ELABORACIÓN DE UNA GUÍA PARA LA INSTALACIÓN, CONFIGURACIÓN Y ADMINISTRACIÓN DE LA RED INFORMÁTICA DE LA FUNDACIÓN COLEGIO UIS (FCUIS) BASADA EN SOFTWARE DE CÓDIGO ABIERTO.

NANCY CAMACHO CUBIDES

HELVERT CASTELLANOS QUIROZ

UNIVERSIDAD INDUSTRIAL DE SANTANDER UIS
FACULTAD DE INGENIERÍA ELECTRÓNICA, ELÉCTRICA Y TELECOMUNICACIONES
ESCUELA DE INGENIERIA ELECTRICA
ESPECIALIZACIÓN EN TELECOMUNICACIONES
BUCARAMANGA
2010

ELABORACIÓN DE UNA GUÍA PARA LA INSTALACIÓN, CONFIGURACIÓN Y ADMINISTRACIÓN DE LA RED INFORMÁTICA DE LA FUNDACIÓN COLEGIO UIS (FCUIS) BASADA EN SOFTWARE DE CÓDIGO ABIERTO.

NANCY CAMACHO CUBIDES

HELVERT CASTELLANOS QUIROZ

Trabajo de grado para optar el título de Especialista en telecomunicaciones

Director:
FREDDY ALFONSO BELTRÁN MIRANDA
Ingeniero de Sistemas
Magíster en Administración de Empresas

UNIVERSIDAD INDUSTRIAL DE SANTANDER UIS
FACULTAD DE INGENIERÍA ELECTRÓNICA, ELÉCTRICA Y TELECOMUNICACIONES
ESCUELA DE INGENIERIA ELECTRICA
ESPECIALIZACIÓN EN TELECOMUNICACIONES
BUCARAMANGA
2010

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

GLOSARIO

Servidor: En informática, un servidor es una computadora que, formando parte de una red, provee servicios a otras computadoras denominadas clientes.
es.wikipedia.org/wiki/Servidor.

Red Hat Linux: Es una de las más grandes compañías dedicadas al software de código abierto y el más grande distribuidor de sistemas operativos Linux. Red Hat fue fundado en 1993 y tiene su sede en Raleigh, Carolina del Norte (EE.UU.). Tiene alrededor de 1.700 empleados (2006), e ingresos por 278 millones de dólares (2006). Desarrolla los productos: Red Hat Enterprise Linux, Red Hat Directory Server, Red Hat Certificate System y Fedora Core.

Proxy: el nombre en inglés de proxy tiene un significado de intermediario. En el contexto de las redes informáticas, el término proxy hace referencia a un programa o dispositivo que realiza una acción en representación de otro. Su finalidad más habitual es la de servidor proxy, que sirve para permitir el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado, esto es, una única dirección IP.

Proxy/cache: Da servicio proxy a solicitudes del tipo http, https y ftp a computadores que están en nuestra red local para que puedan navegar hacia internet y a su vez ofrece el servicio de cache en el cual se guardan localmente las paginas consultadas por los clientes de forma que aumenta la rapidez de acceso a la información web y ftp.

Proxy SSL: Es un servicio de squid compatible con SSL, con el cual se aceleran las peticiones y las peticiones hacia internet estarían cifradas.

ICP, HTCP, CARP, Cache digests: Squid contiene los protocolos ICP, HTCP, CARP y caché digests los cuales tienen como funcionalidad permitir a un proxy "preguntarle" a otros proxys caché si poseen almacenado un recurso determinado. En nuestra red podemos tener varios servidores proxy y buscar la cache en cualquiera de ellos.

Proxy Transparente: Nuestro servidor squid lo podemos configurar como un proxy transparente de manera que las solicitudes son dirigidas por medio de unas reglas de firewall y son enviadas al servidor sin tener la necesidad de configurar los navegadores de los equipos.

WCCP: Intercepta y redirigir el trafico a un router hacia uno o varios proxys caché, haciendo control de la conectividad de estos mismos.

Control de Accesos: En esta parte creamos reglas de control de acceso, esto permite establecer políticas de denegación o aceptación de páginas o archivos en internet.

Aceleración de servidores HTTP: Cuando hacemos solicitudes hacia internet la información es guardada en el cache del squid y si hay otra solicitud el squid le devolverá la petición o paginas que tiene el squid en cache. Si hay algún cambio entonces el squid actualizara la información desde internet.

SNMP: Permite activar el protocolo SNMP, esto nos permite la buena administración de la red, que permite supervisar, analizar y comunicar

información entre varias máquinas, logrando detectar problemas y proporcionar mensajes de estados.

Caché de resolución DNS: Squid también posee un programa llamado dnsserver, que busca nombres de dominio. Cuando Squid empieza a trabajar, utiliza un número configurable de dnsserver, y cada uno de ellos realiza una búsqueda en DNS. Así se reduce la cantidad de tiempo que la caché debe esperar a estas búsquedas DNS.

Un paquete de datos: es una unidad fundamental de transporte de información en todas las redes de computadoras modernas. El término datagrama es usado a veces como sinónimo. Un paquete está generalmente compuesto de tres elementos: una cabecera (header en inglés) que contiene generalmente la información necesaria para trasladar el paquete desde el emisor hasta el receptor, el área de datos (payload en inglés) que contiene los datos que se desean trasladar, y la cola (trailer en inglés), que comúnmente incluye código de detección de errores.

Administración de red: Es un conjunto de técnicas tendientes a mantener una red operativa, eficiente, segura, constantemente monitoreada y con una planeación adecuada y propiamente documentada.

Computación: Es el estudio de los fundamentos teóricos de la información y el cómputo, así como las técnicas prácticas para sus implementaciones y aplicación en sistemas de cómputo.

PHP: Preprocessed Hypertext Pages es un lenguaje interpretado de propósito general ampliamente usado, diseñado especialmente para desarrollo web y que puede ser incrustado dentro de código HTML.

Generalmente se ejecuta en un servidor web, tomando el código en PHP como su entrada y creando páginas web como salida.

Modelo de Capas: Estructura conceptual que explica el propósito y la interacción de un grupo de protocolos. La estructura de capas es benéfica principalmente para los diseñadores de protocolos; una vez implantados, los protocolos pueden utilizarse sin entender la estructura de capas.

Enlace de datos: Conjunto de los medios utilizados para transmitir entre 2 puntos designados una señal digital que tiene una velocidad binaria nominal especificada.

Red de Computadores: Es un conjunto de equipos conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información (archivos), recursos (CD-ROM, impresoras, etc.), servicios (acceso a internet, e-mail, chat, juegos), etc. incrementando la eficiencia y productividad de las personas.

Licencia Gnu/Gpl: La Licencia Pública General GNU, o GPL, es una licencia de código abierto. El código abierto, o "Software Abierto", significa que son abiertos de modificar y redistribuir el código fuente bajo ciertas condiciones. Gratuito no se refiere al precio, se refiere a la libertad.

Firewall: Es un dispositivo que funciona como cortafuegos entre redes, permitiendo o denegando las transmisiones de una red a la otra. Un uso típico es situarlo entre una red local y la red Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial.

DHCP: El Protocolo de configuración de host dinámico es un protocolo que permite que un equipo conectado a una red pueda obtener su configuración (principalmente, su configuración de red) en forma dinámica (es decir, sin intervención particular). Sólo tiene que especificarle al equipo, mediante DHCP, que encuentre una dirección IP de manera independiente. El objetivo principal es simplificar la administración de la red.

DNS: El DNS (Domain Name Service) es un sistema de nombres que permite traducir de nombre de dominio a dirección IP y vice-versa. Aunque Internet sólo funciona en base a direcciones IP, el DNS permite que los humanos usemos nombres de dominio que son bastante más simples de recordar (pero que también pueden causar muchos conflictos, puesto que los nombres son activos valiosos en algunos casos).

Proxy: Hace referencia a un programa o dispositivo que realiza una acción en representación de otro. Su finalidad más habitual es la de servidor proxy, que sirve para permitir el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado, esto es, una única dirección IP.

Servidor Web: Es un programa que está diseñado para transferir hipertextos, páginas web o páginas HTML (HyperText Markup Language): textos complejos con enlaces, figuras, formularios, botones y objetos incrustados como animaciones o reproductores de música. El programa implementa el protocolo HTTP (HyperText Transfer Protocol) que pertenece a la capa de aplicación del modelo OSI. El término también se emplea para referirse al ordenador que ejecuta el programa.

Servidor de Archivos e Impresión: Es un equipo con un software especial que permite centralizar y compartir archivos dentro de su red, en donde

cualquier computador conectado a su red y con los permisos apropiados puede ver o modificar los archivos.

Squid: Servidor proxy-caché Squid es un servidor web proxy-caché con licencia GPL cuyo objetivo es funcionar como proxy de la red y también como zona caché para almacenar páginas web, entre otros.

RESUMEN

TITULO: ELABORACIÓN DE UNA GUÍA PARA LA INSTALACIÓN, CONFIGURACIÓN Y ADMINISTRACIÓN DE LA RED INFORMÁTICA DE LA FUNDACIÓN COLEGIO UIS (FCUIS) BASADA EN SOFTWARE DE CÓDIGO ABIERTO [*]

AUTORES: NANCY CAMACHO CUBIDES Y HELVERT CASTELLANOS QUIROZ[**]

PALABRAS CLAVES: Servidor Contenido Web Proxy Cortafuegos

Descripción detallada de cada uno de los pasos realizados durante el recorrido de la instalación, configuración y administración del sistema operativo basado en código abierto. Con la herramienta se realiza controles de acceso a nivel de seguridad, actividades de control de filtración de datos, permite prohibiciones en la transferencia de archivos y documentos específicos, se garantiza los recursos de la red, restringiendo el acceso a usuarios no autorizados. Mediante el sistema se otorga al usuario políticas de acceso, por ejemplo las máquinas a las que se puede conectar o de las que pueden recibir información y el tipo de datos, haciendo uso de reglas que filtren el tráfico de acuerdo a determinados parámetros, como protocolo, dirección origen o destino y puertos utilizados. Empleando un computador con dos o más tarjetas de red que bloqueen las diferentes redes (o segmentos de ellas) instaladas, se enlazan los paquetes de las redes y se determina cuáles pueden pasar o no y a qué red lo harán, con el propósito de buscar encaminar los paquetes de tránsito entre redes de manera más segura. Con la aplicación se puede administrar mediante el entorno grafico para efectuar tareas complejas como son la de establecer reglas de filtrado para la creación de políticas para el tráfico entrante y saliente de la red interna. Además de utilización de restricciones para dar solución a los problemas de trafico de paquetes en la red.

---

[*] monografía

[**]Facultad De Ingeniería Electrónica, Eléctrica y Telecomunicaciones. Escuela de Inenieria Electrica . Director Freddy Alfonso Beltrán Miranda.

SUMMARY

I TITLE: UNA'S PRODUCTION GUIDES FOR THE INSTALLATION, CONFIGURATION AND ADMINISTRATION OF THE IT NETWORK OF THE FOUNDATION I BECOME A MEMBER OF ASSOCIATION UIS (FCUIS) BASED ON SOFTWARE OF OPENED CODE [*]

AUTHORS: NANCY CAMACHO CUBIDES AND CASTILIAN HELVERT QUIROZ [**]

KEY WORDS: Contained Servant Web Proxy Cortafuegos

Detailed description of each one of the steps realized during the tour of the installation, configuration and administration of the operating system based on opened code. With the tool there are realized controls of access to safety level, activities of control of filtration of information, allow prohibitions in the transfer of files and specific documents, the resources of the network are guaranteed, restricting the access to not authorized users. By means of the system policies of access are granted to the user, for Example the machines to which it is possible to connect or of those who can receive information and the type of information, using rules that leak the traffic of agreement to certain parameters, as protocol, direction origin or destination and used ports. Using a computer with two or more cards of network that block the different networks (or segments of them) installed, the packages of the networks are connected and one determines which can To happen or not and to what network they it will do, with the intention of seeking to direct the packages of traffic between networks of a surer way. With the application it is possible to administer by means of the graphical environment to effect complex tasks since they are her of establishing rules of leaked for the creation of policies for the next and salient traffic of the internal network. Besides utilization of restrictions to give solution to the problems of traffic of packages in the network.

---

[*] Monograp`hy

[**] Faculty Of Electronic, Electrical Engineering and Telecommunications. School Engineering Electrical Director Freddy Alfonso Beltrán Miranda.

INTRODUCCIÓN

Independiente de la forma que se planee el ambiente en el cual se ejecuten los sistemas, no se debe tener la seguridad como algo garantizado, inclusive los sistemas independientes así no estén enlazados con Internet representan un riesgo (indiscutiblemente los peligros son incomparables a otros sistemas que también tengan enlaces fuera de la red corporativa).

Es indispensable considerar todos los peligros que circundan, cuando se trata de dar seguridad a las redes informáticas. Dentro de los posibles conflictos que se pueden presentar están: El origen de las diferentes amenazas a cada uno de los sistemas que estén a cargo, El sitio, el tipo de información bajo su cuidado, La periodicidad del ingreso autorizado a los sistemas.

Cuando se establecen parámetros de seguridad, no se debe asumir que las probabilidades de intentos de ataque de los intrusos solo están en el mundo externo, es posible que también estén dentro de la institución. En numerosas ocasiones el individuo labora en la empresa. De tal manera que es bueno observar a todo aquel que asedie la oficina y cuestionarse ¿Qué sucedería si esa gente pretendiera perturbar la seguridad? Lo cual no quiere decir que los compañeros de trabajo son unos criminales. Sencillamente representa que se debe revisar el esquema de trabajo de cada persona y definir las posibles violaciones de seguridad para poder implementar de acuerdo a los perfiles, en caso de que fuesen esas las intenciones.

