

# UNIDAD 6

## Servicio proxy

### 1. El servicio proxy

#### 1.1. ¿Qué es el servicio proxy?

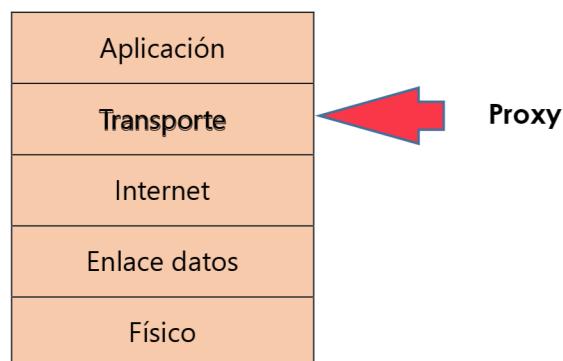
Un proxy es un dispositivo intermediario que puede actuar como un cliente y como un servidor. Acepta peticiones del cliente como si fuera el servidor destino y las reenvía al servidor real, que cree estar comunicándose directamente con el cliente. Después, cuando el servidor entrega la respuesta al proxy, este se encarga de hacérsela llegar al cliente.

Estas son algunas **ventajas** del uso del proxy:

- **Control:** permite limitar las peticiones de los equipos y restringir el acceso a los usuarios.
- **Velocidad:** acelera el acceso a los recursos mediante el uso de la función caché.
- **Filtrado:** emplea políticas de acceso a contenidos específicos como, por ejemplo, bloquear la conexión con determinados sitios web.
- **Seguridad:** mantiene el anonimato de los clientes.

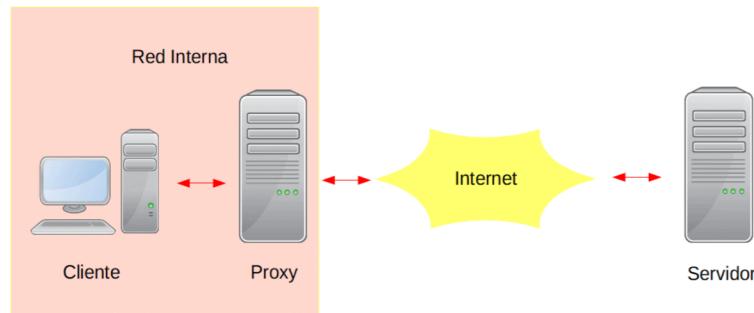
Algunas **desventajas** del uso del proxy son las siguientes:

- Debido a que todas las peticiones pasan a través del proxy y a que puede guardar datos en su memoria secundaria, existe una **possible vulneración de la intimidad del cliente**.
- El acceso a Internet mediante el uso de un proxy **dificulta la realización de operaciones avanzadas** a través de algunos puertos y protocolos.



Proxy en el modelo TCP/IP

Niveles modelo TCP/IP	
Aplicación	Transporte
Proxy	TCP(3128, 8080)

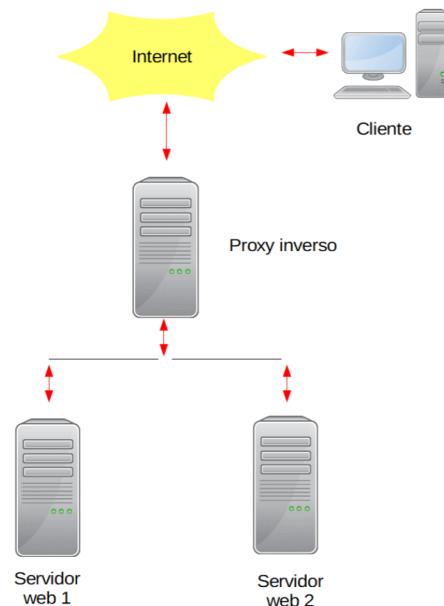


## 1.2. Funciones del servicio proxy

### Pasarela

Se denomina pasarela a la función del proxy que permite comunicar al cliente con el servidor. Esta comunicación se puede llevar a cabo de dos formas:

- *Forward proxy* o proxy de reenvío: es la función más común en un servidor proxy. Permite comunicar a un cliente situado en una red interna con Internet. El servidor recibe la petición del cliente y la comprueba. Si la petición no es válida, la rechaza y, en caso contrario, la tramita.
- *Reverse proxy* o proxy inverso: es un proxy situado en el lado del servidor. De esta manera, uno o varios servidores web podrían proporcionar contenidos de forma transparente al cliente.



#### Advertencia

Un servidor proxy caché puede ofrecer información desactualizada si se han realizado cambios en los datos del servidor original desde que se consultó por última vez.

#### Caché en cliente y en servidor

En el protocolo HTTP, además del proxy, tanto el cliente como el servidor suelen disponer de una caché. Respecto al primero, logra que la carga de páginas web sea casi inmediata y reduce el tráfico de la red, mientras que respecto al segundo mejora el rendimiento del sitio web.

Como podemos ver en la figura anterior existen tres servidores en la red interna, pero solo uno está disponible para acceder a él desde Internet mediante una IP pública relacionada con un nombre de dominio. Si queremos que los clientes también puedan alcanzar los recursos de los otros dos servidores, que solo son accesibles desde la red interna, debemos configurar el primer servidor como proxy inverso. De este modo, los contenidos de los otros servidores estarán disponibles a través del dominio contratado.

### Caché

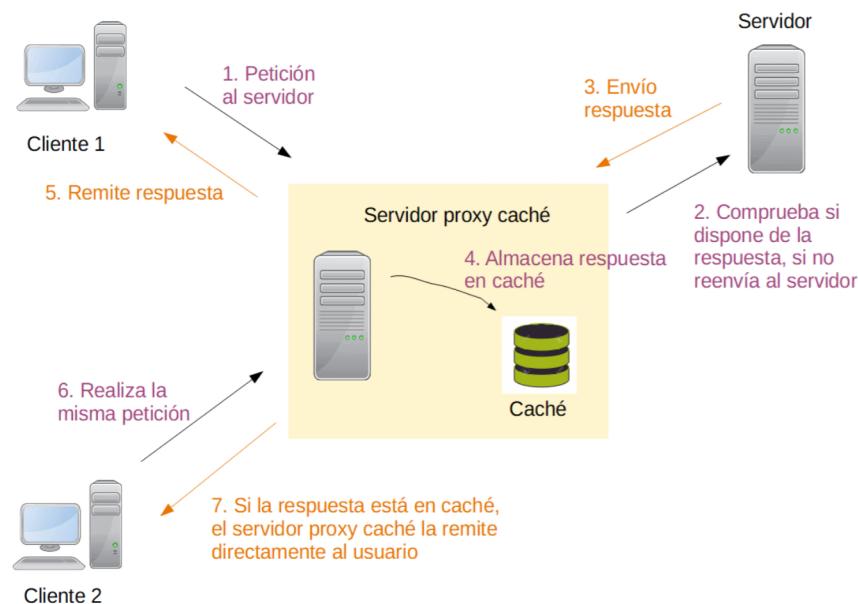
Normalmente, en redes del tipo TCP/IP, múltiples usuarios acceden a la misma información. Esto tiene dos inconvenientes:

- Saturación de los servidores de red.
- Desaprovechamiento del ancho de banda.

