Instalación y configuración de servidores proxy

Seguridad y Alta Disponibilidad

Autor: Miguel Ángel García Felipe

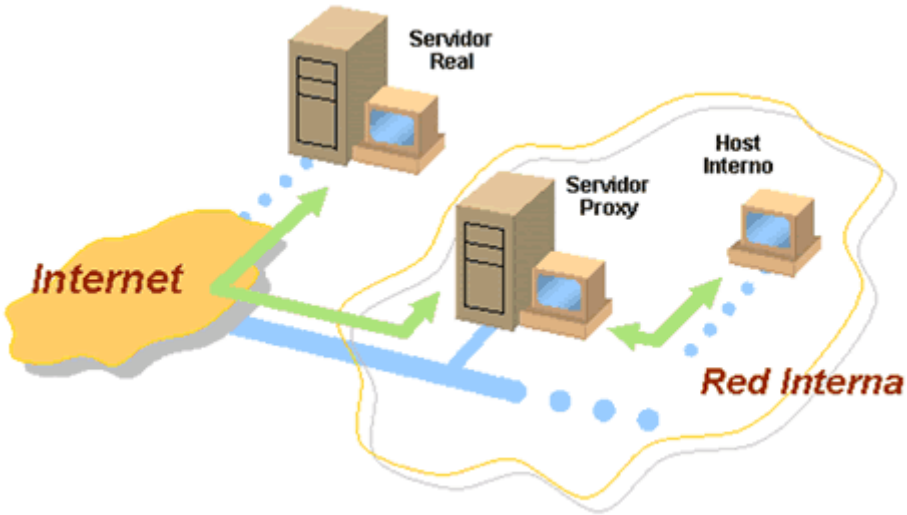
I.E.S GREGORIO PRIETO

ÍNDICE:

- **Servidores proxy:**

Los proxies son máquinas que tienen como misión distribuir el tráfico en la red, de tal manera que las conexiones que se solicitan desde un ordenador local a Internet, pueden dirigirse hacia un servidor o hacia otro según la carga solicitada.

Los proxies instalados en una red también tienen una función "caché". Cuando se solicita una conexión a la red (URL), la página que se ha "bajado" hasta el ordenador a través del navegador, se guarda en la memoria de ese servidor proxy durante un periodo de tiempo y así, cuando se vuelve a solicitar esa dirección desde otro ordenador de la red, el servidor proxy le ofrece la página que tiene guardada en la memoria, consiguiendo una mayor velocidad de respuesta y un ahorro en el tráfico de la red.



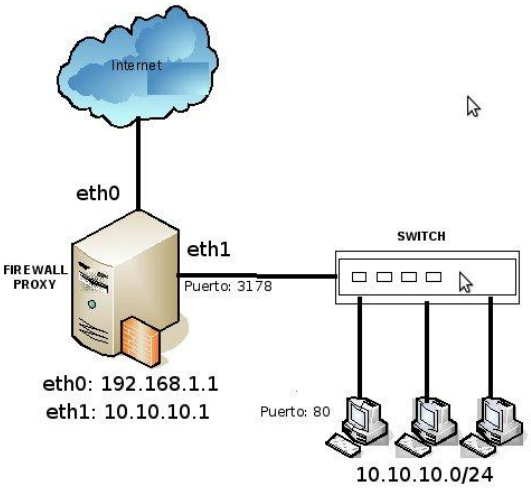
Un **servidor proxy** es un equipo que actúa de intermediario entre un explorador web (como Internet Explorer) e Internet. Los servidores proxy ayudan a mejorar el rendimiento en Internet ya que almacenan una copia de las páginas web más utilizadas. Cuando un explorador solicita una página web almacenada en la colección (su caché) del servidor proxy, el servidor proxy la proporciona, lo que resulta más rápido que consultar la Web. Los servidores proxy también ayudan a mejorar la seguridad, ya que filtran algunos contenidos web y software malintencionado.

Los servidores proxy se utilizan a menudo en redes de organizaciones y compañías. Normalmente, las personas que se conectan a Internet desde casa no usan un servidor proxy.

- **Tipos de «proxy».**

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).

Revela todos tus datos, solamente se utiliza para mejorar la velocidad de descarga.