La persona que tenga la intensión de vulnerar la seguridad a menudo utiliza la inteligencia humana para violar los controles de acceso tecnológico. Los

administradores de sistemas deben tener en cuenta estas situaciones y hacer lo posible por establecer controles de seguridad con la finalidad de realizar un buen desempeño como administrador.

1. EL PROBLEMA

1.1. PLANTEAMIENTO DEL PROBLEMA

La finalidad de este proyecto es elaborar una guía para la implementación de software de código abierto que facilité la administración de la red informática de la Fundación Colegio UIS. En la actualidad la Institución no cuenta con un servidor de seguridad informático, ni tiene implementada ninguna política básica de administración que le permita protegerse del más mínimo ataque informático. La destrucción parcial o total de la información y la manipulación de los datos es una de las mayores preocupaciones de este establecimiento, ya que puede en un momento dado, ocasionar grandes pérdidas económicas y hacer parar la empresa en sus labores cotidianas. En este colegio la información se encuentra centralizada siendo el centro de cómputo el mayor activo, pero a la vez lo hace el más vulnerable.

La función informática trata de nuevas tecnologías, aplicaciones, dispositivos hardware, formas de elaborar información más consistente, etc, pero no se puede pasar por alto la base por la cual existen estos elementos, siendo esta, la información, por esto es importante poseer una guía para la administración de la red informática de la institución.

No obstante las pequeñas y medianas empresas componen la gran parte del inmenso mundo empresarial, y sin embargo con frecuencia se observa que carecen de soluciones tecnológicas que se adapten a sus necesidades o recursos (talento humano, financieros o técnicos) existentes. En la industria de los servidores, se considera que hasta el momento las PYMEs han carecido de opciones de donde elegir, y usualmente hay en el mercado

soluciones sobredimensionadas a sus requerimientos actuales. Además sin elecciones de gestión de redes que cumpliesen con todos los dispositivos requeridos y con facilidad para administrar.

¿Cómo optimizar y mejorar la administración de la red informática de la Fundación Colegio UIS (FCUIS)?

1.2. OBJETIVOS

1.2.1. Objetivo General

Elaborar una guía para la instalación, configuración y administración de las redes informáticas de la Fundación Colegio UIS (FCUIS), mediante servidores de software de código abierto, en busca de optimizar la administración de servicios de la red informática.

1.2.2. Objetivos Específicos

Definir estrategias para la gestión y control de los datos y las aplicaciones, en busca del bloqueo de amenazas e intrusiones, en la red informática de la Fundación Colegio UIS.

Identificar factores limitantes, supervisando el desempeño en su infraestructura de red, con el uso de políticas de acceso al contenido web, buscando mejorar la seguridad en la navegación e incrementando la velocidad.

Crear un documento guía que sirva de ayuda para la instalación, configuración y administración de la red informática de la Fundación Colegio UIS (FCUIS) basado en servidores de software de código abierto.

1.3. JUSTIFICACIÓN

Hoy en día la información es uno de los activos más importantes para las empresas, siendo necesario aplicar políticas efectivas de administración de la red informática, para contrarrestar falencias que se puedan presentar.

El colegio procesa diariamente información confidencial (nomina, presupuesto, planes, cotizaciones, contabilidades, …etc.), por tanto este proyecto busca garantizar que los recursos informáticos estén siempre disponibles, para que puedan utilizarlos y que no estén dañados por problemas externos, como la intrusión de personas no autorizadas al sistema, donde podrían estar viendo o sacando información confidencial y en el caso más extremo dañando todas las bases de información de la institución, para lo cual es necesario contar con una adecuada administración de la red informática, que permita diseñar reglas o actividades que logren prevenir, resguardar y proteger toda la información importante para la empresa.

Realizar una óptima administración de la red informática previene el riesgo de aquellas personas en el mundo con un alto conocimiento en sistemas, dedicadas a buscar compañías y empresas donde no tienen aun un buen sistema de seguridad informático, para robar información y venderla al mejor postor. Estos piratas informáticos pueden proceder de manera externa conectándose vía internet y logrando accesar a nuestra red o también suelen encontrarse dentro de la misma empresa. Según expertos en informática el 70% de intrusiones al sistema proviene de personal interno de las empresas, los cuales conocen cual es la información importante de la compañía y donde se encuentra. Estas situaciones se presentan debido a las débiles políticas en la administración que tienen las empresas en las redes informáticas, lo cual permiten que sea fácil que un pirata manipule la información.

Es aquí donde la solución de una guía para la instalación y administración de la red informática encuentra su encaje, mediante el uso de servidores de software de código abierto para ser implementados en la Fundación Colegio UIS (FCUIS), permitiendo a profesionales TIC administrar todos los servicios de una red informática, tales como el acceso a Internet, la seguridad y la infraestructura de la red, los recursos compartidos o las comunicaciones, a través de una única plataforma. Todas estas funcionalidades están estrechamente integradas, automatizando la mayoría de las tareas y ahorrando tiempo en la administración de sistemas. Estas características pueden desplegarse en distintas máquinas o en un único servidor, eligiendo para cada caso la combinación funcional y de hardware más conveniente.

Este trabajo de grado permite al estudiante aplicar los conocimientos recibidos en la especialización de telecomunicaciones.

1.4. ESTADO DEL ARTE

La Administración de Redes Informáticas son un conjunto de acciones cuyo objetivo primordial es mantener la red operativa, eficiente, y segura.
La administración de la red debe por tanto conseguir:

- Mejorar la continuidad de la red con mecanismos de control interno y externo.
- La resolución de problemas en el menor tiempo posible.
- Hacer uso eficiente de todos los recursos de la red: programas, impresoras.
- Convertir la red lo más segura posible, protegiéndola contra intrusos.
- Controlar cambios y actualizaciones en la red y su software para minimizar las interrupciones en el servicio a los usuarios.

Para ello la administración de la red debe favorecer mecanismos de seguridad para lo siguiente:

- Identificación y autentificación del usuario, una clave de acceso y un password.
- Autorización de acceso a los recursos, es decir, solo personal autorizado.
- Confidencialidad.

Un administrador de redes en general, se encarga principalmente de asegurar el correcto funcionamiento de la red, es lo que también es llamado mantenimiento de redes informáticas[1].

La Administración de Redes es un conjunto de técnicas tendientes a mantener una red operativa, eficiente, segura, constantemente monitoreada y con una planeación adecuada y propiamente documentada.
Sus objetivos son:

Mejorar la continuidad en la operación de la red con mecanismos adecuados de control y monitoreo, de resolución de problemas y de suministro de recursos.

Hacer uso eficiente de la red y utilizar mejor los recursos, como por ejemplo, el ancho de banda.

Reducir costos por medio del control de gastos y de mejores mecanismos de cobro.

Hacer la red más segura, protegiéndola contra el acceso no autorizado, haciendo imposible que personas ajenas puedan entender la información que circula en ella.

[1] http://www.redesinformatica.es/administracion-redes-informaticas.html

Controlar cambios y actualizaciones en la red de modo que ocasionen las menos interrupciones posibles, en el servicio a los usuarios.

La administración de la red se vuelve más importante y difícil si se considera que las redes actuales comprendan lo siguiente:

Mezclas de diversas señales, como voz, datos, imagen y gráficas.

Interconexión de varios tipos de redes, como WAN, LAN y MAN.

El uso de múltiples medios de comunicación, como par trenzado, cable coaxial, fibra óptica, satélite, láser, infrarrojo y microondas.

Diversos protocolos de comunicación, incluyendo TCP/IP, SPX/IPX, SNA, OSI.

El empleo de muchos sistemas operativos, como DOS, Netware, Windows NT, UNÍS, OS/2.

Diversas arquitecturas de red, incluyendo Ethernet 10 base T, Fast Ethernet, Token Ring, FDDI, 100vg-Any Lan y Fiber channel.

Varios métodos de compresión, códigos de línea, etc.

El sistema de administración de red opera bajo los siguientes pasos básicos:

1.- Colección de información acerca del estado de la red y componentes del sistema. La información recolectada de los recursos debe incluir: eventos, atributos y acciones operativas.

2.- Transformación de la información para presentarla en formatos apropiados para el entendimiento del administrador.

3.- Transportación de la información del equipo monitoreado al centro de control.

4.- Almacenamiento de los datos coleccionados en el centro de control.

5.- Análisis de parámetros para obtener conclusiones que permitan deducir rápidamente lo que pasa en la red.

6.- Actuación para generar acciones rápidas y automáticas en respuesta a una falla mayor.

Característica fundamental de un sistema de administración de red moderno es la de ser un sistema abierto, capaz de manejar varios protocolos y lidiar con varias arquitecturas de red. Esto quiere decir: soporte para los protocolos de red más importantes[2].

[2] http://www.scribd.com/doc/15800385/Administrador-de-Red

2. INSTALACIÓN, CONFIGURACIÓN Y ADMINISTRACIÓN DE LA RED INFORMÁTICA DE LA FUNDACIÓN COLEGIO UIS (FCUIS)

Figura 1. Fundaciòn Colegio UIS (FCUIS)

Fuente: PERTENECE A LA FUNDACION COLEGIO UIS

Como primera medida antes de la instalación se requiere contar con un equipo que tenga la utilidad de servidor, el cual debe tener dos tarjetas de red. Por lo general los computadores de hoy en día traen una tarjeta de red interna y solo se necesita instalar una nueva tarjeta de red adicional en la cpu.

El procedimiento de la instalación contempla varias dificultades a la hora de la instalación de la tarjeta de red adicional ya que no todas las tarjetas de red son reconocidas por Linux. Por tanto es aconsejable contar con una tarjeta de red de una marca reconocida para que Linux la detecte e instale los drivers automáticamente.

El equipo deberá contar adicionalmente con una unidad de dvd, para realizar la instalación. Ver Anexo 1. Instalación de Linux RedHat Enterprise 5.

Para que sea más fácil la instalación se debe preparar el disco duro, esto quiere decir que Linux busca particiones libres o sin formato para la instalación, por tanto se recomienda crear una partición grande o toda sin formato, para cuando se arranque desde el dvd el instalador encuentre la partición y comience hacer la instalación automática.

Las características del equipo empleado en la instalación de Linux RedHat Enterprise 5 son: Pentium 4 de 2.8 Ghz, con disco duro de 80 GB, y una memoria RAM de 1GB, teclado en español, monitor lcd de 17 y mouse óptico, las cuales cumplen con los requerimientos de Hardware necesarios para la instalación de RedHat Enterprise 5.

Figura 2. Equipo Servidor

Fuente: Autores del proyecto

En la Fundación Colegio UIS se tienen dos tarjetas de red, la que sirve para conectar el cable que viene del proveedor de internet o desde el modem y la otra tarjeta conecta con el switch que enlaza el servidor con la red. La tarjeta de red que se conecto al modem se denomina etho y la segunda que conecta con el switch se denomino eth1. La tarjeta etho se configura como DCHP porque el proveedor asignó una IP automáticamente, y la tarjeta eth1 se configuró manualmente para asignarle una IP del mismo rango de la red, quedando así: la red es 192.168.1.0/24 y la IP asignada es 192.168.1.100.

2.1. SERVIDOR PROXY SQUID

Figura 3. Servidor Proxy Squid

Imagen: http://www.1800sw.com/esp/Servicios-corporativos/Servidores-Proxy-165-90.html

Los servidores proxy generalmente funcionan como cortafuegos, trabajando como filtro de paquetes, también nuestro servidor proxy trabajara como cache de contenido o cache de páginas web ya visitadas o de archivos ya descargados por nuestros clientes.

La primera vez que un cliente visita una página web, el servidor revisa si esa pagina ya está guardada en la cache del servidor proxy para contestarle, sino busca en internet esa página, luego de descargarla guarda una copia en la cache del servidor y enseguida devuelve la pagina al cliente que la solicito, la

próxima vez que un cliente solicita la misma página, el servidor revisa la cache y cuando encuentra la pagina solicitada la devuelve inmediatamente sin necesidad que salga a internet a buscarla. Esto mismo lo hace con los archivos descargados y almacenados en la cache.

El servidor proxy almacena la cache en un directorio que nosotros más adelante configuraremos, dando su ubicación y tamaño para este servicio.

