }

}

```

reiniciamos SQUID3.



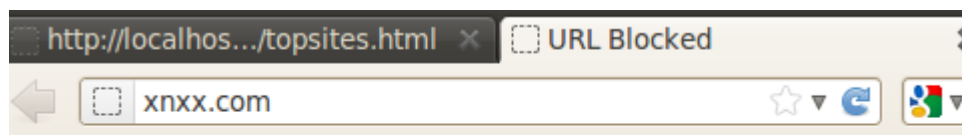
Access to this site / url has been blocked.

If you think this is an error, please contact the help-desk:

Call us - 123-456-789 (ext. 333)

Email us - proxymaster@server1.cyberciti.biz

Vemos que la página de AS.com la bloquea.



Access to this site / url has been blocked.

If you think this is an error, please contact the help-desk:

Call us - 123-456-789 (ext. 333)

Email us - proxymaster@server1.cyberciti.biz

También alguna porno

SARG

apt-get install sarg

language Spanish

access_log /var/log/squid3/access.log

output_dir /var/www/html/squid-reports

title "Reportes de Acceso Web por Aaron Andal"

show_sarg_info yes

show_sarg_log yes

service squid3 restart

sarg



Squid Aaron Reports


Periodo: 2014Apr03-2014Apr03

Clasificado por: BYTES, reverse

Topuser

Topsites

Sitios y Usuarios

NUM		USERID	CONEXION	BYTES	%BYTES	ENTRADA-CACHE-SALIDA	TIEMPO UTILIZADO	MILISEC	%HORA
1		192.168.19.203	258	7.63M	100.00%	0.27% 99.73%	00:00:19	19,787	100.00%
TOTAL			258	7.63M		0.27% 99.73%	00:00:19	19,787	
PROMEDIO			258	7.63M			00:00:19	19,787	

Generado por sarg-2.2.6 Dec-01-2009 el Apr/03/2014 20:32

SHALLA BLACKLIST SQUIDGUARD

adv	Bloquea todo tipo de páginas relacionadas con “publicidad”
Aggresive	Bloquea todo tipo de páginas relacionadas con “agresividad”
Alcohol	Bloquea todo tipo de páginas relacionadas con “Alcohol”
Anonvpn	Bloquea todo tipo de páginas relacionadas con “VPN”
Automobile/planes	Bloquea todo tipo de páginas relacionadas con “Aviones”
Automobile/cars	Bloquea todo tipo de páginas relacionadas con “Coches”
Chat	Bloquea todo tipo de páginas relacionadas con “Chat”
Dating	Bloquea todo tipo de páginas relacionadas con “Citas”
Downloads	Bloquea todo tipo de páginas relacionadas con “Descargas”
drugs	Bloquea todo tipo de páginas relacionadas con “Drogas”
Dynamic	Bloquea todo tipo de páginas relacionadas con “Dinamicas”
Education/school	Bloquea todo tipo de páginas relacionadas con “Educacion”
Finance/banking	Bloquea todo tipo de páginas relacionadas con “Colegio”
Finance/insurance	Bloquea todo tipo de páginas relacionadas con “Seguro”
Finance/moneylending	Bloquea todo tipo de páginas relacionadas con “Dinero”
Forum	Bloquea todo tipo de páginas relacionadas con “Forum”
Gamble	Bloquea todo tipo de páginas relacionadas con “”
Government	Bloquea todo tipo de páginas relacionadas con “Gov”
Hobby	Bloquea todo tipo de páginas relacionadas con “Hobbies”
Homestyle	Bloquea todo tipo de páginas relacionadas con “Estilo de vida”
Hospitals	Bloquea todo tipo de páginas relacionadas con “Hospital”
Imagehosting	Bloquea todo tipo de páginas relacionadas con “Hosting”
ISP	Bloquea todo tipo de páginas relacionadas con “ISP”
Jobsearch	Bloquea todo tipo de páginas relacionadas con “Trabajo”
Library	Bloquea todo tipo de páginas relacionadas con “Libro”
Military	Bloquea todo tipo de páginas relacionadas con “Militar”
Models	Bloquea todo tipo de páginas relacionadas con “Modelo”
Movies	Bloquea todo tipo de páginas relacionadas con “Pelis”
Music	Bloquea todo tipo de páginas relacionadas con “Musica”
Porn	Bloquea todo tipo de páginas relacionadas con “Porno”
Radiotv	Bloquea todo tipo de páginas relacionadas con “Radiotv”
Recreation	Bloquea todo tipo de páginas relacionadas con “Recreacion”
Warez	Bloquea todo tipo de páginas relacionadas con “Warez”
Webmain	Bloquea todo tipo de páginas relacionadas con “Webmail”
weapons	Bloquea todo tipo de páginas relacionadas con “Armas”

<http://www.shallalist.de/categories.html>

