# Squid amb SquidGuard en Ubuntu Server 12.04

| | |
|---|---|
| Lloc web: | http://www.squid-cache.org/ |
| Documentació: | http://www.squid-cache.org/Doc/config/ |
| Documentació en espanyol: | http://tuxjm.net/docs/Manual_de_Instalacion_de_Servidor_Proxy_Web_con_Ubuntu_Server_y_Squid/html-multiples/ |

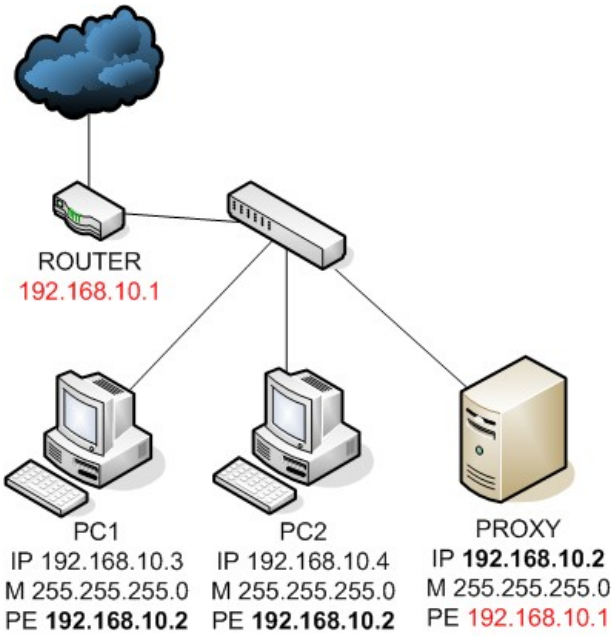
Squid és un proxy cau per al suport web HTTP, HTTPS, FTP i molt més. Redueix l'ample de banda i millora els temps de resposta en memòria cau i reutilitza les pàgines web sol·licitades sovint. Squid té amplis controls d'accés i fa una gran acceleració de servidor. S'executa en els sistemes operatius més disponibles, incloent Windows i està disponible sota la GNU GPL.

Squid és el servidor de proxy i cau per excel·lència. Quan naveguem a través d'un proxy, cada petició que fa el nostre navegador es delega al servidor proxy i és aquest el que es descarrega la pàgina o l'element web que s'ha sol·licitat i l'hi passa al nostre navegador. Per tant és un intermediari entre els usuaris i la web. Com que enmig d'aquest trànsit pot realitzar dues funcions molt importants: controlar els accessos (permetre o denegar segons es disposi en les seves normes), i a més fer de cau d'elements (pàgines web, imatges, icones que un cop es demanen es guarden en la memòria del proxy), de manera que si es demana un element que ja s'ha demanat en lloc de tornar a baixar-se'l d'internet, el serveix el propi proxy. Amb aquesta tècnica de cau ens podem estalviar des d'un 20 a un 40% de trànsit d'Internet.

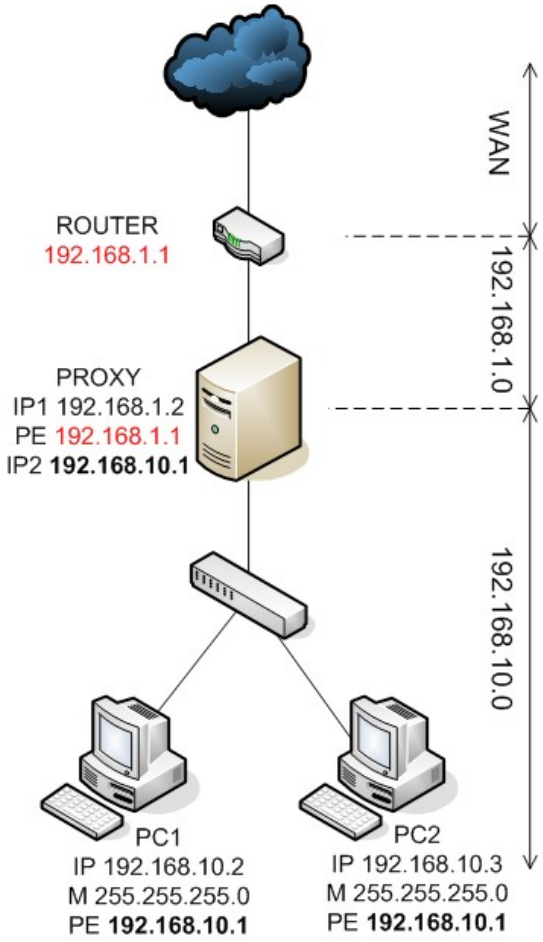
SquidGuard és un plugin per a filtrar webs per a Squid que s'utilitza per restringir l'accés a dominis/URLs basats en llistes de control d'accés. Quan SquidGuard rep una sol·licitud és examinada i, o bé permetrà que la pàgina es carregui o bé es redirigirà a una pàgina de "bloqueig" predeterminada. SquidGuard pren les seves decisions basant-se en l'ús de llistes de control d'accés i bases de dades de dominis, adreces URL i expressions.

