CONFIGURACION DEL SERVIDOR PROXY SQUID

INTRODUCCIÓN

Un servidor Proxy HTTP, es básicamente un programa que acepta peticiones de clientes para las URL, obtiene, y devuelve los resultados al cliente. Los Proxys se utilizan en redes en la que los clientes no tienen acceso directo a Internet, pero tienen que ser capaces de ver páginas Web y para la memoria caché de las páginas comúnmente solicitadas, de manera que si más de un cliente quiere ver la misma página, sólo tiene que ser una vez descargada.

Muchas empresas y organizaciones tienen sus cortafuegos configurado para bloquear todas las entradas y salidas del tráfico en los sistemas internos LAN. Esto puede hacerse por razones de seguridad, o para limitar lo que los empleados puedan tener acceso al Internet. Debido a la posibilidad de ver páginas Web es muy útil, un Proxy es a menudo establecido de manera que los sitios Web se pueden acceder a través de él.

Las grandes organizaciones y proveedores de servicios de Internet con muchos ordenadores cliente, pueden querer acceder a la Web ejecutando un servidor Proxy para reducir la carga sobre sus redes. Una de las principales tareas de un servidor Proxy es el caché de las páginas solicitadas por los clientes, cualquier página solicitada más de una vez será devuelta de la memoria caché en lugar de descargarse del servidor originario. Por esta razón, a menudo se recomienda que los clientes usen un Proxy para acceder a la Web.

Un Proxy es útil solamente si el los navegadores de los clientes están configurados para utilizarlo en lugar de conectarse a sitios Web directamente. Afortunadamente, cada navegador en existencia y casi todos los programas permiten descargar archivos a través de HTTP para diversos fines pueden ser configurado para usar un Proxy.

Los Proxys no son sólo para HTTP - también pueden apoyar solicitudes de los clientes con protocolo Gopher y FTP. Incluso las conexiones encriptadas SSL puede ser manejado por un Proxy, a pesar de que no puede desencriptar la solicitud. En cambio, el Proxy simplemente envía todos los datos del cliente para el servidor de destino y viceversa.

Squid es el Proxy más popular servidor para sistemas Unix. Es libre y esta disponible para su descarga desde www.squid-cache.org, y se incluye como paquete estándar con todas las distribuciones de Linux y muchos otros sistemas operativos. Squid soporta Proxy, caching y aceleración HTTP, y tiene un gran número de opciones de configuración para controlar el comportamiento de estas características.

Squid lee su configuración desde el archivo de texto **`squid.conf`**, por lo general se encuentra en o bajo el directorio **`/etc`**. Este archivo consta de una serie de directivas, uno por línea, cada una de las cuales tiene un nombre y valor. Cada directiva establece algunas opciones, como el puerto TCP para escuchar un directorio o para almacenar en caché los archivos. en Webmin el módulo Squid edita este archivo directamente, haciendo caso omiso de cualquier comentario o directivas que no entiende.

Muchas versiones de Squid han sido liberadas a lo largo de los años, cada una de las cuales ha apoyado diferentes directivas de configuración o asignado diferentes significados a las mismas directivas. Esto significa que un archivo squid.conf de la versión 2.0 pueden no ser compatibles con Squid 2.5 - y uno de Squid 2.5 ciertamente no funcionará con la versión 2.0. Afortunadamente, Webmin sabe cuales directivas apoya cada despacho y sólo permite la edición de esos que se sabe que el funcionamiento según la versión.

Páginas Web almacenadas en caché se almacenan en archivos multi-nivel de estructura de directorios de ficheros para aumentar el rendimiento. Squid puede ser configurado para utilizar múltiples caché directorios separados, de modo que usted puede propagar ficheros a través de distintos discos para mejorar el rendimiento. Cada vez que una página es cacheable le pide que se almacene en un archivo, de modo que cuando una solicitud posterior para la misma página llega el archivo se puede leer los datos y sirve de ella. Debido a que algunas páginas Web cambian con el tiempo (o incluso son generadas dinámicamente), Squid mantiene un registro de la última modificación y fechas de vencimiento de páginas Web para que pueda borrar los datos de la caché cuando se está fuera de fecha.

El programa que actualmente maneja las peticiones de clientes tiene que ser un servidor que este funcionando permanentemente procesando llamados. También puede tener otros sub-procesos para tareas como búsquedas DNS o la autenticación del cliente, pero todo el procesamiento del protocolo HTTP se hace en el único proceso maestro. A diferencia de otros servidores como Apache o Sendmail, Squid no arranca sub-procesos para manejar las peticiones del cliente.

Squid pueden ser compilado en todas las distribuciones de Unix, Webmin apoya y trabaja casi idéntica en todas ellas. Esto significa que el módulo Webmin de la interfaz de usuario es el mismo a través de los sistemas operativos, a excepción de las rutas por defecto que utiliza para el Squid programas y ficheros de configuración.

EL MÓDULO DEL SERVIDOR PROXY SQUID

Si desea establecer o hasta configurar Squid desde Webmin, tendrá que utilizar el módulo Squid Proxy Server, que se encuentra bajo la categoría Servidores. Cuando se hace clic en el icono, la se muestra en la página la captura de la pantalla a continuación, en el supuesto de que Squid este instalado y configurado correctamente. Como puede ver, la página principal se compone sólo de una tabla de iconos, cada una de las cuales se puede hacer clic en para abrir un formulario para editar la configuración de esa categoría.

Webmin módulo Squid Proxy Server

Si no ha configurado o iniciado antes Squid en su sistema, el caché de directorio probablemente no ha sido establecido aún. El módulo de detección de este y mostrara un mensaje como ***Su caché Squid directorio /var/spool/ squid no se ha inicializado*** por encima de la mesa de iconos. Para inicializar la memoria caché, siga estos pasos:

1. Si no estás contento con el directorio caché que aparece, ahora es el momento de cambiarlo. Siga las instrucciones en la sección adición de directorios caché para definir sus propios directorios antes de continuar.
2. En el Unix escriba el nombre del usuario como campo que será el dueño del caché de archivos y el proceso se ejecutará como demonio. Normalmente esto será un usuario Squid creado para el propósito (y en el campo por defecto para los Squids en caso de que dicho usuario existe), pero de hecho cualquier usuario. Yo recomiendo el uso del módulo usuarios y grupos para crear un usuario llamado del Squid, cuyo directorio home es el directorio de caché si es necesario.
3. Haga clic en el botón Iniciar Cache. La configuración de Squid se actualizarán para utilizar su nombre de usuario elegido, y el comando **squid-z** se llevará a cabo para establecer el caché de directorios. Toda la salida que produce se mostrará de modo que usted pueda ver cómo la inicialización se está progresando.
4. Cuando el proceso haya finalizado, el regrese al módulo de la página principal y el mensaje de error debería haber desaparecido.

Si Squid no se instala, en su sistema (o esta instalado en una ubicación distinta a la que se espera Webmin), un mensaje de error como ***The Squid fichero de configuración /etc/squid.conf no existe*** aparecerá en la página principal en lugar de la el cuadro de iconos. Si realmente tiene instalado, lea la ***Configurar el servidor módulo Squid Proxy*** sección para obtener instrucciones sobre cómo cambiar los caminos de usos del módulo. Por otra parte, si realmente no está instalado debe usar el módulo de paquetes de software para instalar el paquete Squid de su distribución Linux CD o página Web.

Si no existe tal paquete de su sistema operativo, tendrá que descargar, compilar e instalar la última versión de Squid de www.squid-cache.org. Como siempre disponga de un compilador instalado en su sistema, este es un proceso relativamente simple, sin dependencias.

Una vez que se instala el servidor, tendrá que crear una acción que se ejecuta como un comando **`*/usr/local/squid/bin/squid-Sy *`**, suponiendo que usted tiene Squid instalado en **`/usr/local/squid`**.

Squid Una vez se ha instalado e inicializado, puede empezar a utilizar este módulo. Cuando Squid esta en funcionamiento, cada página tiene dos enlaces en la parte superior - **`Aplicar los cambios`** que fuerza la configuración actual a ser re-leída, y **`Stop Squid`** que apaga el servidor Proxy. Si el servidor no está funcionando, esos vínculos se sustituyen con **`*Inicio*`** en su lugar, que como su nombre indica intenta iniciar.

