

UT5 - PROXY
PRÁCTICA SQUID



PAULA RUIZ DORAL 2ºA ASIR

ÍNDICE

Introducción.....	3
Instalación de squid.....	3
Apartado 1: ACL “Redes_sociales”.....	6
Apartado 2: ACL “Horas_laborales”.....	12
1º Prueba con horario que me permite comprobar.....	12
2º Horario pedido para la práctica.....	17
Apartado 3: Autenticación de squid con NCSA.....	18
Apartado 4: Autenticación de squid con LDAP.....	21
Apartado 5: URL Github.....	23

Introducción

Squid es un servidor proxy de código abierto que mejora el rendimiento y la seguridad de las redes. Actúa como intermediario entre los usuarios y los servidores web, almacenando en caché contenido para un acceso más rápido y controlando el acceso a Internet.

Sus características principales incluyen; el almacenamiento en caché de contenido, filtrado de contenido, control de acceso y soporte para diversos protocolos.

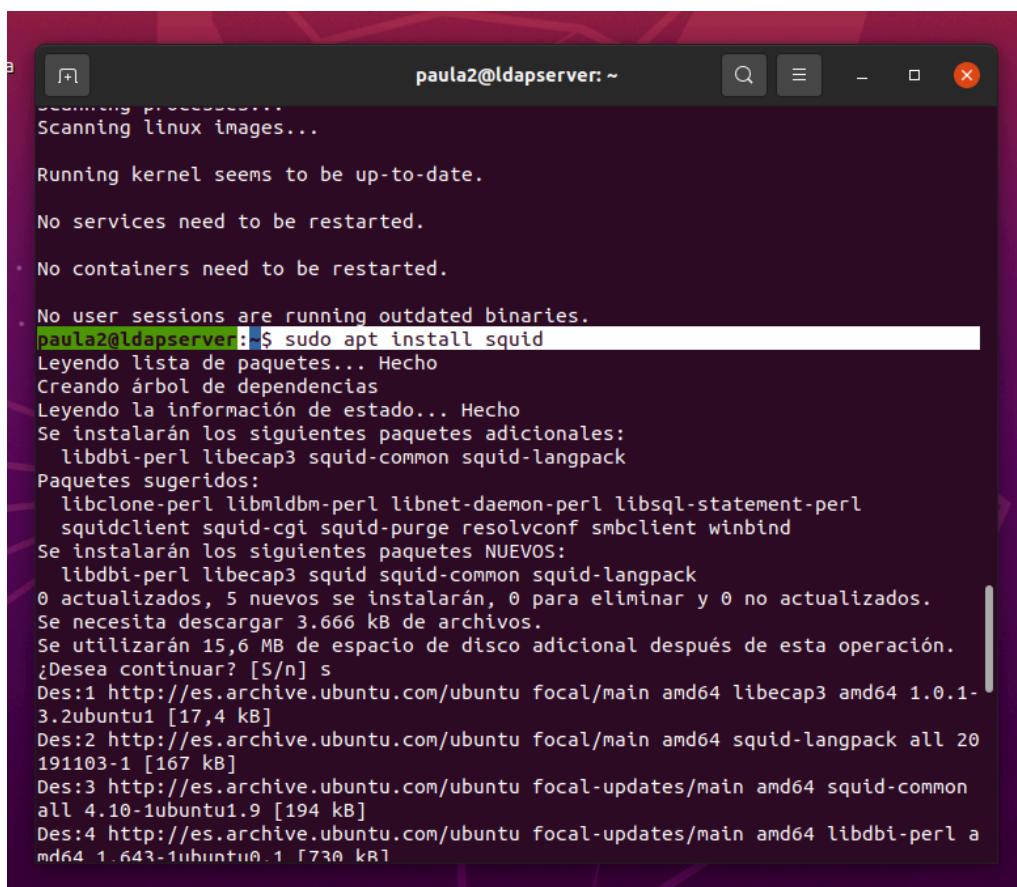
Es ampliamente utilizado en entornos empresariales y proveedores de servicios de Internet debido a su flexibilidad y capacidades de configuración.

Las Listas de Control de Acceso (ACL) son una característica clave que permite a los administradores definir políticas precisas para el acceso y el filtrado de contenido como vamos a ver a continuación con ejemplos en los siguientes apartados.

Instalación de squid

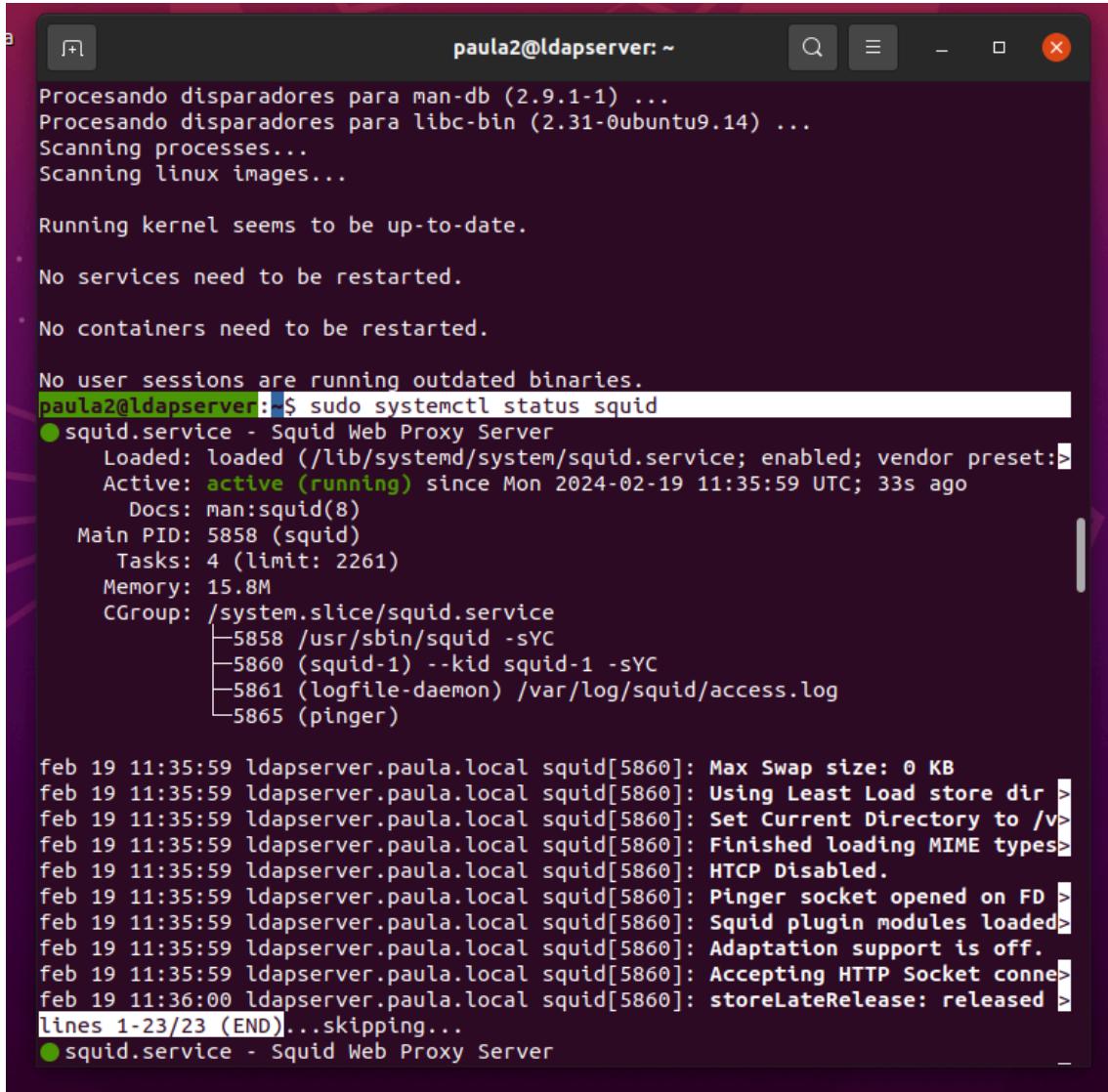
Para realizar esta práctica voy a utilizar el Ubuntu 20.04 utilizado en prácticas anteriores.