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).

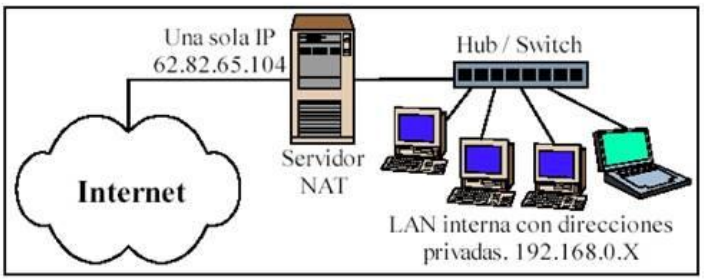
- **Distribución de Carga:** el "reverse proxy" puede distribuir la carga entre varios servidores web. En ese caso, el "reverse proxy" puede necesitar reescribir las URL de cada página web (traducción de la URL externa a la URL interna correspondiente, según en qué servidor se encuentre la información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

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

Proxy NAT/ 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.

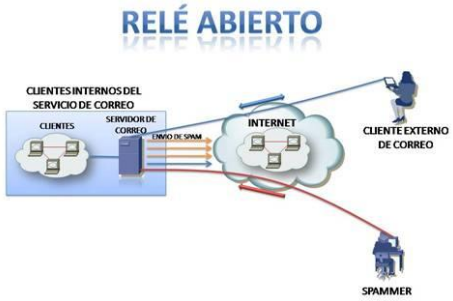
La función de NAT reside en los Cortafuegos y resulta muy cómoda porque no necesita de ninguna configuración especial en los equipos de la red privada que pueden acceder a través de él como si fuera un mero encaminador.

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 todointernet, 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 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.

Proxies anónimos

Estos proxies ocultan la dirección ip del cliente proporcionando una forma de navegar anónima, (No envía ninguna variable mostrando tu IP, pero si avisa que estas utilizando un proxy). La forma en que ocultan la dirección ip del cliente hace que un proxy se clasifique en una de las siguientes categorías:

- **Simples:** No se oculta el hecho de que se está utilizando un proxy, únicamente se guarda la dirección ip del proxy en ambos cabeceras, sin que aparezca por ningún sitio la del cliente.

- **Proxys ruidosos:** Son similares al anterior caso con la salvedad de que en vez de guardar su dirección ip, guardan una generada aleatoriamente.

- **Proxys de alta anonimicidad:** Este tipo de proxys oculta el hecho de que se esté utilizando un proxy para realizar la petición. Para ello sustituyen la dirección IP existente y no lo indican mediante ninguna otra cabecera, por lo que no es posible saber que se está utilizando un proxy (No envían ninguna variable de ningún tipo a nadie).

- Características.

Las características más importantes son:

- Permite definir los permisos que tienen los usuarios de la red interna sobre los servicios, dominios, IP externas.

- Todos los usuarios de la red interna comparten una única dirección IP de forma que desde el exterior no se puede diferenciar a unos de otros.

- Puesto que todo el tráfico que circula de la red interna hacia internet y viceversa pasa por el proxy, se puede auditar el uso que se hace de internet.

- Permite almacenar las páginas recientemente consultadas en una cache para aumentar el rendimiento de la red. Por ejemplo, la página que se almacena en la caché de un proxy para que al recibir la petición cargue más rápido.

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.

Ventajas

En general (no sólo en informática), los proxies hacen posible:

- **Control**: sólo el intermediario hace el trabajo real, por tanto se pueden limitar y restringir los derechos de los usuarios, y dar permisos sólo al proxy.

- **Ahorro**. Por tanto, sólo *uno* de los usuarios (el proxy) ha de estar equipado para hacer el trabajo real.

- **Velocidad**. Si varios clientes van a pedir el mismo recurso, el proxy puede hacer caché: guardar la respuesta de una petición para darla directamente cuando otro usuario la pida. Así no tiene que volver a contactar con el destino, y acaba más rápido.

- **Filtrado**. El proxy puede negarse a responder algunas peticiones si detecta que están prohibidas.

- **Modificación**. Como intermediario que es, un proxy puede falsificar información, o modificarla siguiendo un algoritmo.

