

INSTALACION DE SQUID



Esta nota servirá para mostrar una configuración adecuada de squid, con cosas que probablemente no se ven en otros tutoriales.

Introducción.

El squid es un proxy a nivel de aplicación, que viene con la mayoría de las distros de linux. En particular, usare para la nota debian, por lo que lo que deberiamos hacer, en esta ocasión, es lo siguiente.

debian:~# apt-get install squid

Leyendo lista de paquetes... Hecho

Creando Arbol de dependencias... Hecho

Se instalarán los siguientes paquetes extras:

squid-common

Paquetes sugeridos:

squidclient squid-cgi logcheck-database resolvconf smbclient

Se instalarán los siguientes paquetes NUEVOS:

squid squid-common

Esto nos descargará el squid, en nuestra pc, y de acá, lo que deberemos hacer, es configurar el archivo /etc/squid/squid.conf.

pero antes, deberemos tener en cuenta, que antes, el squid, genera archivos de logueo, en /var/log/squid/, y que estos seran muy importantes, para en el futuro poder ver la actividad del proxy.

Empezando.

Veremos los archivos de configuración:

Directivas:

Las directivas en el squid, son los parametros a pasar. Asi , por ejemplo, es normal, que el http_port (Puerto de Squid), este seteado en el port 3128,

pero tambien, mucha gente lo usa en el 8080 (Como lo usaba el viejo Proxy de Microsoft).

¿Como cambiar esto?.

Sencillo, deberemos ubicar la directiva

http_port 3128

y la cambiamos a

http_port 8080

Visible Hostname

Existe una clausula, llamada visible hostname, que es muy importante. En esta clausula, se define el nombre del proxy

por ejemplo

visible_hostname proxy.midominio.com.ar

Es muy importante que este clausula este correctamente seteada, sino, no se podra iniciar el servicio de squid.

ACLS:

Bueno, acá empieza la parte fundamental del funcionamiento del squid. Todos sabemos que la función primordial del squid, es el filtrado de contenido. Las acls, lo que hacen, precisamente es ello.

Por ejemplo, vamos a ver lo siguiente

```
acl redlocal src 192.168.4.0/24
```

Que significa todo esto?

Se define una acl llamada red local, y se define como src (origen), todo lo que viene desde la red, 192.168.4.0/24, o sea toda la red con mascara 2

255.255.255.0.

Esta es una ACL mas bien sencilla, ya veremos mas adelante, como se complicara todo.

Paso a paso:

Insertaremos la nueva acl, en el archivo de configuración simplificado, le hemos sacado todos los comentarios a nuestro archivo, para una mejor comprensión

```
http_port 3128
```

```
visible_hostname proxy.midominio.com.ar
```

```
acl redlocal src 192.168.4.0/24
```

```
#Recommended minimum configuration:
```

```
acl all src 0.0.0.0/0.0.0.0
```

```
acl manager proto cache_object
```

```
acl localhost src 127.0.0.1/255.255.255.255
```

```
acl to_localhost dst 127.0.0.0/8
```

```
acl SSL_ports port 443 563
```

```
acl Safe_ports port 80 # http
```

```
acl Safe_ports port 21 # ftp
```

```
acl Safe_ports port 443 563 # https, snews
```

```
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
```

```
# Deny requests to unknown ports
```

```
http_access deny !Safe_ports
```

```
# Deny CONNECT to other than SSL ports
```

```
http_access allow red_local
```

```
http_access deny all
```

Digamos que con esta mínima configuración, tenemos acceso a toda la red, [192.168.4.0/24](#), sin ningun tipo de restricciones. Ahora bien, supongamos que por un enlace punto a punto, o tambien podria ser via vpn, o diversas configuraciones locales, tenemos una red, por ejemplo en Villa Dolores(Cba).

Definiremos esa red

acl villa_dolores [192.168.5.0/24](#)

donde es obvio, que estamos dejando pasar a toda la red [192.168.5.0/24](#)

Complicando un poco mas, y entendiendo la sintaxis de las acls.

Veremos, en un primer momento, yo quisiera que toda la red de villa dolores, tenga acceso a internet, pero que no pueda descargarse archivos.

esto ya se esta complicando aun un poco mas, por eso, deberemos primero generar una acl archivos, y ya veremos como.

```
acl archivos urlpath_regex "/etc/squid/archivos"
```

aca vemos, que usaremos una regex(Expresion regular), para ver que tipos de archivos están envueltos en esta regla. Obviamente, como la mayoría habrá supuesto, existirá un archivo llamado /etc/squid/archivos. En caso de no existir este archivo, al restartear squid, seremos informados.

en el archivo, /etc/squid/archivos, pongo lo siguiente

```
exe  
avi  
mp3  
mpeg  
mp4  
rad
```

Y con esto, agregamos estos tipos de archivos a la acl archivos. Ahora veremos como aplicar esta acl.

