Squid y las listas de control de acceso. Configuración básica en Ubuntu

Imagina que eres el administrador de una red de área local y no deseas que los usuarios de la red se conecten a Internet a partir de cierta hora, o que no que no puedan hacer uso de Internet los fines de semana, no se puedan descargar archivos .exe o acceder a ciertas páginas de Internet. Todo eso y más lo podemos controlar con Squid, el servidor proxy más popular y extendido entre las diferentes distribuciones basadas en GNU/Linux. Un proxy es un servidor cuyo objetivo es la centralización del tráfico entre Internet y una red local, de esa forma, cada uno de los ordenadores de la red local no tiene necesidad de disponer de una conexión directa a Internet. Además, también se utiliza para controlar los accesos no permitidos desde Internet hacia la red local o viceversa.

A continuación mostraré como instalar y configurar Squid en Ubuntu. A través de varios ejemplos también mostraré algunos archivos de configuración básicos para comprender mejor como funciona.

Instalación y arranque de Squid

Para instalar squid tan sólo tendremos que abrir el terminal y escribir:

- sudo apt-get install squid.

Para arrancar squid escribimos:

- /etc/init.d/squid start

Para pararlo:

- /etc/init.d/squid stop

Y para reiniciarlo:

- /etc/init.d/squid restart

Configuración básica de Squid

El archivo de configuración se encuentra en /etc/squid/ y se llama squid.conf. Una configuración básica debe incluir, al menos, los parámetros que se indican a continuación:

- **http-port**: Establece el puerto de escucha para squid (por defecto puerto 3128).
- **visible_hostname**: nombre del equipo.
- **acl**: a cada ACL o lista de control de acceso se le hace corresponder una regla de control de acceso (http_access) que es la que permite o deniega las conexiones definidas en cada acl (más adelante veremos que son las acl).

Otros parámetros importantes son:

- cache_dir. Establece la localización y el tamaño de la caché en el disco duro.

Ejemplo: cache_dir ufs /var/spool/squid 100 16 256

ufs es el sistema de almacenamiento que utiliza squid. 100 el tamaño en megas de la caché, 16 el nivel de subdirectorios de primer nivel y 256 el segundo nivel de subdirectorios por cada directorio de primer nivel.

Las listas de control de acceso o ACL

Las listas de control de acceso nos permitirán designar qué máquinas o redes tienen permitido, o no, acceder al servidor. A continuación, a cada ACL creada se le hace corresponder una regla de control de acceso (http_access) que es la que permite o deniega las acciones definidas en la ACL.

El siguiente ejemplo muestra una lista de control de acceso que identifica a nuestra red de área local (suponiendo que tiene la dirección de red 192.168.1.0 y máscara 255.255.255.0).

- acl red_local src 192.168.1.0/255.255.255.0

Si queremos permitir el acceso al servidor proxy a todos los ordenadores de la red, tendríamos que escribir la siguiente línea en el archivo de configuración de squid (/etc/squid/squid.conf)

- http_access allow red_local

Y si queremos denegar el acceso:

- http_access deny red_local

Tras acl se pone el nombre que se le asigna a la lista de control de acceso. Las listas de control de acceso emplean algunos parámetros como los siguientes:

- src hace referencia a la IP de un ordenador o a una dirección de red
- time permite denegar conexiones dentro de un rango horario.

- srcdomain y dstdomain permiten denegar conexiones a un determinado dominio web.
- url_regex permite definir una ACL que identifica sitios web dependiendo que la URL contenga ciertos caracteres o palabras.

Configuración de los clientes

Para que cada uno de los clientes de la red puedan comunicarse con Squid, debemos configurar el navegador en cada uno de ellos para que salgan a Internet a través del proxy. En Mozilla Firefox, por ejemplo, debemos ir a Editar/Preferencias/Avanzado/Red/Configuración. Seleccionamos a continuación "Configuración manual del proxy" e introducimos la IP y puerto de escucha del proxy.

Modificación de los mensajes de error de Squid

Por lo general Squid viene preconfigurado con mensajes en inglés, podemos modificarlo para que estos mensajes de error salgan en español o poner los nuestros propios. Si queremos que aparezcan en español en el archivo de configuración de squid pondremos:

- error_directory /usr/share/squid/errors/Spanish

Si queremos modificar por ejemplo el mensaje de error que aparece al impedir el acceso a una determinada página editaremos el archivo ERR_ACCESS_DENIED.

Veamos a continuación algunos ejemplos de archivos de configuración

Ejemplo 1

Crear un archivo de configuración para denegar el acceso a todos los equipos a la dirección www.google.es

```
visible_hostname alex-laptop
http_port 8080
acl all src 0.0.0.0/0.0.0.0
acl no_permitido1 dstdomain www.google.es
acl localhost src 127.0.0.1
http_access deny no_permitido1 !localhost
```

En este ejemplo construimos la acl llamada localhost que representa el servidor proxy (dirección loopback). Observa que en http_access se ha puesto !localhost para denegar el acceso a todos los ordenadores de la red menos al ordenador local. De esta manera el ordenador en el que está instalado squid puede acceder a la página www.google.es

Ejemplo 2

Crear un archivo de configuración que deniegue el acceso a las direcciones www.google.es y www.alejandrox.com

```
visible_hostname alex-laptop
http_port 8080
acl all src 0.0.0.0/0.0.0.0
acl localhost localhost src 127.0.0.1
acl no_permitido1 dstdomain www.google.es www.alejandrox.com
http_access deny no_permitido1 !localhost
```

En este caso el fichero de configuración es similar al caso anterior. Tan sólo hay que poner www.alejandrox.com después de www.google.es en la acl no_permitido1.

