



UNIVERSIDAD DE QUINTANA ROO

División de Ciencias e Ingeniería

**Servidor Proxy Transparente en
Redes Locales**

**TRABAJO MONOGRÁFICO
Para obtener el grado de**

Profesional Asociado en Redes

PRESENTA

Iván Giovanni Olivera Montalvo

SUPERVISORES

M.T.I. Melissa Blanqueto Estrada
M.C. Javier Vázquez Castillo
Dr. Jaime Silverio Ortegón Aguilar

Chetumal, Quintana Roo, México, Julio de 2008.



UNIVERSIDAD DE QUINTANA ROO
División de ciencias e ingeniería

Trabajo monográfico elaborado bajo la supervisión del Comité de Asesoría y aprobada como requisito parcial para obtener el grado de:

PROFESIONAL ASOCIADO EN REDES

COMITÉ DE TRABAJO MONOGRÁFICO

Supervisor: _____
M.T.I. Melissa Blanqueto Estrada

Supervisor: _____
M.C. Javier Vázquez Castillo

Supervisor: _____
Dr. Jaime Silverio Ortegón Aguilar

Chetumal, Quintana Roo, México, Julio de 2008

Agradecimientos

A Mis Padres:

Agradezco a mis padres el Sr. Carlos Olivera Martínez y a la Sra. Francisca Montalvo Martín, por todo el apoyo brindado durante tantos años hasta llegar a esta instancia.

A Mis Maestros:

A todos y cada uno de mis maestros, en especial a los profesores Rubén, Víctor, Javier, Melissa y Jaime, quienes invirtieron parte de su tiempo en mi preparación académica y en la revisión de este documento.

A Mi Hermano:

Hermanito querido, gracias por tu paciencia al no poder prestarte la computadora.

A Mi Tía Lourdes:

Tía, gracias por todas las facilidades que me diste.

A Mi Abuelo Ramón:

Gracias abuelo por prestarme el dinero y poder obtener mi título cuanto antes.

A Mis Compañeros:

Agradezco a todos ustedes quienes compartieron conmigo muchas y valiosas experiencias en las aulas de clase.

Dedicatoria

Dedico este trabajo a mis padres, el Sr. Carlos Olivera Martínez y la Sra. Francisca Montalvo Martín, quienes siempre estuvieron conmigo brindándome todo su apoyo incondicional, día a día, siempre me ofrecieron todo lo que necesite, dándome todas las facilidades para mis estudios y llegar a obtener los conocimientos para poder desarrollar este proyecto y poder redactar este trabajo.

Así también, les agradezco enormemente por todos sus consejos y por orientarme a ser una persona de bien.

Gracias.

Resumen

Debido a que existe una creciente demanda de computadoras e Internet, las redes LAN se han vuelto mas traficadas. En la Secretaria de Desarrollo Urbano y Medio Ambiente todos los usuarios tenían acceso ilimitado a Internet, perdiendo su tiempo laboral visitando paginas con contenidos no autorizados, descargando música y videos o platicando mediante programas de mensajería instantánea, saturando la red y volviéndola lenta. Por lo anterior, el objetivo de este trabajo monográfico es el de implementar un “Servidor Proxy Transparente” en la red de SEDUMA mediante la configuración de un servidor bajo el sistema operativo GNU/Linux Fedora Core 5, esto en base a las políticas de seguridad previamente establecidas por el titular de la Unidad de Informática, las cuales fueron planificadas y diseñadas para permitir que se aproveche de una manera mucho mas apropiada el ancho de banda de la SEDUMA ya que el servidor bloqueara las páginas con contenidos no autorizados, los programas p2p y los programas de mensajería instantánea a excepción de ciertos usuarios con privilegios de conexión. Al momento de haber implementado el servidor se noto una gran mejora en la velocidad de la red, ya que los usuarios ya no podían acceder a ninguna de las aplicaciones previamente mencionadas.

Índice

1. Introducción.	1
1.1. ¿Qué es la SEDUMA?.....	1
1.2. Justificación.....	1
1.3. Objetivo General.....	1
1.4. Objetivos Particulares.....	2
2. Marco Teórico.....	3
2.1. Red.....	3
2.1.1. Red de área local (LAN).....	3
2.2. Topología de red.	3
2.2.1. Topología de red en bus lineal.....	4
2.2.2. Topología de red en anillo.....	4
2.2.3. Topología de red en anillo doble.....	5
2.2.4. Topología de red en estrella.	5
2.2.5. Topología de red en estrella extendida.	6
2.3. Definición de términos.	6
3. Configuración de un servidor Proxy en GNU Linux/Fedora Core 5.	12
3.1. Instalación del sistema operativo GNU Linux/Fedora Core 5.	12
3.2. Primer arranque (Firstboot).	20
3.3. Configuración del servidor Proxy/Squid.....	24
3.3.1. Localización del archivo squid.conf.....	24
3.3.2. Creación de un nuevo archivo de texto llamado squid.conf.	25
3.3.3. Configuración del parámetro http_port.....	26
3.3.4. Configuración del parámetro cache_mem.	27
3.3.5. Configuración del parámetro cache_dir.	27
3.3.6. Creación de las listas de control de acceso.	28
3.3.7. Aplicación de reglas a las listas de control de acceso.	33
3.3.8. Caché con aceleración.....	35
3.3.9. Redireccionamiento del puerto 80 al 3128.....	36
4. Pruebas de funcionamiento.....	38

5. Conclusiones.	39
6. Referencias bibliográficas.	40

1. Introducción.

1.1. ¿Qué es la SEDUMA?.

La Secretaría Estatal de Desarrollo Urbano y Medio Ambiente, decretada su creación al inicio de esta administración, como un instrumento fundamental para impulsar con suficiente fuerza, una cultura ecológica que anteponga el cuidado del entorno y la preservación ambiental, en la forma de decisiones en todos los niveles y sectores.

Con la visión de un Quintana Roo líder en la restauración, protección, conservación y aprovechamiento racional de sus recursos naturales, donde el desarrollo económico, turístico y urbano, se lleve conforme a reglas claras y precisas establecidas en los programas de ordenamiento ecológico territorial y en los planes de manejo de las Áreas Naturales Protegidas[1].

1.2. Justificación.

La implementación de un servidor Proxy para el filtrado de tráfico en una LAN (Red de Área Local), se ha vuelto cada vez más importante e indispensable. Un servidor Proxy (Servidor de pasarela) permite obtener el mejor aprovechamiento de la LAN, liberando ancho de banda que pudiera estar ocupado por tráfico no indispensable, tales como programas punto a punto (p2p, por ejemplo: Ares, Kazaa y e-Mule). Así, también, se pueden restringir páginas con contenidos no autorizados que no sigan con el objetivo laboral de la SEDUMA. Por lo anterior, es necesario instalar en la red LAN de SEDUMA un sistema el cual incremente la funcionalidad de la misma y la optimice utilizando un Servidor Proxy. Dicho servidor será configurado acorde a las políticas establecidas por SEDUMA.

1.3. Objetivo General.

Implementar un servidor Proxy transparente en la red LAN de SEDUMA.

1.4. Objetivos Particulares.

- a) Revisar las políticas de seguridad de la red LAN de SEDUMA.
- b) Planificar las acciones y estrategias acorde a las políticas de seguridad de SEDUMA.
- c) Seleccionar el servidor que se utilizará.
- d) Instalar y configurar un servidor Proxy.
- e) Implementar las políticas de seguridad.
- f) Realizar pruebas de funcionamiento.
- g) Documentar la implementación del servidor Proxy.

2. Marco Teórico.

2.1. Red.

Entre las definiciones de red podemos mencionar la siguiente:

“Una red no es más que un grupo de computadoras interconectadas mediante cables o algún otro medio” [2].

2.1.1. Red de área local (LAN).

Las redes de área local (generalmente conocidas como LAN) son redes de propiedad privada que se encuentran en un solo edificio o en un campus de pocos kilómetros de longitud. Se utilizan ampliamente para conectar computadoras personales y estaciones de trabajo en oficinas de una empresa y de fábricas para compartir recursos (por ejemplo, impresoras) e intercambiar información. Las LAN son diferentes de otros tipos de redes en tres aspectos: 1) tamaño; 2) tecnología de transmisión, y 3) topología [3].

Su tamaño puede abarcar el área de un edificio o el área de una universidad que tiene distribuidos varios edificios pero siempre dentro de su misma área que abarca la universidad, escuela, empresa por mencionar algunos ejemplos [3].

