

Manual Instal·lació i Configuració SQUID - 2.6.STABLE16

Autor: Robin Pascual

Some rights reserved

Index de Continguts:

1- Instal·lació - Ubuntu 7.10 Gutsy.....	2
2- Configuració bàsica.....	3
3- Restriccions.....	4
3.1 Restricció per ip.....	5
3.2 Denegació de Paraules.....	5
3.3 Restricció de llocs web.....	6
3.4 Delimitació per Horaris.....	6
4- Configuració acl.....	7
5- Personalització d'errors.....	7

1- Instal·lació - Ubuntu 7.70 Gutsy

La instal·lació és ràpida i senzilla, com qualsevol altra aplicació a ubuntu. Executem les següents comandes.

-Mirem si al repositori tenim el paquet de l'squid.

```
$sudo apt-cache search squid | grep -i proxy
```

-Una vegada hem comprabat que tenim el paquet "squid" l'instalem

```
$sudo apt-get install squid
```

Només amb això ja tenim el servei a la nostra màquina preparat per a ser configurat.


A tenir en compte:

Com qualsevol altre servei que estigui corrent a la nostra màquina, Squid, pot ser encès/apagat/reiniciat, per a fer-ho farem servir la següent comanda, amb els paràmentres respectivament.

```
$sudo /etc/init.d/squid [start|stop|restart]
```

En principi, el servei esta llest per a poder-se inciar, això si, sense cap configuració especifica per a la nostra xarxa.

*Si en iniciar el servei, reps un missatge com aquest:

A terminal window with a dark background and light text. The prompt is 'robin@Robin-Garg:~\$'. The user enters 'sudo /etc/init.d/squid start'. The output shows: '* Starting Squid HTTP proxy squid', 'FATAL: Could not determine fully qualified hostname. Please set 'visible_hostname'', 'Squid Cache (Version 2.6.STABLE14): Terminated abnormally.', 'CPU Usage: 0.004 seconds = 0.000 user + 0.004 sys', 'Maximum Resident Size: 0 KB', 'Page faults with physical i/o: 0', and 'Aborted (core dumped)'. The prompt returns to 'robin@Robin-Garg:~\$'. A small red '[fail]' icon is visible in the bottom right corner of the terminal window.

```
robin@Robin-Garg:~$ sudo /etc/init.d/squid start
* Starting Squid HTTP proxy squid
FATAL: Could not determine fully qualified hostname. Please set 'visible_hostname'
Squid Cache (Version 2.6.STABLE14): Terminated abnormally.
CPU Usage: 0.004 seconds = 0.000 user + 0.004 sys
Maximum Resident Size: 0 KB
Page faults with physical i/o: 0
Aborted (core dumped)
robin@Robin-Garg:~$
```

Hauràs de escriure la linea següent en l'apartat visible_hostname:

```
visible_hostname [nom_de_la_maquina]
```

Passem tot seguit a especificar les definicions i restriccions que hem creat per a aquesta xarxa.

2- Configuració bàsica

La configuració bàsica, no és res més que definir els paràmetres per a que squid, pugui treballar correctament, això inclou, ports de comunicació, tamany de la cache, i volum de l'emmagatzematge.

*Nota: Algunes d'aquestes configuracions hauran de variar en funció del tipus de màquina que estem fent servir. Aquí es definirà una configuració molt accessible, però que pot ser ampliada si el recurs ho permet.

- **http_port:** És el port a través del que es comunicarà el servidor squid amb els clients que el tinguin assignat com a proxy de xarxa. El port per defecte de l'squid, és el 3128, però podem fer que escolti més d'un port a la vegada, ja que algunes aplicacions que fan servir internet viatjen per el port 8080. Si no especifiquèssim el segon port la comunicació que viatjes per allà, no seria vista per el proxy.

```
Per tant es recomana: http_port 3128
                      http_port 8080
```