- **Anonimato**. Si todos los usuarios se identifican como uno sólo, es difícil que el recurso accedido pueda diferenciarlos. Pero esto puede ser malo, por ejemplo cuando hay que hacer necesariamente la identificación.

Desventajas

En general (no sólo en informática), el uso de un intermediario puede provocar:

- **Abuso.** Al estar dispuesto a recibir peticiones de muchos usuarios y responderlas, es posible que haga algún trabajo que no toque. Por tanto, ha de controlar quién tiene acceso y quién no a sus servicios, cosa que normalmente es muy difícil.

- **Carga.** Un proxy ha de hacer el trabajo de muchos usuarios.

- **Intromisión.** Es un paso más entre origen y destino, y algunos usuarios pueden no querer pasar por el proxy. Y menos si hace de cachéy guarda copias de los datos.

- **Incoherencia.** Si hace de caché, es posible que se equivoque y dé una respuesta antigua cuando hay una más reciente en el recurso de destino. En

realidad este problema no existe con los servidores proxy actuales, ya que se conectan con el servidor remoto para comprobar que la versión que tiene en cache sigue siendo la misma que la existente en el servidor remoto.

- **Irregularidad.** El hecho de que el proxy represente a más de un usuario da problemas en muchos escenarios, en concreto los que presuponen una comunicación directa entre 1 emisor y 1 receptor (como TCP/IP).

- Funcionamiento.

Entenderemos fácilmente como funciona un proxy si tenemos claro cómo funciona Internet. Internet está basado en el **modelo Cliente-Servidor**. A grandes rasgos, un usuario (cliente) hace una solicitud (petición de un archivo) al Servidor, que devolverá una respuesta (el archivo). Para ello, el servidor web requiere una información adicional. Esta información es transmitida al servidor por un navegador o un servidor proxy.

Generalmente, lo que solicita el servidor es:

- Nombre y versión del **SO**
- Nombre y versión del **navegador**
- **Configuración** del navegador (resolución de pantalla, profundidad de color, si existe soporte para java / javascript…).
- Dirección **IP** del cliente
- Otra información

Así, el término proxy hace referencia a cualquier dispositivo o aplicación que hace de **intermediario** entre un ordenador conectado a Internet y el servidor al que se conecta. *Su uso más común es permitir la conexión a Internet de varios equipos conectados en red a través de uno que es el que está conectado realmente a Internet.*

Pero, los proxy's tienen otros usos interesantes para los "navegantes". En ciertas ocasiones, por tema de **rendimiento** es conveniente conectarse a través de un proxy web que es un dispositivo que se encuentra "más cerca" que el servidor al nos queremos conectar. Este dispositivo va almacenando en caché la información de las páginas que visitamos, de forma que la primera vez este proxy sí que hace la solicitud al servidor. Pero, si varias personas se conectan a páginas ya almacenadas en caché no es necesario hacer la solicitud al servidor con la consiguiente mejora de rendimiento.

Otras veces, por temas de seguridad, confidencialidad o **anonimato** queremos visitar ciertas páginas sin que se conozca nuestra dirección IP, que es nuestra identidad en Internet. Aquí es donde entran en funcionamiento los proxy's anónimos.

A grandes rasgos, según el nivel de **anonimicidad** podemos clasificar los proxy's en:

- **Públicos**, no ocultan la identidad.
- **Anónimos**, ocultan la identidad pero te delatan en la intención, ya que muestran que te conectas a través de proxy.
- **Élite** o high-anonymous, utilizados para ocultar la identidad y además ocultar que estás tras un proxy.

- Instalación de servidores «proxy».

Vamos a ver un ejemplo de instalación del servidor proxy Squid en Linux.

Para instalar Squid escribe en un terminal:

- **sudo aptitude install squid**

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**

Squid necesita conocer el nombre de la máquina. Para ello, ubica la línea visible_hostname.

Por ejemplo, si la máquina se llama "ubuntu", ponemos:

- **visible_hostname ubuntu**

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**

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**

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**

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**

Por defecto, Squid sólo autoriza el trafico 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 seria 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**

(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.