Para resolverlos, se utiliza una caché o memoria local que almacena de manera temporal las distintas respuestas que devuelven los servidores a las consultas que realizan los clientes para poder utilizarlas en un futuro cercano.

Cuando un servidor proxy implementa la gestión de esa memoria local, se dice que actúa como servidor proxy caché. Los protocolos que suelen emplearlo son HTTP, FTP, SSL y SOCKS.

En la siguiente figura se puede apreciar el funcionamiento de un servidor proxy caché.



### Filtrado

Otra de las funciones importantes de un proxy es la poder interpretar e inspeccionar los mensajes que circulan entre las aplicaciones situadas entre el cliente y el servidor. De esta manera, el proxy puede analizar el significado del protocolo que emplea una aplicación concreta, lo que le permite:

- Evitar abusos por parte de alguna aplicación no permitida.
- Limitar el uso de determinadas características de un protocolo.
- Detectar si un protocolo no autorizado utiliza puertos estándar.

Por ejemplo, un proxy puede impedir el acceso de determinados usuarios al servidor. También puede prevenir que un protocolo como FTP ejecute un conjunto de comandos o incluso establecer filtros para direcciones URL concretas cuando se emplea el protocolo HTTP.

Esto se consigue mediante reglas explícitas que indican si se aceptan o se rechazan determinados usos.

El inconveniente principal es que, al ser un filtro a nivel de aplicación, el proxy debe ser configurado para cada servicio de red.

A los proxy que realizan estas tareas también se les conoce con el nombre de **cortafuegos a nivel de aplicación**.

#### **Directivas de acceso**

El proxy de Microsoft Forefront Threat Management Gateway (TMG) llama **directivas de acceso** a las reglas utilizadas para filtrar el tráfico de la red, mientras que el proxy más empleado en GNU/Linux, Squid, las denomina **listas de control de acceso** (ACL, del inglés *Access Control List*)

#### **Filtrado de paquetes vs. Filtrado de mensajes a nivel de aplicación**

La diferencia entre el filtrado de mensajes a nivel de aplicación y el filtrado de paquetes en un cortafuegos estriba en que el primero realiza su trabajo en la capa de aplicación y el segundo en la capa de Internet.

### **1.3. Configuraciones proxy**

Un servidor proxy puede configurarse de varias formas para que realice su cometido, según los requerimientos de la utilización que se le quiera dar. Así, entre otras posibilidades, podemos establecer que un proxy sea transparente o anónimo.

#### **Proxy transparente**

Es aquel que no modifica la petición del cliente ni la respuesta del servidor, más allá de lo requerido para la autenticación e identificación.

En general, un cliente debe cambiar su configuración si desea hacer uso de un proxy. Sin embargo, si un proxy se configura de manera transparente, se evita que el cliente deba modificar su configuración y, por tanto, que esta se pueda variar de forma malintencionada.

Para que un proxy sea transparente se debe establecer un mecanismo que capture las peticiones de un cliente a un puerto determinado y las reenvíe hacia el proxy. Por ejemplo, si se trata de un proxy web, debe interceptar las peticiones al puerto 80 y enviárselas al proxy.

#### **Proxy anónimo**

Permite ocultar la dirección IP del cliente mientras navega y que esta no quede registrada en servidores web u otros dispositivos de la red. Para ello, el cliente se conecta a un proxy que se encarga de reenviar las peticiones a los servidores incluyendo su propia dirección IP en vez de la del cliente. Existen multitud de servidores proxy anónimos en la web.

#### **¿Hay intermediarios?**

Si un proxy se configura para que actúe de forma transparente, los clientes pueden no ser conscientes de que están accediendo a Internet a través de un intermediario.

#### **Advertencia**

Pese a emplear un proxy anónimo, la identidad del cliente no se oculta del todo, dado que las peticiones a nuestro ISP son totalmente visibles. Además, los servidores proxy también registran en sus bitácoras los accesos realizados.

## 2. Proxy en sistemas GNU/Linux

La empresa CieloAzul, en esta ocasión, os plantea la implantación de un servicio que permita, además de la racionalización del empleo de la línea de Internet, el control del uso que sus trabajadores hacen de ella. Así, se pretende:

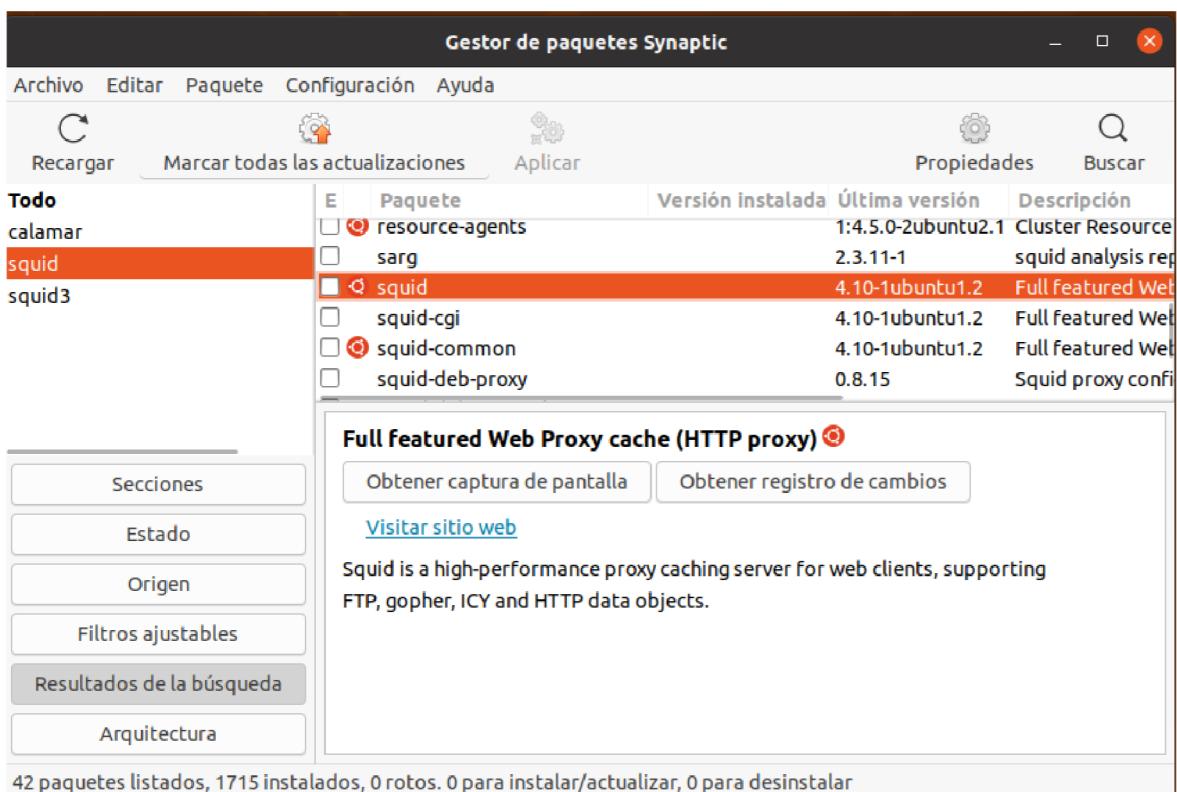
- Aumentar la productividad de sus empleados gracias a las restricciones en el acceso a Internet.
- Si en un futuro se detecta la sobrecarga de la línea de Internet, poder agilizar las comunicaciones reduciendo el tráfico que circula a través del router.

