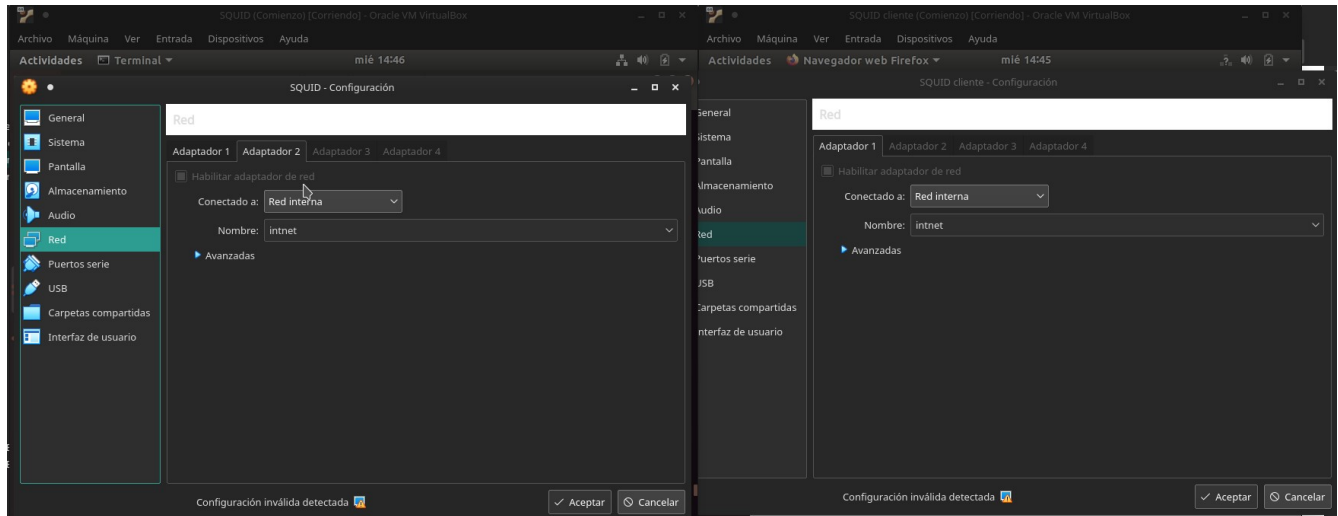


Practicas con Squid

Primeramente preparamos las 2 Maquinas e instalamos el Squid en una que es donde estará el proxy, luego la otra sera el cliente quedando asi.

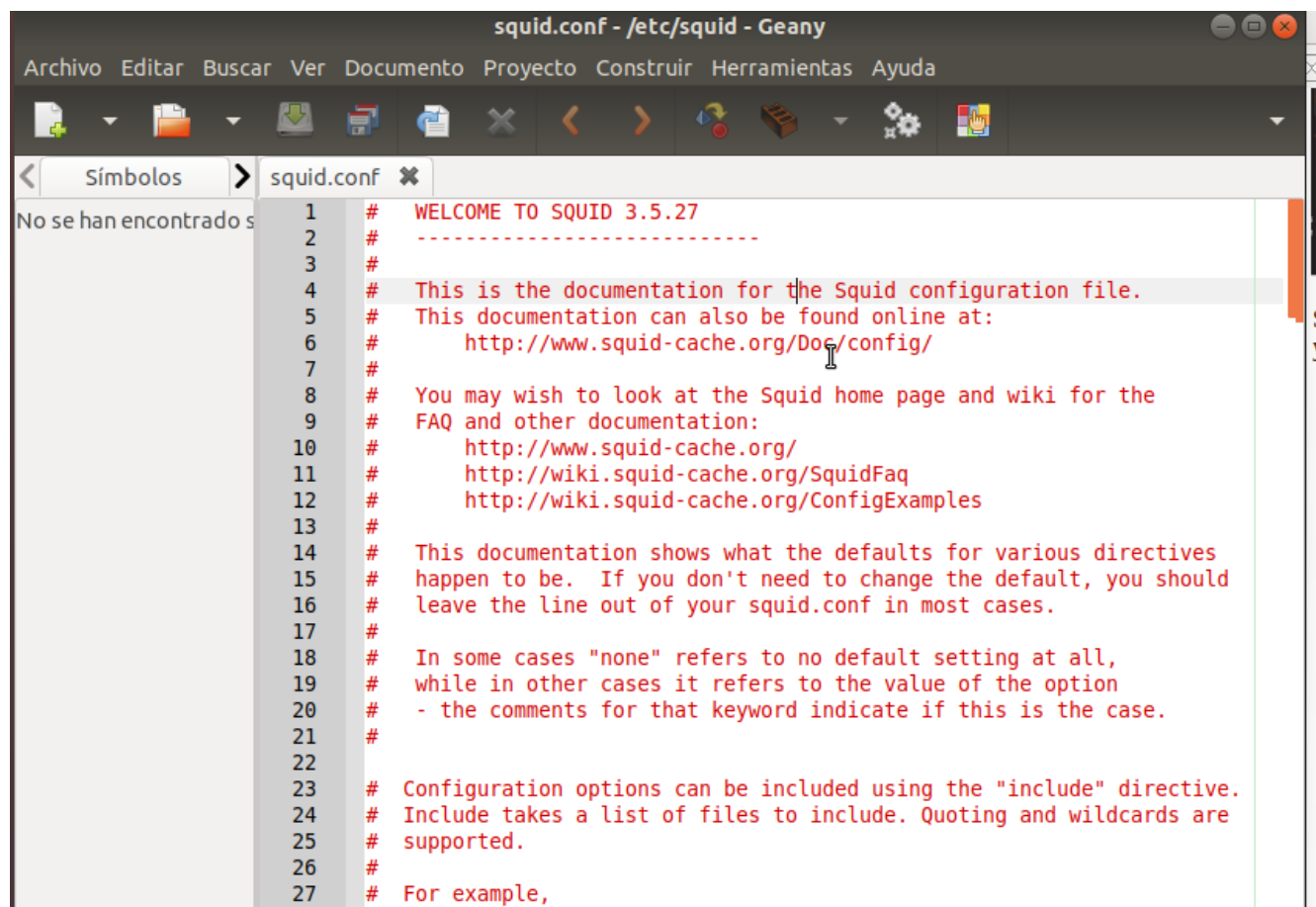
Quedando asi

La maquina SQUID tendre 2 adaptadores de red el primero tendra una conexión NAT y la segunda estara en Red Interna conectaca con SQUID cliente.



Practicas con Squid

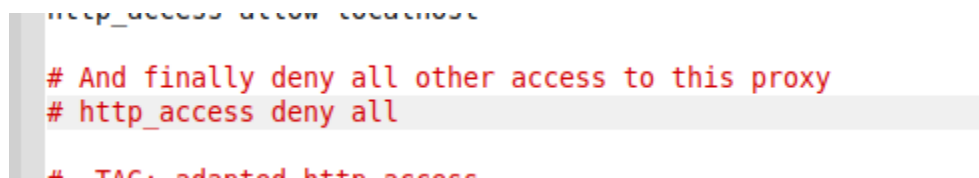
Seguidamente instalaremos Squid y al instalarlo nos creara un archivo, que contendrá la configuración y las instrucciones de esta. Es `/etc/squid/squid.conf`. Para trabajar mejor utilizare el editor geany



```
1  # WELCOME TO SQUID 3.5.27
2  # -----
3  #
4  # This is the documentation for the Squid configuration file.
5  # This documentation can also be found online at:
6  #   http://www.squid-cache.org/Doc/config/
7  #
8  # You may wish to look at the Squid home page and wiki for the
9  # FAQ and other documentation:
10 #   http://www.squid-cache.org/
11 #   http://wiki.squid-cache.org/SquidFaq
12 #   http://wiki.squid-cache.org/ConfigExamples
13 #
14 # This documentation shows what the defaults for various directives
15 # happen to be. If you don't need to change the default, you should
16 # leave the line out of your squid.conf in most cases.
17 #
18 # In some cases "none" refers to no default setting at all,
19 # while in other cases it refers to the value of the option
20 # - the comments for that keyword indicate if this is the case.
21 #
22 #
23 # Configuration options can be included using the "include" directive.
24 # Include takes a list of files to include. Quoting and wildcards are
25 # supported.
26 #
27 # For example,
```

Como se aprecia el documento es enorme donde hay unas normas ya predeterminadas que podremos comentar o descomentar.

