

# CAPÍTULO 11

## Configuración de un Proxy

Los usuarios de un sistema navegan por la red de dos formas distintas; el primer método consiste en utilizar el navegador de Internet para solicitar páginas directamente desde servidores web remotos (método directo).

Pero existe otro modo que implica el almacenamiento o “cacheo” (caching) de la web. Siempre que un usuario quiera visitar una página web, mejor que hacer que su cliente vaya al servidor remoto, el cliente solicita la página al servidor de caché; el servidor entonces mira a ver si la página ya ha sido descargada. Si es así, la página estará almacenada en la caché del servidor o almacén de datos. El servidor comprobará si hay disponible una nueva versión de la página y si no existe, pasará la versión que tiene guardada al navegador cliente.

Proporcionar un servicio como éste puede acelerar enormemente el tiempo de descarga de una página web, ya que sólo aquellas que es necesario se descargan realmente de nuevo. Por otro lado las descargas de las páginas que todavía no han sido almacenadas no se ralentizan.

El programa Squid es un servidor proxy con dos propósitos básicos; una la de proporcionar servicio proxy a máquinas que comparten el acceso a Internet; la otra es la de almacenar. Los navegadores actuales suelen proporcionar este servicio pero a cada usuario independientemente; squid lo hace para todo el que pueda acceder a la red. Squid puede actuar de proxy para los protocolos FTP, HTTP, HTTPS y DNS.

Lo primero que debes hacer es instalarlo, porque no viene en GuadaLinux; el paquete se llama “squid” y puedes instalarlo por ejemplo mediante apt. Tras la instalación aparecerá el script que controla el demonio en /etc/init.d y el archivo de configuración, llamado /etc/squid.conf; es un archivo relativamente largo, pero la mayoría son comentarios (en inglés) de las opciones.

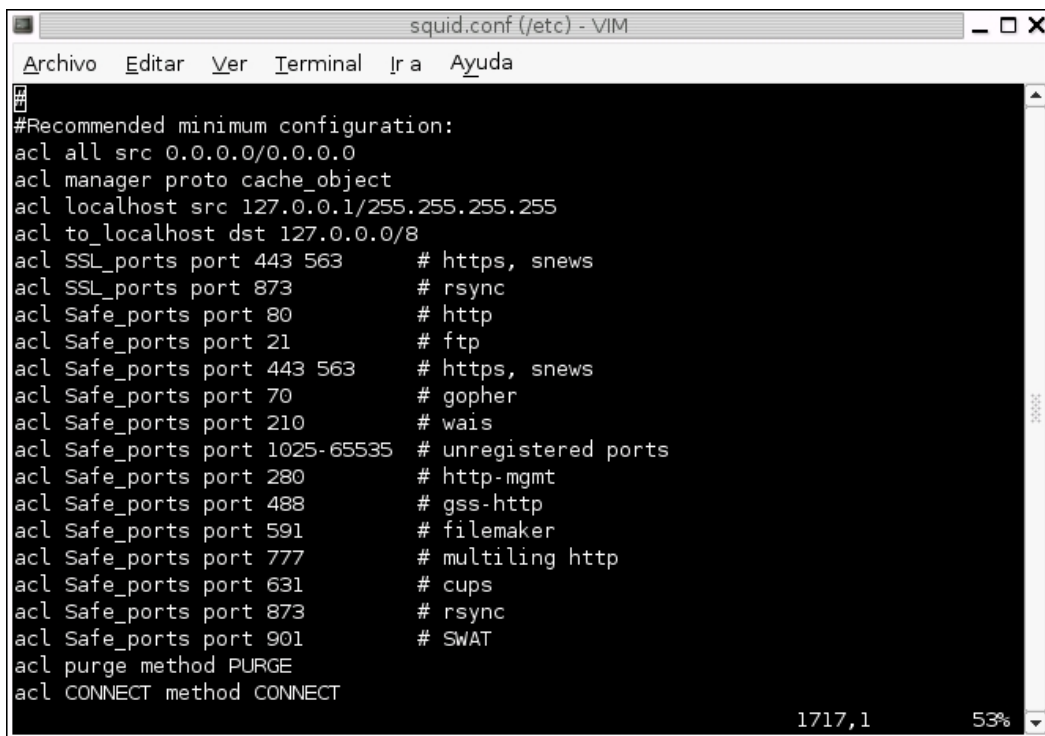
Es posible que aparezca un error y no arranque el servidor; no te preocupes, más adelante veremos cómo solucionar esto (el error te avisa sobre definir algo llamado “visible\_hostname”).