Squid es un servidor que hace la función de intermediario entre internet y la red local de nuestra empresa, es un servidor de gran desempeño que ha sido desarrollado por muchos años y es muy popular y muy utilizado por las grandes empresas por lo confiable, estable y robusto. Se distribuye con Licencia Pública General **GNU (GNU/GPL).** Es de código Libre

2.2. INSTALACIÓN DEL SERVIDOR PROXY SQUID

Figura 4. Instalación Del Servidor Proxy Squid

Fuente: Autores del proyecto

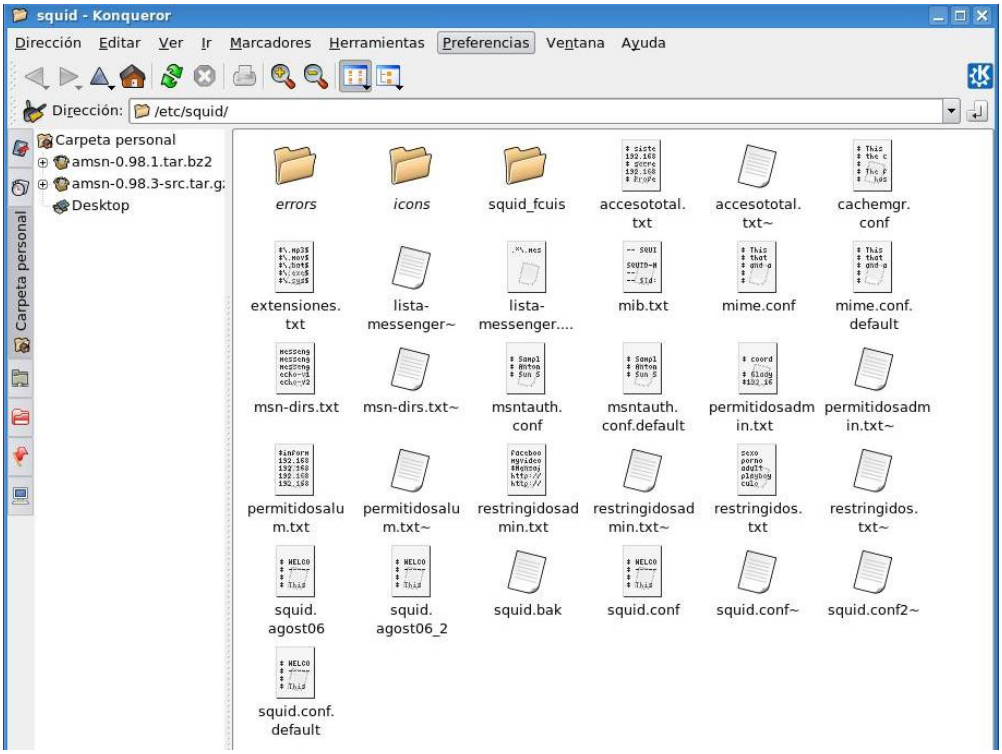
Para poder instalar el servicio de squid tendremos que ejecutar lo siguiente como usuario root.

[root@fcuis~]# yum install squid

Con esto instalaremos nuestro servidor squid más las dependencias que tenga.

Ahora que tenemos nuestro servidor squid instalado deberemos saber en donde se encuentra todos los archivos de configuración del mismo.

Figura 5. /etc/squid



Fuente: Autores del proyecto

Dentro de este directorio se encuentran varios archivos pero el más importante es el squid.conf el cual se encarga de la configuración del servicio.

Ahora es recomendable sacar una copia del archivo que vamos a editar.

[root@fcuis squid]# cp squid.conf squid.conf-bak

2.2.1. Configuración Squid

Comenzaremos a configurar nuestro servidor squid, lo podemos editar con un editor grafico como el Kwrite o con uno de la consola como el Vi[root@fcuis squid]# vi squid.conf

Parámetro http_port

En este parámetro configuramos el puerto de escucha de nuestro servidor squid, por default es el puerto 3128, pero también puede ser utilizado el 8080. http_port 3128

Parámetro cache_mem

Aquí configuraremos la cantidad de memoria RAM que destinaremos para almacenar los datos más solicitados. Esta opción viene comentada por los cual la des comentaremos para darle un valor reservado en memoria RAM.

cache_mem 8 MB

por

cache_mem 256 MB

El valor depende de la cantidad de memoria Ram que tengamos, podemos colocar una tercera parte de nuestra memoria si el equipo lo tenemos solo dedicado a este servicio.

Parámetros cache_swap

Dentro del cache_swap, existen dos parámetros: cache_swap_low y cache_swap-hight Con estos le decimos a squid que mantenga los niveles del espacio del área de intercambio o también conocido como swap. Estos

parámetros vienen siempre desactivados por el cual los buscaremos para activarlos.

#cache_swap_low 90

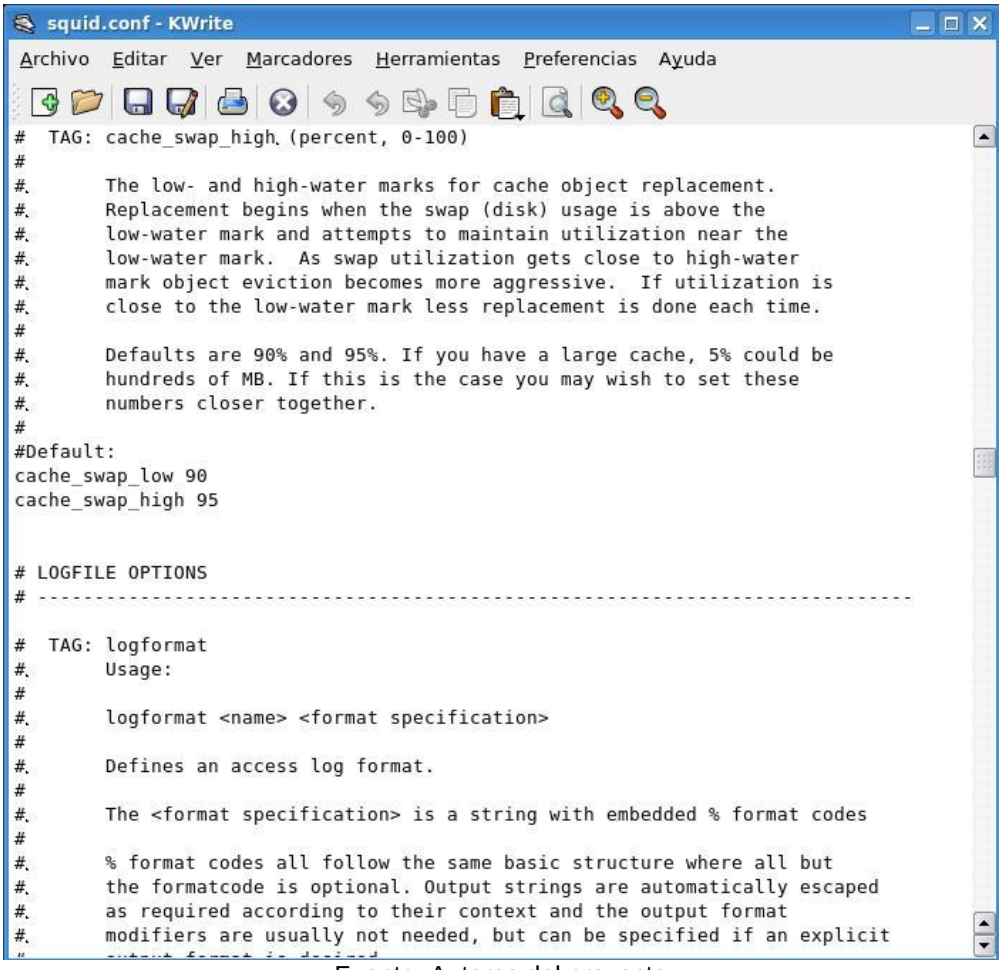
#cache_swap_high 95

por

cache_swap_low 90

cache_swap_high 95

Figura 6. swap_high 95



Fuente: Autores del proyecto

Con esto decimos al squid que mantenga los niveles del espacio del área de intercambio entre 90% y 95%.

Utilizamos esta directiva para indicar el tamaño máximo para los objetos a almacenar en la cache.
#maximum_object_size 4096 KB
Por
maximum_object_size 10240 MB

Parámetro hierarchy_stoplist

Este parámetro es de utilidad para indicarle a nuestro squid que paginas que contengan ciertos caracteres no deben almacenarse en cache. También se pueden incluir como sitios de webmail y paginas locales en su red ya que no sería necesario almacenarlas en el cache, esta opción ya viene habilitada solamente tendremos que modificarle algunos datos de la misma.
hierarchy_stoplist cgi-bin ?
Por
hierarchy_stoplist cgi-bin ? hotmail gmail yahoo fcuis.edu.co

Parámetro visible_hostname

Es el nombre que le hemos dado al equipo a la hora de instalación, el nombre debe ser igual a los siguientes ficheros /etc/hosts y en /etc/sysconfig/network. Este parámetro no viene configurado en el archivo, tendremos que agregar esta línea en nuestro archivo de configuración squid.conf.
A veces por la falta de esta línea nuestro servicio de squid no arranca
También podemos escribir el nombre de localhost o fcuis
visible_hostname fcuis

Parámetro cache_dir

En este parámetro digitaremos el tamaño que deseamos que tenga la cache en nuestro disco duro, por lo cual tendremos que habilitar y modificar el siguiente dato.

#cache_dir ufs /var/spool/squid 100 16 256

Por

cache_dir ufs /var/spool/squid 5000 16 256

Con esto configuraremos el tamaño que deseamos que tenga la cache en el disco, se puede incrementar hasta el tamaño que deseemos, nosotros establecemos 5000 MB (5 GIGAS de cache con 16 directorios subordinados y 256 niveles cada uno.

Parámetro access_log

Indicaremos en que directorio guardaremos el registro de accesos al squid, este parámetro es importante para auditar problemas en nuestro servicio de squid.

access_log /var/log/squid/access.log squid

Parámetro cache_log

Establece en donde se almacenaran los mensajes del comportamiento de la cache de squid. Por defecto viene desactivado.

cache_log /var/log/squid/cache.log

Regla Tipo macaddress

En esta regla podemos administrar squid utilizando Mac Address.

acl [Nombre] arp “Mac Address”

Ejemplo: Esta regla se llama sistemas Mac por la cual proporcionamos las Mac Address de las máquinas clientes.

acl sistemasmac arp 09:00:2b:23:45:67 00:1f:3c:5f:fd:b1
00:1e:ec:70:7e:24

Regla Tipo password

En esta regla, se administra el acceso a internet utilizando un usuario y contraseña, para lograr habilitar este método debemos hacer lo siguientes pasos de configuración.

1) Debemos crear el archivo que contiene las claves.
[root@fcuis squid]# touch claves
2) Le damos permisos de Lectura/Escritura y usuario encargado del archivo.
[root@fcuis squid]# chmod 600 claves
[root@fcuis squid]# chown squid.squid claves

3) Creación de usuario y password para el acceso a internet.
[root@fcuis squid]# htpasswd claves sistemas

4) Habilitamos las siguientes opciones dentro del archivo de configuración del servidor squid, veamos el primer parámetro: auth_param basic.
#auth_param basic program <descomente y complete esta línea

Este parámetro lo arreglaremos de la siguiente forma.
auth_param basic program /usr/lib/squid/ncsa_auth /etc/squid/claves
Hemos enlazando el programa que nos permitiría autenticarnos, y el archivo donde se encuentran las cuentas de los usuarios.

acl password proxy_auth REQUIRED

5) Ya al final tendremos que habilitar la regla acl encargada de la autenticación de la contraseña o password.

#acl password proxy_auth REQUIRED

Por

acl password proxy_auth REQUIRED

Con esto ya tendremos configurada y habilitada la regla para la autenticación de los usuarios.

Reglas acl (Listas de Control de Acceso)

Listas de Control de Acceso, por medio de estas reglas podremos dar permisos a grupos de usuarios o archivos que contengan ciertas reglas, direcciones web, ips etc.

Figura 7. Sala informática

Fuente: Autores del proyecto

Tabla 1. Tipo src

src	time
dts	url_regex
srcdomain	urlpath_regex
dstdomain	req_mime
srcdom_regex	macaddress
dstdom_regex	password

Fuente: http://www2.linuxparatodos.net/web/comunidad/base-de-conocimiento/-/wiki/Base%20de%20Conocimiento/Servidor+Proxy

Regla Tipo src

Esta regla especifica una o varias direcciones IP o un segmento de red con su máscara de red.

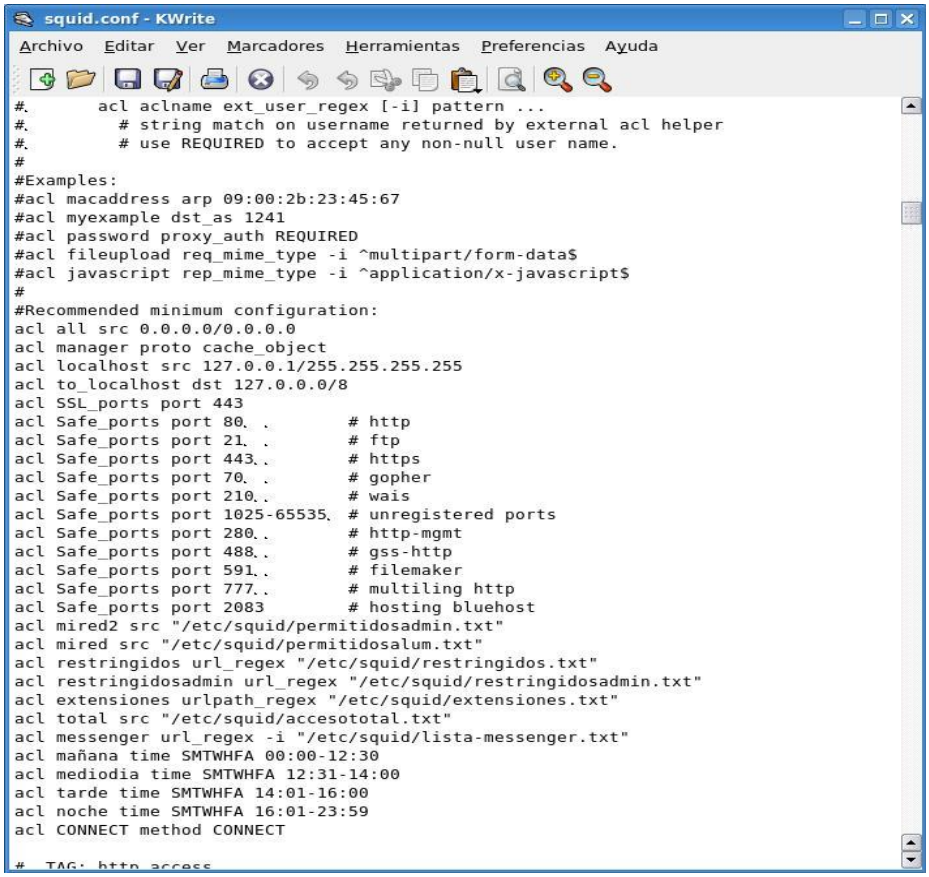
acl [Nombre] src [Contenido]

la primera src que utilizaremos es la que creamos para indicar todos las direcciones ips de internet y que la llamamos **all**
acl all src 0.0.0.0/0.0.0.0
con esta regla podremos dar permiso a las demás direcciones y luego denegar al resto de direcciones utilizando la palabra **all** la cual ya hemos definido anteriormente como todas las direcciones ips excepto las direcciones que hayamos permitido antes.