Primeramente si comentamos `http_access deny all` ya tendríamos acceso a internet desde el cliente



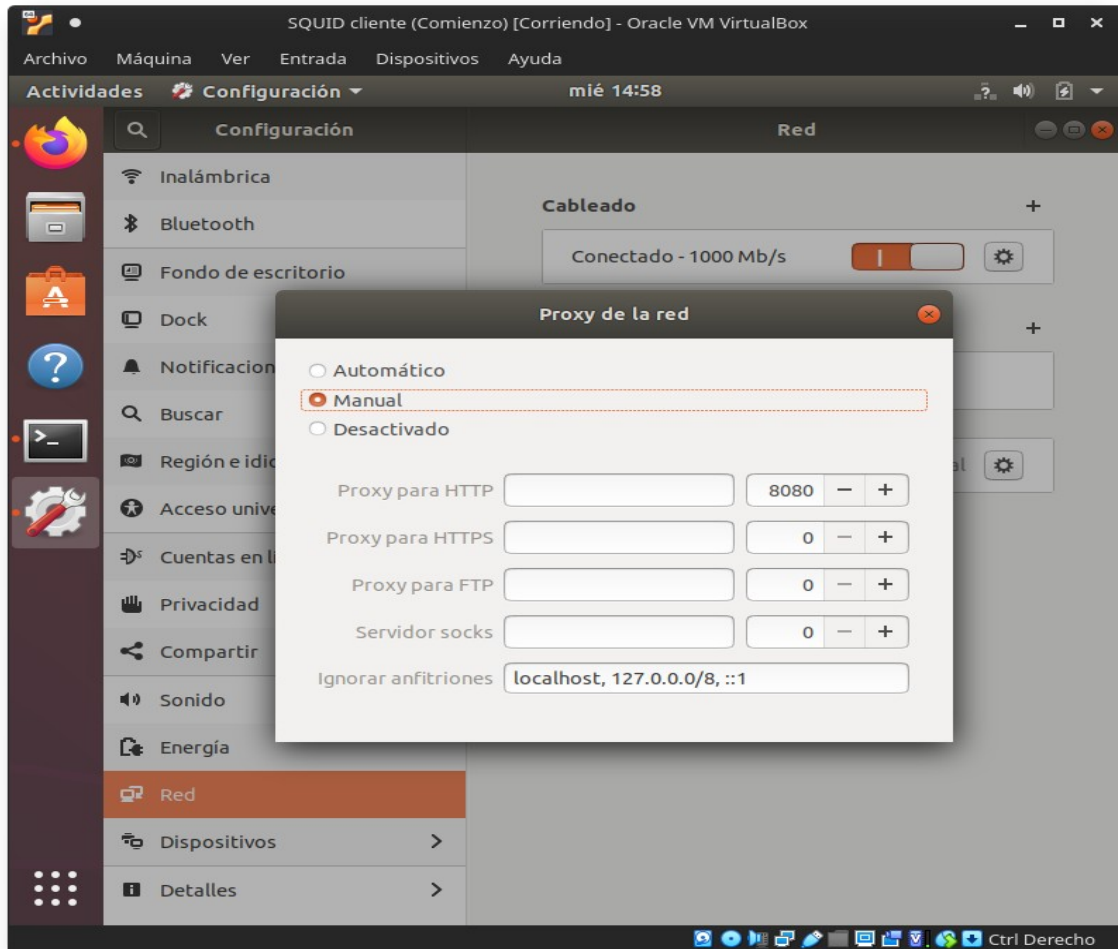
```
# And finally deny all other access to this proxy
# http_access deny all
```

Despues al guardar el archivo de configuración para que este surja efecto reiniciaremos el server con

Practicas con Squid

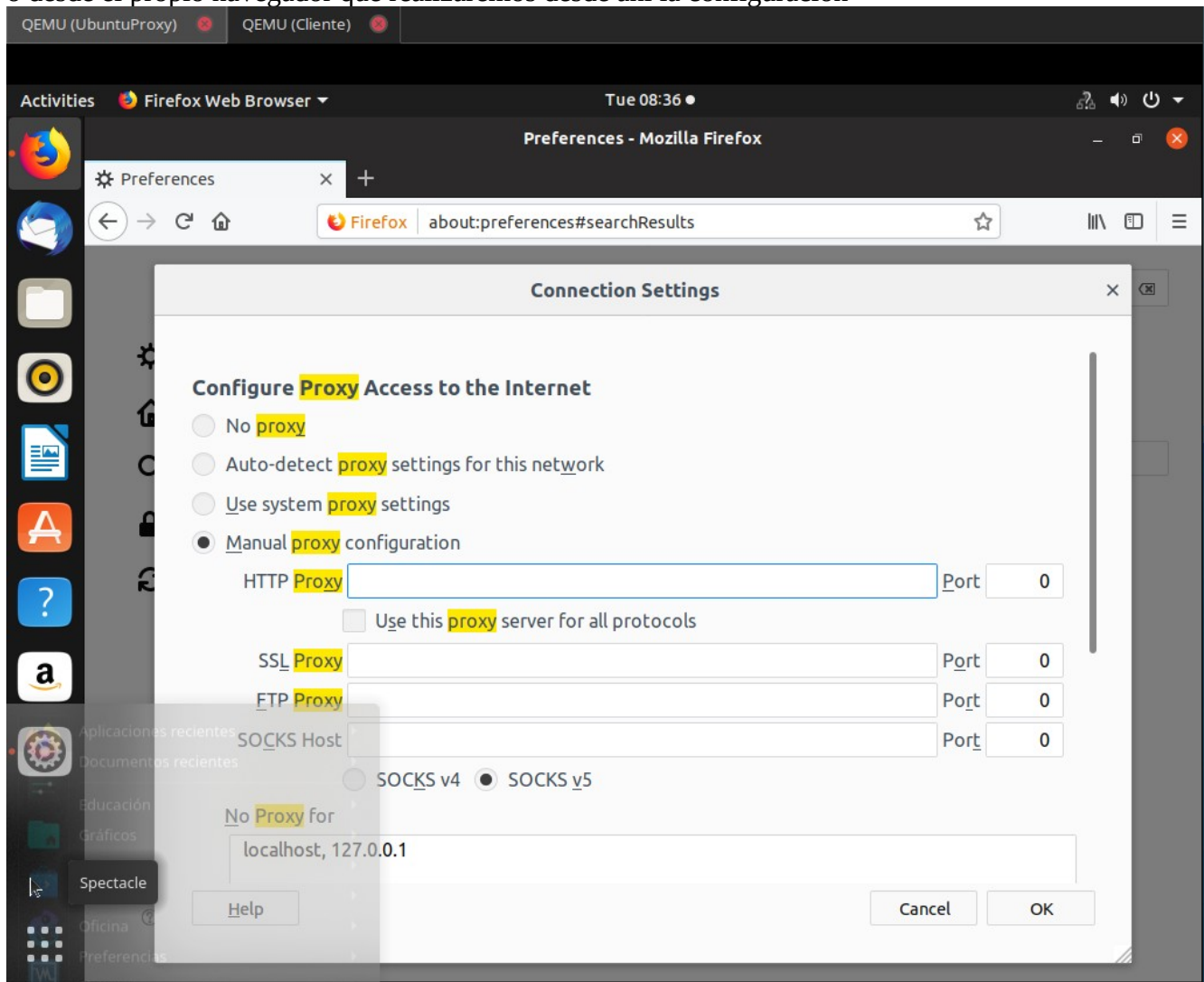
```
llorens@llorens-VirtualBox:~$ sudo systemctl restart squid
llorens@llorens-VirtualBox:~$ ^C
llorens@llorens-VirtualBox:~$ sudo systemctl restart squid
```