Consideráis que la instalación de Squid satisfará las necesidades de la empresa. Squid, publicado bajo la licencia GNU GPL, es un proxy que, entre otras características, ofrece reducción de ancho de banda utilizando, caché para HTTP, HTTPS y FTP, filtrado y control de acceso.

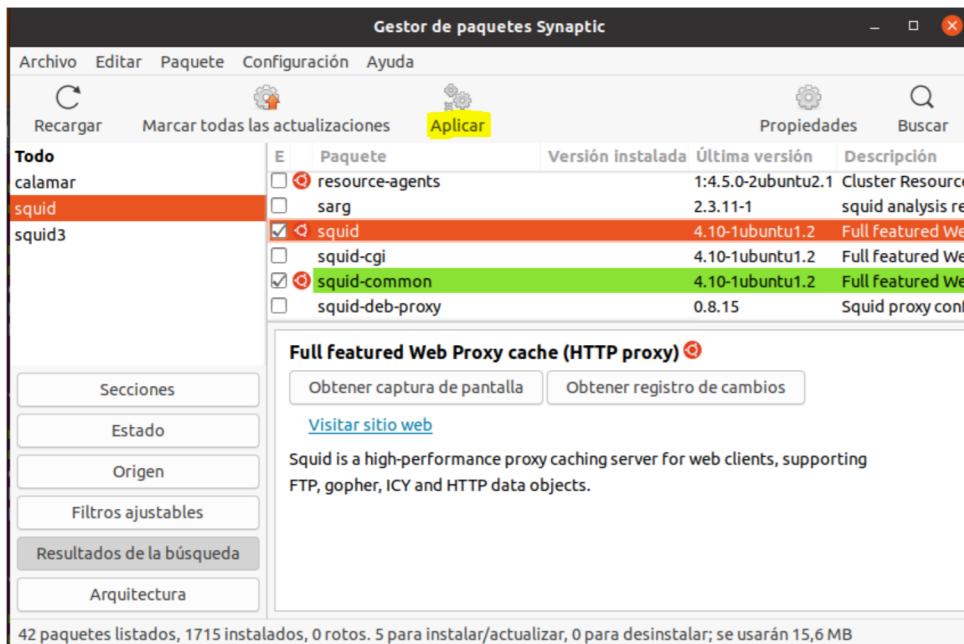
### 2.1. Instalación del servidor

Sigue estas indicaciones para instalar el proxy:

1. Abre el gestor de paquetes Synaptic en el servidor.
2. Haz clic en el botón *Recargar* para actualizar la lista de paquetes disponibles en los repositorios de Internet (debemos asegurarnos tener salida a internet, para ello probaremos con el comando ping 8.8.8.8, además nos conectaremos a los datos móviles para que el firewall del centro no nos bloquee las descargas).
3. Accede a la herramienta de búsqueda, escribe *squid* en el cuadro de texto y haz clic sobre el botón “*Buscar*”.



4. Haz doble clic en la casilla de verificación que está delante del paquete squid y haz clic en el botón *Marcar* para permitir la instalación de los paquetes adicionales.
5. Haz clic sobre el botón *Aplicar* para iniciar la instalación.



6. Se abrirá la ventana *Resumen*. Haz clic en el botón *Aplicar* y se abrirá la ventana *Aplicando cambios*. Al finalizar la instalación se cerrará automáticamente para dar paso a la ventana *Cambios aplicados*.
7. Haz clic en el botón *Cerrar* que se encuentra en el cuadro de diálogo *Cambios aplicados*.
8. Haz clic sobre el botón *Cerrar* para finalizar la aplicación de Synaptic.
9. Si por lo contrario preferimos la terminal, ejecutaremos los siguientes comandos:  
`$sudo apt update -> $sudo apt upgrade] -> $sudo apt install squid`

## 2.2. Configuración del servidor

Aunque el servidor proxy tiene muchas funciones, solo vamos a configurar la autenticación básica.

### Acceso al módulo *Squid-Servidor Proxy*

Sigue estas indicaciones para actualizar la lista de servidores de Webmin:

1. Abre el navegador web en el servidor y accede a Webmin.
2. Haz clic sobre el enlace “Reajustar Módulos” (Refresh Module si lo tenemos en inglés) para que Webmin agregue Squid en su menú. Espera unos segundos mientras esta aplicación busca los módulos instalados y actualiza la lista de servidores.