Debido a que cada versión de Squid ha introducido nuevas directrices de configuración, este módulo de interfaz de usuario aparecerá diferente dependiendo de la versión de Squid que detecta en su sistema. Todas las instrucciones de este capítulo se han escrito para Squid 2,4 ya que es actualmente la más ampliamente implementado versión. Si usted está ejecutando una liberación posterior, los distintos campos pueden aparecer en los formularios o tienen más o menos opciones. Por ejemplo, cada nueva versión ha introducido diferentes tipos de ACL, autenticación y ha sido tratado en tres formas diferentes a través de la historia del programa. Sin embargo, los conceptos básicos han sido siempre la misma.

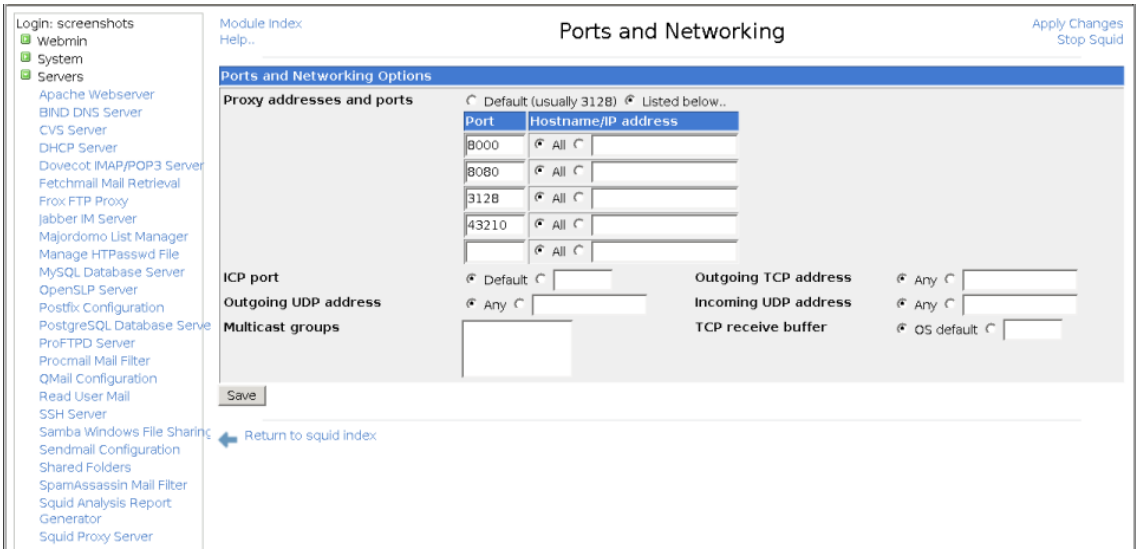
Cuando se está utilizando este módulo, asegúrese de que el navegador está configurado para no utilizar el Proxy Squid para acceder a su servidor Webmin. De lo contrario se corre el riesgo de cortar su propio acceso al módulo si haces un error de configuración o apagar el servidor. Todos los navegadores que puede utilizar un Proxy tienen un ámbito de inclusión en la lista de hosts para conectar directamente, en el que puede escribir el nombre de host de su servidor Webmin.

CAMBIAR DIRECCIONES DE PUERTOS EN EL PROXY

Por defecto, la escucha de peticiones del Proxy Squid es en el puerto TCP 3128 para todas las direcciones IP de su sistema. Debido a que este no es el puerto habitual asignado se ejecutan en (8000 y 8080 parece ser el más común), es posible que lo desee cambiar. Usted también puede editar la dirección de escucha de modo que sólo los clientes en su red interna se pueden conectar, si su sistema tiene más de una interfase de red.

Para especificar los puertos que usa Squid, siga estos pasos:

1. En el módulo principal de la página, haga clic en el icono puertos y conexión en red para abrir el formulario.
2. En el Proxy direcciones y puertos, seleccione continuación la opción A. En la tabla siguiente, cada fila define un puerto de escucha y, opcionalmente, una dirección de obligar a hacerlo. Todos los puertos existentes y direcciones aparecen en la lista, seguida de una sola fila en blanco para añadir una nueva. En el primer campo vacío en la columna Puerto, introduzca un número de puerto como el 8000 o 8080. En el nombre de la columna dirección IP, bien seleccionar a aceptar todas las conexiones en cualquiera de sus interfaces del sistema, o la segunda opción para ingresar una dirección IP en el cuadro de texto adyacente. El uso de este cuadro, Squid puede ser configurado para escuchar en el mayor número de puertos que lo desee. Sin embargo, debido a que sólo una línea en blanco aparece en un momento tendrá que guardar y volver a abrir la forma de añadir más de un nuevo puerto.
3. ICP es un protocolo utilizado por Squid para comunicarse con otros agentes en un grupo. Para escuchar en un puerto que no sea la predeterminada de 3130 para el ICP, rellene el puerto ICP campo. Esto no es necesario en general, sin embargo, otros Proxys usan este protocolo.
4. Squid normalmente aceptar conexiones ICP en cualquier dirección IP. Para cambiar esto, seleccione el segundo botón en la UDP Próximos campo de dirección y entrar en uno de sus interfaz del sistema de IPs en su campo de texto. Esto puede ser útil si todos los demás Proxys que su servidor pueda desea comunicarse con están en una sola LAN interna.
5. Haga clic en el botón Guardar en la parte inferior de la página para actualizar el archivo de configuración con la nueva configuración, a continuación, haga clic en Aplicar los cambios enlace a la página principal para activarlos.



Los puertos y la forma creación de redes

AGREGANDO DIRECTORIOS CACHÉ

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.

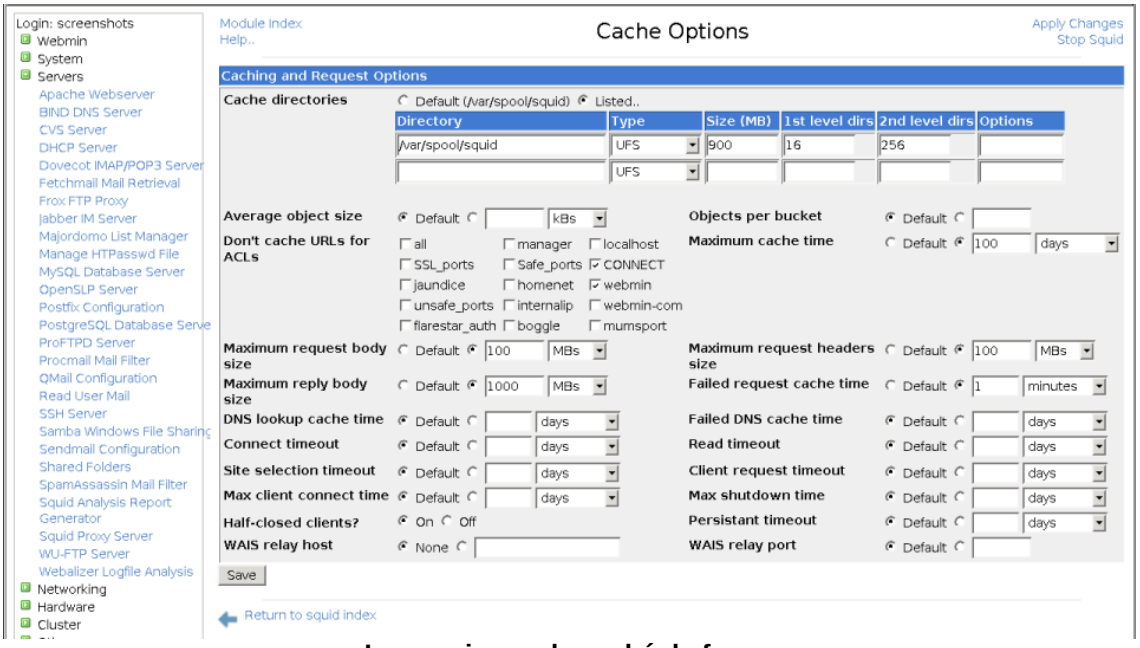
En un sistema que se dedica a ejecutar un servidor Proxy, el importe máximo de caché en cada directorio debe ser aproximadamente el 90% del espacio disponible. Es imprudente o configurar Squid para permitir utilizar todo el espacio libre en disco, ya que muchos sistemas de ficheros sufren menor rendimiento. 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.



