Squid Transparente, Optimizado y... protector.

Autor: Arturo 'Buanzo' Busleiman <buanzo@buanzo.com.ar>

Bienvenidos a éste, mi segundo artículo para la revista SoloLinux. Hoy vuestro servidor les presentará una guía de configuración y optimización de Squid, el famoso HTTP Proxy-Cache Libre y Abierto. Adicionalmente veremos cómo instruir a nuestro kernel Linux para "engañar" a los clientes de nuestra red Interna, para que toda petición HTTP saliente hacia Internet pase sí o sí por las manos de Squid, todo mediante el uso de la utilidad Iptables, manipuladora de la funcionalidad de filtrado de paquetes existente desde el kernel Linux 2.4, Netfilter. Y para terminar, una perlita: configuración de DansGuardian para proveer de filtrado de contenido para adultos, muy útil en Cybercafés y casas de familia donde los padres o tutores deseen hacer uso de ésta tecnología.

Introducción

Existen una cierta cantidad de términos que debemos conocer antes de configurar un servidor proxy, sea directo o transparente. Entender dichos términos nos permitirá comprender en mayor profundidad los comentarios, ejemplos y documentación que suelen acompañar a los paquetes de software de esta categoría, y de todo el software libre en general, así como también permitirnos avanzar aún más en este apasionante mundo de las redes, la seguridad y la programación. En este caso, términos como "proxy" son tomados de forma incorrecta, y hablan de "proxies" cuando en verdad hablan de un "router", o de NAT. A tal efecto, veamos algunos detalles de estos términos:

Capa de Red y de Aplicación: Usualmente debería despachar una descripción del modelo OSI teórico y/o del modelo TCP/IP, pero voy a simplificar la cuestión. Cuando nos referimos a la Capa de Red, estamos hablando de toda cuestión vinculada con direcciones IP, enrutado, túneles, filtrado, etc. Y claro, cuando hablamos de Capa de Aplicación, nos referimos a todo lo que tiene que ver con el nivel mas alto de funcionamiento. Si, adivinaron: las aplicaciones. En términos prácticos, entonces, si alguien habla de un "Firewall de Capa de Aplicación", se refiere a poder implementar filtrado según parámetros del protocolo de alto nivel. Por ejemplo, el l7-filter es una aplicación que pueden encontrar en www.freshmeat.net que permite filtrar según aplicación: MSN Messenger, FTP, etc, más allá del puerto donde estén ocurriendo dichas conecciones. ¿Interesante, no?

Netfilter: Funcionalidad y esquema interno del Núcleo Linux en las versiones 2.4 y 2.6 que proveen Firewall con conocimiento de Estado (Stateful Firewall). Un firewall, o cortafuegos, habilita la capacidad de aplicar políticas sobre los paquetes, como por ejemplo “permitir acceso desde cualquier IP al puerto 80 de la interfaz eth0”, o tal vez “denegar el acceso al puerto 22, excepto a las IP 1, 2 y 3”. La cuestión de conocimiento de estado está vinculada conque Netfilter mantiene una tabla de las conecciones entrantes y salientes, y de esta forma nos permite armar reglas en base a parámetros "de estado", como conección establecida, relacionada o nueva. Por ejemplo, supongan que de 8 a 19hs se permiten nuevas conecciones salientes hacia Internet. Pasado este horario podríamos armar una regla que especifique que solamente las conecciones relacionadas o establecidas, pero no nuevas puedan seguir saliendo a Internet. De esta forma, la descarga de un archivo continuará hasta su fin, incluso pasado este horario, pero no se podrá ingresar a nuevos sitios. ¿Qué tiene esto que ver con un Proxy Transparente? Simple: Netfilter también permite aplicar ciertas reglas de redireccionamiento, no solo las clásicas de “ACEPTAR” y “RECHAZAR”. En resumen, vamos a tener que aplicar un par de

reglas de Netfilter (quizá a la mayoría les suene mas por su conjunto de utilidades, Iptables) para lograr nuestro acometido. Les recomiendo la lectura de algunos artículos sobre Iptables introductorios, o mejor aún, leer de pies a cabeza la página del manual para "iptables".

