INSTALACION Y CONFIGURACION DE UN PROXY

Guía de configuración de squid3

**ACL (listas de control de acceso)**

**Las acl son un conjunto de reglas que permiten controlar el tráfico de la red a través de la aprobación o denegación de estas.**

**Para definir las acl se debe realizar desde el fichero /etc/squid3/squid.conf. Las acl deben especificarse de manera ordenada en el fichero puesto que guardan un orden secuencial.**

**Para facilitar el bloqueo a varios sitios de una sola vez, podemos realizar una acl que carga los dominios o palabras de un fichero y permite/deniega el acceso a dichos sitios web.**

**Acl nombre\_acl dstdomain “/dirección del fichero”=>dominio**

**La estructura de un ACL es: acl nombreacl tipoacl valor……[fichero]**

**Algunos elementos de ACL:**

**src:** es la dirección IP del del cliente, puede ser una IP o un rango

**url-regex**: tipo con soporte para expresiones regulares para la url solicitado por el cliente

**time**:Hora del día y de la semana….etc

**Construcción de una regla ACL**

Una vez definida una ACL se pueden construir reglas de acceso basadas en ella. Estas reglas concederán o denegarán a las peticiones que cumplan a la ACL asociada a la regla. Existen múltiples tipos de reglas de control, por ejemplo de acceso a http, de control de direcciones IP, de control de puertos..etc

Las reglas **http\_access** se utilizan para permitir o denegar el acceso mediante las palabras reservadas **allow o deny. Se construyen: http\_access allow/deny acl.**

# **1-RESTRICCIONES DE ACCESO**

Algunos pasos a tener en cuenta configurar **Squid** para:

* Permitir o denegar acceso a Internet
* Permitir o denegar acceso a páginas web en concreto.
* Restricciones de descarga de tipos de archivos (restricciones por extensión de archivos).

# **1.1-ACCESO A INTERNE**T **(HTTP\_ACCESS)**

# **CONFIGURACIÓN PARA ACCESO DE LOS EQUIPOS**

Antes de nada debemos declarar una **acl** para toda la red, la sintaxis para declarar la red es la siguiente:

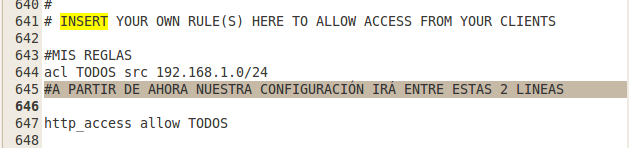
**acl <NOMBRE\_ACL> src <IP\_red>/<MASCARA\_RED>**

Así que supongamos que nuestra red es **192.168.1.0** con mascara **/24**, nuestra acl sería la siguiente:

**acl TODOS src 192.168.1.0/24**

Y le damos acceso a toda la red

**http\_access allow TODOS**

[](http://www.sospedia.net/wp-content/uploads/2015/03/acl_all_squid.conf_1.png)

**Esto es muy importante**,  el permitir a toda la red el acceso siempre será nuestra última línea de configuración para evitar problemas.

Una vez esto ya podemos ir creando las acl para los equipos de la red, para ello tenemos dos opciones, crear acl individuales para cada equipo o por “grupos”.

**Para crear una acl para un equipo individual, se crea de la siguiente forma**:

**acl <NOMBRE\_ACL> src <IP\_DEL\_EQUIPO>**

Ejemplo:

**acl PC1 src 192.168.1.117**

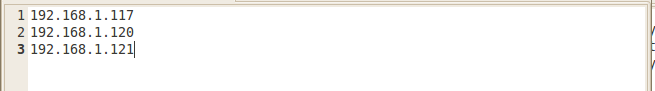
En cambio, si optamos por crear un grupo donde van a tener una configuración en común para más de un equipo, **Squid** permite crear un archivo con una lista de ip’s de los equipos. Dicho archivo se debe ubicar en “/etc/squid3/”:

**acl <NOMBRE\_GRUPO\_ACL> src “/etc/squid3/<NOMBRE ARCHIVO>”**

Ejemplo

**acl PORTATILES src “/etc/squid3/lista\_portatiles.txt”**

Ejemplo archivo:

[](http://www.sospedia.net/wp-content/uploads/2015/03/lista_acl.png)

Una vez creadas ya podemos controlar el  acceso a internet del equipo o equipos configurados:

**http\_access <allow/deny> <NOMBRE\_ACL>**

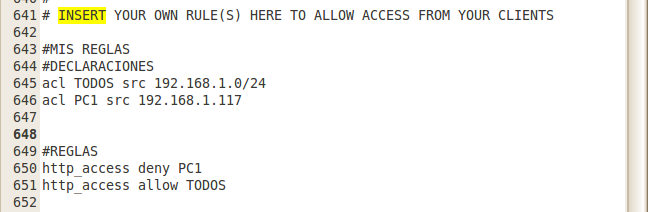
 Suponemos que se ha creado el PC1 con ip 192.168.117 así que insertare las siguientes líneas:

Declaro:

**acl PC1 src 192.168.1.117**

Y para probar le denegamos el permiso de acceso

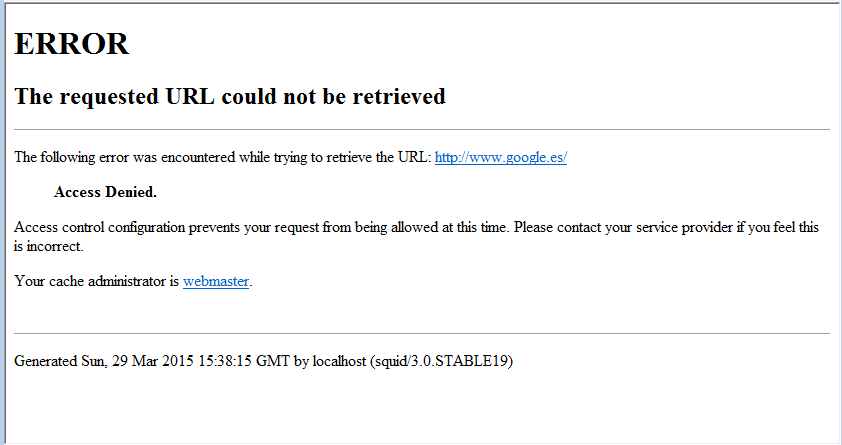
**http\_access deny PC1**

[](http://www.sospedia.net/wp-content/uploads/2015/03/permiso-para-un-equipo.png)

Guardamos el archivo de configuración, lo cerramos y validamos la configuración:

|  |  |
| --- | --- |
| 1 | sudo squid3 -k reconfigure |

Si no nos da ningún error probamos el equipo al que supuestamente le ha sido denegado el acceso a internet

[](http://www.sospedia.net/wp-content/uploads/2015/03/Error-acceso-squid3.png)

Como vemos en la imagen nos dice que tenemos el acceso denegado por el **Squid3**

#### 1.2-CONFIGURACIÓN ACCESO POR TIEMPO

Ahora que tenemos los equipos configurados, podemos controlar el acceso por periodos de tiempo, para declarar un periodo de tiempo se hace de la siguiente manera:

**acl <NOMBRE> time <DIAS> hh:mm-hh:mm**

DIAS:

M – Lunes

T – Martes

W – Miércoles

H – Jueves

F – Viernes

A – Sábado

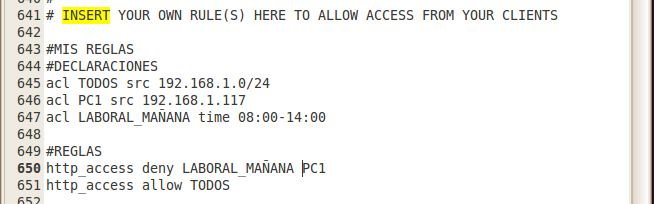
S – Domingo

EJEMPLO:  
**acl LABORAL\_MAÑANA time MTWHF 08:00-14:00**

Para utilizar esta acl, no sirve por si sola, se debe usar junto a una acl de equipo

