PROXY SERVER SQUID

SQUID

El término *PROXY* es bastante ambiguo y muy general, sin embargo, se puede definir como un servidor que permite a los clientes realizar conexiones de red indirectas hacia otros servicios de red

Instalación y configuración

Se instala mediante el paquete *squid*

El archivo de configuración se encuentra en */etc/squid/squid.conf*

Inicio, parada y reinicio del servicio squid

service squid start | *stop* | *restart*

Opciones de configuración

NOTA El archivo squid.conf es similar a cualquier otro archivo de configuración GNU/LINUX, pero este no permite espacios en blanco antes de las directivas de configuración

OPCIONES GENERALES

OPCIÓN	DESCRIPCIÓN	VALOR POR DEFECTO
http_port	Puerto de escucha utilizado por **SQUID**	3128
visible_hostname	Nombre del servidor proxy **SQUID** Normalmente será el nombre del ordenador donde se ejecuta **SQUID**	-
error_directory	Establece el idioma de las diferentes páginas de error o informativas Para establecer el idioma español */usr/share/squid/errors/es-es*	-
auth_param basic program	Indica el módulo de autenticación que utilizará **SQUID**	-
redirect_program	Permite a SQUID trabajar conjuntamente con otros programas	-
access_log	Registro de accesos a través de **squid** Tiene que especificarse	-

OPCIONES DE FILTRADO

acl	Establece una lista de control de acceso	-
http_access	Establece una regla de control de acceso	-

Ejemplo. Archivo de configuración mínima de un servidor proxy **SQUID**

```
#SERVIDOR PROXY SQUID
#OPCIONES GENERALES
http_port 3128
visible_hostname nombre_servidor
access_log /var/log/squid/access.log
error_directory /usr/share/squid/errors/es-es

#LISTAS CONTROL ACCESO
acl all src all
acl localhost src 127.0.0.1/32
acl localnet src 192.168.1.0/24

#REGLAS CONTROL ACCESO
http_access allow localhost
http_access allow localnet
http_access deny all
```

PROXY SERVER SQUID

CONTROL DE ACCESO

CONTROL DE ACCESO MEDIANTE DIRECCIONES IPS

Los controles de acceso se basan en **LISTAS DE CONTROL DE ACCESO** y **REGLAS DE CONTROL DE ACCESO** que permitirán o negarán el acceso a **SQUID**

Listas de control de acceso

Se podría definir como QUE y A QUIEN se le aplicará una **regla de control de acceso**

Su sintaxis es acl [nombre_lista] src [componentes_lista]

Ejemplo. Crear una lista de control de acceso que abarca toda la red

```
acl red_local src 192.168.1.0/24
```

También se pueden crear listas de control de acceso especificando la ruta hacia un archivo determinado

Ejemplo. Crear una lista de control de acceso "denegados" mediante un fichero

```
acl denegados src "/etc/squid/listas/denegados"
```

El archivo "denegados" quedaría

```
#FILTRO IP
192.168.1.1
192.168.1.2
192.168.1.3
```

Reglas de control de acceso

Definen si se permite o no el acceso hacia **squid** a las **listas de control de acceso** definidas

Su sintaxis es http_access [deny | allow] [lista_control_acceso]

Ejemplo. Permitir el acceso a **SQUID** a una lista llamada "red_local"

```
http_access allow red_local
```

También pueden definirse reglas con el signo **!** el cual significa **no**

Ejemplo. Definir dos **listas de control de acceso** "lista1" y "lista2" y establecer una **regla de control** que permita el acceso a lo que comprenda "lista1" pero no a lo que comprenda "lista2"

```
http_access allow lista1 !lista2
```

PROXY SERVER SQUID

CONTROL DE ACCESO POR AUTENTICACIÓN

Autenticación a través del módulo NCSA

*NOTA Para poder hacer uso del módulo de autenticación de **SQUID** es necesario instalar el paquete **APACHE2***

La autenticación de usuarios en **SQUID** se realiza mediante el módulo *ncsa_auth* que ya viene incluido en el propio paquete de instalación **SQUID** en la mayoría de distribuciones. Este módulo provee una autenticación muy sencilla a través de un archivo de texto simple cuyas claves de acceso se generan mediante el comando *htpasswd*

Ejemplo. Configuración servidor proxy **SQUID** con autenticación de usuarios

NOTA Se supone que todos los pasos se realizan con el usuario root

1. Creación del archivo passwd que almacenará los usuarios y sus claves de acceso (cifradas)
   NOTA El archivo puede estar en cualquier lugar del sistema con la única condición de que tendrá que ser accesible por el usuario proxy

   ```
   touch /etc/squid/passwd

   chown proxy:proxy /etc/squid/passwd
   chmod 600 /etc/squid/passwd
   ```

2. Añadir usuarios al archivo *passwd* mediante el comando *htpasswd*
   NOTA Las cuentas de usuario creadas con el comando htpasswd son independientes de las demás cuentas del sistema