Lo primero será hacer un update y un upgrade para actualizar paquetes y dejar la máquina preparada para la instalación de squid y usar este comando para su instalación:



```
Scanning...  
Scanning linux images...  
Running kernel seems to be up-to-date.  
No services need to be restarted.  
No containers need to be restarted.  
No user sessions are running outdated binaries.  
paula2@ldapserver:~$ sudo apt install squid  
Leyendo lista de paquetes... Hecho  
Creando árbol de dependencias  
Leyendo la información de estado... Hecho  
Se instalarán los siguientes paquetes adicionales:  
  libdbi-perl libecap3 squid-common squid-langpack  
Paquetes sugeridos:  
  libclone-perl libldb-perl libnet-daemon-perl libsql-statement-perl  
  squidclient squid-cgi squid-purge resolvconf smbclient winbind  
Se instalarán los siguientes paquetes NUEVOS:  
  libdbi-perl libecap3 squid squid-common squid-langpack  
0 actualizados, 5 nuevos se instalarán, 0 para eliminar y 0 no actualizados.  
Se necesita descargar 3.666 kB de archivos.  
Se utilizarán 15,6 MB de espacio de disco adicional después de esta operación.  
¿Desea continuar? [S/n] s  
Des:1 http://es.archive.ubuntu.com/ubuntu focal/main amd64 libecap3 amd64 1.0.1-3.2ubuntu1 [17,4 kB]  
Des:2 http://es.archive.ubuntu.com/ubuntu focal/main amd64 squid-langpack all 20191103-1 [167 kB]  
Des:3 http://es.archive.ubuntu.com/ubuntu focal-updates/main amd64 squid-common all 4.10-1ubuntu1.9 [194 kB]  
Des:4 http://es.archive.ubuntu.com/ubuntu focal-updates/main amd64 libdbi-perl amd64 1.643-1ubuntu0.1 [730 kB]
```

Puedo consultar su estado y ver que está corriendo.



The screenshot shows a terminal window titled "paula2@ldapserver: ~". The terminal displays the output of a system status check and the status of the squid service. The status check includes messages about man-db, libc-bin, processes, and kernel. The squid service status shows it is active (running) since Mon 2024-02-19 11:35:59 UTC; 33s ago. It lists the main PID (5858), tasks (4), memory usage (15.8M), and CGrou

```
Procesando disparadores para man-db (2.9.1-1) ...
Procesando disparadores para libc-bin (2.31-0ubuntu9.14) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

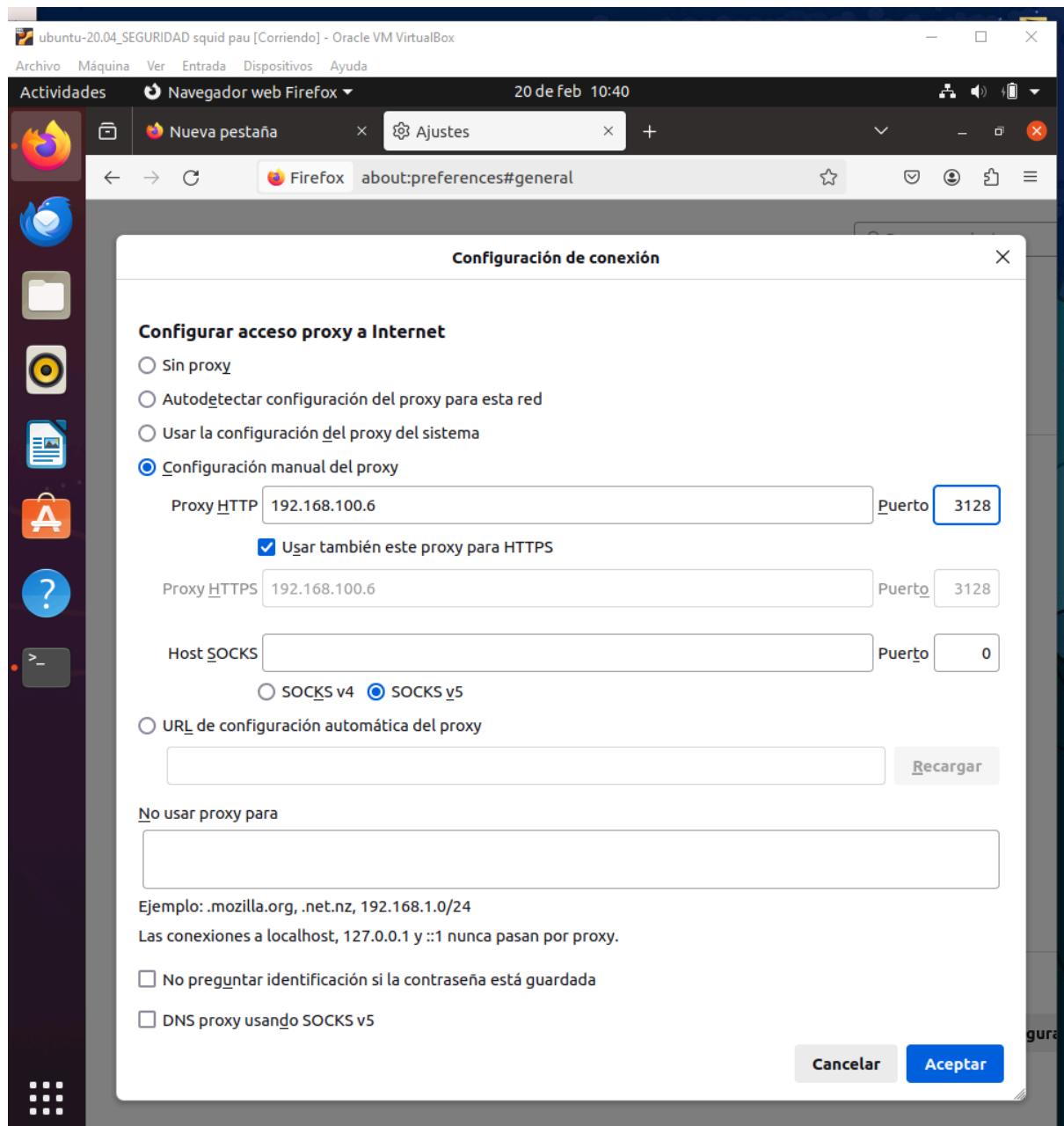
No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.
paula2@ldapserver:~$ sudo systemctl status squid
● squid.service - Squid Web Proxy Server
  Loaded: loaded (/lib/systemd/system/squid.service; enabled; vendor preset:>)
  Active: active (running) since Mon 2024-02-19 11:35:59 UTC; 33s ago
    Docs: man:squid(8)
   Main PID: 5858 (squid)
     Tasks: 4 (limit: 2261)
    Memory: 15.8M
      CGroup: /system.slice/squid.service
              └─5858 /usr/sbin/squid -sYC
                  ├─5860 (squid-1) --kid squid-1 -sYC
                  ├─5861 (logfile-daemon) /var/log/squid/access.log
                  └─5865 (pinger)

feb 19 11:35:59 ldapserver.paula.local squid[5860]: Max Swap size: 0 KB
feb 19 11:35:59 ldapserver.paula.local squid[5860]: Using Least Load store dir >
feb 19 11:35:59 ldapserver.paula.local squid[5860]: Set Current Directory to /v>
feb 19 11:35:59 ldapserver.paula.local squid[5860]: Finished loading MIME types>
feb 19 11:35:59 ldapserver.paula.local squid[5860]: HTCP Disabled.
feb 19 11:35:59 ldapserver.paula.local squid[5860]: Pinger socket opened on FD >
feb 19 11:35:59 ldapserver.paula.local squid[5860]: Squid plugin modules loaded>
feb 19 11:35:59 ldapserver.paula.local squid[5860]: Adaptation support is off.
feb 19 11:35:59 ldapserver.paula.local squid[5860]: Accepting HTTP Socket conn>
feb 19 11:36:00 ldapserver.paula.local squid[5860]: storeLateRelease: released >
lines 1-23/23 (END)...skipping...
● squid.service - Squid Web Proxy Server
```