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

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)

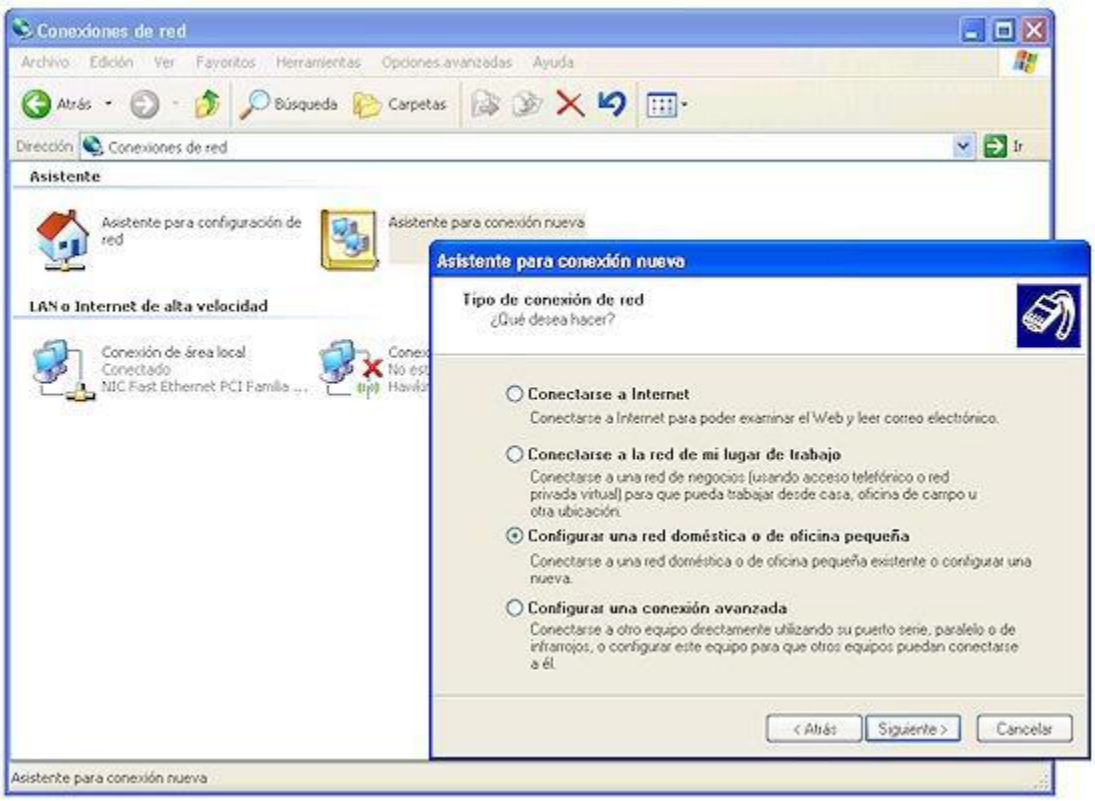
- **cache_dir ufs /var/spool/squid 200 16 256**

- Instalación y configuración de clientes «proxy».

Cómo configurar el Proxy de Windows XP

PASO 1. Configuración del PC que hará de servidor

- Para ello, pulsamos en "**Inicio**", "**Configuración**", "**Panel de control**" y ejecutamos "**Conexiones de red**".
- Ejecutamos la opción "*Configurar una red doméstica o para pequeña oficina*". Entonces, aparecerá un asistente para configuración de red, pulsamos "**Siguiente**". Comprobamos que cumplimos los requisitos, es decir, tenemos un adaptador de red, módem u otro tipo de dispositivo utilizado para la conexión a Internet y estamos conectados en este momento a Internet.



- En la siguiente ventana, marcamos la primera opción "*Este equipo se conecta directamente a Internet. Los otros equipos de mi red se conectan a Internet a través de este equipo*". Pulsamos "**Siguiente**".
- Escogemos la conexión a Internet que estamos utilizando, y "**Siguiente**".
- Seleccionamos el adaptador de red (u otro dispositivo) mediante el cual se conecta el equipo con los demás de la red local (LAN).
- Introducimos la descripción del equipo y el nombre. Y en la siguiente ventana, el grupo de trabajo para la red y "**Siguiente**".