Las LAN podrían utilizar una tecnología de transmisión que consiste en un cable al cual están unidas todas las máquinas. Las LAN tradicionales se ejecutan a una velocidad de 10 a 100 Mbps, tienen un retardo bajo (microsegundos o nanosegundos) y cometen muy pocos errores. Las LAN más recientes funcionan hasta a 10 Gbps. 1 Mbps es igual a 1, 000,000 de bits por segundo y 1 Gbps es igual a 1, 000, 000,000 de bits por segundo [3].

2.2. Topología de red.

La topología de una red define únicamente la distribución del cable que interconecta las diferentes computadoras, es decir, es el mapa de distribución del cable que forma la intranet. Define cómo se organiza el cable de las estaciones de trabajo. A la hora de instalar una red, es importante seleccionar la topología más adecuada a las necesidades existentes [4].

2.2.1. Topología de red en bus lineal.

La topología en bus tiene todos sus host directamente conectados a un enlace, y no tiene otras conexiones entre host. Cada host está conectado a un cable común. Una ventaja de esta topología es que todos los host están conectados entre sí y, por tanto, se pueden comunicar directamente. Un inconveniente de esta topología es que una rotura del cable desconecta todos y cada uno de los host de todos los demás. Una topología en bus permite que todos los dispositivos de la red vean las señales de todos los demás dispositivos. Esto puede ser una ventaja si quiere que toda la información vaya a todos los dispositivos a la vez [4]. Ver figura 1.

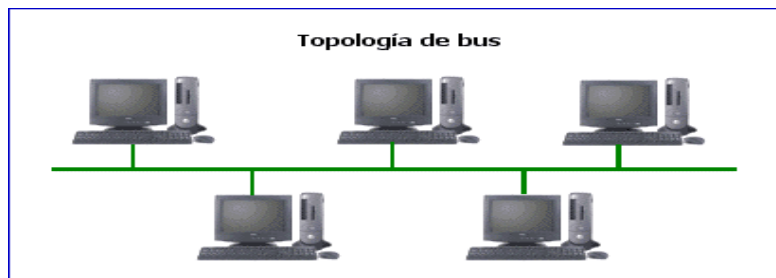


Figura 1: Topología de Bus.

2.2.2. Topología de red en anillo.

Una topología en anillo es un único anillo cerrado compuesto de host y enlaces, con cada host conectado sólo a los dos host adyacentes. La topología muestra todos los dispositivos cableados directamente entre sí en lo que se llama cadena enlazada [4]. Ver figura 2.

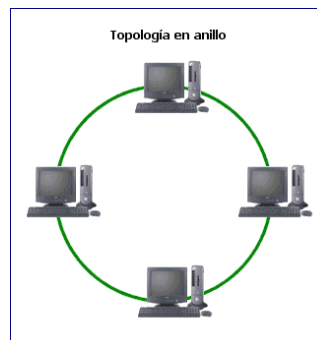


Figura 2: Topología en Anillo.

2.2.3. Topología de red en anillo doble.

Una topología en anillo doble se compone de dos anillos concéntricos. Los dos anillos no están conectados. Una topología en anillo doble es lo mismo que una topología en anillo, exceptuando que un segundo anillo redundante conecta los mismos dispositivos. En otras palabras, para proporcionar fiabilidad y flexibilidad a la red, cada dispositivo de red es parte de dos topologías en anillo independientes. Debido a las características de tolerancia a fallos y auto recuperación de esta topología, los anillos se pueden volver a configurar para formar un anillo mayor y la red seguirá funcionando cuando se produzca un fallo en el medio [4].

2.2.4. Topología de red en estrella.

Una topología en estrella es una arquitectura LAN en la que los puntos extremos de una red se conectan a un hub central común o a un switch mediante enlaces dedicados. Una topología en estrella tiene un nodo central con todos los enlaces a los nodos que parten de él, y no permiten otros enlaces. Su principal ventaja es que permite que todos los demás nodos se comuniquen entre sí de forma conveniente. Su principal inconveniente es que si el nodo central falla, la red completa se desconecta. Dependiendo del tipo de dispositivo de red utilizado en el centro de la red en estrella, las colisiones pueden ser un problema. El flujo de toda la información iría a través de un dispositivo. Esta topología puede ser conveniente por razones de seguridad y acceso restringido, sin embargo, de nuevo, sería muy susceptible a problemas en el nodo central de la estrella [4]. Ver figura 3.

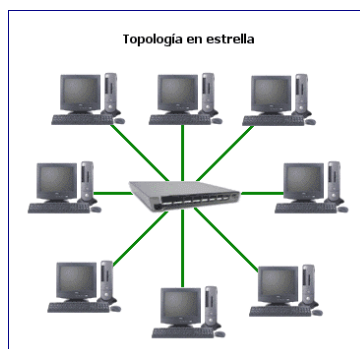


Figura 3: Topología en estrella.

2.2.5. Topología de red en estrella extendida.

Una topología de red en estrella extendida tiene una topología en estrella central, con cada uno de los nodos extremos de la topología central actuando como el centro de su propia topología en estrella. La ventaja es que hace que el cableado sea más corto y limita el número de dispositivos necesarios para interconectar cualquier nodo central. Una topología en estrella extendida es muy jerárquica, y se puede configurar (con el equipamiento apropiado) para “animar” a que el tráfico permanezca local. Así es como el sistema telefónico está actualmente estructurado [4].

2.3. Definición de términos.

Cliente

Se le llama cliente a una computadora personal.

Dispositivo de red.

Se le llama dispositivo de red, a cualquier aparato electrónico que permita al usuario acceder y usar los servicios de red.

Servidor.

Un servidor es la interacción de hardware y software diseñados para funcionar como tal, con el cual se pueden brindar uno o más servicios en una LAN [5].

Dominio.

Un dominio identifica un lugar del espacio de Internet administrado por el Servicio de Nombres de Dominio (DNS. Normalmente, las empresas y los usuarios particulares registrarán el dominio ante la autoridad oficial responsable, y comunicarán los nombres de sus ordenadores en el contexto de este dominio [5].

Demonio.

En los Sistemas Operativos Unix o derivados, a los diferentes tipos de servicios se les denominan demonios. Existen diferentes tipos de servicios, por ejemplo: servicios de red o los servicios de impresión.

Proxy.

Un servidor Proxy es un sistema que reside entre Internet y una red privada. Normalmente, un servidor Proxy oculta la red privada de Internet. Puede implementar o no un firewall, aunque para los ejemplos que aquí se muestran, el firewall se implementará con el servidor Proxy.

Squid.

Squid es un servidor Proxy de caché y es conocido por su excelente rendimiento y sus múltiples funcionalidades. Squid soporta los protocolos mas usuales de Internet, incluyendo FTP, gopher y HTTP [6].

Squid tiene muchas otras funciones además del almacenamiento de objetos de Internet. Entre otras funciones se encuentran las siguientes:

- Almacenamiento en una caché RAM de metadatos y de objetos de tipo host.
- Almacenamiento en caché de las búsquedas de DNS.
- Almacenamiento en caché negativa de las peticiones fallidas.
- Gestión de todas las peticiones en un único proceso, al contrario que otros muchos servidores de caché.
- Soporte de SSL.

Firewall.

Firewall o cortafuegos es un software para servidor que sirve como barrera para filtrar el tráfico de información entre redes.

IPTABLES.

Iptables es el nombre de la herramienta de espacio de usuario (User Space, es decir, área de memoria donde todas las aplicaciones, en modo de

usuario, pueden ser intercambiadas hacia memoria virtual cuando sea necesario) a través de la cual los administradores crean reglas para cada filtrado de paquetes y módulos de NAT. Iptables es la herramienta estándar de todas las distribuciones modernas de GNU/Linux. [7]

SELinux.

El marco de trabajo de SELinux (Linux con Seguridad Mejorada) es parte de Fedora. SELinux limita las acciones que los usuarios y los programas pueden hacer obligando políticas de seguridad a través del sistema operativo. Sin SELinux, los errores de software o los cambios de configuración pueden hacer al sistema más vulnerable. Las restricciones impuestas por las políticas de SELinux proveen una seguridad adicional a los accesos no autorizados [8].

Las políticas inflexibles de SELinux pueden inhibir muchas actividades normales en un sistema Fedora. Por esta razón Fedora hace uso de políticas destinadas, que sólo afectan servicios de red específicos. Estos servicios no pueden realizar acciones que no sean parte de sus funciones normales. Las políticas destinadas reducen o eliminan los inconvenientes que SELinux puede causar a los usuarios. Fije el modo de SELinux a uno de los siguientes:

Enforcing (Obediente): Seleccione este modo para usar la política SELinux destinada en su sistema Fedora. Este es el modo por defecto en instalaciones Fedora.

Permissive (Permisivo): En este modo, el sistema está configurado con SELinux, pero cualquier brecha en la política de seguridad solamente causa que aparezca un mensaje de error. No se prohíbe actualmente ninguna actividad cuando SELinux se instala en este modo. Puede cambiar el modo SELinux a Obediente en cualquier momento después de arrancar.