# Configuració de la xarxa

## Opció A:




## Opció B:



## Instal·lació i configuració

1. apt-get install squid
2. nano /etc/rc.local

   Abans de la línia: `exit 0`
   Afegeix:

```
echo "1" > /proc/sys/net/ipv4/ip_forward
# proxy transparent
iptables -t nat -A PREROUTING -i eth0 -s 192.168.10.0/24 ! -d
192.168.10.0/24 -p tcp --dport 80 -j REDIRECT --to-port 3128
```

3. nano /etc/squid3/denegats

```
# llistat de pàgines web que no es podran visitar
http://www.youtube.com
elpais.com
rastreator
```

4. chmod 644 /etc/squid3/denegats
5. wget http://www.proferamon.com/documents/proxy/squid3.conf
6. mv ./squid3.conf /etc/squid3/squid.conf
7. apt-get install squidguard
8. wget http://squidguard.mesd.k12.or.us/blacklists.tgz
9. mv ./blacklists.tgz /var/lib/squidguard/db/
10. cd /var/lib/squidguard/db/
11. tar zxvf blacklists.tgz
12. rm blacklists.tgz
13. wget http://www.proferamon.com/documents/proxy/squidGuard.conf
14. nano ./squidGuard.conf

    Cerca `192.168.1.XXX` i substitueix per la IP del teu servidor

15. mv ./squidGuard.conf /etc/squid/
16. chown proxy:proxy -R /var/lib/squidguard/db/*
17. find /var/lib/squidguard/db -type f | xargs chmod 644
18. find /var/lib/squidguard/db -type d | xargs chmod 755
19. apt-get install apache2
20. nano /etc/apache2/httpd.conf

    Afegeix la línia: `ServerName 192.168.1.`**`XXX`**

21. sudo -u proxy squidGuard -C all
22. nano /etc/squid3/squid.conf

    Sota la línia: `http_port 3128 transparent`
    Afegeix la línia: **`redirect_program /usr/bin/squidGuard`**

23. wget http://www.proferamon.com/documents/proxy/block.html
24. mv ./block.html /var/www/
25. squid3 -k reconfigure
26. shutdown -r now

**Per comprovar que funciona squidGuard:**

27. echo "http://www.rotten.com / - - GET" | squidGuard -d

**Per actualitzar la llista negra:**

Executa l'script squid_blacklists_updates.sh o bé pots programar les actualitzacions amb el cron fent:

```
# sudo crontab -e
```

```
00 5 * * * sh /root/squid_blacklist_update.sh
```

**Després d'haver actualitzat la llista negra:**

```
# sudo -u proxy squidGuard -C all
# squid3 -k reconfigure
```

# Annexos

## Annex 1 - /etc/rc.local

```
#!/bin/sh -e
#
# rc.local
#
# This script is executed at the end of each multiuser runlevel.
# Make sure that the script will "exit 0" on success or any other
# value on error.
#
# In order to enable or disable this script just change the
execution
# bits.
#
# By default this script does nothing.

echo "1" > /proc/sys/net/ipv4/ip_forward
# proxy transparent
iptables -t nat -A PREROUTING -i eth0 -s 192.168.10.0/24 ! -d
192.168.10.0/24 -p tcp --dport 80 -j REDIRECT --to-port 3128

exit 0
```

## Annex 2 - /etc/squid/denegats

```
http://www.youtube.com
elpais.com
rastreator
```

## Annex 3 - /etc/squid3/squid.conf

```
acl manager proto cache_object
acl localhost src 127.0.0.1/32 ::1
acl xarxa_local src 192.168.10.0/24
acl to_localhost dst 127.0.0.0/8 0.0.0.0/32 ::1
acl SSL_ports port 443
acl Safe_ports port 80 # http
acl Safe_ports port 21 # ftp
acl Safe_ports port 443 # https
acl Safe_ports port 70 # gopher
acl Safe_ports port 210 # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280 # http-mgmt
acl Safe_ports port 488 # gss-http
acl Safe_ports port 591 # filemaker
```

```
acl Safe_ports port 777 # multiling http
acl CONNECT method CONNECT
acl denegats url_regex "/etc/squid3/denegats"
http_access allow manager localhost
http_access deny manager
http_access deny !Safe_ports
http_access deny denegats
http_access allow localhost
http_access allow xarxa_local
http_access deny all
http_port 3128 transparent
redirect_program /usr/bin/squidGuard
cache_dir ufs /var/spool/squid3 512 16 256
coredump_dir /var/spool/squid3
refresh_pattern ^ftp:         1440  20%   10080
refresh_pattern ^gopher:      1440  0%    1440
refresh_pattern -i (/cgi-bin/|\?) 0 0%    0
refresh_pattern (Release|Packages(.gz)*)$      0       20%     2880
refresh_pattern .       0     20%   4320
error_directory   /usr/share/squid3/errors/Catalan
```