Proxy: Mucha gente confunde el término Proxy con el de Gateway (o “puerta de enlace predeterminada”, según la traducción de cierta empresa de software privativo). En toda red TCP/IP, por ejemplo en una red privada 192.168.0.0 Clase C (Máscara 255.255.255.0 o '/24'), se necesita un gateway si es que deseamos llegar a otras redes, como Internet. Dicho Gateway poseerá la cantidad de interfaces necesarias y rutas establecidas y políticas de acceso que permitirán o no el acceso a ciertos destinos desde esta red interna. Por supuesto, en este caso hablamos de acceso “transparente” (por así decirlo) a la red destino en cuestión. Esto significa que el Gateway no tiene en cuenta el protocolo de aplicación (HTTP, FTP, etc) o mejor dicho que “no los entiende ni tiene en cuenta excepto por puerto de origen o destino”. Por ejemplo, se puede asumir que en el puerto 80 de cierta IP de destino habrá un servicio que entienda HTTP... pero el gateway no puede asegurarlo.
Un proxy actúa como gateway pero a un nivel más alto, en la llamada “capa de aplicación”. Significa que entiende HTTP, FTP, u algún otro protocolo de alto nivel, y que acepta por parte de un cliente (de la red interna, por ejemplo) solicitudes vinculadas a dicho protocolo. El proxy realizará, a su vez, la solicitud al servidor de destino, tomará el resultado y lo devolverá. Al tener conocimiento del protocolo se pueden aplicar reglas mucho más interesantes, como restricciones basadas en contenido, partes del nombre de un sitio, usuario, grupo al que un usuario pertenece, IP de origen, etc. Squid es un proxy de HTTP y FTP, y a su vez provee la funcionalidad de cache: guarda copias de las páginas y archivos visitados. De esta forma, cada vez que un usuario vuelve a acceder a cierto sitio, sólo el contenido que haya cambiado será transferido, logrando una reducción de la utilización del ancho de banda disponible. En resumen, el cliente no accede realmente a internet, sino que le solicita al proxy lo que quiere, el proxy a su vez lo busca en Internet, lo transfiere, y luego se lo da al cliente. Es menos directo, si, que NAT, donde se trabaja a nivel TCP/IP y no a nivel aplicacion.

NAT: Corresponde a Network Address Translation o Traducción de Dirección de Red. Las direcciones IP de una red privada no son direccionables en Internet, por lo que el Gateway suele aplicar lo que se llama comunmente “enmascaramiento” (Masquerading) de la IP de origen, reemplazando la interna por la correspondiente a la interfaz de red pública del Gateway. Por supuesto, se mantiene una tabla con los datos necesarios para poder relacionar las respuestas que provengan de internet con su destino “real” en la red privada.

Transparente: Bien, ya sabemos que es un Gateway, Netfilter y un Proxy. El hecho de que sea transparente permite al administrador lograr que toda solicitud HTTP (puerto de destino 80/tcp) realizada por un cliente de la red interna sea automáticamente redirigida al Proxy, evitando la salida directa. Los motivos para realizar ésto pueden depender del administrador, pero seguramente tengan que ver con políticas de administración de recursos, seguridad, performance, etc. Esto se realiza, como ya dijimos, mediante reglas de redireccionamiento de Netfilter (aplicadas con la utilidad Iptables).

ES IMPORTANTE ACLARAR que cierta funcionalidad del protocolo HTTP se pierde al utilizar un proxy transparente en vez de uno debidamente configurado en los clientes. Va más atllá del propósito de éste artículo el explicar dichos problemas. A modo general podemos responder “probablemente no tengas problemas notables”. La práctica será lo mejor.

Ventajas y Desventajas

Veamos las ventajas de usar Squid:
1) Soporta HTTP y FTP.
2) Tiene un avanzado mecanismo de autentificacion y control de acceso (o sea, a quien y cuando permitimos utilizar el proxy).
3) Permite actuar como 'cache' de Internet, copiando contenido en forma local para que se lo pueda accesar rápidamente.
4) Es Software Libre.

Ahora, las desventajas, pero de usar un Proxy en general:
1) La maquina donde funcionara el Proxy debe tener capacidad de almacenamiento acorde a la cache que necesitemos o querramos.
2) Debe tener un buen poder de procesamiento, ya que no es solo un 'reenvio' de paquetes tcp/ip. Recuerden que estamos trabajando en la Capa de Aplicación.
3) En modo transparente existen algunos problemas de compatibilidad (mínimos, pero existen).
4) Hay que configurar la utilizacion del Proxy en cada cliente (hay 2 formas de salvar este inconveniente, que veremos mas adelante).