**Archivo de configuración general**  
`/etc/squid/squid.conf`

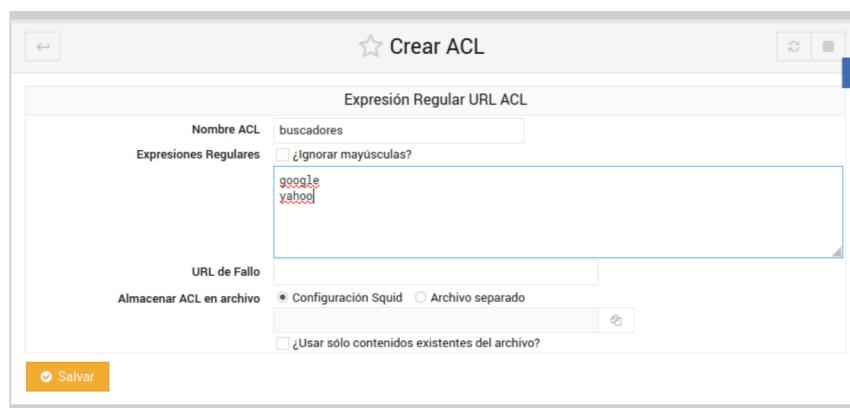
**Archivo usuarios**  
`/etc/webmin/squid/users`

**Archivo de registro de accesos**  
`/var/log/squid/acces.log`

## Definición de una ACL

Una **lista de control de acceso** o ACL (Access Control List) define una condición que se aplicará para permitir o denegar el acceso. Sigue las indicaciones descritas a continuación:

1. Abre Webmin en el servidor y accede al enlace *Squid-Servidor Proxy* de la sección *Servidores* del menú principal.
2. Haz clic en el enlace *Control de Acceso*.
3. Selecciona el valor *Expresiones regular URL* en la lista desplegable, al lado del botón de *Crear nueva ACL*.
4. Haz clic en el botón *Crear nueva ACL*.
5. Escribe *buscadores* en el cuadro de texto *Nombre ACL*.
6. En *Expresiones regulares*, escribimos en una línea google y en la otra yahoo.
7. Haz clic sobre el botón *Guardar* para guardar la nueva ACL.



## Creación de una restricción proxy

Vas a crear una restricción basada en la ACL que has creado en el epígrafe anterior. Luego la colocarás en la posición correcta dentro de la lista de restricciones, de forma que sea evaluada antes de la restricción que deniega todo el tráfico, la cual, por defecto, se sitúa la última. Sigue estos pasos:

1. Abre Webmin en el servidor y accede al enlace *Squid-Servidor Proxy* de la sección *Servidores*.
2. Haz clic en el enlace *Control de Acceso*.
3. Accede a la pestaña *Restricciones Proxy* para configurar una restricción usando la nueva ACL.
4. Haz clic en el enlace *Añadir restricción proxy*.
5. Selecciona la opción *Permitir* del control *Acción* y, a continuación, haz clic sobre *buscadores* de la lista *Coincidir con ACLs*.



6. Haz clic en el botón *Guardar* para guardar la restricción.
7. Para situar la nueva restricción en la posición correcta, haz clic sobre su correspondiente flecha de la columna *Mover*. Vemos que hay una línea que pone "*Denegar all*" (esto significa que bloqueará todas las páginas). La pondremos como ultima para que la regla de permitir a los buscadores tenga mayor prioridad.

Acción	ACLs	Mover
<input type="checkbox"/> Denegar	!Safe_ports	<span style="color: blue;">▲</span>
<input type="checkbox"/> Denegar	CONNECT_ISSL_ports	<span style="color: blue;">▲</span>
<input type="checkbox"/> Permitir	localhost manager	<span style="color: blue;">▲</span>
<input type="checkbox"/> Denegar	manager	<span style="color: blue;">▲</span>
<input type="checkbox"/> Permitir	localhost	<span style="color: blue;">▲</span>
<input type="checkbox"/> Permitir	buscadores	<span style="color: blue;">▲</span>
<input type="checkbox"/> Denegar	all	<span style="color: blue;">▲</span>

**Añadir restricción proxy**

**Eliminar restricciones seleccionadas**

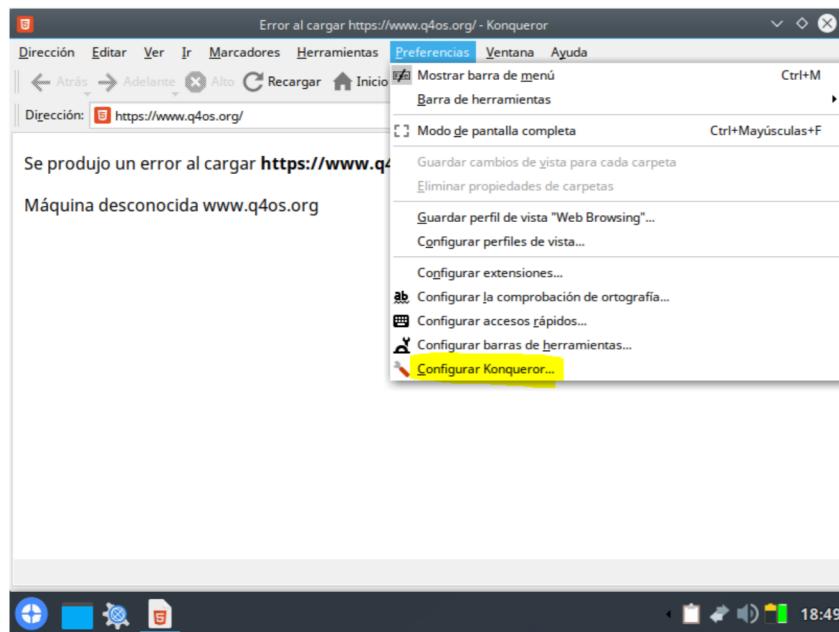
Comprobaremos que se nos queda como en la imagen anterior. Para subir o bajar las restricciones usaremos las flechas laterales.

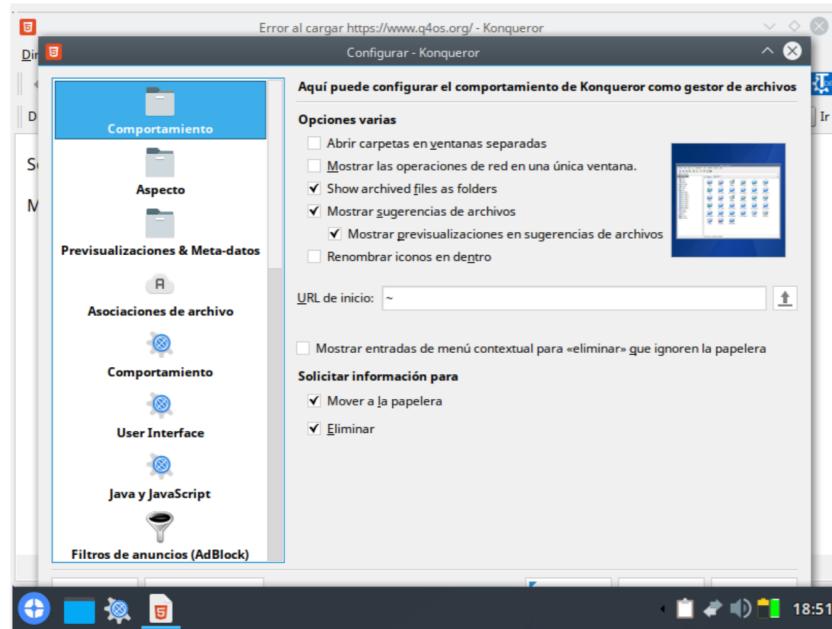
8. Haz clic sobre el enlace *Regresar a índice Squid*. Ten en cuenta que, como siempre, tienes que actualizar los cambios.

