UNIVERSIDAD LUTERANA SALVADOREÑA

FACULTAD DE CIENCIAS DEL HOMBRE Y LA NATURALEZA

LICENCIATURA EN CIENCIAS DE LA COMPUTACIÓN

ASIGNATURA:

REDES I

TEMA:

“FILTRO WEB, USANDO EL SERVIDOR PROXY SQUID3”

DOCENTE:

ING. MANUEL FLORES VILLATORO

PRESENTADO POR:

CARNET	NOMBRE	PARTICIPACIÓN
AG01133314	EDENILSON ARISTIDEZ AYALA GUARDADO	100%
CH01133374	CRISTIAN ANTONIO CERÓN HENRÍQUEZ	100%
P01133622	ALEX MARVÍN PÉREZ	100%

SAN SALVADOR, 18 DE NOVIEMBRE DE 2017

Índice de contenido

Índice de tablas

Índice de ilustraciones

I. OBJETIVO GENERAL

Implementar un Filtro web, haciendo uso del servido proxy Squid3, para restringir el acceso de algunos sitios o páginas y a la vez comparar su funcionalidad con otros software similares.

II. OBJETIVOS ESPECÍFICOS

1. Configurar un filtro web, como proyecto de la materia de Redes 1, haciendo uso del servidor proxy Squid3.
2. Comparar documentalmente el funcionamiento de Squid 3, con otros servidores proxy o programas utilizados para filtrado de sitios web.
3. Comprender la instalación, configuración y funcionamiento de Squid3 en la implementación de un filtro web en una red LAN.

III. RESUMEN

Un filtro web, denominado normalmente "software de control de contenidos", es un tipo de software diseñado para restringir los sitios web que puede visitar un usuario en su ordenador. Estos filtros pueden utilizar una lista blanca o una lista negra: la lista blanca solo ofrece acceso a sitios seleccionados específicamente por la persona que configuró el filtro y la lista negra restringe el acceso a sitios no deseados determinados por los estándares instalados en el filtro.

Los filtros web también suelen utilizarse como herramienta de prevención contra malware, ya que bloquean el acceso a los sitios que alojan malware, como los sitios relacionados con pornografía o apuestas. Además, los filtros más avanzados pueden bloquear incluso la información que se envía a través de Internet para garantizar la privacidad de los datos confidenciales.

Para la implementación del proyecto de filtrado web se ha utilizado el Servidor Proxy Squid3, el cual es gratuito, de licencia libre y de código abierto; siendo muy conocido y utilizado en plataformas Linux, realizando su instalación y configuración en modo consola, pudiendo a través de un archivo externo, crear la lista de sitos que se desean restringir. Ver en Anexos, ***Ilustración 2: Instalación de squid3 en Debían.***

Al igual que Squid3, existen otros programas (libres o privativos), con los que se pueden implementar filtros web, por lo que se realizaron comparaciones para establecer similitudes o diferencias tanto cualitativas como cuantitativas; que puedan aportar información importante a tener en cuenta a la hora de realizar este tipo de proyectos ya se con fines didácticos, familiares o laborales.

Los software con los que se comparó Squid3, son los siguientes: Squid3, WEBlocker, WinGate 8.5.9 y Anti-Porn 20.7.4.25.

IV. PALABRAS CLAVES

Filtro web, Firewall, Servidor Proxy, Privacidad, Control, Instalación, Estándares, UNIX, Linux, Plataforma, URL, ISP, Software de control de contenidos, tráfico web.

V. INTRODUCCIÓN

El presente trabajo esta enfocado en un Servidor Proxy y es dar a conocer su función principal el cual es filtrar contenido web, es decir restringir ciertas páginas o sitios, configuradas previamente por el administrador para que el cliente no pueda ingresar. Lo que significa que se encarga de interceptar los datos de navegación interponiéndose entre un cliente que hace una petición y el servidor que deberá resolver. Teniéndose como principales razones para usar un filtro web: la seguridad, el rendimiento, anonimato, entre otros.

El proyecto se configura por medio de Squid3, que es un software para servidor Proxy muy popular y extendido entre los sistemas operativos basados sobre UNIX y otros. Es muy confiable, robusto y versátil. Al ser software libre, además de estar disponible el código fuente, está libre del pago de costosas licencias por uso ó con restricción a un uso con determinado número de usuarios.

Además se muestran comparaciones tanto cualitativas, como cuantitativas con otros software que pueden realizar la misma función, con el fin de establecer diferencias y semejanzas que puedan aportar un mejor conocimiento a la hora de elegir implementar un filtro web.

VI. MARCO TEÓRICO

1. Filtro web:

Un filtro web, denominado normalmente "software de control de contenidos", es un tipo de software diseñado para restringir los sitios web que puede visitar un usuario en su ordenador. Estos filtros pueden utilizar una lista blanca o una lista negra: la lista blanca solo ofrece acceso a sitios seleccionados específicamente por la persona que configuró el filtro y la lista negra restringe el acceso a sitios no deseados determinados por los estándares instalados en el filtro. Estos programas buscan en la URL y en el contenido del sitio en cuestión las palabras clave restringidas para, a continuación, bloquear o permitir la conexión. Los filtros se suelen instalar como una extensión del navegador, como un programa independiente en el ordenador o como parte de la solución general de seguridad. No obstante, también se pueden instalar en la red con la ayuda de una empresa o proveedor de servicios de Internet (ISP) con el fin de restringir el acceso simultáneo a Internet por parte de varios usuarios. Algunos motores de búsqueda disponen también de filtros rudimentarios que eliminan las páginas no deseadas de los resultados de búsqueda.

2. Software de filtrado:

El software de filtrado web tiene cuenta con dos tipos de cliente principales: padres que quieren evitar que sus hijos accedan a contenido inadecuado y empresas que desean impedir que sus empleados accedan a sitios web no relacionados con la actividad laboral. Los filtros web también suelen utilizarse como herramienta de prevención contra malware, ya que bloquean el acceso a los sitios que alojan malware, como los sitios relacionados con pornografía o apuestas. Además, los filtros más avanzados pueden bloquear incluso la información que se envía a través de Internet para garantizar la privacidad de los datos confidenciales.

Hay algunos aspectos que escapan al control del software de filtrado web como, por ejemplo, el uso de un proxy basado en la Web, el acceso de sitios web en otro idioma o la creación de una VPN para un servidor proxy personal. Debido a estas carencias, los administradores de red o los padres preocupados por la seguridad de sus hijos deben asegurarse de que el filtro que elijan sea capaz de hacer mucho más que simplemente bloquear o permitir el acceso a determinados sitios web.

3. Proxy:

Un proxy, o servidor proxy, en una red informática, es un servidor (un programa o sistema informático), que hace de intermediario en las peticiones de recursos que realiza un cliente (A) a otro servidor (C). Por ejemplo, si una hipotética máquina A solicita un recurso a C, lo hará mediante una petición a B, que a su vez trasladará la petición a C; de esta forma C no sabrá que la petición procedió originalmente de A. Esta situación estratégica de punto intermedio suele ser aprovechada para soportar una serie de funcionalidades: control de acceso, registro del tráfico, prohibir cierto tipo de tráfico, mejorar el rendimiento, mantener el anonimato, proporcionar Caché web, etc; este último sirve para acelerar y mejorar la experiencia del usuario mediante permisos que guardará la web, esto se debe a que la próxima vez que se visiten las páginas web no se extraerá información de la web si no que se recuperara información de la caché.

4. Características:

La palabra inglesa proxy significa: ***procurador en español***.

El uso más común es el de servidor proxy, que es un ordenador que intercepta las conexiones de red que un cliente hace a un servidor de destino.