Configuración Genérica de Squid

Lo principal es saber que el sitio oficial es www.squid-cache.org y no www.squid.org. De hecho es tan común esta equivocación que www.squid.org tiene un mensaje "¿Está buscando la Cache? Haga click sobre esta URL". Desde el sitio oficial de Squid podemos bajar la ultima version de desarrollo (DEVEL), que es el codigo fuente "no-estable". Sino, podemos bajar la version "estable" (STABLE, recomendada para sistemas en produccion). Si nos acercamos a Squid como programadores, porque queremos extenderlo o corregir algun error, debemos utilizar la version DEVEL, o acceder mediante CVS (ya trataremos este tema mas adelante).

Al momento de escribir este articulo, la ultima version estable del Squid Cache es la 2.5-STABLE7. Pueden elejir entre formato tar.gz o . tar.bz2 - Para descomprimir un tar.bz2 o tbz2, utilicen el parámetro "-j" del tar, en vez del "-z". El bzip2 comprime generalmente mejor.

Voy a asumir que instalaremos el Squid desde sus fuentes. Este método de instalación sirve para tener una idea de lo que los pre-empaquetados o lo que las distribuciones basadas en fuentes hacen o pueden pedirnos que hagamos post-instalación.

Una vez que hayamos bajado y desempaquetado el archivo de la distribución de Squid, cambiemos al directorio donde quedo almacenado, y ejecutemos las 3 famosas sentencias de compilacion:

1) ./configure --prefix=/usr/local/squid - Para que el Squid, sus binarios, archivos de configuracion, etc, esten en /usr/local/squid.
2) Si el paso 1 termino sin problemas, podemos hacer 'make'.
3) Ahora, 'make install', para copiar los archivos necesarios a las ubicaciones establecidas dentro de la jerarquia /usr/local/squid

NOTA: Si utilizan Gentoo, un simple "emerge squid" es más que suficiente. Recuerden prestar atención a las instrucciones que aparezcan al finalizar el emerge!

Una vez compilado e instalado el Squid, debemos configurarlo. A decir verdad esto

es bastante simple: el archivo de configuracion squid.conf (en /usr/local/squid/etc) esta LLENO de parametros, pero solo unos pocos debemos modificar SI o SI. El Squid, como lo indica su documentacion, tiene muchas funciones, pero solo utilizaremos lo mas basico al comienzo. Editemos el squid.conf con el editor que mas nos guste. Veran que es de un estilo muy simple: bien comentado, pero cada parametro de configuracion es una linea, que contiene un parametro o comando, y una serie de valores. Antes de empezar a modificar estos valores, seria conveniente leer todo el squid.conf completo, para tener una idea, una vision general de lo que se puede hacer desde alli, de esta forma si un dia tenemos que hacer algo en particular, quiza podamos recordar si hacerlo desde squid.conf o desde otro lado.

El primer parametro a tocar es 'cache_mem'. Especifica la cantidad de memoria (no de disco duro) que Squid utilizará. Según recomendacion de los autores, si tenemos "X" RAM libre que querramos dedicar al Squid, pongamos aqui un TERCIO de dicho valor (X/3).

Luego podemos seguir por 'cache_dir', donde especificaremos el donde y el cuanto de la Cache. Por ejemplo: 'cache_dir /usr/local/squid/cache 100 16 256'. El valor 100 indica '100 MB de cache'. Al 16 y al 256 es probable que no necesitemos nunca cambiarlos, e indican al Squid como utilizar los 100mb. Luego veremos como optimizar esta sentencia.

Ahora viene algo importante: las reglas de acceso y el acceso a los protocolos http e icp. Por defecto querremos permitirle la utilizacion del Proxy a nuestra red interna solamente. El siguiente bloque es un ejemplo para una red 192.168.10.0 con mascara 255.255.255.0. Se permitira acceso toda esta red y al localhost/127.0.0.1, esto se logra definiendo 4 acl's: la del administrador (de uso interno del Squid), la de localhost, una global que hable de TODA direccion IP posible y la de permitidos (nuestra red privada). En este ejemplo, asumimos una red privada clase C 192.168.10.0 a la cual denominamos "permitidos". La regla acl "todos" generalmente se denomina "all" en Squid, y viene definida por defecto. Aquí la traduje a efectos de que sea mas claro el ejemplo.

```
acl localhost src 127.0.0.1/255.255.255.255
acl todos src 0.0.0.0/0.0.0.0
acl permitidos src 192.168.10.0/255.255.255.0

http_access allow permitidos localhost
http_access deny todos

icp_access allow permitidos localhost
icp_access deny todos
```

Los indicadores 'deny' y 'allow' significan "denegar" y "permitir", respectivamente, a las solicitudes que concuerden con las ACL definidas mas arriba en cada protocolo. El orden es de 'allow, deny'. Primero indico a quienes permito, luego deniego a todos los demas. Quiza quieran hacer esto por cada {PROTOCOLO}_access que les parezca.