- Es importante que si queremos permitir que los otros equipos puedan acceder a carpetas e impresoras compartidas del PC que hace de Servidor de Proxy marquemos la primera opción: "*Activar el uso compartido de archivos e impresoras*".
- En la última ventana nos aparece un resumen de las opciones seleccionadas, pulsamos "**Siguiente**" si todo es correcto.

PASO 2. Configuración de la red

- En este momento, el asistente inicia el proceso de configuración de la red.
- Tras la configuración nos aparece una ventana que nos permite la posibilidad de crear un disco de configuración de red para ejecutarlo en los PC's clientes. Pulsamos en "*Crear Disco de configuración de red*", introducimos un disquete formateado y vacío. Y "**Siguiente**".
- Tras la creación del disquete de configuración nos aparece una última ventana indicando que el proceso ha finalizado. También nos indica los pasos necesarios para configurar los demás equipos de la red mediante el disquete creado. Es necesario reiniciar el PC Servidor para finalizar con la configuración.

- Para consultar la configuración de red que ha dejado el asistente, pulsamos el botón derecho del ratón sobre "**Mis sitios de red**" y "**Propiedades**". Seleccionamos la tarjeta de red que utilizamos para la conexión entre los equipos de nuestra red y pulsamos con el botón derecho del ratón, "**Propiedades**". Seleccionamos "**Protocolo Internet (TCP/IP)**" y pulsamos en "**Propiedades**". El asistente configura como dirección IP del equipo que hará de servidor Proxy, la dirección 192.168.0.1 y la máscara de subred: 255.255.255.0.

PASO 3. Configuración de los equipos clientes

- Introducimos el disquete, generado en el proceso de configuración del Servidor Proxy, en cada equipo y accederemos a la unidad A: para ejecutar el fichero "*netsetup.exe*". Se abrirá el asistente de configuración.
- En este paso seleccionamos "*Este equipo se conecta a Internet a través de una puerta de enlace residencial o de otro equipo de mi red*".

- Tras la finalización del asistente, reiniciamos el equipo y probamos la conexión a Internet.

- En este caso, el asistente marca todas las opciones como **automáticas** para que las IP's y la puerta de enlace se asignen automáticamente (las asignará el Servidor Proxy). Si queremos ver la IP que le ha asignado el Servidor Proxy al equipo cliente podemos hacerlo pulsando en "**Inicio**" – "**Ejecutar**" y escribiendo

"*cmd*", y "**Aceptar**". Nos aparece una ventana de consola donde escribimos el comando "*ipconfig*" y pulsamos "**Enter**". Este comando nos mostrará la configuración de la red, algo de este estilo:

- IP: 192.168.0.48
- Puerta de enlace: 192.168.0.1 (la del equipo Servidor Proxy).

Una de las **ventajas** más importantes del Proxy de Windows XP es que funcionará casi cualquier tipo de aplicación que utilice Socket (conexión directa puerto a puerto), POP3, SMTP y cualquier otro programa que utilice vías de conexión a Internet diferentes al protocolo HTTP. Además, no se necesita ningún software adicional. Como **inconveniente** resaltar que se tienen que cambiar todas las direcciones IP's de la red, utilizando el rango 192.168.0.xxx.

- Configuración del almacenamiento en la caché de un «proxy».

En su configuración por defecto de costumbre, Squid utiliza un solo directorio para almacenar páginas en caché. En la mayoría de 100 MB de datos se almacenan en este directorio, que no es probable que sea suficiente si actúa un gran número de clientes activos. Si su sistema tiene más de un disco duro, tiene sentido para difundir la memoria caché a través de múltiples discos para mejorar el rendimiento. Esto puede hacerse mediante la especificación de varios directorios, cada una con su propio tamaño máximo.

En un sistema que se dedica a ejecutar un servidor Proxy, el importe máximo de caché en cada directorio debe ser aproximadamente el 90% del espacio disponible. Es imprudente o configurar Squid para permitir utilizar todo el espacio libre en disco, ya que muchos sistemas de ficheros sufren menor rendimiento. Por otra parte, el espacio en disco puede ser utilizado por los archivos de registro y datos del usuario. Si Squid llena todo el disco duro, los problemas pueden ocurrir debido a otros programas no son capaces de crear archivos temporales o escribir registros.