Una vez tenemos esta habría 2 formas de configurarlo desde el sistema o



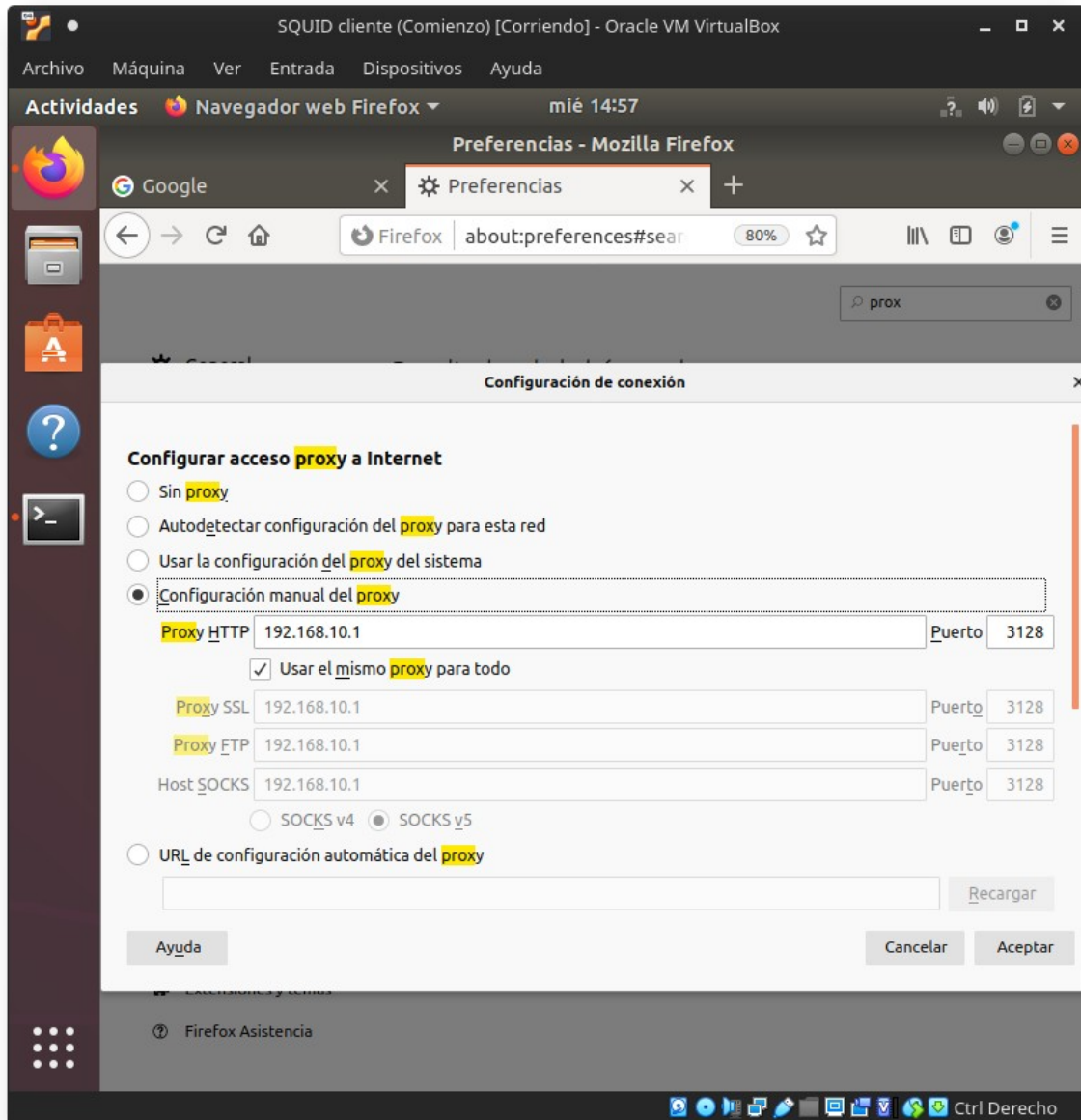
Practicas con Squid

o desde el propio navegador que realizaremos desde ahí la configuración



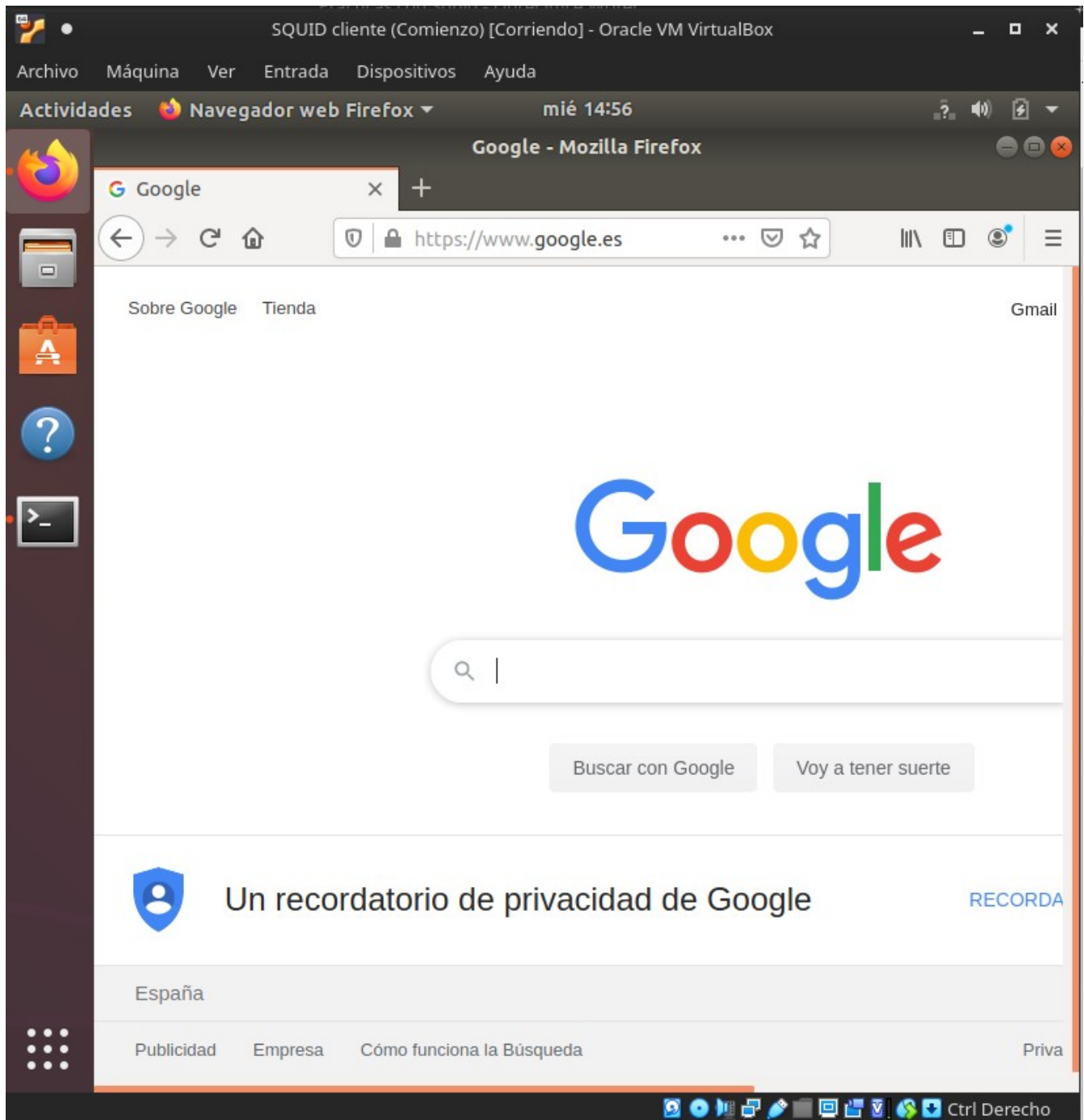
Practicas con Squid

introducimos la ip



Practicas con Squid

Y comprobamos si ya funciona.



Practicas con Squid

Después para seguir con la practica volveremos a descomentar `http_access deny all` para que podamos aplicar las reglas de las próximas practicas y reiniciamos el server.

```
397
398 # And finally deny all other access to this proxy
399 http_access deny all
400
```

Después vamos a realizar un par de configuraciones recomendables para que funcione correctamente.

Como dije anteriormente dije instale el editor de texto Geany ya que el archivo de configuracion es enorme. La configuración siempre esta comentada por lo que es fácil caer en el error de escribirla directamente. Pero a falta de saber manipular mejor Nano y Vim me esta ayudando mucho a buscar el contenido.

Descomentamos la siguiente configuracion para habilitar la cache de servidor

```
#
#
# Uncomment and adjust the following to add a disk cache directory.
cache_dir ufs /var/spool/squid 100 16 256
```

Y seguidamente descomentamos la cantidad de RAM de esta

```
# If shared memory caching is enabled, Squid does not use the share
# cache space for in-transit objects, but they still consume as muc
# local memory as they need. For more details about the shared memo
# 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
```

Practicas con Squid

Después anteriormente era solo una prueba para que los clientes tengan acceso correctamente a Internet por el proxy no era comentar “http_access deny all” era una simple prueba.

Debemos ir al acl localnet y descomentar la que se habrá definidas en RFC1918 entonces en nuestro caso como conocemos que debemos habilitar la red del cliente se quedara así.

```
#acl localnet src 10.0.0.0/8      # RFC1918 possible internal network
#acl localnet src 172.16.0.0/12 # RFC1918 possible internal network
acl localnet src 192.168.0.0/16 # RFC1918 possible internal network
#acl localnet src fc00::/7       # RFC 4193 local private network ra
#acl localnet src fe80::/10      # RFC 4291 link-local (directly plu
```

Y seguidamente descomentamos http_access allow localnet

```
# Adapt localnet in the ACL sec
# from where browsing should be
http_access allow localnet
http_access allow localhost
```

1. autenticación de usuarios en Squid3 y ACLs

Primeramente habilitamos la parte de la configuración donde hace referencia al autentificacion dejándolo así.

```
441 ##
442 auth_param basic program /usr/lib/squid3/basic_ncsa_auth /etc/squid/passwd
443 auth_param basic children 5 startup=5 idle=1
444 auth_param basic realm Squid proxy-caching web server
445 auth_param basic credentialsttl 2 hours
446 #Default:
```

Despues creamos el ACL auth_users con la opcion de que requiere autentificacion

```
1077 #
1078 acl localhost src 127.0.0.1
1079 acl PC1 src 192.168.10.2/24
1080 acl auth_users proxy_auth REQUIRED
1081 # acl my_other_proxy srcdomain proxy.example.com
```

Mas abajo ahora creamos el acceso para el ACL

```
# http_access allow all
http_access allow auth_users
# And finally deny all other access to this proxy
http_access deny all
```