Quiza querramos modificar el 'cache_mgr', para indicar la direccion de eMail nuestra, asi si algun usuario tiene problemas, sabe a quien contactar. 'visible_hostname' indicara el nombre del Host que se publicara en paginas de error, etc, generadas por Squid.

Luego, debemos indicar con que usuario y grupo debe funcionar el Squid luego de

haber sido iniciado con root desde los scripts de inicio (o a mano por el root mismo). Esto lo hacemos con 'cache_effective_user' y 'cache_effective_group'. Valores recomendados: algo del estilo 'nobody' y 'nogroup'. Una vez editado el squid.conf, debemos inicializar la cache, y luego ejecutar el Squid. Esto lo hacemos de la siguiente forma:

Inicializar la cache: /usr/local/squid/bin/squid -z
Ejecutar el Squid: /usr/local/squid/bin/squid

Ahora, debemos revisar /usr/local/squid/logs/cache.log. Debemos fijarnos si esta todo bien. Van a encontrar un par de errores al principio de todo, algo comun la primera vez que se ejecuta el Squid. Una vez andando, debemos probarlo: vayamos a un cliente, configuremos el uso del proxy para el protocolo HTTP en el puerto 3128 (el por defecto de Squid, el cual se puede cambiar con 'http_port') y listo. Si anda, perfecto. Si no, verifiquen que el Squid este ejecutándose ('ps ax', 'nmap', ´lsof -iTCP:3128', etc).

"Transparentización" del Squid

Una vez configurado el Squid, debemos probarlo en formato “no-transparente”, configurando un navegador para que lo utilice. Recuerden que Squid utiliza el puerto 3128/tcp para recibir las solicitudes. Si funciona, podemos pasar a la siguiente etapa: la transparentización (!?) de Squid.

En principio, son sólo 4 los parámetros los que debemos configurar. Uno de estos parámetros no lo encontrarán comentado y con un valor por defecto, sino que deberán tipearlo desde cero. Los parámetros y sus correspondientes valores, son los siguientes:

httpd_accel_host virtual
httpd_accel_port 80
httpd_accel_with_proxy on
httpd_accel_uses_host_header on

¿Qué significa cada uno de ellos?

httpd_accel_host : Squid puede configurarse como cache, como acelerador de navegación o como ambos. Este parámetro indica el nombre de host o IP de un Squid configurado como acelerador. En nuestro caso usaremos el valor “virtual”, ya que vamos a usar el modo transparente.

httpd_accel_port : Este es el puerto donde generalmente los servidores web esperan solicitudes. En el caso de que usemos Squid como frente de un grupo de servidores web locales, habria que hacer que Squid escuche en el 80 y no en el 3128, y que los servidores web escuchen en otro puerto, y NO en el 80.

httpd_accel_with_proxy : Al habilitar httpd_accel_host la función de cache deja de funcionar. Para que vuelva a funcionar, debemos forzarlo con el valor “on”.

httpd_accel_users_host_header : En modo transparente, las solicitudes salientes al puerto 80 de algun servidor externo son redirigidas al puerto 3128 del Gateway, en el que Squid espera solicitudes. Si no se habilitara esta opción los sitios que manejen sitios web virtuales, o sea, mas d eun sitio por dirección IP, no serían correctamente cacheados. La cabecera Host definida en HTTP 1.1 siempre tiene como valor el nombre de Host de la URL a donde estemos intentando navegar.

Squid, si se habilita este parámetro, la utiliza y nos entrega el contenido requerido.

Reglas de Netfilter – Ultimo paso

Una vez configurado Squid con las opciones de proxy transparente requeridas, tan solo nos queda armar la regla de Iptables necesaria. Si utilizan Shorewall como solución de Firewall (muy buena, por cierto), en su FAQ y Documentación encontrarán como crear esta regla desde su sistema de configuración. (ver recuadro). La regla en cuestión es la siguiente:

iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 -j REDIRECT --to-port 3128

En este caso asumimos que "eth1" es nuestra interfaz de red conectada a la red privada.

Recuerden que el archivo access.log (definido en squid.conf) nos irá mostrando las solicitudes que se realizan, y así podremos verificar el correcto funcionamiento de la regla de direccionamiento.

Pueden ver un script de firewall simple para un gateway que solo admite SSH en el recuadro.

