



Proxy HTTP con caché y filtrado de contenidos en un puente

FILTRO PUENTE

Los proxies caché recuerdan las páginas webs y las sirven de forma local, ahorrando tanto dinero como tiempo. Los miembros más inteligentes de esta familia también eliminan el contenido peligroso y proporcionan un acceso transparente. **POR TOBIAS EGGENDORFER**

Cuando varios usuarios de una misma red acceden a Internet múltiples veces para ver una misma página, se paga el coste del ancho de banda y del tiempo. Un proxy caché reduce el tráfico almacenando las páginas webs solicitadas por los usuarios y sirviéndolas de nuevo cuando las vuelvan a solicitar.

Un proxy caché HTTP como Squid [1] se ejecuta en la capa 7 del modelo de referencia OSI (Open Systems Interconnection); dicho de otro modo, el servidor proxy Squid “habla” el protocolo de aplicación y puede

reconocer los datos que transporta este protocolo. Además, el proxy es capaz de comprobar el contenido de una página y proporcionar un filtro de contenido. Dependiendo de la dirección de destino, un proxy puede o bien bloquear el acceso a páginas indeseadas, como las de contenidos para adultos en redes escolares, o puede evitar la entrada de malware en la red de una empresa.

Modificaciones Molestas

Si se instala un proxy en una red, probablemente se tenga que enfrentar a una

lista de ajustes de configuración. Hay que añadir los detalles del proxy en cada navegador web, o bien establecer la opción de autoconfiguración del proxy de los navegadores, y modificar el cortafuegos para que deniegue los intentos de envío HTTP. Como alternativa, se puede instalar un proxy transparente utilizando una regla del cortafuegos que redirija todo el tráfico HTTP saliente al proxy. Pero de nuevo, hay que modificar el cortafuegos.

Una solución más elegante sería añadir simplemente el proxy a la red, tras el último

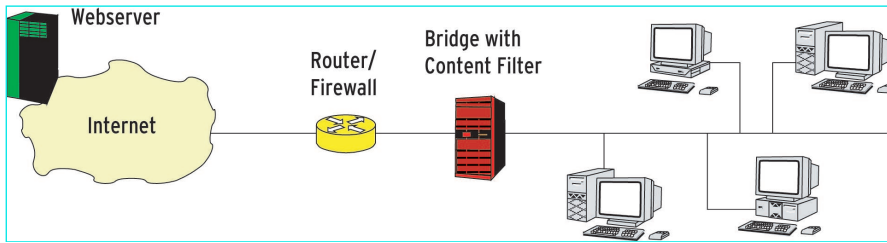


Figura 1: El filtro de contenidos se encuentra instalado en el puente en este escenario. Esta configuración se ajusta fácilmente a las redes existentes sin la necesidad de reconfigurar ni el router ni las máquinas clientes.

switch y justo delante del router. Esta propuesta, que elimina la necesidad de modificar los navegadores o el router, es una reminiscencia del papel que juega un puente o switch en una red. El propósito original de un puente era organizar el tráfico de la red basándose en las direcciones MAC y segmentar de este modo la red, pero los kernels modernos de Linux permiten a los administradores asumir el papel de un puente incluyendo reglas de cortafuegos invisibles basándose en filtros de estado a nivel de la capa TCP.

Conveniencia y Práctica

Una solución lógica es ejecutar un filtro de la capa de Aplicación en un puente (Figura 1). Estas dos extrañas parejas pueden parecer integradas en una red existente sin que el administrador o los usuarios tengan que modificar la configuración de los routers, los clientes o las aplicaciones. La única forma de pasarse el proxy es a través de un túnel, como OpenVPN o SSH. Sin embargo, la opción del túnel está siempre abierta, sin importar la solución que se escoja, y supone un esfuerzo y un conocimiento mayor.

Quien quiera que cree un túnel para evitar el proxy necesita un servidor de Internet como punto final del mismo y tiene que tener la capacidad de instalar software al otro lado del túnel.

Configuración Básica

Para instalar el proxy, se podría empezar instalando un sistema Linux mínimo. La máquina tiene que tener dos NICs, que por ahora no van a tener asignadas ninguna dirección IP. Como normalmente habrá que recompilar el kernel (para habilitar la función de puente) y como es preferible compilar Squid y DansGuardian desde el código fuente (véase más abajo), habrá que tener los correspondientes paquetes de desarrollo en el sistema. Posteriormente, antes de poner el

puente en uso, se debería limpiar la máquina y eliminar cualquier paquete que ya no se vaya a volver a utilizar de nuevo.