Las opciones de caché de forma

EDICIÓN DE OPCIONES CACHING PROXY

Squid tiene numerosos ajustes que limitan el tamaño de caché de objetos, el tamaño de las peticiones de los clientes y los tipos de páginas de caché. Se pueden utilizar para detener el servidor de almacenamiento de enormes archivos (como descargar imágenes ISO), para limitar el tamaño de los archivos que los clientes pueden cargar o descargar, y para evitar la caché de páginas que cambian con frecuencia (como los generados por los scripts CGI). Los valores por defecto por lo general funcionan bien, sin embargo, con la posible excepción del tamaño de subida máxima que sólo es 1 MB.

Para editar las opciones de almacenamiento en caché, siga estos pasos:

1. Haga clic en el icono Opciones de caché de la página principal para mostrar el formulario para mostrar una vez más por encima.
2. Para definir el tamaño máximo de archivos que ha subido, seleccionar la segunda opción en la máxima solicitud tamaño corporal sobre el terreno, introducir un número en el cuadro de texto y seleccionar algunas unidades en el menú.
3. MB debería ser más que suficiente para cualquiera.
4. Para detener la descarga de clientes archivos de gran tamaño, a llenar la máxima respuesta tamaño corporal sobre el terreno de la misma manera. Esto podría ser usado por impedir el uso indebido de su red de clientes la descarga de grandes películas o archivos ISO, pero a menudo puede ser subvertido por la descarga de un archivo grande en trozos.
5. Si desea establecer un límite superior en el archivo de una página que puede ser almacenada en la caché, rellene el tiempo máximo de caché de campo en vez de dejar que los predeterminados. De lo contrario los datos se almacenan en caché para un máximo de un año, o hasta que expire la fecha fijada por el servidor de origen.
6. Así como la memoria caché los archivos descargados, Squid recordarán los mensajes de error de servidores y devolverlos a los clientes que soliciten la misma página. Puede cambiar la cantidad de tiempo que los errores

se guardan en caché por introducir un número y la selección de unidades de la solicitud Error caché tiempo sobre el terreno. Si se elige por defecto, los errores se almacenan en caché durante 5 minutos. Incluso esto puede ser molesto mucho si usted acaba de fijarse un error en un sitio Web aunque.

7. Squid cachea de las respuestas a las búsquedas de host para reducir la cantidad de DNS actividad, independientemente de la TTLS que el suministro de servidores DNS. Si está seleccionado por defecto en la caché de DNS lookup tiempo sobre el terreno, las respuestas será recordado por 6 horas. Si esto parece mucho para usted, seleccione el segundo botón y escriba su propia caché tiempo su lugar.
8. El No caché URL para ACLs campo puede ser usado para prevenir completamente la memoria caché para ciertos URL, servidores Web o clientes. Toda solicitud que coincide con una de las ACLs comprobado en este ámbito nunca serán caché, y, por tanto, siempre será descargue directamente. Puede utilizar esta función para bloquear el caching de páginas generadas dinámicamente mediante la creación de una ruta de URL para REGEXP ACL. Cgi o cgi-bin y seleccionando aquí. Véase el Uso de listas de control de acceso sección para más detalles sobre cómo ACLs trabajo y puede ser definido.
9. Pulse el botón Guardar en la parte inferior de la página, para volver al menú principal. Dado que algunas opciones adicionales se deposita en la memoria y el uso de disco, haga clic en el icono Uso de la memoria para mostrar que.
10. Para limitar la cantidad de memoria que va a utilizar Squid, rellene el uso de memoria límite de campo. Tenga en cuenta que este límite sólo efectos el máximo de memoria utilizada para el almacenamiento en tránsito y con frecuencia acceder a los archivos, y las respuestas negativas. Porque Squid utiliza la memoria para otros fines, sin duda, consumen más de lo que entre aquí. Si se selecciona por defecto, un límite de 8 MB a ser aplicada, que es probablemente demasiado baja para un servidor ocupado.
11. Para evitar el almacenamiento en caché de archivos grandes, llenar en el máximo tamaño de caché objeto sobre el terreno. El valor por defecto es sólo de 4 MB, así que si usted tiene un montón de espacio en disco que debería ser aumentado.
12. Pulse el botón Guardar en la parte inferior del formulario y luego la Aplicar cambios enlace en la página principal de activar todos los de su nueva configuración.

INTRODUCCIÓN A LAS LISTAS DE CONTROL DE ACCESO

ACLs (listas de control de acceso) son posiblemente Squid más potente característica. Un ACL es simplemente una prueba que se aplica a petición de un cliente para ver si éste coincide o no. Luego, sobre la base de la ACL que coincide con cada solicitud se puede optar por bloquear, impedir que la memoria caché, la fuerza que un retraso en la piscina, o entregarlos a otro servidor Proxy. Muchos tipos diferentes de ACL existe - por ejemplo, un tipo comprueba una dirección IP del cliente, coincide con la otra URL que se solicita, mientras que otros comprobar el puerto de destino, nombre de host del servidor Web, el usuario autenticado y así sucesivamente.

El uso más común de ACLs está bloqueando las conexiones de clientes fuera de su red. Si ejecuta un servidor Proxy, lo que está conectado y accesible desde Internet, hosts fuera de tu red local no debe permitirse que la utilicen. Malintencionado de personas suelen utilizar otros poderes para el blanqueo de conexiones utilizados para la piratería, el envío de spam o acceder a sitios Web que no debe permitirse.

Debido a que el representante especial CONNECT solicitud puede ser utilizado para conectar a cualquier puerto, una lista ACL se utiliza a menudo para bloquear su uso para cualquier puerto que no sea 443 (el SSL por defecto). Esto deja de usuarios a través de su servidor Proxy para conectarse a servidores que no sean servidores Web, tales como AIM, ICQ o MSN. Del mismo modo, una lista de control de acceso puede configurarse para bloquear las normales peticiones HTTP como a los puertos 22, 23 y 25 que se utilizan normalmente para ssh, telnet y SMTP.

Sólo la definición de una lista de control de acceso a la configuración de Squid en realidad no hacer nada - que debe ser aplicado de alguna manera a tener efecto alguno. En esta sección se explica cómo usarlos para controlar el que se pide a su servidor son autorizados o rechazados. Otras secciones explican cómo se relacionan con la memoria caché y el acceso a otros servidores.

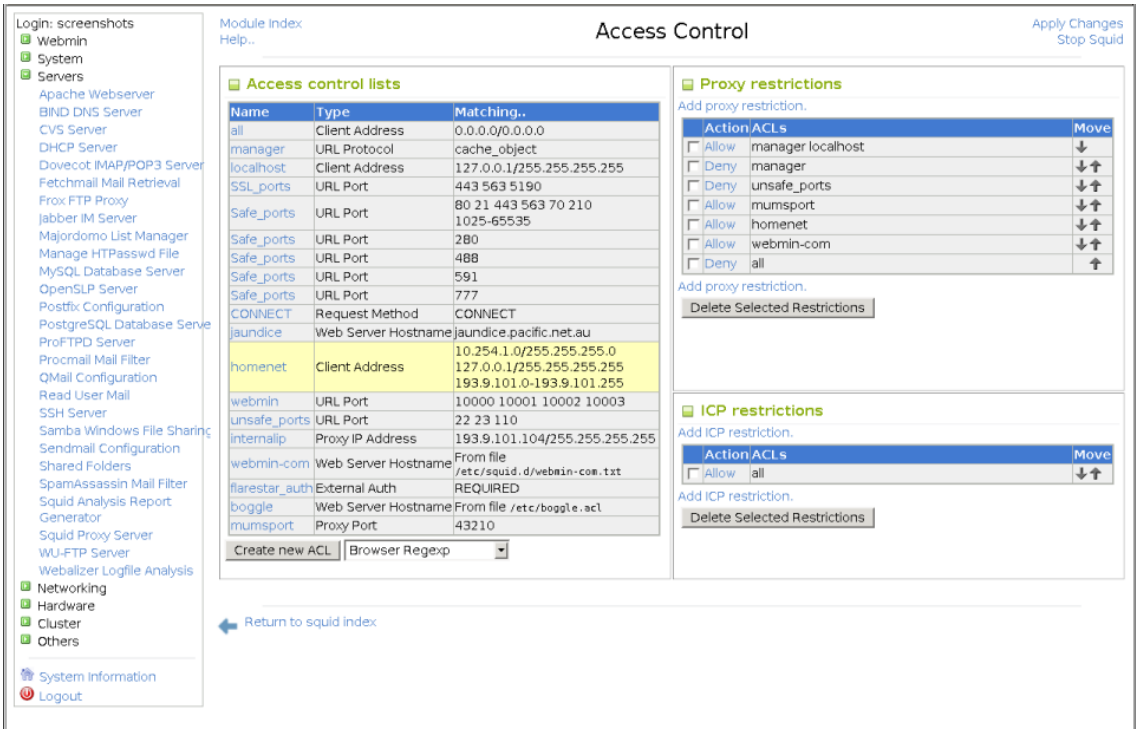
Cuando se recibe una solicitud, Squid primero determina que se halla en consonancia con ACLs. A continuación, se compara esta lista de partidos en contra de una lista de restricciones del Proxy, cada uno de los cuales contiene uno o varios ACLs una acción y llevar a cabo (ya sea Permitir o Denegar). Tan pronto como una restricción se comprueba que coincide con la ACL para la solicitud, su acción determina si la petición se acepta o niega. En caso de que no coincidan con las restricciones, lo contrario de la última acción en la lista se aplica. Por esta razón, el acto final en la mayoría de configuraciones de Squid es Permitir o Denegar todas.