Disable (Desactivado): Si elige este modo de SELinux, Fedora no configura el sistema de control de acceso para nada. Para activar SELinux más tarde, se deberá seleccionar Sistema → Administración → Nivel de Seguridad y Cortafuego.

Para ajustar SELinux, elija Modificar la Política de SELinux. Para exceptuar un servicio clave de las restricciones de SELinux, seleccione el servicio de la lista y elija la opción Desactivar la Protección de SELinux. El ítem Servicio de Protección de SELinux en la lista incluye las opciones para deshabilitar restricciones de SELinux en servicios adicionales [8].

Políticas de Seguridad.

Todo el tráfico de red que no se permitirá es acorde al criterio del administrador de la red, y se establece en las políticas de seguridad. Las políticas de seguridad son un conjunto de reglas que se implantan para controlar todo lo que deseamos proteger y son importantes pues brindan seguridad y mejoran el rendimiento de la red, lo que significa estabilidad en la LAN.

ACL.

ACL significa Listas de Control de acceso y estas definen que parámetros se van a denegar [9].

Una Lista de Acceso esta compuesta de la siguiente forma:

Sintaxis:

```
acl [ Nombre de la acl ] [ Tipo de acl ] [ Componente de la acl ]
```

```
acl [ Nombre de la acl ] [ Tipo de acl ] [ "Ruta a la lista de componentes de la acl" ]
```

Ejemplo:

```
acl ejemplo src 192.168.1.0/255.255.255.0
```

```
acl redlocal src "/etc/squid/redlocal.txt"
```

Donde redlocal.txt es el nombre del archivo que contiene la IP de la red LAN y "/etc/squid/" es la ruta donde se encuentra dicho archivo.

Algunos tipos de ACL son:

Src (Origen). Especifica una dirección origen de una conexión en formato IP/Máscara, también se puede especificar rangos de direcciones mediante este tipo de acl.

Dst (Destino). Especifica una dirección destino de una conexión en formato IP/máscara, también se pueden especificar hosts destino concretos mediante este tipo de acl.

Srcdomain. Especifica un nombre de dominio origen, el cual se determina por resolución DNS inversa de la IP de la PC.

Dstdomain. Especifica un nombre de dominio destino, la cual se comprueba con el dominio que se haya especificado en la petición de página Web.

Time. Permite especificar una franja horaria concreta dentro de una semana.

Url_regex. Permite especificar expresiones regulares para comprobar una URL completa, desde el <http://inicial>.

Req_mime_type. Se utilizan para comprobar la petición por tipo de archivo (mime type) que realiza un cliente, y se puede utilizar para detectar ciertas descargas de archivos o ciertas peticiones en túneles HTTP.

Tráfico de Red. Es toda la información que viaja por la red.

Administrador de la Red. Persona encargada de vigilar y mantener el buen funcionamiento de la red.

IP. Una dirección IP es un número que identifica de manera lógica y jerárquica a una interfaz de un dispositivo (habitualmente una computadora)

dentro de una red que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red o nivel 3 del modelo de referencia OSI [10].

Petición. Se le llama petición a la solicitud de un servicio que hace un cliente hacia otro cliente o a un servidor.

Redireccionamiento. El redireccionamiento es la desviación de peticiones de un puerto hacia otro puerto.

Puerto. Un puerto es una interfaz, cuya definición es una conexión física entre dos aparatos o sistemas independientes [10].

GRUB. En computación, el GRand Unified Bootloader (GRUB) es un gestor de arranque múltiple que se usa comúnmente para iniciar dos o más sistemas operativos instalados en una misma computadora [12].

Sistema de Archivos. Los sistemas de archivos (filesystem en inglés), estructuran la información guardada en una unidad de almacenamiento (normalmente un disco duro) de una computadora, que luego será representada ya sea textual o gráficamente utilizando un gestor de archivos. La mayoría de los sistemas operativos poseen su propio sistema de archivos [13].

3. Configuración de un servidor Proxy en GNU Linux/Fedora Core 5.

Antes de iniciar con la configuración, es importante mencionar que se eligió GNU/Linux por ser un sistema operativo robusto, seguro y estable para redes y servidores.

Se tomo la decisión de instalar Fedora Core 5 por las siguientes razones:

- Es un software libre y de distribución gratuita
- Fácil acceso y descarga desde la Web.
- Es estable y seguro
- Conocimientos previos

3.1. Instalación del sistema operativo GNU Linux/Fedora Core 5.

En esta sección se pretende mostrar paso a paso la instalación y configuración de un Servidor Proxy bajo el sistema operativo GNU Linux/Fedora Core 5.

Arranque desde el CD de instalación.



Figura 4: Pantalla de Arranque Desde el CD.

Clic en el botón “Siguiente”



Figura 5: Pantalla del Inicio de la Instalación.

Selección del idioma a utilizar durante la instalación.



Figura 6: Pantalla del Idioma de la Instalación.

Posteriormente dar clic en el botón “Siguiente”.

Selección del idioma apropiado para el teclado.



Figura 7: Pantalla del Idioma del Teclado.

Para continuar dar clic en el botón "Siguiente".

Requerimientos de partición en el disco duro.

Este paso es a criterio de cada usuario. La opción por defecto es "Remove all partitions on selected drives and create default layout", pero se puede desplegar el menú y elegir la opción que más convenga.



Figura 8: Pantalla de Requerimientos de Partición.

Clic en el botón "Siguiente".

Configuración del gestor de arranque GRUB.



Figura 9: Pantalla de Configuración del Gestor de Arranque GRUB.
Posteriormente clic en el botón "Siguiente".

Configuración de los dispositivos de red.

Para configuración automática dar clic el botón "Siguiente", sino modificar los parámetros correspondientes. Ver figura 10.



Figura 10: Pantalla de Configuración de los Dispositivos de Red.
Nota: Activar todas las tarjetas de red en la columna "Activar al inicio".
Clic en el botón "Siguiente".

Selección de la región para la zona horaria.



Figura 11: Pantalla de Selección de la Región para la Zona Horaria.

Clic en el botón "Siguiente".

Asignación de una contraseña a la cuenta root.



Figura 12: Pantalla de Asignación de una Contraseña a la Cuenta Root.

Dar clic en el botón "Siguiente".

Selección de los tipos de aplicaciones.

Marcar opción “Personalizar ahora”



Figura: 13: Pantalla de Selección de los Tipos de Aplicaciones.

Clic en el botón “Siguiente”.

Selección del servidor.

En la lista de la izquierda seleccionar la categoría “Servidores” y en la lista de la derecha activar la casilla del tipo de servidor a instalar. Ver la figura 14.



Figura 14: Pantalla de Selección del Servidor.

Posteriormente clic en el botón “Siguiente”.

Comprobación de las dependencias de los paquetes que se han seleccionado.



Figura 15: Pantalla de Comprobación de las Dependencias.

Iniciando la instalación



Figura 16: Pantalla de Inicio de la Instalación.

Clic en el botón “Siguiente”.

Formateo del sistema de archivos que se utilizará



Figura 17: Pantalla de Formateo del Sistema de Archivos.

Instalación del sistema base y todas las aplicaciones seleccionadas



Figura 18: Pantalla de Instalación del Sistema.

Finalizando y reiniciando



Figura 19: Pantalla de Finalizada la Instalación.

Una vez finalizada la instalación dar clic en el botón "Reiniciar".

3.2. Primer arranque (Firstboot).

Al reiniciar el sistema aparecerá la pantalla de Bienvenida del firstboot (Primer Arranque), donde se configurarán lo últimos ajustes del sistema.



Figura 20: Pantalla de Bienvenida.

Clic en el botón "Adelante"

Configuración del Firewall.

En Firewall se deberá verificar que la opción “Enable” este seleccionada, y en “Servicios confiables” activar todos aquellos servicios que no estén seleccionados. Ver figura 21. Clic en “Siguiente”.



Figura 21: Pantalla de Configuración del Firewall.

Configuración del SELinux.

Verificar que en SELinux este seleccionada la opción “Enforcing” (Obediente). Como se observa en la figura 22. Clic en “Adelante”



Figura 22: Pantalla de Configuración del SELinux.

Configuración de la fecha y la hora del sistema.



Figura 23: Configuración de la Fecha y Hora del Sistema.

Clic en el botón “Adelante”.

Configuración de la resolución de pantalla.



Figura 24: Configuración de la Resolución de Pantalla.

Posteriormente clic en el botón “Adelante”.

Crear un usuario para uso no administrativo del sistema.



Figura 25: Creación de Nuevo Usuario.

Clic en el botón “Adelante”.