para la configuración del colegio fcuis hemos configurado dos listas mas con el parámetro src, la primera la hemos llamado **mired** que contiene en un archivo llamado permitidosalum.txt las direcciones ips de los equipos que pertenecen a las aulas informáticas de los estudiantes y que lo hemos

almacenado en /squid/etc/permitidosalum.txt y la segunda la hemos llamado **mired2** que contiene un archivo llamado permitidosadmin con las direcciones ips de los equipos administrativos y que lo hemos almacenado en la misma dirección anterior. /squid/etc/permitidosadmin.txt

Figura 8. acl mired src "/squid/etc/permitidosalum.txt"



Fuente: Autores del proyecto

#informática bto
192.168.1.100
192.168.1.101
192.168.1.102
192.168.1.103
192.168.1.104
192.168.1.105
192.168.1.106
192.168.1.107

192.168.1.108
192.168.1.109
192.168.1.110
192.168.1.111
192.168.1.112
192.168.1.113
192.168.1.114
192.168.1.115
192.168.1.116
192.168.1.117
192.168.1.118
192.168.1.119
192.168.1.120
192.168.1.121
192.168.1.122
192.168.1.123
192.168.1.124
192.168.1.125
192.168.1.126
192.168.1.127
192.168.1.128
192.168.1.129
192.168.1.130
192.168.1.131
192.168.1.132
192.168.1.133
192.168.1.134
192.168.1.135
192.168.1.136
192.168.1.137
192.168.1.138
192.168.1.139
192.168.1.140
192.168.1.141
192.168.1.142

#sala informática pria

192.168.1.50
192.168.1.51
192.168.1.52
192.168.1.53
192.168.1.54
192.168.1.55
192.168.1.56

192.168.1.57
192.168.1.58
192.168.1.59
192.168.1.60
192.168.1.61
192.168.1.62
192.168.1.63
192.168.1.64
192.168.1.65
192.168.1.66
192.168.1.67
192.168.1.68
192.168.1.69
192.168.1.70
192.168.1.71
192.168.1.72
192.168.1.73
192.168.1.74
192.168.1.75
192.168.1.76
192.168.1.77
192.168.1.78
192.168.1.79
192.168.1.80
192.168.1.81
192.168.1.82

#Preescolar
192.168.1.157

acl mired2 src "/squid/etc/permitidosadmin.txt"

Coordinación Académica

192.168.1.164

192.168.1.160

#Coordinación General

192.168.1.162

#equipo emisora
192.168.1.243

#Asopadres
192.168.1.196

Sala de profesores bto
192.168.1.236
192.168.1.205
192.168.1.206

#Sala de Idiomas
192.168.1.245

#sala de Música
192.168.1.167

#Recursos Humanos
192.168.1.235
192.168.1.239

#secretaria Académica

192.168.1.174
192.168.1.145

192.168.1.173
#Servidor Impresoras
192.168.1.253

#Equipo de Artes (audio visuales)
192.168.1.254

#biblioteca
192.168.1.161

#terapia ocupacional
192.168.1.215

Sala de profesores pria
192.168.1.175
192.168.1.208

#almace
192.168.1.240

#Rectoría
192.168.1.238

#Psicología

192.168.1.210
192.168.1.222

#Laboratorio Química
192.168.1.166

#Publicaciones
192.168.1.170
#Cafetería

192.168.1.251

#Practicante SENA
192.168.1.252

#Laboratorio física
192.168.1.163

#Mantenimiento
192.168.1.237

192.168.1.50

192.168.1.143

192.168.1.248

192.168.1.250

Otra regla es para los jefes y administradores que no tienen ninguna restricción. A esta regla la hemos llamado “accesototal”

acl total src "/squid/etc/accesototal.txt"

La cual contiene las ips de los administradores dentro del archivo accesototal.txt

Regla Tipo dts

Crea una dirección de destino en formato IP y mascara o el nombre del sitio a visitar.

acl [Nombre] dts [Contenido]

Esta regla la llamamos webmail la cual contendrá como destino final las direcciones de webmail más conocidos en internet.

acl webmail dst www.gmail.com www.hotmail.com www.yahoo.com fcuis.edu.co

Regla Tipo time

Esta regla establece un tiempo límite de conexión dentro de una semana.
Con esta regla podremos definir los tiempos en que determinados usuarios pueden navegar en internet, ya sea configurándolo por días o por horas. Aquí utilizaremos una letra en mayúscula que hace referencia a un dia de la semana. Los días están en Ingles y por eso la letra esta también en ingles.
Ejemplo: para el domingo que en ingles es Sunday, utilizaremos la letra S, para el Lunes que en Ingles es Monday utilizaremos la M, y así sucesivamente para el resto de días, la única excepción es con el sábado que en ingles se llama Saturday utilizaremos la segunda letra la A, ya que la S ya la utilizamos para el domingo.

Tabla 2. Parámetros fecha

Parámetros	Días
S	Domingo
M	Lunes
T	Martes
W	Miércoles
H	Jueves
F	Viernes
A	Sábado

Fuente: http://www2.linuxparatodos.net/web/comunidad/base-de-conocimiento/-/wiki/Base%20de%20Conocimiento/Servidor+Proxy

En el manejo de las horas se establece un horario de 24:00 hrs

acl [Nombre] time [días][horas]

En la Fundación Colegio UIS hemos establecido las siguientes reglas para ayudar administrar el uso del internet según las políticas de la Institución.

acl mañana time SMTWHFA 00:00-12:30
acl mediodia time SMTWHFA 12:31-14:00
acl tarde time SMTWHFA 14:01-16:00
acl noche time SMTWHFA 16:01-23:59

Hemos creado una regla que se llama **mañana** que establece un horario desde las 00:00 horas hasta las 12:30 del día.

Otra llamada mediodía que va desde las 12:31 hasta las 2:00 de la tarde
Otra llamada tarde que va desde las 02:01 pm hasta las 04:00 de la tarde
Y la ultima que la llamamos noche que va desde las 04:01 pm hasta las 11:59 de la noche

En esta configuración el horario hay que definirlo en hora militar que es como el squid lo reconoce, por eso las 2 de la tarde lo llamaremos las 14:00 horas.

Regla Tipo url_regex

Por medio de esta regla especificaremos expresiones para comprobar urls, para este tipo de regla debemos tener un archivo en cual agregamos todas las palabras que creemos importantes.

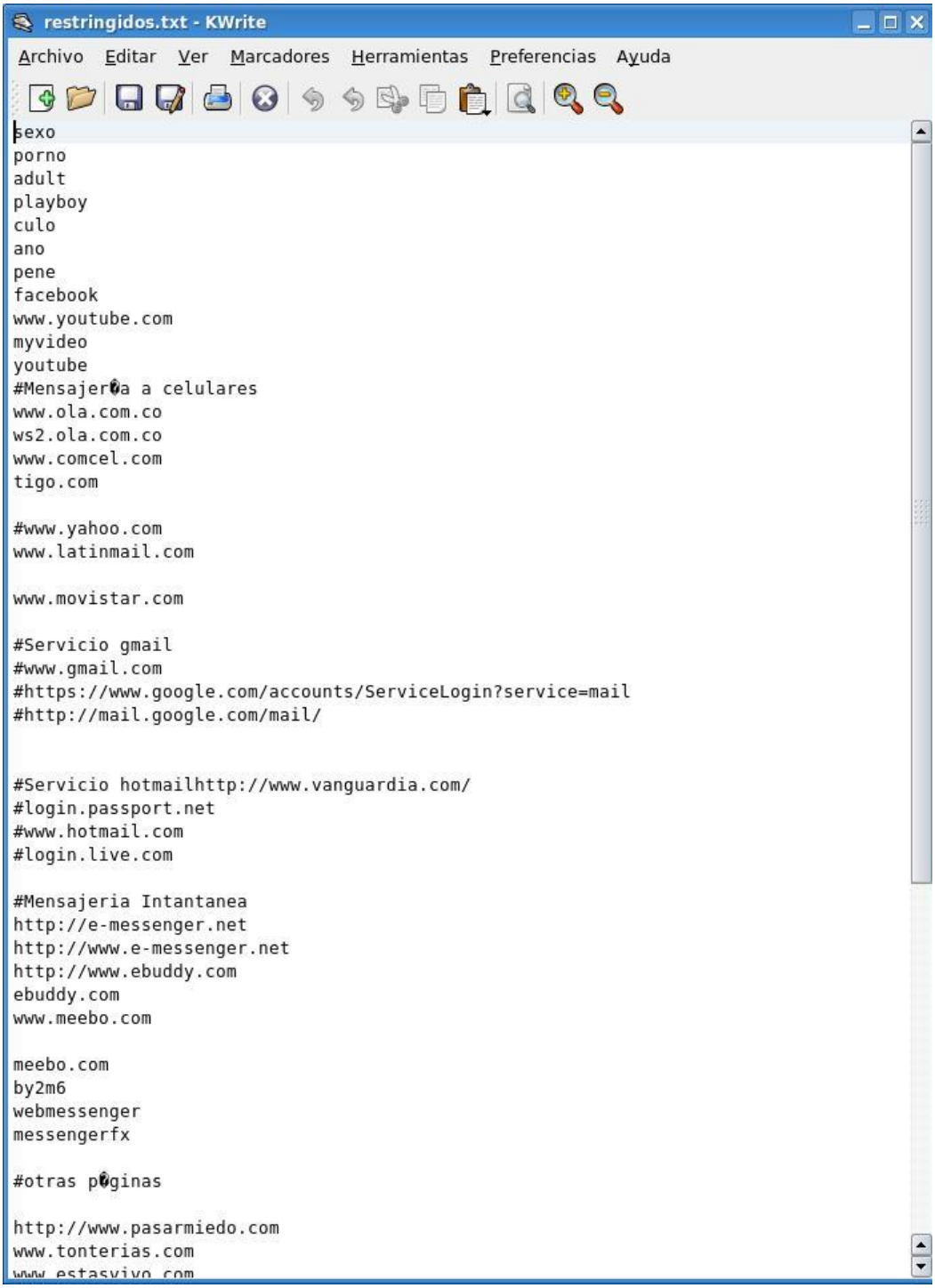
acl [Nombre] url_regex “Path”
Para nuestra configuración del squid hemos creado la siguiente regla
acl restringidos url_regex "/etc/squid/restringidos.txt"
acl extensiones urlpath_regex "/etc/squid/extensiones.txt"
acl messenger url_regex -i "/etc/squid/lista-messenger.txt"
Donde tenemos los contenidos de los archivos anteriormente mencionados, el archivo “restringidos.txt” contiene la lista de urls restringidas por la institución:
facebook
www.youtube.com
myvideo
youtube
#Mensajería a celulares
www.ola.com.co
ws2.ola.com.co
www.comcel.com
tigo.com

#www.yahoo.com
www.latinmail.com
www.movistar.com

#Servicio gmail
#www.gmail.com
#https://www.google.com/accounts/ServiceLogin?service=mail
#http://mail.google.com/mail/
#Servicio hotmail
#login.passport.net
#www.hotmail.com
#login.live.com
#Mensajeria Intantanea
http://e-messenger.net
http://www.e-messenger.net
http://www.ebuddy.com
ebuddy.com
www.meebo.com
meebo.com
by2m6
webmessenger
messengerfx
#otras páginas
http://www.pasarmiedo.com
www.tonterias.com
www.estasvivo.com
www.malgusto.com
www.soho.com
www.venus.com
podrido.com
minijuegos.com
helmerpardo.com
2600metros
elbananero.com

quegonorrea.com
iloveim
myspace.com
estasmuerto.com
/juegos/jugar.php?id=6829

Figura 9. Restringidos.txt



Fuente: Autores del Proyecto

Otra regla que utilizamos mucho es la de bloquear el msn live, a través del tiempo era muy fácil bloquear el Messenger pero con los nuevos msn que han salido como es el “msn live” poseen muchos servidores y puertos por medio del cual trabajan, pero después de una búsqueda intensa y pruebas en el servidor hemos logrado bloquear este servicio que es el más criticado por los gerentes y jefes de las empresas e instituciones educativas como es nuestro caso.

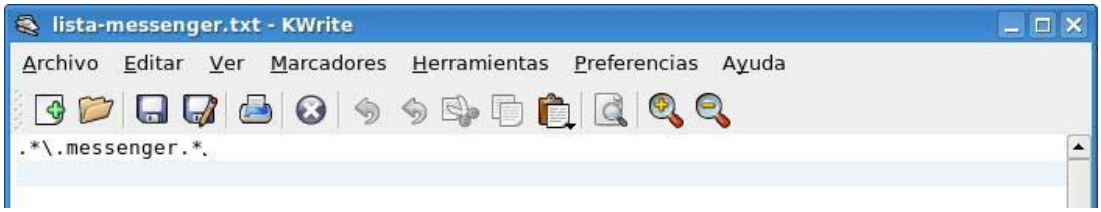
La regla es la siguiente:

Creamos un archivo llamado lista-messenger.txt y asignamos una **ACL** o lista de control de acceso para este archivo.

acl messenger url_regex -i "/etc/squid/lista-messenger.txt"

El contenido del archive es el siguiente;

Figura.10. *\.messenger.*.