Ahora para que mi navegador firefox use squid como proxy tengo que meterme a la configuración y en el apartado de red, meter la ip de mi máquina en la que tengo squid funcionando (es esta misma) y manualmente escribirla además del puerto de squid:

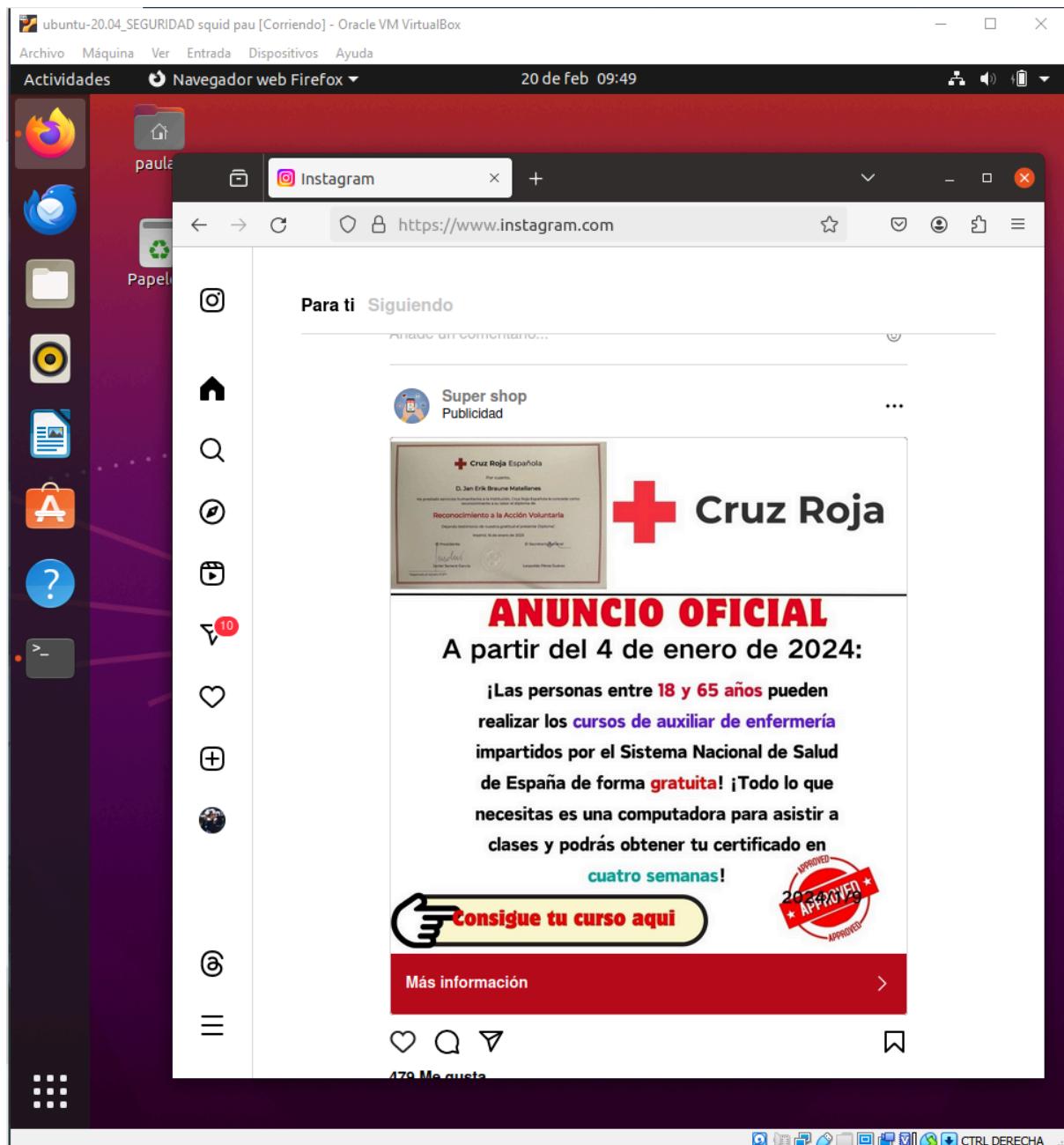


De esta forma ya está mi dispositivo usando squid como proxy

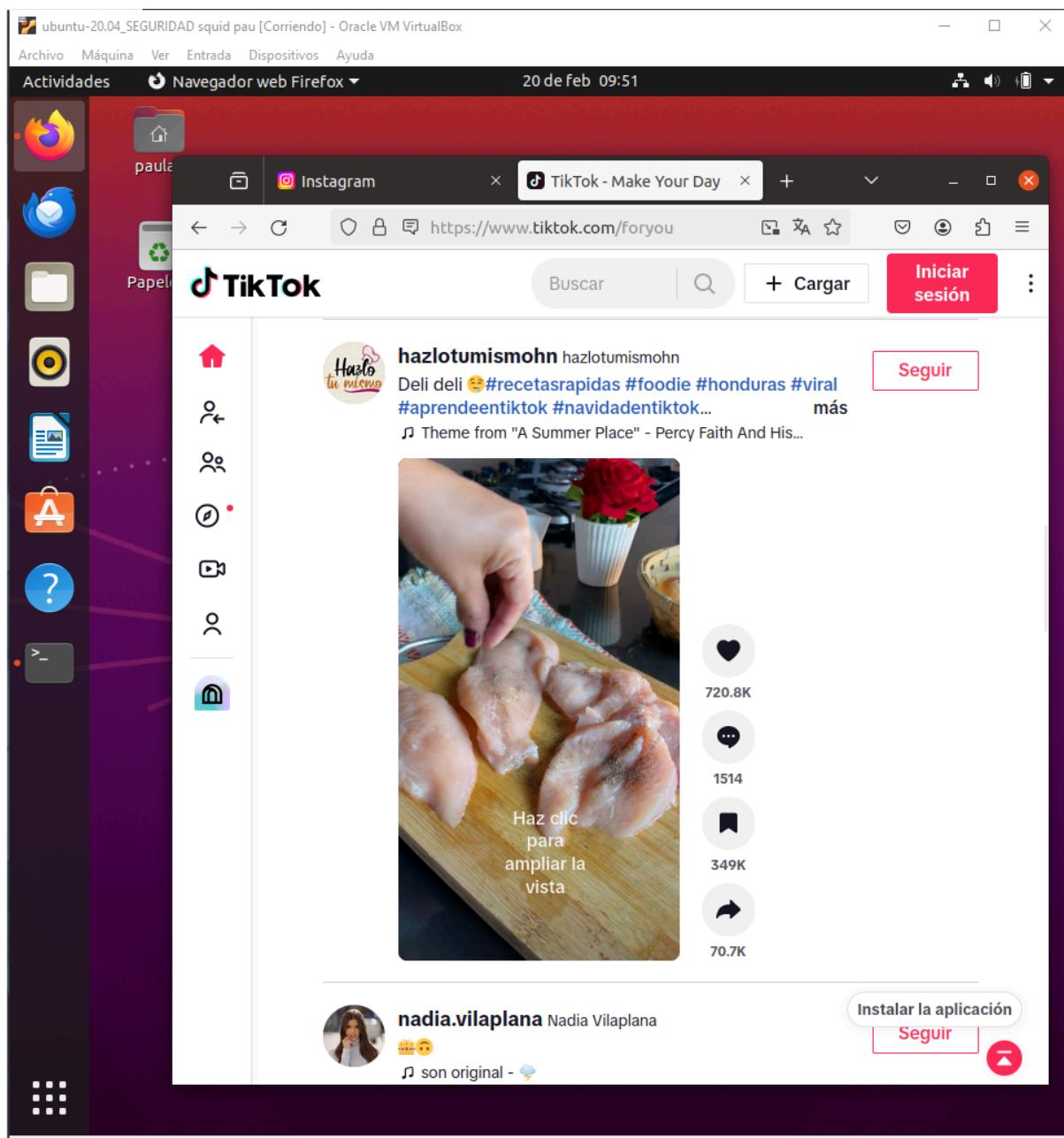
Apartado 1: ACL “Redes_sociales”

Antes de crear y aplicar la ACL voy a meterme a las dos redes sociales que quiero restringir para verificar que puedo acceder a ellas.

Me meto a mi cuenta de instagram:



También accedo a la pantalla principal de Tiktok:



Ahora me voy a meter en el archivo de configuración de squid donde escribiré las ACL

```
 paula2@ldapserver:~$ cd /etc/squid
 paula2@ldapserver:/etc/squid$ ls -l
 total 320
 drwxr-xr-x 2 root root    4096 feb 19 11:35 conf.d
 -rw-r--r-- 1 root root    1800 ene 16 01:11 errorpage.css
 -rw-r--r-- 1 root root 316874 ene 16 01:11 squid.conf
 paula2@ldapserver:/etc/squid$ sudo nano squid.conf
```

Como el archivo contiene mucha información, en vez de bajar hasta el final voy a escribir arriba, quitando las almohadillas ya no serán comentarios, pongo lo siguiente:

The screenshot shows a terminal window titled "paula2@ldapserver: /etc/squid". The file being edited is "squid.conf". The content of the file includes documentation for the Squid configuration file, a section defining an ACL for social media sites, and a note about documentation defaults. At the bottom of the screen, there is a status bar with keyboard shortcuts for nano editor.

```
GNU nano 4.8          squid.conf          Modificado
#      WELCOME TO SQUID 4.10
#
#
# This is the documentation for the Squid configuration file.
# This documentation can also be found online at:
#     http://www.squid-cache.org/Doc/config/
#
# You may wish to look at the Squid home page and wiki for the
# FAQ and other documentation:
#     http://www.squid-cache.org/
#     http://wiki.squid-cache.org/SquidFaq
#     http://wiki.squid-cache.org/ConfigExamples

acl redes_sociales dstdomain .instagram.com .tiktok.com
http_access deny redes_sociales
http_access allow all

#
# This documentation shows what the defaults for various directives

^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar Tex^J Justificar^C Posición
^X Salir      ^R Leer fich.^I Reemplazar^U Pegar      ^T Ortografía^L Ir a línea
```

Para que los cambios se apliquen voy a hacer un reload de squid y lo reinicio:

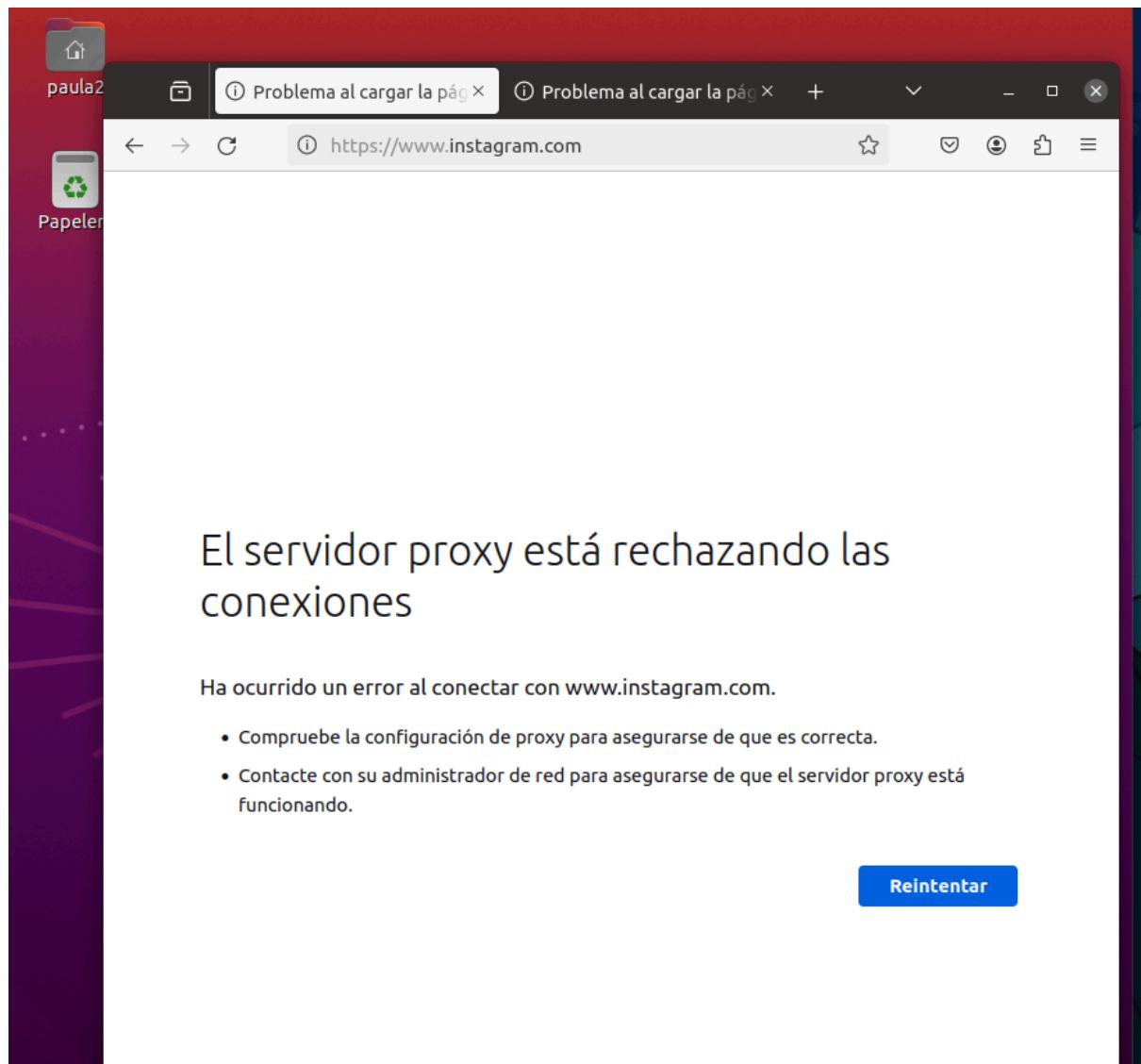
The screenshot shows a terminal window with several command executions related to the squid service. It includes commands for reloading and restarting the service, as well as checking its status. The status output shows the service is active and running.

```
paula2@ldapserver:/etc/squid$ sudo systemctl reload squid
paula2@ldapserver:/etc/squid$ sudo systemctl restart squid

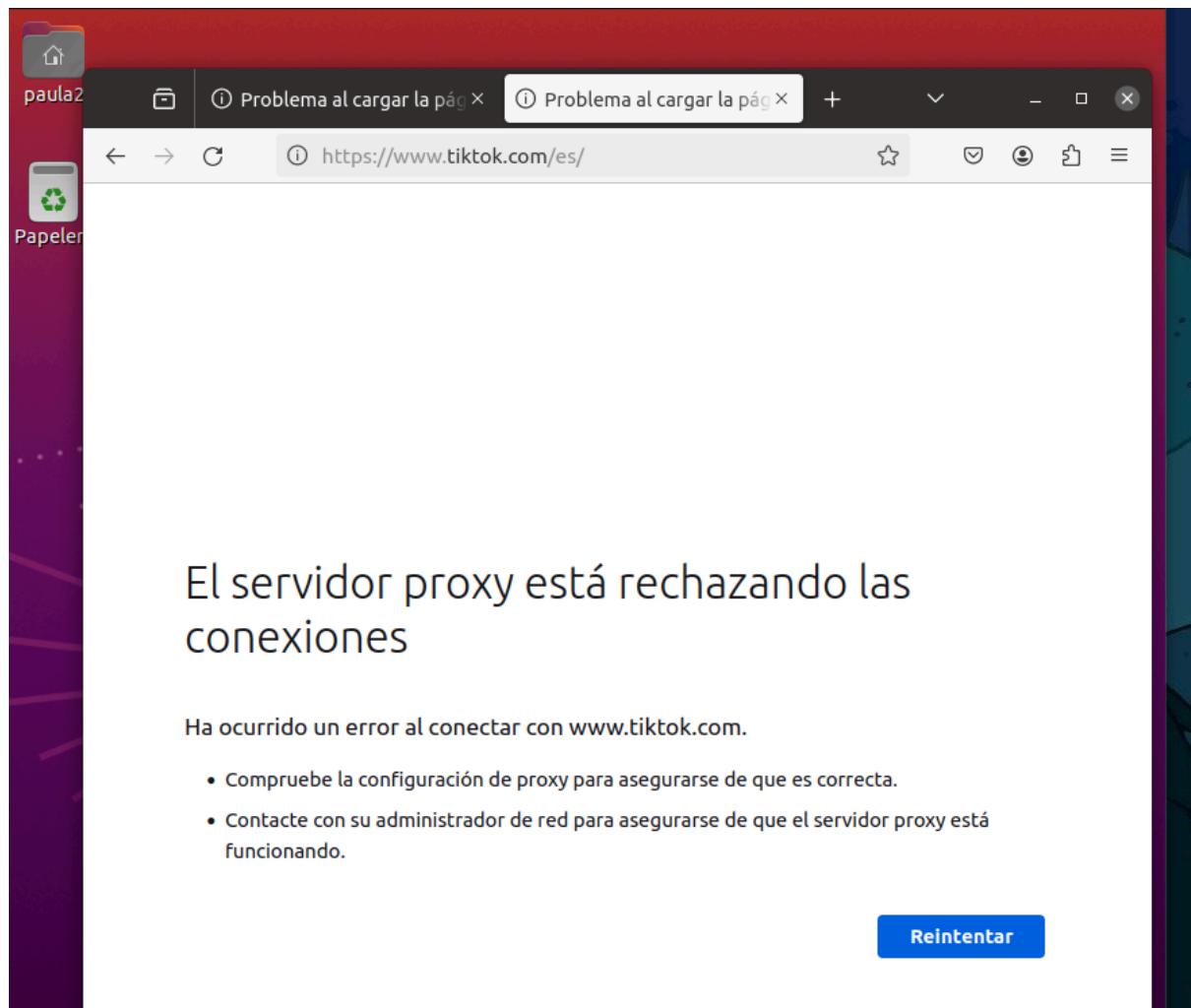
paula2@ldapserver:/etc/squid$ 
paula2@ldapserver:/etc/squid$ sudo systemctl status squid
● squid.service - Squid Web Proxy Server
    Loaded: loaded (/lib/systemd/system/squid.service; enabled; vendor preset:>)
    Active: active (running) since Tue 2024-02-20 10:00:32 UTC; 7s ago
      Docs: man:squid(8)
```

Voy a comprobar si puedo acceder a instagram y tiktok

Instagram:



Tiktok:



Ya no puedo acceder por lo que mis ACL están funcionando correctamente (si puedo acceder por ejemplo a twitter ya que no se me ha pedido bloquear su acceso)