De ellos, el más famoso es el servidor proxy web (comúnmente conocido solamente como «proxy»). Intercepta la navegación de los clientes por páginas web, según la configuración previa.

También existen proxy para otros protocolos, como el proxy de FTP.

El proxy ARP puede hacer de enrutador en una red, ya que hace de intermediario entre ordenadores.

Proxy (patrón de diseño) también es un patrón de diseño (programación) con el mismo esquema que el proxy de red.

Un componente hardware también puede actuar como intermediario para otros.

Como se ve, proxy tiene un significado muy general, aunque siempre es sinónimo de intermediario. Cuando un equipo de la red desea acceder a una información o recurso, es realmente el proxy quien realiza la comunicación y a continuación traslada el resultado al

equipo que la solicitó.

Hay dos tipos de proxys dependiendo quien es el que quiere implementar la política:

1. **Proxy local:** En este caso el que quiere implementar la política es el mismo que hace la petición. Por eso se le llama local. Suelen estar en la misma máquina que el cliente que hace las peticiones. Son muy usados para que el cliente pueda controlar el tráfico y pueda establecer reglas de filtrado que por ejemplo pueden asegurar que no se revela información privada (Proxys de filtrado para mejora de la privacidad).
2. **proxy externo:** El que quiere implementar la política del proxy es una entidad externa. Por eso se le llama externo. Se suelen usar para implementar cacheos, bloquear contenidos, control del tráfico, compartir IP, etc.

5. Ventajas:

Los proxys hacen posible:

Control: Sólo el intermediario hace el trabajo real, por tanto se pueden limitar y restringir los derechos de los usuarios, y dar permisos sólo al proxy.

Ahorro: Sólo uno de los usuarios (el proxy) ha de estar preparado para hacer el trabajo real. Con estar preparado queremos decir que es el único que necesita los recursos necesarios para hacer esa funcionalidad. Ejemplos de recursos necesarios para hacer la función pueden ser la capacidad y lógica de cómputo o la dirección de red externa (IP).

Velocidad: Si varios clientes van a pedir el mismo recurso, el proxy puede hacer caché: guardar la respuesta de una petición para darla directamente cuando otro usuario la pida. Así no tiene que volver a contactar con el destino, y acaba más rápido.

Filtrado: El proxy puede negarse a responder algunas peticiones si detecta que están prohibidas.

Modificación: Como intermediario que es, un proxy puede falsificar información, o modificarla siguiendo un algoritmo.

6. Desventajas:

El uso de un intermediario puede provocar:

Anonimato: Si todos los usuarios se identifican como uno sólo, es difícil que el recurso accedido pueda diferenciarlos. Pero esto puede ser malo, por ejemplo cuando hay que hacer necesariamente la identificación.

Abuso: Al estar dispuesto a recibir peticiones de muchos usuarios y responderlas, es posible que haga algún trabajo que no toque. Por tanto, ha de controlar quién tiene acceso y quién no a sus servicios, cosa que normalmente es muy difícil.

Carga: Un proxy ha de hacer el trabajo de muchos usuarios.

Intromisión: Es un paso más entre origen y destino, y algunos usuarios pueden no querer pasar por el proxy. Y menos si hace de caché y guarda copias de los datos.

Incoherencia: Si hace de caché, es posible que se equivoque y dé una respuesta antigua cuando hay una más reciente en el recurso de destino. En realidad este problema no existe con los servidores proxy actuales, ya que se conectan con el servidor remoto para comprobar que la versión que tiene en caché sigue siendo la misma que la existente en el servidor remoto.

Irregularidad: El hecho de que el proxy represente a más de un usuario da problemas en muchos escenarios, en concreto los que presuponen una comunicación directa entre 1 emisor y 1 receptor (como TCP/IP).

Aplicaciones:

El concepto de proxy es aplicado de muy distintas formas para proporcionar funcionalidades específicas.

Proxy Caché:

Conserva el contenido solicitado por el usuario para acelerar la respuesta en futuras peticiones de la misma información de la misma máquina u otras. Habitualmente se trata de proxys HTTP/HTTPS accediendo a contenido web.

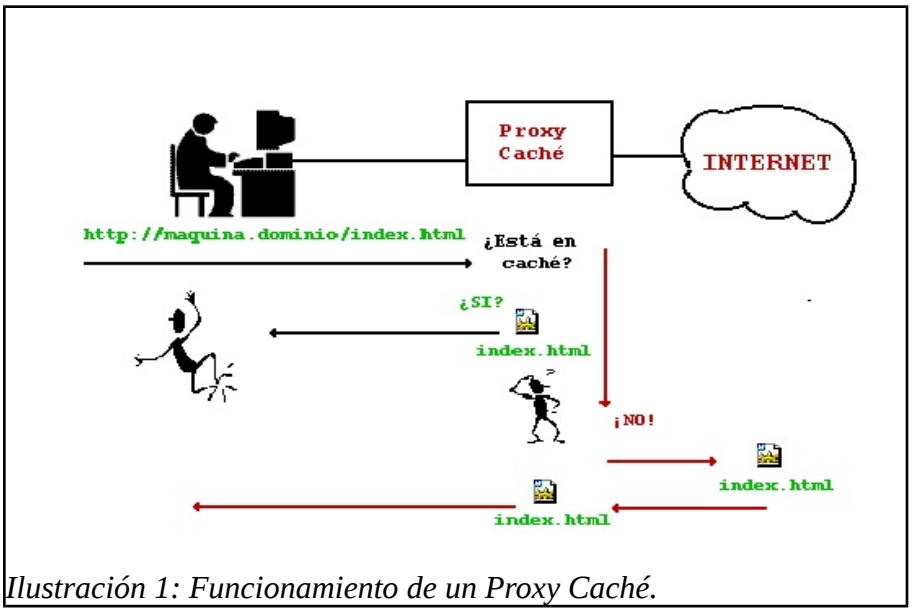

Ilustración 1: Funcionamiento de un Proxy Caché.

Proxy de Web:

Se trata de un proxy para una aplicación específica: el acceso a la web con los protocolos HTTP y HTTPS, y accesoriamente FTP. Aparte de la utilidad general de un proxy puede proporcionar una caché compartida para las páginas web y contenidos descargados, actuando entonces como servidor proxy-cache. Esta caché es compartida por múltiples usuarios con la consiguiente mejora en los tiempos de acceso para consultas coincidentes y liberando de carga a los enlaces de acceso a Internet.

7. Funcionamiento:

El usuario realiza una petición (por ejemplo, en un navegador web) de un recurso de Internet (una página web o cualquier otro archivo) especificado por una URL.

Cuando el proxy caché recibe la petición, busca la URL resultante en su caché local. Si la encuentra, contrasta la fecha y hora de la versión de la página demanda con el servidor remoto. Si la página no ha cambiado desde que se cargo en caché la devuelve inmediatamente, ahorrándose mucho tráfico dado que solo envía un paquete por la red para comprobar la versión. Si la versión es antigua o simplemente no se encuentra en la caché, lo solicita al servidor remoto, lo devuelve al cliente que lo pidió y guarda o actualiza una copia en su caché para futuras peticiones. Ver ***Ilustración1: Funcionamiento de un Proxy Caché.***

Posibles usos: Los proxys web pueden aportar una serie de funcionalidades interesantes en distintos ámbitos:

Reducción del tráfico mediante la implementación de caché en el proxy. Las peticiones de páginas Web se hacen al servidor Proxy y no a Internet directamente. Por lo tanto se aligera el tráfico en la red y descarga los servidores destino, a los que llegan menos peticiones.