Configuración de la tarjeta de sonido.



Figura 26: Configuración de la Tarjeta de Sonido.

Clic en el botón “Finalizar” para continuar con la carga del sistema.

Por último, en la figura XXX se presenta la pantalla de acceso (login), donde se podrá ingresar como root para poder iniciar con la configuración del servidor Proxy.



Figura 27: Pantalla de Acceso al Sistema.

3.3. Configuración del servidor Proxy/Squid.

3.3.1. Localización del archivo squid.conf.

Este archivo se encuentra en la ruta `/etc/squid/squid.conf`, una vez ubicado, borrarlo y crear uno nuevo o eliminar todo el contenido del archivo para iniciar una nueva configuración. Esto es debido a que contiene mucho texto basura que podría causar algún error al momento de ejecutar el demonio (servicio) del squid. Para poder realizar lo anterior habrá de seguirse los siguientes pasos:

- Abrir la carpeta de Personal.
- Mostrar el árbol de directorios.
- Entrar a la carpeta etc.
- Entrar a la carpeta squid.
- Borrar el archivo squid.conf.

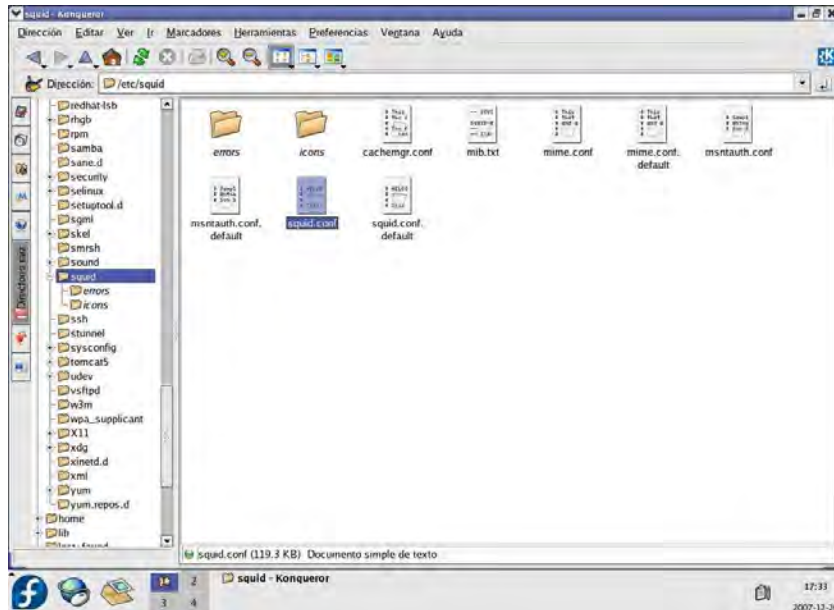


Figura 28: Ruta de Localización del Archivo squid.conf.

3.3.2. Creación de un nuevo archivo de texto llamado squid.conf.

Para esto se deberá seguir los siguientes pasos:

- Hacer clic con el botón derecho del ratón.
- Posicionar el puntero sobre la opción Crear nuevo.
- Al salir el menú emergente se deberá hacer clic sobre la opción Archivo de texto.
- Nombrar al archivo de texto squid.conf.

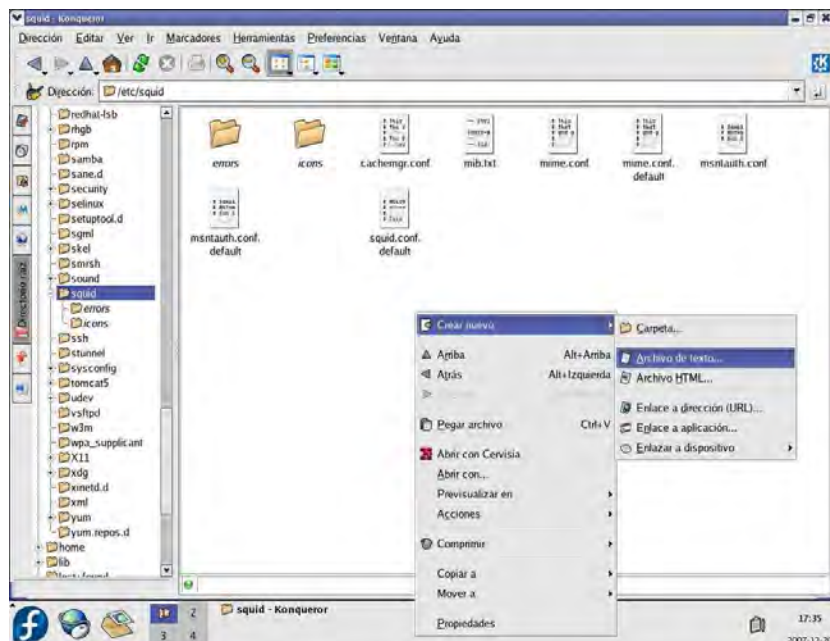


Figura 29.1: Creación del Nuevo Archivo squid.conf.

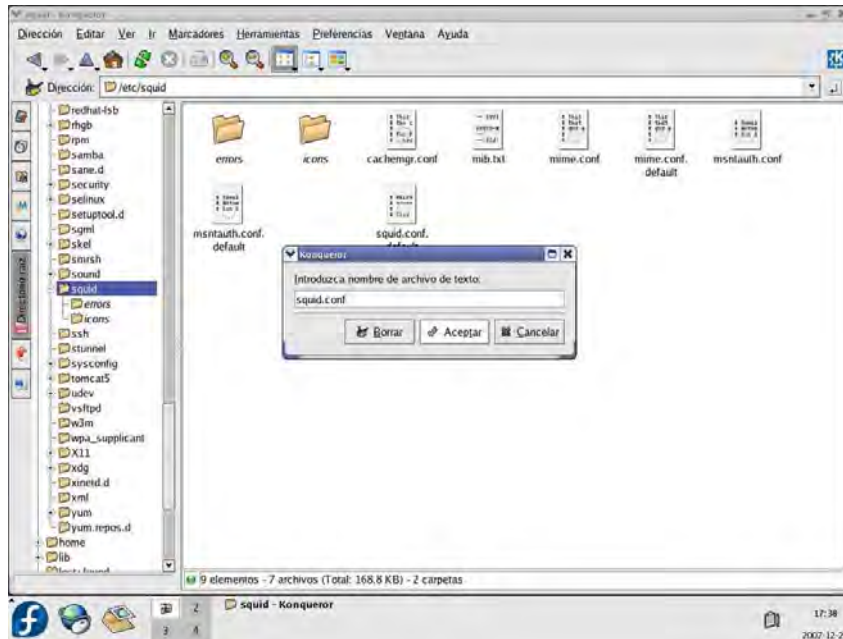


Figura 29.2: Creación del Nuevo Archivo squid.conf.

Teniendo un archivo en blanco se comenzará con la configuración.

3.3.3. Configuración del parámetro http_port.

http_port: El parámetro http_port sirve para especificar el puerto por el cual Squid escuchara peticiones de entrada o salida. Por defecto usa el 3128. Ver figura 30.

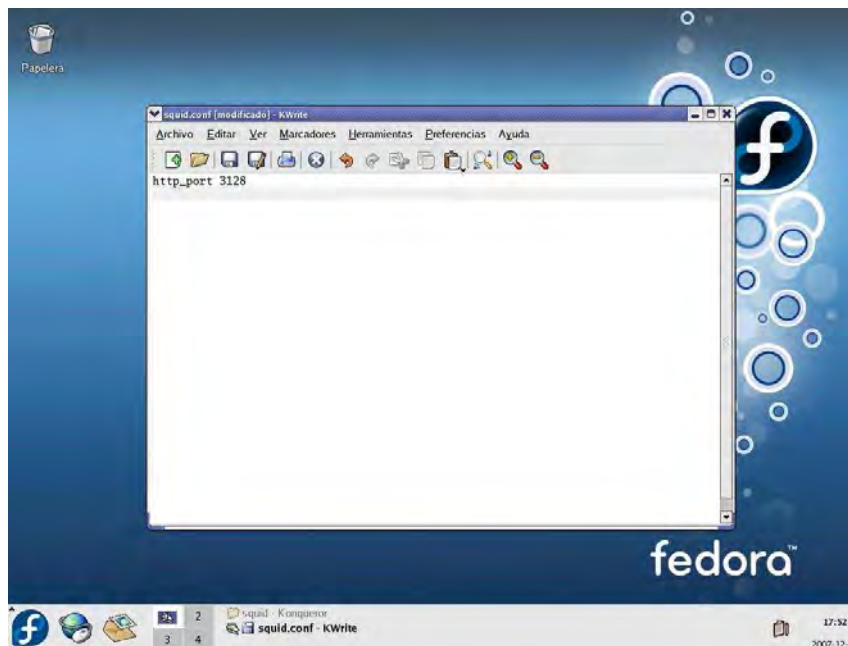


Figura 30: Configuración del Parámetro http_port.