Cuestiones sobre el Kernel

Para hacer al sistema más seguro, probablemente se desee compilar un kernel estático sin soporte de módulos. Esta configuración deshabilita la interfaz de módulos que muchos rootkits del kernel explotan. Cuando se compile el kernel, hay que asegurarse de que se seleccionan la NIC correctas y los controladores del disco duro. Además, también hay que asegurarse de que el kernel soporte la función de puente a nivel del núcleo (Figura 2). Los administradores preocupados por la seguridad probablemente querrán instalar los parches de seguridad como el GR Security [2].

Tras arrancar el sistema con el nuevo kernel, habrá que configurar el puente: El comando `brctl addbr br0` añade un nuevo dispositivo de red denominado `br0`. Como un puente requiere dos NICs, será preciso asignarle las dos tarjetas de red por medio del siguiente comando:

```
brctl addif br0 eth0
brctl addif br0 eth1
```

Luego, con el comando `ip` se ejecutan las tarjetas y el puente:

```
ip link up eth0
ip link up eth1
ip link up br0
```

Ahora puede probarse. Simplemente hay que conectarlo a la red. Los paquetes deberían pasar entre los dos segmentos de red, aunque se puede utilizar una herramienta de análisis de red, como `tcpdump` [3], para verificar que está realmente funcionando. Si se prefiere así, ahora se puede configurar un cortafuegos con `iptables` y `Physdev-Match` o `eatables`.

Instalando Squid

Primero hay que instalar Squid para el proxy. Para descargar el código fuente desde [1], el sistema necesita una dirección IP y una puerta de enlace predeterminada en su tabla de enrutamiento. El siguiente comando se encarga de ello:

```
ifconfig br0 192.0.2.8
netmask 255.255.255.0
route add default gw 192.0.2.1
```

A continuación hay que descomprimir y configurar Squid: `./configure --enable-linux-netfilter --disable-ident-lookups`. El primero de estos parámetros habilita el soporte de Linux Netfilter en Squid. Este paso es necesario si se desea utilizar Squid como un proxy transparente. El segundo parámetro deshabilita las consultas del servicio Ident del lado cliente, aunque

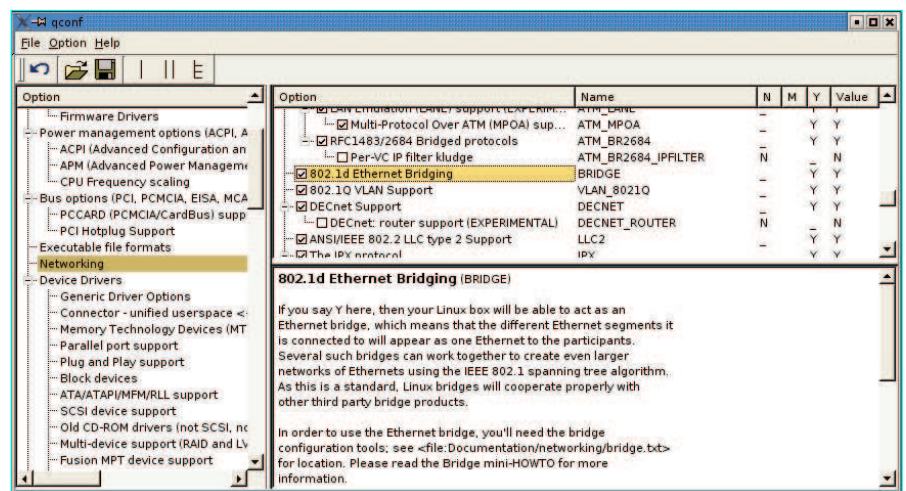


Figura 2: La opción BRIDGE en Networking | Networking support | Networking options | 802.1d Ethernet Bridging especifica si el kernel (2.6.17.7 en nuestro caso) soportará el modo puente.

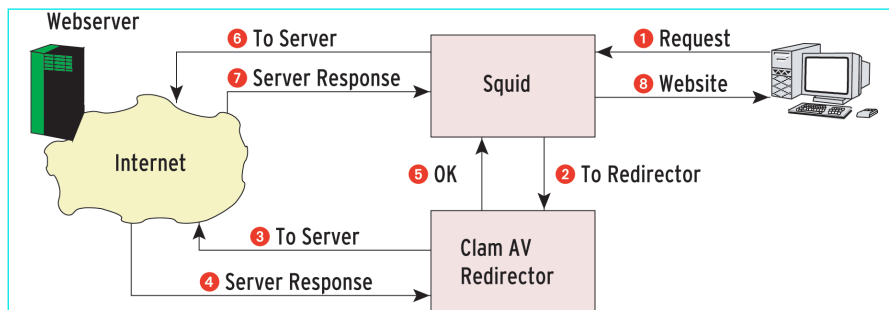


Figura 3: A la caza de virus con ClamAV.

Ident normalmente no está instalado y es bloqueado por la mayoría de los cortafuegos. Dependiendo de las preferencias de cada uno, puede utilizarse el parámetro `—prefix=/usr/local/squid` para ubicar todo esto dentro de un directorio. A continuación con el siguiente comando se compila e instala Squid: `make && make install`.

El siguiente paso consiste en modificar los ficheros de configuración de Squid para que se ajusten a las necesidades del usuario. El prefijo mencionado anteriormente sitúa el fichero `squid.conf` en el directorio `/usr/local/squid/etc`. Los administradores no tendrán que trabajar mucho con este fichero, pues el puerto que hay que indicarle a Squid que utilice es una cuestión de gustos; por defecto, Squid usa el 3128. Si se prefiere cambiarlo, habrá que añadir la siguiente línea al fichero de configuración de Squid:

```
http_port 127.0.0.1:65080
```

Esta línea le indica a Squid que escuche en el puerto 65080. El comando también configura a Squid para que se asegure de que solamente el proxy que se encuentra en localhost reaccionará a las conexiones. Esto es necesario para el filtrado de contenidos posterior.

Squid soporta el protocolo ICP (Inter Cache Protocol), que permite a los proxies intercambiar el contenido de sus cachés. Este soporte es irrelevante para nuestro caso y es fácil de deshabilitar: `icp_port 0`. Además, una entrada ACL (Access Control List) se asegura de que sólo al localhost le está permitido acceder a Squid: `http_access allow localhost`.

Filtrado de Contenido

El proxy aún se está ejecutando sin ningún filtro de contenidos. Ahora es el momento de la elección, elección que puede ser sencilla si se sabe qué es lo que se desea filtrar. La frase podría ser “proteger las máquinas Windows contra el intento del malware de alcanzarlas a través de las respuestas HTTP”.

En otros entornos, se podría necesitar un filtro que bloquee el acceso a ciertos tipos de contenidos y a sitios web indeseables. Por ejemplo, los colegios a menudo estipulan que los sitios con contenido de adultos o ilegal deben ser bloqueados. No vamos a meternos en la discusión sobre cómo de útil o efectiva es esta clase de protección. El siguiente ejemplo no censura ninguna página sino que se centra en combatir los virus.

De nuevo, la elección del software antivirus es una cuestión de gustos. En un entorno completamente de código abierto, un antivirus de código abierto como ClamAV [4] es una buena elección. Los pasos para configurar otros antivirus son similares; sólo habría que escoger uno distinto o incluso varios de ellos, el proceso debería ser bastante simple.

Se pueden encontrar diversas soluciones para integrar un filtro de contenidos en Squid: una opción muy popular es la interfaz `redirector`. Squid le pasa la URL descargada y todos los parámetros a este script. Dependiendo del valor devuelto por el script, Squid capturará el documento al que apunta la URL. Esto tiene sentido si el filtro simplemente inspecciona la URL y no el documento al que apunta.

Obstáculos Redirectores

En el caso de un antivirus, del que `SquidClamAVRedirector` proporciona el interfaz, el uso de redirector no es una

buena opción. Ante todo, redirector descarga la URL, evitando que Squid la procese; entonces analiza el contenido y luego hace que Squid solicite la página (Figura 3). Dicho de otro modo, cada descarga crea el doble del tráfico, y esto es exactamente lo que se pretende evitar usando un proxy caché.

Utilizando algunos trucos se puede hacer que redirector haga uso de Squid para que se encargue de la descarga. Este paso implica configurar a Squid para que no pase la solicitud de descarga de localhost a `SquidClamAVRedirector`, y por ello evitar entrar en un bucle infinito. Pero este esquema es problemático cuando se utiliza un proxy transparente, ya que cada petición parece como si procediese del localhost desde el punto de vista de Squid. Probablemente se esté de acuerdo que esta solución es algo chapucera y no es lo que deseamos precisamente.

Cadena de Proxies

La alternativa es añadir un proxy dedicado como filtro de contenidos justo delante o detrás de Squid. DansGuardian [5] es un buen candidato. El mejor sitio para situar a DansGuardian es entre el servidor proxy y la red interna (Figura 4a, aunque ambas aplicaciones se pueden ejecutar en la misma máquina). Esto significa que las solicitudes desde la red interna primero se envían a DansGuardian, éste se las pasa a Squid, luego recibe las respuestas de Squid, posiblemente de la caché, si Squid ya ha procesado anteriormente esta petición y comprueba si dichas respuestas contiene virus, gusanos y otras clases de malware.

En teoría, se puede cambiar el orden, colocando el filtro de contenidos en el lado externo y situando el proxy en el lado interno (Figura 4b). La ventaja de esta solución es que el antivirus sólo tendrá que analizar cada fichero descargado una única vez. Esta configuración minimiza el análisis de malware, pero también contiene un pro-

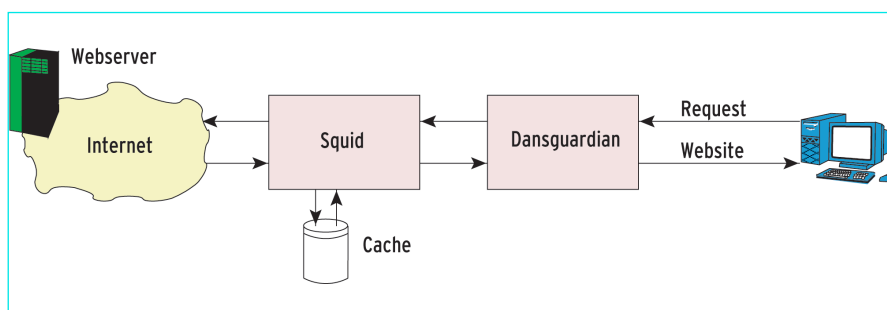


Figura 4a: Ubicando el filtro de contenidos DansGuardian entre los usuarios y el proxy caché Squid se asegura de que DansGuardian aplicará las reglas de filtrado en cada petición.

blema de seguridad. Si el antivirus no detecta un virus, éste llegará al proxy caché, donde estará a salvo de ser detectado en el futuro, incluso aunque se haya actualizado el antivirus, se seguirá teniendo la amenaza. Si el filtro de contenido está, por el contrario, entre el usuario y el proxy caché, analizará cada página solicitada, independientemente de si la página es servida desde la caché o desde un servidor externo.

Instalación de DansGuardian

Hay que asegurarse de tener instalado ClamAV antes de instalar DansGuardian. ClamAV es bastante fácil de instalar. Su página web contiene los binarios para la mayoría de las distribuciones Linux. Si se prefiere una instalación desde los ficheros fuente, los pasos habituales son suficientes: `./configure && make && make install`. Cuando se instala DansGuardian, hay que establecer una opción para el script Configure para que lo compile con el soporte de ClamAV. Si se prefiere, puede moverse el paquete compilado a otro directorio. Ello nos deja con los tres comandos siguientes para la instalación:

```
./configure --enable-clamav \
--prefix=/usr/local/dansguardian
make
make install
```

El parámetro `proxyport=8080` del fichero `dansguardian.conf` le indica al filtro que permanezca a la escucha en el puerto 8080. Además, el filtro necesita saber qué puerto es el que tiene asignado Squid: `filterport=65080`. Por último, es probable que también sea necesario quitarle el comentario a la línea `contentscanner` que apunta a ClamAV y modificar la configuración de ClamAV si fuera necesario.

El siguiente paso es el mensaje de error que verán los usuarios si solicitan una página con