Supongamos que a la red de villa dolores, le quisiera dar internet, pero no quisiera que se pudieran bajar de una pagina, los siguientes archivos, entonces,generaría una regla del siguiente tipo

```
http_access allow villa_dolores !archivos
```

como vemos, el !archivos, funciona como un NOT. entonces, dejara pasar la acl definida en villa_dolores, que es que toda la red [192.168.5.0](#) pueda navegar, pero no dejare que bajen los archivos.

Viendo otro ejemplo mas

Supongamos ahora mismo, que queremos filtrar una gran cantidad de palabras obsenas, como puede ser, (vamos, las que uds. ya conocen!!).

generamos una acl, que ahora, tenga como sentido el filtro de palabras.

```
acl filtrar url_regex "/etc/squid/filtrar"
```

con esto, el url_regex, filtrara las palabras que estarán en el archivo filtrar

en el archivo filtrar por ejemplo ponemos

```
pedofilia
```

```
gays
```

```
travestis
```

Y si en la url destino, encontráramos esas palabras, se denegaría el acceso.

filtro MSN:

Esto me costo bastante, y fue mas bien viendo por donde se metia el msn, en los logs del squid.

```
acl filtro_msn dstdomain "/etc/squid/msn"
```

aca vemos la directiva dstdomain. Se filtrara por el dominio de destino, que estará especificado en /etc/squid/msn

en ese archivo, pondremos.

[gateway.messenger.hotmail.com](#)

[login.live.com](#)

[login.live.com:443](#)

[messenger.hotmail.com](#)

[messenger.msn.com](#)

[messenger.microsoft.com](#)

[echo-v1.msgr.hotmail.com](#)

[echo-v2.msgr.hotmail.com](#)

[echo-v3.msgr.hotmail.com](#)

[echo-v4.msgr.hotmail.com](#)

[echo-v5.msgr.hotmail.com](#)

[echo-v6.msgr.hotmail.com](#)

[echo-v7.msgr.hotmail.com](#)

[echo-v8.msgr.hotmail.com](#)

[echo-v9.msgr.hotmail.com](#)

[echo-v10.msgr.hotmail.com](#)

[g.msn.com](#)

[rsi.hotmail.com](#)

[config.messenger.msn.com](#)

y con esto, nos aseguramos que no se puedan conectar al msn. Si bien anteriormente al MSN Live, se podia hacer una regla por aplicacion, pero ahora ya no.

entonces, simplificando, imaginemos que queremos que la red de villa dolores, no tenga ni msn, ni baje archivo, ni vea paginas con palabras prohibidas,

generamos la siguiente acl.

```
http_access allow villa_dolores !filtro_msn !archivos !filtrar
```

con esto, demostramos que se puede filtrar, y usando la logica, podemos incluir muchisimas directivas.

Configuracion final del /etc/squid/squid.conf

```
http_port 3128
```

```
visible_hostname proxy.midominio.com.ar
```

```
acl redlocal src 192.168.4.0/24
```

```
acl villa_dolores src 192.168.5.0/24
```

```
acl filtrar url_regex "/etc/squid/filtrar"
```

```
acl filtro_msn dstdomain "/etc/squid/msn"
```

```
acl archivos urlpath_regex "/etc/squid/archivos"
```

```
#Recommended minimum configuration:
```

```
acl all src 0.0.0.0/0.0.0.0
```

```
acl manager proto cache_object
```

```
acl localhost src 127.0.0.1/255.255.255.255
```

```
acl to_localhost dst 127.0.0.0/8
```

```
acl SSL_ports port 443 563
```

```
acl Safe_ports port 80 # http
```

```
acl Safe_ports port 21 # ftp
acl Safe_ports port 443 563 # https, snews
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
# Deny requests to unknown ports
http_access deny !Safe_ports
# Deny CONNECT to other than SSL ports
http_access allow red_local
http_access allow villa_dolores !filtro_msn !archivos !filtrar
http_access deny all
```

Otros tipos de configuraciones y directivas:

Existe la posibilidad de filtrar por horario de trabajo, por grupos y dominios (Para eso utilizaremos Winbind, si queremos unir el server a un dominio), o también, la posibilidad de conectar a un árbol de directorio LDAP, (OpenLdap, Novell eDirectory, y también hasta a Microsoft Active Directory). Cambien existe la validación básica, usuario a usuario.

Vamos por el log

Si nosotros quisiéramos visualizar la actividad del squid, deberíamos buscar esto en el archivo de log del squid (/var/log/squid/squid.log)