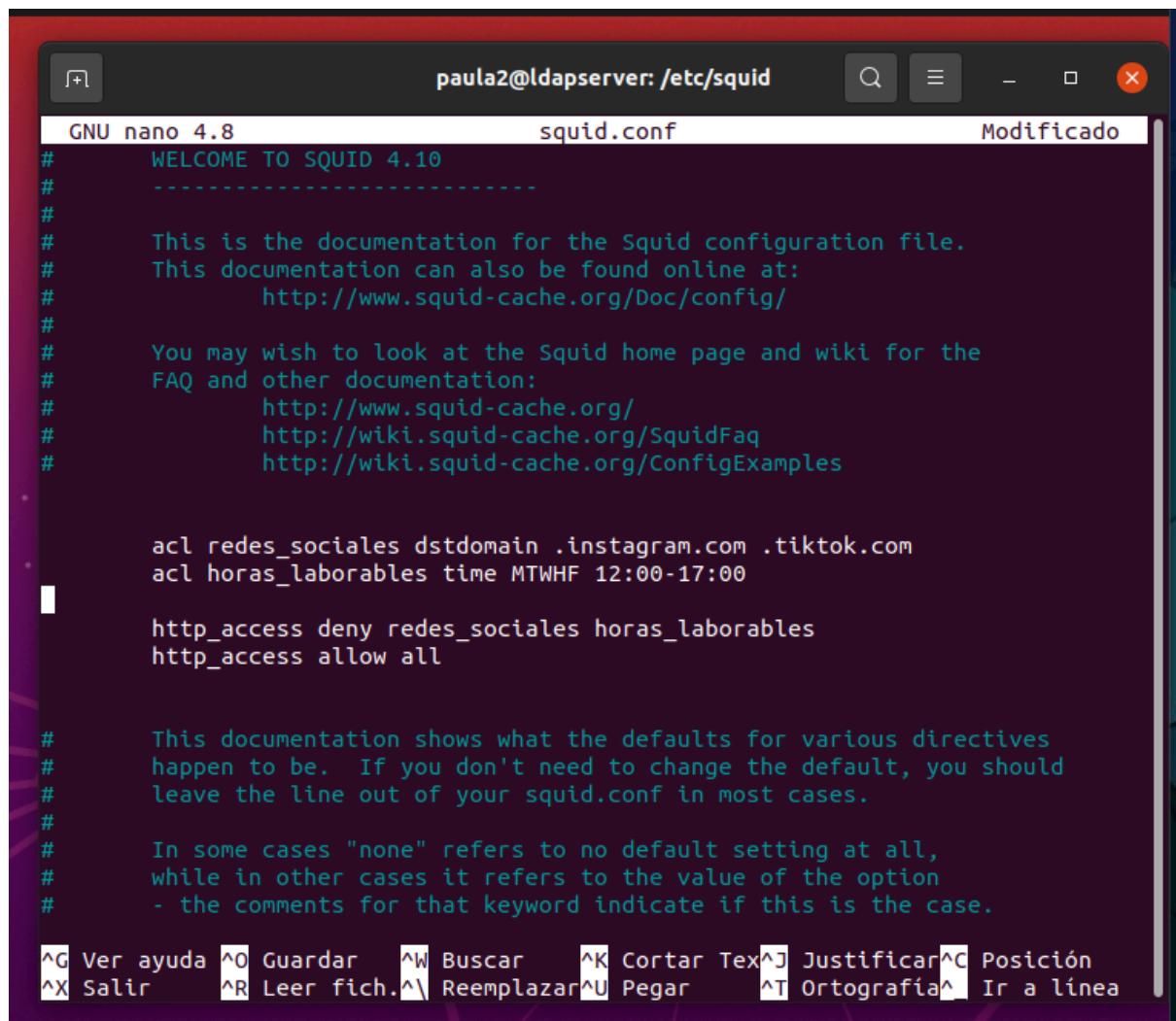
The image shows a screenshot of a web browser window displaying the Twitter sign-up page. The URL in the address bar is <https://twitter.com/?lang=es>. The page features a large, stylized 'X' logo at the top left. Below it, the text 'Lo que está pasando ahora' is displayed in a large, bold, black font. Underneath this, there is a section titled 'Únete Hoy' with two sign-up buttons: 'Registrarse con Google' and 'Registrarse con Apple'. A third button, 'Crear cuenta', is located below them. At the bottom of the page, a small note states: 'Al registrarte, aceptas los [Términos de servicio](#) y la [Política de privacidad](#), incluida la política de [Uso de Cookies](#)'. There is also a link to '¿Ya tienes una cuenta?'. The browser interface includes tabs for other open pages like 'Problema al car'.

Apartado 2: ACL “Horas_laborales”

Si lo que nos interesa es que no se pueda acceder a estas redes sociales en un horario concreto, tenemos que establecer otra ACL de la siguiente forma:

1º Prueba con horario que me permite comprobar.