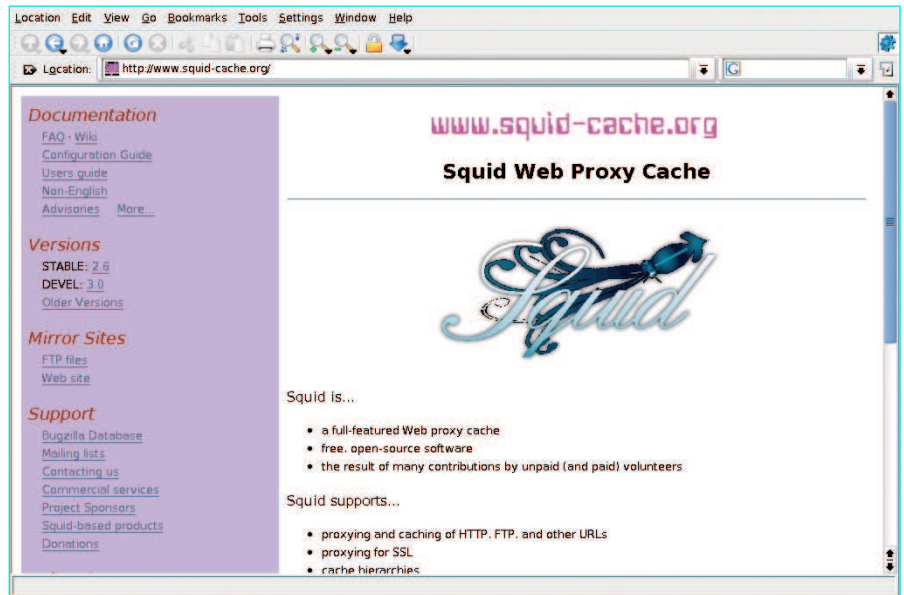


Figura 5: Se puede descargar gratuitamente Squid desde la página web www.squid-cache.org.

contenido peligroso. La forma más sencilla de producir el mensaje es tener una página en el servidor web de la intranet y redirigir el navegador a esta página. Como alternativa, se puede utilizar un servidor externo para que sirva una página con un mensaje. DansGuardian proporciona un ejemplo de página en `share/dansguardian.pl`. La directiva `accessdeniedaddress` en el fichero de configuración de DansGuardian le indica a la herramienta qué mensaje tiene que mostrar.

Habilitación del Filtro

Actualmente, DansGuardian no puede ver ninguna petición del cliente, la solicitud pasa directamente por el puente al servidor de destino. Una regla de Netfilter redireccionará el tráfico a través del filtro:

```
iptables -t nat -A PREROUTING \
-m physdev --physdev-in eth0 \
-p tcp --dport 80 -j REDIRECT \
--to-port 8080
```

El parámetro `physdev` restringe el uso del proxy a los clientes del lado interno del puente. Si no se tiene un cortafuegos que proteja el puente, sería bastante sencillo para un atacante externo explotar el proxy como un proxy abierto.

Si funciona, todas las peticiones web que se hagan a las redes externas deberían ser registradas en los ficheros de registro del proxy. El sistema es completamente transparente desde el interior. El proxy establece una conexión nueva a la página solicitada, proporcionando su propia dirección IP como dirección fuente. Los desarrolladores están trabajando para eliminar esta traza para tener un proxy completamente transparente.

Entorno Seguro

Con un filtro de malware y un proxy caché en el puente, la red interna estará bien protegida de los virus y los gusanos que intenten atacar a través de HTTP. La sencilla instalación hace que el puente sea fácil de usar. Tras la configuración de la máquina, simplemente hay que conectarla a cualquier red sin modificar la configuración de la misma.

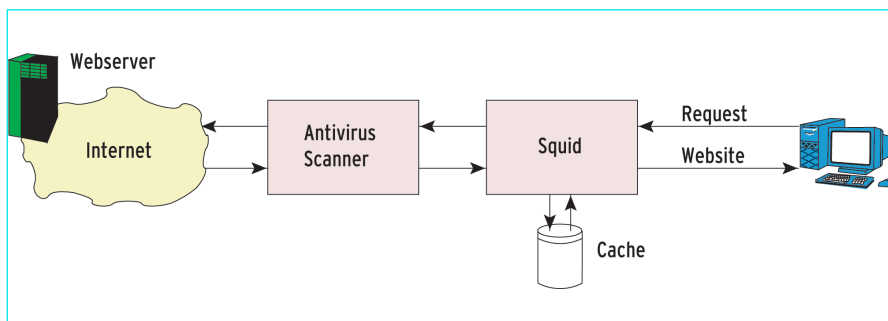


Figura 4b: Ubicando el filtro de contenidos en lado de Internet de la caché es menos seguro. Cada fichero sólo se analiza una única vez. Un virus que se haga con la caché nunca sería descubierto, incluso actualizando el antivirus.

RECURSOS

- [1] Proxy Web Squid: <http://www.squid-cache.org>
- [2] GR-Security: <http://www.grsecurity.org>
- [3] Tcpdump: <http://www.tcpdump.org>
- [4] ClamAV: <http://www.clamav.net>
- [5] DansGuardian: <http://dansguardian.org/>