## 2.3. Configuración del cliente

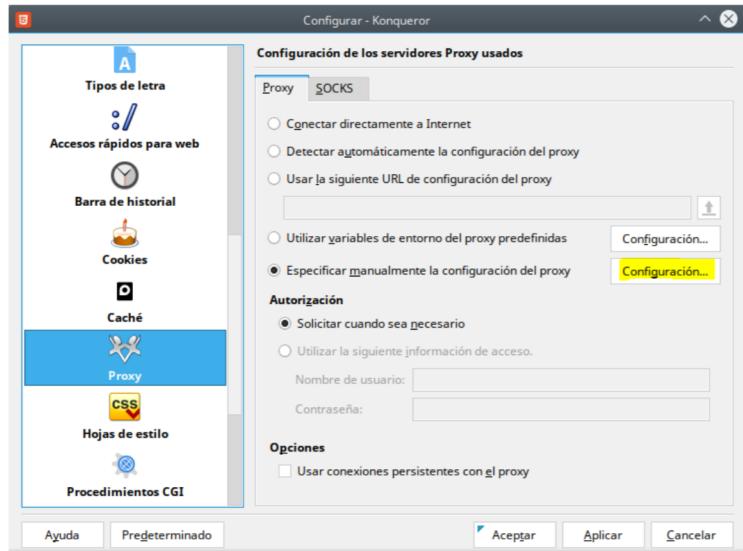
Sigue estos pasos para poder navegar a través del servidor proxy:

1. Arranca el cliente y abre la sesión.
2. Abre el navegador web.
3. Elige en el menú *Prefeencias-Configurar Konqueror...*

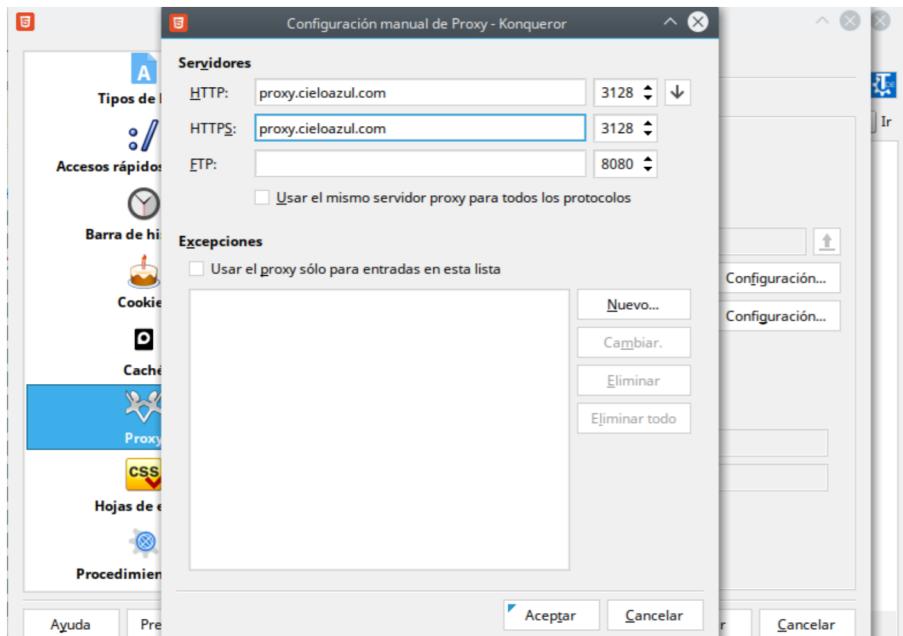




4. En el panel lateral de la izquierda bajaremos y buscaremos y haremos clic en el ícono que ponga *proxy*.
5. Marca el botón *Especificar manualmente la configuración del proxy* y entra en la configuración.



6. Pon como servidores HTTP y HTTPS la dirección *192.168.10.2* y el puerto *3128* (si tienes instalado y operativo el servidor DNS podrás poner *proxy.cieloazul.com* en lugar de la dirección IP, pero ten en cuenta que debes tener ese registro añadido).
7. Acepta todo y aplica los cambios (realizaremos los mismos pasos con todos los clientes).



## 2.4. Comprobaciones

### Comprobación del estado del servicio

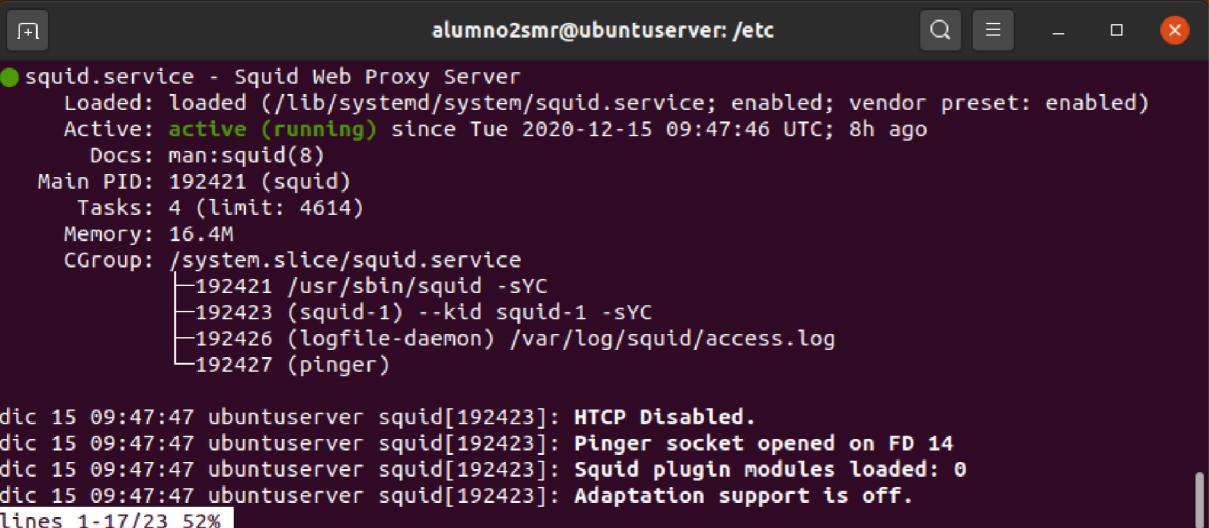
Sigue estos pasos para asegurarte de que el servidor está en ejecución:

1. Abre Webmin en el navegador web del servidor, despliega el menú *Herramientas* y haz clic sobre el enlace *Estado de sistema y de servidor*.
2. Busca *Squid Proxy Server* y comprueba que, a su derecha, hay un símbolo de color verde que indica que está arrancado.