Practicas con Squid

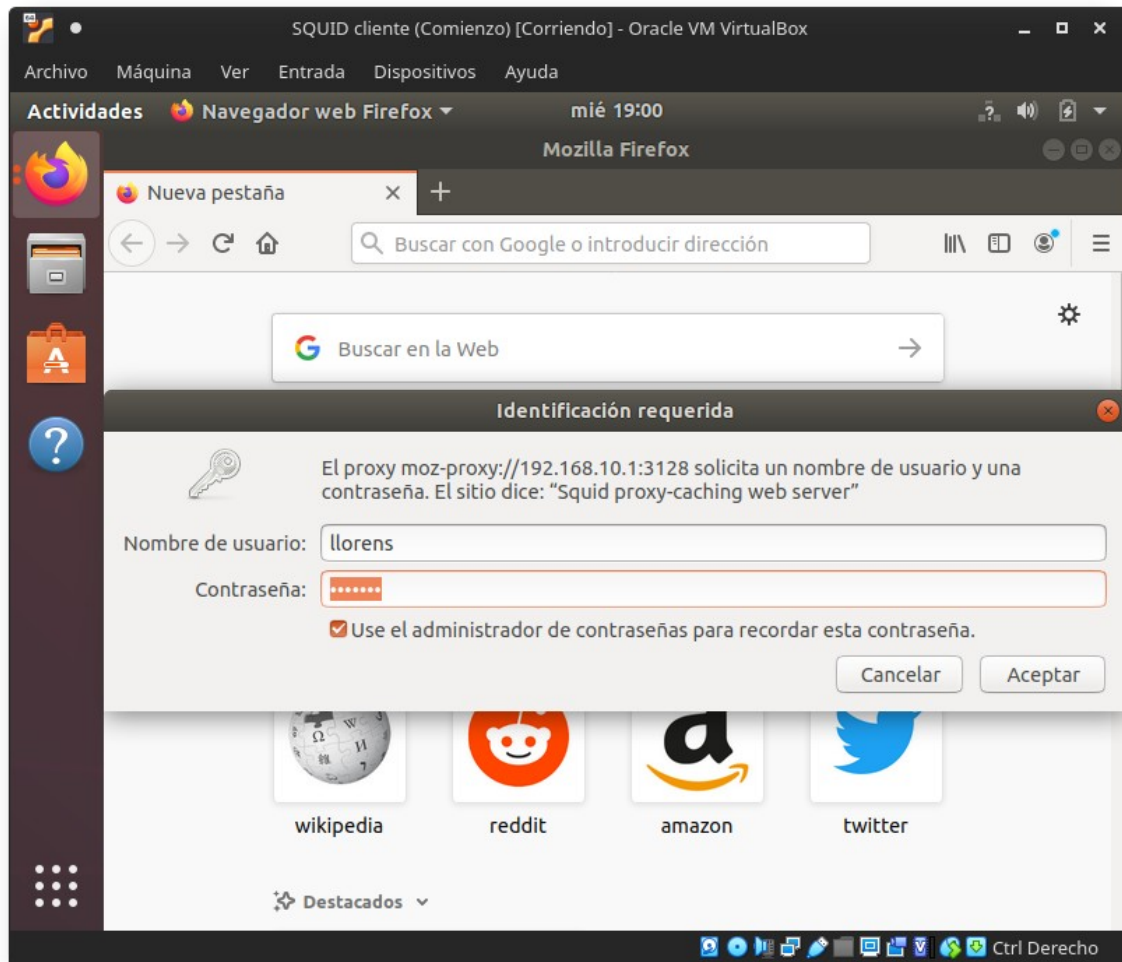
Creo un archivo llamado claves para guardar las claves de usuario que quiero configurar y creo un usuario y contraseña para que me las pida el proxy cuando haga una petición http, creo llorens

Para habilitar htpasswd previamente instalaremos apache2

```
osboxes@osboxes:~$ sudo touch /etc/squid/claves
osboxes@osboxes:~$ sudo htpasswd -c /etc/squid/claves llorens
New password:
Re-type new password:
Adding password for user llorens
osboxes@osboxes:~$
```

Y finalmente comprobamos en el cliente como a partir de ahora si queremos conectarnos nos pedirá usuario/contraseña

Practicas con Squid



Seguimos con la practica....

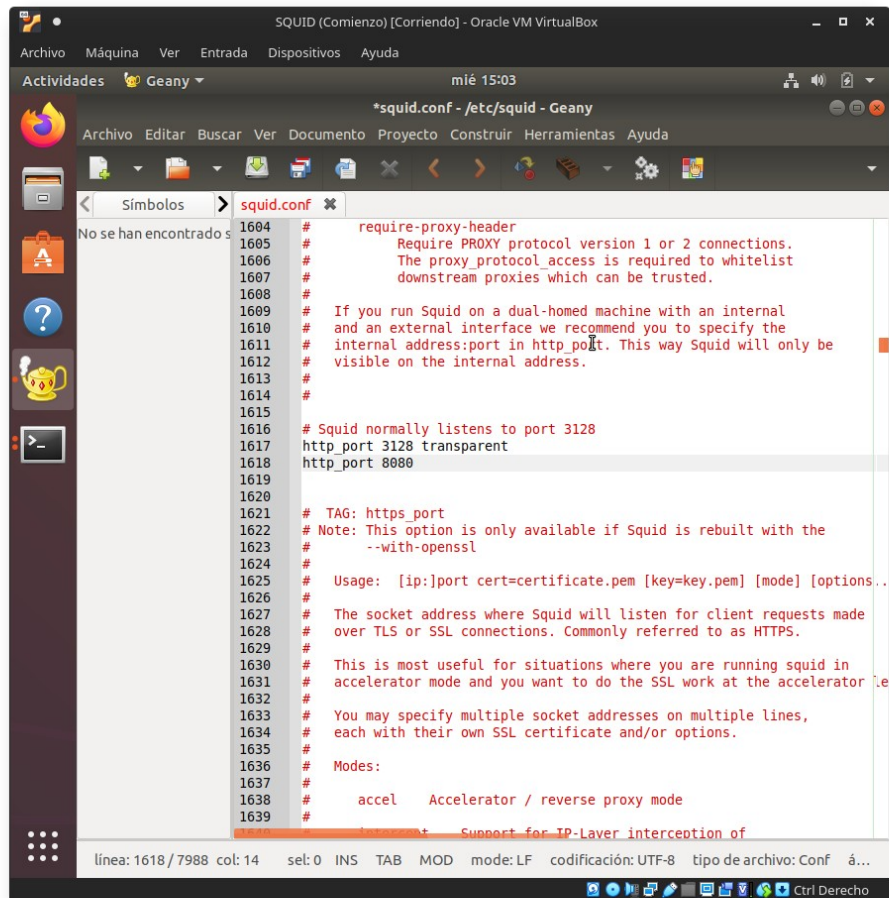
2. Proxy transparente

Practicas con Squid

Para que el Proxy funcione en modo transparente, además del comando de iptables, debemos indicarlo con las siguientes líneas (la segunda permite puerto 8080 en modo normal):

NOTA: el proxy transparente no funciona con la autenticación de usuarios

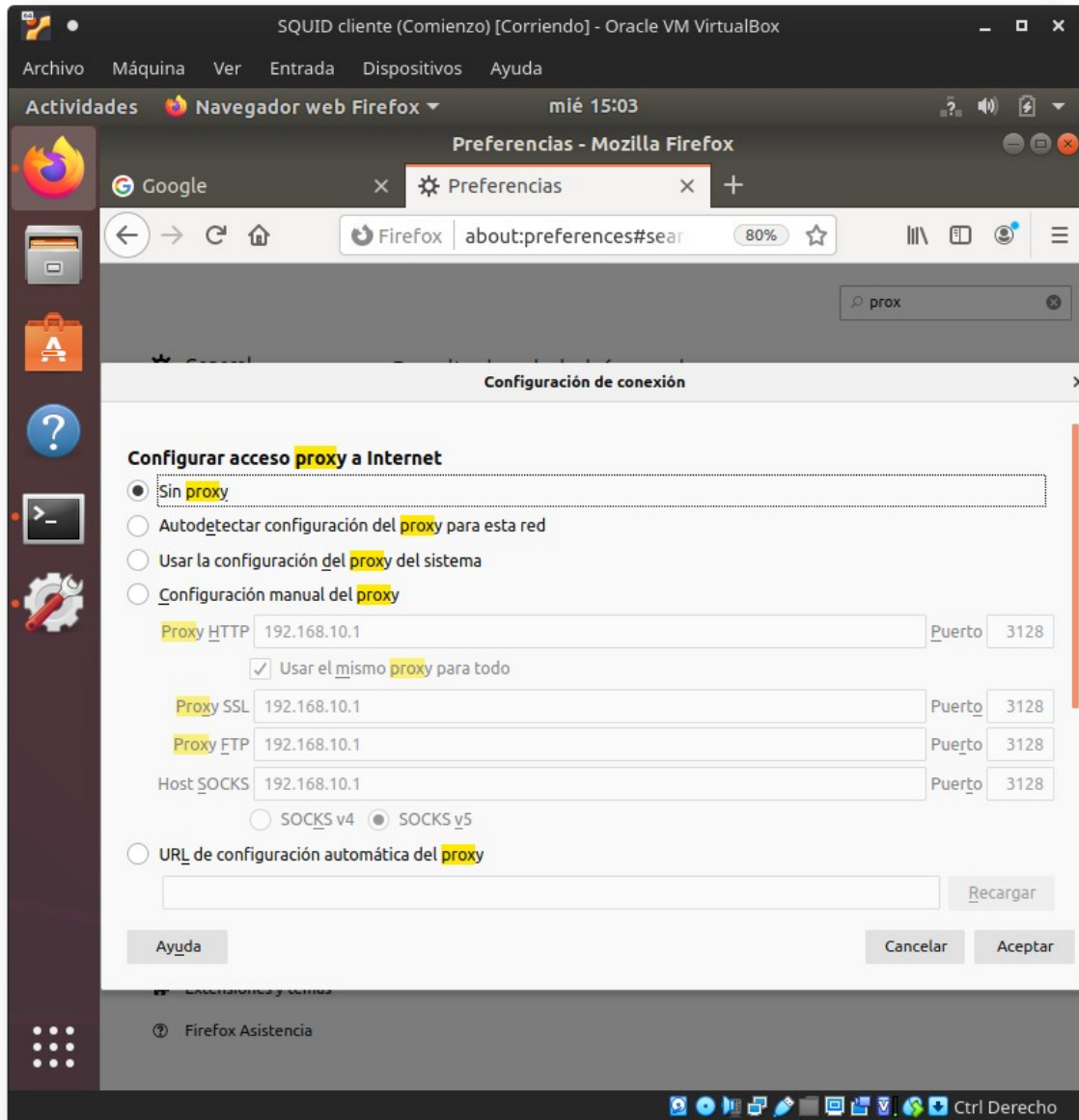
Editamos la configuración y reiniciamos el servicio



```
1604 # require-proxy-header
1605 #     Require PROXY protocol version 1 or 2 connections.
1606 #     The proxy_protocol_access is required to whitelist
1607 #     downstream proxies which can be trusted.
1608 #
1609 # If you run Squid on a dual-homed machine with an internal
1610 # and an external interface we recommend you to specify the
1611 # internal address:port in http_port. This way Squid will only be
1612 # visible on the internal address.
1613 #
1614 #
1615 #
1616 # Squid normally listens to port 3128
1617 http_port 3128 transparent
1618 http_port 8080
1619
1620 #
1621 # TAG: https_port
1622 # Note: This option is only available if Squid is rebuilt with the
1623 # --with-openssl
1624 #
1625 # Usage: [ip:]port cert=certificate.pem [key=key.pem] [mode] [options..
1626 #
1627 # The socket address where Squid will listen for client requests made
1628 # over TLS or SSL connections. Commonly referred to as HTTPS.
1629 #
1630 # This is most useful for situations where you are running squid in
1631 # accelerator mode and you want to do the SSL work at the accelerator
1632 #
1633 # You may specify multiple socket addresses on multiple lines,
1634 # each with their own SSL certificate and/or options.
1635 #
1636 # Modes:
1637 #
1638 #     accel    Accelerator / reverse proxy mode
1639 #
1640 # Support for IP-Layer interception of
```