Fuente: Autores del Proyecto

Aquí vemos cuando un usuario intenta ingresar al msn y está restringido por el servidor Proxy

Figura 11. Regla msn

Fuente: Autores del Proyecto

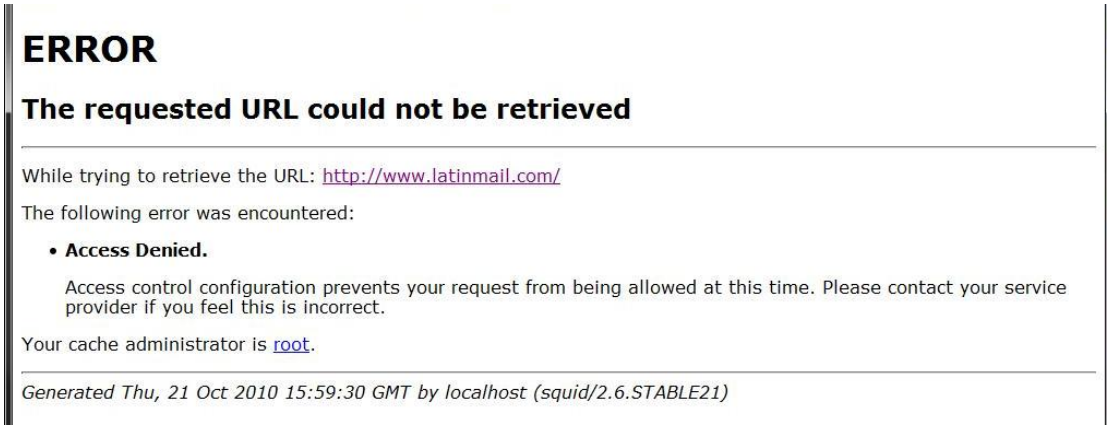
Otra regla muy utilizada es la de bloquear el facebook

Figura 12. Regla facebook

Fuente: Autores del Proyecto

También podemos bloquear páginas como por ejemplo: www.latinmail.com

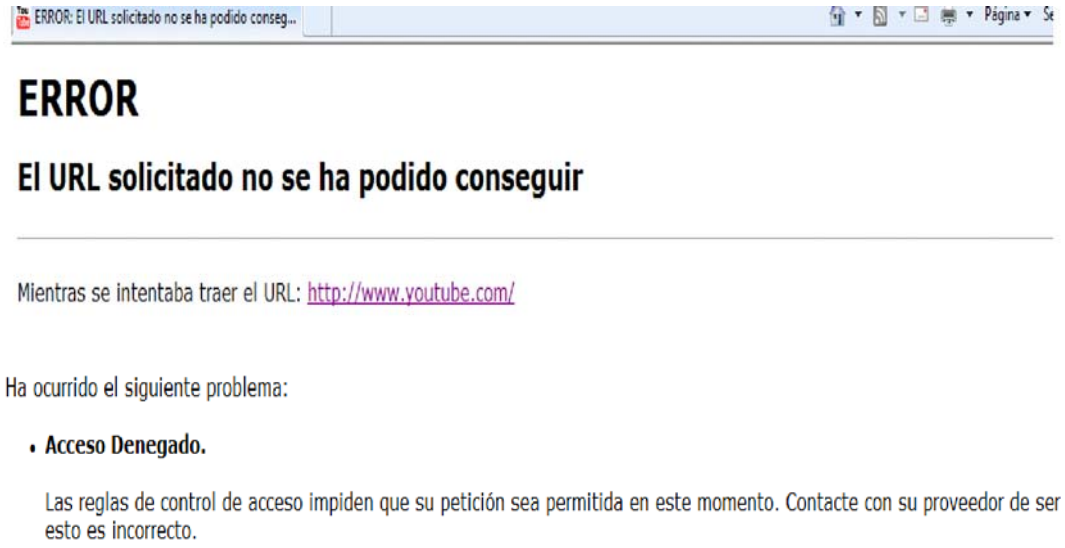
Figura 13. latinmail.com



Fuente: Autores del Proyecto

También podemos bloquear las páginas con videos como www.youtube.com para procurar mantener el ancho de banda para todos los usuarios.

Figura 14 regla yuotube

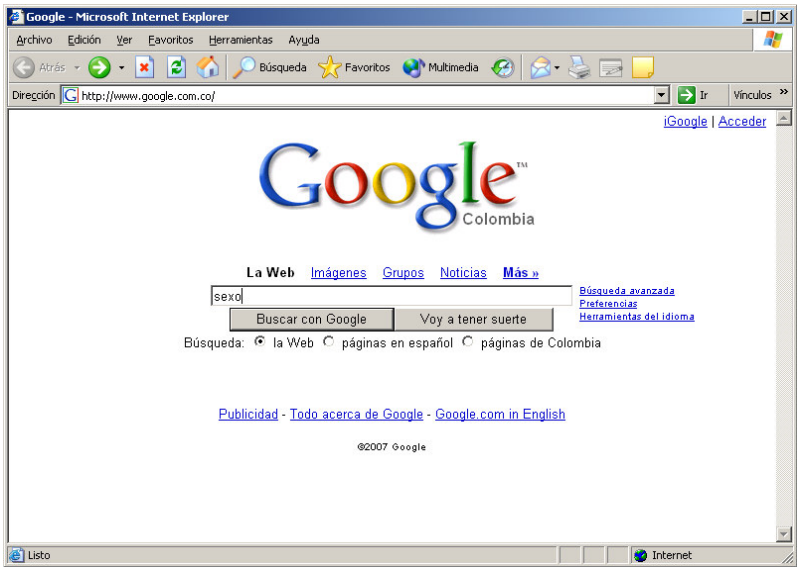


Fuente: Autores del Proyecto

Podemos también bloquear la búsqueda de diferentes palabras como por ejemplo:

Sexo, pornografía, y muchísimas palabras mas que estén prohibida para el estudiantado del Colegio.

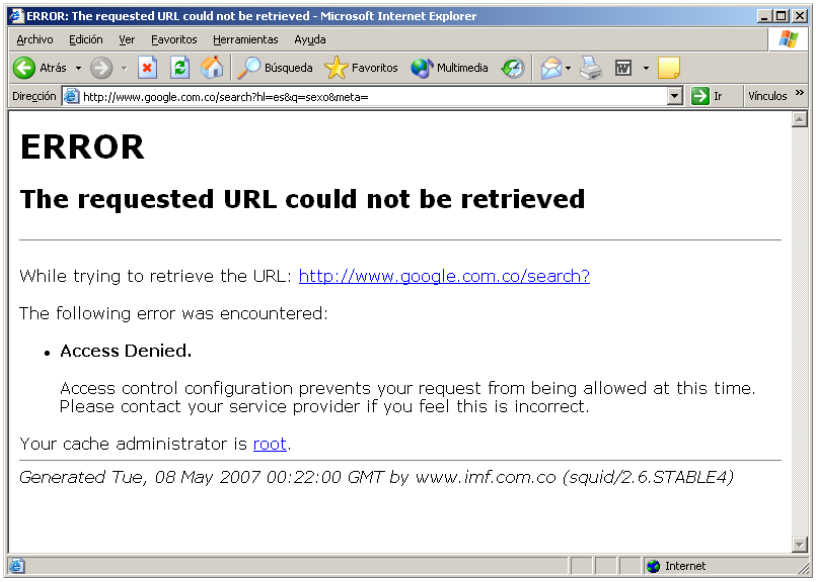
Figura 15. Mensaje servidor



Fuente: Autores del Proyecto

El mensaje que nos saca nuestro servidor proxy al usuario es el siguiente:

Figura 16. Regla urlpath_regex



Fuente: Autores del Proyecto

Regla Tipo urlpath_regex

Esta regla permite la administración de descargas por medio de las extensiones de los archivos.

acl [Nombre] urlpath_regex “Path”

acl extensiones urlpath_regex "/etc/squid/extensiones.txt"

A continuación tenemos el contenido de este archivo:

\.mp3$

\.mov$

\.bat$

\.exe$

\.sys$

\.com$

\.avi$

\.zip$
\.mpg$
\.pps$

Control de Acceso

El control de acceso define si se permite o deniega el acceso a las reglas para que empecemos a crear el filtrado.

http_access allow/Deny Regla

#en esta regla a continuación damos acceso al equipo donde está instalado el squid. Osea el equipo que llamamos local
http_access allow localhost

#en esta regla le damos acceso a la regla llamada mired2(a los equipos de las oficinas del colegio) en un horario de las 00:00 horas hasta las 12 del dia que es el horario configurado en la regla llamada **"mañana"**
Excepto las páginas restringidas y el messenger

http_access allow mañana mired2 !restringidosadmin !messenger

#en esta regla le estamos dando acceso a internet a los equipos de las oficinas en un horario de 12:00 hasta las 02:00 de la tarde que es la que tenemos definida en la regla llamada **"mediodía"** sin restricciones y con el Messenger funcionando.

Esta política está definida por la rectoría para que los empleados tengan un tiempo libre ya que es su hora de descanso y almuerzo.

http_access allow mediodia mired2

Aquí vuelve y se da internet de 02 de la tarde hasta las 4 restringiendo el messenger y las paginas prohibidas.

http_access allow tarde mired2 !restringidosadmin !messenger

En la siguiente regla damos acceso a internet en un horario de 4 pm hasta las 12 de la noche sin tener restricciones para los empleados.

http_access allow noche mired2

La siguiente regla es la que define el acceso a internet para todos los estudiantes con restricciones en las extensiones de los archives a descargar, en páginas, urls y en el Messenger.

La red de los estudiantes la hemos llamado “mired” y la red de la parte administrativa la hemos llamado “mired2”

http_access allow mired !extensiones !restringidos !messenger
(Da acceso a toda mired excepto a extensiones restringidos y al msn)

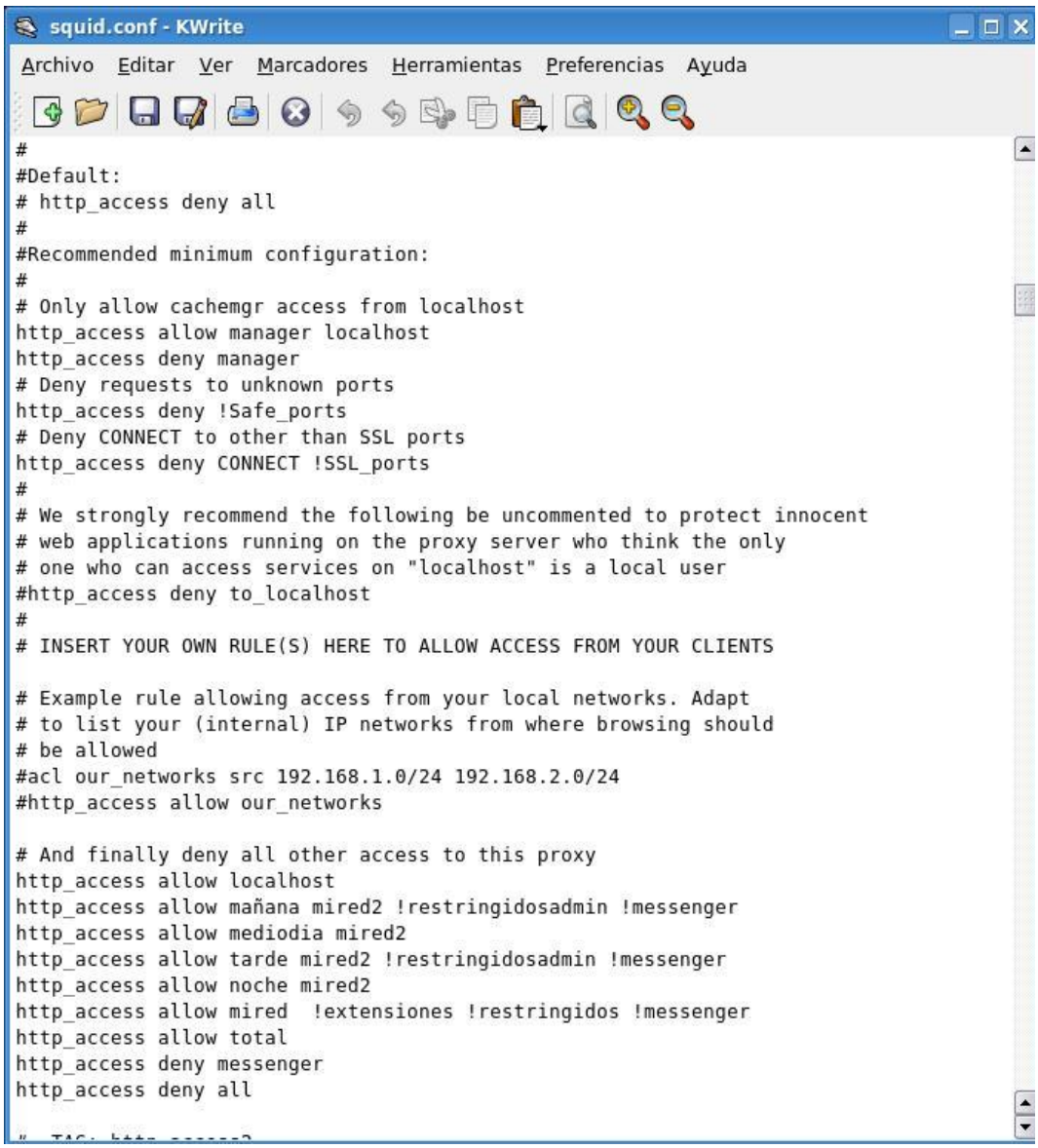
En esta regla le damos acceso total a una lista llamada “total.txt” con las ips de los jefes y administradores de la institución.