El caché utiliza normalmente un algoritmo configurable para determinar cuándo un documento está obsoleto y debe ser eliminado de la caché. Como parámetros de configuración utiliza la antigüedad, tamaño e histórico de acceso. Dos de esos algoritmos básicos son el LRU (el usado menos recientemente, en inglés "Least Recently Used") y el LFU (el usado menos frecuentemente, "Least Frequently Used").

Mejora de la velocidad en tiempo de respuesta mediante la implementación de caché en el proxy. El servidor Proxy crea un caché que evita transferencias idénticas de la información entre servidores durante un tiempo (configurado por el administrador) así que el usuario recibe una respuesta más rápida. Por ejemplo supongamos que tenemos un ISP que tiene un servidor Proxy con caché. Si un cliente de ese ISP manda una petición por ejemplo a Google esta llegará al servidor Proxy que tiene este ISP y no irá directamente a la dirección IP del dominio de Google. Esta página concreta suele ser muy solicitada por un alto porcentaje de usuarios, por lo tanto el ISP la retiene en su Proxy por un cierto tiempo y crea una respuesta en mucho menor tiempo. Cuando el usuario crea una búsqueda en Google el servidor Proxy ya no es utilizado; el ISP envía su petición y el cliente recibe su respuesta ahora sí desde Google.

El proxy puede servir para implementar funciones de filtrado de contenidos. Para ello es necesaria la configuración de una serie de restricciones que indiquen lo que no se permite. Observar que esta funcionalidad puede ser aprovechada no sólo para que ciertos usuarios no accedan a ciertos contenidos sino también para filtrar ciertos ficheros que se pueden considerar como peligrosos como pueden ser virus y otros contenidos hostiles servidos por servidores web remotos.

Un proxy puede permitir esconder al servidor web la identidad del que solicita cierto contenido. El servidor web lo único que detecta es que la ip del proxy solicita cierto contenido. Sin embargo no puede determinar la ip origen de la petición. Además, si se usa una caché, puede darse el caso de que el contenido sea accedido muchas más veces que

las detectadas por el servidor web que aloja ese contenido.

Los proxys pueden ser aprovechados para dar un servicio web a una demanda de usuarios superior a la que sería posible sin ellos.

El servidor proxy puede modificar los contenidos que sirven los servidores web originales. Puede haber diferentes motivaciones para hacer esto. Veamos algunos ejemplos:

Algunos proxys pueden cambiar el formato de las páginas web para un propósito o una audiencia específica (Ej. mostrar una página en un teléfono móvil o una PDA) traduciendo los contenidos.

Hay proxys que modifican el tráfico web para mejorar la privacidad del tráfico web con el servidor. Para ello se establecen unas reglas que el proxy tiene que cumplir. Por ejemplo el proxy puede ser configurado para bloquear direcciones y Cookies, para modificar cabeceras de las peticiones o quitar javascript que se considere peligroso.

Es frecuente el uso de este tipo de proxys en las propias máquinas de los usuarios (proxys locales) para implementar un paso intermedio y que las peticiones no sean liberadas/recibidas a/de la red sin haber sido previamente limpiadas de información o contenido peligroso o privado. Este tipo de proxys es típico en entornos donde hay mucha preocupación sobre la privacidad y se suele usar como paso previo a la petición del contenido a través de una red que persiga el anonimato como puede ser Tor. Los programas más frecuentes para hacer este tipo de funcionalidad son:

Privoxy: Se centra en el contenido web. No presta servicio de cache. Analiza el tráfico basándose en reglas predefinidas que se asocian a direcciones especificadas con expresiones regulares y que aplica a cabeceras, contenido, etc. Es altamente configurable. Tiene extensa documentación.

Polipo: Tiene características que lo hacen más rápido que privoxy (cacheo, pipeline, uso inteligente de rango de peticiones). Su desventaja es que no viene configurado por defecto para proveer anonimicidad a nivel de la capa de aplicación.

El servidor proxy proporciona un punto desde el que se puede gestionar de forma centralizada el tráfico web de muchos usuarios. Eso puede aprovecharse para muchas funciones adicionales a las típicas vistas anteriormente. Por ejemplo puede usarse para el establecimiento de controlar el tráfico de web de individuos concretos, establecer cómo se va

a llegar a los servidores web de los cuales se quiere obtener los contenidos (por ejemplo, el proxy puede configurarse para que en lugar de obtener los contenidos directamente, lo haga a través de la red Tor).

Inconvenientes:

Si se realiza un servicio de caché, las páginas mostradas pueden no estar actualizadas si éstas han sido modificadas desde la última carga que realizó el proxy caché.

Un diseñador de páginas web puede indicar en el contenido de su web que los navegadores no hagan una caché de sus páginas, pero este método no funciona habitualmente para un proxy.

El hecho de acceder a Internet a través de un Proxy, en vez de mediante conexión directa, dificulta (necesario configurar adecuadamente el proxy) realizar operaciones avanzadas a través de algunos puertos o protocolos.

Almacenar las páginas y objetos que los usuarios solicitan puede suponer una violación de la intimidad para algunas personas.

8. Aplicaciones Web Proxy :

Su funcionamiento se basa en el de un proxy HTTP/HTTPS, pero en este caso el usuario accede desde el navegador web a este servicio de forma manual a través una Aplicación Web. Ese servidor HTTP, el intermediario, mediante una URL recibe la petición, accede al servidor de la web solicitada y devuelve el contenido dentro una página propia.

Proxy SOCKS

Los servidores SOCKS se diferencian de otros proxys por utilizar en vez de HTTP un protocolo específico, el protocolo SOCKS. El programa cliente es a la vez cliente HTTP y cliente SOCKS. El cliente negocia una conexión con el servidor proxy SOCKS usando el protocolo SOCKS de nivel 5, capa de sesión, del modelo OSI. Una vez establecida la conexión todas la comunicaciones entre el cliente y proxy se realizan usando el protocolo SOCKS. El cliente le dice al proxy SOCKS qué es lo que quiere y el proxy se comunica con el servidor web externo, obtiene los resultados y se los manda al cliente. De esta forma el servidor externo solo tiene que estar accesible desde el proxy SOCKS que es el que se va a comunicar con él.

El cliente que se comunica con SOCKS puede estar en la propia aplicación (Ej. Firefox, putty), o bien en la pila de protocolos TCP/IP a donde la aplicación enviará los paquetes a un túnel SOCKS. En el proxy SOCKS es habitual implementar, como en la mayoría de proxys, autenticación y registro de las sesiones.

En los orígenes de la web fue un protocolo de acceso a web popular, pero el rápido desarrollo de los proxies HTTP o incluso de NAT y otras opciones de aseguramiento de las comunicaciones TCP/IP lo hizo caer en desuso prácticamente absoluto llegado el siglo XXI.

Proxys transparentes

Muchas organizaciones (incluyendo empresas, colegios y familias) usan los proxies para reforzar las políticas de uso de la red o para proporcionar seguridad y servicios de caché. Normalmente, un proxy Web o NAT no es transparente a la aplicación cliente: debe ser configurada para usar el proxy, manualmente. Por lo tanto, el usuario puede evadir el proxy cambiando simplemente la configuración.

Un proxy transparente combina un servidor proxy con un cortafuegos de manera que las conexiones son interceptadas y desviadas hacia el proxy sin necesidad de configuración en el cliente, y habitualmente sin que el propio usuario conozca de su existencia. Este tipo de proxy es habitualmente utilizado por las empresas proveedoras de acceso de Internet.

Proxy inverso (Reverse Proxy) .

Un proxy inverso (reverse proxy en inglés) es un servidor proxy situado en el alojamiento de uno o más servidores web. Todo el tráfico procedente de Internet y con destino en alguno de esos servidores web es recibido por el servidor proxy.