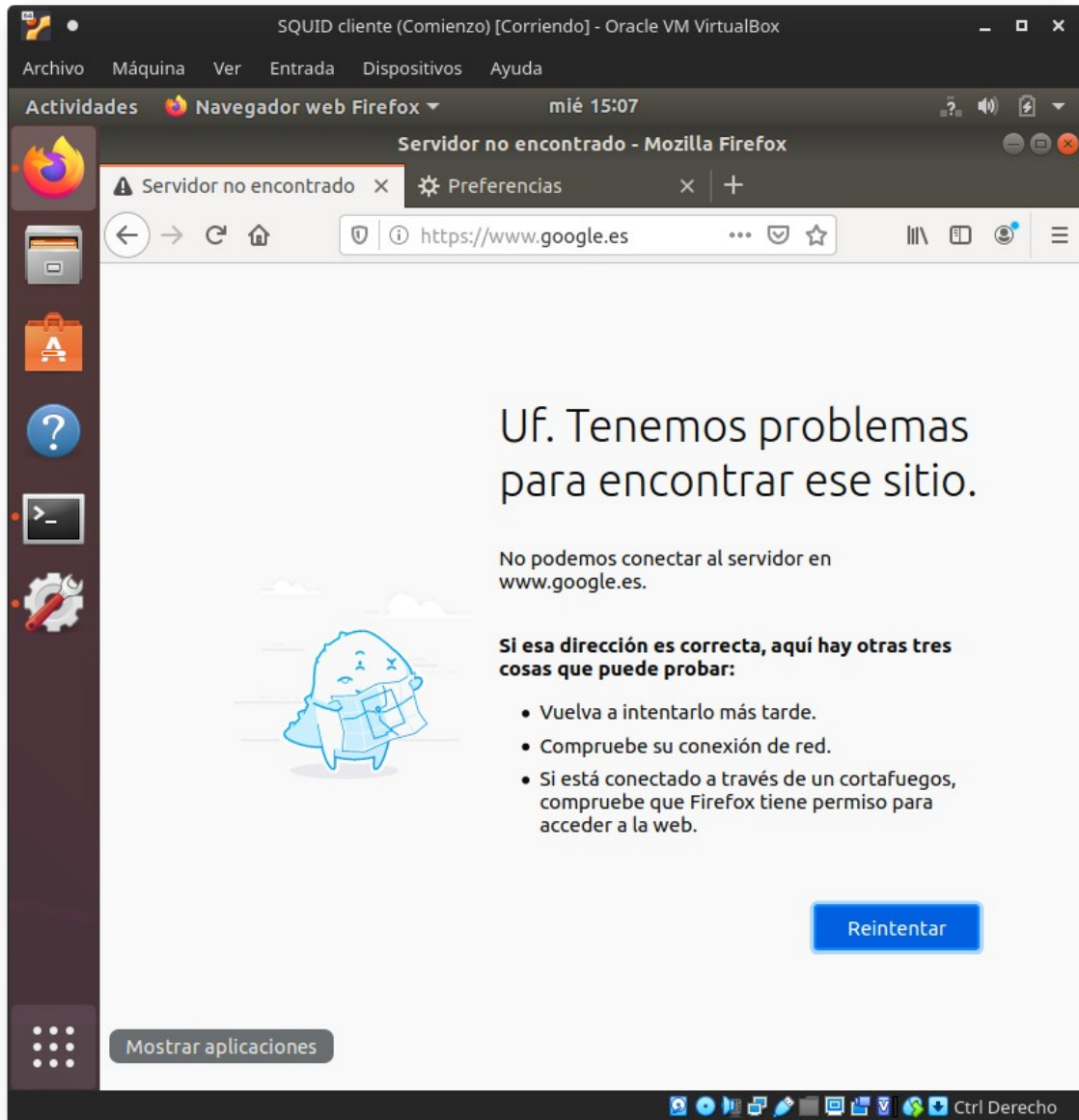
Quitamos la configuración del navegador y comprobamos que volvemos a tener Internet

Practicas con Squid



Pero parece que no me funciona en modo transparente

Practicas con Squid



Ahora vamos a poner en practica las siguientes reglas para limitar la conexión.

Practicas con Squid

1. Deniega las conexiones a todos los equipos en horario de 18:00 a 21:00 horas. Permite el resto.

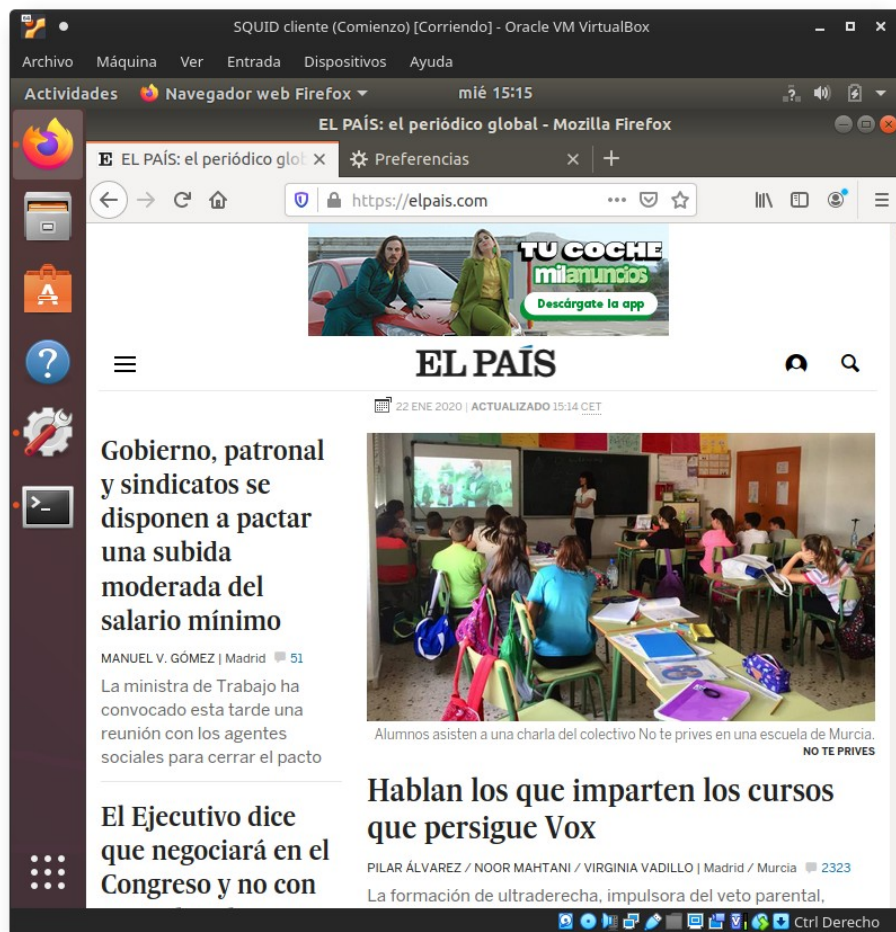
Editamos la configuracion

```
#acl localnet src TC00:://      # Kf
#acl localnet src fe80::/10      # Rf

acl reglauno time 18:00-21:00

acl SSL_ports port 443
```