Para añadir un nuevo directorio de memoria caché y especificar el tamaño máximo de la ya existente, siga estos pasos:

1. Haga clic en el icono Opciones de caché en el módulo de la página principal de educar a la forma en que la captura de pantalla a continuación.

2. En el campo de caché directorios, seleccione la opción de publicación. Si fue elegido por defecto antes, Squid se han estado utilizando el único compilado en caché por defecto en el directorio que aparece entre paréntesis. Si desea seguir utilizando este directorio, debe ser explícitamente incluido en el cuadro. El tamaño predeterminado es de 100 MB, y utiliza 16 1 ª y 2 ª nivel de 256 directorios. Cada fila de la tabla se especifica un único directorio de memoria caché. Todos los directorios

existentes (aparte de por defecto) se enumeran de manera que se puede editar, seguida de una sola fila en blanco. Cada fila tiene campos en las siguientes columnas:

- Directorio de la ruta completa al más alto nivel directorio de memoria caché, por ejemplo, **/var/spool/squid/** o **disk2/cache**. Este directorio debe existir y ser propiedad de la utilización que se ejecuta como Squid (generalmente llamado Squid) - el módulo no lo va a crear para usted.
- El tipo de almacenamiento de tipo de las utilizadas en el directorio. Siempre debe seleccionar UFS aquí.
- Tamaño (MB) La máxima cantidad de datos que contendrá, en megabytes. Una vez se alcanza este límite, la más antigua-pidió a los archivos serán sustituidos por otros nuevos.
- 1er nivel dirs El número de subdirectorios que se creará bajo el directorio de memoria caché. El valor predeterminado de 16 es por lo general bien, pero es posible que desee aumentar este caso de grandes alijos.
- 2 º nivel dirs El número de subdirectorios que serán creados en virtud de cada una de primer nivel de directorio. Usted debe entrar sólo 256 menos que su caché va a ser muy grandes.
- Opciones Deje este campo en blanco - sólo se utiliza para otros tipos de directorios. Si se preguntan por qué Squid tiene que crear dos niveles en virtud de los subdirectorios de cada directorio de memoria caché, la razón es el bajo rendimiento de muchos sistemas de ficheros cuando un directorio contiene una gran cantidad de archivos. Dado que cada página HTML en caché o la imagen se almacena en un archivo separado, el número de archivos en un sistema ocupado Proxy puede ser enorme. Difundir a través de varios directorios resuelve este problema.

3. Después de añadir un directorio, haga clic en el botón Guardar en la parte inferior de la página. Si desea añadir más de uno tendrá que hacer clic en el icono Opciones de caché de nuevo para volver a mostrar la tabla con una nueva fila vacía.

4. Cuando haya terminado de definir los directorios, regreso al módulo de la página principal. Si uno nuevo se ha añadido, un mensaje de error al igual que su cache Squid directorios no han sido inicializadas se mostrará. Haga clic en el botón Iniciar Cache Squid para tener crear todas las sub-directorios en los nuevos directorios de caché. El servidor se apaga durante el proceso, y volver a comenzar cuando se ha completado.

5. Después de la inicialización está completa, haga clic en Aplicar cambios el vínculo en cualquier página para empezar a utilizar sus nuevos directorios.

- Configuración de filtros.

DansGuardian es un filtro directo que se ubica entre el el cliente Web (web browser) y el Servidor Proxy Squid. Dansguardian acepta conexiones en el puerto 8080 y se

conecta a squid en el puerto 3128. Por lo tanto, es importante que no haya otro servicio utilizando el puerto 8080.

Si lo que se desea es poder filtrar por contenido lo que se navega en tu red, DansGuardian te puede ayudar a poder poner las reglas de la navegación, solo se debe parametrizar al gusto y trabaja en conjunto con Squid.

La herramienta DansGuardian es código abierto, está desarrollada en C++ y permite una configuración flexible adaptándose a las necesidades del usuario.

Al instalar el paquete la configuración por defecto ya limita las visitas a páginas prohibidas para menores, pero dispone de gran cantidad de archivos de configuración para llevar a cabo un ajuste del servicio más personalizado.