3.3.4. Configuración del parámetro `cache_mem`.

cache_mem: Este parámetro sirve para configurar cuanta memoria le será asignada a la caché del Proxy. Por defecto son 16 MB, dependiendo del hardware del servidor se le puede asignar mas. Ver figura 31.

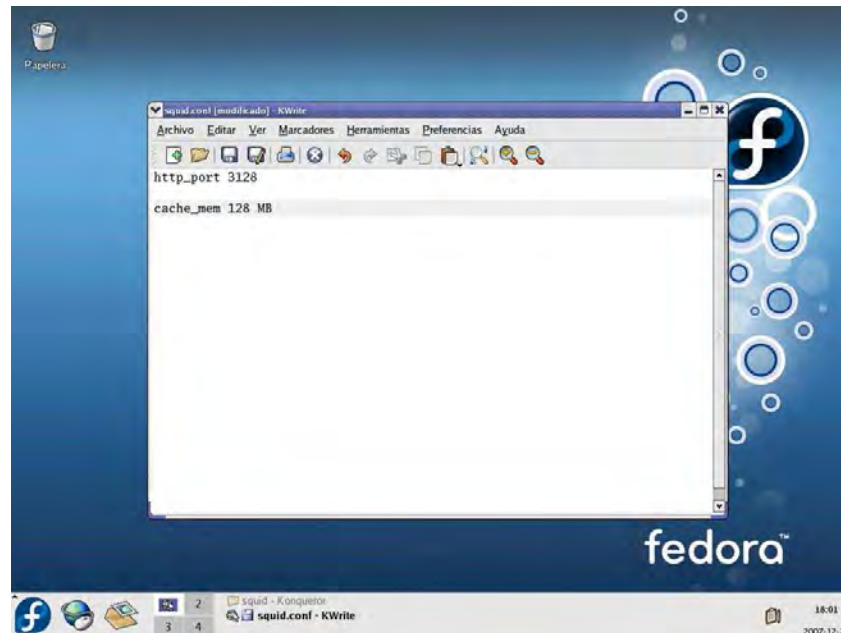


Figura 31: Configuración del Parámetro `cache_mem`.

3.3.5. Configuración del parámetro `cache_dir`.

cache_dir: Aquí se establece cuanta memoria en el disco duro será asignada a la caché del Proxy. Ver figura 32

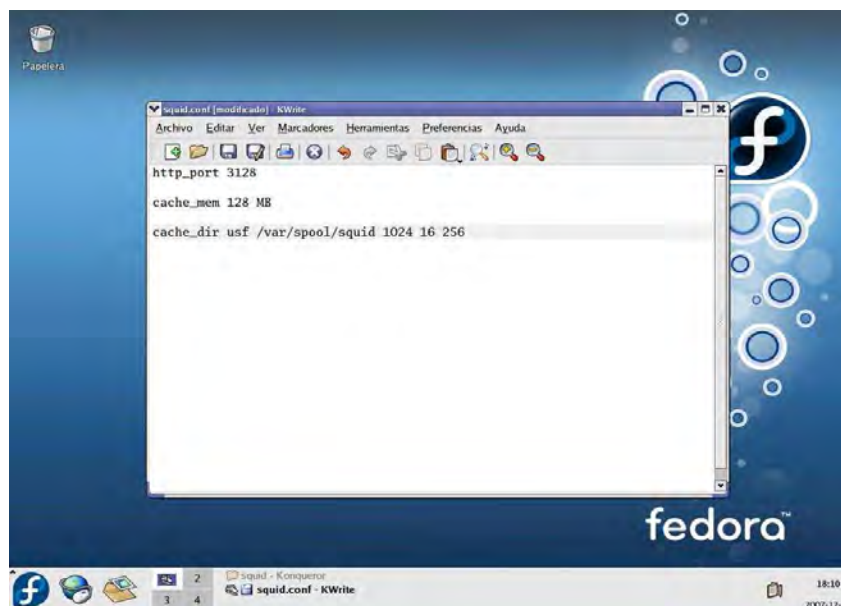


Figura 32: Configuración del Parámetro `cache_dir`.

3.3.6. Creación de las listas de control de acceso.

3.3.6.1. Configuración Mínima Requerida.

Acl all: Se utiliza para establecer una política preestablecida para denegarlo o aceptarlo todo.

```
acl all src 0.0.0.0/0.0.0.0
```

Acl manager: Esta acl define la administración de los objetos en la caché.

```
acl manager proto cache_object
```

Acl localhost: Se definen estas dos acl para utilizar el servidor como origen y destino de las conexiones.

```
acl localhost src 127.0.0.1/255.255.255.255
```

```
acl to_localhost dst 127.0.0.0/8
```

Acl SSL_ports: Este tipo de acl define los puertos que permitirán conexiones SSL.

```
acl SSL_ports port 443 563
```

Acl Safe_ports: Estas acl's definen los puertos seguros para una conexión

```
acl Safe_ports port 50          #protocolo EH
acl Safe_ports port 500        #protocolo udp
acl Safe_ports port 80         # http
acl Safe_ports port 21         # ftp
acl Safe_ports port 443 563    # https, snews
acl Safe_ports port 70         # gopher
acl Safe_ports port 210        # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280        # http-mgmt
acl Safe_ports port 488        # gss-http
acl Safe_ports port 591        # filemaker
acl Safe_ports port 777        # multiling http
```

3.3.6.2. Red local.

```
acl redlocal src 10.0.0.0/255.255.255.0
```

Esta instrucción permite definir a la red LAN.

3.3.6.3. Palabras no autorizadas.

- Primero hay que crear el archivo palabras_denegadas.txt dentro de la carpeta Squid. Para esto hay que seguir el punto 3.3.2, solo que el archivo en vez de llamarse squid.conf se llamará palabras_denegadas.txt.
- Dentro del archivo palabras_denegadas.txt se escribirán línea por línea todas las palabras que se deseen bloquear, por ejemplo:
sex
sexo
lolitas
zorras
- Squid no distingue mayúsculas o minúsculas por lo que para bloquear esas palabras de una manera más eficaz se tiene que escribir la palabra en minúsculas y mayúsculas.

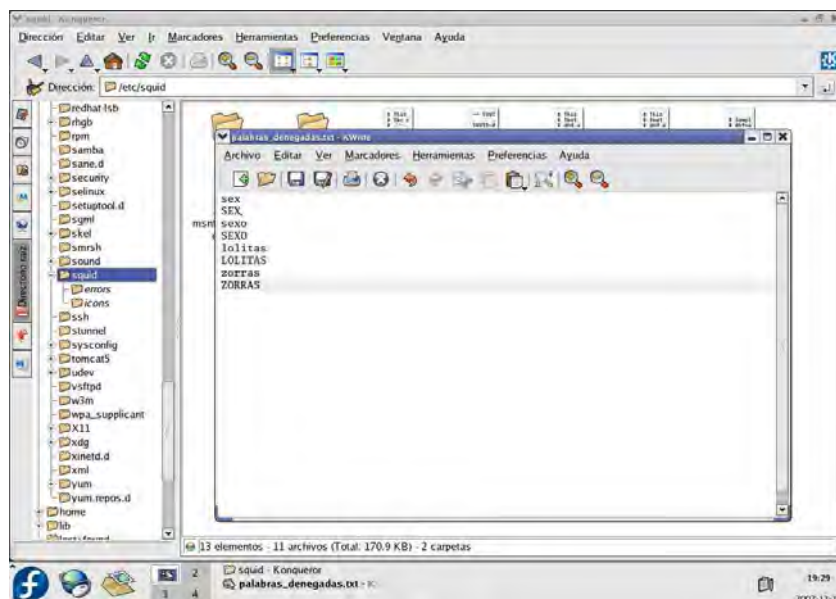


Figura 33: Contenido del Archivo palabras_denegadas.txt.

```
acl palabras_denegadas url_regex "/etc/squid/palabras_denegadas.txt"
```

Esta instrucción deniega en su totalidad palabras no autorizadas o de sentido obsceno. Estas palabras se encuentran listadas en el archivo palabras_denegadas.txt. Por ejemplo, la palabra sexualidad incluye la palabra sex y por lo tanto será bloqueada.

3.3.6.4. Palabras autorizadas.

Primero hay que crear el archivo palabras_permitidas.txt dentro de la carpeta Squid. Para esto hay que seguir el punto 3.3.2, solo que el archivo en vez de llamarse squid.conf se llamará palabras_permitidas.txt.