   ```
   htpasswd /etc/squid/passwd usuario
   ```

3. Editar el archivo *squid.conf* configurando la directiva *auth_param* e indicando el módulo de autenticación (suelen ubicarse en el directorio /usr/lib/squid) a utilizar y ruta del archivo donde se almacenan los usuarios

   ```
   auth_param basic program /usr/lib/squid/ncsa_auth /etc/squid/passwd
   ```

4. Crear las listas y reglas de control de acceso

   ```
   acl autenticación proxy_auth REQUIRED
   http_access allow autenticacion
   ```

RESTRICCIONES DE ACCESO A SITIOS WEB

Su sintaxis es acl [nombre_expresion] url_regex “ruta_lista_expresiones”

Ejemplo. Prohibir a los ordenadores de la red local 192.168.1.xx acceder a sitios que contengan las palabras *torrent* y *elink*

1. Crear fichero con la lista de expresiones que queramos filtrar

   ```
   sudo mkdir /etc/squid/listas
   sudo gedit /etc/squid/listas/prohibidas

   #FILTRO EXPRESIONES URL
   torrent
   elink
   ```

2. Crear las listas y reglas de control de acceso

   ```
   acl prohibidas url_regex “/etc/squid/listas/prohibidas”
   http_access allow localnet !prohibidas
   ```

RESTRICCIONES DE ACCESO A DOMINIOS

Su sintaxis es acl [nombre_expresion] dstdomain “ruta_lista_dominios”

Los nombres de los dominios se pueden ser nombres de dominio específicos *www.facebook.com*, dominios completos (incluyendo subdominios) *.facebook.com*, un dominio de nivel superior genérico *.com* o una combinación de todo lo anterior

NOTA Si se definen dominios completos, ya no es necesario definir dominios específicos de estos, www.facebook.com, mail.facebook.com, etc. puesto que serán subdominios de .facebook.com

Ejemplo. Filtrar los dominios *.facebook.com* y *.twitter.com*

1. Crear fichero con la lista de dominios que queremos filtrar

   sudo gedit /etc/squid/listas/dominios

   #FILTRO DOMINIOS
   .facebook.com
   .twitter.com

2. Crear las listas y reglas de control de acceso

   acl dominios dstdomain “/etc/squid/listas/dominios”
   http_access allow localnet !dominios

RESTRICCIÓN DE ACCESO A CONTENIDO POR EXTENSIÓN

Su sintaxis es acl [nombre_expresion] urlpath_regex “ruta_lista_extensiones”

Ejemplo. Filtrar las extensiones *pdf* y *jpg*

1. Crear fichero con la lista de extensiones que queremos filtrar

   sudo gedit /etc/squid/listas/extensiones

   #FILTRO EXTENSIONES
   \.pdf$
   \.jpg$

2. Crear las listas y reglas de control de acceso

   acl extensiones urlpath_regex “/etc/squid/listas/extensiones”
   http_access allow localnet !extensiones

RESTRICCIÓN DE ACCESO POR HORARIOS

Su sintaxis es acl [nombre_horario] time [días_semana] hh:mm-hh:mm

Los días de la semana se definen con la primera letra del nombre del día en ingles, así lunes **M**, martes **T**, miércoles **W**, jueves **H**, viernes **F**, sábado **A** y domingo **S**

Ejemplo. Establecer una regla que comprenda un horario de 09:00 a 14:00 de lunes a viernes

acl semana time MTWHF 09:00-14:00

Ejemplo. Permitir a los ordenadores del aula 192.168.1 acceder a web en un horario de lunes a viernes de 08:00 a 14:00

acl localnet src 192.168.1.0/24
acl horario time MTWHF 08:00-14:00

http_access allow horario localnet

PROXY SERVER SQUID

SQUIDGUARD

SQUIDGUARD es un plugin para **SQUID** que incrementa las funcionalidades de filtrado de contenido mediante bases de datos con miles de URL´s y dominios agrupados en diferentes categorías

Instalación y configuración

Se instala mediante el paquete *squidguard*

El archivo de configuración se encuentra en */etc/squid/squidGuard.conf*

Las bases de datos se encuentran en */var/lib/squidguard/db*

Opciones de configuración

OPCIÓN	DESCRIPCIÓN
dbhome	indica el directorio donde se almacenan las bases de datos de **SQUIDGUARD**
logdir	indica el directorio donde **SQUIDGUARD** almacenará los informes generados
dest	Crea una lista de control de acceso
acl	Crea una regla de control de acceso

Ejemplo. Archivo de configuración mínimo de **SQUIDGUARD**

```
#CONFIGURACIÓN SQUIDGUARD
dbhome /var/lib/squidguard/db
logdir /var/log/squid

#LISTAS CONTROL ACCESO
dest adultos{
        domainlist adult/domains
        urllist adult/urls
        }

#REGLAS CONTROL ACCESO
acl{
        default{
                pass !adultos all
                redirect http://www.google.es
                }
        }
```