Hay varias razones para ello:

a) **Seguridad:** el servidor proxy es una capa adicional de defensa y por lo tanto protege a los servidores web.

b) **Cifrado / Aceleración SSL**: cuando se crea un sitio web seguro, habitualmente el cifrado SSL no lo hace el mismo servidor web, sino que es realizado en un equipo ajeno equipado incluso con hardware de aceleración SSL/TLS.

c) **Distribución de Carga:** el proxy puede distribuir la carga entre varios servidores web. En ese caso puede ser necesario reescribir la URL de cada página web (traducción de

la URL externa a la URL interna correspondiente, según en qué servidor se encuentre la información solicitada).

d) **Caché de contenido estático**: Un proxy inverso puede descargar de trabajo a los servidores web, almacenando contenido estático como imágenes u otro contenido gráfico. También puede almacenar contenido generado dinámicamente pero que pueda ser en alguna medida reutilizable.

Proxy NAT (Network Address Translation) / Enmascaramiento

Otro mecanismo para hacer de intermediario en una red es el NAT (NAT, Network Address Translation) también es conocida como enmascaramiento de IPs. Es una técnica mediante la cual las direcciones fuente o destino de los paquetes IP son reescritas, sustituidas por otras (de ahí el "enmascaramiento").

Esto es lo que ocurre cuando varios usuarios comparten una única conexión a Internet. Se dispone de una única dirección IP pública, que tiene que ser compartida. Dentro de la red de área local (LAN) los equipos emplean direcciones IP reservadas para uso privado y será el proxy el encargado de traducir las direcciones privadas a esa única dirección pública para realizar las peticiones, así como de distribuir las páginas recibidas a aquel usuario interno que la solicitó. Estas direcciones privadas se suelen elegir en rangos prohibidos para su uso en Internet como 192.168.x.x, 10.x.x.x, 172.16.x.x y 172.31.x.x.

Esta situación es muy común en empresas y domicilios con varios ordenadores en red y un acceso externo a Internet. El acceso a Internet mediante NAT proporciona una cierta seguridad, puesto que en realidad no hay conexión directa entre el exterior y la red privada, y así nuestros equipos no están expuestos a ataques directos desde el exterior.

Mediante NAT también se puede permitir un acceso limitado desde el exterior, y hacer que las peticiones que llegan al proxy sean dirigidas a una máquina concreta que haya sido determinada para tal fin en el propio proxy.

La función de NAT reside en los Cortafuegos y resulta muy cómoda porque no necesita de ninguna configuración especial en los equipos de la red privada que pueden acceder a través de él como si fuera un mero encaminador.

Proxy abierto

Este tipo de proxy es el que acepta peticiones desde cualquier ordenador, esté o no conectado a su red.

En esta configuración el proxy ejecutará cualquier petición de cualquier ordenador que pueda conectarse a él, realizándola como si fuera una petición del proxy. Por lo que permite que este tipo de proxy se use como pasarela para el envío masivo de correos de spam. Un proxy se usa, normalmente, para almacenar y redirigir servicios como el DNS o la navegación Web, mediante el cacheo de peticiones en el servidor proxy, lo que mejora la velocidad general de los usuarios. Este uso es muy beneficioso, pero al aplicarle una configuración "abierta" a todo internet, se convierte en una herramienta para su uso indebido. Debido a lo anterior, muchos servidores, como los de IRC, o correo electrónicos, deniegan el acceso a estos proxys a sus servicios, usando normalmente listas negras ("BlackList").

VII. MATERIALES Y MÉTODOS (METODOLOGÍA)

Materiales a utilizar :

1. Tres computadoras.
2. Un switch.
3. Sistema Operativo GNU/Linux (Ubuntu y Debian).
4. Servidor Proxy (Squid3, WEBlocker, WinGate y Antiporn).
5. 3 cables de red (UTP).

Metodología:

La instalación y configuración de squid3 será realizada a través de la terminal de Linux, modificando el archivo “**squid.conf”,** en el cual colocamos nuestras propias reglas, que posteriormente seguirá squid. Ver ***Ilustración 3: configuración de Squid3.*** Podemos crear un archivo externo para listar las URL, direcciones IP de los sitios o páginas web que se desean bloquear. En nuestro proyecto utilizamos una computadora que realizará la función de servidor y una o más que serán funcionarán como clientes; conectándose por medio de un Switch.

Para comparar squid3 con los demás proxys, nos basamos en el tipo de licencia que utilizan,

el almacenamiento en el disco duro, el costo económico que tiene y otros aspectos importante. Ver **Tabla 3 : Comparación de Squid3 con otros Software Similares.**

El costo del proyecto se detalla en la siguiente tabla:

Costos por recursos materiales				
N	**Concepto**	**Cantidad**	**Precio**	**Total**
1	Alimentación	9	$2,00	$18,00
2	Paquetes de Internet	7	$1,60	$11,20
3	Cables UTP	4	$1,50	$6,00
4	Transporte	10	$0,20	$2,00
5	Horas de energía eléctrica	5	$0,25	$1,25
6	Switch	1	$30,00	$30,00
7	Computadora(para servidor)	1	$700,00	$700,00
Total 1				$768,45
Costos por recursos humanos				
N	**Concepto**	**Horas/Trab.**	**Precio/Hora**	**Total**
1	programador	12	$5,00	$60,00
2	programador	12	$5,00	$60,00
3	programador	12	$5,00	$60,00
Total 2				$180,00
Imprevistos				
Derivado del costo total del proyecto (10%)			Total 3	$94,85
Costo Total del proyecto				$1.043,30

Tabla 1: Costos del proyecto

VIII. RESULTADOS

1. Squid3 (software utilizado en proyecto)

Para el proyecto de filtro web, que como grupo realizaremos, se ha tomado en cuenta a Squid versión 3, el cual se describe a continuación:

Squid es una aplicación de servidor de caché de proxy web completa que proporciona servicios de proxy y caché para el protocolo de transporte de hipertexto (HTTP), protocolo de transferencia de archivos (FTP) y otros protocolos de red populares. Ver ***Ilustración 5: Funcionamiento del Proxy Squid.***

Squid puede implementar el almacenamiento en caché y el proxy de las solicitudes de Secure Sockets Layer (SSL) y el almacenamiento en caché de las búsquedas DNS (Domain Name Server), y realizar el almacenamiento en caché transparente. Squid también admite una gran variedad de protocolos de almacenamiento en caché, como el Protocolo de caché

de Internet (ICP), el Protocolo de caché de texto hipertexto (HTCP), el Protocolo de enrutamiento de array de caché (CARP) y el Protocolo de coordinación de caché Web (WCCP).

El servidor de caché de proxy Squid es una excelente solución para una variedad de necesidades de servidores de proxy y caché y escalas desde la sucursal hasta redes de nivel empresarial, proporcionando mecanismos de control de acceso extensos y granulares y monitorización de parámetros críticos a través del Simple Network Management Protocol SNMP). Al seleccionar un sistema informático para utilizarlo como un servidor dedicado dedicado a caché de caché para muchos usuarios, asegúrese de que está configurado con una gran cantidad de memoria física, ya que Squid mantiene un caché en memoria para un mayor rendimiento.

Squid es un proxy facil de configurar, mediante el archivo **squid.conf,** incluso se puede incluir un archivo externo con las URL que deseamos bloquear. Ver ***Ilustración 6 : Creando archivo externo con las URL a bloquear.***

Ventajas de usar Squid3:

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

Desventajas, pero de usar un Proxy en general:

1. La máquina donde funcionara el Proxy debe tener capacidad de almacenamiento acorde a la cache que necesitemos o queramos.
2. Debe tener un buen poder de procesamiento, ya que no es solo un 'reenvió' de paquetes tcp/ip. Recuerden que estamos trabajando en la Capa de Aplicación.
3. En modo transparente existen algunos problemas de compatibilidad (mínimos, pero existen).
4. Hay que configurar la utilización del Proxy en cada cliente (hay 2 formas de

salvar este inconveniente, que veremos más adelante).