Optimización Básica

Existen 5 parámetros que pueden hacer la diferencia entre un Squid lento y pesado contra uno agil y de buen nivel de respuesta. Hagan los siguientes cambios en squid.conf:

cache_store_log al valor none
half_closed_clientes al valor off
cache_swap_high al valor 100%
cache_swap_low al valor 80%

De la misma forma se puede establecer correctamente el parámetro cache_dir con la siguiente fórmula:

Siendo:
x = Tamaño_de_cache_en_KB
y = Tamaño_de_objeto_promedio_en_KB (aprox. 18Kb)

El valor MD será (((x / y) / 256) / 256) * 2

La línea cache_dir, entonces, será, por ejemplo, para 6Gb de cache:

cache_dir ufs /var/cache/squid 6144 14 256

Filtrado de Contenido para Adultos

El día de hoy no es raro para nada encontrar usuarios de GNU+Linux cuyos hijos utilizan también GNU+Linux. Si hay acceso a la Web, un padre puede preocuparse. Existe software Open Source que puede ayudarlos.

Aquí veremos una solución técnica puntual para una computadora con GNU+Linux desde la cual se acceda a la World Wide Web. Adicionalmente, hemos realizado una corta serie de preguntas a una investigadora en el campo de la protección infantil,

Noelia Negri, quién junto con un grupo de personas analizan la proliferación de la pedofília en Internet, y hacen algo al respecto. Solicitaron no decir más que lo dicho, por lo que ahora comenzaremos con nuestro artículo. Felicitaciones Noelia y asociados!

Diferencias Técnicas

Existen principalmente tres formas de identificar sitios potencialmente ofensivos o inapropiados para los menores de edad: En base a parámetros en la URL (dirección del sitio) lo que incluye bases de datos y listas de sitios a prohibir (blacklists, un término común en paquetes como squidGuard), en base a frases comunmente utilizadas en sitios pornográficos, o en base al "rating" de un sitio, servicio ofrecido por terceros o por el realizador de un sitio web (usalmente mediante el mecanismo PICS - Platform for Internet Content Selection / Plataforma para Selección de Contenido de Internet). En esta guía vamos a hablar de una aplicación llamada DansGuardian, que actúa como intermediario entre el navegador e Internet, o entre el navegador y un Proxy (y, subsecuentemente, Internet). Podríamos decir que DansGuardian es, en si mísmo, un Proxy, aunque el autor nos aclara que en verdad es un redirector de las solicitudes, con una etapa previa de filtrado.

DansGuardian funciona en Linux, FreeBSD, OpenBSD, NetBSD, Mac OS X, HP-UX y Solaris. Entre los métodos de filtrado que DansGuardian implementa se incluyen los ya nombrados basados en URL y nombre de dominio, por frases en el contenido, por calificación o etiquetado PICS, según tipo de archivo (mediante los tipos MIME), por extensión del nombre de archivo. Entre otras características, soporta funcionar "al revés", especificando una lista de sitios válidos a los cuales un navegante puede acceder, denegando al resto de Internet.Tiene un modo invisible de funcionamiento, en el cual los navegantes no saben que están siendo vigilados. En este modo, se reporta en un archivo log los sitios que se habrían bloqueado, pero no se los bloquea. Entre otras ventajas, es mucho más rápido que squidGuard en lo que a filtrado basado en URL se refiere. En este parrafo intenté dar a entender que DansGuardian es mucho mas complejo y potencialmente útil de lo que en esta guía veremos. Pero ya es hora de trabajar.

Comencemos

Asumiremos la siguiente "cadena" para llegar a Internet:

Navegador - Gateway - DansGuardian - Squid - Internet

El navegador no necesitará ser configurado para utilizar DansGuardian: Utilizaremos Netfilter para que sea "transparente", variando la regla de Netfilter utilizada con Squid.

ATENCION: *Si deciden utilizar DansGuardian por delante de Squid, las ACL van a dejar de funcionar, ya que las solicitudes vendrían siempre desde la IP donde funciona DansGuardian. El autor propone dos alternativas: Aplicar un parche al Squid para que reconozca la cabecera X-Forwarded-By, o colocar a DansGuardian por detrás del Squid. No daremos más detalles! Cómo taréa para el lector, asumiremos que no existe una red privada que acceda a los Internet, sino una sola computadora donde funciona tanto navegador, como filtrador [y] proxy, desde la cual navega la familia.*

Como deben suponer, DansGuardian reenviará las solicitudes que reciba del navegador al Squid, por lo que todo se resume en una cuestión de puertos, direcciones IP y comandos de Iptables. Haremos escuchar a DansGuardian en el puerto 8080 de la IP 127.0.0.1 (recuerden que en esta guía asumimos UNA sola

computadora, y no una red privada), y al Squid en el puerto 3128 de 127.0.0.1. DansGuardian funcionará bajo el entorno del usuario y grupo asignado a squid (generalmente usuario squid, grupo squid). Desde ya, la habilitación del filtrado se puede realizar en base al usuario que está utilizando el navegador, por lo que es importante que tanto DansGuardian y Squid compartan usuario y grupo.