**http\_access <allow/deny> LABORAL\_MAÑANA PC1**

vemos un ejemplo:

[](http://www.sospedia.net/wp-content/uploads/2015/03/config-acl-tiempo.png)

Guardamos archivo, lo cerramos y validamos la instalación:

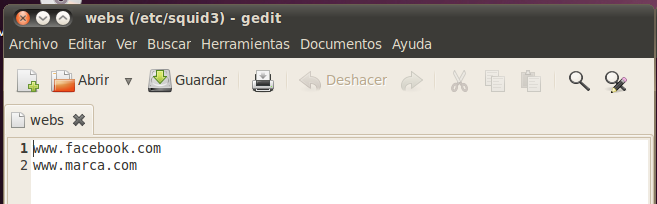
|  |  |
| --- | --- |
| 1 | sudo squid3 -k reconfigure |

Si no nos da ningún error probamos el equipo.  
Ahora el equipo PC1 solo va a tener acceso a internet por las tardes.

# **1.3-CONFIGURACIÓN ACCESO A PÁGINAS**

**Squid** nos permite controlar el acceso a páginas web que queramos, para ello, al igual que para configurar un grupo de equipos, se hace uso de un archivo que hace de lista, en ella pondremos las webs que vamos a querer controlar su acceso. La ubicación del archivo es la misma que la de los equipos en “**/etc/squid3/”.**

Ejemplo del archivo:

[](http://www.sospedia.net/wp-content/uploads/2015/03/listado-webs.png)

Una vez creado el archivo, abrimos el de configuración

**squid3**(/etc/squid3/squid.conf) y declaramos la acl:

**acl <NOMBRE\_acl> url\_regex “/etc/squid3/<nombre\_archivo>”**

Ejemplo:

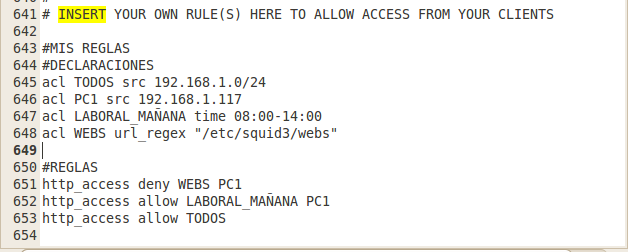
**acl WEBS url\_regex “/etc/squid3/webs”**

Para utilizar esta acl, no sirve por si sola se debe usar junto a una acl de equipo

Ahora la utilizamos con nuestra configuración:

**http\_access <allow/deny> WEBS PC1**

Vemos como lo utilizamos:

[](http://www.sospedia.net/wp-content/uploads/2015/03/acl-control-webs.png)