ICP solicitudes presentadas por los demás apoderados se ha comprobado también que a ver que coinciden con ACLs, y comparado frente a una similar pero diferente lista de ICP restricciones para ver si se les permitirá o no. Véase la

Conexión a otros apoderados sección más tarde por una explicación más compleja de lo que es ICP y cuando se utiliza.

La típica configuración por defecto de Squid incluye varios ACLs y las restricciones del Proxy. Por razones de seguridad, todos los pedidos desde cualquier lugar se les niega por defecto. Esto significa que usted tendrá que cambiar la lista de restricciones antes de que nadie pueda usar su poder. Siga leyendo para averiguar cómo.

Para ver las listas de ACLs definidas, las restricciones del Proxy y el ICP restricciones, haga clic en el icono de control de acceso en el módulo de la página principal. Como la imagen que aparece a continuación muestra una tabla de ACLs mostrando sus nombres, tipos, y los partidos se muestra a la izquierda. A la derecha están los cuadros de Proxy y PCI restricciones mostrando sus acciones y las ACLs que coinciden. La restricción cuadros han flechas arriba y abajo junto a cada entrada para moverlos a la lista, porque su fin.



Las listas de control de acceso

Antes los clientes pueden usar su Proxy tendrás que configurarlo para permitir el acceso de algunas direcciones. Las medidas en este sentido son las siguientes:

1. El control de acceso a la página, seleccione Cliente Dirección del menú a continuación la lista de las ACLs. Al hacer clic en Crear nuevo el botón ACL, un formulario para entrar en direcciones coincidentes aparecerá.
2. En el campo Nombre de ACL, introduzca un nombre corto, como tu red.
3. En el campo vacío bajo Desde el IP introduzca la dirección IP a partir de la gama de permitir, como 192.168.1.1.
4. Si el campo a la propiedad intelectual en virtud de entrar en la dirección que termina en la gama, como 192.168.1.100. Sólo los clientes que entran dentro de esta gama de coincidir con el ACL. No introduzca nada en el campo de máscara de red.
5. Alternativamente, puede especificar una red IP mediante la introducción de la dirección de red en el ámbito de la propiedad intelectual, y la máscara de red (como 255.255.255.0) en el campo de máscara de red. Para introducir más de uno, usted tendrá que guardar y volver a editar esta lista de control de acceso de forma que los nuevos campos aparecen en blanco.
6. Haga clic en el botón Guardar para añadir la lista de control de acceso y volver a la página de control de acceso que en su nueva lista de control de acceso serán enumerados.
7. Haga clic en Añadir Proxy restricción por debajo de la mesa Proxy restricciones.
8. En el formulario que aparece, seleccione Permitir a partir de la acción sobre el terreno.
9. En el Match ACLs lista, seleccione su nuevo yournetwork ACL.

10. Haga clic en el botón Guardar en esta forma para volver a la página de control de acceso de nuevo. La nueva restricción se mostrará en la parte inferior de la tabla, muy probablemente por debajo de la Denegar todas las entradas.
11. Haga clic en la flecha hacia arriba al lado de su nueva restricción a pasar por encima de todos los Denegar. Esto le dice Squid para permitir las conexiones de su red, y negar todos los demás.
12. Por último, haga clic en el vínculo Aplicar cambios en la parte superior de la página. El Proxy será utilizable por los clientes en su red interna, pero nadie más!

Estas instrucciones asumen que usted está comenzando con la configuración por defecto de Squid. Si el Proxy ya se ha configurado para permitir el acceso desde cualquier lugar (por el cambio de denegar todas las restricciones para permitir a todos), debe volver a cambiarlo de nuevo para bloquear clientes de fuera de su red. Para obtener más información sobre los tipos de ACL disponibles y cómo utilizarlos, lea las siguientes dos secciones.

CREACIÓN Y EDICIÓN DE ACLS

Antes de que pueda bloquear o permitir las solicitudes de algunos dirección, en cierta servidor o por alguna página que tendrá que crear un ACL. Los pasos básicos para hacer esto son los siguientes:

1. Seleccione el tipo de ACL para crear desde el menú desplegable que aparece debajo de la listas de control de acceso tabla y haga clic en el botón **`* Crear una nueva lista de control de acceso *`**.
2. En el formulario que aparece, introduzca un nombre para su nueva ACL ACL en el campo de nombre. Si más de uno tiene el mismo nombre, será tratado como corresponde en caso de cualquier ACL con ese nombre partidos. El nombre debe consistir únicamente de letras y números, sin espacios o caracteres especiales.
3. Complete el resto de la forma como se explica en el siguiente cuadro.
4. El incumplimiento en el campo URL, introduzca una URL completa que los clientes que se les niega de esta ACL será redirigida. Esto le permite definir páginas de error personalizado que se mostrará en lugar del default Squid respuestas.
5. Haga clic en el botón Guardar en la parte inferior del formulario.

Una vez que una ACL se ha creado puede editar haciendo clic sobre su nombre en la lista, el cambio de los campos y haga clic en Guardar. O su puede eliminarla (en caso de que no está en uso por parte de algunos Proxy o restricción ICP) con el botón "Eliminar". Como de costumbre, el vínculo Aplicar cambios deben ser utilizados para activar los cambios que se realicen.

Squid tiene un asombroso número de ACL tipos, aunque no todos están disponibles en todas las versiones del servidor. En el cuadro siguiente figura una lista de los que puede crear para Squid 2,4, y explica lo que hacen y lo que los ámbitos en el formulario de creación de una lista ACL para cada tipo de media:

Muchos tipos de ACL no son adecuados para determinadas situaciones. Por ejemplo, si un cliente envía una petición CONNECT la ruta de URL no está disponible, y, por tanto, una ruta de URL REGEXP ACL no funcionará. En casos como este es la ACL no supone automáticamente a la altura.

CREACIÓN Y EDICIÓN RESTRICCIONES DEL PROXY

Una vez que haya creado algunos ACLs, que pueden ponerse en uso mediante la creación, edición y se desplazan en torno a las restricciones del Proxy. Squid comparará cada una de las solicitudes a todas las restricciones definidas en fin, parando cuando se encuentra uno que se ajuste. La acción conjunto para que la restricción entonces determine si la petición se acepta o niega. Este sistema de procesamiento combinado con el poder de ACLs le permite establecer algunos increíblemente complejas reglas de control de acceso - por ejemplo, puede negar el acceso a todos los sitios con temblor en la URL entre 9 AM y 5 PM de lunes a viernes, excepto para determinados clientes direcciones.