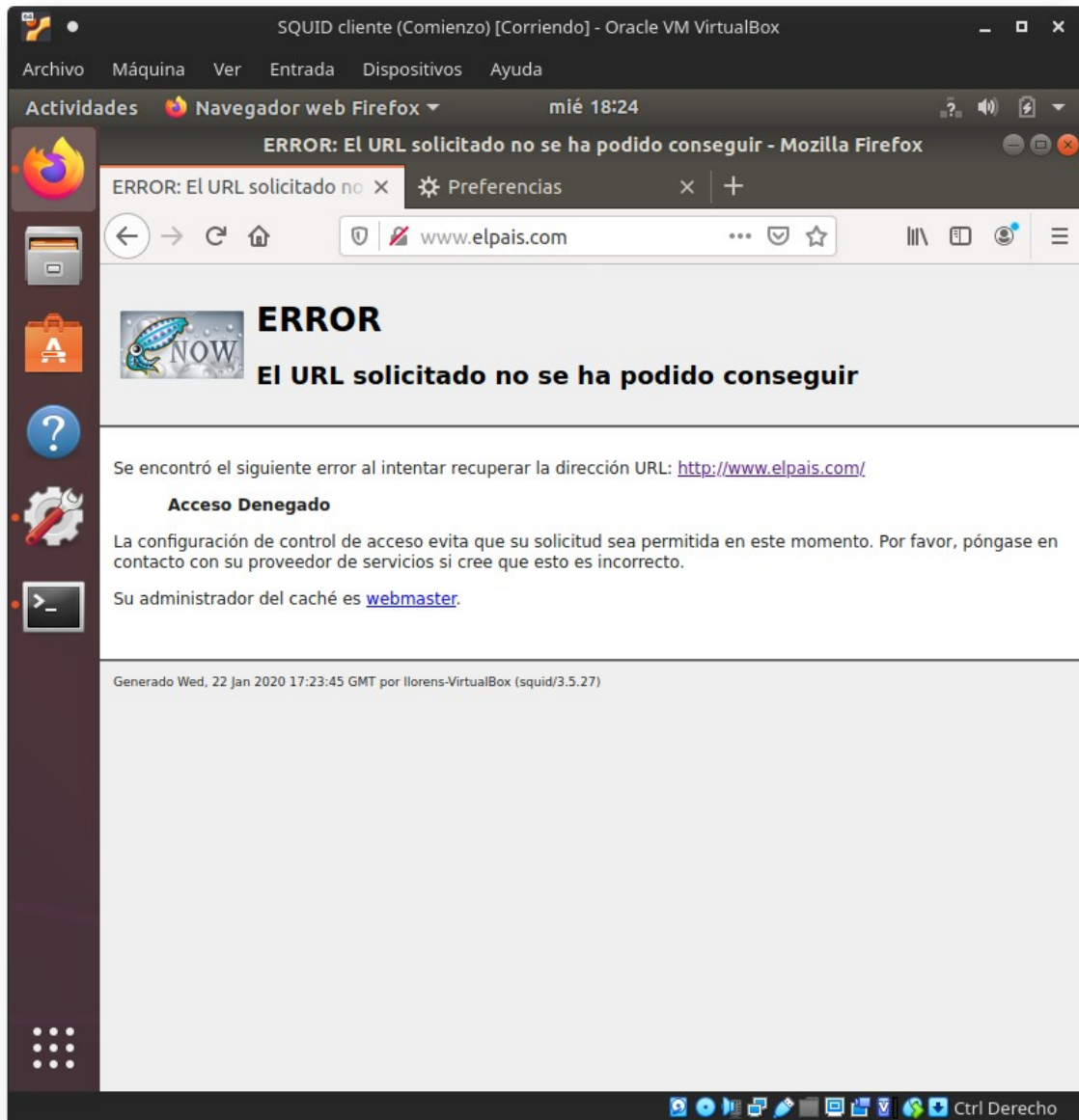
Reiniciamos el servidor y a las 15:15 miramos que funciona



Practicas con Squid

Cambiamos la hora al servidor dentro de la hora configuramos y reintentamos a ver si funciona

Lo ideal para realizar las pruebas horarias es cambiar la hora del sistema ya que las maquinas virtuales la sincronizan de ahí.



2. Deniega las conexiones a todos los equipos en horario de 20:00 a 9:00 horas, así como los fines de semana. Permite el resto.

Practicas con Squid

Para hacerlo en la misma regla, permito el acceso a todos las horas y días menos a los que el ejercicio me pide que no haya acceso

3. Deniega el acceso a un equipo con una IP determinada. El resto de IPs deben estar permitidas.

Para limitar la conexión a un equipo determinado por ejemplo el cliente que estoy utilizando

Se creara un ACL con su IP

```
# acl localhost src 127.0.0.1  
acl PC1 src 192.168.10.2/24
```

Y se crea la regla para denegar el PC1 que tiene el ACL con la IP del cliente

```
# From where browsing should be a  
http_access allow localnet  
http_access allow localhost  
http_access deny PC1  
# http access allow auth users
```

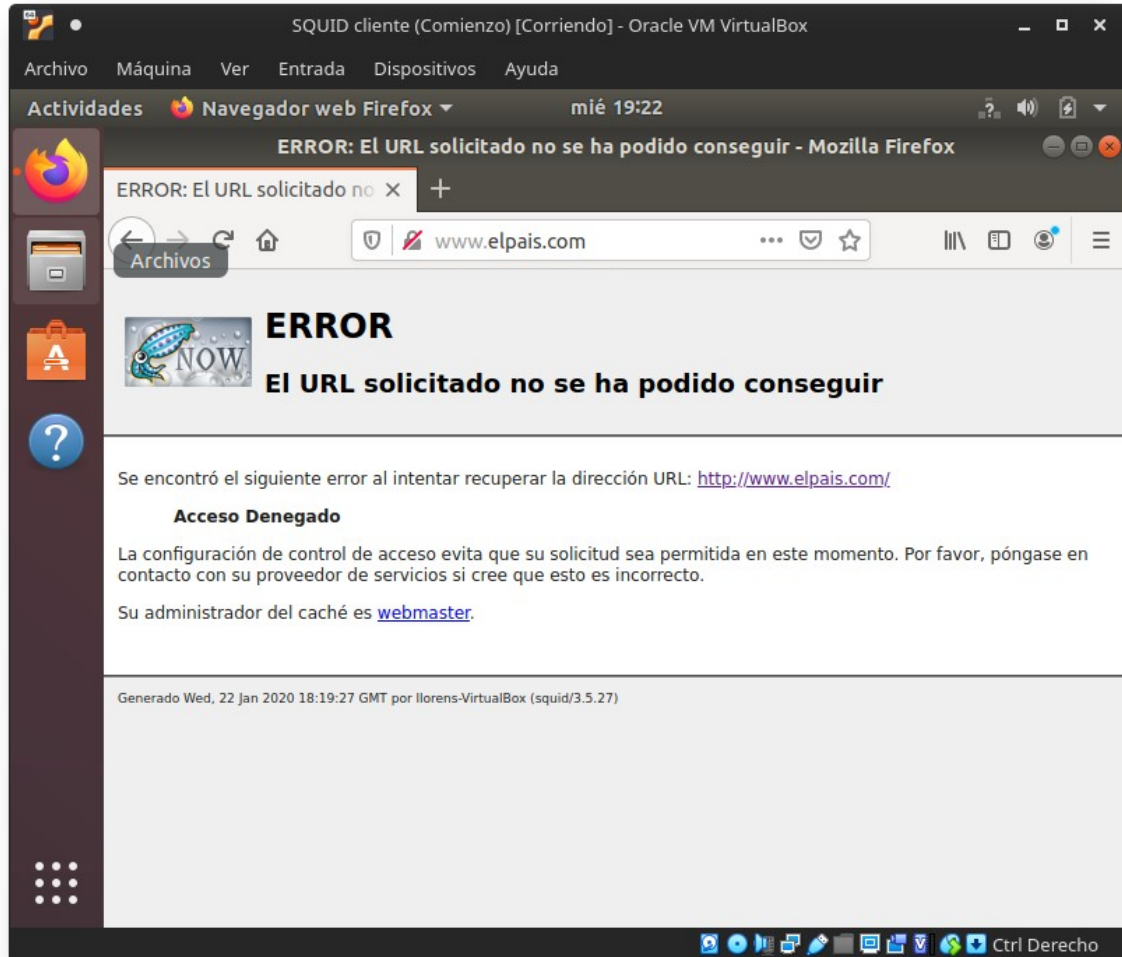
Y veremos como ahora nos denegara la conexión

Si miramos el log /var/log/squid/access.log

```
1579717162.123 0 192.168.10.2 TCP_DENIED/403 5743 GET http://www.elpais.com/ - HIER_NONE/- text/html  
1579717167.920 0 192.168.10.2 TCP_DENIED/403 5743 GET http://www.elpais.com/ - HIER_NONE/- text/html
```