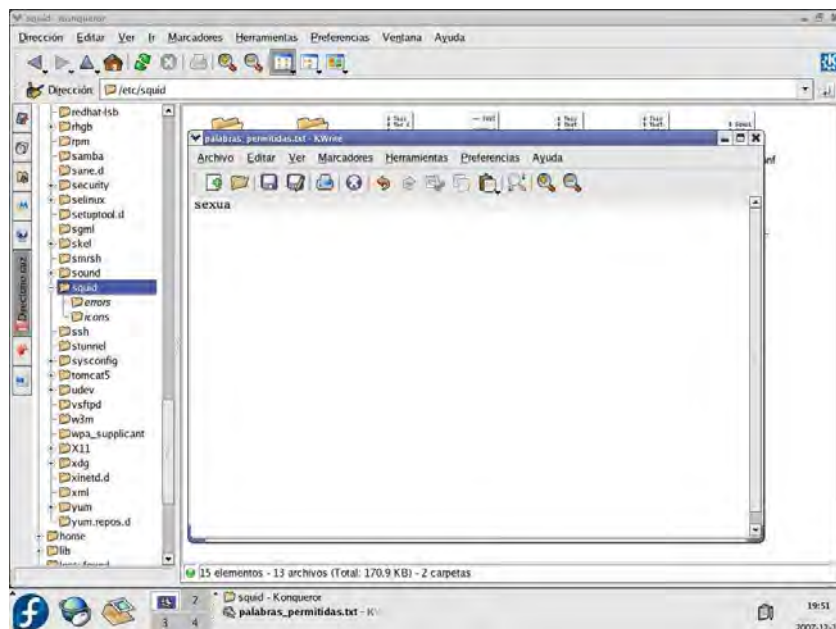


Figura 34: Contenido del Archivo palabras_permitidas.txt.

```
acl palabraspermitidas url_regex "/etc/squid/url_si_admi.txt"
```

Esta instrucción indica que se permitirá desbloquear algunas palabras que por alguna razón se hayan denegado pero no tienen ningún sentido obsceno, por ejemplo la palabra sexualidad, sin embargo se puede desbloquear escribiendo dentro del archivo la palabra “sexua”, de esta forma se le indica a squid que cualquier frase que contenga esa palabra no sea

denegada. Esta lista de palabras se encuentra en el archivo palabras_permitidas.txt

3.3.6.5. Dominios no autorizados.

- Primero hay que crear el archivo dominios_denegados.txt dentro de la carpeta Squid. Para esto hay que seguir el punto 3.3.2, solo que el archivo en vez de llamarse squid.conf se llamará dominios_denegados.txt.

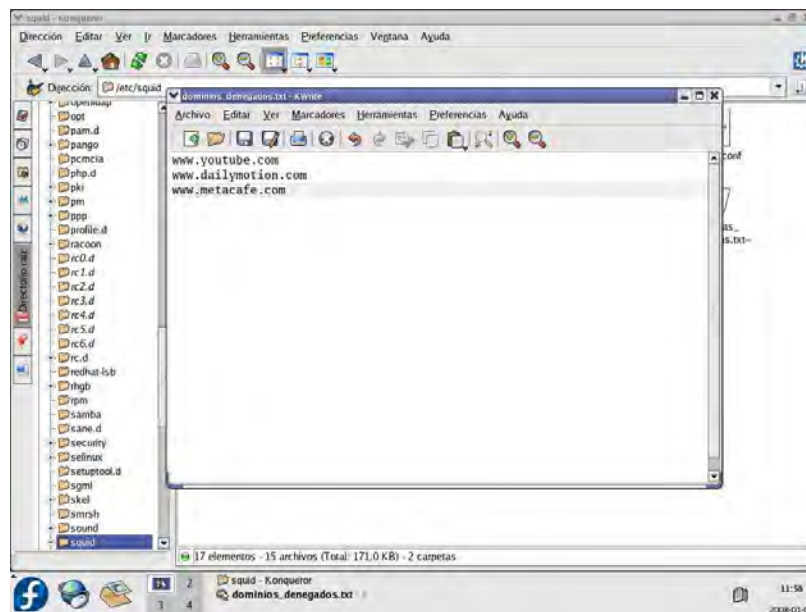


Figura 35: Contenido del Archivo dominios_denegados.txt.

```
acl dominiosdenegados url_regex "/etc/squid/dominiosno.txt"
```

La instrucción anterior nos muestra como bloquear una lista de páginas que no estén autorizadas. Estas páginas se escriben en forma de lista dentro del archivo dominios_denegados.txt, por ejemplo: www.youtube.com.

3.3.6.6. Dominios autorizados.

```
acl dominiospermitidos url_regex "/etc/squid/dominiossi.txt"
```

Este comando nos indica como hacer lo contrario al punto anterior.

3.3.6.7. Prohibir el MSN Messenger.

```
acl messenger_prohibido req_mime_type -i ^application/x-msn-messenger$  
acl MSN url_regex -i gateway.dll
```

Las dos líneas de instrucción anteriores muestran como bloquear el MSN messenger

3.3.6.8. Direcciones IP con privilegios de conexión.

- Primero hay que crear el archivo jefes.txt dentro de la carpeta Squid. Para esto hay que seguir el punto 3.3.2, solo que el archivo en vez de llamarse squid.conf se llamará jefes.txt.

10.0.0.3

10.0.0.10

10.0.0.20

10.0.0.30

10.0.0.40

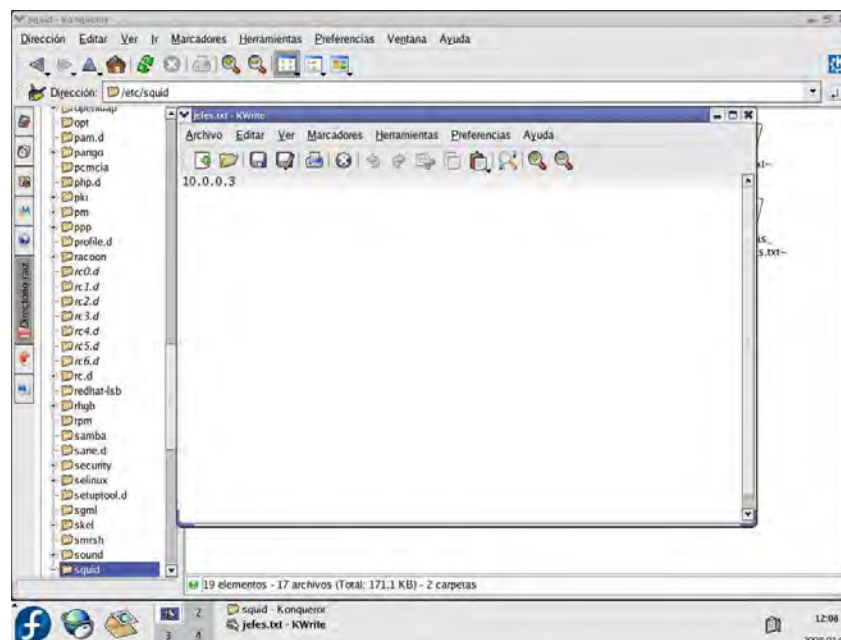


Figura 36: Contenido del Archivo jefes.txt.

```
acl jefes src "/etc/squid/jefes.txt"
```

La instrucción anterior indica como crear una lista de control de acceso llamada jefes, la cual servirá para darle privilegios de conexión a ciertos clientes, dentro del archivo jefes.txt se escribirán línea por línea todas las IP's.

```

cache_mem 128 MB

cache_dir ufs /var/spool/squid 1024 16 256

#Configuración minima recomendada:
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl to_localhost dst 127.0.0.0/8
acl SSL_ports port 443 563
acl Safe_ports port 80          # http
acl Safe_ports port 21         # ftp
acl Safe_ports port 443 563    # https, snews
acl Safe_ports port 70         # gopher
acl Safe_ports port 210        # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280        # http-mgmt
acl Safe_ports port 488        # gss-http
acl Safe_ports port 591        # filemaker
acl Safe_ports port 777        # multiling http
#Listas de control de acceso
acl redlocal src 10.0.0.0/255.255.255.0
acl palabras_denegadas url_regex "/etc/squid/palabras_denegadas.txt"
acl palabras_permitidas url_regex "/etc/squid/palabras_permitidas.txt"
acl dominios_denegados url_regex "/etc/squid/dominios_denegados.txt"
acl dominios_permitidos url_regex "/etc/squid/dominios_permitidos.txt"
acl msn_denegado req_mime_type -i ^application/x-msn-messenger$
acl msn_denegado2 url_regex -i gateway.dll
acl jefes src "/etc/squid/jefes.txt"

```

Figura 37: Configuración Completa de las ACL.