- **cache_mem:** És la quantitat de memòria ram de la màquina servidor que es dedicarà a processar les peticions que rebi el proxy. Aquesta dependrà de les especificacions que posseeixi la nostra màquina. Per a una màquina amb 128 MB de ram, fòra òptim establir un valor de 16 MB. A partir d'aquí es pot escalar progressivament; per 256 MB de ram, 32 MB per al proxy, etc..

```
cache_mem 16 MB
```

- **cache_dir:** És el tamany en MB que volem dedicar a emmagatzemar objectes d'internet. S'ha d'anar amb compte amb la definició, ja que si en algun moment es sobrepassa el limit establert per a Squid, aquest es quedarà bloquejat.

```
cache_dir ufs /var/spool/squid *700 16 256
```

*El nombre marcat en negreta és el tamany especificat, en aquest cas 700 MB.

Amb aquest tres paràmetres, hem amoldat squid al nostre sistema físic, per així dir-ho. Tot seguit veurem com adaptar-lo al nostre esquema lògic, és a dir, a la nostra xarxa.

3- Restriccions

Squid com a servidor proxy, ens permet filtrar el contingut que prové d'internet. Per a fer-ho squid es val de unes llistes de control d'accés (acl), que són les que nosaltres definirem.

El primer que hem de fer, és entendre com treballa squid, aquest ens permet definir unes acl, que no són res més que un conjunt de informació que ell pot entendre, és a dir, ip, direccions web, paraules, etc...
Sobre aquestes llistes, podrem definir unes regles de control d'accés, que seran les que concediran o vetaran l'accés a segons quins recursos o informació.

Totes les configuracions que fem, tindran la mateixa estructura:

- Definirem la acl:

```
acl "nom_de_la_llista" [tipus de parametre] "contingut de la llista"
```

- Aplicarem la regla de control sobre la llista:

```
http_access [allow|deny] "nom_de_la_llista"
```

El que hem de tenir més en compte a l'hora de definir les nostres restriccions, és l'ordre en el que les fem.
Això a més, depen de la política per defecte que volguem dur a terme.
En aquest cas, hem optat per una política de restricció, és a dir, si un ordinador no esta definit per cap regla de control d'accés, per defecte se li denegarà totalment l'accés a internet.

En l'exemple que farem, permetrem accés total a una minoria, després aplicarem restriccions sobre tota la resta de clients a la xarxa, tot seguit permetrem l'accés a internet per a un col·lectiu de treballadors, als quals se'ls hi aplicaran les restriccions definides anteriorment, i finalment, denegarem l'accés a tota la resta.

Per a fer això haurem d'estructurar les nostres regles de la manera següent.

```
permetre a la minoria  
aplicar restriccions  
permetre al col·lectiu  
denegar pas a la resta
```

Les polítiques de control per defecte, es defineixen de la següent manera:

```
http_access [allow|deny] all
```

En comptes de donar una llista com a paràmetre, el que fem és utilitzar la paraula clau "all", que indica "tota la resta".

3.1 Restricció per Ip

La restricció per ip, no és res més que generar una llista amb les direccions ip de la nostra xarxa, per a les quals volem aplicar una regla.

La manera més comode de fer-ho, es definir un fitxer extern on hi hagin contingudes les ip dessitjades. El fitxer ha de presentar obligatoriament un estil semblant a aquest:

```
192.168.8.151
192.168.8.112
...
```

En el nostre cas hem definit dues llistes per ip, una amb les direccions dels caps, als quals tindran lliure acces a internet, i una altra amb les direccions dels treballadors, als quals se'ls hi aplicaran restriccions en l'acces.

- Veiem a continuació la definició de les llistes

```
acl permitidos src "/etc/squid/permitidos" -> caps
```

```
acl trabajadores src "/etc/squid/trabajadores" -> empleats
```

En el cas d'estar definint fitxers que contenen direccions ip, haurem de fer servir la paraula clau "src", i a continuació indicar la ruta absoluta d' on es troba el fitxer que volem incloure a la configuració.