Para crear un Proxy restricción, siga estos pasos:

1. Haga clic en el icono de control de acceso en el módulo de la página principal para abrir la página se muestra en la captura de pantalla anterior.
2. Haga clic en Añadir Proxy restricción a continuación la lista de las restricciones existentes para ir al formulario de creación.
3. Desde el campo de acción seleccione Permitir o Denegar en función de si desea se pongan en venta las solicitudes para ser procesado o no.
4. El Match ACLs lista puede ser usado para seleccionar varios ACLs que si todos son fiel a desencadenar la acción. Del mismo modo, la no coinciden ACLs campo puede ser usado para seleccionar ACLs que no

coinciden con los de la acción para ser activado. Es perfectamente válido para hacer las selecciones de ambas listas para indicar que la acción debe ser activado sólo si todas las ACLs a la izquierda y si coinciden con los de la derecha no lo hacen. En su configuración por defecto de Squid tiene un ACL llamado a todos los partidos que todas las solicitudes. Puede ser útil para crear restricciones que permitir o negar a todo el mundo, uno de los cuales por lo general existe por defecto.

5. Haga clic en el botón Guardar para crear la nueva restricción y volver a la página de control de acceso.
6. Utiliza las flechas junto a ella en la mesa Proxy restricciones para moverlo al lugar correcto. Si su lista termina con un Denegar todas las entradas, tendrá que desplazarse fuera de la parte inferior para que tenga efecto alguno. Si la lista tiene una entrada que permite a todos los clientes de su red y que usted acaba de añadirse una restricción a denegar el acceso a algunos sitios, usted tendrá que pasar por encima de lo que permiten la entrada y para que pueda ser utilizado.
7. Cuando haya acabado la creación y posicionamiento de las restricciones, pulse el vínculo Aplicar cambios en la parte superior de la página para que sean activos.

Después de un Proxy restricción se ha creado puede editar haciendo clic en el vínculo que aparece en la columna Acción para su fila en la tabla. Esto traerá una edición de forma idéntica a la utilizada para la creación de la restricción, pero con Guardar y Eliminar botones en la parte inferior. El primero se guardará cualquier cambio que hagas en la acción o se pongan en venta ACLs, mientras que el segundo se eliminará la restricción por completo. Una vez más, el vínculo Aplicar cambios deben ser utilizados con posterioridad a la actualización o la supresión de una restricción para hacer el cambio activo. Si por alguna razón suprimir todas las restricciones del Proxy, Squid permitirá a todas las peticiones de todos los clientes, que probablemente no es una buena idea.

También en la página de control de acceso es un cuadro para la edición y la creación de las restricciones que se aplican a las solicitudes del PCI ***A medida que la Conexión a otros apoderados*** sección se explica, el PCI es un protocolo utilizado por proxys Squid en un grupo o jerarquía a fin de determinar qué otros servidores URL han caché. Puede agregar y editar las entradas en el PCI restricciones mesa exactamente de la misma forma que las restricciones de Proxy. Si realmente está ejecutando un clúster de servidores Proxy, puede tener sentido para bloquear el PCI solicitudes de otras fuentes distintas de su propia red. Si no es así, la configuración por defecto que permite a todos los paquetes PCI está bien.

CONFIGURACIÓN DE AUTENTICACIÓN DEL PROXY

Aunque es posible configurar Squid para permitir el acceso sólo a determinadas direcciones IP, puede que quiera a la fuerza a los clientes a autenticar el Proxy también. Esto podría tener sentido si se quiere dar sólo ciertas personas el acceso a la Web, y no puede utilizar la dirección IP de validación debido al uso de direcciones asignadas dinámicamente en su red. También es útil para seguir la pista de que lo que ha solicitado a través del Proxy, como nombres de usuario se registran en los registros de Squid.

Todos los navegadores y programas que pueden hacer uso de un Proxy también apoyo Proxy de autenticación. Navegadores aparecerá una ventana de acceso para ingresar un nombre de usuario y contraseña que se enviará a los Proxy la primera vez que les pide, y automáticamente enviar la misma información para todas las solicitudes posteriores. Otros programas (como wget o rpm), exigen el nombre de usuario y contraseña que se especifica en la línea de comandos.

Cada nombre de usuario y contraseña recibidos por Squid se pasa a un programa de autenticación externa, ya sea que lo aprueba o lo niega. Normalmente este programa los controles contra los usuarios de un archivo, pero es posible escribir sus propios programas que utilizan todo tipo de métodos de validación de los usuarios - por ejemplo, podrían ser consultados en una base de datos, o un servidor LDAP, o el usuario de Unix lista. Webmin Webmin viene con un sencillo programa que lee los usuarios de un archivo de texto con el mismo formato que es utilizado por Apache, y este módulo les permite a los usuarios editar dicho archivo.

Entre las medidas que a su vez, para su autenticación Proxy Squid son las siguientes:

1. En el módulo principal de la página, haga clic en el icono de control de acceso para abrir el formulario.
2. Seleccione **Auth** en el menú debajo de la mesa de ACL y pulse Crear el nuevo botón ACL.
3. En el formulario que aparece, introduzca auth para el ACL nombre y seleccione Todos los usuarios en el exterior auth usuarios sobre el terreno. Después haga clic en el botón Guardar.
4. Haga clic en Agregar restricción por debajo de Proxy Proxy restricciones mesa.
5. Seleccione Denegar en el ámbito de acción, y elegir su nueva autorización de la ACL no se corresponden con la lista ACL. Esto bloquear cualquier Proxy peticiones que no están autenticadas, lo que obliga a los clientes de acceso. Selección Permitir y, a continuación, la elección de autoridades de la Match ACLs campo puede

ser usado para un propósito ligeramente diferente. Esto crea un servidor Proxy que permite restringir el acceso a todos los clientes autenticados, que puede ser colocado a la fuerza clientes fuera de su red para acceder a su cuenta mientras que no se requieren para aquellos dentro de la red.

6. Haga clic en el botón **"Guardar"** para regresar a la página de control de acceso de nuevo.
7. Utilice la flecha hacia arriba junto a la nueva restricción a pasar por encima de cualquier entrada en la tabla que permite el acceso de todos a su propia red. Si es por debajo de esa entrada, los clientes de la red será capaz de usar el Proxy sin necesidad de conectarse a todos. Por supuesto, esto puede ser lo que quieres en algunos casos.
8. Volver a la página principal, haga clic en el icono de programas de autentificación.
9. Desde el programa de autenticación de campo Webmin seleccionar por defecto. Esto le dice al módulo de utilizar el simple archivo de texto autenticador que viene con el módulo de modo que usted no tiene que escribir el suyo propio. Por supuesto, usted puede especificar su propio programa personalizado de selección del último botón y entrar en la ruta completa a un script con algunos parámetros en el cuadro de texto adyacente. Este programa debe leer continuamente las líneas que contengan un nombre de usuario y una contraseña (separados por un espacio) como entrada y salida para cada línea o bien el OK o ERR para el éxito o el fracaso, respectivamente. Squid se ejecute varias instancias del programa, ya que los procesos permanentes demonio cuando se inició.
10. La ventana de acceso que aparece en los navegadores incluye una descripción del servidor Proxy, lo que el usuario está accediendo a. Por defecto, esto es Squid Proxy-caché del servidor Web, pero puede introducir sus propios (como Ejemplo Corporación Proxy) rellenando el Proxy de autenticación sobre el terreno.
11. Normalmente, se cache Squid de acceso válido durante 1 hora para evitar que se pongan en el programa de autenticación por cada solicitud. Esto significa que la contraseña cambios pueden tardar hasta una hora en surtir efecto, que puede ser confuso. Para reducir este límite a costa de una mayor carga del sistema y un poco más lento petición de procesamiento, editar el tiempo de caché de contraseñas para el campo.
12. Haga clic en el botón Guardar y, a continuación, haga clic en Aplicar cambios a la página principal.

Ahora que la autenticación está habilitada, cualquier intento de utilizar su poder de un navegador Web causará una ventana de acceso a aparecer. Dado que los usuarios no válidos se han definido aún de acceso no serán aceptadas, lo cual no es particularmente útil! Para crear algunos usuarios para la autenticación, siga estos pasos:

1. Haga clic en el icono del Proxy de autenticación en el módulo de la página principal para que aparezca un cuadro con Proxy los usuarios. En un primer momento, este campo aparecerá vacío.
2. Haga clic en el botón Agregar un nuevo Proxy los usuarios enlace de arriba o por debajo de la mesa para mostrar el formulario de creación de usuario.
3. Introduzca un nombre de inicio de sesión en el campo nombre de usuario y una contraseña para el usuario en el campo Contraseña. NOTA - El nombre de usuario debe ser introducido en minúsculas!
4. Para desactivar temporalmente este usuario sin borrar él, el cambio Activado? Campo a No.
5. Pulse el botón Crear para añadir el usuario y, a continuación, haga clic en el vínculo Aplicar cambios. Este último paso es necesario después de la creación de un usuario para que los cambios surtan efecto, como Webmin Squid autenticación del programa sólo lee el archivo de usuario cuando empecé.