En la fig. 37 podemos observar el archivo squid.conf con las listas de control de acceso configuradas

3.3.7. Aplicación de reglas a las listas de control de acceso.

Hay que tener mucho cuidado a la hora de escribir la regla para cada lista de control de acceso, así como también llevar un orden.

3.3.7.1. Red local.

```
http_access deny !redlocal
```

3.3.7.2. Palabras autorizadas.

```
http_access allow palabras_permitidas
```

3.3.7.3. Dominios autorizados.

```
http_access allow dominios_permitidos
```


3.3.7.4. Palabras no autorizadas.

```
http_access deny palabras_denegadas
```

3.3.7.5. Dominios no autorizados.

```
http_access deny dominios_denegados
```

3.3.7.6. MSN Messenger.

Nota: Recordar que hay clientes con privilegios de conexión.

```
http_reply_access deny msn_denegado !jefes
```

```
http_reply_access deny msn_denegado2 !jefes
```

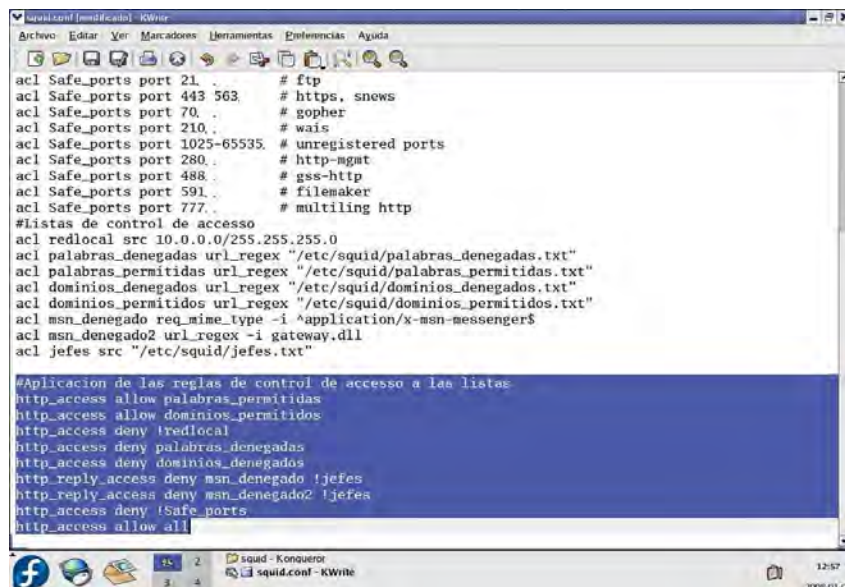
Con esta regla estamos diciendo que se deniegue la conexión a todos los clientes excepto para los que se encuentren en la lista de control de acceso jefes.

3.3.7.7. Puertos seguros (SafePorts).

```
http_access deny !Safe_ports
```

3.3.7.8. Por defecto.

```
http_access allow all
```



```
ac1 Safe_ports port 21 . # ftp
ac1 Safe_ports port 443 563. # https, snws
ac1 Safe_ports port 70. . # gopher
ac1 Safe_ports port 210. . # wais
ac1 Safe_ports port 1025-65535. # unregistered ports
ac1 Safe_ports port 280. . # http-mgmt
ac1 Safe_ports port 488. . # gss-http
ac1 Safe_ports port 591. . # filemaker
ac1 Safe_ports port 777. . # multiling http
#Listas de control de acceso
ac1 redlocal src 10.0.0.0/255.255.255.0
ac1 palabras_denegadas url_regex "/etc/squid/palabras_denegadas.txt"
ac1 palabras_permitidas url_regex "/etc/squid/palabras_permitidas.txt"
ac1 dominios_denegados url_regex "/etc/squid/dominios_denegados.txt"
ac1 dominios_permitidos url_regex "/etc/squid/dominios_permitidos.txt"
ac1 msn_denegado req_mime_type -i ^application/x-msn-messenger$
ac1 msn_denegado2 url_regex -i gateway.dll
ac1 jefes src "/etc/squid/jefes.txt"

#Aplicacion de las reglas de control de acceso a las listas
http_access allow palabras_permitidas
http_access allow dominios_permitidos
http_access deny !redlocal
http_access deny palabras_denegadas
http_access deny dominios_denegados
http_reply_access deny msn_denegado !jefes
http_reply_access deny msn_denegado2 !jefes
http_access deny !Safe_ports
http_access allow all
```

Figura 38: Aplicación de las Reglas a las Listas de Control.

En la Fig. 38 podemos observar el archivo Squid.conf con las reglas de control de acceso aplicadas a las listas de control.

3.3.8. Caché con aceleración.

El caché con aceleración es una funcionalidad del Proxy que permite acceder rápidamente a una página Web sin acceder a Internet. Por ejemplo, cuando un usuario hace petición hacia un objeto en Internet, este es almacenado en el caché de Squid. Si otro usuario hace petición hacia el mismo objeto, y este no ha sufrido modificación alguna desde que lo accedió el usuario anterior, Squid mostrará el que ya se encuentra en el caché en lugar de volver a descargarlo desde Internet. Esta función optimiza enormemente la utilización del ancho de banda en la red LAN.

3.3.8.1. Configuración de la dirección IP.

Se debe de especificar la dirección IP de cualquier servidor HTTP en la red local.

```
httpd_accel_host 10.0.0.3
```

3.3.8.2. Puerto.

```
httpd_accel_port 80
```

3.3.8.3. Activación del acelerador.

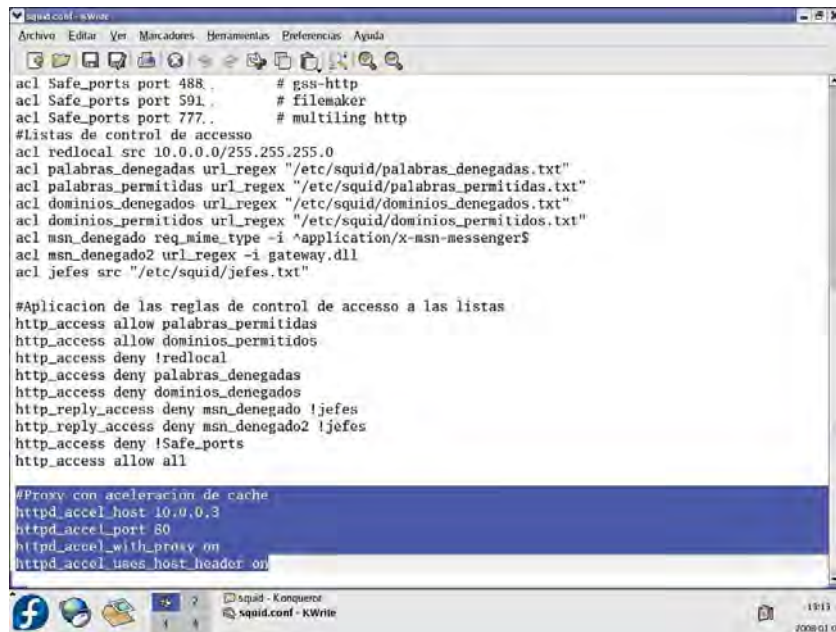
Para utilizar Squid como un acelerador de httpd local y como un servidor Proxy, cambiar la opción “off” a “on”.

```
httpd_accel_with_proxy on
```

3.3.8.4. Activación del encabezado de hostname.

Para activar el encabezado en el cual es el hostname del URL cambiar la opción “off” a “on” del siguiente parámetro.

```
httpd_accel_uses_host_header on
```



```
acl Safe_ports port 488 . # gss-http
acl Safe_ports port 591 . # filemaker
acl Safe_ports port 777 . # multiling http
#Listas de control de acceso
acl redlocal src 10.0.0.0/255.255.255.0
acl palabras_denegadas url_regex "/etc/squid/palabras_denegadas.txt"
acl palabras_permitidas url_regex "/etc/squid/palabras_permitidas.txt"
acl dominios_denegados url_regex "/etc/squid/dominios_denegados.txt"
acl dominios_permitidos url_regex "/etc/squid/dominios_permitidos.txt"
acl msn_denegado req_mime_type -i ^application/x-msn-messenger$
acl msn_denegado2 url_regex -i gateway.dll
acl jefes src "/etc/squid/jefes.txt"

#Aplicacion de las reglas de control de acceso a las listas
http_access allow palabras_permitidas
http_access allow dominios_permitidos
http_access deny !redlocal
http_access deny palabras_denegadas
http_access deny dominios_denegados
http_reply_access deny msn_denegado !jefes
http_reply_access deny msn_denegado2 !jefes
http_access deny !Safe_ports
http_access allow all

#Proxy con aceleración de cache
httpd_accel_host 10.0.0.3
httpd_accel_port 80
httpd_accel_with_proxy on
httpd_accel_uses_host_header on
```

Figura 39: Configuración del Caché con Aceleración.