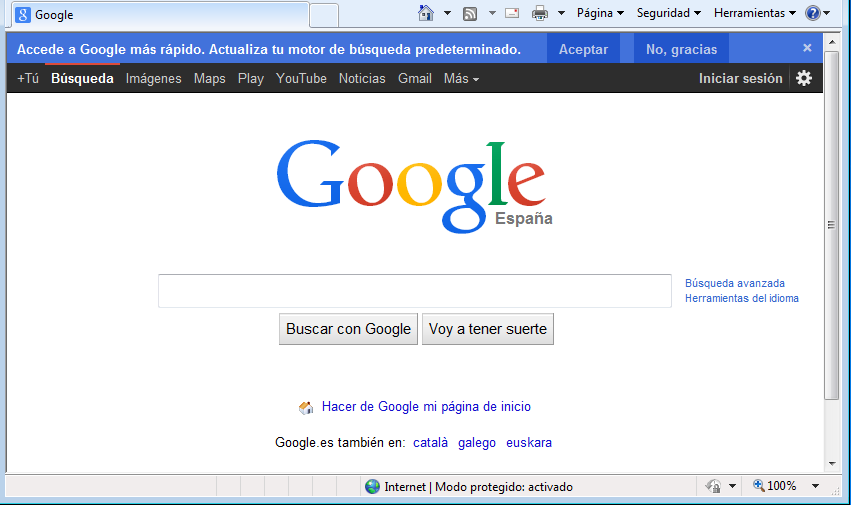
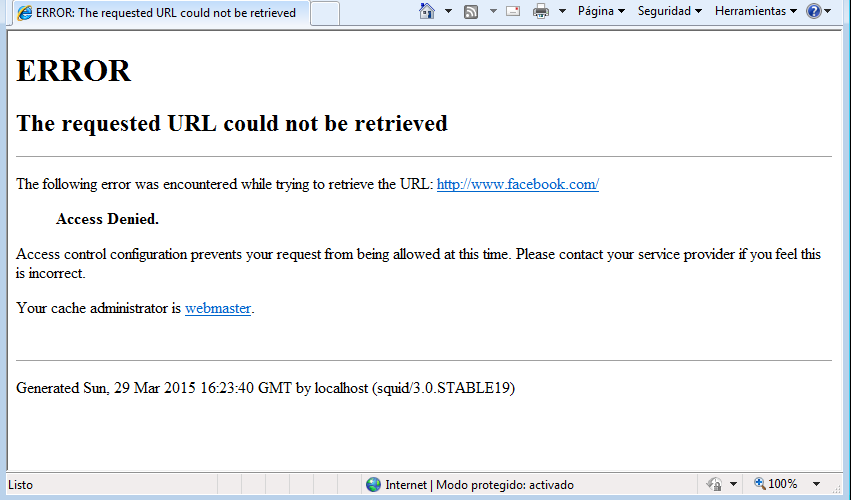
En este ejemplo vamos a denegar acceso a **facebook** y **marca** para el equipo PC1

Como siempre, guardamos, cerramos y validamos configuración:

|  |  |
| --- | --- |
| 1 | sudo squid3 -k reconfigure |
|  |  |
|  |  |

Si no nos da ningún error vamos al equipo PC1 y comprobamos que nos permite ir a la web de **Google** pero no nos dejará ir a **Facebook** o **Marca.**

|  |  |
| --- | --- |
|  |  |

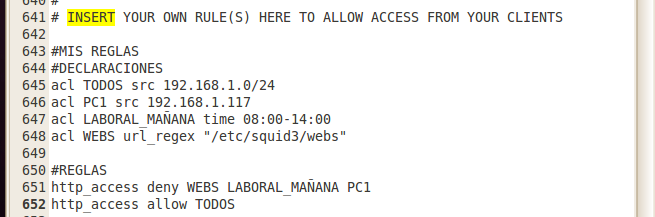
[](http://www.sospedia.net/wp-content/uploads/2015/03/google.png) [](http://www.sospedia.net/wp-content/uploads/2015/03/facebook.png)

Vemos que nos permite acceder a la web de **google,** pero no nos permite acceder a **facebook.**

Ahora que conocemos todos estos métodos podemos combinar los 3 a la vez, por ejemplo si queremos restringir el acceso a las webs citadas anteriormente solo por la mañana sería:

**http\_access deny WEBS LABORAL\_MAÑANA PC1**

Ejemplo:

[](http://www.sospedia.net/wp-content/uploads/2015/03/combinacion-acl-squid3.png)

Pasos a seguir:

1. Crear una RED donde tendremos un **Ubuntu** de servidor
2. Instalar el proxy que será **squid3**
3. Configurar el archivo **squid.conf**
4. Creación del archivo **noperm** para denegar las páginas que queremos denegar
5. Por ultimo configurar los **navegadores** web de los clientes