Practicas con Squid

Y en el navegador



Practicas con Squid

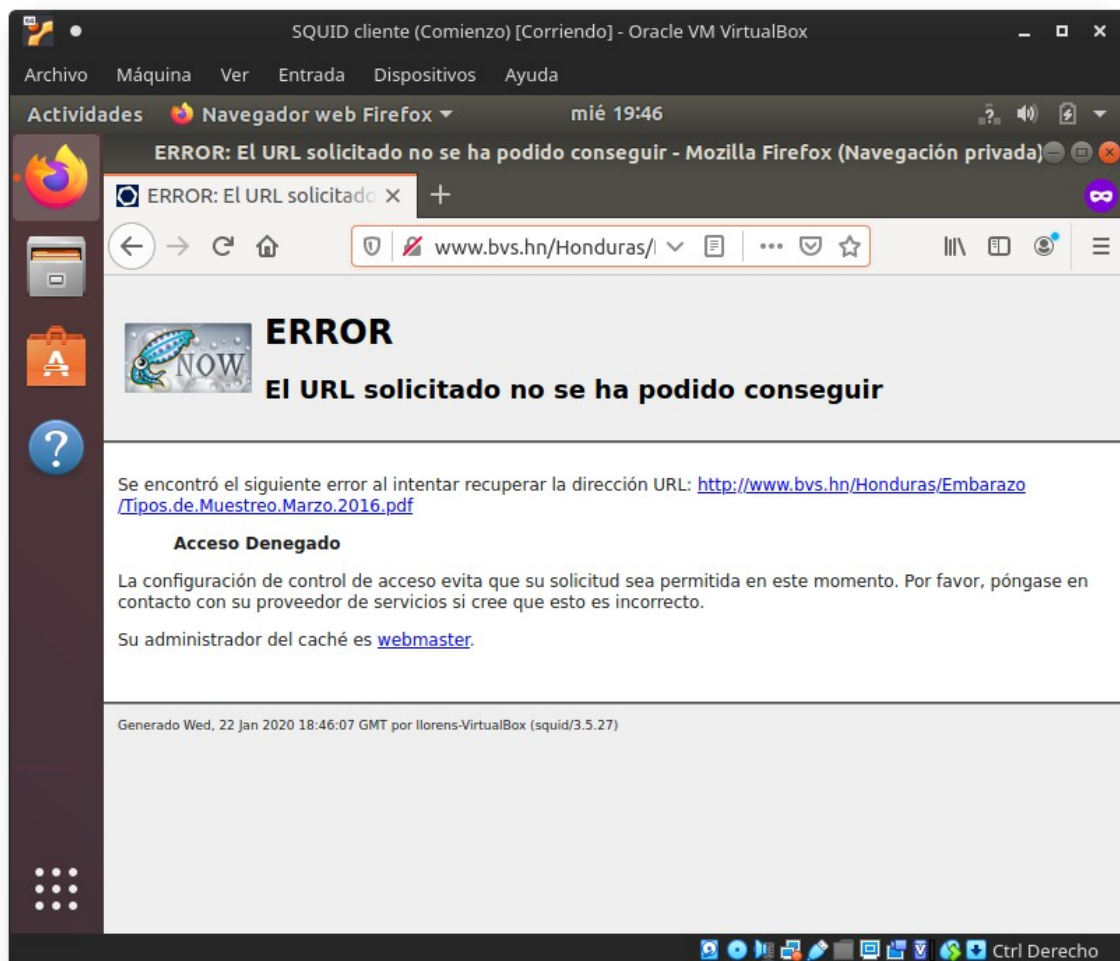
4. Restringe el acceso a todo el contenido con extensión .mp3 u otra extensión que puedas probar.

```
# From where browsing should be allowed  
http_access allow localhost !extension  
http_access allow localhost
```

Creamos la ACL

```
acl extension urlpath_regex .pdf
```

Y comprobamos el acceso denegado



Practicas con Squid

5. Restringe el acceso a todo el contenido con extensión .mp3 (u otra) en horario de 9:00 a 14:00 horas.

Añadimos una ACL para indicar el horario y seguidamente aplicamos el http_access correspondiente

```
acl morning time SMTWHFA 09:00-14:00
acl extension urlpath_regex .pdf
```

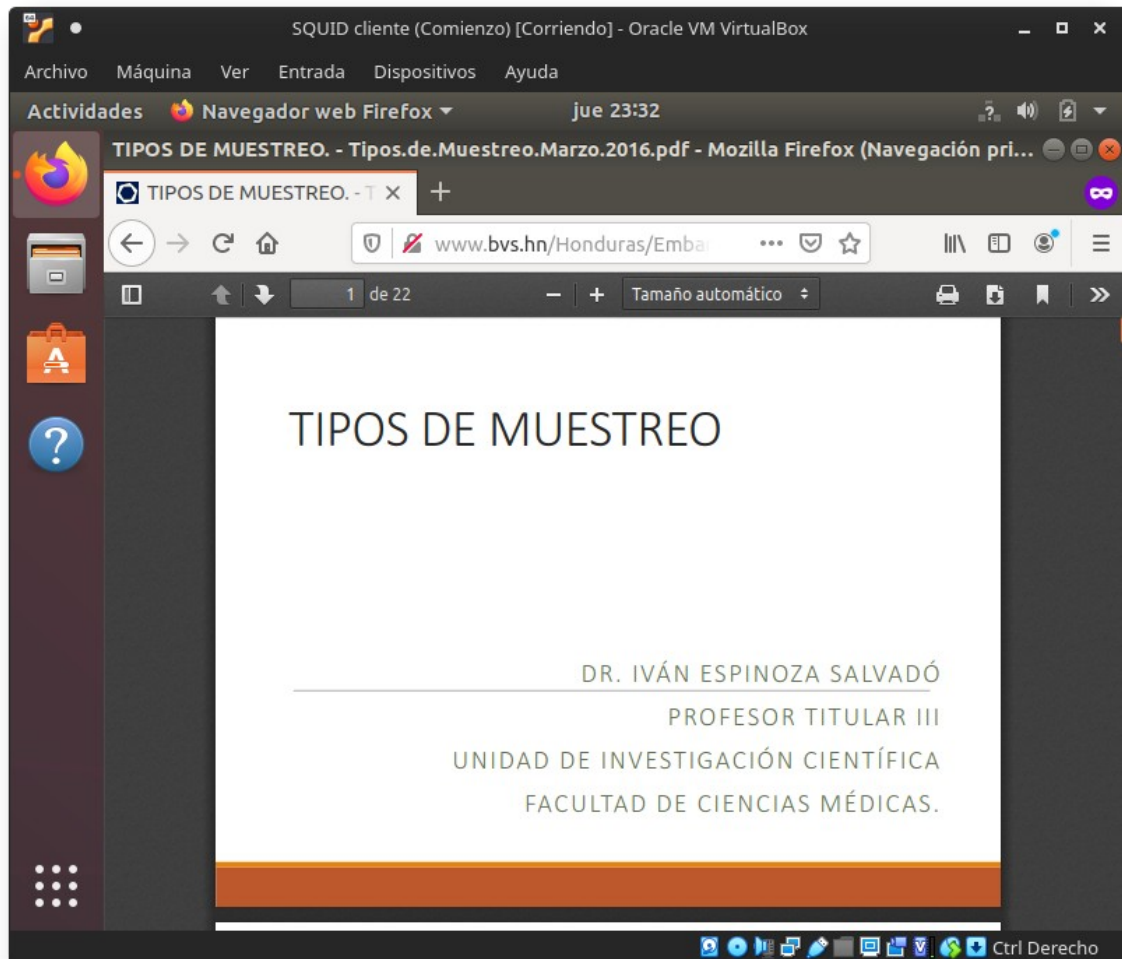
```
http_access allow !morning localnet !extension
http_access allow localhost

# http_access allow auth_users
# And finally deny all other access to this proxy
http_access deny all
```

Practicas con Squid

Y procedemos a realizar las pruebas horarias.

A las 23:30 aprox. me deja conectar



```
1579818649.420 3376 192.168.10.2 TCP_MISS/206 66023 GET http://www.bvs.hn/Honduras/Embarazo/Tipos.de.Muestreo.Marzo.2016.pdf - HIER_D  
IRECT/65.182.2.244 application/pdf
```

Practicas con Squid

A las 13 aprox. no me deja

```
E/- text/html
1579781085.789      0 192.168.10.2 TCP_DENIED/403 4372 GET http://www.bvs.hn/Honduras/Enbarazo/Tipos.de.Muestreo.Marzo.2016.pdf - HIER_
NONE/- text/html
```