El proyecto de Filtro web, con Squid3, se puede representar en el siguiente cuadro de las Capas del modelo OSI:

N°	CAPAS	PROTOCOLOS	COMANDOS
7	Aplicación	HTTP, HTTPS, FTP	tcpdump tcp port 80
6	Presentación	HTTP, HTTPS, FTP	tcpdump tcp port 80
5	Sesión	HTTP y HTTPS	tcpdump tcp port 80
4	Transporte	TCP y UDP	netstat -putona, netstat -apA inet, lsof -i | grep squid3
3	Red	IPv4, ARP y ICMP	ip add, ip config, ping, arping
2	Enlace de datos	MAC, Ethernet	Ifconfig, /sbin/ifconfig | grep Hwaddr
1	Física	Bits	lspci (puertos)

Tabla 2: Capas del Modelo OSI en el proyecto de Filtro web.

Representación de diagrama de un filtro web:

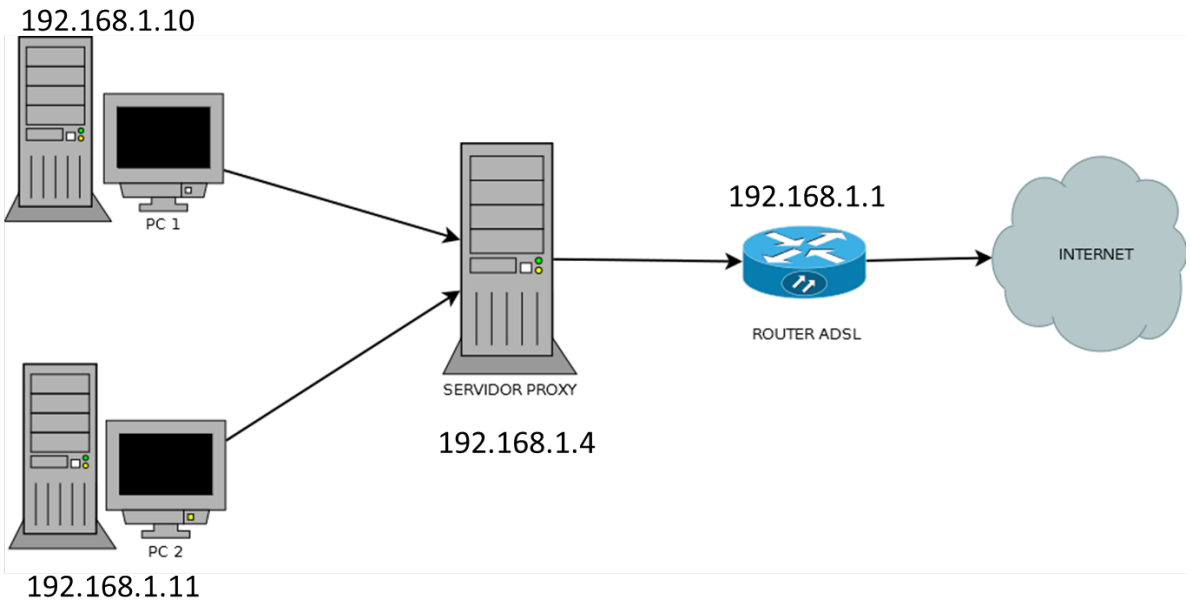

Ilustración 2: Diagrama de Red de Un Filtro Web

Otros comandos importantes, para squid3:

a) Para comprobar que la lista externa que tiene el archivo **prohibidas.** Con el comando

`cat /etc/squid3/prohibidas`

b) para verificar que realmente squid3 escucha en el puerto 3128

`netstat -anp | grep 3128` **ó** **`lsof -i | grep 3128`**

2. WEBlocker:

WEBlocker es un programa que nos permite bloquear páginas web no apropiadas ejerciendo un control parental sobre las mismas.

Características.

Con WEBlocker dispondremos de una herramienta potente y eficaz que nos permitirá bloquear páginas web. Indicado sobre todo a padres que quieran tener un control parental sobre el acceso y páginas que consideren no apropiadas para sus hijos. El programa es muy sencillo de utilizar y no deberemos de ser expertos para saber utilizarlo, solo deberemos saber el dominio o el subdominio de las paginas en cuestión. El programa también bloqueara cualquier programa de descarga o intercambio de archivos. Si lo considera necesario también permitirá bloquear todo el acceso a interne.

Ventajas:

- Muy sencillo de utilizar.
- Funciona con todos los navegadores web.
- Opciones de bloqueo.

Desventajas:

- Es Software privativo.

3. Anti-Porn:

Anti-Porn es un programa de protección con el que podremos controlar el contenido visible en nuestro ordenador procedente de internet.

Características.

Con Anti-Porn dispondremos de una herramienta de seguridad, sobre todo para nuestros hijos y menores. Con este programa podremos controlar el contenido que queramos que aparezca en nuestro ordenador a la hora de conectarnos a internet, bloqueando el contenido no deseado. No solo podremos controlar y bloquear contenido pornográfico, sino que podremos bloquear contenido violento y no apto para menores.

El programa dispone de un filtro muy robusto que logra bloquear cualquier página con contenido pornográfico y también dispone de la opción de introducir la dirección de páginas inapropiadas manualmente. Podremos crear lista de páginas permitidas y otro de páginas prohibidas que serán bloqueadas.

Podremos configurar todas las opciones y eliminar las prohibiciones de forma sencilla, introduciendo la contraseña personal. Además de filtrar y bloquear contenido inapropiado, podremos configurar el programa para que os haga un informe de todos los archivos ejecutados en el PC, como por ejemplo imágenes, videos, música, etc.

Anti-Porn es una fantástica herramienta de control. Podremos configurar el PC para que sea totalmente seguro para cuando nuestros hijos y persona menores que lo utilicen. El programa dispone de una buena interfaz que permite configurar las distintas opciones de forma sencilla. Una gran herramienta si queremos proteger a nuestros hijos y menores del contenido inapropiado que existe en internet.

Ventajas:

- Muy sencillo de utilizar.
- Efectivo.
- Funciona de forma oculta.
- Podemos programar el tiempo de conexión a internet.

Inconvenientes:

- Nada reseñable.

4. WinGate

WinGate es un sofisticado puerto de Internet integrado y servidor de comunicaciones diseñado para satisfacer las necesidades de control, seguridad y correo electrónico de los

actuales negocios conectados a Internet.

Principales funciones:

- Dar seguridad y control del acceso a internet a toda la empresa vía una sola conexión o multiples conexiones de internet compartidas.
- Aplicar un avanzado y flexible control de acceso junto con políticas de uso.
- Monitorizar el uso en tiempo real, y mantener auditorías por usuario y por servicio.
- Bloquear virus, spam y contenido inapropiado en la entrada a la red
- Ofrecer servicios de correo electrónico en internet e intranet.
- Proteger los servidores contra amenazas tanto internas como externas.
- Mejorar el rendimiento de la red y respuesta con el Cache de la web y DNS.
- Fácil administración de WinGate.

Usar WinGate para controlar activamente el uso de internet y recursos de la red puede ofrecer muchos beneficios, incluyendo:

- Mejorar la productividad de los empleados
- Minimizar el tiempo y recursos requeridos para mantener la integridad de la red
- Mejora de la eficiencia, la flexibilidad y la fiabilidad del acceso a la red.