**Para reiniciar el servicio: “sudo service squid3 restart”**

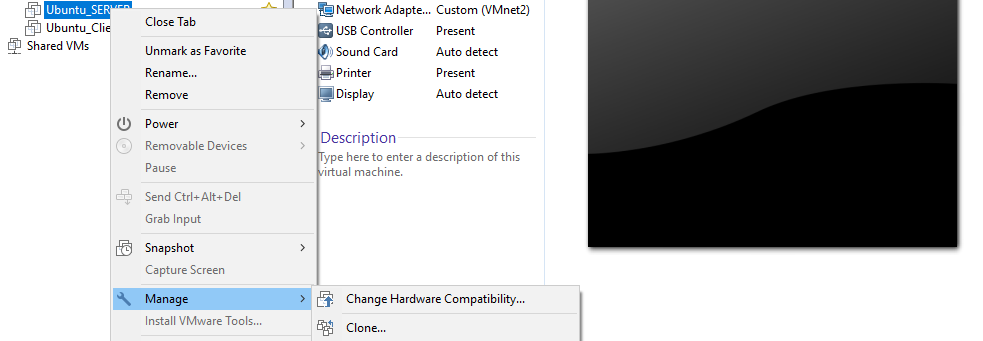
Creación de la RED:

Tendremos que tener una maquina limpia de Ubuntu con acceso a internet es decir con una NAT

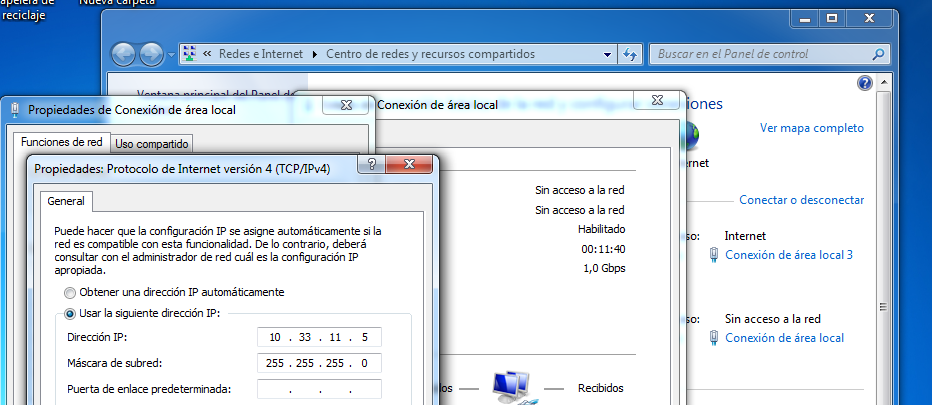
Nos vendrá con una IP genérica con acceso a internet la cual utilizaremos para configurar nuestro proxy en mi caso las tengo asignadas de la siguiente manera

* IP Ubuntu \_Server **192.168.88.181**

Después Proseguiremos clonando nuestro servidor, el motivo de esto es para que la maquina clonada genere una ip del mismo rango que nuestro server evitándonos poner IPs



En Windows tendremos que acceder al centro de redes y configurar nuestra IP de manera gráfica tal como viene en la imagen

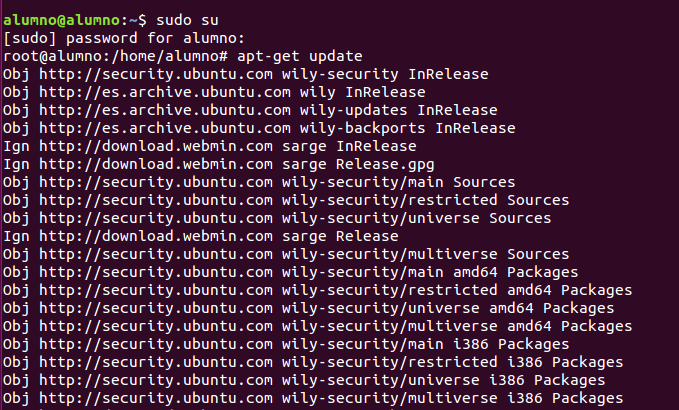


Instalación Del Servidor Proxy:

En el terminal haciendo el uso del comando “sudo su” entramos como Administrador

Después actualizaremos los paquetes con la instrucción “apt-get update”

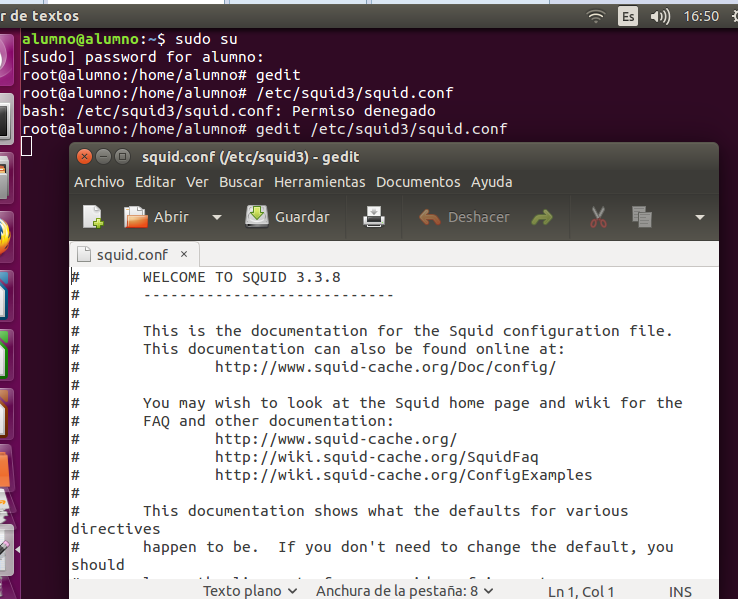
Una vez hecho lo anterior ejecutamos la orden “apt-get install squid3” para instalar el proxy





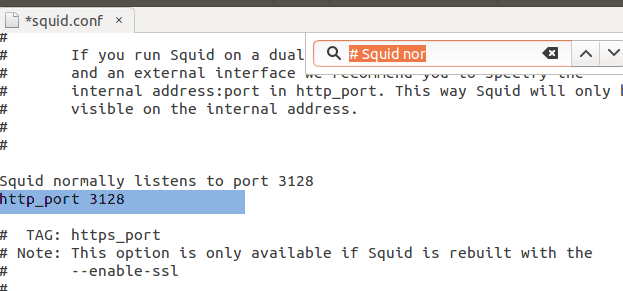
Configuración de squid.conf:

Lo primero será acceder al terminal con la siguiente instrucción “gedit /etc/squid3/squid.conf”

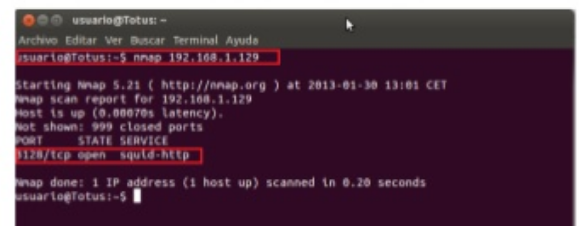


Una vez dentro debemos de buscar una serie de comandos que debemos de descomentar (eliminar el símbolo #) para buscarlos debemos pulsar **Ctrl+F**

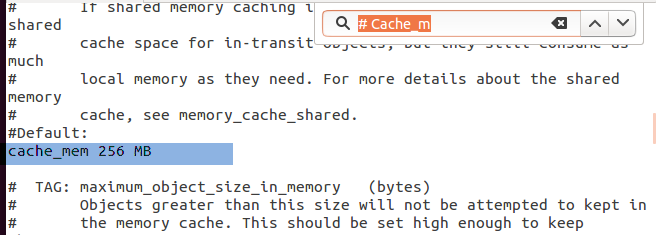
El primer comando que buscaremos será “http\_port 3128” y ver si esta descomentado

Si comprobamos el estado de los puertos. 3128 puerto por donde escucha squid.