Monitorizando	En host	Estado	Monitorizando	En host	Estado
<input type="checkbox"/> Servidor ProFTP	Local	✓	<input type="checkbox"/> Squid Proxy Server	Local	✓
<input type="checkbox"/> NFS Server	Local	✗	<input type="checkbox"/> MySQL Database Server	Local	—
<input type="checkbox"/> QMail Server	Local	—	<input type="checkbox"/> Internet and RPC Server	Local	—
<input type="checkbox"/> Samba Servers	Local	—	<input type="checkbox"/> Apache Webserver	Local	✓
<input type="checkbox"/> Sendmail Server	Local	—	<input type="checkbox"/> Extended Internet Server	Local	—
<input type="checkbox"/> BIND DNS Server	Local	✓	<input type="checkbox"/> Postfix Server	Local	—
<input type="checkbox"/> DHCP Server	Local	✗	<input type="checkbox"/> PostgreSQL Database Server	Local	—

Seleccionar todo    Invertir selección  
 Borrar Seleccionados    Actualizar seleccionado

Para comprobarlo desde la terminal, ejecutamos `$sudo service squid status`



```

● squid.service - Squid Web Proxy Server
   Loaded: loaded (/lib/systemd/system/squid.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2020-12-15 09:47:46 UTC; 8h ago
     Docs: man:squid(8)
     Main PID: 192421 (squid)
        Tasks: 4 (limit: 4614)
       Memory: 16.4M
      CGroup: /system.slice/squid.service
              └─192421 /usr/sbin/squid -sYC
                  ├─192423 (squid-1) --kid squid-1 -sYC
                  ├─192426 (logfile-daemon) /var/log/squid/access.log
                  └─192427 (pinger)

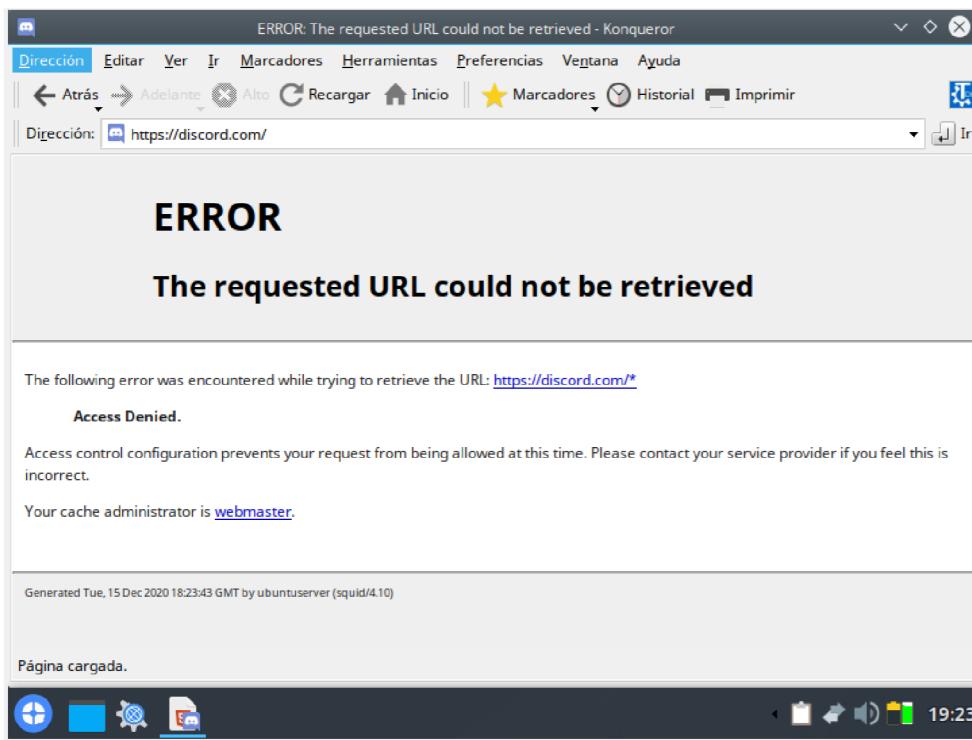
dic 15 09:47:47 ubuntuserver squid[192423]: HTCP Disabled.
dic 15 09:47:47 ubuntuserver squid[192423]: Pinger socket opened on FD 14
dic 15 09:47:47 ubuntuserver squid[192423]: Squid plugin modules loaded: 0
dic 15 09:47:47 ubuntuserver squid[192423]: Adaptation support is off.
lines 1-17/23 52%

```

## Verificación de la navegación web

Sigue los siguientes pasos para comprobar que funciona el servidor proxy:

1. Arranca el cliente y abre una sesión.
2. Abre el navegador.
3. Si entramos en la página [www.google.es](https://www.google.es) nos debería resolver y mostrar la página (ya que en nuestra configuración hemos denegado todo menos la ACL "buscadores").
4. Sin embargo, a la hora de entrar en cualquier otra página nos debería dar error y aparecer una página como esta.



Debéis de tener en cuenta que con esta ACL le hemos dicho al *proxy* que sólo entre en las páginas de Google y de Yahoo, y sabemos que la página de Yahoo la tiene capada el cortafuegos del instituto. Si no estáis seguros de que os funciona el *proxy* podéis permitir todo, ya que por defecto está puesto que no deje salida a nada, y luego ir aplicando restricciones.

¿Cómo podemos permitir todo? Es muy sencillo. Nos vamos a las *Listas de control de Acceso* y hay una pestaña al lado que se llama *Restricciones Proxy*. Vemos que aparece una lista con acciones y ACLs. La última es *Denegar all*. Vamos a moverla hacia arriba del todo con las flechas que tenemos a la derecha, y el *Denegar* lo vamos a cambiar a *Permitir*. Como las ACLs se van aplicando en orden, va a ser la que se va a aplicar, puesto que es la primera. Ahora puedes comprobar en un cliente si tienes salida a Internet si has hecho todo bien.

También te puede ayudar mirar el fichero (con *cat* pues es sólo mirar, no editar) que tiene el registro de accesos *access.log*. En él puedes ver si el *proxy* ha funcionado y el mensaje que se ha almacenado.