Un usuario puede editar haciendo clic en su nombre en la lista de usuarios Proxy, cambiar el nombre de usuario, contraseña o permitido la situación y golpear el botón Guardar. También puede eliminar completamente un usuario con el botón **"Eliminar"** en su edición de forma. Una vez más, Aplicar cambios hay que hacer clic para hacer las modificaciones o supresiones activa. Asimismo, se cache Squid contraseñas válidas (como se ha explicado anteriormente) para reducir la carga sobre el programa de autenticación, por lo que un cambio de contraseña puede tomar algún tiempo para surtir efecto.

El módulo de gestión de usuario de la característica sólo funcionará si elige Webmin por defecto en el programa de autenticación de campo, o si su propio programa toma la ruta completa a un estilo de Apache usuarios archivo como parámetro. Si su programa valida usuarios contra algún otro servidor o base de datos, o si el módulo no puede averiguar qué fichero contiene los usuarios de mando, el Proxy de autenticación icono no aparecerá.

A veces puede que desee permitir que los usuarios habituales de Unix para acceder a su programa con la misma contraseña que utilizan para telnet y ftp. A pesar de que es posible escribir un programa que hace de Proxy de autenticación contra la base de datos de usuarios de Unix, existe otra solución - configurar el módulo para añadir, borrar y actualizar Proxy los usuarios de Unix cuando un usuario es creado, eliminado o renombrado. Esto es muy útil para mantener los nombres de usuario y contraseñas en sincronización sin necesidad de conceder el acceso a cada usuario de Unix. Una vez que haya establecido la autenticación normal como se ha explicado anteriormente, la sincronización puede ser activada por los siguientes pasos:

1. En el módulo principal de la página, haga clic en el vínculo del módulo de configuración en la esquina superior izquierda.
2. Como sus nombres indican, los usuarios Crear Proxy al crear usuarios de la red, actualización de Proxy los usuarios al actualizar los usuarios del sistema y Eliminar Proxy los usuarios al eliminar usuarios del sistema de control de los campos de creación automática, modificación y supresión de Proxy los usuarios cuando lo mismo sucede con un usuario de Unix. Para cada uno puede seleccionar Sí o No. Recomiendo de inflexión en la sincronización de actualizaciones y supresiones, pero dejando fuera de las creaciones de manera que puede hacerla el control que le da acceso al Proxy.
3. Pulse el botón Guardar en la parte inferior del formulario para activar la nueva configuración. A partir de ahora, las acciones realizadas en la Webmin usuarios y grupos módulo también el efecto Squid lista de usuarios en las maneras en que usted ha elegido. Sin embargo, la adición de un usuario a la línea de comandos con useradd o cambiar una contraseña con el comando passwd no.

Ver UsersAndGroups para obtener más detalles sobre la forma de sincronización con otros módulos de las obras y cómo activarlo.

CONFIGURACIÓN DEL REGISTRO

Squid escribe a cada uno de los archivos de registro, uno para el registro de las solicitudes de acceso de cliente, una caché de eventos y otro para información de depuración. La más útil es el archivo de registro de acceso, que pueden ser analizados por un programa como Webalizer para generar informes sobre los clientes, pidió a las URL y los usuarios individuales. El registro está habilitado de forma predeterminada a caminos compilados en Squid y, por tanto, depende de su sistema operativo, pero se puede cambiar los destinos para los archivos de registro y algunos detalles del formato de registro de acceso.

Para configurar cómo y dónde se escriben los registros, siga estas instrucciones:

1. Haga clic en el icono de registro en el módulo de la página principal, que previsiblemente le llevará al registro.
2. Para cambiar la ubicación del cliente de acceso del archivo de registro, editar el contenido del archivo de registro de acceso sobre el terreno. Si se selecciona por defecto, el camino compilado en Squid se utilizará (que puede ser **`/usr/local/squid/log/access.log`** o **`/var/log/squid/ access.log`**).
3. Para cambiar la ubicación de la memoria caché de almacenamiento de registro, editar el archivo de registro de almacenamiento sobre el terreno. El valor por defecto es siempre la store.log en el mismo directorio que el archivo **`access.log`**.
4. Para cambiar el camino que el debug log está escrito a manera de editar el archivo de registro de depuración sobre el terreno. Una vez más, el valor por defecto es cache.log en el mismo directorio que access.log.
5. Squid normalmente utiliza su propio formato personalizado para el registro de acceso. Para forzar el uso del formato utilizado por Apache en lugar de ello, cambiar el uso httpd formato de registro? Campo a Sí. Este formato puede ser necesario para la transformación de algunas aplicaciones, pero no registra toda la información que la opción por defecto hace.
6. Para escribir Squid han resuelto cliente nombres de host para el registro de acceso en lugar de sólo las direcciones IP, seleccione Sí en el Registro de nombres de host completo? Campo. Esto evita la necesidad de resolverlos más tarde, cuando la generación de informes, pero se ralentizará el servidor debido al tiempo que invertir búsquedas DNS puede tomar.
7. El ident o RFC931 protocolo puede ser usado para encontrar el nombre del usuario de Unix que está haciendo una conexión con el Proxy de algunos host remoto. Lamentablemente, es a menudo discapacitados y no apoya a otros sistemas operativos, por lo que es de uso limitado. Sin embargo, puede configurar Squid RFC931 para incluir la información a los usuarios el acceso a su archivo de registro de la selección de algunas de las ACLs en el RFC931 ident Realizar búsquedas de ACLs sobre el terreno. Idealmente, usted debe crear un cliente especial Dirección ACL que coincide con sólo Unix hosts con el demonio ident en su red y seleccionar sólo. Si lo hace permitir búsquedas usuario remoto, el tiempo de ident RFC931 campo puede ser usado para fijar una cantidad máxima de tiempo que va a Squid esperar una respuesta de un cliente. Si se selecciona por defecto el servidor esperará como máximo 10 segundos para una respuesta antes de darse por vencido (pero que aún permite la solicitud).
8. Haga clic en el botón Guardar en la parte inferior de la página para registrar los cambios introducidos en este formulario, y luego el vínculo Aplicar cambios a activarlos.

Muchos paquetes de Linux Squid incluyen un archivo de configuración para el programa logrotate para tener los archivos de registro rotar, comprimido y eventualmente suprimido cuando se convierten en demasiado viejos. Si cambia los caminos a los archivos de registro siguiendo las instrucciones descritas anteriormente, la rotación ya no será realizada y los logs pueden consumir sin límites y la cantidad de espacio en disco. En un sistema ocupado, esto

podría dar lugar a una escasez de espacio en el registro de ficheros que se evitarían si la rotación se encuentra en vigor.

CONEXIÓN A OTROS PROXYS

En lugar de recuperar pidió directamente las páginas Web, Squid se puede configurar para conectarse a otro servidor Proxy en lugar y algunas o todas las peticiones a él. Esta función es útil si su organización tiene un poder para cada departamento y un maestro para la caché de toda la red, y quiere tener todos los poderes departamento de consulta para el maestro pide que no pueden servir de sus propios escondites. También puede ser necesario si su proveedor de acceso a Internet se ejecuta un servidor Proxy y que desea configurar Squid para su red doméstica como así, y aún así hacer uso de la caché del ISP.

Al hacer uso de ACLs para categorizar las solicitudes, puede configurar Squid que transmita sólo algunas peticiones a otro Proxy, mientras que el resto de manipulación con normalidad. Por ejemplo, su Proxy puede manejar siempre las peticiones de páginas Web en su red local, pero sigue con interés todo lo demás a un maestro Proxy caché del sistema.