Si comprobamos el estado de los puertos en nuestro equipo mediante “nmap” ejecutado desde otra máquina, podremos comprobar que ha quedado habilitado el puerto por defecto.

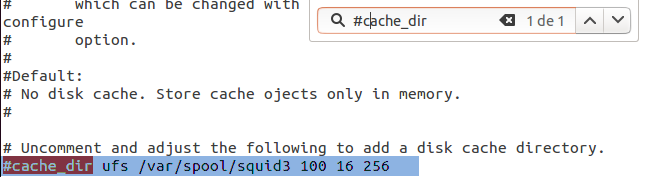


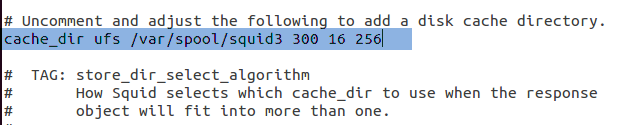
El siguiente parámetro será “cache\_mem 256”



Squid no solo es un proxy web, también integra un servidor de caché que almacena las páginas descargadas.

Ahora buscamos el parámetro “cache\_dir ufs /var/spool/squid3”



Una vez descomentado tendremos que cambiar la cantidad asignada que es 100 a 300 para evitar fallos.

**Cahe\_dir** es un conjunto de directorios donde se guardan las páginas visitadas para no volver a cargar las páginas.

**Ufs** es el método de almacenamiento que utiliza squid en el disco, y /var/spool/squid3 será la ruta donde se guardan las páginas, 100 es el tamaño que viene predeterminado, pero no puede ser inferior al de la memoria caché, por lo que pondremos 300MB. Y 16 será el nº de directorios que se crean por defecto (caché)

El filtrado de conexiones se realiza en squid mediante reglas ACL, en este fichero de configuración.

Nuevamente buscamos la siguiente línea “acl CONNECT method CONNECT”

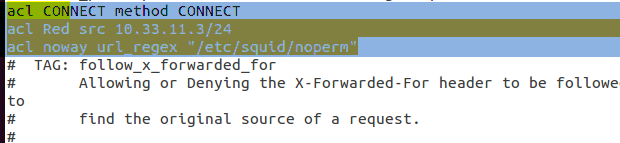
Debajo de esta línea escribimos lo siguiente:

* acl Red src 192.168.88.181/24 🡪 Asignamos nuestra IP para que haga de proxy

Red será el nombre de la etiqueta que haga una búsqueda y la dirección de mi red

* acl noway url\_regex “etc/squid3/noperm”🡪Es nuestro archivo de denegación es

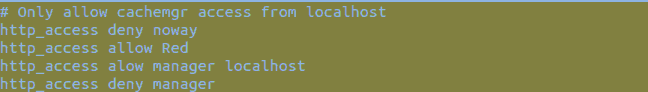
decir donde pondremos las palabras que no queremos que aparezcan.

Noway=> no permitir y ponemos la ruta donde se creará el fichero, en este caso dentro de la carpeta de squid.

Una vez hecho lo anterior buscamos “# only allow chaemgr Access from localhost”

Añadimos las siguientes líneas:

* http\_access deny noway=> deniega todo lo que tenemos en noway
* http\_access allow Red =>

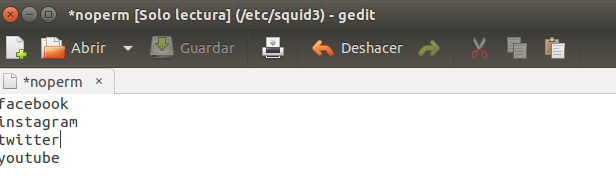


Guardamos el fichero y cerramos el editor de texto

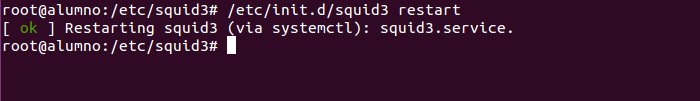
Creación del Archivo noperm:

Tenemos que entrar crear el fichero noperm ya que no existe para ellos ejecutamos la orden:

* “gedit /etc/squid3/noperm” 🡪esto creara el fichero y además nos dejara editarlo y añadimos las palabras que no queremos que tengan acceso

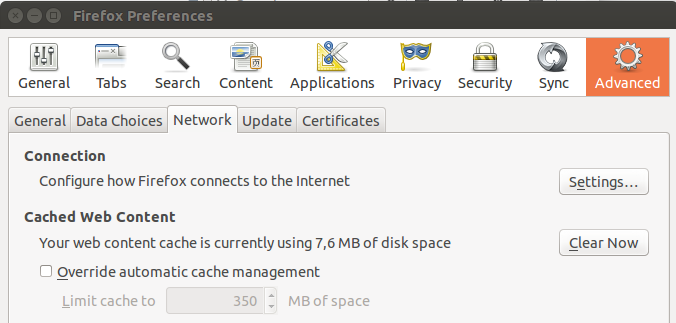


Finalmente reiniciamos el servidor con la siguiente orden “/etc/init.d/squid3 restart”

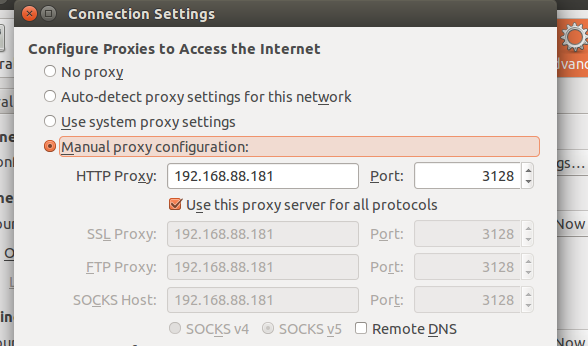


Configuración del Navegador:

Para configurar el proxy en el navegador entramos en preferences y en Advanced

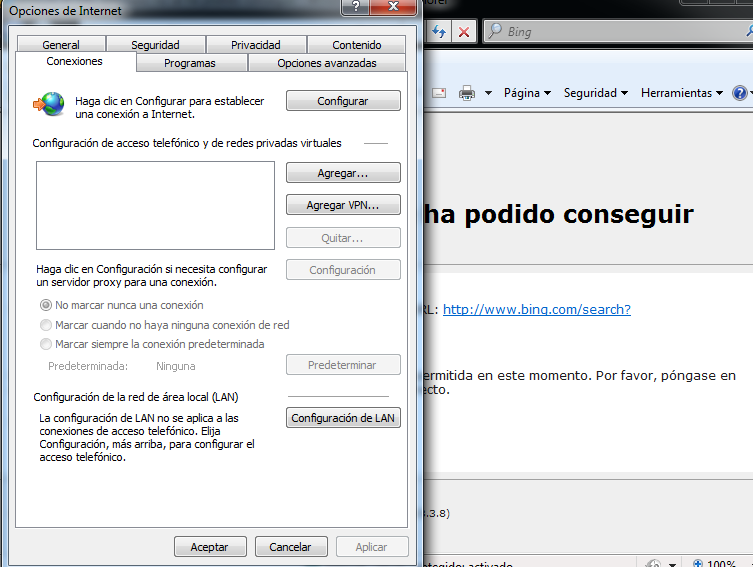


Después seleccionamos la última opción y ponemos la IP de nuestro servidor con el puerto que le dimos



En Windows tendremos que hacer lo siguiente:

Buscar Herramientas y en opciones de internet en la pestaña conexiones



Ahora en la pestaña de configuración de LAN