3.2 Denegació de paraules

La operativa, és practicamente la mateixa, només canvia la manera de definir la llista. Ens haurem de crear un fitxer extern que contingui un llista vertical (com la de direccions ip), amb el seguit de paraules que voldrem vetar als usuaris de la xarxa. Així per exemple quan busquin paraules malsonants a "www.google.es", aquest no els hi mostrarà.

- Definició

```
acl palabras_denegadas url_regex "/etc/squid/palabras_denegadas"
```

On "url_regex" indica a squid que es tracta d'un fitxer de paraules, i a continuació la ruta absoluta dintre del nostre sistema de fitxers.

3.3 Restricció de llocs web

La forma de per a definir una restricció d'aquest tipus, és exactament igual a les vistes anteriorment, només hem de substituir la paraula clau, que indica el tipus de fitxer del qual es tracta.

Aquest tipus de restricció, ens permet vetar l'accés a una web independentment del seu contingut.

- Definició

```
acl webs_deny dstdomain "/etc/squid/webs_deny"
```

On "dstdomain", és el domini de destí al qual ens estem referint.

3.4 Delimitació per horaris

Per últim i per complir amb la petició de l'empresa, hem de restringir l'accés a internet només a les hores d' oficina, impedint que certs treballadors es quedin a fer hores extres per a utilitzar aquest recurs de xarxa.

- Definició

```
acl RestringirPorHoras time MTWHF 08:00-20:00*
```

Com podem veure, la definició base de la acl, és la mateixa per a totes les restriccions. El que varia en aquest cas, és que squid, no busca l'informació en un fitxer extern, sinó que esta definit dins del propi archiu.

La paraula reservada "time", ens indica que es tracta d'una restricció horaria.

Les sigles "MTWHF", són les inicials dels dies de la setmana respectivament, és a dir, en aquest camp definim per a quins dies te validesa la llista de control d'accés que estem creant.

A continuació hem de definir el rang d'hores per als dies indicats anteriorment.

En aquest cas de 8 del mati a 8 del vespre que és l'horari d' oficines.

*Nota: Val a dir, que els rangs d'hores han de ser sempre ascendents dins d'un mateix dia, és a dir, només es poden definir rangs, de matinada cap a nit, mai de nit cap a mati del dia següent.

4- Configuració acl

Aquest és l'aspecte que presentaran les regles de control d'accés que han d'adaptar-se a les condicions imposades per a l'empresa que sol·licitava una sol·lució de xarxa.

```
http_access allow permitidos
http_access deny webs_deny
http_access deny palabras_denegadas
http_access deny !RestringirPorHoras
http_access allow trabajadores

http_access deny all
```

Una breu explicació del resultat obtingut:

- Amb la primera sentència, estem permetent als usuaris inclosos dintre de la acl "permitidos" un lliure accés a internet, que en aquest cas aniria destinat als caps.
- Apliquem una restricció per a les webs de la acl "webs_deny"
- Impedim que es puguin fer cerques de paraules malsonants
- Restringim l'ús d'internet als horaris d'oficina especificats anteriorment.
- Permetem accés a internet als treballadors. Val a dir que les restriccions que hem aplicat a sobre, afecten a aquest grup de clients, però no al primer de tots que és el de caps. Això és degut a que squid executa aquestes línies seqüencialment.
- Amb l'última línia, deneguem l'accés total a internet per a aquells usuaris que no hagin estat definits en els casos anteriors.

5- Personalització d'errors

Per a fer més amigable i propera l'aparició d'errors en els clients quan aquest intentin accedir a un lloc restringit, squid permet canviar l'idioma en el que apareixen els errors, o inclús modificar les webs per a crear errors personalitzats.

Per a canviar l'idioma per defecte, hem de crear un enllaç simbòlic entre el directori de l'squid, i la carpeta a on es troben els arxius originals.

- Executem en consola (rutes per defecte, poden variar.)

```
$sudo ln -s /usr/share/squid/errors/Spanish/* /etc/squid/errors/
```

- I tot seguit canviar a l'arxiu de configuració:

```
error_directory /usr/share/squid/errors/Spanish
```