En la Fig. 39 se observa el archivo Squid.conf con el proxy acelerado configurado.

3.3.9. Redireccionamiento del puerto 80 al 3128.

Esto obliga a que todas las peticiones que los clientes hagan hacia Internet tengan que ser filtradas por el Proxy, y si las peticiones no son válidas de acuerdo a la aplicación de las listas de acceso, las peticiones serán bloqueadas. Para ello se hace lo siguiente:

- Editar el archivo rc.local que se encuentra en la ruta /etc/rc.d/rc.local.

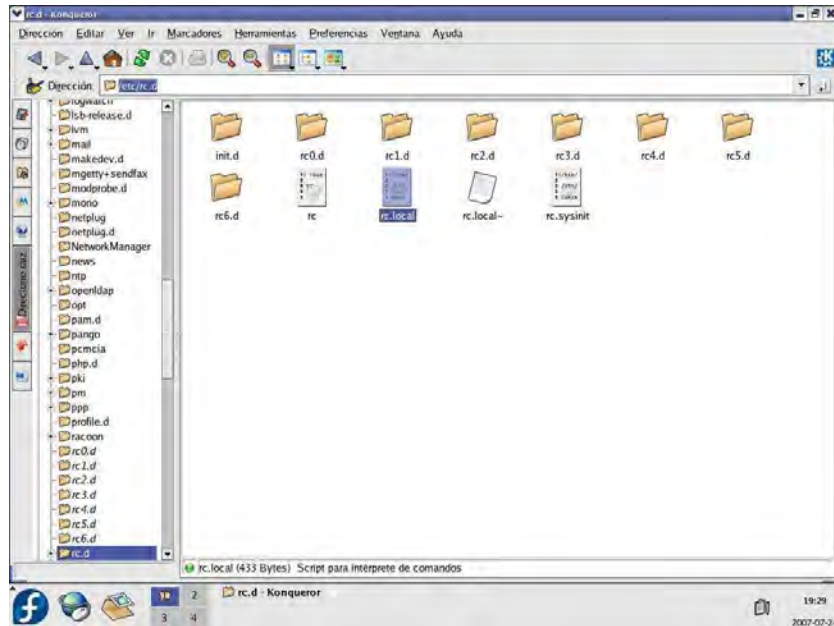


Figura 40: Ruta del Archivo rc.local.

- Usar IPTABLES para el redireccionamiento

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

El comando anterior indica que todas las peticiones hacia el puerto 80 que entran por la interfaz eth1 bajo el protocolo TCP serán redireccionadas al puerto 3128.

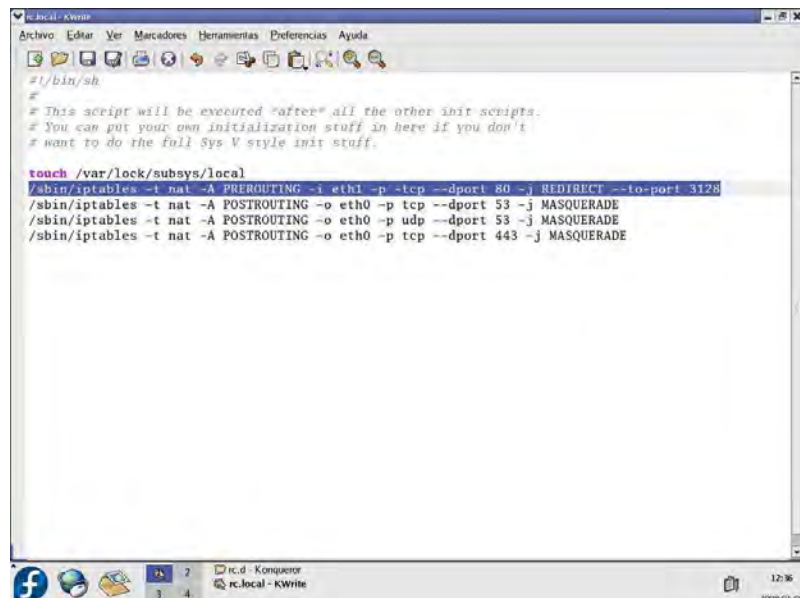


Figura 41: Comando de Redireccionamiento de Puertos.

4. Pruebas de funcionamiento.

A continuación se describen las principales pruebas llevadas a cabo después de haber implantado el Proxy.

Tipo de Prueba	Problemas	Solución
Prueba 1.- Verificar si el Proxy bloquea correctamente las palabras no autorizadas	El Proxy solo bloquea palabras escritas con las minúsculas	Bloquear las palabras de la siguiente forma: sexo SEXO
Prueba 2.- Verificar si el Proxy bloquea correctamente los dominios no autorizados	El Proxy solo bloquea dominios de tipo WWW	Bloquear los dominios de la siguiente forma: www.sexo.com sexo.com
Prueba 3.- Verificar si el Proxy bloquea correctamente programas no autorizados	Algunos programas no tienen un solo método de conexión a la Web	Investigar todos los métodos de conexión del programa a bloquear: Puertos Protocolos Etc.
Prueba 4.- Verificar el redireccionamiento	Al configurar el cliente, este seguía teniendo acceso a Internet	Revisar la instrucción de redireccionamiento, que sean los parámetros, protocolos y puertos correctos. Si el redireccionamiento esta hecho de manera correcta al desconfigurar el Proxy del cliente, estos no deben de tener acceso a Internet.

5. Conclusiones.

Trabajar en este proyecto fue muy enriquecedor y me permitió participar con entusiasmo. Comprendí que un servidor Proxy es un sistema que funciona como una barrera que filtra el tráfico de información entre una red LAN y la Internet. Desde el primer momento de haber implementado el servidor, la red comenzó a funcionar de forma más rápida.

Antes de instalar el servidor se pensó en un software que sea libre de licencias, sin costo alguno, de fácil acceso, seguro y estable. Fedora Core brinda todas las características anteriores, ya que, al ser software libre no cuenta con licencias y por lo tanto es sin costo alguno, es de fácil acceso ya que puede descargarse una copia del sistema desde Internet las veces que se desee. Además, es un sistema seguro y estable ya que cuenta con el núcleo Linux haciendo de Fedora Core un sistema robusto para redes y servidores.

Una vez que el servidor Proxy fue configurado, se realizaron pruebas de funcionamiento, observando si los dominios y palabras introducidos en el navegador eran bloqueados correctamente.

Trabajar en este proyecto me permitió consolidar mis conocimientos y experiencia, ya que gracias a él, pude aplicar en forma práctica los conocimientos adquiridos durante mi formación en la Universidad.

6. Referencias bibliográficas.

- [1] DIAZ Carvajal, Francisco Javier. “*SEDUMA*”. 2007
URL:<http://seduma.groo.gob.mx>
- [2] CRAIG, Zacker. “*Redes: Manual de Referencia*”. Primera Edición, McGraw-Hill, México, 2002. 1046 p. ISBN: 970-10-4882-2
- [3] TANENBAUM, Andrew S. “*Redes de computadoras*”. Cuarta Edición, Pearson Educación, México, 2003. 912 p. ISBN: 970-26-0162-2
- [4] CISCO SYSTEMS, INC. “*Academia de Networking de Cisco Systems: Guía del Primer Año*”. Segunda Edición, Pearson Educación, Madrid, 2002. 920 p. ISBN: 84-2053296-7
- [5] CIMINO, James D. “*Intranets*”. Primera Edición, Paraninfo, Madrid, 1997. 366 p. ISBN: 84-283-2369-0
- [6] SCHENK, Thomas. “*Administración de Red Hat Linux*”. Primera Edición, Prentice Hall, Madrid, 2001. 1192 p. ISBN: 84-205-3124-3
- [7] BARRIOS Dueñas Joel. “*Acerca de IPTABLES y NetFilter*”. 5 de Febrero de 2007.
URL:<http://www.linuxparatodos.net/portal/staticpages/index.php?page=como-shorewall-3-interfaces-red>
- [8] FEDORA PROJECT. SELinux, Capítulo 17: Primer Arranque
URL: <http://docs.fedoraproject.org/install-guide/f8/es/sn-firstboot-selinux.html>
- [9] FÁBREGA Martínez Pedro Pablo. “*Administración de Linux: Control de acceso a la Web*”. URL: <http://dns.bdat.net/documentos/squid/t1.html>

[10] MCCARTY Bill. *“El Libro Oficial de Red Hat Linux: Firewalls”*. Primera Edición, Anaya Multimedia, Madrid, 2003. 560 p. ISBN: 84-415-1584-0