Editando el archivo se observa que todos las directivas de control de los servicios están deshabilitadas; esto es así porque squid funciona con unos puertos predeterminados para cada uno de los servicios soportados (si se especifica, porque puede aparecer “none” si no está activado por defecto). En el caso de coincidir con otro puerto que se esté utilizando hay que borrar el símbolo “#” e introducir el número de puerto a utilizar; por ejemplo para utilizar el puerto 3128 (el que se usa mientras no se diga lo contrario) hay que poner en la línea correspondiente:

http\_port 3128

Y a partir de entonces se ofrece el servicio proxy para http en ese puerto. Ten siempre presente cuando cambies un puerto comprobar que no se utiliza en algún servicio; consulta el archivo /etc/services para no tener ninguna duda; también recuerda evitar los números de puertos inferiores al 1024 porque suelen estar reservados.

El archivo tiene muchas opciones, pero verdaderamente interesante resulta comentar el sistema de control de acceso, que es realmente complejo y potente; su funcionamiento se basa en unas listas de control de acceso o ACL (Access Control List). Para acceder a esta sección debes ir a la línea 1590 aproximadamente (aunque dependerá de la versión que instales), donde se define la directiva “acl”; existen algunas ya creadas como puedes ver en la imagen.



```
#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      # https, snews
acl SSL_ports port 873         # rsync
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 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
```

La estructura de esta directiva es:

acl      nombre\_lista tipo\_lista      elemento

El valor de nombre\_lista es el que le vamos a dar a esa lista; puede ser cualquiera, pero suele identificar al grupo que queremos controlar; el tipo\_lista es el tipo de elementos a incluir en la lista, y puede ser entre otros uno de los siguientes:

|           |                                                                      |
|-----------|----------------------------------------------------------------------|
| dst       | especifica la IP de la máquina o red de destino (con o sin máscara). |
| dstdomain | nombre de domino del destino.                                        |
| port      | indica los puertos a buscar.                                         |
| proto     | protocolo a buscar                                                   |
| src       | especifica la IP de la máquina o red de origen (con o sin máscara).  |
| srcdomain | nombre de dominio del destino.                                       |
| time      | tiempo a buscar.                                                     |

Este último se expresa con una letra que indica el día de la semana seguido de hora1:minuto1-hora2:minuto2; las letras para los días son S (Domingo), M (Lunes), T (Martes), W (Miércoles), H (Jueves), F (Viernes) y A (Sábado).

Como ejemplos, para crear una lista para acceder los lunes de 9 a 2:

```
acl    Mañanas                    time            M      9:00-14:00
```

Y para crear otra para aplicarla a los puertos web y ftp:

```
acl    DosPuertos   port            80 21
```

Para realizar alguna acción sobre los elementos de una lista, se utiliza la directiva http\_access, seguida de la acción a tomar (permitir o “allow”, y denegar o “deny”); si quisiéramos permitir el uso de los puertos web y ftp pero no por las mañanas:

```
http_access   allow            DosPuertos
http_access   deny            Mañanas
```

Hay que hacer un par de precisiones aquí; la primera es que el orden es muy importante, ya que las listas de control (directivas http\_access) se aplican en orden consecutivo. En el ejemplo anterior efectivamente se permite utilizar el proxy para los puertos 80 y 21, pero se deniega su uso los lunes por la mañana; si hubiéramos cambiado el orden primero se denegaría el uso del proxy los lunes por la mañana (de todo el proxy), mientras que se permitiría usar esos puertos en otro momento; la diferencia es que otro puerto (por ejemplo el 443, que es el que utiliza https) no podría ser usado tampoco los lunes por la mañana, ya que la denegación no se realiza por puertos sino por horario.