http_access allow total

Aquí denegamos el servicio para la regla llamada messenger

http_access deny messenger

Figura 17. access deny messenger



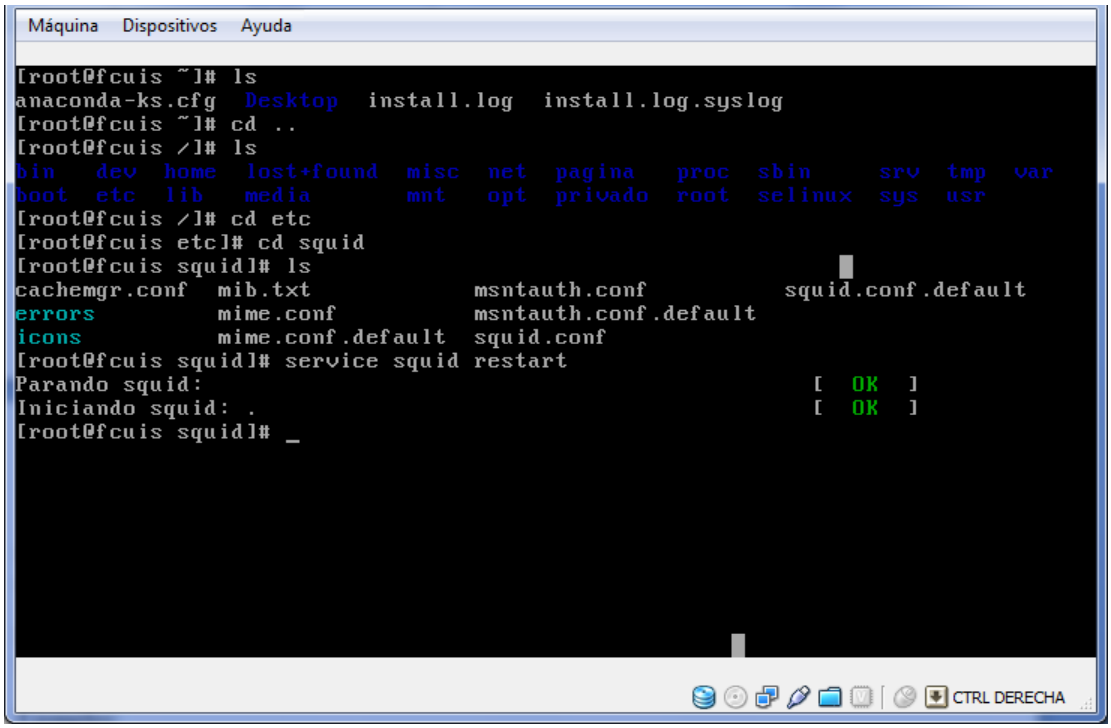
Fuente: Autores del Proyecto

Por último denegamos todo en la regla llamada all que definimos anteriormente con todas las direcciones de la web, excepto las direcciones anteriormente mencionadas con permisos para navegar.

http_access deny all

Ahora iniciamos el servicio de squid

Figura 18. squid



Fuente: Autores del Proyecto

Configuración de Navegadores Web.

Solo nos queda por configurar los browser o navegadores de nuestros clientes configuraremos la salida a internet por el proxy.

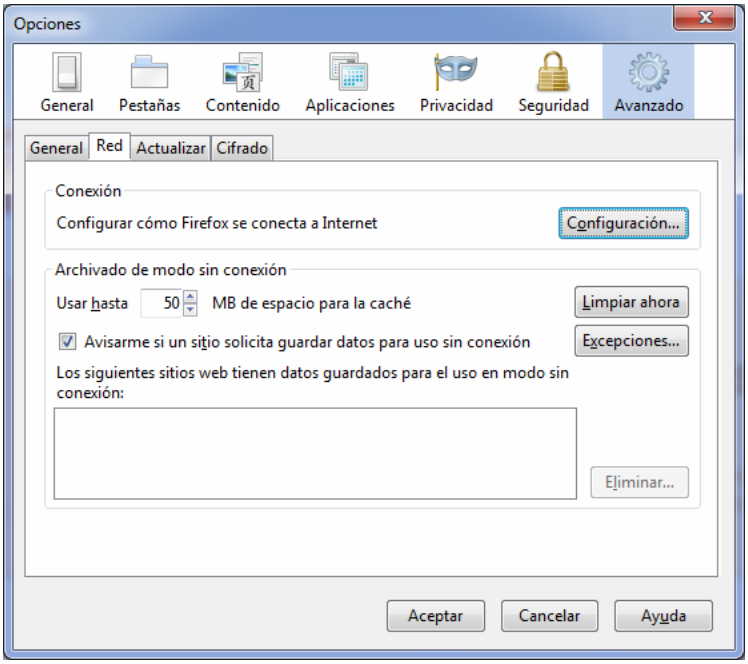
En la institución hemos configurado el servidor proxy con la dirección ip 192.168.1.100 y puerto 3128

Ejemplos:

- **Firefox**

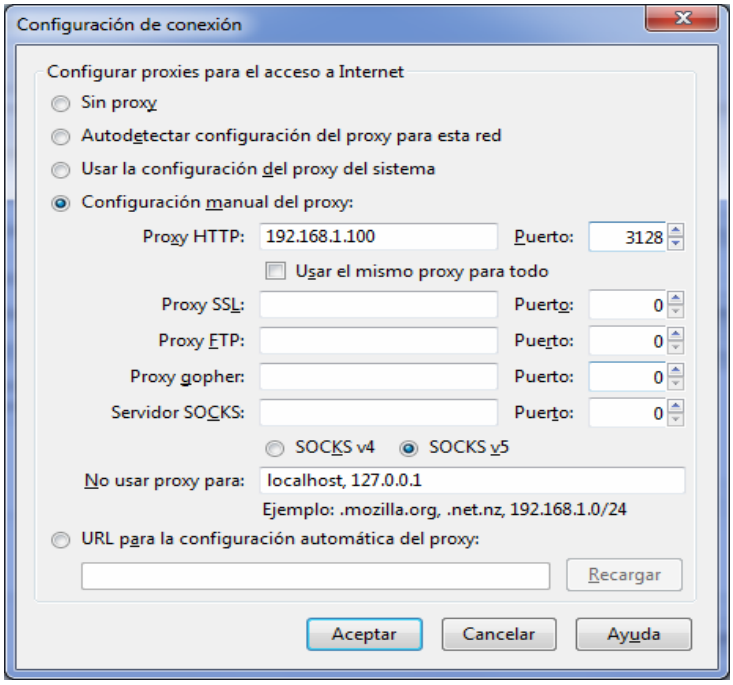
Menú Editar ---> Avanzadas ---> Red ---> Configuración de red.

Figura. 19. Firefox



Fuente: Autores del Proyecto

En la ventana de Avanzado escogemos la pestaña de Red, dentro de esta ventana escogemos la opción de configuración



Fuente: Autores del Proyecto

Aquí escogemos la opción de **configuración manual del proxy** y en la casilla de Proxy HTTP: digitamos nuestra dirección ip del servidor proxy, en nuestro caso la 192.168.1.100 con Puerto 3128 que es por donde escucha el Squid.

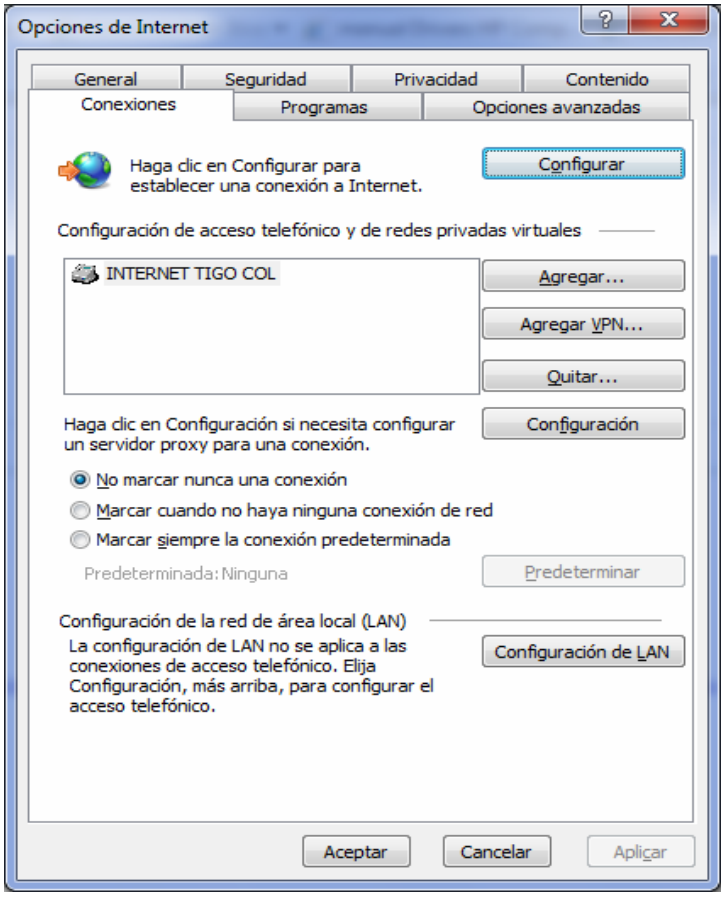
- **Opera.**

Menú Herramientas ---> Preferencias ---> Avanzadas ---> Red

- **Internet Explorer.**

Menú Herramientas ---> Opciones de Internet --->Conexiones ---> Configuración de LAN

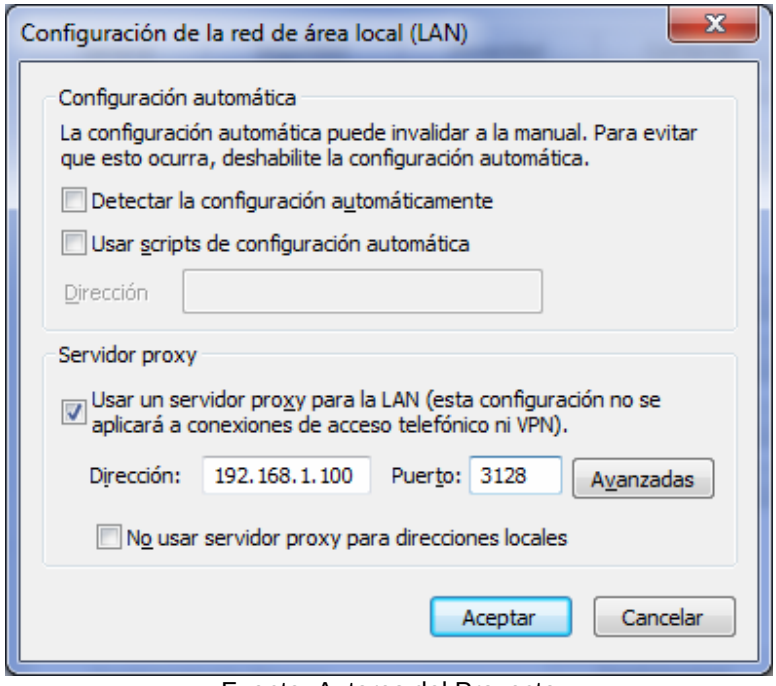
Figura 20. Configuración de LAN



Fuente: Autores del Proyecto

En esta ventana escogemos el botón de “configuración de Lan”, luego en la siguiente ventana escogemos la opción de “servidor proxy” y digitamos nuestra dirección ip del servidor proxy 192.168.1.100 y puerto 3128

Figura 21. Configuración LAN 2



Fuente: Autores del Proyecto

2.2.2. Configuración del Idioma de los Mensajes De Error

Ahora configuraremos los mensajes de error que sale en la pantalla del usuario

Asi es como esta la linea original

[root@fcuis squid]# ls -l
total 464
-rw-r----- 1 root squid 367 ago 16 2010 cachemgr.conf
lrwxrwxrwx 1 root root 20 ago 20 12:40 errors ->
/usr/share/squid/errors/English
Y se cambia a:
[root@fcuis squid]# **unlink errors**
[root@fcuis squid]# **ln -s /usr/share/squid/errors/Spanish errors**

```
[root@fcuis squid]# ls -l
total 404
-rw-r----- 1 root squid 419 sep 4 2010 cachemgr.conf
lrwxrwxrwx 1 root root 30 sep 7 14:40 errors ->
/usr/share/squid/errors/Spanish
lrwxrwxrwx 1 root root 22 sep 22 11:20 icons -> /usr/share/squid/icons
-rw-r--r-- 1 root root 27702 oct 12 2010 mib.txt
-rw-r--r-- 1 root root 11651 sep 12 2010 mime.conf
-rw-r--r-- 1 root root 11651 sep 12 2010 mime.conf.default
-rw-r--r-- 1 root root 421 sep 12 2010 msntauth.conf
-rw-r--r-- 1 root root 421 sep 12 2010 msntauth.conf.default
-rw-r----- 1 root squid 148027 sep 12 2010 squid.conf
-rw-r--r-- 1 root root 148027 sep 12 2010 squid.conf.default
```