Ejemplo 3

Crea en tu carpeta personal un archivo llamado no_permitidos que contenga las direcciones de los tres siguientes dominios:

www.google.es
http://es.yahoo.com/
http://es.msn.com/

Para crear este archivo puedes abrir el terminal (Aplicaciones/Accesorios/Terminal) y escribir:
gedit /home/nombre_de_usuario/no_permitidos.

A continuación crea un archivo de configuración squid.conf que deniegue las conexiones a las direcciones que se encuentran en el archivo no_permitidos.

visible_hostname alex-laptop
http_port 8080
acl all src 0.0.0.0/0.0.0.0
acl localhost src 127.0.0.1
acl no_permitido1 url_regex "/home/alex/no_permitidos"
http_access deny no_permitido1 !localhost

Ejemplo 4

Se dispone de una red local con dirección 192.168.1.0 y máscara 255.255.255.0. Crear un archivo de configuración squid.conf que permita el acceso a Squid a todos los ordenadores de la red y no lo permita a los restantes.

visible_hostname alex-laptop
http_port 8080
acl all src 0.0.0.0/0.0.0.0
acl todalared src 192.168.1.0/255.255.255.0
acl localhost src 127.0.0.1
http_access allow todalared
http_access deny all !localhost

Ejemplo 5

Se dispone de una red de área local con dirección 192.168.1.0 y máscara 255.255.255.0. Se desea permitir el acceso a Squid a los ordenadores con las IP que están comprendidas en el rango 192.168.1.1 y 192.168.1.10 (ambas incluidas). Crea en tu directorio personal un fichero llamado ip_permitidas que tenga estas direcciones (cada dirección en una línea diferente). A continuación indica que fichero de configuración para Squid crearías para permitir el acceso a Squid a todas estas direcciones y denegar el acceso a las restantes.

visible_hostname alex-laptop
http_port 8080
acl all src 0.0.0.0/0.0.0.0
acl red_local src "home/nombre_usuario/ip_permitidas"
acl localhost src 127.0.0.1

```
http_access allow red_local
http_access deny all !localhost
```

Ejemplo 6

Impide la conexión a Internet a todos los equipos en horario de 18:00 a 21:00 horas.

```
visible_hostname alex-laptop
http_port 8080
acl all src 0.0.0.0/0.0.0.0
acl localhost src 127.0.0.1
acl horario time 18:00-21:00
http_access deny horario !localhost
```

Ejemplo 7

Deniega las conexiones a todos los equipos en horario de 18:00 a 21:00 horas, pero sólo los lunes, martes y miércoles.

```
visible_hostname alex-laptop
http_port 8080
acl all src 0.0.0.0/0.0.0.0
acl horario time MTW 18:00-21:00
http_access deny horario !localhost
```

Ejemplo 8

Deniega el acceso a Squid al equipo con IP 192.168.1.5. Permite el resto de accesos a Squid.

```
visible_hostname alex-laptop
http_port 8080
acl all src 0.0.0.0/0.0.0.0
acl equipo5 src 192.168.1.5
http_access deny equipo5
```

Ejemplo 9

Deniega el acceso a Squid al equipo con IP 192.168.1.5 en horario de 18:00 a 21:00 horas. Permite el resto de accesos a Squid.

```
visible_hostname alex-laptop
http_port 8080
acl all src 0.0.0.0/0.0.0.0
acl equipo5 src 192.168.1.5
```

```
acl horario time 18:00-21:00
http_access deny equipo5 horario
```

Ejemplo 10

Deniega el acceso a Squid al equipo con IP 192.168.1.5 en horario de 18:00 a 21:00 horas. Para el resto de equipos permitir el acceso sólo en horario de 10:00 a 14:00 horas. Se supone que los equipos pertenecen a la red 192.168.1.0 con máscara 255.255.255.0.

```
visible_hostname alex-laptop
http_port 8080
acl all src 0.0.0.0/0.0.0.0
acl red_local src 192.168.1.0/255.255.255.0.
acl equipo5 src 192.168.1.5
acl horario1 time 18:00-21:00
acl horario2 time 10:00-14:00
http_access deny equipo5 horario1
http_access allow red_local horario2
http_access allow equipo5
```

Ejemplo 11

En el archivo /etc/squid/permitidos se tiene una lista de todas las direcciones IP de la red local. El equipo10 tiene la dirección IP 192.168.1.10. Se permite el acceso a Internet al equipo10 de lunes a miércoles de 9:00 a 14:00 horas. También se permite el acceso a los equipos de la red local de lunes a miércoles. Se prohíbe el acceso en el resto de casos.

```
visible_hostname alex-laptop
http_port 8080
acl all src 0.0.0.0/0.0.0.0
acl localhost src 127.0.0.1
acl redlocal src “/etc/squid/permitidos”
acl equipo10 src 192.168.1.10
acl horario time MTWHF 9:00-14:00
acl horario2 time MTW
http_access allow equipo10 horario
http_access allow redlocal horario2
http_access allow localhost
http_access deny all
```

Ejemplo 12

Restringe el acceso a todo el contenido con extensión .mp3 a los ordenadores de la red.

```
visible_hostname alex-laptop
http_port 8080
acl all src 0.0.0.0/0.0.0.0
acl redlocal src 192.168.1.0/255.255.255.0
acl musica urlpath_regex \.mp3
http_access allow redlocal !musica
http_access deny all
```