La segunda observación es más evidente: un servidor squid bien configurado puede evitar el uso de un cortafuegos. El caso típico es una máquina conectada a Internet y a la red local dedicada únicamente a tareas de proxy.

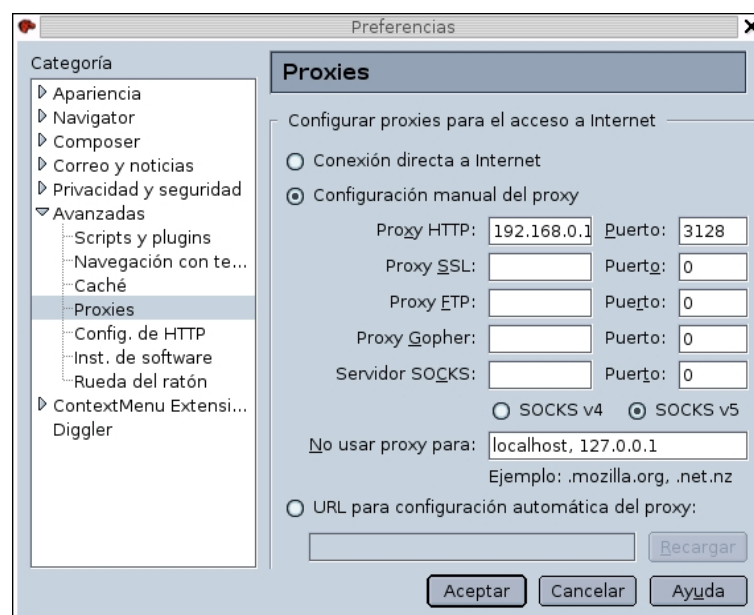
Si no lo has hecho ya define la directiva “visible\_hostname” con el nombre completo de tu dominio. Otras opciones que quizá te gustaría modificar son:

- cache\_mem 8 MB: cantidad de memoria Ram que se utilizará para uso interno.
- maximum\_object\_size 4096 KB: no almacenar objetos con un tamaño mayor.
- fdncache\_size 1024: cantidad de nombres de dominio que se almacenan.
- cache\_dir /var/spool/squid 100 16 256: por defecto se usa ese directorio y 100 MB de espacio para la caché.

Squid posee características avanzadas entre las que se encuentran:

- Posibilidad de limitar los recursos a utilizar en la máquina (memoria, espacio en disco, procesos, ...)
- Posibilidad de configurar políticas de reemplazos de los datos en la almacenados en la caché.
- Puede utilizarse en una estructura jerárquica, con otras máquinas con squid también instalado.
- Es posible utilizarlo para balancear la carga de un sitio web (redirigir peticiones a diferentes máquinas para no colapsar ningún servidor.

Para poder utilizar el servidor proxy, lo único que tienen que hacer las máquinas clientes es comunicarle al navegador la dirección IP del servidor y el puerto que debe utilizar. Por ejemplo en Mozilla está en el menú Editar -> Preferencias -> Avanzadas -> Proxies.



## ***Ejercicios***

1) Crea una lista de acceso para utilizar el servicio web los días laborables de 4 a 7 de la tarde.

2) Establece un tamaño máximo de utilización del disco de 150 MB

### **Soluciones**

1) Deberás crear las siguiente entradas:

```
acl    ejercicio    time    M    16:00-19:00
acl    ejercicio    port    80
http_access    allow    ejercicio
```

2) Simplemente modifica esta línea y sustituye el 100 por 150:

```
cache_dir /var/spool/squid 150 16 256
```