El mecanismo es el siguiente: los clientes mediante sus navegadores web hacen peticiones de páginas que son recibidas por DansGuardian y sólo son redireccionadas al servidor proxy SQUID aquellas que superan la fase de filtrado.

Cliente web -> DansGuardian -> Squid -> servidor En realidad DansGuardian se ejecuta como un demonio independiente del proxy, acepta peticiones en el puerto 8080 y las redirecciona al proxy SQUID, que escucha en el puerto 3128.

Por lo tanto, cuando una petición entra por el puerto 8080, DansGuardian la filtra y la pasa al proxy SQUID por el puerto 3128.

Es importante, en consecuencia, que ningún otro servicio esté utilizando el puerto 8080.

Si el resultado del filtrado (dependiendo de los filtros configurados) es una denegación de acceso a una determinada página web se muestra al usuario el mensaje correspondiente al 'Acceso Denegado'.

Si DansGuardian está en la máquina que hace de cortafuegos y se configura un proxy transparente1 en SQUID, habrá que redireccionar todo el tráfico saliente en el cortafuegos del puerto 80 al puerto 8080. Es decir, se capturan todas las peticiones que se hagan a un servidor http (petición de páginas web) y se envían a DansGuardian (8080) para que se encargue del filtrado.

INTALACION Y CONFIGURACION

En primer lugar vamos a instalar Dansguardian en nuestra máquina, desde un terminal tecleamos:

- **sudo apt-get install dansguardian**

Ya tenemos Dansguardian instalado en nuestra máquina.

Configuración

Una vez instalado, pasamos a configurarlo. Para ello abrimos el fichero **/etc/dansguardian/dansguardian.conf.**

- **sudo gedit /etc/dansguardian/dansguardian.conf**

En primer lugar vamos a ponerlo en castellano, buscamos la directiva language, y la dejamos así:

- **language = 'spanish'**

Ahora vamos a comentar una línea del archivo, en la que indicamos a Dansguardian que ya está configurado por nosotros, el hecho de no comentar esta línea supone un modesto recordatorio cuando reiniciamos Dansguardian.

La línea en concreto es la siguiente:

- **# UNCONFIGURED - Please remove this line after configuration**

Debemos dejarla como en la imagen, con # delante. Eso hará que la línea esté comentada, y por lo tanto omitida para Dansguardian.

Otras directivas a tener en cuenta

Hay otras directivas importantes, que no vamos a configurar, pero que si vamos a comentar porque hay que tenerlas muy en cuenta a la hora de configurar Dansguardian. Dichas directivas son:

- ***filterport = 8080***: Esta directiva define el puerto que usará Dansguardian para filtrar.
- ***proxyip = 127.0.0.1***: Esta directiva define la dirección IP de nuestro proxy.
- ***proxyport = 3128***: Esta directiva define el puerto que usa nuestro proxy.

Restringiendo contenidos

Ahora vamos a restringir el contenido de una página web, de un formato y de un límite de palabras prohibidas. Esto será lo que vamos a prohibir:

- ***www.minijuegos.com***
- ***formato *.exe***
- ***juegos***

Pasemos a prohibir la página web, en primer lugar abrimos con un editor de textos el fichero**/etc/dansguardian/lists/bannedsitelist**, desde un terminal escribimos:

- **sudo gedit /etc/dansguardian/lists/bannedsitelist**

Cuando tenemos el archivo abierto, nos vamos a la zona #List other sites to block: y añadimos la página web que queremos bloquear, en nuestro caso, www.minijuegos.com.

Ahora vamos a prohibir la descarga de archivos .exe. Las extensiones prohibidas están en el fichero /etc/dansguardian/lists/bannedextensionlist, para editarlo nos vamos a un terminal y tecleamos:

- **sudo gedit /etc/dansguardian/lists/bannedextensionlist**

En ese archivo tenemos todas las extensiones para los archivos que Dansguardian no permite descargar. Por defecto vienen la gran mayoría prohibidos, lo que vamos a hacer es comentarlos todos menos el que queremos prohibir, la extensión .exe.

Ya tenemos prohibidas las descargas de archivos .exe, vamos ahora a prohibir la entrada a páginas que contengan la expresión “juegos“.

Desde un terminal abrimos el archivo /etc/dansguardian/lists/bannedphraselist

sudo gedit /etc/dansguardian/lists/bannedphraselist

Ahora nos vamos al final del fichero, y añadimos la palabra que queremos prohibir, guardamos los cambios y listo.

Ahora toca reiniciar Dansguardian para que los cambios surtan efecto, desde un terminal tecleamos:

- **sudo /etc/init.d/dansguardian restart**

Verificando el funcionamiento

Vamos ahora a comprobar que todos las modificaciones que hemos realizado son correctas, para ello necesitamos abrir el Mozilla Firefox, a entrar en minijuegos.com y descargar un archivo .exe.

Al entrar en minijuegos.com ocurriría lo siguiente:

Al intentar descargar un archivo .exe, Dansguardian nos mostraría el siguiente error.

Para modificar el template de Dansguardian el directorio se encuentra en ***/etc/dansguardian/languages/spanish/template.html.***

- **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 (explicita 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 específica 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 Origen-IP si en 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 colectar 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 colectar 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.

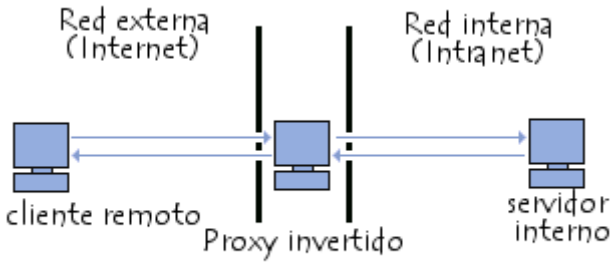
2) Para un forward proxy, el modo default es “Auto” y la opción por default de la configuración de autenticación es por “cookies”, de esta forma funciona de la mejor manera y con menos problemas.

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.

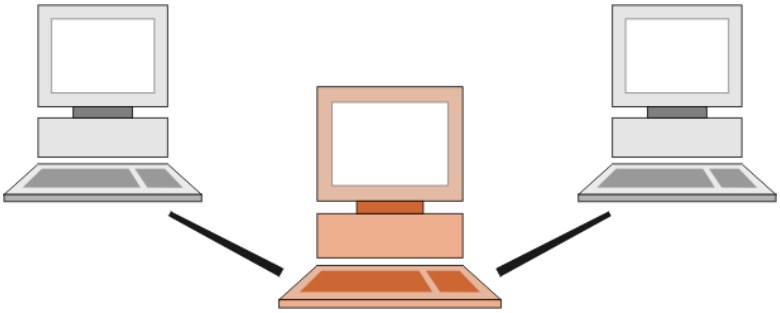
- **Cifrado / Aceleración SSL:** cuando se crea un sitio web seguro, habitualmente el cifrado SSL no lo hace el mismo servidor web, sino que es realizado por el "reverse proxy", el cual está equipado con un hardware de aceleración SSL (Security Sockets Layer).

- **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 gráfico.

- **«proxys» encadenados.**

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 más 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 paraempezar a buscar y a testear proxysHacemos 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 más largo mas difícil se hace el rastreo pero también más lenta se vuelve la conexión.

- **Pruebas de funcionamiento. Herramientas gráficas**

- Squid 2.7, no posee una interfaz gráfica, utiliza líneas de comando (insertas en un archivo de texto), por lo que se requiere de cierto conocimiento técnico. La instalación y configuración de este software es compleja, pero eficaz en funcionamiento.

- PerProxy, se ejecuta a través de un archivo java fácil de usar y configurar, pero es muy básico y no cumple con la característica de principal utilidad en un colegio, que es el web caché.
- AnalogX Proxy, se basa en activar o desactivar el servicio por medio de botones, no permite mayor configuración, muy básico y sencillo. No posee la funcionalidad de web caché.
- DDProxy, tiene una interfaz similar a FreeProxy sencilla y ordenada, pero no cuenta con web caché. Filtra contenido pero sólo mediante sitios web y no por palabras.
- FreeProxy, se presenta como la alternativa más completa. Posee una interfaz gráfica amigable, de fácil uso, instalación y configuración. Posee filtro de contenido, web-caché, utiliza métodos de seguridad como nombre de usuario y contraseña, es capaz de segmentar la red en grupos