6. Deniega el acceso a una serie de sitios de Internet en un horario a tu elección. Permite el resto.

Editamos la configuracion con las siguientes ACT, HTTP_ACCESS

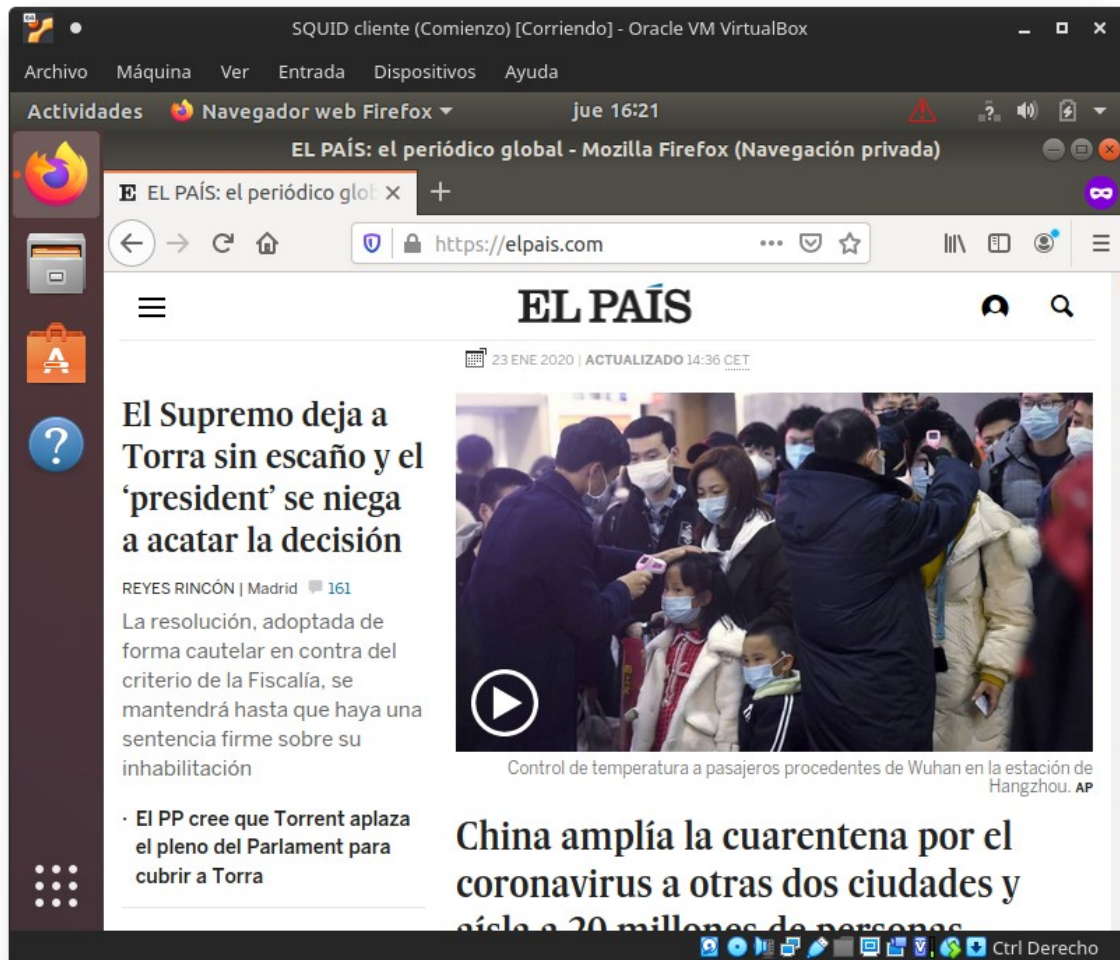
```
acl morning time SMTWHFA 09:00-14:00
acl denegarsitio dstdomain www.facebook.es www.elpais.com
acl extension urlpath_regex .pdf
acl auth_users proxy_auth REQUIRED
```

Aquí deniego el acceso cumpliéndose las condiciones, horario y sitios denegados

```
http_access allow localnet !morning
http_access allow localnet !denegarsitio
http_access allow localhost
```

Fuera de horario me permite el acceso

Practicas con Squid



Y con las dos condiciones de horario y web prohibida no me permite el acceso.

```
llorens@llorens-VirtualBox: ~  
1579771916.911 0 192.168.10.2 TCP_DENIED/403 4115 CONNECT incoming.telemetry.mozilla.org:4  
43 - HIER_NONE/- text/html  
1579771922.409 0 192.168.10.2 TCP_DENIED/403 4073 CONNECT www.facebook.com:443 - HIER_NONE  
/- text/html  
1579771926.343 0 192.168.10.2 TCP_DENIED/403 4073 CONNECT www.facebook.com:443 - HIER_NONE  
/- text/html  
1579771932.043 0 192.168.10.2 TCP_DENIED/403 4073 CONNECT www.facebook.com:443 - HIER_NONE  
/- text/html  
1579771934.507 0 192.168.10.2 TCP_DENIED/403 4073 CONNECT www.facebook.com:443 - HIER_NONE  
/- text/html  
llorens@llorens-VirtualBox:~$
```

Practicas con Squid

7. Deniega el acceso a una serie de sitios de Internet en un horario a tu elección desde algunas IPs. Permite el resto.

Utilizo las ACL anteriores y dos IP al as que se restringirá el acceso en el horario indicado a las web elegidas

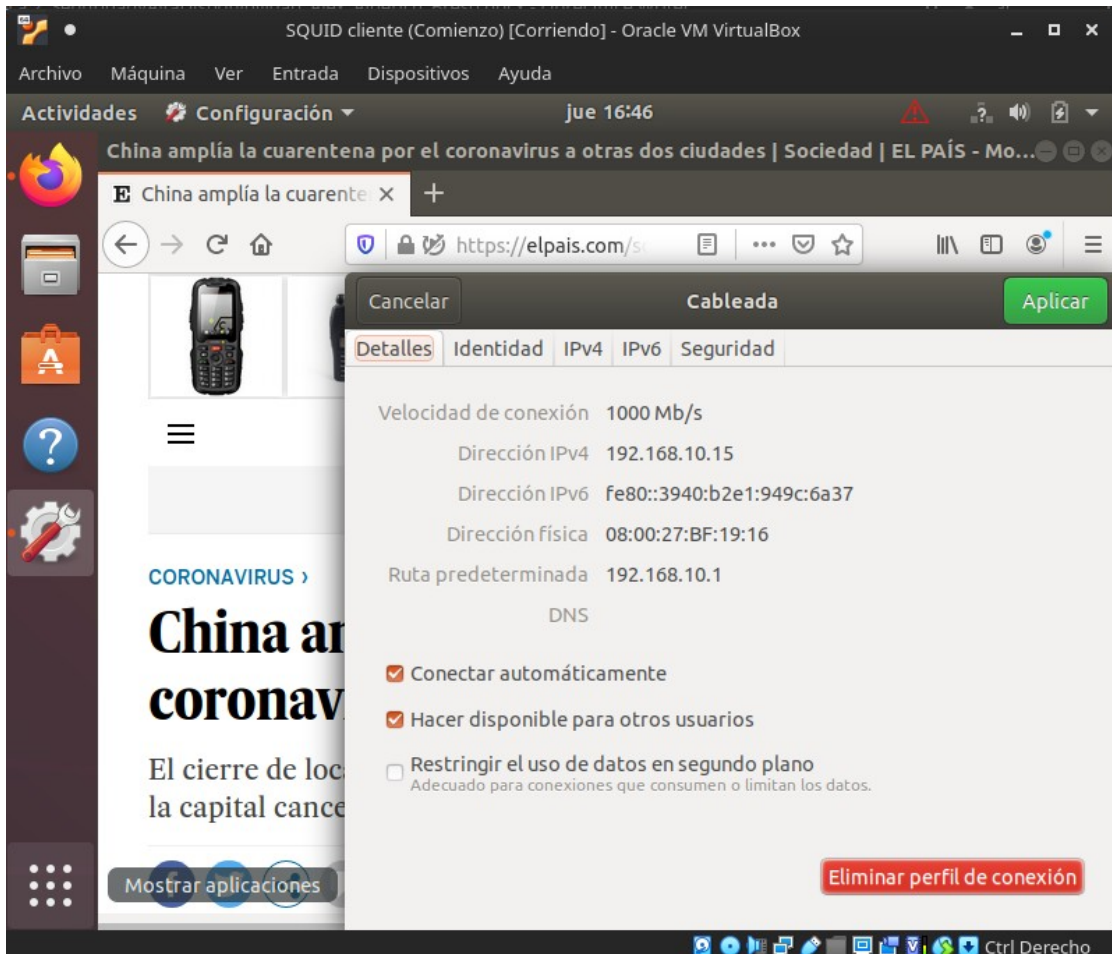
```
acl morning time SMTWHFA 09:00-14:00
acl denegarsitio dstdomain www.facebook.es www.elpais.com
acl ipseleccionadas src 192.168.10.15 192.168.10.25
```

Añado una condición AND a las otras 2

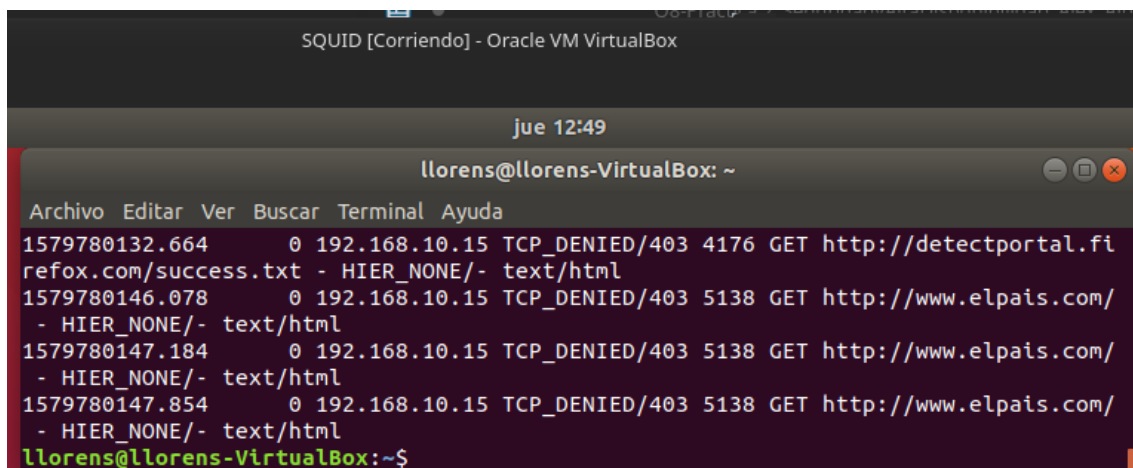
```
http_access allow localnet !morning
http_access allow localnet !denegarsitio
http_access allow localnet !ipseleccionadas
```


Practicas con Squid

Vemos como fuera del horario, la Ip 192.168.10.15 sí que puede navegar a una web prohibida, ya que no se dan las tres condiciones:



Con las tres condiciones(horario, web e IP), no podemos acceder a la web prohibida



Practicas con Squid

Si cambio la Ip del cliente, ya nos permite navegar, aun estando en el horario restringido y a una web prohibida, ya que no se dan las tres condiciones:

