

**SEGURIDAD Y ALTA
DISPONIBILIDAD UD-5**

2º ASIR

09/02/2012

VICEN MORALES

INDICE UD-5

Servidores proxy:

- Tipos de «proxy».
- Características.
- Funcionamiento.
- Instalación de servidores «proxy».
- Instalación y configuración de clientes «proxy».
- Configuración del almacenamiento en la caché de un «proxy».
- Configuración de filtros.
- Métodos de autenticación en un «proxy».
- «proxys» inversos.
- «proxys» encadenados.
- Pruebas de funcionamiento. Herramientas gráficas

UD 5: Instalación y configuración de servidores “proxy”

*Servidores proxy:

Un **proxy**, en una red informática, es un programa o dispositivo que realiza una acción en representación de otro, esto es, si una hipotética máquina **A** solicita un recurso a una **C**, lo hará mediante una petición a **B**; **C** entonces no sabrá que la petición procedió originalmente de **A**. Su finalidad más habitual es la de **servidor proxy**, que sirve para interceptar las conexiones de red que un cliente hace a un servidor de destino, por varios motivos posibles como seguridad, rendimiento, anonimato, etc.

Servidor Proxy

Un proxy es un programa o dispositivo que realiza una tarea acceso a Internet en lugar de otro ordenador. Un proxy es un punto intermedio entre un ordenador conectado a Internet y el servidor al que está accediendo. Cuando navegamos a través de un proxy, nosotros en realidad no estamos accediendo directamente al servidor, sino que realizamos una solicitud sobre el proxy y es éste quien se conecta con el servidor que queremos acceder y nos devuelve el resultado de la solicitud.

Ventajas de un servidor Proxy

Un servidor **Proxy** actúa como intermediario entre el programa cliente (Netscape, Mozilla, Internet Explorer...) y el servidor web que contiene la información que queremos obtener. Su función consiste en almacenar páginas de Internet, gráficos, fotos, archivos de música... para que la próxima vez que se pida el mismo objeto no se deba acceder de nuevo al servidor web que lo alojaba, sino que se sirva directamente desde su memoria o lo que es lo mismo desde su caché.

En cuanto a las ventajas, un servidor **Proxy con caché** en principio realiza la misma función que el resto de caches privados como los que utilizan los **navegadores**, pero de manera compartida por un conjunto grande de usuarios que acceden a través de él. Al tratarse de un almacenamiento compartido es más probable que varios usuarios pidan los mismos objetos consiguiéndose de este modo una reducción en los tiempos de espera para el usuario final. Ésta no es la única ventaja de disponer de éste sistema, a continuación se indican otras ventajas a considerar.

Puede **controlar el acceso** a Internet prohibiendo por ejemplo la entrada a determinadas páginas web por su contenido erótico o por cualquier otro motivo, ya que un servidor Proxy puede realizar simplemente la función de pasarela sin realizar caché.

El coste del software y su instalación tienen un **precio prácticamente nulo** para acceder a Internet mediante una sola línea, a diferencia del coste de usar cualquier router.

Un servidor Proxy además también actúa como una barrera (firewall) que **limita el acceso a la red** desde el exterior.

Desventajas de un servidor Proxy

Utilizar un servidor **Proxy-Caché** en principio puede parecer una gran ventaja ya que se disminuye el tiempo de acceso al contenido deseado y además el servidor que aloja el contenido no recibe tantas peticiones, pero no todo son ventajas, a continuación se indican posibles inconvenientes.

Debido a que el funcionamiento de un Proxy no es conocido por todos los usuarios o webmasters, puede suponer un inconveniente al visualizar las páginas ya que éstas pueden **no mostrarse actualizadas** si no entendemos su funcionamiento.

Un diseñador de páginas web puede indicar en el contenido de su web que los navegadores no hagan una caché de sus páginas, pero este método no funciona para un Proxy (a menos que se utilicen lenguajes como PHP).

El hecho de acceder a Internet a través de un Proxy, en vez de mediante conexión directa, **impide realizar operaciones avanzadas** a través de algunos puertos o protocolos, aunque también es cierto que algunas pueden habilitarse tal como veremos más adelante.

Almacenar las páginas y objetos que los usuarios solicitan puede suponer una **violación de la intimidad** para algunas personas, aunque también es cierto que desde el punto de vista de las empresas es una manera de controlar las actividades de sus trabajadores.

Todas las pruebas que se presentan en este manual o han sido realizadas sobre Linux RedHat con una conexión de ADSL y un procesador Pentium con 128MB de RAM.

Configuración e instalación de Squid

Como instalar el servidor Squid



Instalación mediante RPM

La manera más sencilla de instalar el servidor Squid en nuestro sistema, es mediante una versión en RPM ya sea desde el CD de nuestra distribución o desde por ejemplo nuestra sección privada, ninguna versión anterior a la 2.4 STABLE1 se considera apropiada y lógicamente nosotros recomendamos instalar la versión estable más reciente posible.

Para instalar una versión en RPM, simplemente tenemos que ejecutar como usuario root la siguiente orden:

```
rpm -i squid-2.4.STABLE6-6.7.3.i386.rpm
```

(El RPM indicado viene con la distribución de RedHat 7-3 y es el que utilizaremos para realizar esta documentación).

Instalación mediante código fuente

Si no deseamos esperar a que salga la última versión en RPM y queremos instalar Squid desde el código fuente, simplemente tenemos que descargar la versión más actualizada desde www.squid-cache.org y descomprimirla mediante la orden:

```
tar -xzvf squid-2.5.STABLE2.tar.gz
```

Una vez descomprimido el paquete debemos de ejecutar el siguiente script con los siguientes parámetros:

```
./configure --prefix=/usr/local/squid
```

Esta orden permite especificar el directorio donde instalaremos Squid. Una vez realizada esta operación se generan los ficheros Makefiles y librerías necesarias para compilar el código.

Para compilar el código fuente ejecutar la orden `make all` y posteriormente `make install` para instalar el software de Squid en nuestro sistema.

Ejemplo de configuración de sus directivas

En esta sección se muestra un ejemplo de las directivas más importantes que deberían de situarse descomentadas dentro del fichero `squid.conf`, para hacer funcionar el servidor Squid.

#Directivas para Proxy y caché

```
http_port 3128  
cache_mem 16 MB
```

```
cache_dir ufs /var/spool/squid 100 16 256
maximum_object_size 4096 KB
cache_access_log /var/log/squid/access.log
reference_age 1 month
refresh_pattern . 0 20% 4320
ftp_user Carles@mi-dominio.net
ftp_passive on
```

#Directivas para definir listas

```
acl password proxy_auth REQUIRED
acl redlocal src 192.168.0.0/255.255.255.0
acl adult url_regex www.sex microsoft
```

#Mínimas por defecto

```
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/32
acl SSL_ports port 443 563 --> HTTPS, SNEWS
acl Safe_ports port 80 21 443 563 --> HTTP, FTP, HTTPS, SNEWS
acl Safe_ports port 70 210 1025-65535 --> GOPHER, WAIS, Rango puertos
acl Safe_ports port 280 488 --> HTTP-MGMT, GSS-HTTP
acl CONNECT method CONNECT
```

#Directivas para definir reglas sobre las listas

```
http_access allow adult password
http_access allow redlocal
```

#Mínimas por defecto

```
http_access allow manager localhost
http_access deny manager
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access deny all
```

#Otras directivas

```
no_cache deny adult
reply_body_max_size 4096 KB
cache_mgr Carles@mi-dominio.net
authenticate_program /usr/lib/squid/nca_auth /etc/squid/squid-passwd
```

#Directivas para la jerarquía de caches

```
icp_port 3130
cache_peer 192.168.0.84 parent 3128 3130
cache_peer 192.168.0.90 sibling 3128 0
```

En el siguiente apartado se muestra una descripción detallada con ejemplos de cada una de las directivas presentadas y en el orden en que se encuentran en esta página.

Explicación de las directivas

Una vez presentadas las directivas explicaremos su utilidad y funcionamiento para una mayor comprensión de sus posibilidades.

Para el correcto funcionamiento de las directivas, se aconseja descomentarlas situándolas a la izquierda del todo.

http_port (Asignar Puerto)

Permite especificar uno o varios puertos de escucha para el servidor Squid. Sus valores pueden ser: [dirección-IP:]puerto... tal como se muestra a continuación.

```
http_port 3128 80
http_port 192.168.0.87:3128
```

La segunda línea especifica la dirección IP de la máquina donde se encuentra el Proxy. Si queremos que Squid escuche en el puerto 80, debemos de tener en cuenta que los servidores web como Apache utilizan este puerto por defecto y por tanto deberemos de asignarle uno diferente.

cache_mem (Tamaño para la caché en memoria)

Permite indicar la cantidad ideal de memoria RAM como máximo para almacenar caché de objetos en tránsito, objetos Hot y objetos negativamente almacenados en la caché.

Los datos de estos objetos se almacenan en bloques de 4KB. Cache_mem especifica un límite ideal en el tamaño total de bloques acomodados, donde los objetos en tránsito tienen mayor prioridad, es decir que el resto de objetos la podrán usar hasta que sea requerida.

En el supuesto caso que el objeto en tránsito requiera una memoria mayor a la especificada se excederá para satisfacer la petición, a continuación se muestra un ejemplo.

```
cache_mem 16 MB
```

Si el servidor tiene como mínimo 128 MB de RAM es aconsejable indicar este valor.

cache_dir (Tamaño y directorio para la caché física)

Permite indicar la cantidad de memoria física máxima para almacenar caché en el disco duro, es decir cuanto espacio almacenar de objetos de Internet. Sus valores pueden ser: tipo directorio tamaño numero_subdir numero_niveles, tal como se muestra a continuación

```
cache_dir ufs /var/spool/squid 100 16 256
```

El numero 100 corresponde a 100MB como espacio máximo para almacenar caché, el 16 son el numero de subdirectorios que contendrá el directorio principal (en este caso /var/spool/squid) y el 256 significa el numero de niveles para cada subdirectorio. En caso de especificar un tamaño máximo inferior al espacio real disponible, el servidor Squid se bloqueará.

maximum_object_size (Tamaño máximo para cacheados)

Permite especificar en kilobytes el tamaño máximo de los objetos que se pueden cachear, es decir, los objetos más grandes del tamaño indicado no serán cacheados, a continuación se muestra un ejemplo.

```
maximum_object_size 4096 KB
```

En el ejemplo se han indicado 4MB como tamaño máximo de objetos en la caché.

cache_access_log (Log de peticiones y uso de la caché)

Permite definir en que fichero Squid debe guardar una lista de las peticiones que va recibiendo, con la información de la página que se ha consultado y si ésta ha sido facilitada desde la caché o desde el servidor web, a continuación se muestra un ejemplo.

```
cache_access_log /var/log/squid/access.log
```

Squid presenta más directivas para definir donde registrar sus logs, a continuación se muestran las siguientes dos que pueden ser de mayor utilidad.

```
cache_log /var/log/squid/cache.log  
cache_store_log /var/log/squid/store.log
```

reference_age (Tiempo máximo en la caché)

Permite especificar el tiempo máximo que puede permanecer un objeto en la caché sin que se acceda a él, transcurrido ese tiempo será borrado.

Squid el objeto que ha estado mas tiempo sin ser accedido lo calcula dinámicamente con el fin de ser borrado según el espacio disponible en la caché. Sus valores pueden ser: time-units, tal como se muestra a continuación.

```
reference_age 1 year  
reference_age 3.5 days  
referense_age 2 hours
```

refresh_pattern (Factor para páginas sin caducidad)

Permite especificar que fecha en minutos deben de tener los documentos que su servidor no estableció una cabecera Expires indicando su caducidad.

Sus valores pueden ser: expresión_regular mín porcentaje máx, tal como se muestra a continuación.

```
refresh_pattern -i \.gif$ 14400 70% 43200  
refresh_pattern ^ftp: 1440 20% 10080  
refresh_pattern . 0 20% 4320
```

El valor correspondiente a la expresión regular debe de contener la especificación del objeto basándose en la dirección (URL) de la petición o un "." para indicar el resto. En los ejemplos se muestra como especificar cualquier objeto "gif" y cualquier petición "FTP".

El valor mín corresponde a los minutos mínimos que un objeto que no dispone de una cabecera Expires (indicando su caducidad), pueda ser considerado como no caducado (fresco). El valor "0" se recomienda para que no se obligue la retención de objetos no deseados como pueden ser los dinámicos.

El valor porcentaje sirve para especificar en aquellos objetos sin fecha de caducidad, cual será su fecha, aplicando un porcentaje sobre su tiempo desde la última modificación (la última modificación de un objeto se obtiene de la cabecera Last-Modified).

El valor máx corresponde a los minutos máximos que un objeto podrá ser considerado como no caducado.

ftp_user (Acceso anónimo para FTP)

Permite indicar el correo que debe usarse como contraseña para acceder de forma anónima a un servidor FTP. Esto es útil si se desea acceder a servidores que validan la autenticidad de la dirección de correo especificada como contraseña, a continuación se muestra un ejemplo.

```
ftp_user Carles@mi-dominio.net
```

Requerir autenticación por contraseña

Hasta el momento hemos visto mediante las directivas acl y http_access como controlar el acceso según el origen de la petición o según el destino. En este apartado aprovechando también estas directivas mostraremos como conseguir que independientemente de la máquina que se utilice se requiera introducir un nombre de usuario y una contraseña en el cliente para poder acceder a través del Proxy.

1. Crear el fichero que contendrá los usuarios y sus contraseñas de forma encriptada.

```
touch /etc/squid/squid-passwd
```

2. Establecer permisos de lectura y escritura para Squid.
3.

```
chmod 600 /etc/squid/squid-passwd
```

```
chown squid:squid /etc/squid/squid-passwd
```

4. Dar de alta los usuarios con sus contraseñas.

```
htpasswd /etc/squid/squid-passwd nombre_usuario
```

La orden nos pedirá introducir su contraseña correspondiente. El nombre de usuario es lógicamente independiente a los que hay ya definidos en el sistema y la orden htpasswd está disponible en el paquete: apache-1.3.22 o superior.

5. Definir en el fichero squid.conf que programa gestiona las autenticaciones (ver sección: Explicación de las directivas).

```
authenticate_program /usr/lib/squid/ncsa_auth /etc/squid/squid-passwd
```

6. Definir en el fichero squid.conf la lista acl correspondiente.

```
acl password proxy_auth REQUIRED
```

7. Aplicar reglas en el fichero squid.conf para quienes queramos que sean autenticados.

```
acl all src 0.0.0.0/0.0.0.0 --> Todas las IP's posibles
```

```
acl redlocal src 192.168.0.0/24 --> Red correspondiente a 192.168.0.*
```

```
http_access allow redlocal password --> Usuarios con esas IP's autenticarse
```

```
http_access deny all --> Denegamos el acceso a los demás.
```

```
acl all src 0.0.0.0/0.0.0.0 --> Todas las IP's posibles
```

```
acl redlocal src 192.168.0.0/24
```

```
acl adult url_regex www.sex.com erotic
```

```
http_access allow adult password --> Solo acceder a contenido adulto mediante  
previa autenticación.
```

```
http_access allow redlocal --> Permitimos el acceso a las IP's de la red.
```

```
http_access deny all --> Denegamos el acceso a los demás.
```

Una vez hemos configurado nuestro servidor Proxy solo tenemos que realizar una petición a un contenido prohibido y observaremos como nuestro navegador muestra una ventana para que nos autentiquemos.

Configuración e instalación de Apache

Como instalar el servidor Apache-Proxy

Instalación mediante RPM

La manera más sencilla de poner en funcionamiento Apache en nuestro sistema es instalar una versión en RPM ya sea desde el CD de nuestra distribución o desde por ejemplo nuestra zona privada, ninguna versión anterior a la 1.1 es recomendada y nosotros aconsejamos lógicamente obtener la más actualizada posible.

Para instalar una versión en RPM como ya sabemos, simplemente tenemos que ejecutar como usuario root la siguiente orden:

```
rpm -i apache-1.3.27-2.i386.rpm
```

(El RPM indicado viene con la distribución de RedHat 7-3 y es el que utilizaremos para realizar esta documentación).

Una vez instalado nuestro servidor Apache únicamente tenemos que editar el fichero de configuración de Apache llamado httpd.conf (generalmente situado en /etc/httpd/conf/httpd.conf), ya que el módulo para la función de Proxy ya estará compilado y únicamente tendremos que cargarlo.

Para activarlo simplemente descomentar las dos siguientes líneas:

```
#Load Module proxy_module /usr/lib/apache/libproxy.so  
#AddModule mod_proxy.c
```

Una vez descomentadas las dos líneas ya tenemos cargada la funcionalidad de Proxy-Caché y podremos pasar a configurar y utilizar las directivas deseadas.

Instalación mediante código fuente

En caso que ya tengamos una versión de Apache en nuestro sistema y no aparezcan las dos líneas descritas en Instalación mediante RPM, posiblemente no tengamos compilado el módulo para poder utilizar el servidor como Proxy. En este caso deberíamos comprobar si disponemos de la librería libproxy.so en nuestro sistema, si es así, simplemente añadimos las dos líneas que faltan en httpd.conf. En caso de no disponer de la librería, debemos recompilar e instalar el código fuente.

Recomendamos guardar el archivo httpd.conf si deseamos conservar nuestra configuración actual. Una vez estemos seguros que no disponemos de la librería libproxy.so, podemos proceder a la descarga del paquete con el código fuente desde www.apache.org.

Para descomprimir el paquete utilizar la siguiente orden:

```
tar -xvzf apache_1.3.27.tar.gz
```

Una vez descomprimido el paquete debemos de ejecutar el siguiente script con los siguientes parámetros:

```
./configure -prefix=/usr/local/apache
```

Esta orden permite especificar el directorio donde se instalará el servidor apache (deberíamos especificar el mismo que teníamos). Una vez realizado esto se generarán los Makefiles y un nuevo fichero llamado config.status que actúa como script para seguir configurando. Por tanto indicaremos los módulos que queremos instalar que en éste caso serán: el modulo para poder utilizar módulos y el módulo para Proxy, tal como mostramos a continuación:

```
./config.status --active-module=src/modules/standard/mod_so.c  
./config.status -enable-module=proxy
```

Una vez hemos realizados los pasos indicados, simplemente tenemos que compilar el código fuente mediante la orden make all y posteriormente indicar que se instale en el sistema mediante make install.

Ejemplo de configuración de sus directivas

En éste apartado mostramos un pequeño ejemplo de las directivas que deberían de situarse descomentadas dentro del fichero httpd.conf para poder utilizar el servidor Apache como Proxy y como Proxy con caché.

```
<If Module mod_proxy.c>  
#Directivas para realizar función de Proxy  
ProxyRequest On  
Listen 80  
Listen 8087  
AllowCONNECT 443 563 23  
ProxyBlock www.sex.com www.microsoft.com  
#ProxyRemote * http://192.168.0.84:8087  
#NoProxy www.hotmail.com  
#ProxyPass / http://192.168.0.84/  
#ProxyPassReverse / http://192.168.0.84/  
<Directory proxy:*>  
    Order deny, allow  
    Deny from all  
    Allow from .informatica.escoladeltreball.org  
</Directory>  
ProxyVia Full  
  
#Directivas para realizar la función de caché  
CacheRoot "/var/cache/httpd"
```

```
CacheSize 50000
CacheGcInterval 1
CacheMaxExpire 24
CacheLastModifiedFactor 0.1
CacheDefaultExpire 3
CacheForceCompletion 90
#NoCache pc47.informatica.escoladeltreball.org
</IfModule>
```

En el siguiente apartado se describe el significado y la utilidad de las directivas en el orden presentado.

Explicación de las directivas

Una vez presentadas las directivas describiremos su utilidad y funcionamiento para una mayor comprensión de las posibilidades de Apache-Proxy.

ProxyRequest (Activar Proxy)

Esta directiva permite activar o desactivar la función de Proxy. Tener en cuenta que se anularán todas las directivas tanto para funciones de caché como de Proxy, excepto la directiva ProxyPass.

Sus valores pueden ser On u Off tal como se muestra a continuación y solo está disponible en Apache 1.1 y superiores.

```
ProxyRequest On
ProxyRequest Off
```

Listen (Asignar Puerto)

Permite indicar a Apache que escuche peticiones en más de una dirección IP o puerto. Por defecto si no especificamos ninguna IP escucha para todas, pero solo para el puerto indicado.

Sus valores pueden ser [dirección-IP:]puerto tal como se muestra a continuación y solo está disponible en Apache 1.1 y superiores.

```
Listen 8087
Listen 80
Listen 192.168.0.87:8080
```

AllowCONNECT (Permitir método CONNECT)

Permite especificar una lista de puertos a los que el Proxy mediante el método CONNECT quizá conecte.

Sus valores pueden ser port [port]... tal como se muestra a continuación y solo está disponible en Apache 1.3.2 y superiores.

```
AllowCONNECT 443 563 23
```

Son los puertos que utiliza HTTPS, SNEWS y telnet respectivamente.

Un ejemplo práctico

Para probar su funcionamiento utilizaremos el cliente telnet con el fin de realizar una conexión a un host remoto a través del Proxy mediante el protocolo HTTP.

1. Hacemos un telnet al servidor Proxy en el puerto que está escuchando.

```
telnet 192.168.0.87 8087
```

2. Una vez realizada la conexión, el cliente telnet espera que le indiquemos una petición. Conectamos desde el Proxy al ordenador deseado mediante el puerto 23 que utiliza telnet.

```
CONNECT 192.168.0.84:23 http/1.0
```

3. Presionamos la tecla Enter y la sesión telnet se realiza a través del Proxy y lógicamente mantenida por éste ya que si desactivamos Apache con la orden: service httpd stop, la conexión se pierde.

ProxyBlock (Control acceso URL, control según destino)

Bloquea peticiones HTTP, HTTPS y FTP de documentos que contengan en su dirección la palabra, el host o el dominio especificado.

Sus valores pueden ser *|word|host|domain [word|host|domain]... tal como se muestra a continuación y solo está disponible en Apache 1.2 y superiores.

```
ProxyBlock www.sex.com rocky.wotsamattau.edu  
ProxyBlock *
```

Tener en cuenta que especificar la palabra "sex" ya es suficiente para bloquear direcciones como: www.sex.com www.sexista.com http://sexologia.com y que utilizar el "*" significa bloquear todas las peticiones.

Además, esta directiva es muy interesante ya que en caso de enviar las peticiones a un Proxy remoto mediante la directiva ProxyRemote, el bloqueo se continúa realizando y

por tanto se podrían utilizar Proxys para restringir el acceso a determinados usuarios y un Proxy remoto para realizar las peticiones que se hubieran permitido.

ProxyRemote (Desviar a un Proxy, control según destino)

Permite indicar que páginas web serán gestionadas por un servidor Proxy remoto, es decir será el remoto quien realizará la petición al servidor y la cacheará.

Sus valores pueden ser URL `http://hostname[:port]` tal como se muestra a continuación y solo está disponible en Apache 1.1 y superiores.

```
ProxyRemote http://hotmail.com/ http://192.68.0.84:8087
ProxyRemote * http://192.68.0.84:8087
ProxyRemote ftp http://192.68.0.84:8087
```

En la segunda línea se especifica que todas las peticiones de direcciones web las procesará un servidor remoto y en la tercera que todas las peticiones ftp las gestionará un servidor remoto.

NoProxy (No desviar a otro Proxy, control según destino)

Esta directiva hace referencia a la directiva ProxyRemote y permite especificar que peticiones no las ha de enviar al Proxy remoto sino que las tiene que procesar él directamente.

Sus valores pueden ser: `domain|SubRed|IpAddress|Hostname` [`domain|SubRed|IpAddress|Hostname`]..., tal como se muestra a continuación y solo está disponible en Apache 1.3 y superiores.

```
ProxyRemote * http://192.68.0.84:8087
NoProxy .company.com 192.168.112.0/21 www.hotmail.com
```

Los ejemplos mostrados corresponden a un dominio una subred y un hostname.

ProxyPass (Desviar contenidos a un nuevo web server)

Permite al servidor Proxy local actuar como un espejo del servidor que en realidad ahora está sirviendo el contenido. Esta directiva es útil si en un pasado nuestro servidor Apache servía unos documentos web que ahora los sirve otro servidor, ya que no será necesario avisar a la gente del traslado y podrán continuar haciendo la petición al servidor antiguo ya que la directiva redireccionará sin que el usuario se dé cuenta de nada. Además esta directiva sigue funcionando aunque deshabilitemos la función de Proxy.

Sus valores pueden ser: path url, donde "path" es el nombre del antiguo "path virtual local" y "url" es una dirección parcial del servidor remoto, tal como se muestra a continuación y solo está disponible en Apache 1.1 y superiores.

```
ProxyPass /mirror/foo/ http://server2.org/
```

A la práctica si nuestro servidor local tuviera la dirección `http://server.org/` y ya no ofreciera el contenido web, al pedir `http://server.org/mirror/foo/web.html` se redireccionaría la petición a `http://server2.org/web.html`.

Un ejemplo práctico

Tenemos un servidor Apache que ya no contiene documentos, con la dirección IP: 192.168.0.87 y un nuevo servidor Apache con la dirección IP: 192.168.0.84 que se encargará de servir los documentos a partir de ahora. Configuramos en el servidor 192.168.0.87 la directiva de redirección:

```
ProxyPass / http://192.168.0.84/
```

Ahora con el cliente pedimos `http://192.168.0.87/icons/` y recibimos los documentos todo y que ya no los tiene, debido a que automáticamente a realizado la petición a `http://192.168.0.84/icons/`.

Conceptos y trucos para Apache y Squid

Cabeceras HTTP y funcionamiento de la caché

La finalidad de este apartado consiste en explicar como un navegador almacena y consulta las páginas de su caché y como lo hace un servido Proxy, de esta manera podemos presentar como modificar su comportamiento por defecto y averiguar posibles deficiencias. Antes de empezar se muestran algunas de las cabeceras del protocolo HTTP/1.1 que se suelen utilizar en Proxys y navegadores.

Cabeceras del mensaje

Las siguientes cabeceras forman parte del protocolo HTTP/1.1 definidas en el RFC2616, salvo que se indique lo contrario.

Cache-Control

Permite indicar si un elemento puede ser cacheado y su caducidad.

Valor

Significado

| | |
|-----------------|--|
| public | Indica que la respuesta a una petición puede ser ocultada (cacheada) tanto por clientes como por el Proxy. |
| private | Indica que la respuesta no se puede cachear por caches compartidas, es decir, solamente en teoría podría cachearla un cliente. |
| no-cache | No puede cachear el elemento ni el cliente ni el Proxy. |
| max-age | Segundos máximos que se considera un objeto no caducado desde que se realizó su petición. |
| must-revalidate | Obliga a comparar con el servidor web antes de usar el caché. |

Pragma

Corresponde al HTTP/1.0 pero por razones de compatibilidad actualmente se considera soportado aunque solo para peticiones. Su sintaxis es la misma que en Cache-Control.

Via

Usado por Proxys o gateways para indicar el protocolo intermedio entre el cliente y el servidor. Generalmente se suele añadir la maquina y la versión del software del Proxy.

Valor

Significado

- On Mostrará información como el nombre de la máquina del Proxy.
- Off No añade información en la cabecera Via.
- Full Mostrará información como el nombre de la máquina y la versión del software.
- Block Eliminará las líneas en que aparezca la cabecera Via.

Expires

Indica cuando caducará una respuesta dada por el servidor web. El formato de esta cabecera esta definido en el RFC850.

Ejemplo fecha sin caducar --> Sun, 17 Jan 2038 20:14:07 GMT

Ejemplo fecha caducada --> Wed, 26 Feb 2001 08:21:57 GMT

Last-Modified

Indica en una respuesta cuando el servidor considera que se modificó por última vez la página o objeto que proporciona. Si la cabecera Expires no está presente, se toma este valor para determinar la caducidad. Cada Proxy y navegador utiliza su criterio, pero un ejemplo consistiría en que si tenemos un objeto en el caché desde hace 10 días y cuando se introdujo se sabía que había sido modificado 150 días antes, es lógico considerar que todavía no se habrá modificado.

X-Cache

Esta cabecera no pertenece a ningún estándar, la consideramos ya que servidores Proxy como Apache o Squid la añaden para indicar si la página ha sido cogida desde el caché o bien desde el servidor.

| Valor | Significado |
|-------|--|
| MISS | La página no se ha servido desde el caché. |
| HIT | La página se ha servido desde el caché. |

Fichero de auto-configuración para navegadores

El fichero de auto-configuración permite indicar a los navegadores que Proxy deben utilizar para realizar sus peticiones, de esta manera evitamos que el usuario sea el encargado de configurar manualmente su conexión a Internet.

El hecho de utilizar un fichero ya configurado permite además, modificar el puerto y las IP's de los servidores Proxy sin tener que volver a re-configurar todos los navegadores.

Creación del fichero

Para que el fichero pueda ser accesible desde cualquier navegador, podemos almacenarlo en un servidor web, en un directorio de red o en un servidor FTP, a continuación se muestran los pasos para que el navegador pueda acceder a este fichero mediante Apache Web Server.

1. Añadir la siguiente línea en el fichero `/etc/mime.types` que utiliza Apache Web Server para indicar al navegador (mediante la cabecera `Content-Type`), que tipo de fichero está recibiendo.

```
application/x-ns-proxy-autoconfig pac
```

De esta manera indicamos que todos los ficheros `.pac` que sirve Apache se interpreten como ficheros de auto-configuración.

2. Añadir las siguientes líneas en `httpd.conf` para que se pueda acceder al fichero de auto-configuración mediante por ejemplo: `http://host/proxy/proxy.pac`
 3. Alias `/proxy/ /ruta/del/fichero/`
 4. `<Directory /ruta/del/fichero>`
 5. `Options None`
 6. `AllowOverride None`
 7. `Order allow,deny`
 8. `Allow from all`
- ```
</Directory>
```

9. Creamos el fichero proxy.pac con permisos de lectura para todos.
10. touch /ruta/del/fichero/proxy.pac  
chmod 644 /ruta/del/fichero/proxy.pac

### Configuración del fichero

El fichero proxy.pac que hemos creado en la sección anterior debe de ser escrito en JavaScript y presentar como "main" la función FindProxyForURL(url, host), la cual recibe del navegador los dos argumentos especificados y devuelve a éste un valor que le indica como debe de actuar, los valores de retorno posibles se describen a continuación.

```
DIRECT
PROXY host:port
```

### Ejemplo

```
return "PROXY 192.168.0.87:3128";
```

A continuación, presentamos un ejemplo del código que debe de tener el fichero de auto-configuración para que sea interpretado por los navegadores.

```
function FindProxyForURL(url, host)
{
<!-- Establecemos No Proxy for: -->
if (shExpMatch(url, "*.tu-dominio.org"))
 return "DIRECT";
<!-- Una red utiliza un Proxy -->
else if (isInNet(myIpAddress(), "192.168.0.0", "255.255.255.0"))
 return "PROXY 192.168.0.87:3128";
<!-- El resto utiliza otro Proxy -->
else
 return "PROXY 192.168.0.87:8087";
}
```

### Configuración de los clientes

El código del fichero de auto-configuración que hemos presentado es válido para navegadores como Mozilla y Netscape, donde funciona correctamente.

1. Seleccionar en el menú de Mozilla y Netscape: Edit - Preferences - Advanced - Proxies

En caso de Internet Explorer seleccionar: Herramientas - Opciones de Internet - Conexiones - Configuración de LAN

2. Introducir la siguiente línea en la opción:

Automatic proxy configuration URL --> En Mozilla y Netscape

Usar secuencia de comandos de configuración automática --> En Internet Explorer

`http://host/proxy/proxy.pac`

3. Presionar la tecla Reload para activar los cambios en Mozilla y Netscape o reiniciar el navegador para que se lea el fichero en caso de Internet Explorer.

## \* Tipos de «proxy».

- 1) Transparente: revela todos tus datos, solamente se utiliza para mejorar la velocidad de descarga.
- 2) Anónimo: No envía ninguna variable mostrando tu IP, pero si avisa que estas utilizando un proxy.
- 3) Muy Anónimo: No envían ninguna variable de ningún tipo a nadie.

### Proxies transparentes

Muchas organizaciones (incluyendo empresas, colegios y familias) usan los proxies para reforzar las políticas de uso de la red o para proporcionar seguridad y servicios de caché. Normalmente, un proxy Web o NAT no es transparente a la aplicación cliente: debe ser configurada para usar el proxy, manualmente. Por lo tanto, el usuario puede evadir el proxy cambiando simplemente la configuración. Una ventaja de tal es que se puede usar para redes de empresa.

Un **proxy transparente** combina un servidor proxy con NAT (Network Address Translation) de manera que las conexiones son enrutadas dentro del proxy sin configuración por parte del cliente, y habitualmente sin que el propio cliente conozca de su existencia. Este es el tipo de proxy que utilizan los proveedores de servicios de internet (ISP).

### Reverse Proxy / Proxy inverso

Un *reverse proxy* es un servidor proxy instalado en el domicilio de uno o más servidores web. Todo el tráfico entrante de Internet y con el destino de uno de esos servidores web pasa a través del servidor proxy. Hay varias razones para instalar un "reverse proxy":

- Seguridad: el servidor proxy es una capa adicional de defensa y por lo tanto protege los servidores web.
- Cifrado / Aceleración SSL: cuando se crea un sitio web seguro, habitualmente el cifrado SSL no lo hace el mismo servidor web, sino que es realizado por el "reverse proxy", el cual está equipado con un hardware de aceleración SSL (Security Sockets Layer).
- Distribución de Carga: el "reverse proxy" puede distribuir la carga entre varios servidores web. En ese caso, el "reverse proxy" puede necesitar reescribir las URL de cada página web (traducción de la URL externa a la URL interna correspondiente, según en qué servidor se encuentre la información solicitada).
- Caché de contenido estático: Un "reverse proxy" puede descargar los servidores web almacenando contenido estático como imágenes u otro contenido gráfico.

### Proxy NAT (Network Address Translation) / Enmascaramiento

Otro mecanismo para hacer de intermediario en una red es el NAT.

La traducción de direcciones de red (NAT, Network Address Translation) también es conocida como enmascaramiento de IPs. Es una técnica mediante la cual las direcciones fuente o destino de los paquetes IP son reescritas, sustituidas por otras (de ahí el "enmascaramiento").

Esto es lo que ocurre cuando varios usuarios comparten una única conexión a Internet. Se dispone de una única dirección IP pública, que tiene que ser compartida. Dentro de la red de área local (LAN) los equipos emplean direcciones IP reservadas para uso privado y será el proxy el encargado de traducir las direcciones privadas a esa única dirección pública para realizar las peticiones, así como de distribuir las páginas recibidas a aquel usuario interno que la solicitó. Estas direcciones privadas se suelen elegir en rangos prohibidos para su uso en Internet como 192.168.x.x, 10.x.x.x, 172.16.x.x y 172.31.x.x

Esta situación es muy común en empresas y domicilios con varios ordenadores en red y un acceso externo a Internet. El acceso a Internet mediante NAT proporciona una cierta seguridad, puesto que en realidad no hay conexión directa entre el exterior y la red privada, y así nuestros equipos no están expuestos a ataques directos desde el exterior.

Mediante NAT también se puede permitir un acceso limitado desde el exterior, y hacer que las peticiones que llegan al proxy sean dirigidas a una máquina concreta que haya sido determinada para tal fin en el propio proxy.

La función de NAT reside en los Cortafuegos y resulta muy cómoda porque no necesita de ninguna configuración especial en los equipos de la red privada que pueden acceder a través de él como si fuera un mero encaminador..

### **Proxy abierto**

Este tipo de proxy es el que acepta peticiones desde cualquier ordenador, esté o no conectado a su red.

En esta configuración el proxy ejecutará cualquier petición de cualquier ordenador que pueda conectarse a él, realizándola como si fuera una petición del proxy. Por lo que permite que este tipo de proxy se use como pasarela para el envío masivo de correos de spam. Un proxy se usa, normalmente, para almacenar y redirigir servicios como el DNS o la navegación Web, mediante el cacheo de peticiones en el servidor proxy, lo que mejora la velocidad general de los usuarios. Este uso es muy beneficioso, pero al aplicarle una configuración "abierto" a todo internet, se convierte en una herramienta para su uso indebido.

Debido a lo anterior, muchos servidores, como los de IRC, o correo electrónicos, deniegan el acceso a estos proxys a sus servicios, usando normalmente listas negras ("BlackList").

### Cross-Domain Proxy

Típicamente usado por Tecnologías web asíncronas (flash, ajax, comet, etc) que tienen restricciones para establecer una comunicación entre elementos localizados en distintos dominios.

En el caso de Ajax, por seguridad sólo se permite acceder al mismo dominio origen de la página web que realiza la petición. Si se necesita acceder a otros servicios localizados en otros dominios, se instala un **Cross-Domain proxy**<sup>2</sup> en el dominio origen que recibe las peticiones ajax y las reenvía a los dominios externos.

En el caso de flash, también han solucionado creando la revisión de archivos xml de Cross-Domain, que permiten o no el acceso a ese dominio o subdominio.

## \*Características.

La palabra **proxy** se usa en situaciones en donde tiene sentido un unos algunos *intermediario*.

- El uso más común es el de **servidor proxy**, que es un ordenador que intercepta las conexiones de red que un cliente hace a un servidor de destino.
  - De ellos, el más famoso es el **servidor proxy web** (comúnmente conocido solamente como «**proxy**»). Intercepta la navegación de los clientes por páginas web, por varios motivos posibles: seguridad, rendimiento, anonimato, etc.
  - También existen proxies para otros protocolos, como el **proxy de FTP**.
  - El proxy ARP puede hacer de enrutador en una red, ya que hace de intermediario entre ordenadores.
- Proxy (patrón de diseño) también es un patrón de diseño (programación) con el mismo esquema que el proxy de red.
- Un componente hardware también puede actuar como intermediario para otros.

Como se ve, **proxy** tiene un significado muy general, aunque siempre es sinónimo de **intermediario**.

## \* Funcionamiento.

1. El cliente realiza una petición (p. ej. mediante un navegador web) de un recurso de Internet (una página web o cualquier otro archivo) especificado por una URL.
2. Cuando el *proxy* caché recibe la petición, busca la URL resultante en su caché local. Si la encuentra, contrasta la fecha y hora de la versión de la página demanda con el servidor remoto. Si la página no ha cambiado desde que se cargo en caché la devuelve inmediatamente, ahorrándose de esta manera

mucho tráfico pues sólo intercambia un paquete para comprobar la versión. Si la versión es antigua o simplemente no se encuentra en la caché, lo captura del servidor remoto, lo devuelve al que lo pidió y guarda o actualiza una copia en su caché para futuras peticiones.

El caché utiliza normalmente un algoritmo para determinar cuándo un documento está obsoleto y debe ser eliminado de la caché, dependiendo de su antigüedad, tamaño e histórico de acceso. Dos de esos algoritmos básicos son el LRU (el usado menos recientemente, en inglés "Least Recently Used") y el LFU (el usado menos frecuentemente, "Least Frequently Used").

Los *proxies* web también pueden filtrar el contenido de las páginas Web servidas. Algunas aplicaciones que intentan bloquear contenido Web ofensivo están implementadas como *proxies* Web. Otros tipos de *proxy* cambian el formato de las páginas web para un propósito o una audiencia específicos, para, por ejemplo, mostrar una página en un teléfono móvil o una PDA. Algunos operadores de red también tienen *proxies para interceptar virus* y otros contenidos hostiles servidos por páginas Web remotas.

Un cliente de un ISP manda una petición a Google la cual llega en un inicio al servidor Proxy que tiene este ISP, no va directamente a la dirección IP del dominio de Google. Esta página concreta suele ser muy solicitada por un alto porcentaje de usuarios, por lo tanto el ISP la retiene en su Proxy por un cierto tiempo y crea una respuesta en mucho menor tiempo. Cuando el usuario crea una búsqueda en Google el servidor Proxy ya no es utilizado; el ISP envía su petición y el cliente recibe su respuesta ahora sí desde Google.

## \* Instalación de servidores «proxy».

### Instalar un servidor proxy HTTP (Squid)

#### 1. Instalar el proxy

Para instalar Squid escribe en un terminal:  
sudo aptitude install squid

#### 2. Configurar el proxy

La configuración de Squid se hace editando el archivo **/etc/squid/squid.conf**

Para editar este archivo, presiona Alt+F2 y:  
gksu gedit /etc/squid/squid.conf



### 2.1 Nombrar el proxy

Squid necesita conocer el nombre de la máquina. Para ello, ubica la línea **visible\_hostname**.

Por ejemplo, si la máquina se llama “ubuntu”, pon:

```
visible_hostname ubuntu
```

### 2.2 Elegir el puerto

Por defecto, el puerto de escucha del servidor proxy será 3128. Para elegir otro puerto, ubica la línea:

```
http_port 3128
```

Y cambia el número de puerto, por ejemplo:

```
http_port 3177
```

### 2.3 Elegir la interfaz

Por defecto el servidor proxy escucha por todas las interfaces. Por razones de seguridad, sólo debes hacer que escuche en tu red local.

Por ejemplo si la tarjeta de red ligada a tu LAN tiene el IP 10.0.0.1, modifica la línea a:

```
http_port 10.0.0.1:3177
```

### 2.4 Definir los derechos de acceso

Por defecto, nadie está autorizado a conectarse al servidor proxy, excepto tu máquina. Entonces hay que crear una lista de autorización.

Por ejemplo vamos a definir un grupo que abarca toda la red local.

Ubica la línea del archivo que comienza por **acl localhost...**

Al final de la sección, agrega:

```
acl lanhome src 10.0.0.0/255.255.255.0
```

(lanhome es un nombre arbitrario que hemos elegido)

```
#
#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 # https
acl SSL_ports port 563 # snews
acl SSL_ports port 873 # rsync
acl Safe_ports port 80 # http
acl Safe_ports port 21 # ftp
acl Safe_ports port 443 # https
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
acl lanhome src 10.0.0.0/255.255.255.0
```

## 2.5 Autorizar al grupo

Ahora que el grupo está definido, vamos a autorizar para que utilice el proxy.

Ubica la línea **http\_access allow...**

Y agrega debajo (antes de la línea **http\_access deny all**)

**http\_access allow lanhome**

```
Example rule allowing access from your local networks. Adapt
to list your (internal) IP networks from where browsing should
be allowed
#acl our_networks src 192.168.1.0/24 192.168.2.0/24
#http_access allow our_networks
http_access allow localhost
http_access allow lanhome

And finally deny all other access to this proxy
http_access deny all
```

## 2.6 Autorizar los puertos no estándar

Por defecto, Squid sólo autoriza el tráfico HTTP en algunos puertos (80, etc.)

Esto puede ocasionar problemas a algunas páginas web que utilizan otros puertos

Ejemplo: <http://toto.com/81/images/titi.png> sería bloqueado por Squid.

Para evitar que lo bloquee, encuentra la línea:

**http\_access deny !Safe\_ports**

Y agrega un comentario:

**#http\_access deny !Safe\_ports**

### 3. Iniciar el proxy

(Re)inicia el proxy para que tome en cuenta la nueva configuración que acabamos de realizar.

Escribe:

```
sudo /etc/init.d/squid restart
```

A partir de ahora el proxy debería funcionar. Sólo hay que configurar los diversos programas para que lo utilicen.

#### Información

Los logs del proxy se encuentran en `/var/log/squid/access.log`

#### Modificar el tamaño del caché

Por defecto, el caché de Squid está activado, lo que permite que las páginas se carguen más rápido.

El tamaño por defecto es de 100 Mo (ubicado en `/var/spool/squid`).

Para cambiar su tamaño, modifica el archivo `/etc/squid/squid.conf`

Encuentra la línea:

```
cache_dir ufs /var/spool/squid 100 16 256
```

Modifícala, puedes cambiar el valor de 100 por el valor que desees (por ejemplo 200 para 200 Mo):

```
cache_dir ufs /var/spool/squid 200 16 256
```

#### Configuración del Proxy HTTP con Zentyal

Para configurar el proxy HTTP iremos a *Proxy HTTP* ▶ *General*. Podremos definir si el proxy funciona en modo *Proxy Transparente* para forzar la política establecida o si por el contrario requerirá configuración manual. En este último caso, en *Puerto* estableceremos dónde escuchará el servidor conexiones entrantes. El puerto preseleccionado es el 3128, otros puertos típicos son el 8000 y el 8080. El proxy de Zentyal únicamente acepta conexiones provenientes de las interfaces de red internas, por tanto, se debe usar una dirección interna en la configuración del navegador.

El tamaño de la caché define el espacio en disco máximo usado para almacenar temporalmente contenidos web. Se establece en *Tamaño de caché* y corresponde a cada administrador decidir cuál es el tamaño óptimo teniendo en cuenta las características del servidor y el tráfico esperado.

Además también estableceremos aquí la *Política predeterminada* para el acceso al contenido web HTTP a través del proxy. Esta política determina si se puede acceder o

no a la web y si se aplica el filtro de contenidos. Puede configurarse de las siguientes maneras:

*Permitir todo:*

Con esta política se permite a los usuarios navegar sin ningún tipo de restricciones pero todavía disfrutando de las ventajas de la caché, ahorro de tráfico y mayor velocidad.

*Denegar todo:*

Esta política deniega totalmente el acceso a la web. Aunque a primera vista podría parecer poco útil ya que el mismo efecto se podría conseguir con una regla de cortafuegos, sin embargo podemos establecer posteriormente políticas particulares para objetos, usuarios o grupos, pudiendo usar esta política para denegar en principio y luego aceptar explícitamente en determinadas condiciones.

*Filtrar:*

Esta política permite a los usuarios navegar pero activa el filtrado de contenidos que puede denegar el acceso web según el contenido solicitado por los usuarios.

*Autorizar y filtrar, permitir todo o denegar todo:*

Estas políticas son versiones de las políticas anteriores que incluyen autorización. La autorización se explicará en la sección *Configuración Avanzada para el proxy HTTP*.

Proxy HTTP [\(mostrar ayuda\)](#)

Configuración General

Proxy Transparente:

Nótese que no se puede usar proxy HTTPS de forma transparente. Se necesitará añadir una regla de firewall si se habilita este modo.

Puerto:

Tamaño de los ficheros de caché (MB):


Política predeterminada: Siempre denegar ▼


Filter significa que las peticiones HTTP pasan por el filtro de contenidos y que podrían ser rechazados si el contenido no se considera válido.

Change

Excepciones en la caché

[+ Añade nuevo](#)

| Dirección del nombre de dominio                 | Negar almacenamiento en caché del dominio | Action                                                                                |
|-------------------------------------------------|-------------------------------------------|---------------------------------------------------------------------------------------|
| <input type="text" value="miorganizacion.com"/> | <input checked="" type="checkbox"/>       |  |

10 ▼ Página 1 

Proxy HTTP

Es posible indicar que dominios no serán almacenados en caché. Por ejemplo, si tenemos servidores web locales no se acelerará su acceso usando la caché y se desperdiciaría memoria que podría ser usada por elementos de servidores remotos. Si un dominio está exento de la caché, cuando se reciba una petición con destino a dicho dominio se ignorará la caché y se devolverán directamente los datos recibidos desde el servidor sin almacenarlos. Estos dominios se definen en *Excepciones a la caché*.

Tras establecer la política global, podemos definir políticas particulares para *Objetos de red* en *Proxy HTTP* ▶ *Política de objetos*. Podremos elegir cualquiera de las seis políticas para cada objeto; cuando se acceda al proxy desde cualquier miembro del objeto esta política tendrá preferencia sobre la política global. Una dirección de red puede estar contenida en varios objetos distintos por lo que es posible ordenar los objetos para reflejar la prioridad. Se aplicará la política del objeto de mayor prioridad que contenga la dirección de red. Además existe la posibilidad de definir un rango horario fuera del

cual no se permitirá acceso al objeto de red aunque esta opción sólo es compatible con políticas de permitir o denegar y no con políticas de filtrado de contenidos.

Política de Objeto [\(mostrar ayuda\)](#)

Lista de objetos

[+ Añade nuevo](#)

| Objeto | Política            | Periodo de tiempo permitido | Política de grupo | Perfil de filtrado | Action |
|--------|---------------------|-----------------------------|-------------------|--------------------|--------|
| Guest  | Authorize and allow | 08:00-20:00 MTW             |                   | default            |        |
| Ventas | Always allow        | All time                    |                   | default            |        |
| IT     | Always allow        | All time                    |                   | default            |        |
| DMZ    | Always deny         | All time                    |                   | default            |        |

10 ▼ Página 1

Políticas de objeto

**Eliminando anuncios de la web**

El proxy HTTP puede eliminar anuncios de las paginas web. Esto ahorrara ancho de banda y reducirá distracciones para los usuarios. Para usar esta característica, debemos acceder a *Proxy HTTP* ▶ *General* y activar la opción *Bloqueo de propaganda*.

La eliminación de anuncios afecta a todos los accesos web a través del proxy.

**Limitación de las descargas con Zentyal**

Otra de las características configurables en Zentyal es limitar el ancho de banda de las descargas usando objetos de red mediante *Delay Pools*. Para configurarlas accederemos a *HTTP Proxy* ▶ *Limitación de ancho de banda*. Las *Delay Pools* pueden entenderse como cajas en las que se dispone de una determinada cantidad de ancho de banda; se van llenando poco a poco y se van vaciando mientras se usa la red, cuando se vacían se limita el ancho de banda, la velocidad de descarga. Teniendo en cuenta esta explicación, veamos los valores que podemos establecer por cada caja:

*Ratio:*

Ancho de banda máximo que se podrá utilizar cuando se vacíe la caja.

*Volumen:*

Capacidad máxima de la caja en bytes, es decir, la caja se vaciará si se han transmitido tantos bytes como los indicados en el volumen.

Zentyal permite limitar el ancho de banda mediante dos métodos diferentes, las *Delay Pools* de clase 1 y las de clase 2. Las restricciones de la clase 1 tienen prioridad sobre las de la clase 2, si un objeto de red no se corresponde con los limitados por alguna de las reglas no se le aplica ninguna.

*Delay pools* de clase 1:

Limitan el ancho de banda globalmente para una subred, permiten configurar un límite de datos transferidos, el *Tamaño de fichero* y una restricción de ancho de banda máximo, el *Velocidad de descarga*. La limitación se activa cuando el límite de datos ha sido superado. Estas *Delay Pools* se componen de una sola caja compartida por todo el objeto de red.

*Delay pools* de clase 2:

Estas *Delay Pools* se componen de dos tipos de cajas, una general en la que como en las de clase 1 se va acumulando todo el tráfico transmitido a la subred y una dedicada a cada cliente. Si un miembro de la subred vacía su caja se limitará su ancho de banda al *Velocidad de descarga del cliente*, pero no a los demás, si entre todos vacían la caja agregada, se limita el ancho de banda de todos los clientes a *Velocidad de descarga de la red*.

Limitación de Ancho de Banda [\(mostrar ayuda\)](#)

**Añadiendo un/a nuevo/a regla**

Habilitado:

Objeto de red: local\_clients

Velocidad de descarga: 15 KB/s  
Máxima velocidad de descarga para esta red. Use -1 para desactivar esta opción.

Tamaño de fichero: 15000 KB  
Máximo tamaño de fichero no limitado para esta red. Use -1 para desactivar esta opción.

**Añadiendo un/a nuevo/a regla**

Habilitado:

Objeto de red: local\_clients

Velocidad de descarga de la red: 0 KB/s  
Máxima velocidad de descarga para esta red. Use -1 para desactivar esta opción.

Máximo tamaño de fichero: 0 KB  
Máximo tamaño de fichero no limitado para esta red. Use -1 para desactivar esta opción.

Velocidad de descarga del cliente: 0 KB/s  
Máxima velocidad de descarga por cliente. Use -1 para desactivar esta opción.

Tamaño de fichero por cliente: 0 KB  
Tamaño máximo de fichero no limitado por cliente. Use -1 para desactivar esta opción.

Limitación de ancho de banda

### Filtrado de contenidos con Zentyal

Zentyal permite el filtrado de páginas web en base a su contenido. Para ello, es necesario que la política global o la política particular de cada objeto desde el que se accede sea de *Filtrar* o *Autorizar y Filtrar*.

Se pueden definir múltiples perfiles de filtrado en *Proxy HTTP* ▶ *Perfiles de Filtrado* pero si no hay ninguno específico aplicándose al usuario, grupo u objeto se aplicará el perfil *default*.



Filtrar perfiles [\(mostrar ayuda\)](#)

Lista de perfiles

[+ Añade nuevo](#)

| Filtrar grupo | Configuración                                                                     | Action                                                                                                                                                                  |
|---------------|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| default       |  |   |
| Ventas        |  |   |
| IT            |  |   |

10 ▼ Página 1 

### Perfiles de filtrado

El filtrado de contenidos de las páginas web se utiliza diferentes métodos incluyendo filtrado heurístico, tipos MIME, extensiones, listas blancas y listas negras entre otros. La conclusión final es determinar si una página o un recurso web puede ser visitado o no.

El primer filtro que podemos configurar es el antivirus. Para poder utilizarlo debemos tener el módulo de Antivirus instalado y activado. Si está activado se bloqueará el tráfico HTTP en el que sean detectados virus.

El filtrado heurístico consiste principalmente en el análisis de los textos presentes en las páginas web, si se considera que el contenido no es apropiado (pornografía, racismo, violencia, etc) se bloqueará el acceso a la página. Para controlar este proceso se puede establecer un umbral más o menos restrictivo, siendo este el valor que se comparará con la puntuación asignada a la página para decidir si se bloquea o no. El lugar donde establecer el umbral es la sección *Umbral de filtrado de contenido*. Se puede desactivar este filtro eligiendo el valor *Desactivado*. Hay que tener en cuenta que con este análisis se pueden llegar a bloquear páginas no deseadas, lo que se conoce como un falso positivo. Este problema se puede remediar añadiendo los dominios de estas páginas a una lista blanca, pero siempre existirá el riesgo de un falso positivo con nuevas páginas.

También tenemos a continuación el *Filtrado de extensiones de fichero*, el *Filtrado de tipos MIME* y el *Filtrado de dominios*.

Umbral de filtrado de contenido

Usar el umbral del perfil por defecto:

Umbral: Medio ▼

Esto especifica cuán estricto es el filtro

Change

Filtrado de extensiones de fichero

**Filtrado de tipos MIME**

Filtrado de dominios para grupo de filtros

Usar perfil predeterminado para el filtrado de MIME









Usar configuración del perfil predeterminado:





Change

 Tipo MIME añadido

Configurar tipos MIME permitidos

[+ Añade nuevo](#)

| Tipo MIME            | Permitir                            | Action                                                                                                                                                                      |
|----------------------|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| application/compress | <input checked="" type="checkbox"/> |   |
| application/gzip     | <input checked="" type="checkbox"/> |   |
| audio/mpeg           | <input checked="" type="checkbox"/> |   |
| audio/x-wav          | <input checked="" type="checkbox"/> |   |

10 ▼ Página 1    

Configurar politica para todos los tipos MIME

Permitir todos Tipos MIME:

Usar este campo para cambiar el valor de todas filas de arriba a la vez

Change

Perfil de filtrado

En la pestaña de *Filtrado de extensiones de fichero* se puede seleccionar qué extensiones serán bloqueadas. De manera similar en *Filtrado de tipos MIME* se pueden indicar qué tipos MIME se quieren bloquear y añadir otros nuevos si es necesario, al igual que con las extensiones.

En la pestaña de *Filtrado de dominios* encontraremos la configuración del filtrado basado en dominios. Podemos:

- *Bloquear dominios especificados sólo como IP*, esta opción bloquea cualquier página que se intente acceder especificado únicamente su dirección IP y no el dominio asociado.
- *Bloquear dominios no listados*, esta opción bloquea todos los dominios que no estén presentes en la sección *Reglas de dominios* o en las categorías presentes en *Ficheros de listas de dominios* y cuya política no sea *Ignorar*.

A continuación tenemos la lista de dominios, donde podemos introducir nombres de dominio y seleccionar una política para ellos entre las siguientes:

*Permitir siempre:*

El acceso a los contenidos del dominio será siempre permitido, todos los filtros son ignorados.

*Denegar siempre:*

El acceso nunca se permitirá a los contenidos de este dominio.

*Filtrar:*

Se aplicarán las reglas usuales a este dominio. Resulta útil si está activada la opción *Bloquear dominios no listados*.

Filtrado de extensiones de fichero
Filtrado de tipos MIME
Filtrado de dominios para grupo de filtros

### Usar perfil predeterminado para el filtrado de dominios

Usar configuración del perfil predeterminado:

[Change](#)

### Configuración del filtrado de dominio

Bloquear dominios y URLs no listados:

Si esta opción está habilitada, cualquier dominio que no esté en la sección *Reglas de dominios*, ni en *Ficheros de listas de dominios* debajo será prohibido.

Bloquear sitios especificados sólo como IP:

[Change](#)

### Reglas de dominios y URLs

[+ Añade nuevo](#)

[Buscar](#)

| Dominio o URL      | Política     | Action |
|--------------------|--------------|--------|
| miorganizacion.com | Always allow |        |

10 ▼ Página 1

### Ficheros de las listas de dominios para el filtrado de grupo

[+ Añade nuevo](#)

[Buscar](#)

| Description      | Categorías | Fichero                   | Action |
|------------------|------------|---------------------------|--------|
| shalla blacklist |            | shalla_blacklist Download |        |

10 ▼ Página 1

### Filtrado de dominios

Podemos simplificar el trabajo del administrador usando listas clasificadas de dominios. Estas listas son normalmente mantenidas por terceros y tienen la ventaja de que los dominios están clasificados por categorías, permitiéndonos seleccionar una política para una categoría entera de dominios. Estas listas son distribuidas en forma de archivo comprimido. Una vez descargado el archivo, podemos incorporarlo a nuestra configuración y establecer políticas para las distintas categorías de dominios. Las políticas que se pueden establecer en cada categoría son las mismas que se

pueden asignar a dominios y se aplican a todos los dominios presentes en dicha categoría. Existe una política adicional *Ignorar* que, como su nombre indica, simplemente ignora la existencia de la categoría a la hora de filtrar. Dicha política es la elegida por defecto para todas las categorías.

**Domains list categories**

Search

| Category   | Policy       | Action                                                                                |
|------------|--------------|---------------------------------------------------------------------------------------|
| adv        | Always deny  |    |
| aggressive | Always deny  |    |
| astronomy  | Ignore       |    |
| banking    | Always allow |    |
| bikes      | Ignore       |    |
| boats      | Ignore       |    |
| cars       | Ignore       |    |
| chat       | Always deny  |  |
| chemistry  | Ignore       |  |
| cooking    | Ignore       |  |

10 Page 1 of 7 

### Listado de categorías

Mediante las Actualizaciones Avanzadas de Seguridad de Zentyal [3] podemos instalar automáticamente una base de datos actualizada de categorías de dominios para disponer de las funcionalidades requeridas para una política de filtrado de contenidos de nivel profesional.

### Instalación de un Servidor Proxy en una Red Local

La instalación de un Servidor Proxy en su Red Local es super sencilla. En este apartado damos por supuesto que usted sabe:

- Cómo instalar y configurar el protocolo TCP/IP en la máquina en la que se instalará el Servidor Proxy (sea un Windows NT o un Windows 95)
- Cómo instalar y configurar el protocolo TCP/IP en los Puestos de Trabajo de su Red Local (sean estos Puestos de Trabajo ordenadores Windows 3.11, Windows 95, Macintosh, UNIX, o cualquier otro sistema operativo)

- Cómo instalar el Módem o la Tarjeta RDSI que utilizará para conectarse a internet
- Cómo instalar el Acceso Remoto a Redes (RAS) de Windows NT o el Acceso Telefónico a Redes de Windows 95

Si usted carece de estos conocimientos, en la documentación de Windows NT y de Windows 95 encontrará gran cantidad de información útil.

### **Asignación de Direcciones IP a los Puestos de Trabajo de su Red Local**

Antes de instalar el Servidor Proxy, Usted deberá haber instalado y configurado el protocolo TCP/IP en su Red Local. No es necesario que instale este protocolo en todos los ordenadores de su Red Local, sino solamente en aquellos en los que querrá utilizar servicios de internet, y también en aquel en el que vaya a querer instalar el Servidor Proxy.

Cuando instale el protocolo TCP/IP, asigne a los Puestos de Trabajo de su Red Local direcciones de la **subred de Clase B 192.168.X.X**. Este rango de direcciones IP está reservado para su uso en intranets, y le proporciona un espacio seguro de direcciones.

**Debe asignar una dirección IP diferente a cada conexión de su Red Local** (a partir de ahora nos referiremos a su Red Local como su ``intranet").

Por ejemplo, puede comenzar por **192.168.0.1, 192.168.0.2, 192.168.0.3**, etc...

Le recomendamos que reserve la dirección **192.168.0.1** para el ordenador en el que vaya a instalar el Servidor Proxy, ya que esta dirección le resultará más fácil de recordar.

### **Comprobación de la Instalación del Protocolo TCP/IP**

Para comprobar que la instalación del protocolo TCP/IP ha sido correcta, haga un PING a cada una de las direcciones IP que haya definido en su intranet. Si no obtiene respuesta de alguna de ellas repase la configuración y solucione el error antes de continuar. Para realizar un PING desde una máquina con sistema operativo Windows, abra una ventana MS-DOS y teclee:

```
C:> ping 192.168.x.x
```

donde 192.168.x.x es la dirección IP de la máquina que está interrogando.

### **Instalación del Módem o de la Tarjeta RDSI**

En el ordenador en el que va a instalar el Servidor Proxy, debe haber instalado y configurado correctamente el Módem o la Tarjeta RDSI. La correcta instalación del hardware es imprescindible para realizar el siguiente paso.

### **Instalación del Acceso Remoto a Redes (RAS) de Windows NT o el Acceso Telefónico a Redes de Windows 95**

En el ordenador en el que va a instalar el Servidor Proxy, deberá haber instalado el servicio del sistema operativo que le permite conectarse a internet. La conexión a internet deberá hacerse utilizando los datos de su Cuenta de Acceso a internet, proporcionados por su Proveedor de Acceso a internet:

- \* Identificador de usuario
- \* Password de Acceso
- \* DNS
- \* Dirección IP dinámica (la asignará el proveedor en cada conexión)

Es importante que cuando configure este servicio no active la utilización de otro protocolo de red que no sea el TCP/IP.

El acceso a internet debe funcionar correctamente antes de intentar instalar el Servidor Proxy.

### **Instalación del Servidor Proxy en Windows NT y en Windows 95**

La instalación en Windows NT la debe realizar el Administrador del Sistema con los discos originales o el fichero instalador obtenido de internet. La instalación no entraña ninguna dificultad.

La instalación en Windows 95 se realiza con los discos originales o el fichero instalador obtenido de internet de manera idéntica a como se realiza cualquier otra instalación en este sistema operativo. La instalación no entraña ninguna dificultad.

Una vez finalizada la instalación, se habrá creado un directorio o carpeta que contiene los ficheros del Servidor Proxy, así como la documentación en línea en formato HTML, que resulta muy útil en el momento de configurar el Servidor Proxy.

Las aplicaciones **CSM Proxy** y **CSM Proxy Plus** son las que bajo Windows 95 deben ejecutarse para que el Servicio de Proxy esté activo en su intranet. En Windows NT es el Administrador del Sistema el que debe activar el servicio correspondiente.

La aplicación **CSM Proxy Admin (local)** es la que permite la Configuración del Servidor Proxy.

### **Configuración de un Servidor Proxy en una Red Local**

La Configuración del Servidor Proxy es la que determinará el comportamiento del Servidor Proxy y cómo éste responderá a las peticiones que reciba de los Puestos de Trabajo de su intranet.

La Configuración Básica incluye:

- \* Especificar qué Conexión de RAS o Acceso Telefónico a Redes se utilizará para conectar a internet
- \* Especificar cada uno de los servicios que el Servidor Proxy dará o no dará a la intranet, y configurarlos. Los servicios básicos habituales son 5: HTTP Proxy, FTP Proxy, SMTP Proxy, POP Proxy y DNS Proxy
- \* Confirmar Permisos generales de acceso

### **Configurar la Conexión RAS o de Acceso Telefónico a Redes**

En la Configuración de Marcado (Dialing) especificaremos la Conexión RAS o de Acceso Telefónico a Redes que ya estaba definida en el ordenador en el que hemos instalado el Servidor Proxy. En el supuesto de que exista más de una Conexión disponible, elegiremos una de ellas; que será la que siempre utilice el Servidor Proxy.

Introduciremos la información de **Identificador de Usuario** y **Password** necesaria para poder realizar la Conexión, y comprobaremos con el botón **TEST** que el Servidor Proxy es capaz de iniciar una conexión a internet.

Resulta útil **configurar el Servidor Proxy para que corte la conexión transcurrido un tiempo de inactividad, para así ahorrar en gasto telefónico**. El tiempo óptimo de inactividad necesario para cortar la transmisión en una conexión a través de infovia puede estar en torno a los 600 segundos (10 minutos), pero depende del tipo de uso que Usted haga de internet.

### HTTP Proxy

Este servicio estará normalmente **ACTIVADO** en el puerto **8080**.

El servicio de transferencia de ficheros rutado por HTTP también estará normalmente **ACTIVADO** en el puerto **8080**.

Las **opciones de Cache** deberían indicar únicamente que se compruebe la página original antes de entregar la página que está en el Cache. En este apartado pueden indicarse aquellas direcciones para las que no queremos la función de Cache.

### FTP Proxy

Este servicio estará normalmente **ACTIVADO** en el puerto **21**.

CSM Proxy Plus proporciona también funciones de Cache para el servicio FTP.

### SMTP Proxy

Este servicio estará normalmente **ACTIVADO** en el puerto **25** de entrada y **25** de salida, y asociado al servidor SMTP que nos haya indicado nuestro Proveedor de Acceso a internet. Para ello, debemos crear un "Enlace Mapeado" por el que indicamos al Servidor Proxy que todos los paquetes de datos que se reciban de la intranet en el puerto 25 deben ser enviados al servidor SMTP de internet por el puerto 25.

### POP Proxy

Este servicio estará normalmente **ACTIVADO** en el puerto **110** y con "delimitador" #.

El delimitador es un caracter especial que sustituirá en la intranet a la @ de la dirección de correo electrónico. Más adelante se explica el mecanismo que utiliza el Servidor Proxy para realizar las conexiones al buzón correspondiente a cada usuario de la intranet.

### DNS Proxy

Este servicio estará normalmente **ACTIVADO** en el puerto **53** y apuntará a las direcciones IP de los DNS proporcionados por su Proveedor de Acceso a Internet.

### Puesta en Marcha de un Servidor Proxy en una Red Local

Una vez Configurado el Servidor Proxy, ya puede poner en marcha el servicio. En el caso de Windows 95 le resultará de utilidad crear un Acceso Directo a la aplicación **CSM Proxy** o **CSM Proxy Plus** en la **Carpeta de Inicio** para que el Servidor Proxy se inicie automáticamente nada más encender el ordenador en el que está instalado. Hay que recalcar que el Servidor Proxy sólo generará una llamada telefónica y abrirá una conexión con internet cuando cualquiera de los Puestos de Trabajo de la intranet soliciten un acceso a internet por cualquiera de los servicios activados al configurar el Servidor Proxy, y siempre que el Puesto de Trabajo tenga las autorizaciones definidas en el momento de la Configuración.



## \* Instalación y configuración de clientes «proxy».

### Configuración de los Puestos de Trabajo de una Red Local con un Servidor Proxy

Una vez el Servidor Proxy está en marcha en un ordenador de la Red Local, todos los Puestos de Trabajo y demás Servidores de la intranet pueden utilizar los servicios que hayan sido configurados.

No nos cansamos de recalcar el hecho de que el Servidor Proxy presta sus servicios a toda la intranet TCP/IP, por lo que no tiene ninguna importancia si el Puesto de Trabajo se corresponde a un sistema operativo o a otro. En una Red Local en la que todos los Puestos de Trabajo sean **Apple Macintosh**, basta un único PC con **Windows 95** o **Windows NT** con el software **CSM Proxy** o **CSM Proxy Plus** instalado para que desde cualquier **Macintosh** se pueda acceder a internet. Y quien dice un Macintosh podría decir cualquier otro tipo de Puesto de Trabajo con cualquier sistema imaginable que tenga implementado el protocolo de Red TCP/IP.

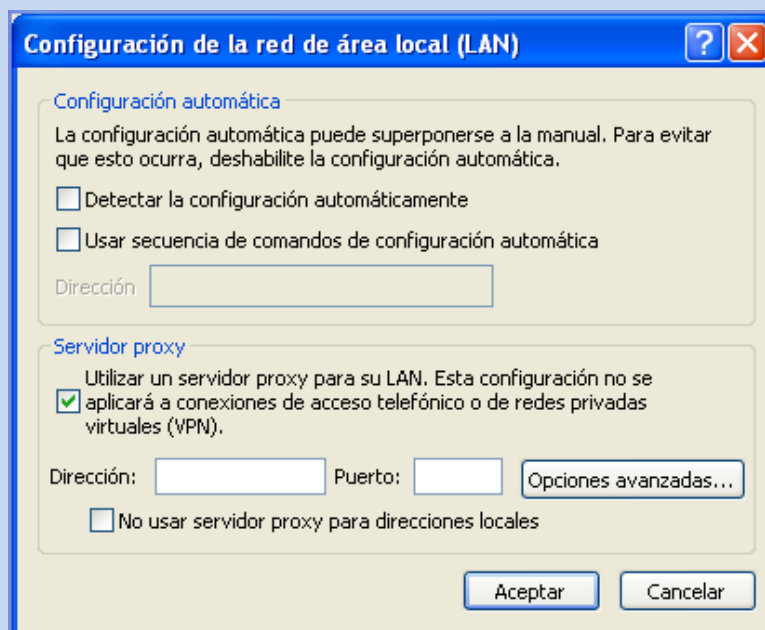
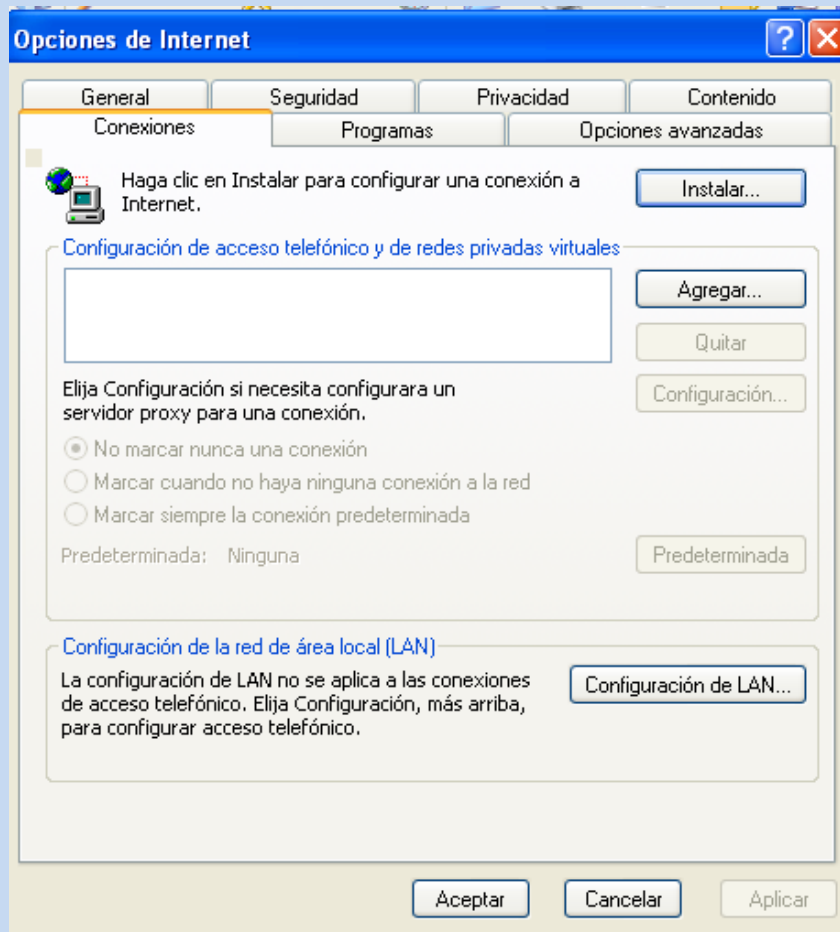
Lógicamente, el software "cliente" para cada plataforma será diferente.

Afortunadamente, las aplicaciones cliente más populares de internet tienen versiones para casi todas las plataformas que nos podemos encontrar en el mercado. En este ejemplo nos centraremos en la configuración del programa **Netscape Navigator 3.01**, que utilizaremos como browser de páginas web y también como aplicación de correo electrónico. De la misma manera que configuraremos este programa para que opere sin problemas en la intranet, podemos configurar cualquier otra aplicación de internet como: Microsoft Internet Explorer, Eudora, Pegasus Mail, CuteFTP, Anarchie, Claris EMailer, etc...

*Los clientes proxy web* son aplicaciones que realizan solicitudes de descarga HTTP, HTTPS o FTP a través de HTTP al puerto TCP en el que Forefront TMG escucha las solicitudes web salientes de la red del cliente. A diferencia de los clientes de Firewall, los clientes de proxy Web no requieren la instalación de ningún software de cliente. Sólo hay que configurar el explorador Web. El explorador Web transmite la información de autenticación. Los equipos cliente de Firewall y de SecureNAT también pueden ser clientes de proxy Web si sus exploradores se configuran para ello. Para configurar el explorador Web Microsoft Internet Explorer 6.0 como cliente de proxy Web

1. En el menú **Herramientas** de Internet Explorer, haga clic en **Opciones de Internet**, haga clic en la ficha **Conexiones** y haga clic en **Configuración LAN**.
2. En **Servidor proxy**, active la casilla **Utilizar un servidor proxy para su LAN**.
3. En el cuadro **Dirección**, escriba la dirección IP del servidor ISA.
4. En el cuadro **Puerto**, escriba el número de puerto que utiliza el servidor ISA para las conexiones de cliente (de forma predeterminada, 8080).
5. Puede activar la casilla **No usar servidor proxy para direcciones locales** si no desea utilizar el equipo ISA Server al conectarse a un equipo de la red local (esto puede acelerar el rendimiento).
6. Haga clic en **Aceptar** para cerrar el cuadro de diálogo **Configuración LAN**.

7. Haga clic en **Aceptar** de nuevo para cerrar el cuadro de diálogo **Opciones de Internet**.

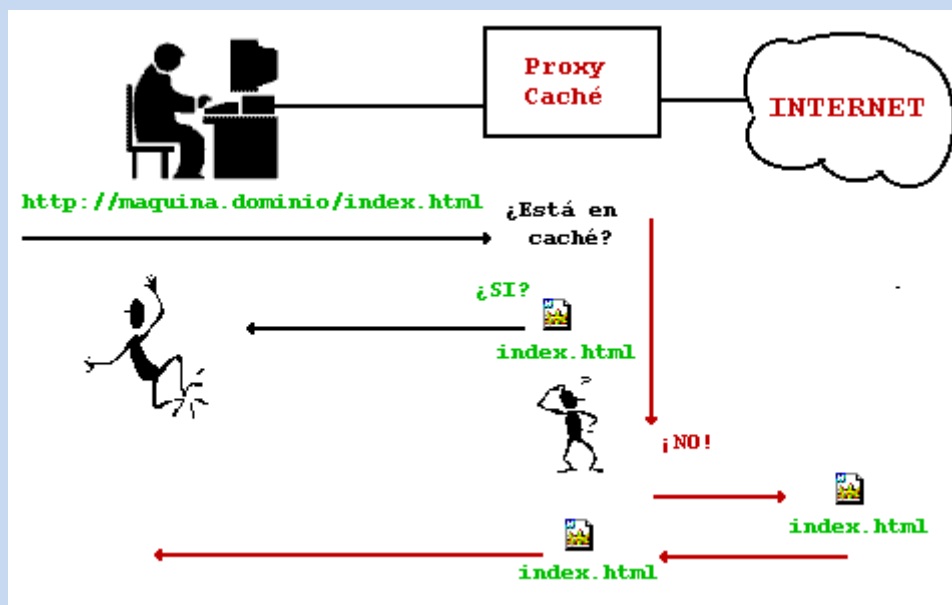


## \* Configuración del almacenamiento en la caché de un «proxy».

### Servicio Proxy-Caché

Un servicio proxy-caché permite incrementar la velocidad de acceso a Internet al mantener localmente las páginas más consultadas por los usuarios de una organización, evitando las conexiones directas con los servidores remotos.

Los usuarios configuran su navegador web para dirigir sus accesos al servicio proxy-caché en vez de ir directamente al destino final. El servidor proxy-caché se encarga de proporcionarle la página pedida bien obteniéndola de su caché o accediendo al documento original; al dar servicio a muchos usuarios la caché contendrá muchos documentos beneficiándose toda la organización de ello. Se evitan transferencias innecesarias y con ello se aumenta la velocidad en la carga de las páginas, ya que no es necesario pedir una página cuando ya esté almacenada en la caché (porque otro la había pedido antes).



La Red Informática de la Universidad de Jaén (RIUJA) dispone de un servidor que puede actuar como servidor proxy-caché.

Evidentemente, **sólo pueden usar este servicio las máquinas de la Universidad de Jaén**. Para beneficiarse de estas ventajas, primero ha de configurar su navegador. Para algunos PCs la configuración del servicio proxy es obligatoria, en caso contrario no podrán salir a Internet.

### Configuración de los clientes

Podemos encontrar dos tipos de configuración en los clientes: manual y automática.

- **Manual:** Indicando en nuestro navegador la dirección de la máquina que actúa como proxy.
- **Automatizada (recomendada):** Indicando en nuestro navegador la dirección URL de un archivo de autoconfiguración (<http://www.ujaen.es/sci/redes/proxy/proxy.pac>)

Una vez configurado el acceso a WWW a través de un proxy-caché todos los accesos se realizarán a través de la caché de forma transparente al usuario.

Algunos de los clientes en los que puede configurarlo son:

- [Netscape Navigator y Communicator](#)
- [Microsoft Internet Explorer](#)
- [Mozilla](#)

### **Cómo configurar el proxy-caché en el navegador.**

La mayoría de los navegadores permiten entre sus opciones especificar el servidor proxy-caché o alternativo mediante el cual acceder a Internet por tanto sólo hay que indicarles como acceder a la máquina que actuará de servidor proxy-caché. Se explica a continuación cómo realizar la configuración automática (recomendada) de los navegadores más usados.

- **En Netscape Communicator y Mozilla.**

Netscape Navigator/Communicator permite configurar el uso de proxy-caché tanto de forma manual como de forma automática, consiguiéndose similares resultados. Se explica a continuación como configurarlo de forma automática para el Netscape Communicator 4.03, aunque para otras versiones se hace de manera similar. El navegador Mozilla hereda de Netscape Communicator gran parte de su funcionalidad y apariencia por lo que lo explicado a continuación sirve de referencia para la activación del proxy-caché en Mozilla.

#### Paso 1

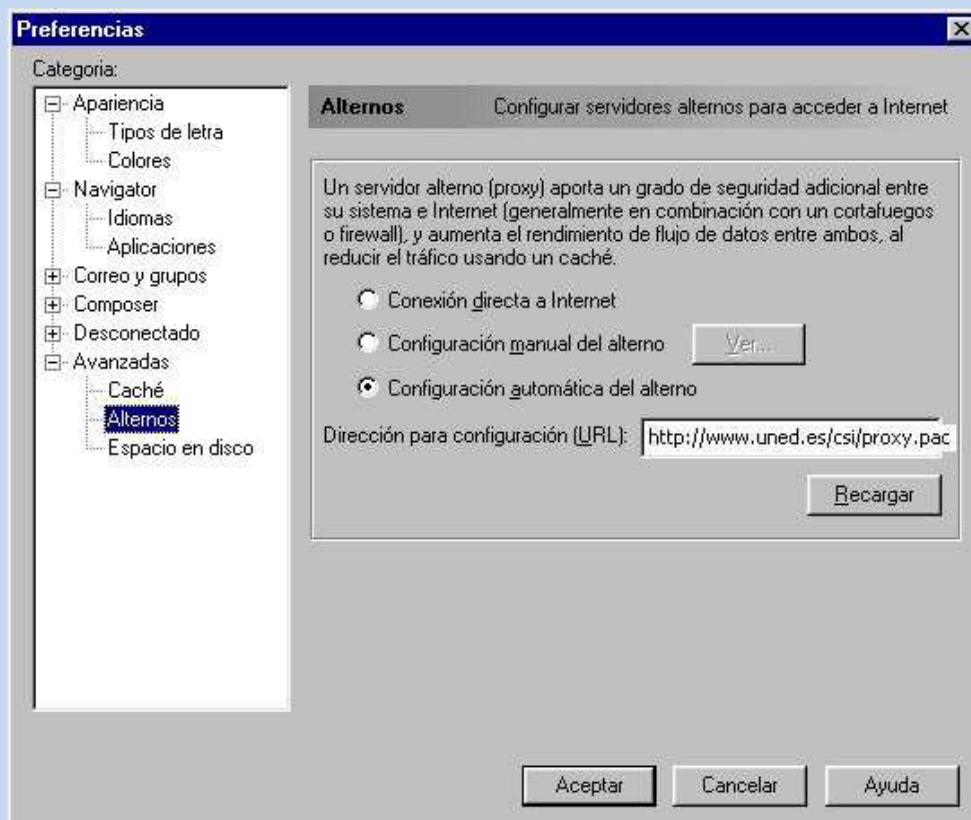
Seleccionar el menú Preferencias situado dentro del menú principal Edición (**Edición -> Preferencias**)



## Paso 2

Elegir ahora dentro del menú Avanzados el submenú Alternos (**Avanzados ->Alternos**).

Marcar la tercera opción "Configuración automática del altero" y escribir la URL del archivo de configuración automática (<http://www.uned.es/csi/proxy.pac>) en la caja de texto como se indica en el siguiente gráfico:



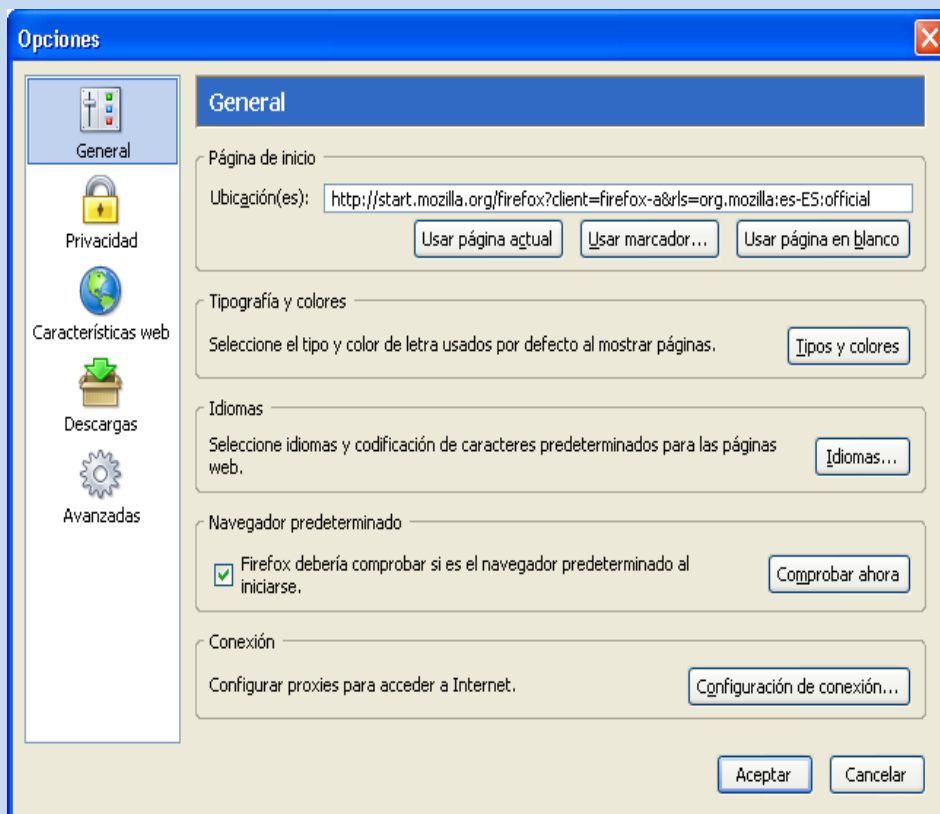
Para utilizar el proxy-caché sin tener que cerrar y abrir el navegador pulsar **Recargar**. Una vez realizados todos los pasos pulsar **Aceptar** para que los cambios de configuración sean permanentes.

- **En Firefox.**

Mozilla Firefox permite configurar el uso de proxy-caché tanto de forma manual como de forma automática, consiguiéndose similares resultados. Se explica a continuación como configurarlo de forma automática para Mozilla Firefox 1.0.4, aunque para otras versiones se hace de manera similar.

### Paso 1

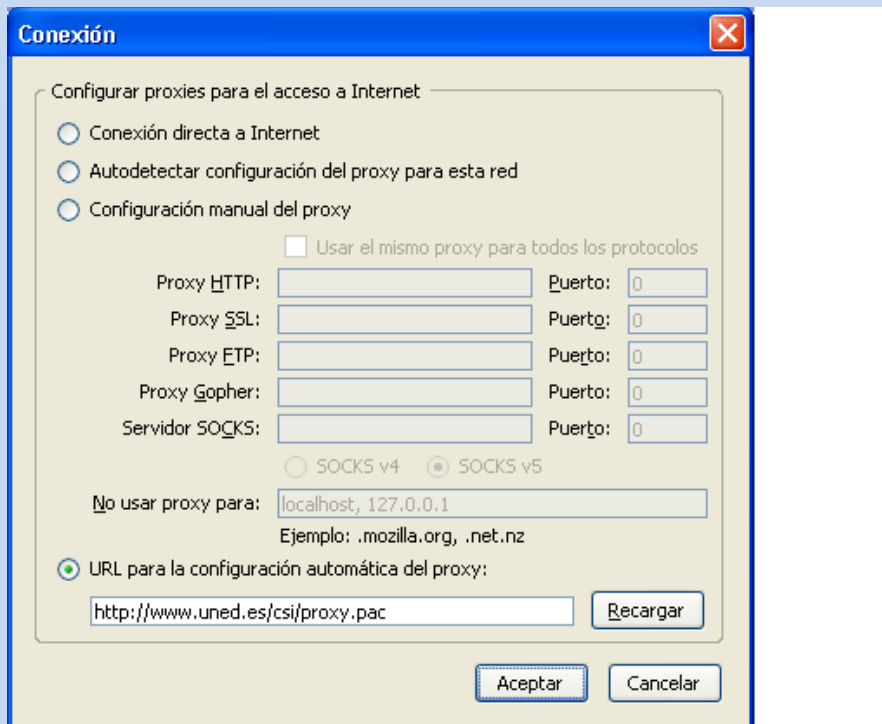
Seleccionar el menú Preferencias situado dentro del menú principal Herramientas (**Herramientas -> Preferencias**)



### Paso 2

Picar en el botón **Configuración de conexión....**

Marcar la cuarta opción "URL para la configuración automática del proxy" y escribir la URL del archivo de configuración automática (<http://www.uned.es/csi/proxy.pac>) en la caja de texto como se indica en el siguiente gráfico:

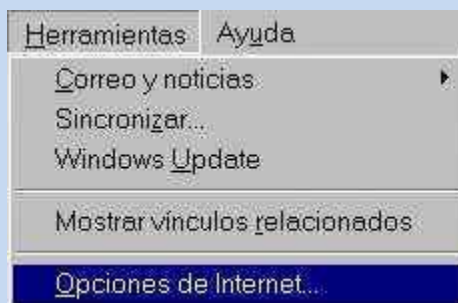


- **En Internet Explorer 5.x conectado a una red de área local.**

Se explica para la versión de Internet Explorer 5.0. La configuración para usar el proxy-caché es distinta si se tiene el ordenador conectado a Internet mediante una tarjeta de red que si se conecta a través de modem. En este apartado se explica la configuración para cuando el ordenador está conectado a una LAN (red de area local). Es decir, el ordenador está conectado en el despacho de la universidad o en casa usando un router ADSL. Si su ordenador se conecta a Internet usando un modem, ya sea modem ADSL o modem tradicional, puede ver cómo configurar el uso de proxy-caché usando modem más adelante.

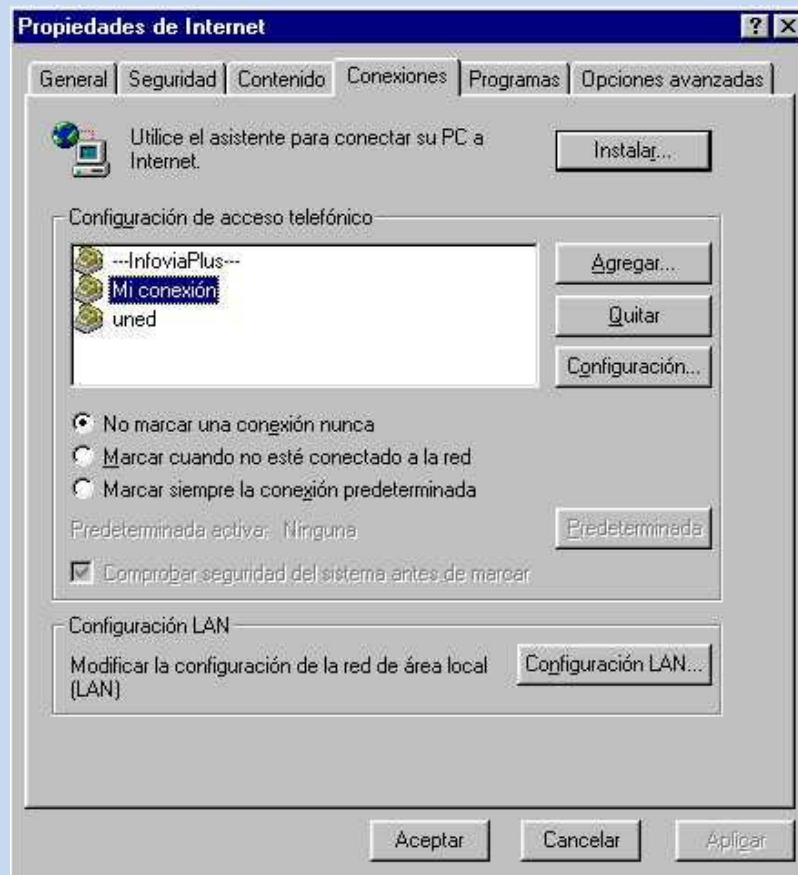
- Paso 1

Seleccionar la entrada de menú Opciones de Internet situado dentro del menú general Herramientas (**Herramientas --> Opciones de Internet**)



Paso 2

En la ventana que aparece activar la pestaña Conexiones y pulsar el botón Configuración LAN... (**Conexiones --> Configuración LAN...**)

Paso 3

Escribir la URL del archivo de configuración automática (<http://www.uned.es/csi/proxy.pac>) en la caja de texto como se indica en el siguiente gráfico:





Una vez realizados todos los pasos pulsar **Aceptar** para que los cambios de configuración sean permanentes.

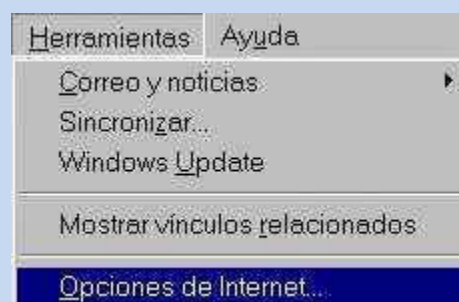
- **En Internet Explorer 5.x conectado a red por modem.**

Se explica para la versión de Internet Explorer 5.0. La configuración para usar el proxy-caché es distinta si se tiene el ordenador conectado a Internet mediante una tarjeta de red que si se conecta a través de modem. En este apartado se explica la configuración para cuando el ordenador está conectado a Internet usando un modem. Es decir, el ordenador está conectado desde casa usando la línea telefónica y un modem ADSL o modem tradicional. Si su ordenador se conecta a Internet a través de LAN puede ver cómo configurar el uso de proxy-caché conectado a una red de área local más arriba.

Agradecer a la profesora Fania Herrero que nos llamara la atención sobre la necesidad de esta documentación y por los gráficos usados a continuación.

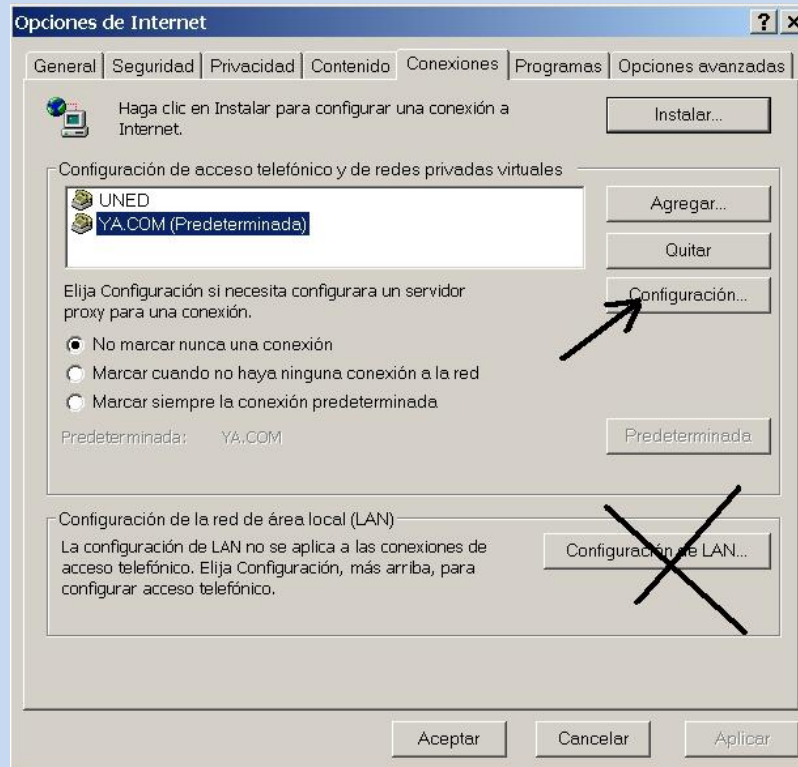
#### Paso 1

Seleccionar la entrada de menú Opciones de Internet situado dentro del menú general Herramientas (**Herramientas --> Opciones de Internet**)



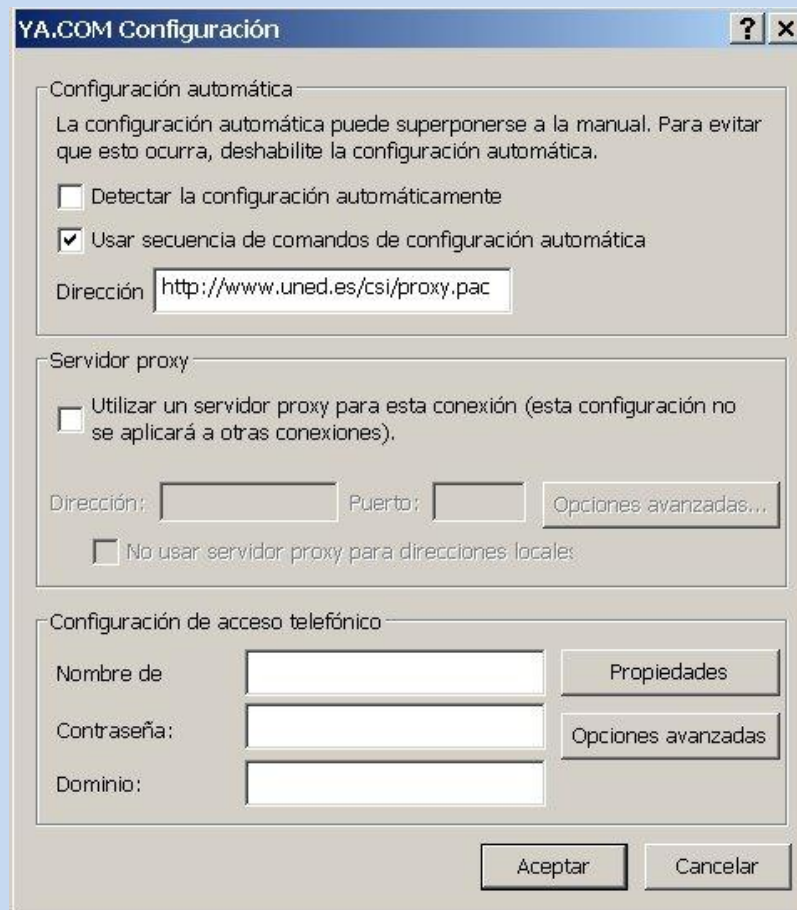
### Paso 2

En la ventana que aparece activar la pestaña Conexiones, marcar en "Configuración de acceso telefónico" la conexión que se usa para conectarse a Internet y pulsar el botón Configuración... (**Conexiones --> Configuración de acceso telefónico --> Configuración...**)



### Paso 3

Marcar "Usar secuencia de comandos de configuración automática" y escribir la URL del archivo de configuración automática (<http://www.uned.es/csi/proxy.pac>) en la caja de texto como se indica en el siguiente gráfico:



Una vez realizados todos los pasos pulsar **Aceptar** para que los cambios de configuración sean permanentes.

## \* Configuración de filtros.

Cuando un ordenador se conecta a Internet, no lo hace de forma directa, sino a través de equipos intermedios. Por un lado están los switches y routers, y por otro los servidores, ordenadores configurados para proporcionar servicios de red (descarga de archivos, obtención de IPs, resolución de nombres de dominio, etc). El tipo de servidor que se analiza en este tutorial es el servidor proxy (o proxy a secas).

Veamos un ejemplo de cómo funciona un proxy. En una red de área local, hay diez ordenadores, uno de los cuales es un proxy. Éste es el único que se conecta directamente a Internet, y a través del cual se conectan todos los demás; del proxy depende íntegramente el acceso de los otros ordenadores a Internet. Si un usuario externo a esta red quisiera rastrear el origen de un paquete de red procedente de uno de estos ordenadores, sólo podría llegar hasta el proxy, ya que es el único que puede crear los paquetes de red.

Debido a estas características, el proxy puede controlar completamente la conexión de red de los equipos que dependan de él. Y esto nos lleva al filtro de contenidos. Un filtro de contenidos es un proxy configurado para limitar el acceso a la red de sus

equipos clientes en base a unos parámetros preestablecidos, mediante una aplicación de filtrado. Se puede utilizar una aplicación para Ubuntu llamada Squid.

### \* Métodos de autenticación en un «proxy».

Como el proxy es una herramienta intermediaria indispensable para los usuarios de una red interna que quieren acceder a recursos externos, a veces se lo puede utilizar para autenticar usuarios, es decir, pedirles que se identifiquen con un nombre de usuario y una contraseña. También es fácil otorgarles acceso a recursos externos sólo a las personas autorizadas y registrar cada uso del recurso externo en archivos de registro de los accesos identificados. Este tipo de mecanismo, cuando se implementa, obviamente genera diversos problemas relacionados con las libertades individuales y los derechos personales. Existen dos conceptos importantes para entender los modos de autenticación.

**Tipo de desafío** (type of challenge): indica el tipo de desafío que se le presentara al cliente.

**Credenciales sustitutas** (surrogate credentials): las credenciales sustitutas son algo que se utiliza para autenticar la transacción en lugar de las credenciales “reales”.

#### modos de Autenticación

**Auto:** el modo default es seleccionado basándonos en la petición que haga el cliente. Auto puede seleccionar cualquier de las opciones, proxy, origin, origin-ip, o origin-cookie-redirect dependiendo en el tipo de conexión (explícita o transparente) y la configuración de la cookie de autenticación en modo transparente.

**Proxy-IP:** El proxy utiliza un desafío en forma explícita y la IP del cliente como credenciales sustitutas. Proxy-IP especifica un forward proxy inseguro. En algunos casos el desafío del proxy no funciona por lo que “origin” desafíos deben de ser generados.

**Origin:** El proxy actúa como una OCS y genera desafíos OCS. La conexión autenticada sirve como credenciales sustitutas.

**Origin-IP:** el proxy actúa como una OCS y genera desafíos OCS. La dirección del cliente es usada como credenciales sustitutas. Origin-IP es usado para soportar autenticación por IWA cuando el cliente no puede manejar credenciales por cookies.

**Origin-Cookie:** El ProxySG actual como un servidor de origen y genera desafíos de servidor de origen. Una cookie es generada como credenciales sustitutas. Origin-Cookie es usado en forward proxies para soportar autenticación pass-through de manera más segura que Origin-IP si el cliente entiende cookies. Solamente los protocolos HTTP y HTTPS soportan cookies; todos los demás protocolos son degradados a utilizar automáticamente Origin-IP.

**Origin-cookie-redirect:** El cliente es redirigido a una URL Virtual para ser autenticado, y las cookies son usadas como credenciales sustitutas. El Proxy SG no soporta Origin-Redirect con el método de CONNECT. Para forward proxy, solamente modos origin-\*

redirect son soportados para autenticación por Kerberos/IWA. (Cualquier otro modo utiliza NTLM)

**SG2:** Este modo es seleccionado automáticamente, basando en la petición, y usa las reglas definidas del SGOS 2.x.

**From-IP:** una forma es presentada para recolectar las credenciales del usuario. La forma es presentada cada vez que el caché de las credenciales del usuario expiren.

**From-Cookie:** Una forma es presentada para coleccionar las credenciales del usuario. Las cookies son setiadas en el dominio OCS solamente y el usuario es presentado con una nueva forma para cada dominio. Este modo es más utilizado en escenarios de proxy reverso donde hay un número limitado de dominios.

**From-Cookie-Redirect:** Una forma es presentada para coleccionar las credenciales del usuario. El usuario es re direccionado a la URL Virtual antes de ser presentada la forma. La cookie de autenticación es setiada en ambos, la URL Virtual y el dominio OSC. El usuario es desafiado solamente cuando el cache de las credenciales expira.

**From-IP-Redirect:** Este es similar a From-IP con la excepción que el usuario es re direccionado a la URL Virtual de autenticación antes que la forma sea presentada.

#### **REGLAS BASICAS.**

- 1) No utilice Credenciales sustitutas por IP a menos que sea absolutamente necesario. Si usted tiene NAT o un sistema multiusuario no puede utilizar este modo.
- 2) Para un forward proxy, el modo default es "Auto" y la opción por default de la configuración de autenticación es por "cookies", de esta forma funciona de la mejor manera y con menos problemas.
- 3) Para usar SSL en la autenticación en un forward proxy, usted tiene que usar los desafíos por Origin-Redirect u Origin-Cookie-Redirect siendo este ultimo el más recomendado.
- 4) Para configuraciones en proxies reversos, use "origen". Si el server de origen también necesita autenticar al usuario y no puede ser modificado para usar un trusted header, use "Origin-Cookie".

#### **\* «proxys» inversos.**

Un **proxy inverso** es un servidor proxy-caché "al revés". Es un servidor proxy que, en lugar de permitirles el acceso a Internet a usuarios internos, permite a usuarios de Internet acceder indirectamente a determinados servidores internos.

El servidor de proxy inverso es utilizado como un intermediario por los usuarios de Internet que desean acceder a un sitio web interno al enviar sus solicitudes indirectamente. Con un proxy inverso, el servidor web está protegido de ataques externos directos, lo cual fortalece la red interna. Además, la función caché de un proxy inverso puede disminuir la carga de trabajo del servidor asignado, razón por la cual se lo denomina en ocasiones acelerador de servidor. Finalmente, con algoritmos

perfeccionados, el proxy inverso puede distribuir la carga de trabajo mediante la redirección de las solicitudes a otros servidores similares. Este proceso se denomina equilibrio de carga. Hay varias razones para instalar un "reverse proxy":

**Seguridad:** el servidor proxy es una capa adicional de defensa y por lo tanto protege los servidores web.

**Cifrado / Aceleración SSL:** cuando se crea un sitio web seguro, habitualmente el cifrado SSL no lo hace el mismo servidor web, sino que es realizado por el "reverse proxy", el cual está equipado con un hardware de aceleración SSL (Security Sockets Layer).

**Distribución de Carga:** el "reverse proxy" puede distribuir la carga entre varios servidores web. En ese caso, el "reverse proxy" puede necesitar reescribir las URL de cada página web (traducción de la URL externa a la URL interna correspondiente, según en qué servidor se encuentre la información solicitada).

**Caché de contenido estático:** Un "reverse proxy" puede descargar los servidores web almacenando contenido estático como imágenes u otro contenido

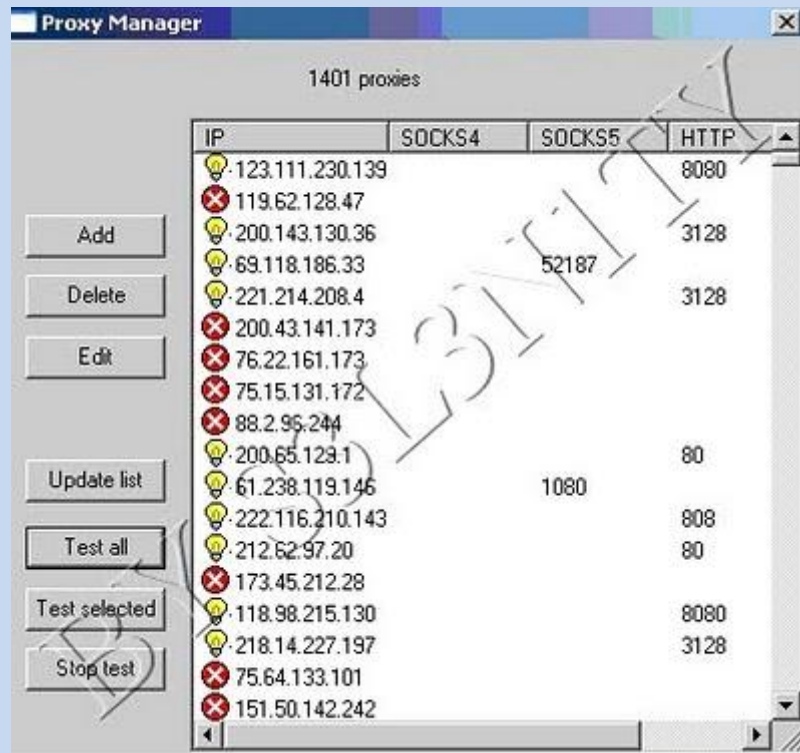
### \* «proxys» encadenados.

Pues ahora vamos a rizar el rizo usando proxys encadenados por lo que incrementaremos el anonimato respecto a las formas que hemos visto hasta ahora, aunque ello también significa que ralentizaremos más nuestra navegación porque usaremos varios intermediarios por lo que el recorrido de la señal es mas largo, debemos tener esto en cuenta para elegir el procedimiento adecuado dependiendo de cada ocasión.

Para ello vamos a utilizar un programa que nos servirá para encadenar los proxies, en este caso usare SocksChain, pero hay más programas.

La ventaja que tiene este programa es que nos facilita la tarea de comprobar los proxies y tampoco tenemos que buscar la lista porque nos rastrea el mismo desde varios servidores, así que lo único que tenemos que hacer para echar a andar el programa es hacer clic en **tool**, luego en **Proxy manager** para empezar a buscar y a testear proxys





Hacemos clic en **update list** y comenzaran a aparecer proxys, a continuación **test all** y se mostraran los validos con una bombilla amarilla y los inservibles con un asterisco en rojo ,en cuanto tengamos 10 o 15 validos (bombillas) podemos borrar el resto.

Ahora solo tenemos que ir a nuestro navegador y configurar la conexión de red donde dice IP **127.0.0.1** y el puerto **1081** y ya estamos navegando mediante encadenamiento de proxys, cuanto mas largo mas difícil se hace el rastreo pero también más lenta se vuelve la conexión.

### Reverse Proxy / Proxy inverso

Un *reverse proxy* es un servidor proxy instalado en el domicilio de uno o más servidores web. Todo el tráfico entrante de Internet y con el destino de uno de esos servidores web pasa a través del servidor proxy. Hay varias razones para instalar un "reverse proxy":

- Seguridad: el servidor proxy es una capa adicional de defensa y por lo tanto protege los servidores web.
- Cifrado / Aceleración SSL: cuando se crea un sitio web seguro, habitualmente el cifrado SSL no lo hace el mismo servidor web, sino que es realizado por el "reverse proxy", el cual está equipado con un hardware de aceleración SSL (Security Sockets Layer).
- Distribución de Carga: el "reverse proxy" puede distribuir la carga entre varios servidores web. En ese caso, el "reverse proxy" puede necesitar reescribir las URL de cada página web (traducción de la URL externa a la URL interna correspondiente, según en qué servidor se encuentre la información solicitada).

- Caché de contenido estático: Un "reverse proxy" puede descargar los servidores web almacenando contenido estático como imágenes u otro contenido gráfico.

### **Proxy NAT (Network Address Translation) / Enmascaramiento**

Otro mecanismo para hacer de intermediario en una red es el NAT.

La traducción de direcciones de red (NAT, Network Address Translation) también es conocida como enmascaramiento de IPs. Es una técnica mediante la cual las direcciones fuente o destino de los paquetes IP son reescritas, sustituidas por otras (de ahí el "enmascaramiento").

Esto es lo que ocurre cuando varios usuarios comparten una única conexión a Internet. Se dispone de una única dirección IP pública, que tiene que ser compartida. Dentro de la red de área local (LAN) los equipos emplean direcciones IP reservadas para uso privado y será el proxy el encargado de traducir las direcciones privadas a esa única dirección pública para realizar las peticiones, así como de distribuir las páginas recibidas a aquel usuario interno que la solicitó. Estas direcciones privadas se suelen elegir en rangos prohibidos para su uso en Internet como 192.168.x.x, 10.x.x.x, 172.16.x.x y 172.31.x.x

Esta situación es muy común en empresas y domicilios con varios ordenadores en red y un acceso externo a Internet. El acceso a Internet mediante NAT proporciona una cierta seguridad, puesto que en realidad no hay conexión directa entre el exterior y la red privada, y así nuestros equipos no están expuestos a ataques directos desde el exterior.

Mediante NAT también se puede permitir un acceso limitado desde el exterior, y hacer que las peticiones que llegan al proxy sean dirigidas a una máquina concreta que haya sido determinada para tal fin en el propio proxy.

La función de NAT reside en los Cortafuegos y resulta muy cómoda porque no necesita de ninguna configuración especial en los equipos de la red privada que pueden acceder a través de él como si fuera un mero encaminador..

### **Proxy abierto**

Este tipo de proxy es el que acepta peticiones desde cualquier ordenador, esté o no conectado a su red.

En esta configuración el proxy ejecutará cualquier petición de cualquier ordenador que pueda conectarse a él, realizándola como si fuera una petición del proxy. Por lo que permite que este tipo de proxy se use como pasarela para el envío masivo de correos de spam. Un proxy se usa, normalmente, para almacenar y redirigir servicios como el DNS o la navegación Web, mediante el cacheo de peticiones en el servidor proxy, lo que mejora la velocidad general de los usuarios. Este uso es muy beneficioso, pero al



aplicarle una configuración "abierta" a todo internet, se convierte en una herramienta para su uso indebido.

Debido a lo anterior, muchos servidores, como los de IRC, o correo electrónicos, deniegan el acceso a estos proxys a sus servicios, usando normalmente listas negras ("BlackList").

### \* Pruebas de funcionamiento. Herramientas gráficas.

Para comprobar si nuestro sistema está funcionando bajo un proxy podemos realizar algunas pruebas, para ello existen innumerables herramientas on line o descargándolas con las que podemos ver el funcionamiento.

Una de ellas es la que se presenta a continuación:

