

UT05: Instalación y configuración de servidores proxy – 1) Instalación y Configuración servidor Proxy Squid – Modo Directo.

Nombre: Francisco Jesús García – Uceda Díaz - Albo

Curso: 2º ASIR.

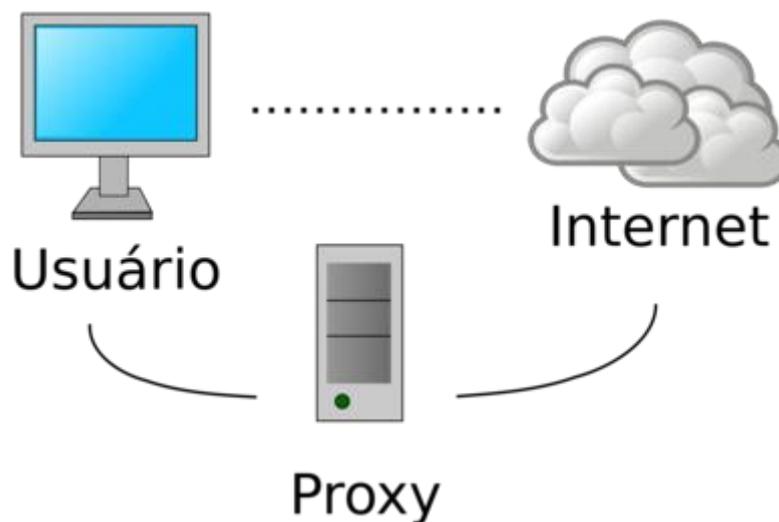
Índice

Introducción	2
1. Instalación y configuración del servidor Proxy “Squid” en GNU/Linux, en modo proxy directo, realizando algunas funcionalidades:.....	2
- Configuración de parámetros generales.....	4
- Archivos de log.	6
- Autenticación de usuarios.	8
- Filtros web mediante listas de control de acceso.	11
Asimismo, demuestre la funcionalidad de dicho servidor proxy en un escenario creado mediante la configuración de un cliente Proxy en GNU/Linux y un cliente Proxy en Windows.	14
Conclusión	19

Introducción

En esta práctica aprenderemos que es un servidor Proxy e instalaremos y configuraremos un servidor Proxy Squid en modo directo. Realizaremos después distintos apartados en su configuración y aprenderemos sobre estos.

1. Instalación y configuración del servidor Proxy “Squid” en GNU/Linux, en modo proxy directo, realizando algunas funcionalidades:



Un proxy es un equipo informático que hace de intermediario entre las conexiones de un cliente y un servidor de destino, filtrando todos los paquetes entre ambos. Siendo tú el cliente, esto quiere decir que el proxy recibe tus peticiones de acceder a una u otra página, y se encarga de transmitírselas al servidor de la web para que esta no sepa que lo estás haciendo tú.

De esta manera, cuando vayas a visitar una página web, en vez de establecer una conexión directa entre tu navegador y ella puedes dar un rodeo y enviar y recibir los datos a través de este proxy. La página que visites no sabrá tu IP sino la del proxy, y podrás hacerte pasar por un internauta de otro país distinto al tuyo.

Los proxies directos (forward proxy servers) envían las solicitudes de un cliente a un servidor web. Los usuarios acceden a proxies directos navegando directamente a una dirección de proxy web o estableciendo sus configuraciones de internet. Los proxies directos permiten eludir los firewalls y aumentar la privacidad y la seguridad de un usuario.

Los proxies inversos (reverse proxies) manejan de forma transparente todas las solicitudes de recursos en los servidores de destino sin requerir ninguna acción por parte del solicitante.

Se utilizan proxies inversos:

- Para habilitar el acceso indirecto cuando un sitio web no permite conexiones directas como medida de seguridad.
- Para permitir el equilibrio de carga entre los separadores.
- Para transmitir contenido interno a los usuarios de internet.
- Para deshabilitar el acceso a un sitio, por ejemplo, cuando un ISP o un gobierno desea bloquear un sitio web.



Squid es un servidor proxy para web con caché. Es una de las aplicaciones más populares y de referencia para esta función, es un desarrollo en software libre publicado bajo licencia GPL. Entre sus utilidades está la de mejorar el rendimiento de las conexiones de empresas y particulares a Internet guardando en caché peticiones recurrentes a servidores web y DNS, acelerar el acceso a un servidor web determinado o añadir seguridad realizando filtrados de tráfico.

Empezaremos instalando Squid en un servidor Debian.

```
franciscojesus@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@debian:/home/franciscojesus# apt-get install squid
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
  erlang-asn1 erlang-base erlang-crypto erlang-edoc erlang-goldrush erlang-inets erlang-jiffy erlang-lager erlang-mnesia
  erlang-odbc erlang-p1-cache-tab erlang-p1-iconv erlang-p1-stringprep erlang-p1-tls erlang-p1-utils erlang-p1-xml erlang-p1-yaml
  erlang-p1-zlib erlang-proper erlang-public-key erlang-runtime-tools erlang-ssl erlang-syntax-tools erlang-xmerl libodbc1
  libsctp1
Utilice «sudo apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes adicionales:
  libcap3 squid-common squid-langpack
Paquetes sugeridos:
  squidclient squid-cgi squid-purge resolvconf smbclient ufw winbindd
```

- Configuración de parámetros generales.

El archivo de configuración de squid se encuentra situado en `/etc/squid/squid.conf` Iremos a él.

```
franciscojesus@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@debian:/home/franciscojesus# gedit /etc/squid/
squid/ squirrelmail/
root@debian:/home/franciscojesus# gedit /etc/squid/squid.conf
```

Lo primero que haremos es crear una regla en iptables para que los equipos que se conecten puedan acceder a internet.

```
franciscojesus@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@debian:/home/franciscojesus#
root@debian:/home/franciscojesus# echo 1 > /proc/sys/net/ipv4/ip_forward
root@debian:/home/franciscojesus# iptables -t nat -A POSTROUTING -s 192.168.100.0/24 -o enp0s3 -j MASQUERADE
root@debian:/home/franciscojesus#
```

Squid permite un gran número de configuraciones y opciones, algunas de las más típicas son las siguientes:

Existen un gran número de opciones, de los cuales configuraremos los siguientes:

- Al menos una Lista de Control de Acceso
- Al menos una Regla de Control de Acceso
- `http_port`
- `cache_dir`
- `error_directory`, sólo si va a personalizar mensajes de error.

En el archivo de configuración podemos ver el puerto de escucha de Squid.

```
Abrir [icon] squid.conf /etc/squid
# require-proxy-header
#       Require PROXY protocol version 1 or 2 connections.
#       The proxy_protocol access is required to whitelist
#       downstream proxies which can be trusted.
#
#       If you run Squid on a dual-homed machine with an internal
#       and an external interface we recommend you to specify the
#       internal address:port in http_port. This way Squid will only be
#       visible on the internal address.
#
#
# Squid normally listens to port 3128
http_port 3128
# TAG: https_port
# Note: This option is only available if Squid is rebuilt with the
#       --with-openssl
#
# Usage: [ip:]port cert=certificate.pem [key=key.pem] [mode] [options...]
```

Squid permite personalizar la memoria cache que almacenara.

```
Abrir [icon] *squid.conf /etc/squid
# 4 KB blocks allocated. In-Transit objects take the highest
# priority.
#
# In-transit objects have priority over the others. When
# additional space is needed for incoming data, negative-cached
# and hot objects will be released. In other words, the
# negative-cached and hot objects will fill up any unused space
# not needed for in-transit objects.
#
# If circumstances require, this limit will be exceeded.
# Specifically, if your incoming request rate requires more than
# 'cache_mem' of memory to hold in-transit objects, Squid will
# exceed this limit to satisfy the new requests. When the load
# decreases, blocks will be freed until the high-water mark is
# reached. Thereafter, blocks will be used to store hot
# objects.
#
# If shared memory caching is enabled, Squid does not use the shared
# cache space for in-transit objects, but they still consume as much
# local memory as they need. For more details about the shared memory
# cache, see memory_cache_shared.
#Default:
cache_mem 256 MB
# TAG: maximum_object_size_in_memory (bytes)
# Objects greater than this size will not be attempted to kept in
# the memory cache. This should be set high enough to keep objects
# accessed frequently in memory to improve performance whilst low
# enough to keep larger objects from hoarding cache_mem.
#Default:
# maximum_object_size_in_memory 512 KB
```

Squid incluye traducción a distintos idiomas de las distintas páginas de error e informativas que son desplegadas en un momento dado durante su operación. Dichas traducciones se pueden encontrar en /usr/share/squid/errors/. Desde la versión 3.0 de Squid, el idioma se detecta automáticamente a partir del navegador utilizado por el usuario. Es innecesario modificar opción alguna, salvo que se haya personalizado los mensajes, en cuyo caso conviene utilizar una ruta distinta a la del idioma utilizado para evitar ser sobre escritos los archivos después de actualizar el sistema.

```
franciscojesus@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@debian:/home/franciscojesus# ls /usr/share/squid/errors/
af ar-sy Danish en-ie es-cr es-ve fr-mc it-ch ms-my ru sr-latn uk zh-hk
ar ar-tn de en-in es-do et German it-it nl ru-ru sr-latn-cs Ukrainian-1251 zh-mo
ar-ae ar-ye de-at en-jm es-ec et-ee Greek ja nl-nl Russian-1251 sr-latn-me Ukrainian-koi8-u zh-sg
ar-bh az de-ch en-nz es-es fa he ja-jp oc Russian-koi8-r sr-latn-rs Ukrainian-utf8 zh-tw
ar-dz az-az de-de en-ph es-gt fa-fa Hebrew Japanese pl Serbian sr-rs uk-ua
ar-eg Azerbaijani de-li en-sg es-hn fa-ir he-il ka-ge pl-pl sk sr-sp uz
ar-iq bg de-lu en-tt es-mx fi hu ko Polish sk-sk sv vi
ar-jo bg-bg Dutch en-uk es-ni fi-fi hu-hu ko-kp Portuguese sl sv-fi vi-vn
ar-kw Bulgarian el en-us es-pa Finnish Hungarian ko-kr pt Slovak sv-se zh-cn
ar-lb ca el-gr en-za es-pe fr hy Korean pt-br sl-si Swedish zh-hans
ar-ly Catalan en en-zw es-pr fr-be hy-am Lithuanian pt-bz Spanish templates zh-hans-cn
ar-ma cs en-au es es-py fr-ca hy-armn lt pt-pt sr th zh-hans-sg
Armenian cs-cz en-bz es-ar es-sv fr-ch id lt-lt ro sr-cyrl th-th zh-hant
ar-om Czech en-ca es-bo Estonian French id-id lv Romanian sr-cyrl-cs tr zh-hant-hk
ar-qa da en-gb es-cl es-us fr-fr it lv-lv ro-md sr-cyrl-me tr-tr zh-hant-mo
ar-sa da-dk English es-co es-uy fr-lu Italian ms ro-ro sr-cyrl-rs Turkish zh-hant-tw
root@debian:/home/franciscojesus#
```

```
franciscojesus@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@debian:/home/franciscojesus# cat /usr/share/squid/errors/es/ERR_ACCESS_DENIED

<html><head>
<meta type="copyright" content="Copyright (C) 1996-2015 The Squid Software Foundation and contributors">
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>ERROR: EL URL solicitado no se ha podido conseguir</title>
<style type="text/css"><!--
%l
body
:lang(fa) { direction: rtl; font-size: 100%; font-family: Tahoma, Roya, sans-serif; float: right; }
:lang(he) { direction: rtl; }
--></style>
</head><body id="%c">
<div id="titles">
<h1>ERROR</h1>
<h2>EL URL solicitado no se ha podido conseguir</h2>
</div>
<hr>
<div id="content">
<p>Se encontró el siguiente error al intentar recuperar la dirección URL: <a href="%U">%U</a></p>
<blockquote id="error">
<p><b>Acceso Denegado</b></p>
</blockquote>
<p>La configuración de control de acceso evita que su solicitud sea permitida en este momento. Por favor, póngase en contacto con su proveedor de servicios si cree que es to es incorrecto.</p>
<p>Su administrador del caché; es <a href="mailto:%W">%W</a>.</p>
</div>
</hr>
```

- Archivos de log.

Los registros son una valiosa fuente de información sobre las cargas de trabajo y el rendimiento de Squid. Los registros registran no solo la información de acceso, sino también los errores de configuración del sistema y el consumo de recursos.

- **/var/log/squid/access.log:** la mayoría de los programas de análisis de archivos de registro se basan en las entradas de access.log. Puede usar este archivo para averiguar quién está usando el servidor squid y qué están haciendo, etc.
- **/var/log/squid/cache.log:** el archivo cache.log contiene los mensajes de depuración y error que genera Squid.
- **/var/log/squid/store.log:** el archivo store.log cubre los objetos actualmente guardados en el disco o los eliminados. Como una especie de registro de transacciones, generalmente se utiliza con fines de depuración.

Podemos ver información sobre los logs de Squid.

```
franciscojesus@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@debian:/var/log/squid# cat cache.log
2020/02/13 19:21:10 kid1| Set Current Directory to /var/spool/squid
2020/02/13 19:21:10 kid1| Starting Squid Cache version 3.5.23 for x86_64-pc-linux-gnu...
2020/02/13 19:21:10 kid1| Service Name: squid
2020/02/13 19:21:10 kid1| Process ID 2403
2020/02/13 19:21:10 kid1| Process Roles: worker
2020/02/13 19:21:10 kid1| With 65535 file descriptors available
2020/02/13 19:21:10 kid1| Initializing IP Cache...
2020/02/13 19:21:10 kid1| DNS Socket created at [::], FD 6
2020/02/13 19:21:10 kid1| DNS Socket created at 0.0.0.0, FD 8
2020/02/13 19:21:10 kid1| Adding nameserver 8.8.8.8 from /etc/resolv.conf
2020/02/13 19:21:10 kid1| Logfile: opening log daemon:/var/log/squid/access.log
2020/02/13 19:21:10 kid1| Logfile Daemon: opening log /var/log/squid/access.log
2020/02/13 19:21:10 kid1| Local cache digest enabled; rebuild/rewrite every 3600/3600 sec
2020/02/13 19:21:10 kid1| Store logging disabled
2020/02/13 19:21:10 kid1| Swap maxSize 0 + 262144 KB, estimated 20164 objects
2020/02/13 19:21:10 kid1| Target number of buckets: 1008
2020/02/13 19:21:10 kid1| Using 8192 Store buckets
2020/02/13 19:21:10 kid1| Max Mem size: 262144 KB
2020/02/13 19:21:10 kid1| Max Swap size: 0 KB
2020/02/13 19:21:10 kid1| Using Least Load store dir selection
2020/02/13 19:21:10 kid1| Set Current Directory to /var/spool/squid
2020/02/13 19:21:10 kid1| Finished loading MIME types and icons.
2020/02/13 19:21:10 kid1| HTTP Disabled.
```

Descomentaremos las siguientes líneas en el archivo de configuración de squid para activar el access.log

```
Abrir [icon] *squid.conf
/etc/squid

#
# udp To send each log line as text data to a UDP receiver.
# Place: The destination host name or IP and port.
# Place Format: //host:port
#
#
# tcp To send each log line as text data to a TCP receiver.
# Lines may be accumulated before sending (see buffered_logs).
# Place: The destination host name or IP and port.
# Place Format: //host:port
#
# Default:
# access_log daemon:/var/log/squid/access.log squid
#Default:
access_log daemon:/var/log/squid/access.log squid
# TAG: icap_log
# TRAP_log files record TCP transaction summaries one line per
```

Cuando acceden usuarios, podemos verlo en el archivo de access.log

```
franciscojesus@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
franciscojesus@debian:~$ sudo cat /var/log/squid/access.log | tail -20
158126300.093 11022 192.168.100.120 TCP_TUNNEL/200 46998 CONNECT apis.google.com:443 frank HIER DIRECT/216.58.201.174 -
158126300.093 11022 192.168.100.120 TCP_TUNNEL/200 46998 CONNECT apis.google.com:443 frank HIER DIRECT/216.58.201.174 -
158126300.093 9854 192.168.100.120 TCP_TUNNEL/200 4759 CONNECT accounts.google.com:443 frank HIER DIRECT/216.58.211.45 -
158126300.093 9854 192.168.100.120 TCP_TUNNEL/200 4759 CONNECT accounts.google.com:443 frank HIER DIRECT/216.58.211.45 -
158126300.093 6338 192.168.100.120 TCP_TUNNEL/200 8350 CONNECT abs.twimg.com:443 frank HIER DIRECT/151.101.120.159 -
158126300.093 6338 192.168.100.120 TCP_TUNNEL/200 8350 CONNECT abs.twimg.com:443 frank HIER DIRECT/151.101.120.159 -
158126300.093 5318 192.168.100.120 TCP_TUNNEL/200 369036 CONNECT pbs.twimg.com:443 frank HIER DIRECT/192.229.233.50 -
158126300.093 5318 192.168.100.120 TCP_TUNNEL/200 369036 CONNECT pbs.twimg.com:443 frank HIER DIRECT/192.229.233.50 -
158126300.093 7527 192.168.100.120 TCP_TUNNEL/200 4644 CONNECT platform.twitter.com:443 frank HIER DIRECT/93.184.220.66 -
158126300.093 7527 192.168.100.120 TCP_TUNNEL/200 4644 CONNECT platform.twitter.com:443 frank HIER DIRECT/93.184.220.66 -
158126300.093 7788 192.168.100.120 TCP_TUNNEL/200 69108 CONNECT platform.twitter.com:443 frank HIER DIRECT/93.184.220.66 -
158126300.093 7788 192.168.100.120 TCP_TUNNEL/200 69108 CONNECT platform.twitter.com:443 frank HIER DIRECT/93.184.220.66 -
158126303.169 0 192.168.100.120 TCP_DENIED/407 4066 CONNECT www.bing.com:443 - HIER NONE/- text/html
158126303.169 0 192.168.100.120 TCP_DENIED/407 4066 CONNECT www.bing.com:443 - HIER NONE/- text/html
158126304.610 0 192.168.100.120 TCP_DENIED/407 4066 CONNECT www.bing.com:443 - HIER NONE/- text/html
158126304.610 0 192.168.100.120 TCP_DENIED/407 4066 CONNECT www.bing.com:443 - HIER NONE/- text/html
158126306.709 0 192.168.100.120 TCP_DENIED/407 4238 GET http://img.s-msn-com.akamaized.net/tenant/amp/entityid/BBZX6ze.img? - HIER NONE/- text/html
158126306.709 0 192.168.100.120 TCP_DENIED/407 4238 GET http://img.s-msn-com.akamaized.net/tenant/amp/entityid/BBZX6ze.img? - HIER NONE/- text/html
158126306.711 0 192.168.100.120 TCP_DENIED/407 4238 GET http://img.s-msn-com.akamaized.net/tenant/amp/entityid/BBZX6ze.img? - HIER NONE/- text/html
158126306.711 0 192.168.100.120 TCP_DENIED/407 4238 GET http://img.s-msn-com.akamaized.net/tenant/amp/entityid/BBZX6ze.img? - HIER NONE/- text/html
franciscojesus@debian:~$
```

Podemos ver si se le denegó el acceso a un sitio, el sitio que es, la hora, el usuario...

```
franciscojesus@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
158126030.937 132 192.168.100.121 TCP_MISS/200 823 POST http://ocsp.pki.goog/gts101 frank HIER DIRECT/172.217.17.3 application/ocsp-response
158126032.125 140 192.168.100.121 TCP_MISS/200 823 POST http://ocsp.pki.goog/gts101 frank HIER DIRECT/172.217.17.3 application/ocsp-response
158126032.125 140 192.168.100.121 TCP_MISS/200 823 POST http://ocsp.pki.goog/gts101 frank HIER DIRECT/172.217.17.3 application/ocsp-response
158126032.330 135 192.168.100.121 TCP_MISS/200 823 POST http://ocsp.pki.goog/gts101 frank HIER DIRECT/172.217.17.3 application/ocsp-response
158126032.330 135 192.168.100.121 TCP_MISS/200 823 POST http://ocsp.pki.goog/gts101 frank HIER DIRECT/172.217.17.3 application/ocsp-response
158126032.690 130 192.168.100.121 TCP_MISS/200 823 POST http://ocsp.pki.goog/gts101 frank HIER DIRECT/172.217.17.3 application/ocsp-response
158126032.690 130 192.168.100.121 TCP_MISS/200 823 POST http://ocsp.pki.goog/gts101 frank HIER DIRECT/172.217.17.3 application/ocsp-response
158126032.835 114 192.168.100.121 TCP_TUNNEL/200 20486 CONNECT fonts.gstatic.com:443 frank HIER DIRECT/216.58.201.163 -
158126032.835 114 192.168.100.121 TCP_TUNNEL/200 20486 CONNECT fonts.gstatic.com:443 frank HIER DIRECT/216.58.201.163 -
158126035.519 143 192.168.100.121 TCP_MISS/200 824 POST http://ocsp.pki.goog/gts101 frank HIER DIRECT/172.217.17.3 application/ocsp-response
158126035.519 143 192.168.100.121 TCP_MISS/200 824 POST http://ocsp.pki.goog/gts101 frank HIER DIRECT/172.217.17.3 application/ocsp-response
158126040.441 0 192.168.100.121 TCP_DENIED/403 3985 CONNECT www.marca.com:443 frank HIER NONE/- text/html
158126040.441 0 192.168.100.121 TCP_DENIED/403 3985 CONNECT www.marca.com:443 frank HIER NONE/- text/html
158126045.551 0 192.168.100.121 TCP_DENIED/403 4184 GET http://www.marca.com/ frank HIER NONE/- text/html
158126045.551 0 192.168.100.121 TCP_DENIED/403 4184 GET http://www.marca.com/ frank HIER NONE/- text/html
158126045.627 0 192.168.100.121 TCP_MEM_HIT/200 13097 GET http://debian:3128/squid-internal-static/icons/SN.png frank HIER NONE/- image/png
158126045.627 0 192.168.100.121 TCP_MEM_HIT/200 13057 GET http://debian:3128/squid-internal-static/icons/SN.png frank HIER_NONE/- image/png
158126046.260 0 192.168.100.121 TCP_DENIED/403 4118 GET http://www.marca.com/favicon.ico frank HIER NONE/- text/html
```

De igual forma, podemos ver si se le permitió el acceso a un sitio, su hora, el usuario...

```
franciscojesus@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
158126116.218 83509 192.168.100.121 TCP_TUNNEL/200 91207 CONNECT fonts.gstatic.com:443 frank HIER DIRECT/216.58.201.163 -
158126116.221 83824 192.168.100.121 TCP_TUNNEL/200 99282 CONNECT apis.google.com:443 frank HIER DIRECT/216.58.201.174 -
158126116.221 84034 192.168.100.121 TCP_TUNNEL/200 299663 CONNECT www.gstatic.com:443 frank HIER DIRECT/216.58.201.163 -
158126116.221 84127 192.168.100.121 TCP_TUNNEL/200 5764 CONNECT id.google.com:443 frank HIER DIRECT/172.217.16.227 -
158126116.221 84338 192.168.100.121 TCP_TUNNEL/200 89584 CONNECT consent.google.com:443 frank HIER DIRECT/216.58.211.46 -
158126116.221 83824 192.168.100.121 TCP_TUNNEL/200 99282 CONNECT apis.google.com:443 frank HIER DIRECT/216.58.201.174 -
158126116.221 84034 192.168.100.121 TCP_TUNNEL/200 299663 CONNECT www.gstatic.com:443 frank HIER DIRECT/216.58.201.163 -
158126116.221 84127 192.168.100.121 TCP_TUNNEL/200 5764 CONNECT id.google.com:443 frank HIER DIRECT/172.217.16.227 -
158126116.221 84338 192.168.100.121 TCP_TUNNEL/200 89584 CONNECT consent.google.com:443 frank HIER DIRECT/216.58.211.46 -
158126116.225 85474 192.168.100.121 TCP_TUNNEL/200 1232743 CONNECT www.google.com:443 frank HIER DIRECT/172.217.16.228 -
158126116.225 85474 192.168.100.121 TCP_TUNNEL/200 1232743 CONNECT www.google.com:443 frank HIER DIRECT/172.217.16.228 -
158126116.227 86607 192.168.100.121 TCP_TUNNEL/200 4534 CONNECT incoming.telemetry.mozilla.org:443 frank HIER DIRECT/34.210.237.85 -
158126116.227 86607 192.168.100.121 TCP_TUNNEL/200 4534 CONNECT incoming.telemetry.mozilla.org:443 frank HIER DIRECT/34.210.237.85 -
158126116.227 86642 192.168.100.121 TCP_TUNNEL/200 4534 CONNECT incoming.telemetry.mozilla.org:443 frank HIER DIRECT/34.210.237.85 -
158126116.227 86642 192.168.100.121 TCP_TUNNEL/200 4534 CONNECT incomina.telemetry.mozilla.org:443 frank HIER DIRECT/34.210.237.85 -
```

Podemos ver en el cache.log como se va llenando según lo vamos usando. Podemos ver como registro que hemos abierto el archivo.

```
franciscojesus@debian: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
franciscojesus@debian:~$ sudo cat /var/log/squid/cache.log | tail -30  
2020/02/13 21:41:46 kid1| With 65535 file descriptors available  
2020/02/13 21:41:46 kid1| Initializing IP Cache...  
2020/02/13 21:41:46 kid1| DNS Socket created at [::], FD 6  
2020/02/13 21:41:46 kid1| DNS Socket created at 0.0.0.0, FD 8  
2020/02/13 21:41:46 kid1| Adding nameserver 0.0.0.0 from /etc/resolv.conf  
2020/02/13 21:41:46 kid1| helperOpenServers: Starting 0/20 'basic ncsa auth' processes  
2020/02/13 21:41:46 kid1| helperOpenServers: No 'basic ncsa auth' processes needed.  
2020/02/13 21:41:46 kid1| Logfile: opening log daemon:/var/log/squid/access.log  
2020/02/13 21:41:46 kid1| Logfile Daemon: opening log /var/log/squid/access.log  
2020/02/13 21:41:46 kid1| Logfile: opening log daemon:/var/log/squid/access.log  
2020/02/13 21:41:46 kid1| Logfile Daemon: opening log /var/log/squid/access.log  
2020/02/13 21:41:46 kid1| Local cache digest enabled; rebuild/rewrite every 3600/3600 sec  
2020/02/13 21:41:46 kid1| Store logging disabled  
2020/02/13 21:41:46 kid1| Swap maxSize 0 + 262144 KB, estimated 20164 objects  
2020/02/13 21:41:46 kid1| Target number of buckets: 1008  
2020/02/13 21:41:46 kid1| Using 8192 Store buckets  
2020/02/13 21:41:46 kid1| Max Mem size: 262144 KB  
2020/02/13 21:41:46 kid1| Max Swap size: 0 KB  
2020/02/13 21:41:46 kid1| Using Least Load store dir selection  
2020/02/13 21:41:46 kid1| Set Current Directory to /var/spool/squid  
2020/02/13 21:41:47 kid1| Finished loading MIME types and icons.  
2020/02/13 21:41:47 kid1| HTTP Disabled.  
2020/02/13 21:41:47 kid1| Pinger socket opened on FD 15  
2020/02/13 21:41:47 kid1| Squid plugin modules loaded: 0  
2020/02/13 21:41:47 kid1| Adaptation HTTP Socket connections is off.  
2020/02/13 21:41:47 kid1| Accepting HTTP Socket connections at local=[::]:3128 remote=[::] FD 13 flags=9  
2020/02/13 21:41:47 kid1| pinger: Initialising ICMP pinger ...  
2020/02/13 21:41:47 kid1| pinger: ICMP socket opened.  
2020/02/13 21:41:47 kid1| pinger: ICMPv6 socket opened  
2020/02/13 21:41:47 kid1| storeLateRelease: released 0 objects  
franciscojesus@debian:~$
```

De igual manera, podemos ver a las web que se accedieron sin mucha información.

```
franciscojesus@debian: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
2020/02/13 21:39:03 kid1| storeDirWriteCleanLogs: Starting...  
2020/02/13 21:39:03 kid1| Finished. Wrote 0 entries.  
2020/02/13 21:39:03 kid1| Took 0.00 seconds ( 0.00 entries/sec).  
CPU Usage: 1.180 seconds = 0.164 user + 1.016 sys  
Maximum Resident Size: 132528 KB  
Page faults with physical i/o: 0  
2020/02/13 21:39:03 kid1| Logfile: closing log daemon:/var/log/squid/access.log  
2020/02/13 21:39:03 kid1| Logfile Daemon: closing log daemon:/var/log/squid/access.log  
2020/02/13 21:39:03 kid1| Logfile: closing log daemon:/var/log/squid/access.log  
2020/02/13 21:39:03 kid1| Logfile Daemon: closing log daemon:/var/log/squid/access.log  
2020/02/13 21:39:03 kid1| Open FD UNSTARTED 6 DNS Socket IPv6  
2020/02/13 21:39:03 kid1| Open FD READ/WRITE 8 DNS Socket IPv4  
2020/02/13 21:39:03 kid1| Open FD UNSTARTED 9 IPC UNIX STREAM Parent  
2020/02/13 21:39:03 kid1| Open FD UNSTARTED 11 IPC UNIX STREAM Parent  
2020/02/13 21:39:03 kid1| Open FD READ/WRITE 14 basic ncsa auth #1  
2020/02/13 21:39:03 kid1| Open FD READ/WRITE 23 Idle server: 216.58.204.147:80/www.iesgregorioprieto.com  
2020/02/13 21:39:03 kid1| Open FD READ/WRITE 25 Idle server: 216.58.204.147:80/www.iesgregorioprieto.com  
2020/02/13 21:39:03 kid1| Open FD READ/WRITE 27 Idle server: 216.58.204.147:80/www.iesgregorioprieto.com  
2020/02/13 21:39:03 kid1| Open FD READ/WRITE 35 Idle server: 173.194.222.94:80/csi.gstatic.com  
2020/02/13 21:39:03 kid1| Squid Cache (Version 3.5.23): Exiting normally.  
2020/02/13 21:41:46 kid1| Set Current Directory to /var/spool/squid  
2020/02/13 21:41:46 kid1| Starting Squid Cache version 3.5.23 for x86_64-pc-linux-gnu...  
2020/02/13 21:41:46 kid1| Service Name: squid  
2020/02/13 21:41:46 kid1| Process ID 919  
2020/02/13 21:41:46 kid1| Process Roles: worker  
2020/02/13 21:41:46 kid1| With 65535 file descriptors available
```

- Autenticación de usuarios.

Es muy útil el poder establecer un sistema de autenticación para poder acceder hacia Internet, pues esto permite controlar quienes si y quienes no accederán a Internet sin importar desde que máquina de la red local lo hagan. Sera de modo tal que tendremos un doble control, primero por dirección IP y segundo por nombre de usuario y contraseña.

Se requerirá la creación previa de un archivo que contendrá los nombres de usuarios y sus correspondientes contraseñas (cifradas). El archivo puede localizarse en cualquier lugar del sistema, con la única condición que sea asequible para el usuario squid.

```
Archivo Editar Ver Buscar Terminal Ayuda
root@debian:/var/log/squid# touch /etc/squid/claves
root@debian:/var/log/squid# █
```

Salvo que vaya a utilizarse un guion a través del servidor web para administrar las contraseñas, como medida de seguridad, este archivo debe tener atributos de lectura y escritura sólo para el usuario squid:

```
Archivo Editar Ver Buscar Terminal Ayuda
root@debian:/etc/squid# chmod 600 /etc/squid/claves
root@debian:/etc/squid# █
```

A continuación, deberemos dar de alta las cuentas que sean necesarias, utilizando el mandato htpasswd -mismo que viene incluido en el paquete httpd-2.0.x-. Si no lo tenemos, deberemos instalar Apache2.

```
franciscojesus@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@debian:/etc/squid# htpasswd /etc/squid/claves franciscojesus
New password:
Re-type new password:
Adding password for user franciscojesus
root@debian:/etc/squid#
```

Podemos ver el contenido del fichero.

```
Archivo Editar Ver Buscar Terminal Ayuda
root@debian:/etc/squid# cat /etc/squid/claves
franciscojesus:$apr1$KPA4K/zC$D4AxPl6ksXgtTsTfPXnra/
root@debian:/etc/squid# █
```

Todas las cuentas que se den de alta de este modo son independientes a las ya existentes en el sistema. Al dar de alta una cuenta o cambiar una contraseña lo estará haciendo EXCLUSIVAMENTE para el acceso al servidor Proxy. Las cuentas son independientes a las que se tengan existentes en el sistema como serían shell, correo y Samba.

Ahora iremos al archivo de configuración de squid (squid.conf). Lo siguiente será especificar qué programa de autenticación se utilizará. Buscaremos la sección que corresponde a la etiqueta auth_param basic program. De modo predeterminado esta opción viene desactivada. Consideraremos que basic_ncsa_auth se localiza en /usr/lib/squid/basic_ncsa_auth, añadiremos lo siguiente:

```
Abrir [icon] *squid.conf /etc/squid
# settings for each scheme:
#
##auth_param negotiate program <uncomment and complete this line to activate>
##auth_param negotiate children 20 startup=0 idle=1
##auth_param negotiate keep_alive on
##
##auth_param digest program <uncomment and complete this line to activate>
##auth_param digest children 20 startup=0 idle=1
##auth_param digest realm Squid proxy-caching web server
##auth_param digest nonce garbage_interval 5 minutes
##auth_param digest nonce_max_duration 30 minutes
##auth_param digest nonce_max_count 50
##
##auth_param ntlm program <uncomment and complete this line to activate>
##auth_param ntlm children 20 startup=0 idle=1
##auth_param ntlm keep_alive on
##
##auth_param basic program <uncomment and complete this line>
##auth_param basic children 5 startup=5 idle=1
##auth_param basic realm Squid proxy-caching web server
##auth_param basic credentialsttl 2 hours

auth_param basic program /usr/lib/squid/basic_ncsa_auth /etc/squid/claves
```

/usr/lib/squid/basic_ncsa_auth corresponde a la localización del programa para autenticar y especificando como argumento el archivo/etc/squid/claves, el cual corresponde al que contiene los nombres de usuario y sus respectivas contraseñas.

Deberemos especificar una lista de control de acceso denominada passwd la cual se configurará para utilizar de modo obligatorio la autenticación para poder acceder a Squid. Debe localizarse la sección de Listas de Control de Acceso y añadirse la siguiente línea.

```
Abrir [icon] *squid.conf /etc/squid
acl Safe_ports port 21 # ftp
acl Safe_ports port 443 # https
acl Safe_ports port 70 # gopher
acl Safe_ports port 210 # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280 # http-mgmt
acl Safe_ports port 488 # gss-http
acl Safe_ports port 591 # filemaker
acl Safe_ports port 777 # multiling http
acl CONNECT method CONNECT

acl all src 0.0.0.0/0
acl manager proto cache_object
acl localhost src 127.0.0.1/8

acl localnet src 192.168.100.0/24
acl password proxy_auth REQUIRED
```

Procederemos entonces a modificar la regla de control de accesos que ya se tenía para permitir el acceso a Internet. Ahora, añadiremos passwd, la definición de la Lista de Control de Acceso que requiere utilizar contraseña a la regla actual, de modo que quede como se muestra a continuación.

```
Abrir [icon] squid.conf /etc/squid
# one who can access services on localhost is a local user
#http_access deny to_localhost

#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#

# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
http_access allow localhost
http_access allow localnet password

# And finally deny all other access to this proxy
http_access deny all

# TAG: adapted http_access
# Allowing or Denying access based on defined access lists
#
```

Reiniciaremos Squid.

```
franciscojesus@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@debian:/etc/squid# service squid restart
root@debian:/etc/squid# service squid status
● squid.service - LSB: Squid HTTP Proxy version 3.x
   Loaded: loaded (/etc/init.d/squid; generated; vendor preset: enabled)
   Active: active (running) since Thu 2020-02-13 20:21:00 CET; 3s ago
     Docs: man:systemd-sysv-generator(8)
   Process: 2997 ExecStop=/etc/init.d/squid stop (code=exited, status=0/SUCCESS)
   Process: 3023 ExecStart=/etc/init.d/squid start (code=exited, status=0/SUCCESS)
 Main PID: 3065 (squid)
   Tasks: 5 (limit: 4915)
  CGroup: /system.slice/squid.service
          └─3063 /usr/sbin/squid -YC -f /etc/squid/squid.conf
            └─3065 (squid-1) -YC -f /etc/squid/squid.conf
              └─3066 (logfile-daemon) /var/log/squid/access.log
                └─3067 (logfile-daemon) /var/log/squid/access.log
                  └─3068 (pinger)

feb 13 20:21:00 debian squid[3023]: 2020/02/13 20:21:00] WARNING: You should probably remove '127.0.0.1' from the ACL named 'localhost'
feb 13 20:21:00 debian squid[3023]: 2020/02/13 20:21:00] WARNING: (B) '127.0.0.1' is a subnetwork of (A) '127.0.0.0/8'
feb 13 20:21:00 debian squid[3023]: 2020/02/13 20:21:00] WARNING: because of this '127.0.0.0/8' is ignored to keep splay tree searching predictable
feb 13 20:21:00 debian squid[3023]: 2020/02/13 20:21:00] WARNING: You should probably remove '127.0.0.1' from the ACL named 'localhost'
feb 13 20:21:00 debian squid[3063]: Squid Parent: will start 1 kids
feb 13 20:21:00 debian squid[3063]: Squid Parent: (squid-1) process 3065 started
feb 13 20:21:00 debian squid[3023]: .
feb 13 20:21:00 debian systemd[1]: squid.service: PID file /var/run/squid.pid not readable (yet?) after start: No such file or directory
feb 13 20:21:00 debian systemd[1]: squid.service: Supervising process 3065 which is not our child. We'll most likely not notice when it exits.
feb 13 20:21:00 debian systemd[1]: Started LSB: Squid HTTP Proxy version 3.x.
root@debian:/etc/squid#
```

- Filtros web mediante listas de control de acceso.

Una vez realizado esto, crearemos unas reglas para denegar el acceso a webs que nosotros queramos.

Podemos restringir web por expresiones regulares. Lo primero que haremos es definir un archivo en el que crear la lista de expresiones regulares.

```
franciscojesus@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@debian:/etc/squid# mkdir /etc/squid/listas
root@debian:/etc/squid# nano /etc/squid/listas/expreg-denegadas
```

```
franciscojesus@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
GNU nano 2.7.4                                Archivo: /etc/squid/listas/expreg-denegadas
adult
celebri
mp3
otrositioindeseable.com
playstation
porn
sex
sitioindeseable.com
taringa
torrent
warez
wii
```

Ahora editaremos el archivo de configuración de squid. Añadiremos una lista de control, denominada expreg-denegadas, de acceso tipo url_regex (expresiones regulares del URL), que defina la lista en el archivo /etc/squid/listas/expreg-denegadas.

```
Abrir [icon] *squid.conf /etc/squid
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280      # http-mgmt
acl Safe_ports port 488      # gss-http
acl Safe_ports port 591      # filemaker
acl Safe_ports port 777      # multiling http
acl CONNECT method CONNECT

acl all src 0.0.0.0/0
acl manager proto cache object
acl localhost src 127.0.0.1/8

acl localnet src 192.168.100.0/24
acl password proxy_auth REQUIRED

acl expreg-denegadas url_regex "/etc/squid/listas/expreg-denegadas"
|

# TAG: proxy_protocol_access
# Determine which client proxies can be trusted to provide correct
# information regarding real client IP address using PROXY protocol.
# Requests may pass through a chain of several other proxies
```

A continuación, especificaremos una Regla de Control de Acceso existente agregando con un símbolo de ! que se denegará el acceso a la Lista de Control de Acceso denominada expreg-denegadas.

La regla anterior permite el acceso a la Lista de Control de Acceso denominada localnet, pero le niega el acceso a todo lo que coincida con lo especificado en la Lista de Control de Acceso denominada expreg-denegadas.

```
Abrir [icon] *squid.conf /etc/squid
http_access deny manager

# We strongly recommend the following be uncommented to protect innocent
# web applications running on the proxy server who think the only
# one who can access services on "localhost" is a local user
#http_access deny to_localhost

#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#

# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
http_access allow localnet
http_access allow localnet password !expreg-denegadas|
```

Lo siguiente que haremos ahora es enseñar como realizar lo mismo, pero con dominio. Crearemos un archivo con los dominios a guardar.

```
franciscojesus@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@debian:/etc/squid# gedit /etc/squid/listas/dominios-denegados
root@debian:/etc/squid# cat /etc/squid/listas/dominios-denegados
www.facebook.com
www.twitter.com
plus.google.com
www.marca.com
root@debian:/etc/squid# █
```

Se pueden definir también niveles de dominios superiores o subdominio (o una mezcla de todo).

```
Actividades Editor de textos jue 20:39
Abrir [icon] dominios-denegados /etc/squid/listas
.facebook.com
www.twitter.com
plus.google.com
www.marca.com
.xxx
.xyz
```

Volvemos a editar el archivo de configuración de squid. Añada una lista de control, denominada dominios-denegados, de acceso tipo dstdomain (dominios de destino), que defina a la lista en el archivo /etc/squid/listas/dominios-denegados.

```
Abrir [icon] squid.conf /etc/squid
acl safe_ports port 1825-65535 # unregistered ports
acl Safe_ports port 280      # http-mgmt
acl Safe_ports port 488      # gss-http
acl Safe_ports port 591      # filemaker
acl Safe_ports port 777      # multiling http
acl CONNECT method CONNECT

acl all src 0.0.0.0/0
acl manager proto cache object
acl localhost src 127.0.0.1/8

acl localnet src 192.168.100.0/24
acl password proxy_auth REQUIRED

acl expreg-denegadas url regex "/etc/squid/listas/expreg-denegadas"
acl dominios-denegados dstdomain "/etc/squid/listas/dominios-denegados"

# TCP: proxy protocol access
```

Añadiremos una regla de control de acceso que deniegue el acceso a sitios que estén incluidos en la lista de dominios.

```
Abrir [icon] *squid.conf /etc/squid
http_access deny manager

# We strongly recommend the following be uncommented to protect innocent
# web applications running on the proxy server who think the only
# one who can access services on "localhost" is a local user
#http_access deny to localhost

#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#

# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
http_access allow localhost
http_access allow localnet password !expreg-denegadas !dominios-denegados
```

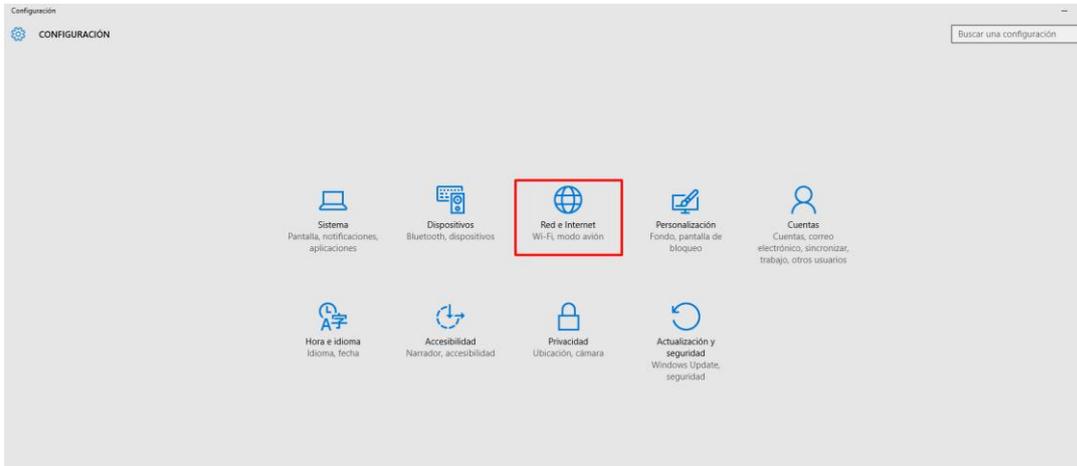
Una vez realizado esto reiniciamos squid y verificamos que funciona.

```
franciscojesus@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@debian:/etc/squid# service squid restart
root@debian:/etc/squid# service squid status
● squid.service - LSB: Squid HTTP Proxy version 3.x
   Loaded: loaded (/etc/init.d/squid; generated; vendor preset: enabled)
   Active: active (running) since Thu 2020-02-13 20:43:07 CET; 59s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 3325 ExecStop=/etc/init.d/squid stop (code=exited, status=0/SUCCESS)
  Process: 3352 ExecStart=/etc/init.d/squid start (code=exited, status=0/SUCCESS)
 Main PID: 3394 (squid)
   Tasks: 5 (limit: 4915)
  CGroup: /system.slice/squid.service
          └─3392 /usr/sbin/squid -YC -f /etc/squid/squid.conf
            └─3394 (squid-1) -YC -f /etc/squid/squid.conf
              └─3395 (logfile-daemon) /var/log/squid/access.log
                └─3396 (logfile-daemon) /var/log/squid/access.log
                  └─3397 (pinger)

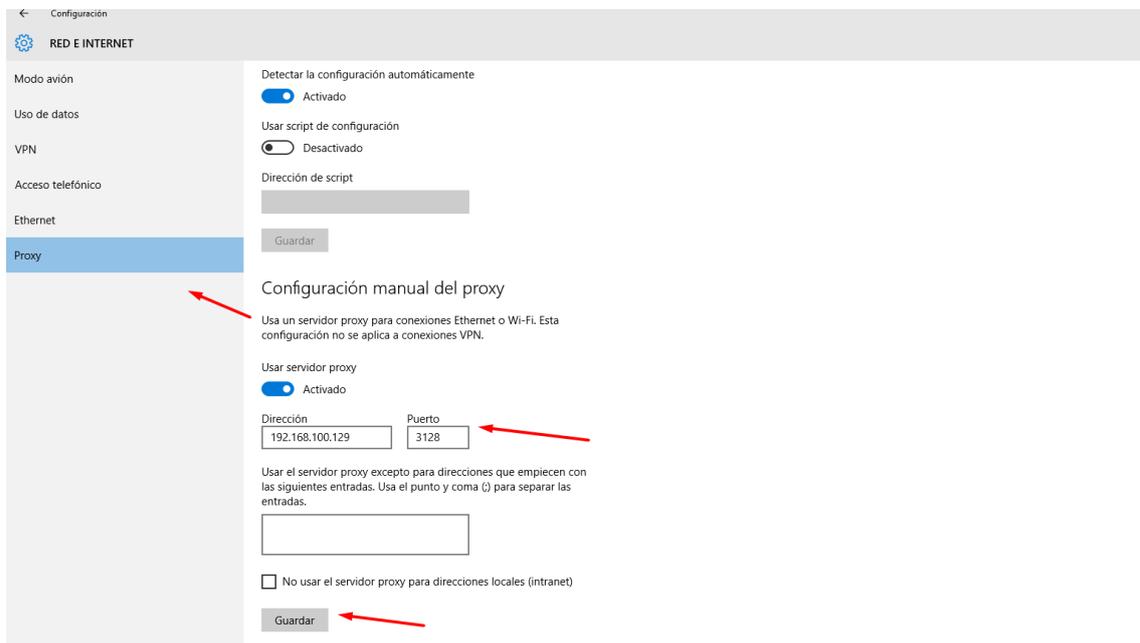
feb 13 20:43:07 debian squid[3352]: 2020/02/13 20:43:07] WARNING: You should probably remove '127.0.0.1' from the ACL named 'localhost'
feb 13 20:43:07 debian squid[3352]: 2020/02/13 20:43:07] WARNING: (B) '127.0.0.1' is a subnetwork of (A) '127.0.0.0/8'
feb 13 20:43:07 debian squid[3352]: 2020/02/13 20:43:07] WARNING: because of this '127.0.0.0/8' is ignored to keep splay tree searching predictable
feb 13 20:43:07 debian squid[3352]: 2020/02/13 20:43:07] WARNING: You should probably remove '127.0.0.1' from the ACL named 'localhost'
feb 13 20:43:07 debian squid[3392]: Squid Parent: will start 1 kids
feb 13 20:43:07 debian squid[3392]: Squid Parent: (squid-1) process 3394 started
feb 13 20:43:07 debian squid[3352]: .
feb 13 20:43:07 debian systemd[1]: squid.service: PID file /var/run/squid.pid not readable (yet?) after start: No such file or directory
feb 13 20:43:07 debian systemd[1]: squid.service: Supervising process 3394 which is not our child. We'll most likely not notice when it exits.
feb 13 20:43:07 debian systemd[1]: Started LSB: Squid HTTP Proxy version 3.x.
root@debian:/etc/squid#
```

Asimismo, demuestre la funcionalidad de dicho servidor proxy en un escenario creado mediante la configuración de un cliente Proxy en GNU/Linux y un cliente Proxy en Windows.

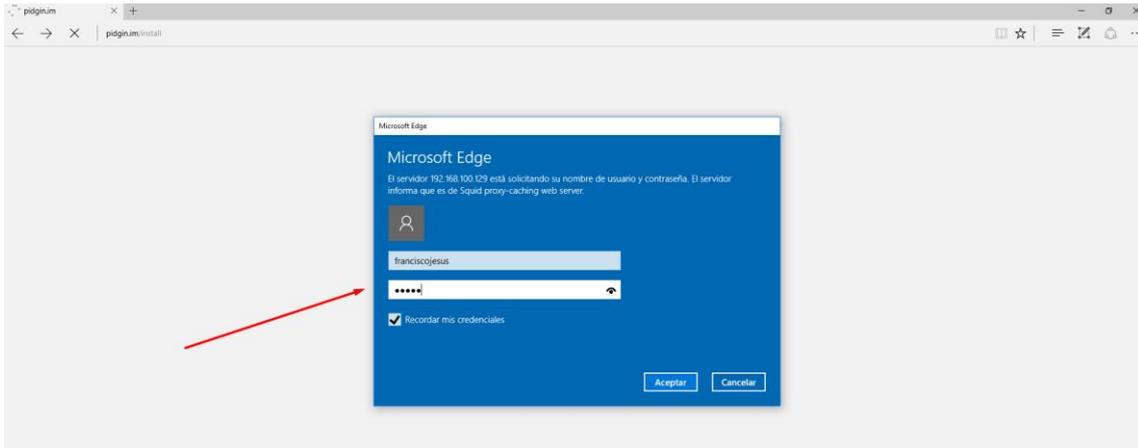
Lo primero que haremos es iniciar una máquina Windows 10. Vamos a *Configuración* → *Red e Internet*.



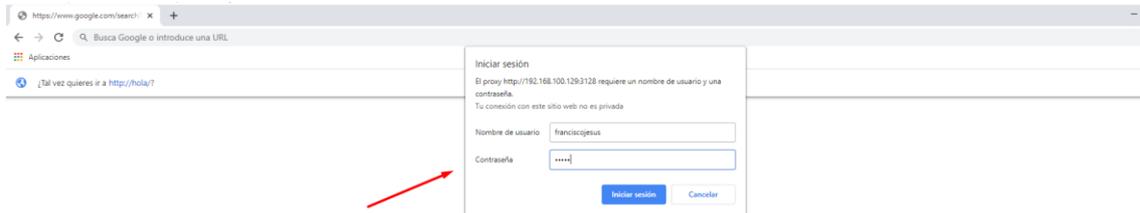
Vamos a Proxy y configuramos el servidor proxy nuestro. Pulsaremos en *guardar* y puede parecer que no hace nada, pero realmente lo guarda.



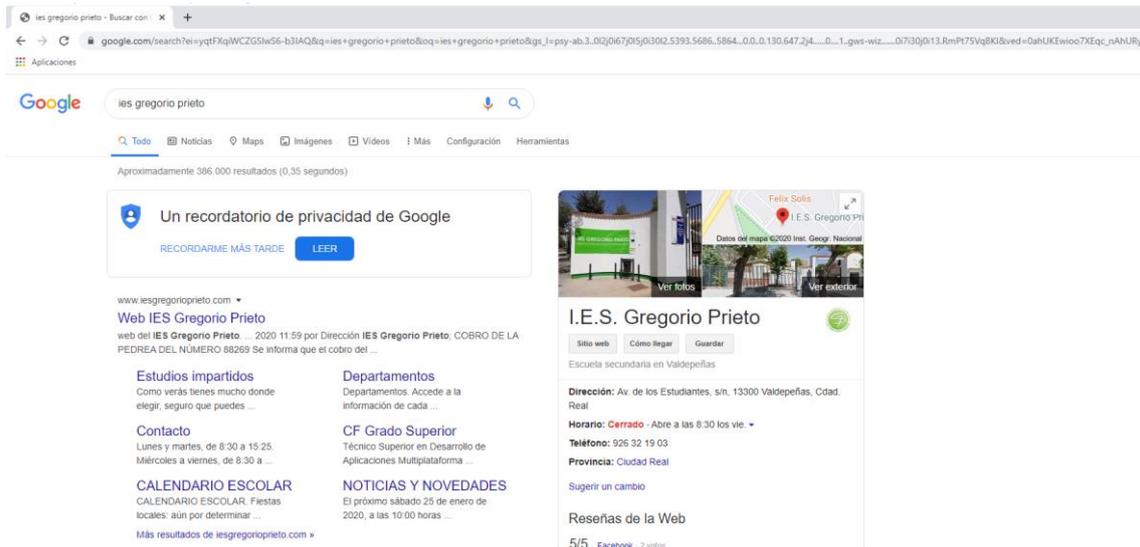
Si entramos en *Edge* vemos como nos pide usuario y contraseña como configuramos en el Proxy Squid.



Nos lo pedirá en cualquier navegador que usemos.



En caso de poner bien el usuario y contraseña vemos como podremos navegar.



No podemos entrar en páginas web bloqueadas. Vemos como nos muestra un error Squid.

ERROR: El URL solicitado no se ha podido conseguir

Se encontró el siguiente error al intentar recuperar la dirección URL: <http://www.marca.com/>

Acceso Denegado

La configuración de control de acceso evita que su solicitud sea permitida en este momento. Por favor, póngase en contacto con su proveedor de servicios si cree que esto es incorrecto. Su administrador del caché es [webmaster](#).

Generado Thu, 13 Feb 2020 20:26:05 GMT por debian (squid/3.5.23)

ERROR: El URL solicitado no se ha podido conseguir

Se encontró el siguiente error al intentar recuperar la dirección URL: <http://otrostitioindeseable.com/>

Acceso Denegado

La configuración de control de acceso evita que su solicitud sea permitida en este momento. Por favor, póngase en contacto con su proveedor de servicios si cree que esto es incorrecto. Su administrador del caché es [webmaster](#).

Generado Thu, 13 Feb 2020 20:26:57 GMT por debian (squid/3.5.23)

En caso de ser un error no reconocido (por ejemplo, bloquear página web HTTPS, Squid no mostrará un error pero no dejará acceder).

No se puede acceder a este sitio web

Es posible que la página web <https://es-es.facebook.com/> esté temporalmente inactiva o que se haya trasladado definitivamente a otra dirección.

ERR_TUNNEL_CONNECTION_FAILED

Podemos ver como funciona también las expresiones regulares (bloquea la palabra mp3).

ERROR: El URL solicitado no se ha podido conseguir

Se encontró el siguiente error al intentar recuperar la dirección URL: <http://mp3-youtube.download/es/your-convertor>

Acceso Denegado

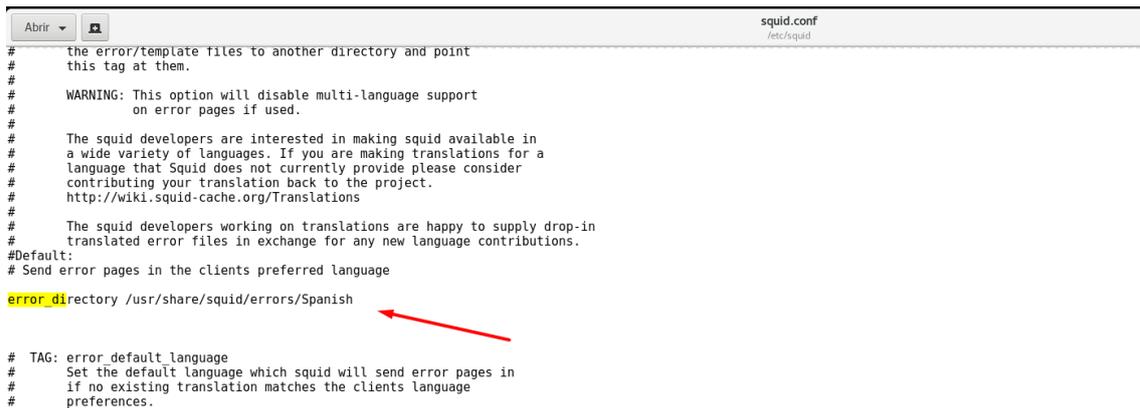
La configuración de control de acceso evita que su solicitud sea permitida en este momento. Por favor, póngase en contacto con su proveedor de servicios si cree que esto es incorrecto. Su administrador del caché es [webmaster](#).

Generado Thu, 13 Feb 2020 20:28:02 GMT por debian (squid/3.5.23)

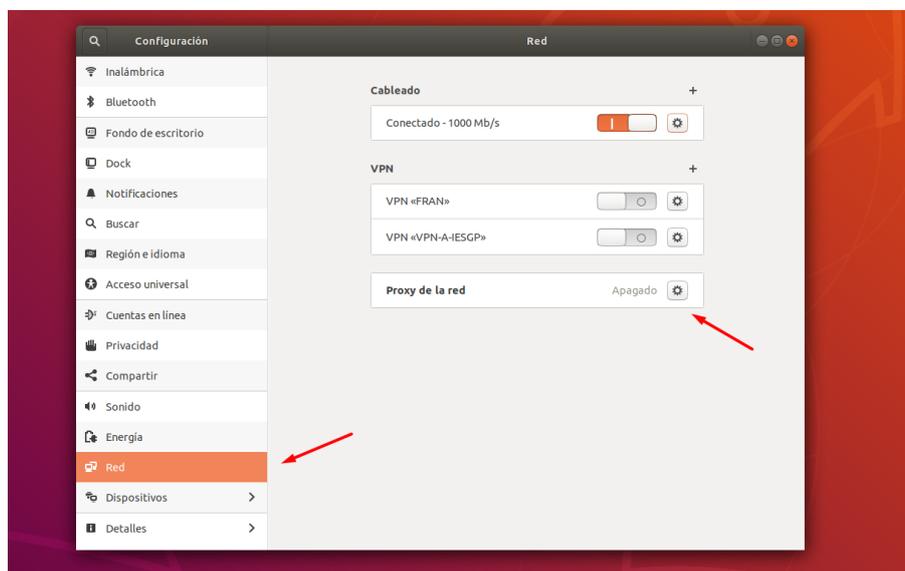
Podremos acceder a web que se nos permite.



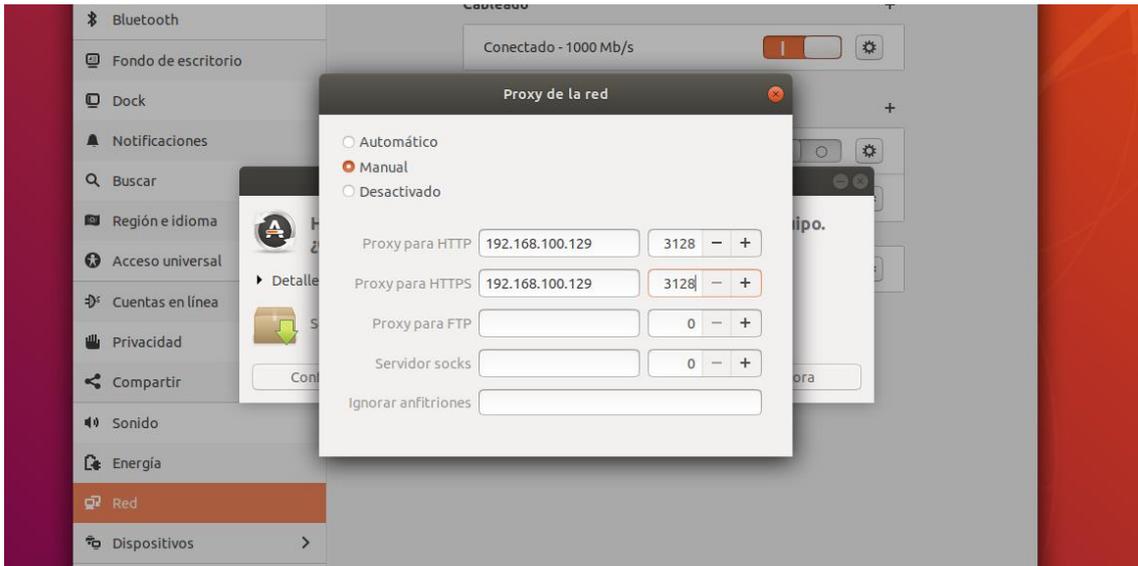
En caso de que queramos definir un idioma específico para los errores, podemos ponerlo en español exclusivamente, de lo contrario, Squid intentará ver que idioma usar desde el navegador del usuario.



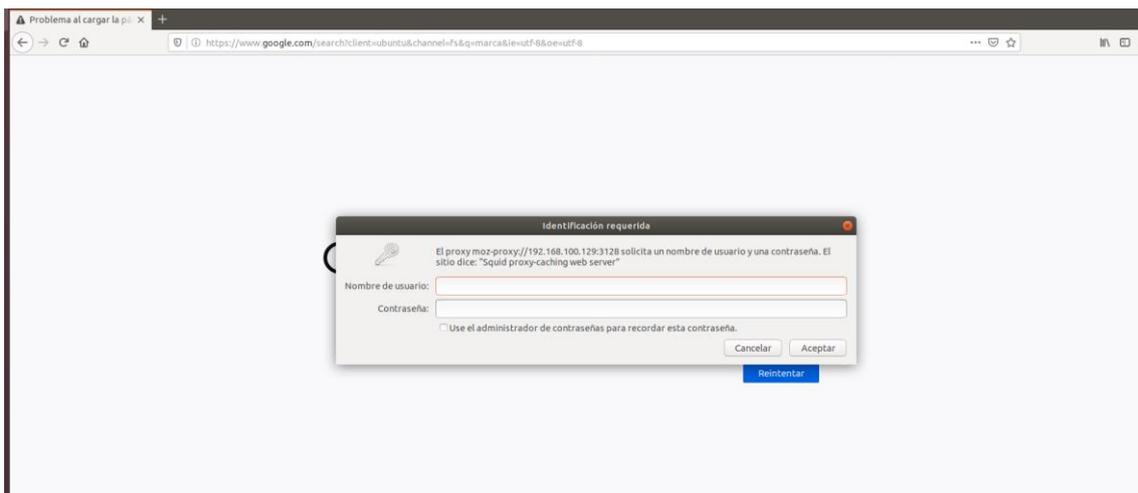
En Ubuntu vamos a la configuración de la red y luego a *Proxy de red*. Entramos a configurarlo.



Pondremos la IP del servidor y su puerto configurado.



Podemos ver, igual que antes, que con cualquier navegador que entremos nos pedirá el usuario y contraseña.



En caso de entrar en una web no permitida la bloqueará mostrando una página de error de Squid como antes.



Vemos como también funciona correctamente las expresiones regulares bloqueando la palabra *wii*.



Podremos entrar en Webs permitidas desde el Proxy correctamente.



Conclusión

La práctica me ha entretenido mucho, me ha gustado aprender las opciones que ofrece Squid y lo útil que puede ser. He aprendido bastante sobre Squid y sobre todo algunas cosas avanzadas. Me parece que los proxys pueden ser fundamentales en las empresas, no solo como cache, si no con opciones como solo permitir las webs de la red interna o controlar lo que hacen y acceden los usuarios como hemos podido ver accediendo a los logs de Squid. Aparte de esto, he aprendido otro método más para no permitir que todos los usuarios puedan salir a internet sin usuario y contraseña en caso de que lo tengamos configurado en el proxy Squid (me lo pedía para todo, incluso para aplicaciones que requieren conexión a internet como One Drive). Otra cosa que me sorprendió de Squid es la manera de crear ACL, al final la sintaxis es distinta, pero sigue una configuración global que hemos visto en otros sitios cuando hemos configurado ACL.