Para configurar su servidor para hacer uso de otro Proxy para las solicitudes salvo las dirigidas a una determinada red o dominio, siga estos pasos:

1. En el módulo principal de la página, haga clic en el icono de control de acceso.
2. Crear un servidor Web de host o Dirección Web Server ACL que coincide con los servidores Web del servidor Proxy que debe buscar directamente. Llame a la lista de control de acceso directo, por ejemplo.
3. Volver a la página principal y haz clic en el icono Otros cachés para abrir una página que contiene una lista de otros conocidos servidores Proxy (si lo hubiere), y una forma de opciones de configuración que controlan cuando se utilizan.
4. Haga clic en "Añadir otro caché para ir a la caché de acogida creación.
5. En el nombre del campo, introduzca el nombre de host completo del capitán caché del servidor, tales como bigproxy.example.com. No sólo tiene que introducir bigproxy, como Squid a veces tiene dificultad para resolver los no-canónico nombres DNS.
6. Desde el menú seleccione Tipo padre, que le dice a Squid que este otro Proxy se encuentra en un nivel más alto (y, por tanto, tiene más páginas en caché) que los suyos.
7. En el campo Proxy puerto entrará un número de puerto que el otro Proxy está a la escucha, como el 8080.
8. En el campo puerto PCI entrar en el puerto que utiliza el Proxy para el PCI solicitudes, que suelen ser 3130. Si no sabe o el capitán del Proxy no es compatible con PCI, de todos modos entrará 3130.
9. Pulse el botón Guardar en la parte inferior de la página para volver a la lista de otros escondites.
10. En el formulario que aparece al final de esa página es una sección titulada ACLs a buscar directamente, que es en realidad una lista ACL cuadro similar al Proxy restricciones cuadro se explica en la Creación y edición de la sección Proxy restricciones. Sin embargo, en lugar de permitir o denegar las solicitudes que determina cuáles son obtenidos directamente y que se remiten a otra caché. Utilice el botón Agregar para buscar ACLs enlace directamente a la primera añada una entrada para permitir que su lista de control de acceso directo y, a continuación, uno a negar todas las ACL. Esto le dice Squid directamente a buscar las páginas locales de los servidores Web, pero pasa todos los demás peticiones al Proxy elegido.
11. Por último, haz clic en Aplicar cambios en la parte superior de la página para tener Squid empezar a utilizar el otro servidor Proxy.

Si sólo quieres tener tu Proxy adelante todas las peticiones a otro, independientemente de su destino, paso por encima de 10 puede ser omitido por completo. Esto funciona porque Squid utilizará los otros Proxy configurado por defecto si no ACLs se han creado a fuerza de obtención directa de determinadas solicitudes.

En una gran red con muchos clientes, un solo sistema que ejecute Squid puede no ser capaz de mantener el volumen con las peticiones de los clientes. Por ejemplo, una gran compañía con cientos de empleados en funcionamiento todos los navegadores Web o un ISP que ha creado un Proxy para los clientes podría poner una enorme carga en un solo servidor Squid. Una solución sería actualizar a una versión más potente máquina - otra sería la de instalar Squid en múltiples sistemas de propagación y el Proxy de carga entre ellos.

Esto es típicamente realizada por la creación de un registro de direcciones DNS para cada sistema de Proxy, todos con el mismo nombre (como proxy.example.com), pero diferentes direcciones IP. Entonces, cuando un cliente busca la dirección IP para proxy.example.com que volver todas las direcciones, y elegir uno al azar de manera efectiva a conectar. Otra alternativa es instalar una capa cuatro interruptor que puede re-direccionar el tráfico hacia la misma

dirección IP a diferentes destinos, tales como múltiples servidores Proxy. Esto es más cara (cuatro conmutadores de capa no es barata), pero más fiable, porque un servidor puede ser detectado y que no se utilicen.

Sin embargo, hay un problema con el uso de varios servidores - cada uno mantiene su propia caché, de modo que si dos clientes solicitar la misma página Web a partir de dos distintos poderes será descargado dos veces! Esto niega la mayor parte de los beneficios de la ejecución de un caching Proxy.

Afortunadamente, Squid tiene características que resolver este problema. Puede ser configurado para contactar con otros escondites en el mismo grupo para cada solicitud, y preguntarles si ya tienen la página en caché. Si es así, se recuperará de los demás en lugar de Proxy de los originarios Web. Debido a que todos los agentes en una organización suelen ser conectado a través de una red rápida, es mucho más eficiente. El protocolo utilizado para este inter-cache de comunicación se llama PCI, y sólo es usado por Squid.

Para configurar dos o más apoderados para hablar unos con otros con el PCI, los pasos a seguir en cada sistema son los siguientes:

1. En el módulo principal de la página, haga clic en el icono Otros cachés.
2. Haga clic en "Añadir otro caché para abrir el caché de acogida creación.
3. En el nombre del campo introduzca el nombre de host completo de uno de los otros escondites.
4. Desde el menú seleccione Tipo hermano, lo que indica que el caché de otros está en el mismo «nivel» como éste.
5. En el puerto del Proxy, escriba el puerto HTTP que el otro escucha en Proxy.
6. En el puerto PCI, escriba el número de puerto que el Proxy otros usos para el PCI (generalmente 3130).
7. Pulse el botón Guardar para añadir el otro Proxy y volver a la lista otros escondites.
8. Repita los pasos 2 a 7 para cada uno de los otros hosts del clúster.
9. Por último, haga clic en Aplicar cambios en la parte superior de la página.

El resultado final debería ser que cada Proxy en el grupo dispone de entradas para todos los demás poderes, por lo que sabe ponerse en contacto con ellos para las solicitudes no en su propio caché.. Sin embargo, puede establecer ACLs a fin de evitar el uso de PCI y la fuerza directa de obtención de ciertas solicitudes, tal y como se puede cuando presenten solicitudes para un maestro caché.

LIMPIANDO EL CACHE

A veces puede ser necesario eliminar todos los archivos en su cache Squid, tal vez para liberar espacio en disco o la fuerza de volver a la carga de las páginas de sus servidores Web originarios. Esto puede hacerse fácilmente utilizando Webmin siguiendo estos pasos:

1. En el módulo principal de la página, haga clic en Borrar el y Reconstruir Caché icono. Una página de confirmación preguntando si está seguro de que realmente se mostrará en su navegador.
2. Para seguir adelante, impactó el **`*Borrar la caché y reconstruir*`** botón. Debido a que el servidor se detendrá durante el proceso de liquidación, no se debe hacer cuando el poder está en uso.
3. Una página que muestra el progreso de Webmin, ya que se apaga Squid, se eliminan todos los archivos de caché, re-inicializa los directorios y, por último, re-inicia Squid se mostrará. Este proceso puede tardar bastante tiempo si usted tiene un gran caché o está usando un sistema de ficheros que es lento para borrar archivos (como UFS en Solaris).

CONFIGURACIÓN DE UN PROXY TRANSPARENTE

Un Proxy transparente es uno que los clientes conectarse a sin ser conscientes de que, debido al uso de las reglas del firewall que re-conexiones directas en el puerto 80 para el sistema de Proxy. La ventaja de esta configuración es que usted no tiene que configurar manualmente todos los clientes Web para utilizar el Proxy -, sino que será conectado a él sin su conocimiento. También significa que los usuarios no pueden obtener en todo el caché y evitar así sus reglas de control de acceso por no configurar en sus navegadores.

Transparent Proxy tiene algunas partes de abajo aunque. No es posible capturar automáticamente FTP o HTTPS conexiones, o aquellos a los sitios Web en los puertos que no sean 80. It También es incompatible con el Proxy de autenticación, como los clientes no pueden decir la diferencia entre la petición del Proxy para acceder a su cuenta y que de un sitio Web. A pesar de autenticación puede aparecer a trabajar, realmente no.

La mayoría de las redes tienen un router que conecta a una LAN interna a la Internet. Para Proxy transparente para el trabajo, este router debe estar configurado para re-direccionar los paquetes salientes por el puerto 80 para el Proxy Squid y el puerto de acogida en lugar. En una pequeña red, el Proxy puede incluso ser ejecutados en el mismo router de acogida. Iptables firewall que viene con Linux pueden realizar dos tipos de re-dirección con ayuda de dispositivos especiales DNAT (Destination Network Address Translation) las normas en la tabla nat.