COMPARACIÓN DE SQUID3 CON OTROS SOFTWARE SIMILARES:				
	Squid3	**WeBlocker**	**WinGate 8.5.9**	**Anti-Porn 20.7.4.25**
Código	Abierto	Privativo	Privativo	Privativo
Tipo de Licencia	GNU GPL.	Copiright	Copiright	Shareware
Costo económico	Gratuito	Gratuito	De prueba = Gratis por 30 días Licenciada = Estandar: 3 usuarios($74.95), 6 usuarios($109.95) , 12 usuarios($199.95). •Profesional: 3 usuarios($99.95), 6 usuarios($164.95), 12 usuarios($329.95), 25 usuarios($549.95), 50 usuarios($824.95), 100 usuario	De prueba = Gratis por 30 días Licenciada = $29.97

COMPARACIÓN DE SQUID3 CON OTROS SOFTWARE SIMILARES:				
	Squid3	**WeBlocker**	**WinGate 8.5.9**	**Anti-Porn 20.7.4.25**
ventajas **ventajas**	• Ahorro de tráfico • Velocidad en tiempo de respuesta. • Demanda a Usuarios. •Filtrado de contenidos •Modificación de contenidos. • cofiable, robusto y versátil.	• Muy sencillo de utilizar. • Funciona con todos los navegadores web. • Opciones de bloqueo.	• Dar seguridad y control del acceso a internet a toda la •empresa via una sola conexión o multiples conexiones de internet compartidas. • Aplicar un avanzado y flexible control de acceso junto con políticas de uso. • Monitorizar el uso en tiempo real,	• Muy sencillo de utilizar. • Efectivo. • Funciona de forma oculta. • Podemos programar el tiempo de conexión a internet.
Desventajas	• Las páginas mostradas pueden no estar actualizadas, si éstas han sido modificadas desde la última carga que realizo el proxy caché. • El hecho de acceder a Internet a través de un proxy, en vez de mediante conexión directa, impide realizar operaciones	• Software Privativo.	• Software Privativo. • La vercion licenciada es muy costosa.	• Software Privativo.

COMPARACIÓN DE SQUID3 CON OTROS SOFTWARE SIMILARES:				
	Squid3	**WeBlocker**	**WinGate 8.5.9**	**Anti-Porn 20.7.4.25**
Espacio que utiliza en el disco duro	11.6MB	668KB	39.3 MB (41,209,856 bytes)	5.40 Mb
Forma de instalación	Modo consola	Modo gráfico	Modo gráfico	Modo gráfico
Modo de gestíon	Modo consola	Modo gráfico	Modo gráfico	Modo gráfico
Compatibilidad	AIX, BSDI, Digital Unix, FreeBSD, HP-UX, IRIX, NU/Linux, Mac OS X, NetBSD, NeXTStep, OpenBSD, SCO Unix, SunOS/Solaris, Windows NT.	Es un programa privativo, compatible Windows XP o superior	Es un programa privativo, compatible Windows 10	Es un programa privativo, compatible Windows

Tabla 3: Comparación de Squid3 con otros software similares

IX. CONCLUSIONES

1. Squid es un software muy útil como servidor proxy; donde se puede crear un filtro web, muy amplio, a través de archivo externo; teniendo además la opción de acceder a la lista de bloqueos para agregar, modificar o eliminar dichos registros, de una forma sencilla y rápida, por tanto es una excelente opción para nuestro proyecto.

2. De los software comparados, WinGate ocupa el primer lugar en seguridad, ya que es muy robusto, pero por ser un software privativo, tiene un costo mayor que cualquier de los demás, cuyos costos pueden ir desde $74.95 hasta $1699.95 según la tabla de comparaciones. Siendo squid3, la segunda mejor en base a seguridad y la primera mejor opción en base a costos ya que es totalmente gratuito.

3. Por ser Software Libre y de código abierto, Squid es la mejor opción para Servidor Proxy, ya que es fácil de configurar y compatible con los sistemas operativos basados en Linux e incluso sistemas operativos privativos.

X. RECOMENDACIONES

1. Para hacer más fácil la configuración del squid, es muy útil crear un archivo externo para listar los sitios que se quieren bloquear. Ya que de esta forma, no se necesita manipular todas las veces el archivo de configuración que squid trae por defecto, para actualizar, modificar o eliminar URL de la lista de bloqueo.

2. Squid es una buena opción, si no se cuentan con recursos económicos y se tienen con los conocimientos básicos de servidor proxy.

3. Este software se debe montar preferiblemente en Ubuntu, Debian o cualquier sistema operativo basado en Linux.

4. Para hacer las pruebas para comprobar el funcionamiento de squid, es preferible hacerlo con conexión cableada.

5. Se recomienda también mantenerse actualizado con la nueva documentación sobre squid3 o versiones posteriores.

XI. GLOSARIO

A

Aplicaciones P2P: (peer to peer) son programas que permiten el intercambio de archivos entre internautas.

C

Cifrado: Método de seguridad que vuelve la información ilegible a quien no tenga la clave para descifrarla. Se utiliza generalmente para proteger las compras y otras transacciones de Internet. Cuando un sitio web indica que es “seguro”, generalmente se refiere a que los datos que se envían y se reciben están cifrados. Consulte también criptografía de clave pública.

Cliente: El cliente es una aplicación informática o un ordenador que consume un servicio remoto en otro ordenador conocido como servidor, normalmente a través de una redde telecomunicaciones.

Conexión: La conexión es el enlace que se establece entre el emisor y el receptor a través del que se envía el mensaje.

D

Dirección IP: es un número que identifica, de manera lógica y jerárquica, a una Interfaz en red (elemento de comunicación/conexión) de un dispositivo (computadora, tableta, portátil, smartphone) que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red del modelo TCP/IP.

Dirección URL: es una sigla del idioma inglés correspondiente a Uniform Resource Locator (Localizador Uniforme de Recursos). Se trata de la secuencia de caracteres que sigue un estándar y que permite denominar recursos dentro del entorno de Internet para que puedan ser localizados.

F

Ficheros: Un archivo o fichero informático es un conjunto de bits que son almacenados en un dispositivo. Un archivo es identificado por un nombre y la descripción de la carpeta o directorio que lo contiene. A los archivos informáticos se les llama así porque son los equivalentes digitales de los archivos escritos en expedientes, tarjetas, libretas, papel o microfichas del entorno de oficina tradicional.

Filtros web: es un tipo de software diseñado para restringir los sitios web que puede visitar un usuario en su ordenador.

Firewall (personal)

Software que controla el acceso y las comunicaciones entre un ordenador e Internet o una red local. Impide el acceso a hackers y otro tipo de tráfico no autorizado, a la vez que permite el tráfico autorizado.

Firewall (red)

Dispositivo de hardware o software, o ambos, que controla el acceso a la red y las comunicaciones entre una red e Internet, o entre una parte de la red y otra.

H

Hub de red: Dispositivo de hardware que conecta ordenadores entre sí en una red local.

HTTP (Hypertext Transfer Protocol): es un protocolo de transferencia donde se utiliza un sistema mediante el cual se permite la transferencia de información entre diferentes servicios y los clientes que utilizan páginas web.

HTTPS (Hypertext Transfer Protocol Secure): es un protocolo de aplicación que se basa en el protocolo http, que está destinado a la transferencia segura de datos de hipertexto. O sea es la versión segura de http.

M

Malware: es la abreviatura de Malicious software y este término engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento.

P

Protocolo: En informática, un protocolo es un conjunto de reglas usadas por computadoras para comunicarse unas con otras a través de una red.