3. CONFIGURACIÓN DEL FIREWALL DE LA RED

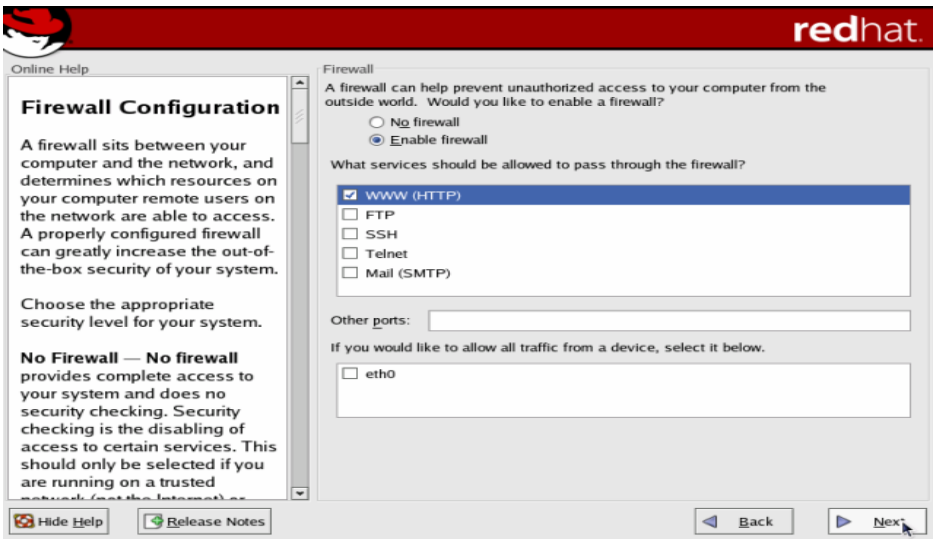
Para incrementar la seguridad en la red, debemos vincular el servicio a nuestra dirección IP del servidor, para que solo se pueda acceder desde la red local.

http_port 192.168.1.100:3128
http_port 192.168.1.100:8080

3.1. CONFIGURACIÓN DEL CORTAFUEGOS

La configuración del cortafuego es muy similar a la pantalla que nos sale cuando estamos instalando el Linux

Figura. 22. Corta Fuegos



Fuente: http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/5/pdf/Installation_Guide/Red_Hat_Enterprise_Linux-5-Installation_Guide-en-US.pdf

Si seleccionamos **Desactivar el cortafuego**, el servidor permitirá acceso completo a cualquier servicio y puertos activos.
La opción **Activar cortafuegos** instala el sistema para no permitir las conexiones entrantes que no sean en respuesta a peticiones salientes.
Si se necesita configurar los servicios que estamos ejecutando en el servidor, podemos seleccionar y permitir servicios específicos a través del cortafuego.

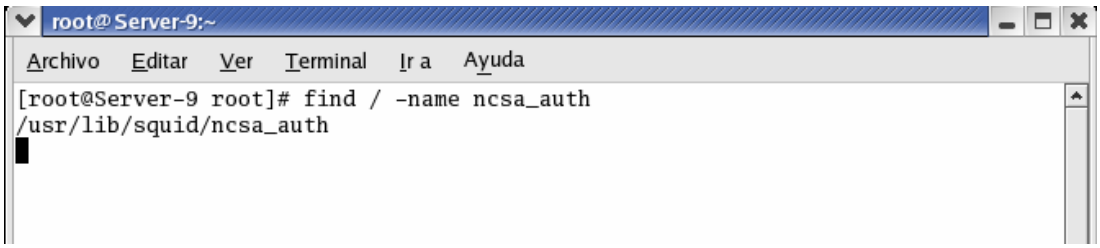
En la opción que dice **otros puertos** podremos agregar los puertos de nuestra confianza, ahí vamos agregar el puerto 3128 de nuestro squid, el cual se abre solo desde la red LAN hacia el servidor.
Para crear el directorio cache, en modo consola ejecutamos;
/usr/local/squid/sbin/squid -z
Una vez terminada la configuración, escribiremos el siguiente comando para iniciar por primera vez **Squid**:
service squid start
Para reiniciar y probar cambios hechos en la configuración, utilizamos lo siguiente:
service squid restart

3.2. CONFIGURACIÓN DE AUTENTICACIÓN DE USUARIOS CON SQUID SERVER

El siguiente paso para poder disfrutar de un Servidor Proxy Squid se debe realizar la configuración de la autenticación de usuarios. A continuación se realizarán cada uno de los pasos a seguir para llevar a cabo este paso, cabe recordar que es necesario hacer la instalación previa a este paso:
Para saber si existe autenticación NCSA en el servidor utilizamos el siguiente comando:

[root@localhost root]# find / -name ncsa_auth
/ usr/lib/squid/ncsa_auth

Figura 23. Configuración de autenticación squid.



Fuente: Autores del Proyecto

Entrando en la ruta del directorio me visualizan diferentes tipos de identificación:

[root@localhost root]# cd /usr/lib/squid

[root@localhost root]# ls

Cachemgr.cgi msnt_auth sal_auth squid_ldap_group wb_group diskd ncsa_auth

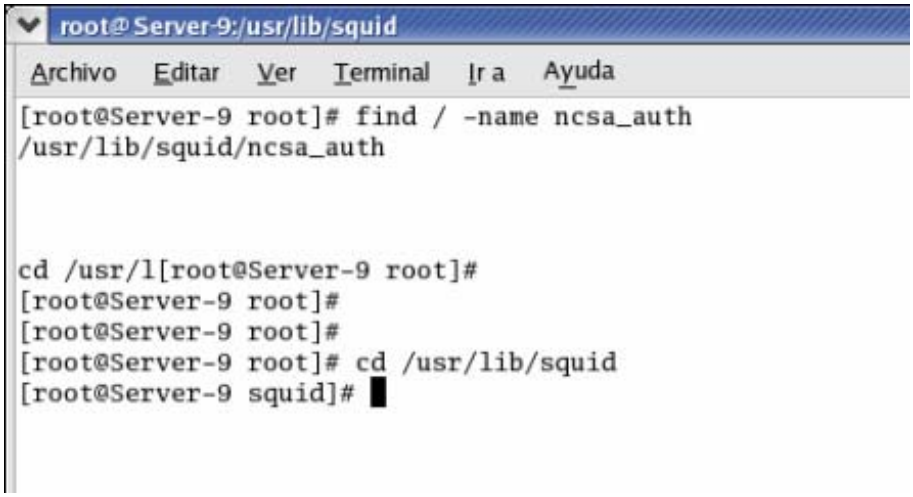
Smb_auth Squid_unix_group wbinfo_group.pl fakeauth_auth ntlm_auth smb_auth.sh

Unlinkd… (se omite).

[root@localhost squid]# cd /etc/squid

nano squid conf

Figura 24. Visualización de diferentes tipos de configuración.

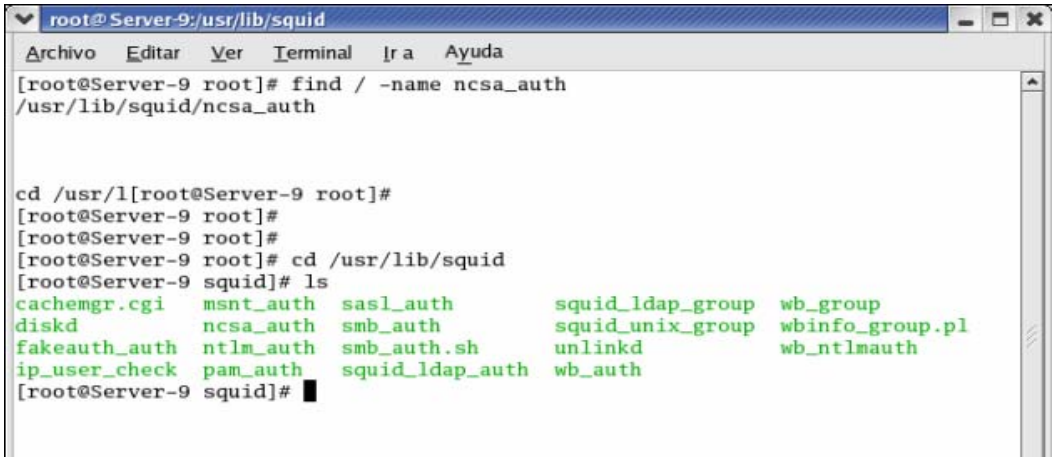


Fuente: Autores del Proyecto

Ahora edito el archivo configuración del squid con el siguiente parámetro, es decir busco la línea y la modifico o la agrego haciendo referencia al path donde se encuentra el demonio de autenticación.

auth_param basic program /usr/lib/squid/ncsa_auth /etc/squid/claves

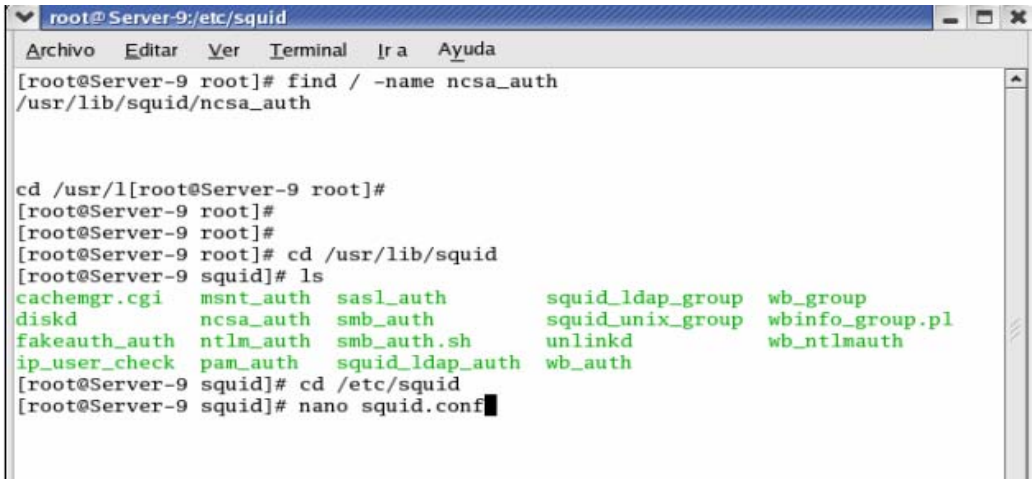
Figura 25. Edición de archivo configuración de squid



Fuente: Autores del Proyecto

Ahora en los parámetros de lista de control de acceso ACL se agrega una lista llamada password.
acl password Proxy_auth REQUIRED

Figura 26. Lista de control de acceso

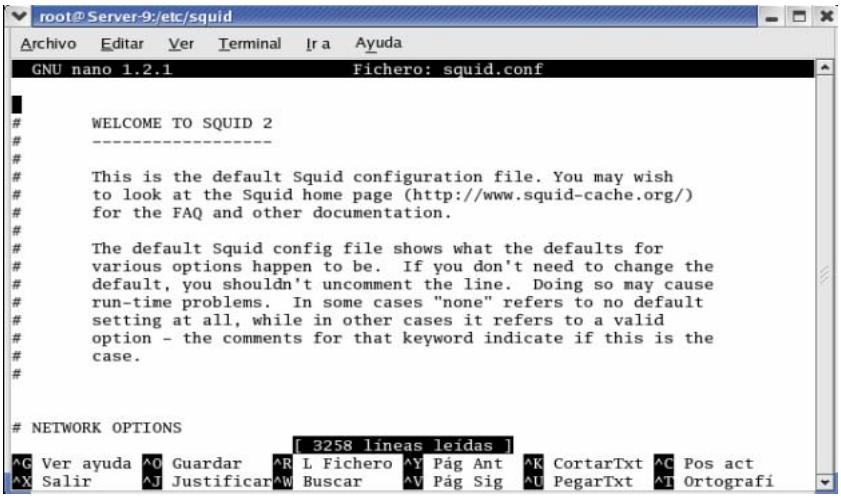


Fuente: Autores del Proyecto

Después se aplica la lista a la definida por usted en este caso sería a la lista llamada ALL.

http_access allow all password

Figura 27. Lista definida ALL.



Fuente: Autores del Proyecto

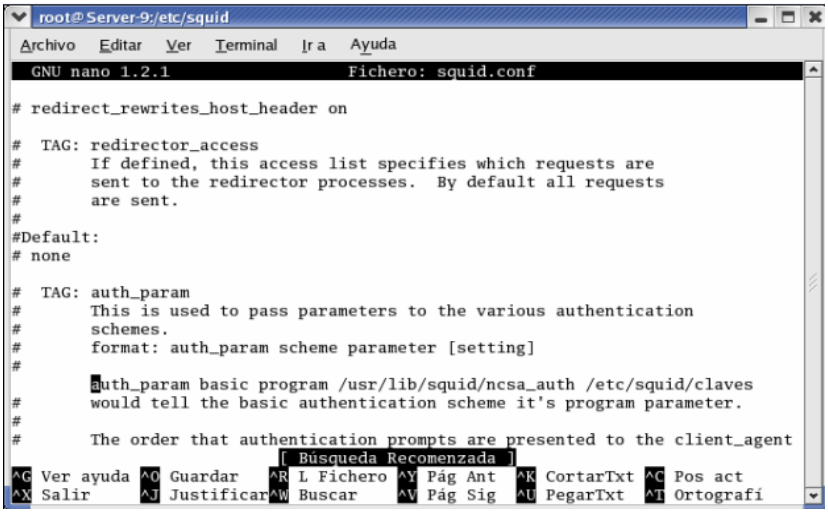
Ahora se crea un archivo llamado claves sobre /etc/suid/claves con el siguiente comando (este archivo claves no tiene contenido)

[root@localhost squid]# nano claves

CRTL+O para guardar (enter).

CTRL+X para salir (enter).

