Configuració d'un servidor proxy transparent amb SquidGuard

1. apt-get install squid
2. nano /etc/rc2.d/S30firewall

   ```
   echo "1" > /proc/sys/net/ipv4/ip_forward
   # proxy transparent
   iptables -t nat -A PREROUTING -i eth0 -s 192.168.1.0/24 -d
   ! 192.168.1.0/24 -p tcp --dport 80 -j REDIRECT --to-port
   3128
   ```

3. chmod 755 /etc/rc2.d/S30firewall
4. nano /etc/squid/denegats

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

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

    Cerca `192.168.1.2XX` i substitueix per la IP del teu servidor

16. cp ./squidGuard.conf /etc/squid/
17. chown proxy:proxy -R /var/lib/squidguard/db/*
18. find /var/lib/squidguard/db -type f | xargs chmod 644
19. find /var/lib/squidguard/db -type d | xargs chmod 755
20. apt-get install sudo
21. sudo -u proxy squidGuard -C all
22. nano /etc/squid/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. cp ./block.html /var/www/
25. squid -k reconfigure
26. echo "http://www.rotten.com / - - GET" | squidGuard -d
27. reboot

Per actualitzar la llista negra:

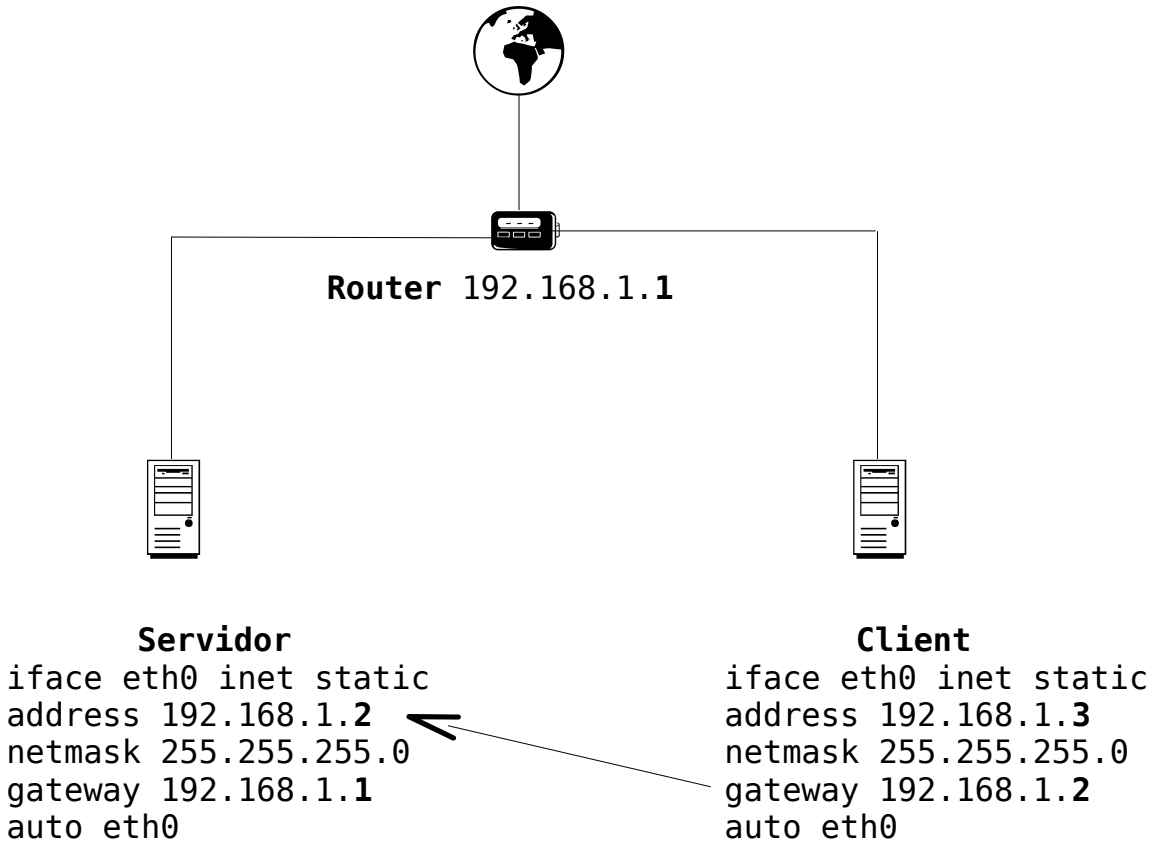
Executa l'script squid_blacklists_updates.sh o bé pots programar les actualitzacions amb el cron fent:

```
# sudo crontab -e
00 5 * * * sh /root/bin/squid_blacklist_update.sh
```

Després d'haver actualitzat la llista negra:

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

Configuració de la xarxa en el servidor i els clients:



Annexos

Annex 1 - /etc/rc2.d/S30firewall

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

iptables -t nat -A PREROUTING -i eth0 -s 192.168.1.0/24 -d !
192.168.1.0/24 -p tcp --dport 80 -j REDIRECT --to-port 3128
```

Annex 2 - /etc/squid/denegats

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

Annex 3 - /etc/squid/squid.conf

```
acl all src all
acl manager proto cache_object
acl localhost src 127.0.0.1/32
acl to_localhost dst 127.0.0.0/8
acl localnet src 10.0.0.0/8 # RFC1918 possible internal network
acl localnet src 172.16.0.0/12 # RFC1918 possible internal network
acl localnet src 192.168.0.0/16 # RFC1918 possible internal network

acl SSL_ports port 443 # https
acl SSL_ports port 563 # snews
acl SSL_ports port 873 # rsync
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 Safe_ports port 631 # cups
acl Safe_ports port 873 # rsync
acl Safe_ports port 901 # SWAT
acl purge method PURGE
acl CONNECT method CONNECT

icp_access allow localnet
icp_access deny all

http_port 3128 transparent
redirect_program /usr/bin/squidGuard
hierarchy_stoplist cgi-bin ?
```

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

refresh_pattern ^ftp:         1440  20%   10080
refresh_pattern ^gopher:      1440  0%    1440
refresh_pattern -i (/cgi-bin/|\?) 0 0%    0
refresh_pattern (Release|Package(.gz)*)$ 0     20%   2880
refresh_pattern .       0     20%   4320

acl apache rep_header Server ^Apache
acl denegats url_regex "/etc/squid/denegats"
http_access deny denegats
http_access allow localnet
http_access allow manager localhost
http_access deny manager
http_access allow purge localhost
http_access deny purge
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost
http_access deny all
broken_vary_encoding allow apache

extension_methods REPORT MERGE MKACTIVITY CHECKOUT

hosts_file /etc/hosts
coredump_dir /var/spool/squid
```

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://192.168.1.2XX/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/bin/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
# /usr/sbin/squidGuard -c /etc/squid/squidGuard.conf  -u

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

sleep 5s

/usr/bin/killall -HUP squid
```