**LABORATORIO No 10: PROXY - Squid**

**Objetivos**

Al finalizar el taller, se espera que el estudiante esté en capacidad de:

* Instalar un servidor PROXY en Linux.
* Configurar el servicio teniendo en cuenta los requerimientos y seguridad.
* Iniciar el servicio PROXY.
* Probar que el servidor PROXY funcione en un ambiente de red.

# PROXY - Squid

# Un servidor proxy tiene como propósito actuar de intermediario en el acceso a un recurso en internet. Suelen utilizarse para acceder o restringir páginas webs en una empresa, es decir, pueden trabajar como muro cortafuegos operando en la capa de red (actuando como filtro de paquetes, como es el caso de iptables) o bien desde la capa de aplicación controlando diferentes servicios.

# Otra de sus funciones es actuar como caché de contenido (principalmente para el protocolo HTTP), proporcionando mayor proximidad de los clientes a un caché de páginas y archivos de forma que estos accedan con tiempos similares a los de una red local.

# El servidor de proxy cache Squid se caracteriza por tener un alto rendimiento y soportar FTP o incluso HTTP sobre IPv4 e Ipv6. Todos los objetos cacheados por Squid permanecen en RAM, incluso consultas de búsquedas DNS. Además, ofrece soporte SSL y listas de control de acceso.

**Instalación de Squid**

Para instalar Squid, se escribe el siguiente comando:

$ sudo apt-get install squid3

**Configuración de Squid**

Para poder configurar el servidor proxy Squid, se debe editar el archivo squid.conf, ubicado en /etc/squid3/. Para ello se abrirá el archivo con el editor nano, ejecutando el comando:

sudo nano /etc/squid3/squid.conf

Por defecto el acceso http esta negado para todas las peticiones. Por esta razón, se debe buscar y colocar en comentarios la línea:

http\_access deny all

Para asignar acceso a los recursos internet, se puede configurar una lista de acceso basada en rangos de IP a la que se quiera permitir el acceso, por ejemplo, si se desea proveer de acceso a la dirección de red 192.168.10.X/24, la configuración sería:

acl mi\_red src 192.168.10.0/24

http\_access allow mi\_red

De igual forma, se debe comprobar que la directiva http\_port este apuntando al puerto 3128 por defecto o cambiarlo al que se requiera. Los puertos recomendados para Servidores Proxies son el 3128 y 8080 a través de TCP.:

http\_port 3128

Por otro lado, el parámetro cache\_mem establece la cantidad de memoria RAM dedicada para almacenar los datos más solicitados y datos en tránsito (con mayor prioridad de almacenamiento). Los datos son normalmente almacenados en bloques de 4 Kb. El valor por defecto es de 256 MB, pero puede especificarse una cantidad mayor si es necesario. Por ejemplo puede establecerse 2 GB de memoria:

cache\_mem 2048 MB

Una vez terminada la configuración básica, es necesario reiniciar el servicio squid, de la siguiente manera:

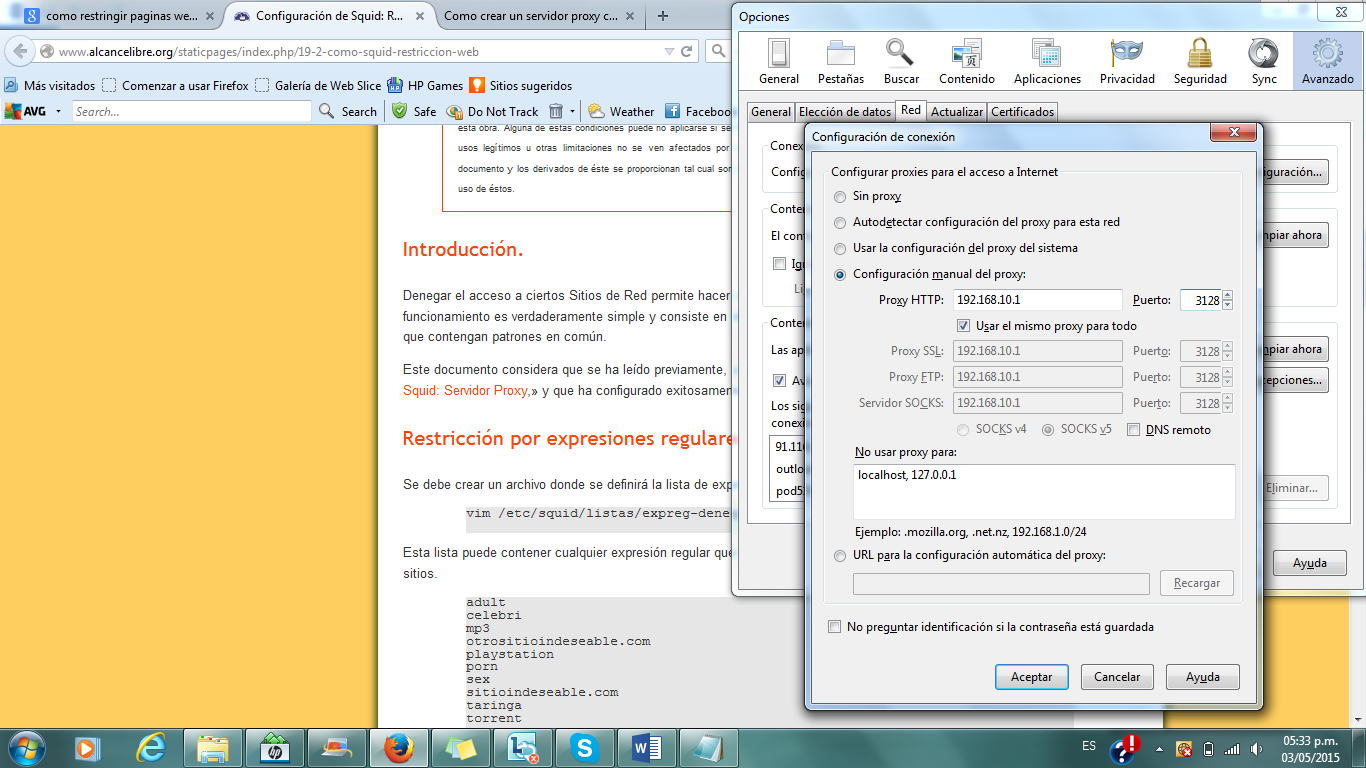
sudo service squid3 restart

Para comprobar que el servicio se está ejecutando correctamente, se ejecuta la instrucción:

sudo service squid3 status

Para empezar a utilizar el servidor proxy, se debe configurar en la sección de preferencias u opciones del browser, la dirección IP de servidor donde está funcionando el proxy y el puerto que se configuró en los pasos anteriores. En la Figura 1, se puede observar la configuración para el browser Mozilla FireFox.

Figura 1. Configuración del browser FireFox.



**Restricción de acceso a Sitios de Internet**

Denegar el acceso a ciertos Sitios web permite hacer un uso más racional del ancho de banda con el que se dispone. El funcionamiento es verdaderamente simple y consiste en denegar el acceso a nombres de dominio o direcciones de Internet que contengan patrones en común.

Una forma de hacerlo es a través de restricciones por expresiones regulares. Para realizar esta actividad, se requiere realizar los siguientes pasos:

* Cree un directorio denominado listas en la ruta /etc/squid3
* Acceda a la ruta /etc/squid3/listas y cree un archivo denominado expregden. Puede utilizar como editor de texto a nano.
* Como parte del contenido del archivo, coloque cualquier expresión regular que se considere sea usualmente utilizadas en las direcciones de ciertos sitios, por ejemplo

adult

mp3

playstation

porn

sex

sitioindeseable.com

taringa

torrent

warez

wii

* Posteriormente, se debe editar el archivo de configuración de Squid

$sudo nano /etc/squid/squid.conf

* A continuación, se debe adicionar una lista de control, denominada lstexpregden, de acceso tipo url\_regex (expresiones regulares del URL), que defina la lista en el archivo /etc/squid/listas/expregden, es decir, en el archivo de configuración de squid debe estar:

acl lstexpregden url\_regex "/etc/squid/listas/expregden"

* Finalmente, se crea una Regla de Control de Acceso agregando con un símbolo de ! que se denegará el acceso a la Lista de Control de Acceso denominada lstexpregden, así:

http\_access allow mi\_red !lstexpregden

La regla anterior permite el acceso a la Lista de Control de Acceso denominada mi\_red, pero le niega el acceso a todo lo que coincida con lo especificado en la Lista de Control de Acceso denominada lstexpregden.