Ejemplo. Instalación y configuración de **SQUIDGUARD** filtrando redes sociales

1. Instalamos el paquete *squidguard*
2. Configuramos **SQUID** para trabajar conjuntamente con **SQUIDGUARD**

   sudo gedit /etc/squid.conf

   añadimos la opción

   redirect_program /usr/bin/squidGuard –c /etc/squid/squidGuard.conf

3. Descargar las bases de datos *cri.univ-tlse1.fr/blacklists/,* descomprimirlas y moverlas al directorio */var/lib/squidguard/db*
   NOTA se supone la base de datos social-networks

4. Crear las listas y reglas de control de acceso

   ```
   #LISTAS CONTROL ACCESO
   dest redes_sociales{
           domainlist social-networks/domains
           log redes_sociales
           }
   ```

```
#REGLAS CONTROL ACCESO
acl{
    default{
        pass !redes_sociales all
        redirect http://www.google.es
        }
    }
```

5. Reiniciar **SQUID**

```
sudo service squid restart
```

SARG

SARG ***S****quid* ***A****nalysis* ***R****eport* ***G****enerator* es una sencilla pero potente herramienta para generar informes en formato HTML a partir de los ficheros logs de **SQUID**. Permite ver con detalle la actividad de todos los equipos y/o usuarios dentro de la red de área local

Instalación y configuración

Se instala mediante el paquete *sarg*

El archivo de configuración se encuentra en */etc/sarg/sarg.conf*

Opciones de configuración

NOTA Existe un error en el paquete pre compilado.deb. Para solucionar dicho error basta deshabilitar la opción site_user_time_date_type

OPCIONES GENERALES

OPCIÓN	DESCRIPCIÓN	VALOR DEFECTO
access_log	Indica la ubicación del log generado por **squid**	/var/log/squid/access.log
output_dir	Establece donde generará **SARG** los informes HTML	/var/lib/sarg
report_type	Indica el tipo de informe generado por **SARG**	Todas las opciones

OPCIONES DE IDIOMAS

OPCIÓN	DESCRIPCIÓN	VALOR DEFECTO
charset	Establece el charset de los informes generados por **SARG** Recomiendo UTF-8 para visualizar correctamente caracteres españoles	Latin1
languaje	Establece el lenguaje en el cual **SARG** generará los informes HTML Spanish para idioma español	English
date_format	Indica el formato de las fechas e para formato europeo	u

OPCIONES DE EXCLUSIÓN

OPCIÓN	DESCRIPCIÓN	VALOR DEFECTO
exclude_users	Ubicación del archivo donde se pueden indicar usuarios que serán excluidos de los informes generados por **SARG**	/etc/sarg/exclude_users
exclude_host	Ubicación del archivo donde se pueden indicar hosts que serán excluidos de los informes generados por **SARG**	/ect/sarg/exclude_hosts

Ejemplo. Instalación **SARG**

1. Instalamos y modificamos las opciones que creamos convenientes
2. Creamos el fichero de configuración en el servidor web **APACHE**

```
sudo gedit /etc/apache2/conf.d/sarg.conf

#CONFIGURACIÓN SARG
Alias /sarg /var/lib/sarg

sudo service apache2 restart
```

3. Lanzamos **SARG**

```
sudo sarg
```

PROXY SERVER SQUID

Ejercicios.

1. Configurar **SQUID** de forma que
   Existe un usuario *administrador* al que no se le aplica ningún tipo de restricción
   Para todos los demás usuarios de la red *192.168.1.*
   - No se podrá acceder a páginas deportivas salvo en la hora de descanso que comprende desde las 11:00 a las 11:45
   - No se podrá acceder a redes sociales
   - No se podrá acceder a páginas de contenido exotérico
   - No se podrán visualizar archivos de imágenes
   - No se podrán visualizar archivos multimedia
   - Se establecerá un horario de acceso a internet de lunes a viernes de 08:30 a 14:00 y de 15:30 a 20:00

2. Configurar **SQUID** de forma que permita solo el acceso a la página web *www.as.com* de 08:00 a 14:00 y a la página web *www.marca.com* de 16:00 a 20:00 de lunes a viernes

3. Asegurar el acceso a internet mediante dos usuarios *squid* y *squidbis* y añadiendo dos filtros de **SQUIDGUARD** redirigiendo los accesos a *www.megaupload.com*

4. Redirigir los accesos a páginas deportivas a la página web *www.as.com* mediante una regla **SQUIDGUARD**

5. Configurar **SQUID** para que cumpla
   - Se permita el acceso a internet todos los días de la semana de 08:00 a 12:00 a dos ordenadores de la red 192.168.1.
   - Se permita el acceso a internet todos los días de la semana de 12:30 a 18:00 a dos ordenadores de la red 192.168.1. distintos a los anteriores
   - Se permita el acceso sin restricciones desde *localhost* pero teniendo que introducir un usuario
   - Se prohíba el acceso a páginas web que contengan las palabras *casillas*, *sergio ramos* y *arbeloa*

6. Asegurar los informes generados por **SARG** permitiendo solamente el acceso desde *localhost* y habilitando el acceso mediante usuario y contraseña