En el caso de que utilicen la distribución Gentoo, podrán instalar todo lo necesario con el comando:

emerge dansguardian squid iptables

Y luego podrán habilitar squid y dansguardian en el inicio del sistema con:

rc-update add squid default
rc-update add dansguardian default

Caso contrario, el procedimiento normal de compilación (./configure && make && make install, ver sección Squid y aplicarla a DansGuardian) se aplica sin mayores problemas, luego de descargar DansGuardian y desempaquetarlo con **tar -zxvf DansGuardian-VERSION-source.tar.gz.** También pueden elejir descargar los RPM que existen disponibles para:

- Fedora Core 2
- Mandrake 8.x
- Debian

En www.rpmsearch.net pueden encontrar más. Tal vez necesiten utilizar el parámetro --nodeps de rpm para poder instalar alguno de estos paquetes.

Si así lo desean, pueden elegir instalar webmin en forma adicional, ya que existe un módulo de configuración de DansGuardian para Webmin, el cual también se descarga desde el sitio de DansGuardian o desde su sitio oficial (ver recuadro).

Configuración de DansGuardian

Una vez instalado DansGuardian, su archivo de configuración, denominado dansguardian.conf se encontrará en el directorio /etc/dansguardian. Si no lo encuentran, intenten 'locate dansguardian.conf' (si usan updatedb), o el simple pero efectivo **find / -name dansguardian.conf**.

El archivo de configuración tiene 370 líneas, de las cuales sólo 51 son sentencias de configuración, y, de las cuales, en esta guía, solo veremos 10. DansGuardian es complejo, se pueden modificar parámetros de red, de performance, y obviamente de restricciónes y algorítmos de decisión. En nuestro caso, modificaremos el idioma en que DansGuardian mostrará mensajes, el usuario y grupo bajo el cual funcionará, cómo y dónde se guardará el archivo log, etc.

Los primeros 8 parámetros los encontrarán casi al principio del archivo, y los últimos dos al final (aproximadamente en la linea 361), y son los siguientes:

reportinglevel - Este parámetro indica que tanta información daremos al navegante cuando se le prohíba ingresar a un sitio. Con el valor 2 se dará un reporte completo. Con el 3 (valor por defecto) podremos especificar una plantilla HTML a utilizar. Con 0 tan solo se dirá "Acceso Denegado".

language - En nuestro caso, podremos seleccionar entre sólo 2 variante del español: "arspanish", en caso de preferir el Español Argentino, o "mxspanish" en el caso de Méjico. Otros lenguajes disponibles pueden encontrarse en el directorio indicado por languagedir.

logfileformat - El formato en que deseamos que DansGuardian escriba al archivo log. Por defecto, el valor 1 indica el formato DansGuardian. Se puede usar un CSV (Valores separados por coma) con el 2, o el formato de access.log de Squid con el 3. El 4 separará los campos con un TAB.

loglocation- Y con este parámetro, podemos especificar donde grabar el log. Por defecto viene comantado. Deben especificar un directorio al cual el usuario con el que DansGuardian funcione tenga acceso de escritura.

filterip -Indica en que dirección (una sola) escuchará DansGuardian. Por defecto escucha en TODA dirección IP disponible, incluso nuestr IP de Internet! En nuestro ejemplo, usaremos el valor 127.0.0.1

filterport - Puerto en el que escuchará DansGuardian. Por defecto, y acorde a nuestro ejemplo, se utiliza el puerto 8080.

proxyip - Dirección IP del servidor proxy. En este caso el valor por defecto sigue siendo acorde a nuestro ejemplo, y es 127.0.0.1. DansGuardian lo utilizará para descargar las páginas que sean admitidas por el filtro.

proxyport - Squid por defecto escucha en el puerto 3128. Justamente, es el valor por defecto de este parámetro.

daemonuser - Usuario con el que funcionará DansGuardian. Debe ser el mismo que utilice Squid, tomando del parámetro cache_effective_user de squid.conf (ver sección Iptables).

daemongroup - Grupo con el que funcionará DansGuardian. Debe ser el mismo que utilice Squid, tomando del parámetro cache_effective_group de squid.conf (ver sección Reglas de Netfilter).