Establezco este horario ya que no estoy dentro de él y puedo entrar a las páginas a las que, posteriormente no podré



```
GNU nano 4.8          squid.conf          Modificado
#      WELCOME TO SQUID 4.10
#
#
#      This is the documentation for the Squid configuration file.
#      This documentation can also be found online at:
#          http://www.squid-cache.org/Doc/config/
#
#      You may wish to look at the Squid home page and wiki for the
#      FAQ and other documentation:
#          http://www.squid-cache.org/
#          http://wiki.squid-cache.org/SquidFaq
#          http://wiki.squid-cache.org/ConfigExamples

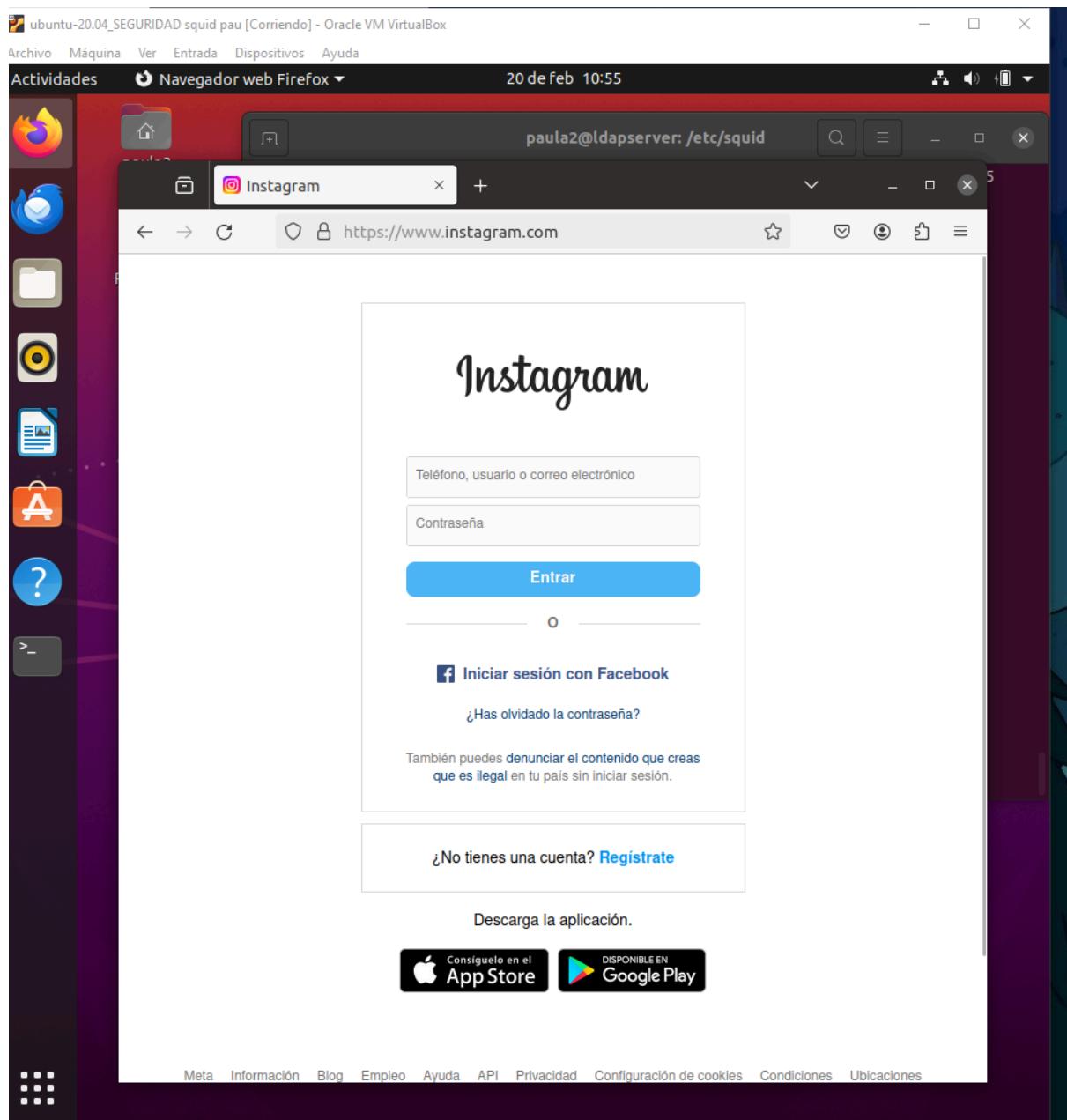
acl redes_sociales dstdomain .instagram.com .tiktok.com
acl horas_laborables time MTWTF 12:00-17:00