Proxy: Un proxy, o servidor proxy es un ordenador que sirve de intermediario entre un navegador Web e Internet. El Proxy contribuye a la seguridad de la red.Los servidores Proxy permiten dar seguridad y mejorar el acceso a páginas Web, conservándolas en la caché.

Proxy caché: es el ordenador que nos proporcionará las páginas de Internet en vez de ir directamente al origen del documento (si hemos configurado nuestro navegador para utilizarlo), lo que acelerará el suministro de información a través de WWW.

Proxy NAT: (Network Address Translation - Traducción de Dirección de Red): es la traducción de direcciones ip privadas en direcciones públicas. Actúa como intermediario entre los equipos de red interna y el exterior permitiendo que estos puedan acceder a los servicios que brinda la web.

R

Red o red informática: Grupo de dos o más ordenadores conectados por cables o señales inalámbricas, o ambos, que pueden comunicarse entre sí mediante protocolos de red. Las redes también pueden incluir otros dispositivos, por ejemplo, impresoras, routers y hubs.

Red LAN: es una red de computadoras que abarca un área reducida a una casa, un departamento o un edificio (Red De Área Local).

Reverse Proxy: Un proxy inverso es un dispositivo o servicio colocado entre un cliente y un servidor en una infraestructura de red. Las solicitudes entrantes son manejadas por el proxy, que interactúa en nombre del cliente con el servidor o servicio deseado que reside en el servidor.

S

Servidor: es una aplicación en ejecución (software) capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia.

Servidor web: Un servidor web o servidor HTTP es un programa informático que procesa una aplicación del lado del servidor, realizando conexiones bidireccionales o unidireccionales y síncronas o asíncronas con el cliente y generando o cediendo una respuesta en cualquier lenguaje o Aplicación del lado del cliente.

SOCKS: es un protocolo de Internet que permite a las aplicaciones Cliente-servidor usar de manera transparente los servicios de un firewall de red. SOCKS es una abreviación de "SOCKetS".

SSL: El cifrado/descifrado SSL son operaciones costosas y pueden reducir el rendimiento del servidor de aplicaciones en más de un 30%.

T

Tráfico web: es la cantidad de datos enviados y recibidos por los visitantes de un sitio web.

XII. BILIOGRAFÍA

- Kaspersky Lab. . (2017). Latam.kaspersky.com. 5 de octubre de 2017, de Kaspersky Lab. Sitio web: https://latam.kaspersky.com/resource-center/definitions/web-filter.
- meca,J. (2010). *Servidor proxy squid y Dansguardian.* octubre 4,2017, de https://prezi.com Sitio web: https://prezi.com/2ewxag1d4ydd/servidor-proxy-squid-y-dansguardian/.
- Leidy,V. (2015). SERVIDORES PROXY Y WEB. octubre3,2017, de https://prezi.com Sitio web: https://prezi.com/on9bjgzomr6d/servidores-proxy-y-web/.
- help.ubuntu.com. (2014). Servidor proxy Squid. octubre 03,2017, de https://help.ubuntu.com Sitio web: https://help.ubuntu.com/lts/serverguide/squid.html.
- ite. (2016). Proxy squid. octubre 03,2017, de http://www.ite.educacion.es Sitio web: http://www.ite.educacion.es/formacion/materiales/85/cd/linux/m6/proxy_squid.html.
- Merlos,J. (2003). Squidguard: filtros de contenido para Squid. octubre 04, 2017, de http://www.merlos.org Sitio web: http://www.merlos.org/linux/2003/09/squidguard.html
- De Luz,S. (2016). Nuevas vulnerabilidades de seguridad en Squid, todas sus versiones están afectadas. octubre 02,2017, de https://www.redeszone.net Sitio web: https://www.redeszone.net/2016/04/26/nuevas-vulnerabilidades-seguridad-squid-todas-versiones-estan-afectadas/
- blogspot.com. (2014). Informática para todos. octubre 04,2017, de http://blogdeinformaticafamiliar.blogspot.com/ Sitio web: http://blogdeinformaticafamiliar.blogspot.com/2014/05/anti-porn-v207425.html
- Chamaco,M. (2012). WEBlocker, bloquea páginas web fácilmente. octubre 04,2017, de http://vidabytes.com Sitio web: http://vidabytes.com/2012/11/weblocker-bloquea-paginas-web-facilmente.html
- QBIK. (2017). WinGate. 0ctubre 05,2017, de http://www.wingate.com Sitio web:

  http://www.wingate.com/download/wingate/download.php

XIII. ANEXOS

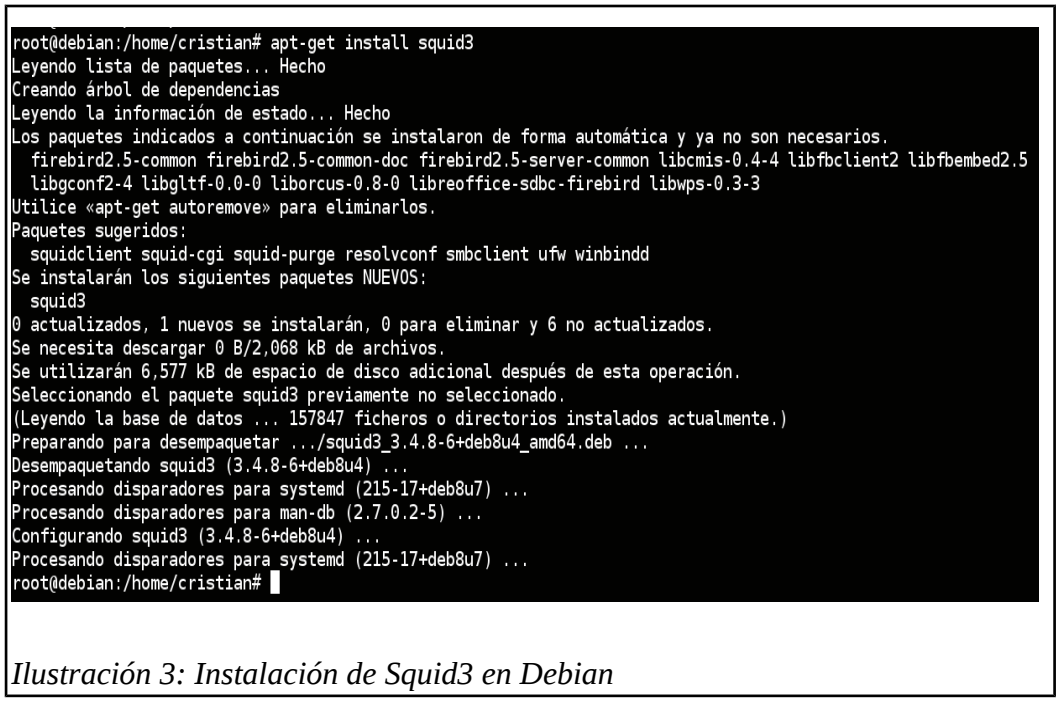

Ilustración 3: Instalación de Squid3 en Debian

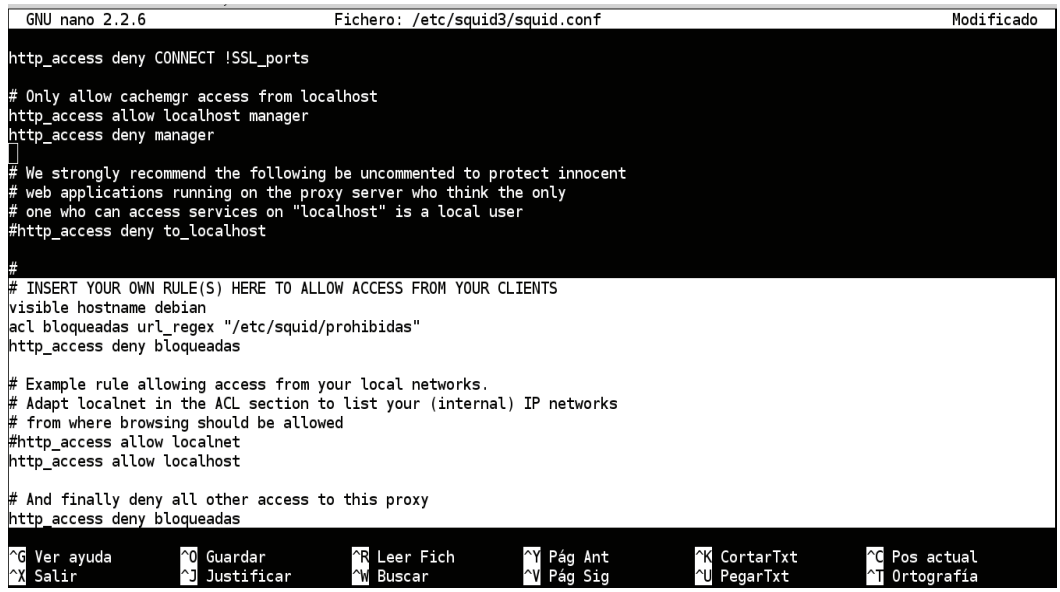

Ilustración 4: configuración de Squid3

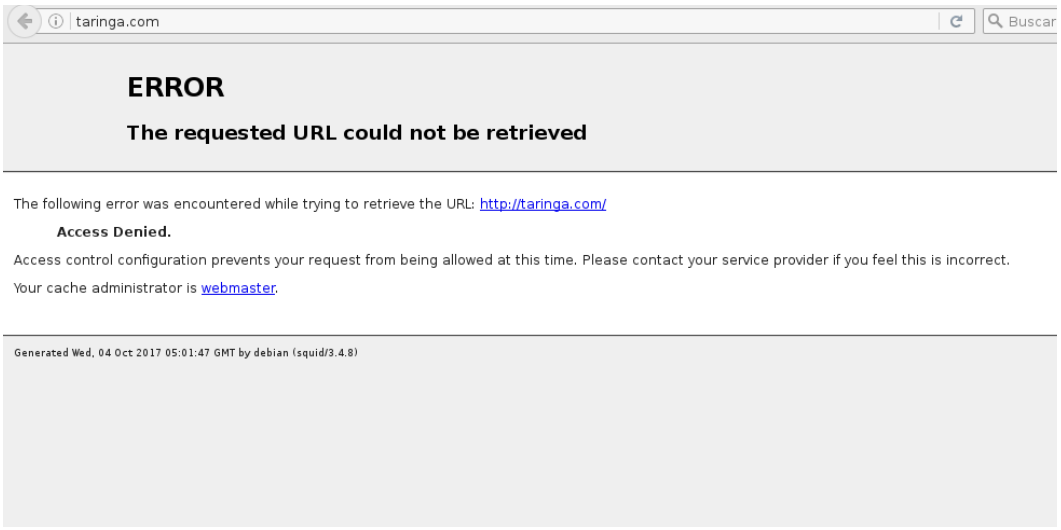

Ilustración 5: Página Web bloqueada con squid3

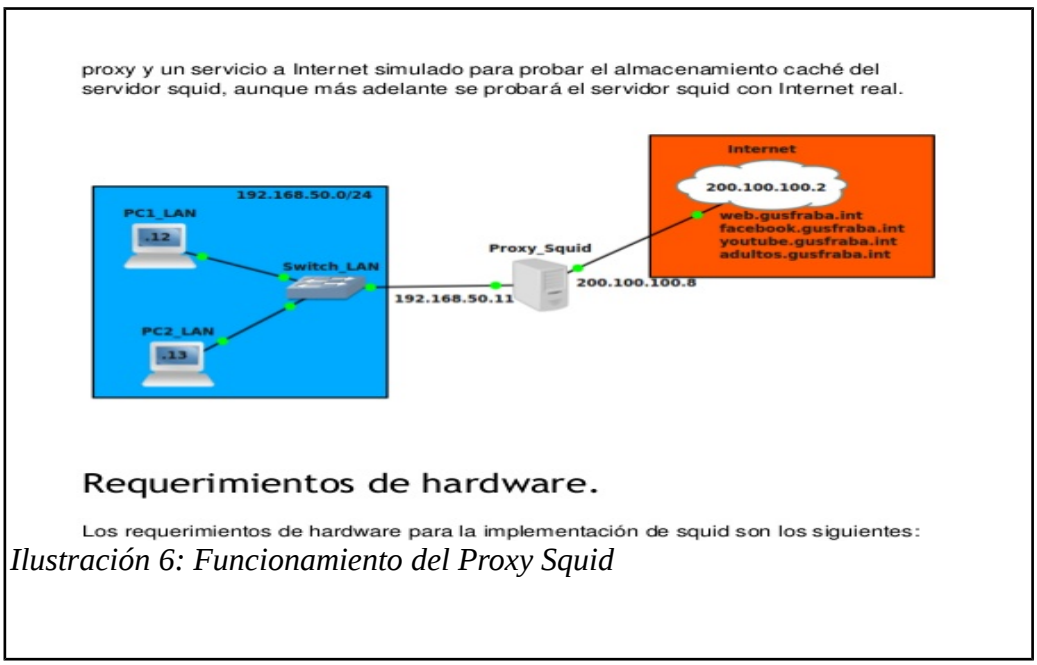

Ilustración 6: Funcionamiento del Proxy Squid

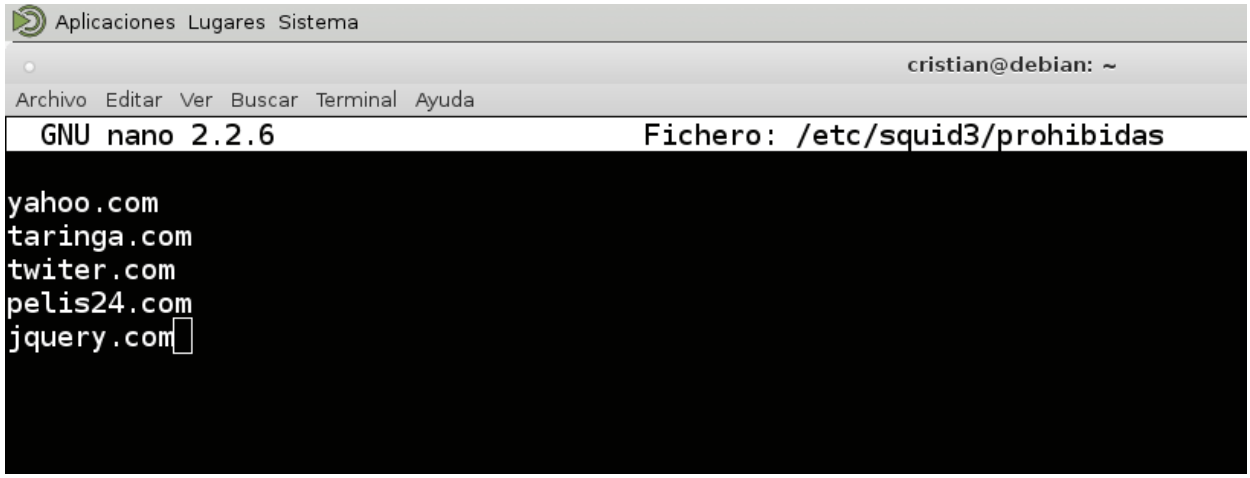

Ilustración 7: Creando archivo externo con las URL a bloquear