## Caso práctico 1

**Objetivo:** mostrar el funcionamiento del servidor proxy.

**Descripción:** vas a crear una ACL (Lista de Control de Acceso) para impedir el acceso a las páginas deportivas de los periódicos (*marca, sport*). La ACL se llamará *nodeportivos*. Se podrá comprobar con cualquier cliente, que permitirá navegar por todo Internet menos esas dos páginas.

**Peso de la nota:** 20% de la nota del tema.

**Se evaluará:**

- Funcionamiento de la práctica (5 puntos).
- Conocimiento de los cambios realizados en el servidor para el correcto funcionamiento (3 p.).
- Integración con el servidor DNS (2 puntos).

## Caso práctico 2

**Objetivo:** mostrar el funcionamiento del servidor proxy con IPs.

**Descripción:** vas a crear una ACL (Lista de Control de Acceso), o varias, para impedir el acceso a las máquinas con IP 192.168.10.11, 192.168.10.12, y con otra restricción que tú decidas. La ACL se llamará *muyrestrictiva* (si utilizas dos ACL se llamarán *muyrestrictiva1* y *muy restrictiva2*).

**Pista:** al poner la máscara de red al hacer una ACL, se pone la inversa.

**Peso de la nota:** 20% de la nota del tema.

**Se evaluará:**

- Funcionamiento de la práctica (5 puntos).
- Conocimiento de los cambios realizados en el servidor para el correcto funcionamiento (3 puntos).
- Originalidad de las restricciones (2 puntos).

**Nota aclaratoria:** para evitar que varios hagáis la misma práctica, tienes que enviarme como comentario las restricciones que va a hacer tu práctica cuando lo hayas decidido, y que no coincida con ninguna de otro alumno.

## Caso práctico 3

**Objetivo:** mostrar el funcionamiento del servidor proxy con restricción horaria.

**Descripción:** vas a crear una ACL, o varias, para impedir el acceso a las máquinas entre las 10:00 y las 10:30, por ser la hora del bocadillo, y otra restricción que se te ocurra. La ACL se llamará *horario* (si son necesarias varias ACL se llamarán *horario1* y *horario2*). Además, cuando no deje navegar pondrá el mensaje "*Ha saltado el proxy del servidor*" como mensaje de error, y una imagen.

**Peso de la nota:** 20% de la nota del tema.

**Se evaluará:**

- Funcionamiento de la práctica (5 puntos).
- Conocimiento de los cambios realizados en el servidor para el correcto funcionamiento (3 puntos).
- Originalidad de las restricciones (2 puntos).

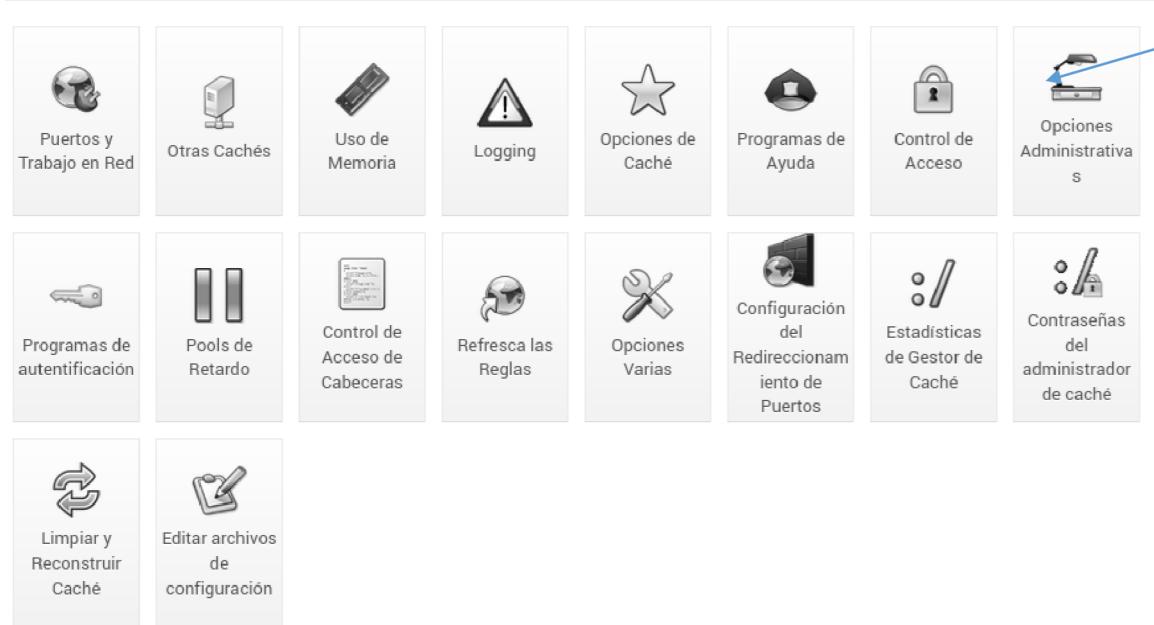
**Nota aclaratoria:** para evitar que varios hagáis la misma práctica, tienes que enviarme como comentario las restricciones que va a hacer tu práctica cuando lo hayas decidido, y que no coincida con ninguna de otro alumno.

## Para más conocimiento

### Añadir información en la página de error

Para hacer más descriptivo el mensaje de error que obtenga el cliente cuando intente acceder a una página restringida haremos lo siguiente:

1. Dentro del menú principal de opciones de *squid*, haremos clic en "Opciones Administrativas"



2. Dentro, modificaremos los campos de tal manera que quede como en la foto

Opciones Administrativas y de Anuncio			
Ejecutar como usuario Unix	<input checked="" type="radio"/> Sin cambios <input type="radio"/>	Ejecutar como grupo Unix	<input checked="" type="radio"/> Sin cambios <input type="radio"/>
Dirección e-mail del gestor de caché	<input type="radio"/> Por defecto <input checked="" type="radio"/> admin.cieloazul.com		
Nombre de máquina visible	<input type="radio"/> Automático <input checked="" type="radio"/> Ubuntuserver		
Nombre de máquina única	<input checked="" type="radio"/> Automático <input type="radio"/>		
Otros nombres de caché DNS	<input checked="" type="radio"/> Ninguno <input type="radio"/>		
Máquina de anuncio de caché	<input checked="" type="radio"/> Por defecto <input type="radio"/>	Puerto de anuncio de caché	<input checked="" type="radio"/> Por defecto <input type="radio"/>
Archivo de anuncio de caché	<input checked="" type="radio"/> Ninguno <input type="radio"/>		
Período de Anunciación	<input checked="" type="radio"/> Por defecto <input type="radio"/>	segundos	<input type="button" value=""/>
<input checked="" type="checkbox"/> Salvar			



Actualizamos la página para comprobar los cambios.