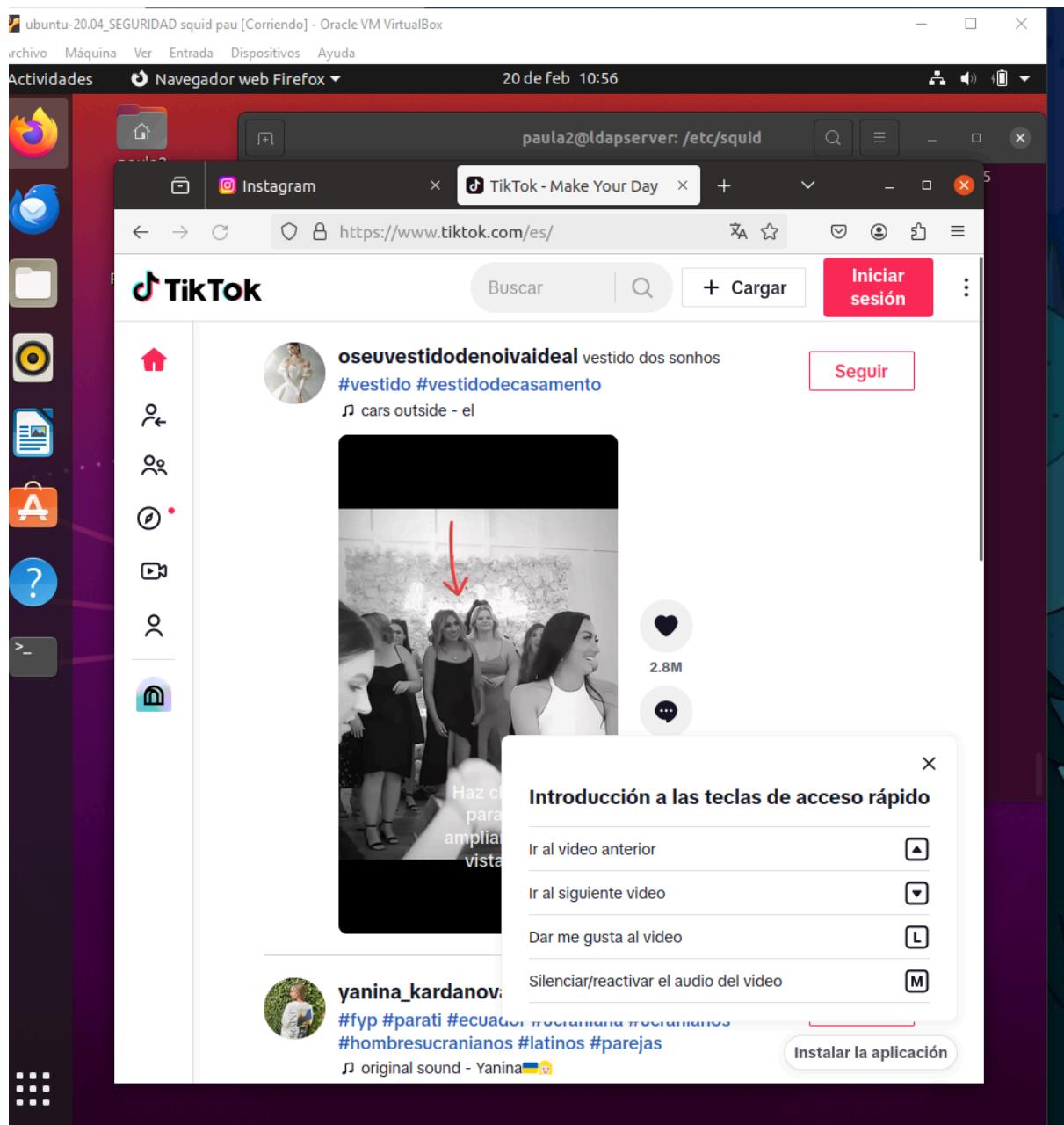
http_access deny redes_sociales horas_laborables
http_access allow all

#
#      This documentation shows what the defaults for various directives
#      happen to be. If you don't need to change the default, you should
#      leave the line out of your squid.conf in most cases.
#
#      In some cases "none" refers to no default setting at all,
#      while in other cases it refers to the value of the option
#      - the comments for that keyword indicate if this is the case.

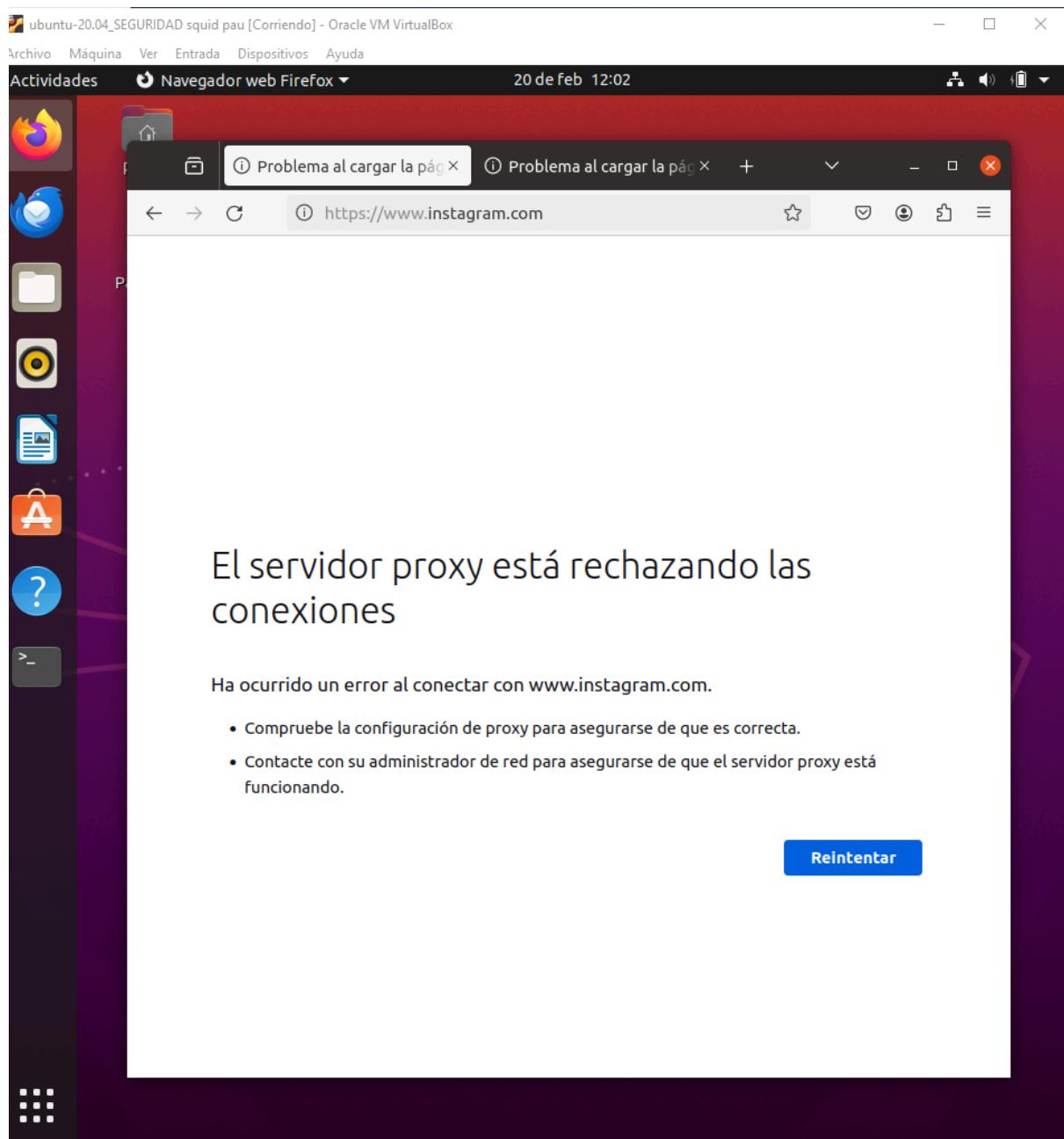
^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar Tex^J Justificar^C Posición
^X Salir    ^R Leer fich.^L Reemplazar^U Pegar    ^T Ortografía^I Ir a línea
```