Debido a que la mayoría de los trabajos es en realidad el hecho de que las reglas del firewall re-direccionar los paquetes salientes, las instrucciones para configurar todo lo que son en la LinuxFirewall en la página Configuración de un Proxy transparente sección. Sin embargo, se escriben para los usuarios de Linux que han instalado IPtables. Si su router está corriendo un sistema operativo distinto (o es un router dedicado, como un hecho por Cisco), los pasos para la creación de reglas de cortafuegos, evidentemente, no se aplicará. Los de la Squid Proxy Server módulo son los mismos sin importar qué tipo de cortafuegos que se estén ejecutando bien.

VER LA CACHÉ GERENTE ESTADÍSTICAS

El Squid software viene con un simple programa llamado CGI cachemgr.cgi que puede conectarse al Proxy y solicitar estadísticas sobre la utilización de memoria, la caché y pierde hits y caché DNS lookup. A pesar de que normalmente se instala para ser ejecutado desde un servidor Web como Apache, puede acceder a ella desde dentro de este módulo de Webmin siguiendo estos sencillos pasos:

1. En la página principal, haga clic en el Cache Manager de Estadística de icono para abrir el programa del formulario de acceso.
2. Deje el campo Cache Anfitrión conjunto a localhost, a menos que se quiere conectar a otro servidor Proxy. La mayoría de ACLs por defecto se han establecido para negar la caché de acceso de administrador en cualquier lugar, excepto aunque localhost.
3. En el campo Cache Puerto, introduzca el número de puerto TCP del servidor Proxy que está a la escucha, como el 8080.
4. El Administrador de nombre y contraseña campos puede dejarse vacía si no se ha Squid configurados para requerir autenticación para recuperar las estadísticas, que no suele ser el caso.
5. Pulse el botón Continuar para acceder a su cuenta, y una página lista todos los diversos tipos de estadísticas disponibles aparecerá. Haga clic sobre cualquiera de los enlaces para visualizar la información detallada.
6. Cuando haya acabado de ver las estadísticas de caché, haga clic en Volver al índice del calamar en la parte inferior de la página para volver al módulo del menú principal.

Porque por defecto Squid acepta sin ninguna solicitud de autenticación mediante el protocolo cache_object especial de localhost, que nadie puede acceder a su sistema a través de telnet o SSH podría ejecutar su propia versión de cachemgr.cgi para ver estas estadísticas. A pesar de que la información disponible no es especialmente sensible, puede que desee configurar Squid para solicitar un nombre de usuario y contraseña, se presentarán para acceder a él.

Esto puede hacerse mediante la creación de autenticación externa y luego editar el gerente Permitir por defecto localhost Proxy restricción a fin de que las nuevas autoridades ACL es seleccionado en el Match ACLs columna también. O mejor aún puede crear otro exterior Auth ACL que tiene sólo unos pocos usuarios que están autorizados a ver las estadísticas enumeradas, y que para asignar el Proxy en lugar de restricción. Esto es aún más seguro, porque evita el problema de todos los telnet o SSH usuario que también tiene un Proxy de acceso normal poder acceder a las estadísticas.

ANALIZANDO LOS REGISTROS DE SQUID

Calamaris es un simple programa en Perl que puede generar un informe de sus archivos de registro de Squid. Si lo tienes instalado, el Calamaris * * Iniciar sesión Análisis icono aparecerá en el módulo de la página principal. Si no, tendrá que descargar e instalar de forma separada, ya que no está incluido en Squid. Algunas distribuciones de Linux tienen un paquete separado de ella, que puede instalarse fácilmente utilizando el módulo de paquetes de software. Si no, el programa puede ser descargado desde http://calamaris.cord.de/, compilado e instalado.

Al hacer clic sobre el icono desencadena la generación de un informe de todos sus registros de acceso de Squid. Por defecto, sólo la última 50000 entradas son procesados para evitar la excesiva carga sobre el sistema - sin embargo, esto se puede ajustar en el módulo de configuración de página (como se explica en la Configuración del Squid Proxy Server módulo de sección). Cuando el informe está completo, éste será mostrado en su navegador como una sola página HTML. En la parte superior están los enlaces a las tablas más abajo en la página, que contiene resúmenes, tales como las solicitudes de acogida, de dominio de destino y de cache afectados.

Incluso si usted ha permitido la rotación de los registros en su sistema periódicamente para renombrar y comprimir los registros de Squid, el módulo se incluye todavía los datos comprimidos en el informe. Se busca todos los archivos de registro en el directorio cuyos nombres comienzan con access.log (como access.log.02.gz) y comprime-si es necesario antes de alimentar a Calamaris. El más reciente archivos son siempre procesados primera aunque, por lo que cualquier registro de líneas límite en vigor corta edad entradas en lugar de las más nuevas.

El Webalizer Análisis LOGFILE módulo (en el capítulo 39) también puede utilizarse para generar informes más impresionantes de los registros de calamares, que contiene gráficos y gráficos circulares. El módulo puede incluso volver a crear un informe sobre el calendario (como todos los días) y se han dirigido por escrito a un directorio para verlo más adelante.

MÓDULO DE CONTROL DE ACCESO

Puede ser muy útil para dar a alguien el derecho a configurar Squid sin dejar daño o cambiar cualquier otra cosa en el sistema. Esto puede hacerse en Webmin mediante la creación de un Webmin los usuarios con acceso al módulo y luego la restricción de lo que él puede hacer con ella. Capítulo 52 explica la idea general que subyace a este tipo de control de acceso con más detalle, mientras que esta sección se refiere a restringir el acceso a Squid el módulo en particular.

Algunos de atención cuando es necesario restringir un usuario de este tipo aunque, según algunas características del módulo puede ser utilizado para modificar archivos o ejecutar comandos con privilegios de root. Por ejemplo, no es una buena idea dejar que un poco de confianza usuario cambiar el caché de directorios, como el establecimiento / o / etc como un alijo podría dañar los archivos en el sistema. Características como Proxy y lista de control de acceso de usuario de edición son bastante seguros aunque, y son probablemente los más útiles para permitir un sub-administrador de usar.

Para crear un usuario que sólo puede configurar Squid, los pasos a seguir son los siguientes:

1. En el módulo de Webmin usuarios, crear un usuario o grupo con acceso a este módulo.
2. Haga clic en Squid Proxy Server al lado del nombre del usuario en la lista en la página principal para abrir el formulario de control de acceso.
3. ¿Puede cambiar la configuración del módulo de edición? Campo a n, por lo que no puede modificar los caminos a los comandos o el archivo de configuración de Squid.
4. En las páginas de configuración permitido lista, seleccione los iconos que módulo debe ser visible para el usuario. Tala, Cache Opciones y programas de ayuda y no debe ser elegido, como las páginas contienen opciones potencialmente peligrosas.
5. Porque Squid puede leer ACLs valores de los archivos separados y este módulo permite a los usuarios editar el contenido de estos archivos ACL, usted debe limitar el directorio en el que se pueden crear. Para ello, introduce un directorio que pertenecen sólo a la Webmin usuario en el directorio raíz de ACL archivos sobre el terreno, tales como / home / joe. Dejando a lo establecido / es una mala idea, ya que esto puede permitir al usuario editar cualquier archivo en su sistema como root.
6. Para evitar que el usuario de cerrar Squid, el cambio se puede iniciar y parar Squid? Campo a No. Él todavía será capaz de aplicar los cambios sin embargo, y probablemente vuelva a configurar el servidor por lo que es no-utilizable.
7. Pulse el botón "Guardar" para activar las restricciones.

CONFIGURAR MÓDULO DEL SERVIDOR SQUID PROXY

Al igual que la mayoría de los módulos, éste tiene varios ajustes que usted puede editar para configurar la interfaz de usuario y los caminos que utiliza para Squid programas y ficheros de configuración. Ellos pueden acceder haciendo clic en el vínculo del módulo de configuración en la página principal, y la forma en que aparece la interfaz de usuario son los campos enumerados en las opciones configurables, mientras que los relacionados con el programa de caminos se encuentran bajo la configuración del sistema.

Debido a que el módulo por defecto de las rutas coincide con los utilizados por el paquete de Squid para su distribución de Linux o sistema operativo (si es que hay uno), los campos en el segundo grupo por lo general no necesitan ser modificadas. Sin embargo, si usted no está usando el paquete suministrado Squid porque usted se ha compilado e instalado el programa desde el código fuente, estas rutas de acceso tendrán que ser cambiado.