Reglas de Netfilter
Los comandos Iptables para implementar el redireccionamiento transparente en este caso son más interesantes, ya que haremos uso del módulo "owner" de Netfilter, para especificar cuál es el usuario que está ejecutando el proceso que intenta acceder al puerto 80 de destino. De esta forma también implementamos que usuarios tendrán excepción, y pasarán directamente al Squid, sin filtrado intermedio.

Si ya tuvieramos un proxy squid funcionando desde antes, sería mas simple tomar el usuario y grupo que Squid utiliza, y aplicarlos al DansGuardian en sus parametros **daemonuser** y **daemongroup.** Para obtener el nombre de usuario y grupo, podemos utilizar el comando **grep**, asumiendo que el archivo de configuración de squid se encuentra en /etc/squid/squid.conf:

Para obtener el usuario:
grep cache_effective_user /etc/squid/squid.conf | grep -v ^#

Para obtener el grupo:
grep cache_effective_group /etc/squid/squid.conf | grep -v ^#

El **grep -v ^#** es para filtrar las líneas que comiencen con #, que serían comentarios.

Asumamos que el usuario "buanzo" será exempto del filtrado, y que el usuario y grupo de squid son squid y squid respectivamente. En este caso los comandos Iptables necesarios serían los siguientes.

iptables -t nat -A OUTPUT -p tcp --dport 80 -m owner --uid-owner squid -j ACCEPT
iptables -t nat -A OUTPUT -p tcp --dport 3128 -m owner --uid-owner squid -j ACCEPT
iptables -t nat -A OUTPUT -p tcp --dport 80 -m owner --uid-owner rcarlos -j ACCEPT
iptables -t nat -A OUTPUT -p tcp --dport 80 -j REDIRECT --to-ports 8080
iptables -t nat -A OUTPUT -p tcp --dport 3128 -j REDIRECT --to-ports 8080

De esta forma, incluso un menor que quiera "saltearse" el filtrado, y acceder directamente al Squid proxy o a Internet, no podrá hacerlo, excepto, claro está, que logre utilizar el usuario "rcarlos".

ATENCION: Esos comandos NO SON un script de Firewall completo, ni intentan serlo, tan solo son los comandos que implementan la funcionalidad que necesitamos. El orden en que se ubiquen en un archivo de reglas definirán si funcionarán o no.

Si utilizan Shorewall, con agregar esos comandos al archivo **start** ubicado en el directorio de configuración de Shorewall, debería alcanzar. (Generalmente, /etc/shorewall).

Finalizando

Existen otras alternativas para realizar el filtrado, como squidGuard, pero el mismo principalmente se basa en listas negras ("blacklists"), que también se pueden utilizar con DansGuardian sin cambios. DansGuardian provee mecanísmos de detección múchisimo más efectivos, y provee métods para reemplazar imágenes, ejecutar scripts CGI o para crear básicas reglas de control de acceso editando archivos de configuración adicionales. No es mi intención presentar un análisis completo de administración e instalación de un servidor de filtrado de contenidos basado en Squid, DansGuardian y Netfilter, pero sí una solución relativamente simple de implementar, y que sirva a los padres.

Acerca de listas negras actualizadas, pueden bajar una de urlblacklist.com, sección Download, donde también pueden subscribirse para recibirlas. El precio de subscripción varía dependiendo del tipo de uso, frecuencia de actualización y cantidad de usuarios.

El hecho de que el software utilizado sea abierto nos permite obtener mayor seguridad, sabiendo que hay más gente utilizándolo y revisándolo, y encontrando y resolviendo errores que podrían hacer fallar a DansGuardian, de forma tal que su función sea evitada.

Como comentario final, la educación constante de nuestros hijos es lo que debe hacer la diferencia. No una aplicación.

Listado de URLs útiles

Squid : http://www.squid-cache.org/
IRCache: http://www.ircache.net/

Shorewall : http://www.shorewall.net/
DansGuardian: http://dansguardian.org
Módulo Webmin DansGuardian: http://sf.net/projects/dgwebminmodule
Script Firewall de Ejemplo: http://blog.buanzo.com.ar/datos/sololinux_fw.sh

Recuadro: Script de Firewall para red privada 192.168.10.0/24 con NAT y Squid Proxy transparente, sin ningún servicio accesible desde Internet:

```
#!/bin/sh

# Interfaz vinculada a Internet
INET_IF=eth1
#Interfaz vinculada a la red privada
PRVT_IF=eth0
#Si tenemos IP fija, definamosla aqui y utilicemos la regla de SNAT
#Caso contrario, habilitemos la regla de MASQUERADE
IP_PUBLICA=1.2.3.4

# Limpieza
iptables -t nat -F
iptables -F
iptables -X
iptables -t nat -X

# Politicas (para el hogar, todo sale, nada entra)
iptables -P INPUT DROP
iptables -P FORWARD ACCEPT
iptables -P OUTPUT ACCEPT

# Filtrado de Entrada
iptables -A INPUT -i lo -j ACCEPT

# Podriamos filtrar CIERTOS paquetes del ICMP, dejemoslo para otro articulo
iptables -A INPUT -i $INET_IF -p icmp -j ACCEPT

# Dejamos entrar lo que este relacionado con conecciones existentes, y
# tambien las ya establecidas.
iptables -A INPUT -i $INET_IF -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A INPUT -i $PRVT_IF -p tcp --dport 8110 -j ACCEPT
iptables -A INPUT -i $PRVT_IF -p tcp --dport 3128 -j ACCEPT
iptables -A INPUT -i $PRVT_IF -p udp --dport 53 -j ACCEPT

# Habilitar Internet para la red interna con SNAT (si tenemos IP publica fija)
echo 1 > /proc/sys/net/ipv4/ip_forward
iptables -t nat -A PREROUTING -i $PRVT_IF -p tcp --dport 80 -j REDIRECT --to-port 3128

# Si tuviesemos IP dinamica de Internet, hariamos MASQUERADE
# y comentariamos la linea de SNAT anterior.
# iptables -t nat -A POSTROUTING -o $INET_IF -j MASQUERADE

iptables -t nat -A POSTROUTING -o $INET_IF -j SNAT --to-source $IP_PUBLICA
```

--

En el caso de Gentoo, guarden este archivo en /var/lib/iptables. Ejecútenlo, recuerden setearle el bit de ejecución con chmod +x, y si todo funciona, ejecuten / etc/init.d/iptables save. De esta forma, las reglas serán guardadas y reestablecidas en el próximo inicio. No olviden agregar iptables al default runlevel, con rc-update add iptables default.

Entrevista a Noelia Negri - Investigadora Independiente.

En la decada pasada los padres controlaban lo que sus hijos miraban en la television. Con la actual Internet, cuyo uno de sus primeros usos fue el de distribuir pornografia, ¿qué tipo de control considera aplicable?

Creo que el mejor control es aplicar filtros a los sitios que son impropios para los niños. Sin embargo, Internet es prácticamente imposible de controlar ya que no se compone unicamente de sitios web, sino de otras utilidades como el e-mail, los foros, el chat etc. Los chicos se relacionan constantemente por estos medios con personas virtuales y anónimas que ellos mismos no conocen personalmente, mucho menos sus padres. Por eso, aunque los filtros sean eficaces, son insuficientes. Seria bueno que los papás animen a sus hijos a charlar sobre el uso que ellos hacen de la Red y que se interesen en las amistades virtuales que hacen sus hijos, sin invadir su privacidad pero controlando que sean inofensivas.

En cybercafés el acceso a la pornografía suele ser más generalizado. ¿Alguna opinión al respecto?

Los cybercafes deberían aplicar filtros para contenidos adultos. Pero ademas, procurar que los mayores no accedan a dichos sitios cerca de los niños. Adicionalmente, los administradores del cybercafe debieran implementar revisiones del contenido que un adulto pudiera haber dejado disponible en la computadora. Un menor podría accidentalmente encontrarse con el mismo.

¿Puede Internet llevar a los niños a encontrarse con su sexualidad en forma temprana?

No necesariamente. Aunque el contenido sexual es muy amplio en la red, e incluso influyente en determinados casos, los padres no deben perder de vista que la educación sexual es responsabilidad exclusiva de ellos. Por lo tanto, si los niños tienen una buena formación en lo que concierne a este tópico, difícilmente Internet pueda tener algún tipo de influencia negativa. Si por el contrario dicha educación contiene carencias, los chicos buscaran saldarlas por otros medios. Aquí entra en juego el contenido de los sitios web, pero principalmente las relaciones que ellos entablan con otras personas mediante listas de correo, foros, chat etc. Estas personas son mucho más influyentes que el material que deambula en sitios pornográficos, por eso es importante fomentar el dialogo y la educación sexual, sin prejuicios, para que ellos puedan disfrutar de Internet sin inconvenientes y los padres podamos dormir tranquilos.

Gracias por su tiempo, Sra. Negri.

Gracias por dedicarle espacio a este tema. Fue un placer colaborar con ustedes.