```

adv      education  imagehosting  radiotv      tracker
aggressive  finance      isp           recreation   updatesites
alcohol   fortunetelling  jobsearch    redirector   urlshortener
anonvpn   forum         library      religion     violence
automobile  futbol      military     remotecontrol  warez
chat      gamble       models       ringtones   weapons
COPYRIGHT global_usage  movies       science     webmail
costtraps government    music        searchengines  webphone
dating    hacking      news         sex          webradio
downloads hobby        podcasts     shopping     webtv
drugs     homestyle    politics     socialnet
dynamic   hospitals    porn         spyware
root@ChaseKiD03:~#

```



Squid Analysis Report Generator

Squid Aaron Reports

Periodo: 2014Apr03-2014Apr03

Top 100 sitios

NUM	SITIO ACCEDIDO	CONEXION	BYTES	HORA
1	www.realmadrid.com	142	2.32M	7.30K
2	safebrowsing-cache.google.com	58	5.05M	5.23K
3	start.ubuntu.com	13	35.66K	2.26K
4	www.google.es	5	4.55K	645
5	www.elpais.com.co	4	2.71K	2
6	www.diariobernabeu.com	4	2.71K	2
7	safebrowsing.clients.google.com	3	12.06K	396
8	proxy.example.com	3	7.60K	55
9	as.com	3	1.63K	26
10	www.google-analytics.com	2	14.42K	108
11	futbol.as.com	2	1.35K	11
12	www.defensacentral.com	2	1.35K	1
13	diario-digital-madridista.blogspot.com.es	2	1.35K	0
14	udc.msn.com	2	511	511
15	widget-staging.cloud.opta.net	1	77.55K	715
16	widget.cloud.opta.net	1	29.38K	646
17	themes.googleusercontent.com	1	22.07K	142
18	maps.gstatic.com	1	17.79K	187
19	www.googletagmanager.com	1	17.32K	135
20	gtglobal-ocsp.geotrust.com	1	1.91K	238
21	maps.google.es	1	1.46K	146
22	clients1.google.com	1	918	127
23	www.google.com	1	818	93
24	diario-digital-madridista.blogspot.com	1	763	559
25	fonts.googleapis.com	1	731	130
26	stats.g.doubleclick.net	1	679	0
27	rmapi.pirendo.com	1	0	110

Generado por sarg-2.2.6 Dec-01-2009 el Apr/03/2014 20:32

ACL SQUID3 PROXY Pract Avaluable

EJERCICIO NOVAL 19/03/2014

ACL ejercicio1

```
acl localhost src 192.168.19.93
acl cliente1 src 172.19.25.0/24
acl pagines dstdomain "/etc/squid3/pagines1"
acl horari time MTWHF 8:00-20:00
```

```
http_access allow cliente1 horari pagines
http_access deny cliente1
http_access allow localhost
```

Ejercicio 2

ACLs

```
acl localhost src 192.168.19.193
acl client1 src 172.19.25.0/24
acl coches dstdomain "/etc/squid3/coches"
```

```
http_access allow client1 !coches
http_access deny localhost
http_access deny all
```

Ejercicio 3

ACLs

```
acl aaron proxy_auth REQUIRED
acl aaron1 proxy_auth "/etc/squid3/andal"
```

```
http_access allow aaron1 aaron
http_access allow localhost
```

Ejercicio 4

ACLs

```
#acl usuarios proxy_auth REQUIRED
#acl grup1 proxy_auth "/etc/squid3/grup1"
#acl grup2 proxy_auth "/etc/squid3/grup2"
#acl gmail dstdomain www.gmail.com
#acl google.es dstdomain www.google.es
#acl depo url_regex "/etc/squid3/deportes"
#acl horarig2 time W 19:00-22:00
```

```
#http_access allow grup1 !gmail !depo
#http_access allow grup2 horarig2 google.es
#http_access deny all
```

#IDENTIFICACION

```
auth_param basic program /usr/lib/squid/ncsa_auth /etc/squid3/andal
```

```
auth_param basic children 5
```

```
auth_param basic realm Squid proxy-caching web server
```

```
auth_param basic credentialsttl 2 hours
```

```
auth_param basic casesensitive off
```

```
# Squid normally listens to port 3128
```

```
http_port 3128 transparent|
```

```
# Autenticacion No compatible con transparente
```