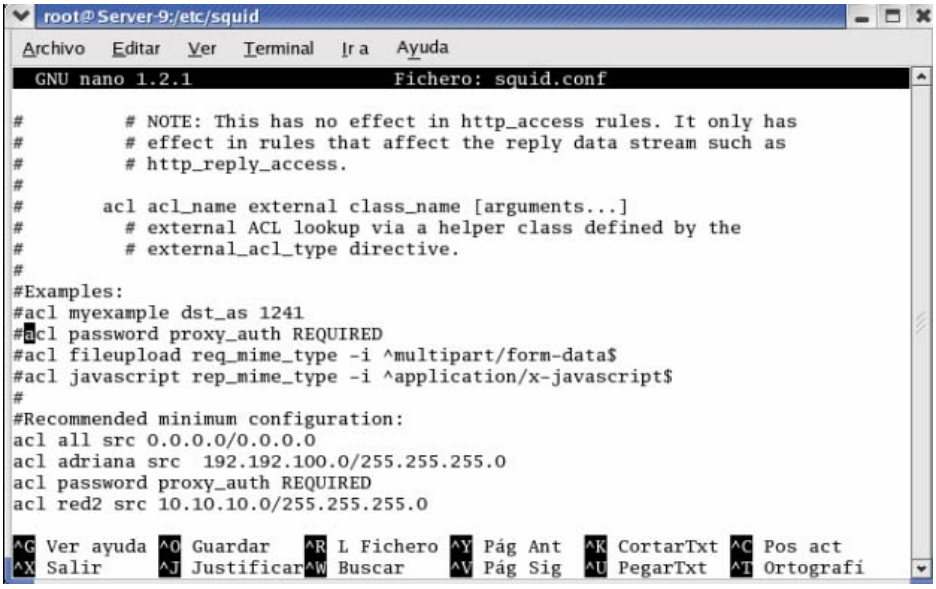
Figura 28. Crear archivo Claves.



Fuente: Autores del Proyecto

Ahora por último creamos los usuarios que van a hacer autenticados son el squid con el comando:
Htpasswd /etc/squid/claves beppo

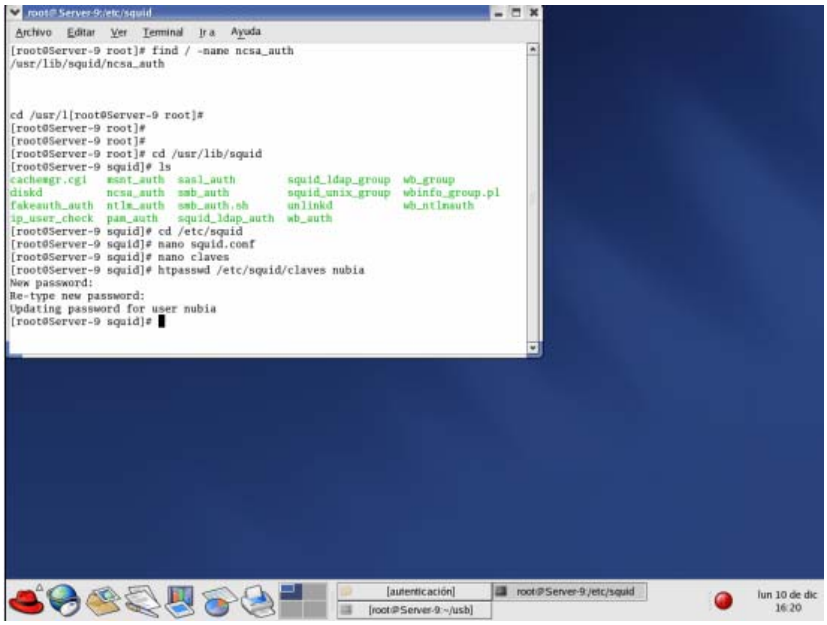
Figura 29. Usuarios Autenticados.



Fuente: Autores del Proyecto

Por último, puede observar los usuarios autenticados accediendo al servidor.

Figura 30. Finalización.



Fuente: Autores del Proyecto

3.3. HISTORIAL O LOGS DEL SERVIDOR PROXY SQUID

Cuando tenemos un servidor proxy squid instalado en nuestro servidor una de las tareas mas frecuentes del administrador es analizar los logs que este proxy nos da.

Una de las formas mas tradicionales es abrir el archivo llamado **access.log** desde consola con un editor de texto como el **VI**, pero también podemos utilizar varias herramientas que encontramos en internet para hacer este trabajo mas sencillo, una de estas es llamada Sarg(Squid Analisys Report Generator), es muy sencilla de utilizar y tiene varias configuraciones que podemos administrar a nuestra preferencia.

Para la instalación podremos descargar el archivo desde sarg.sourcefourge.net

Podemos descargar el paquete a usr/src

Luego lo descomprimimos con la siguiente instrucción:

#tar -xvzf sarg-2.2.3.1.tar.gz

Accedemos al directorio donde se ha descomprimido el archivo

#cd sarg-2.2.5

Una vez parados en el directorio ejecutamos lo siguiente en la consola

#./configure y compilamos el paquete con #make y #make install

Luego de instalado buscamos el archivo de sarg.conf que se debe encontrar en /etc/squid aquí podremos hacerle todas las configuraciones necesarias para nuestra buena administración de los logs.

Otro archivo de log muy utilizado tiene que ver con los errores de inicio del squid podremos ir a un archivo de configuración que nos muestra porque no arranca el squid. El archivo lo encontramos en /var/log/squid/squid.out, aquí nos muestra los errores y el numero de la línea donde el squid tuvo algún fallo, siendo muy practico y rápido llegar a encontrar el problema por el cual el servidor no arranco.

4. APAGADO AUTOMÁTICO DEL SERVIDOR PROXY

Se ha visto la necesidad de apagar el servidor automáticamente todos los días a las 8 de la noche, ya que a esa hora no hay nadie en la oficina de sistemas para apagar el equipo y dejarlo descansar hasta el otro día que se vuelve a encender. Pero también resulta el inconveniente que los viernes no se puede apagar porque el sábado no hay nadie en la oficina de sistemas para encenderlo, sino hasta el lunes en la mañana.

4.1. QUE ES CRON

Cron es un programa que permite a los usuarios de Linux ejecutar automáticamente comandos o grupos de comandos a una hora o fecha especifica como lo hace el Windows con su programador de tareas.

Usualmente para comandos de tareas administrativas como copias de seguridad, pero lo podremos utilizar para cualquier cosa.

4.2. INICIAR CRON

Cron es un servicio lo que quiere decir que solo necesitamos iniciarlo una vez, en nuestro servidor este servicio está instalado automáticamente
Ahora veremos los diferentes campos que conforman una instrucción del comando cron y algunos ejemplos para una mayor compresión.

Tabla 3. Iniciar CRON

Campo	Descripción
Minuto	El primer campo controla el minuto de la hora en que el comando será ejecutado, este valor debe de estar entre 0 y 59.
Hora	El segundo campo controla la hora en que el comando será ejecutado, tiene un formato de 24 horas, los valores deben estar entre 0 y 23, 0 es medianoche.
Día del Mes	El tercer campo es el Día del mes en que se quiere ejecutar el comando. Por ejemplo se indicaría 20, para ejecutar el comando el día 20 del mes.
Mes	El cuarto campo es el Mes en que el comando se ejecutará, puede ser indicado como (1-12), o por el nombre del mes en inglés, solo las tres primeras letras del mes
Día de la semana	El quinto campo es el Día en la semana en que se ejecutará el comando, puede ser (0-7) o por el nombre del día en inglés, solo las tres primeras letras. (0 = domingo)
Usuario	Es el Usuario que ejecuta el comando.
Comando	Es un Comando, script o programa que se desea ejecutar. Este campo puede contener varias palabras y espacios.
Ejemplo	**Descripción**
01 * * * *	Se ejecuta al minuto 1 de cada hora de todos los días
15 8 * * *	A las 8:15 a.m. de cada día
15 20 * * *	A las 8:15 p.m. de cada día
00 5 * * 0	A las 5 a.m. todos los domingos
* 5 * * Sun	Cada minuto de 5:00a.m. a 5:59a.m. todos los domingos
45 19 1 * *	A las 7:45 p.m. del primero de cada mes
01 * 20 7 *	Al minuto 1 de cada hora del 20 de julio
10 1 * 12 1	A la 1:10 a.m. todos los lunes de diciembre
00 12 16 * Wen	Al mediodía de los días 16 de cada mes y que sea Miércoles
30 9 20 7 4	A las 9:30 a.m. del día 20 de julio y que sea jueves
30 9 20 7 *	A las 9:30 a.m. del día 20 de julio sin importar el día de la semana
20 * * * 6	Al minuto 20 de cada hora de los sábados
20 * * 1 6	Al minuto 20 de cada hora de los sábados de enero

http://lindasantini.wordpress.com/2010/04/19/baseline-de-un-so-linux/

Entonces lo que tenemos que hacer es decirle al servidor que apague el computador automáticamente los días Domingo, lunes, martes, miércoles y jueves a las 8 de la noche, el viernes no, y el sábado tampoco, pero el domingo sí, ya que el lunes en la mañana lo podremos encerder temprano.

La instrucción sería la siguiente utilizando un cron o demonio (programa anteriormente mencionado) que posee el Linux.

Nos ubicamos en la consola de Linux como administradores o super usuarios **root**, luego digitamos crontab –e (este comando es para editar el crontab)

Debemos tener en cuenta que el editor predeterminado de Linux en consola es el **vi**, ahí nos aparecerá un archivo nuevo vacio, debemos teclear INSERT y escribir la siguiente línea
0 20 * * 4 shutdown -h now
Luego de escribir esta línea le oprimimos la tecla ESC para salir de la edición de texto, a continuación tecleamos: wq y enter. Así guardamos y salimos del editor.

Para consultar si la instrucción de crontab nos quedo bien podemos digitar en la consola **crontab –l** para que nos visualice lo que tiene el crontab programado, nos tiene que mostrar la misma línea que digitamos
0 20 * * 4 shutdown -h now (esta línea quiere decir que:

0 20 * * 4 shutdown –h now
- - - - -
| | | | |
| | | | +—— día de la semana (desde el Domingo hasta el Jueves) (Jueves=4)

| | | +——- mes(Todos los meses de Enero a Diciembre)
| | +——— día del mes (Todos los días del mes)
| +———— hora (20 hora militar = 8 pm)
+————-- minutos (0)

Esta tarea de apagar el computador (shutdown) solo se ejecutara cuando cumpla con los 5 campos, es decir que para que la tarea se ejecute tendrá que ser un día que sea de domingo a jueves y que sean las 8 de la noche.

5. CONCLUSIONES

Gracias al desarrollo de esta monografía y a la orientación del director del proyecto, logramos profundizar los conocimientos adquiridos en la especialización de Telecomunicaciones.

En el transcurso de la investigación aprendimos las diferentes herramientas que existen en el software de código libre para la implementación de políticas de seguridad en servidores proxy.

En el desarrollo de esta investigación logramos adquirir destrezas y habilidades en cuanto a la configuración de firewall en redes LAN.

La presente investigación se ha dedicado al estudio de las estrategias de controles de acceso a la información, por considerar que estas representan confiabilidad y estabilidad, para el bloqueo de amenazas e intrusiones en la red informática de la Fundación Colegio UIS.

En el desarrollo del trabajo de investigación que ha dado lugar a la presente monografía se han alcanzado los objetivos inicialmente planteados de seguridad informática y disponibilidad, debido a que con la aplicación Linux redhat Enterprise, se realiza captura de información en tiempo real para el control de gestión, se implementan políticas de acceso al contenido web para detectar factores limitantes, se supervisa el desempeño en la infraestructura de red, por lo cual se concluye que se mejoro la seguridad en la navegación y se incremento la velocidad.

En esta monografía se documento paso a paso el procedimiento realizado en la Fundación Colegio UIS, para la instalación de la herramienta Linux redhat Enterprise, la cual requiere mayor conocimiento para la configuración y capacitación para la administración.

BIBLIOGRAFÍA

- HERNÁNDEZ Sampieri, Roberto; Fernández Collado, Carlos; Batista Lucio, Pilar. Metodología de la Investigación. Mc Graw Hill. Segunda edición. México 2002

- Eyler, Pat. Redes Linux con TCP/IP: guía avanzada. Madrid: Prentice Hall, c2001

- Marsh, Matthew G. Encaminamiento regulado con Linux. Madrid: Prentice Hall, 2001

- Aguilar Sindes, Luis. Midiendo redes: análisis de tráfico y de protocolos para diagnóstico de problemas de calidad de servicios en redes de datos. Buenos Aires: Aguilar, 2002

- Montagnier, Jean-Luc e Amadeu Brugués. Administración Unix: System V y redes TCP/IP. Barcelona: Ediciones Gestión 2000, 1995

- SALINAS, J. (1999): “Uso educativo de las redes informáticas”. Revista EDUCAR, 25, pp. 81-92

- http://www2.linuxparatodos.net/web/comunidad/base-de-conocimiento/-/wiki/Base%20de%20Conocimiento/Servidor+Proxy

- http://docs.redhat.com/docs/es-ES/Red_Hat_Enterprise_Linux/5/pdf/Installation_Guide/Red_Hat_Enterprise_Linux-5-Installation_Guide-es-ES.pdf

- http://www.ibiblio.org/pub/linux/docs/LuCaS/Tutoriales/doc-servir-web-escuela/doc-servir-web-escuela-html/x518.html

- http://bulma.net/body.phtml?nIdNoticia=441

- http://www.alejandrox.com/2008/01/squid-y-las-listas-de-control-de-acceso-configuracion-basica-en-ubuntu/

- http://lindasantini.wordpress.com/2010/04/19/baseline-de-un-so-linux/