## Annex 4 - /etc/squid/squidGuard.conf

```
#
# CONFIG FILE FOR SQUIDGUARD
#

dbhome /var/lib/squidguard/db/blacklists
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
#}

#
# SOURCE ADDRESSES:
#

#src admin {
#       ip              1.2.3.4 1.2.3.5
#       user            root foo bar
#       within          workhours
#}
```

```
#src foo-clients {
#       ip              172.16.2.32-172.16.2.100 172.16.2.100
172.16.2.200
#}

#src bar-clients {
#       ip              172.16.4.0/26
#}

#
# DESTINATION CLASSES:
#

dest good {
}

dest local {
}

dest ads {
        domainlist      ads/domains
        urllist         ads/urls
}

dest aggressive {
        domainlist      aggressive/domains
        urllist         aggressive/urls
}

dest audio-video {
        domainlist      audio-video/domains
        urllist         audio-video/urls
}
dest drugs {
        domainlist      drugs/domains
        urllist         drugs/urls
}

dest gambling {
        domainlist      gambling/domains
        urllist         gambling/urls
}


dest hacking {
        domainlist      hacking/domains
        urllist         hacking/urls
}

dest mail {
        domainlist      mail/domains
}

dest porn {
        domainlist      porn/domains
        urllist         porn/urls
}

dest proxy {
```

```
        domainlist      proxy/domains
        urllist         proxy/urls
}

dest redirector {
        domainlist      redirector/domains
        urllist         redirector/urls
}

dest spyware {
        domainlist      spyware/domains
        urllist         spyware/urls
}

dest suspect {
        domainlist      suspect/domains
        urllist         suspect/urls
}


dest violence {
        domainlist      violence/domains
        urllist         violence/urls
}

dest warez{
        domainlist      warez/domains
        urllist         warez/urls
}


acl {
#       admin {
#               pass     any
#       }

#       foo-clients within workhours {
#               pass     good !in-addr !adult any
#       } else {
#               pass any
#       }

#       bar-clients {
#               pass    local none
#       }

        default {
                pass !ads !aggressive !audio-video !drugs !gambling
!hacking !mail !porn !proxy !redirector !spyware !suspect !violence
!warez all
#               rewrite  dmz
                redirect        http://192.168.1.XXX/block.html

        }
}
```

## Annex 5 - /var/www/block.html

```
<html>

<head>
<meta http-equiv="Expires" content="0"><meta http-equiv="Content-
Type" content="text/html; charset=iso-8859-1">
<title>Web tancada</title>
</head>

<body bgcolor=#000000 text=#FFFFFF>

<p><br><br><br></p>

<table border=0 width=100% bgcolor=#FF0000 height=1>
<tr><td> </td></tr>
</table>

<p><br></p>

<p align=center>
<font size=5>Web tancada pel filtre SquidGuard</font>
</p>

<p><br></p>

<table border=0 width=100% bgcolor=#FF0000 height=1>
<tr><td> </td></tr>
</table>

<p align=right><a href=http://www.proferamon.com style="text-
decoration:none; font-stretch:wider">
<font style="font-weight:900; font-size:125%" face="Arial,
Helvetica, Geneva, Swiss, SunSans-Regular, sans-serif"
color=#FFFFFF size="4">proferamon.com</a>
</p>

</body>

</html>
```

## Annex 6 - /root/squid_blacklist_update.sh

```
TARGET=/var/lib/squidguard/db/blacklists

cd $TARGET || exit

# only run if squidGuard is active!
[ "`ps auxw | grep squid[G]uard`" ] || exit

rsync -az squidguard.mesd.k12.or.us::filtering $TARGET

for DIR in `ls $TARGET`
do
        if [ -f $DIR/domains.include ]
        then
                TMP=$RANDOM
                cat $DIR/domains $DIR/domains.include | sort | uniq
> $DIR/domains.$TMP
                mv -f $DIR/domains.$TMP $DIR/domains
```

```
        fi
        if [ -f $DIR/urls.include ]
        then
                TMP=$RANDOM
                cat $DIR/urls $DIR/urls.include | sort | uniq >
$DIR/urls.$TMP
                mv -f $DIR/urls.$TMP $DIR/urls
        fi
done

/usr/bin/squidGuard -c /etc/squid/squidGuard.conf  -C all

chown -R proxy:proxy $TARGET
chown -R proxy:proxy /var/log/squid/squidGuard.log

sleep 5s

/usr/bin/killall -HUP squid3
```