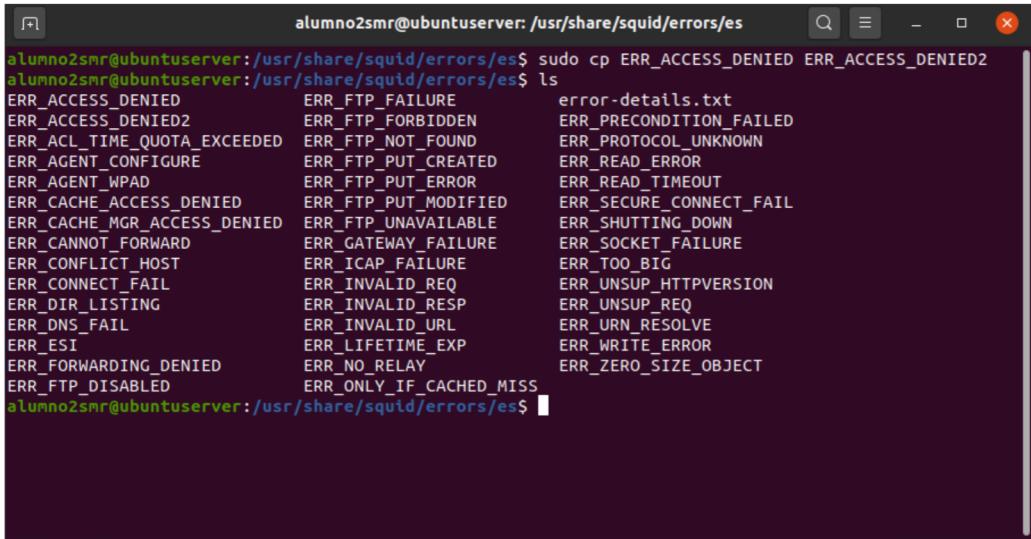
## Cambiar la página que el cliente ve cuando se le deniega el acceso

Las páginas de error predeterminadas se encuentran en la ruta `/usr/share/squid/errors/es`. Entonces, si lo que queremos es mostrarle al cliente una página diferente, haremos lo siguiente:

1. Abriremos una terminal y entraremos al directorio indicado anteriormente con el comando `cd`(change directory), usaremos `ls` para listar todos los códigos de error.

```
alumno2smr@ubuntuserver:~$ cd /usr/share/squid/errors/es
alumno2smr@ubuntuserver:/usr/share/squid/errors/es$ ls
ERR_ACCESS_DENIED           ERR_FTP_FORBIDDEN          ERR_PRECONDITION_FAILED
ERR_ACL_TIME_QUOTA_EXCEEDED ERR_FTP_NOT_FOUND         ERR_PROTOCOL_UNKNOWN
ERR_AGENT_CONFIGURE          ERR_FTP_PUT_CREATED        ERR_READ_ERROR
ERR_AGENT_WPAD               ERR_FTP_PUT_ERROR          ERR_READ_TIMEOUT
ERR_CACHE_ACCESS_DENIED      ERR_FTP_PUT_MODIFIED       ERR_SECURE_CONNECT_FAIL
ERR_CACHE_MGR_ACCESS_DENIED  ERR_FTP_UNAVAILABLE        ERR_SHUTTING_DOWN
ERR_CANNOT_FORWARD           ERR_GATEWAY_FAILURE        ERR_SOCKET_FAILURE
ERR_CONFLICT_HOST            ERR_ICAP_FAILURE           ERR_TOO_BIG
ERR_CONNECT_FAIL              ERR_INVALID_REQ           ERR_UNSUP_HTTPVERSION
ERR_DIR_LISTING               ERR_INVALID_RESP          ERR_UNSUP_REQ
ERR_DNS_FAIL                  ERR_INVALID_URL           ERR_URN_RESOLVE
ERR_ESI                       ERR_LIFETIME_EXP          ERR_WRITE_ERROR
ERR_FORWARDING_DENIED        ERR_NO_RELAY             ERR_ZERO_SIZE_OBJECT
ERR_FTP_DISABLED              ERR_ONLY_IF_CACHED_MISS
ERR_FTP_FAILURE               error-details.txt
```

2. El que nos interesa es el primero (ERR\_ACCESS\_DENIED) que es la página mostrada cuando se le restrinja el acceso a un cliente. Para mantener el fichero original, lo copiaremos y le cambiaremos el nombre.



```

alumno2smr@ubuntuserver:/usr/share/squid/errors/es$ sudo cp ERR_ACCESS_DENIED ERR_ACCESS_DENIED2
alumno2smr@ubuntuserver:/usr/share/squid/errors/es$ ls
ERR_ACCESS_DENIED          ERR_FTP_FAILURE           error-details.txt
ERR_ACCESS_DENIED2         ERR_FTP_FORBIDDEN        ERR_PRECONDITION_FAILED
ERR_ACL_QUOTA_EXCEEDED    ERR_FTP_NOT_FOUND        ERR_PROTOCOL_UNKNOWN
ERR_AGENT_CONFIGURE        ERR_FTP_PUT_CREATED      ERR_READ_ERROR
ERR_AGENT_WPAD             ERR_FTP_PUT_ERROR       ERR_READ_TIMEOUT
ERR_CACHE_ACCESS_DENIED    ERR_FTP_PUT_MODIFIED     ERR_SECURE_CONNECT_FAIL
ERR_CACHE_MGR_ACCESS_DENIED ERR_FTP_UNAVAILABLE     ERR_SHUTTING_DOWN
ERR_CANNOT_FORWARD         ERR_GATEWAY_FAILURE     ERR_SOCKET_FAILURE
ERR_CONFLICT_HOST          ERR_ICAP_FAILURE        ERR_TOO_BIG
ERR_CONNECT_FAIL           ERR_INVALID_REQ        ERR_UNSUP_HTTPVERSION
ERR_DIR_LISTING            ERR_INVALID_RESP       ERR_UNSUP_REQ
ERR_DNS_FAIL               ERR_INVALID_URL        ERR_URN_RESOLVE
ERR_ESI                     ERR_LIFETIME_EXP      ERR_WRITE_ERROR
ERR_FORWARDING_DENIED     ERR_NO_RELAY          ERR_ZERO_SIZE_OBJECT
ERR_FTP_DISABLED           ERR_ONLY_IF_CACHED_MISS
alumno2smr@ubuntuserver:/usr/share/squid/errors/es$ 

```

3. Ahora editaremos el original (ERR\_ACCESS\_DENIED) con lo que queremos que vea el usuario, para ello usamos el comando:
- `$sudo nano ERR_ACCESS_DENIED`
4. En mi caso, pondré una imagen de un gato