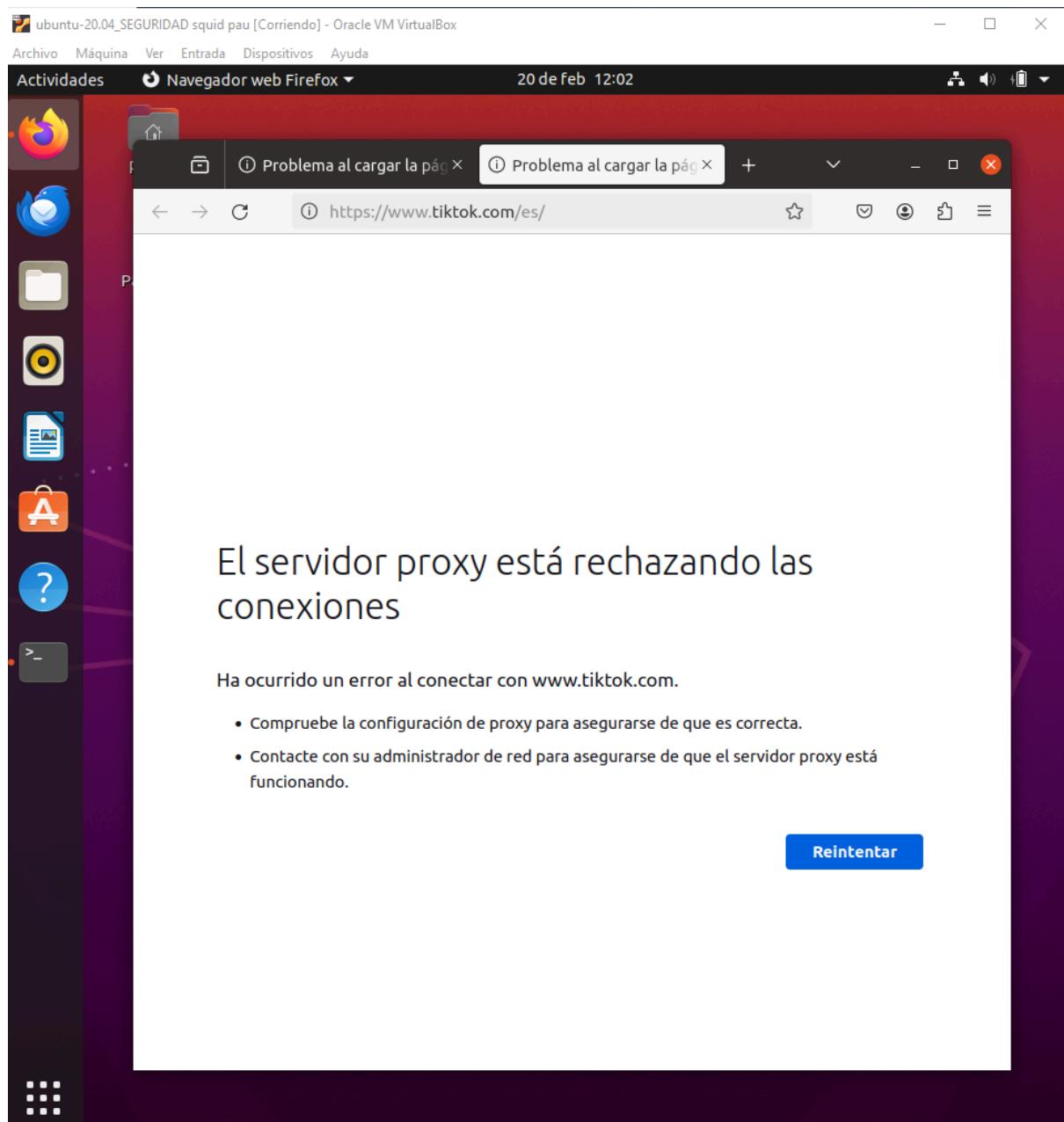
Son las 10:55 de la mañana por lo que no estoy en ese horario laboral y puedo ver instagram y tiktok





Ahora son las 12:00, voy a probar a entrar de nuevo

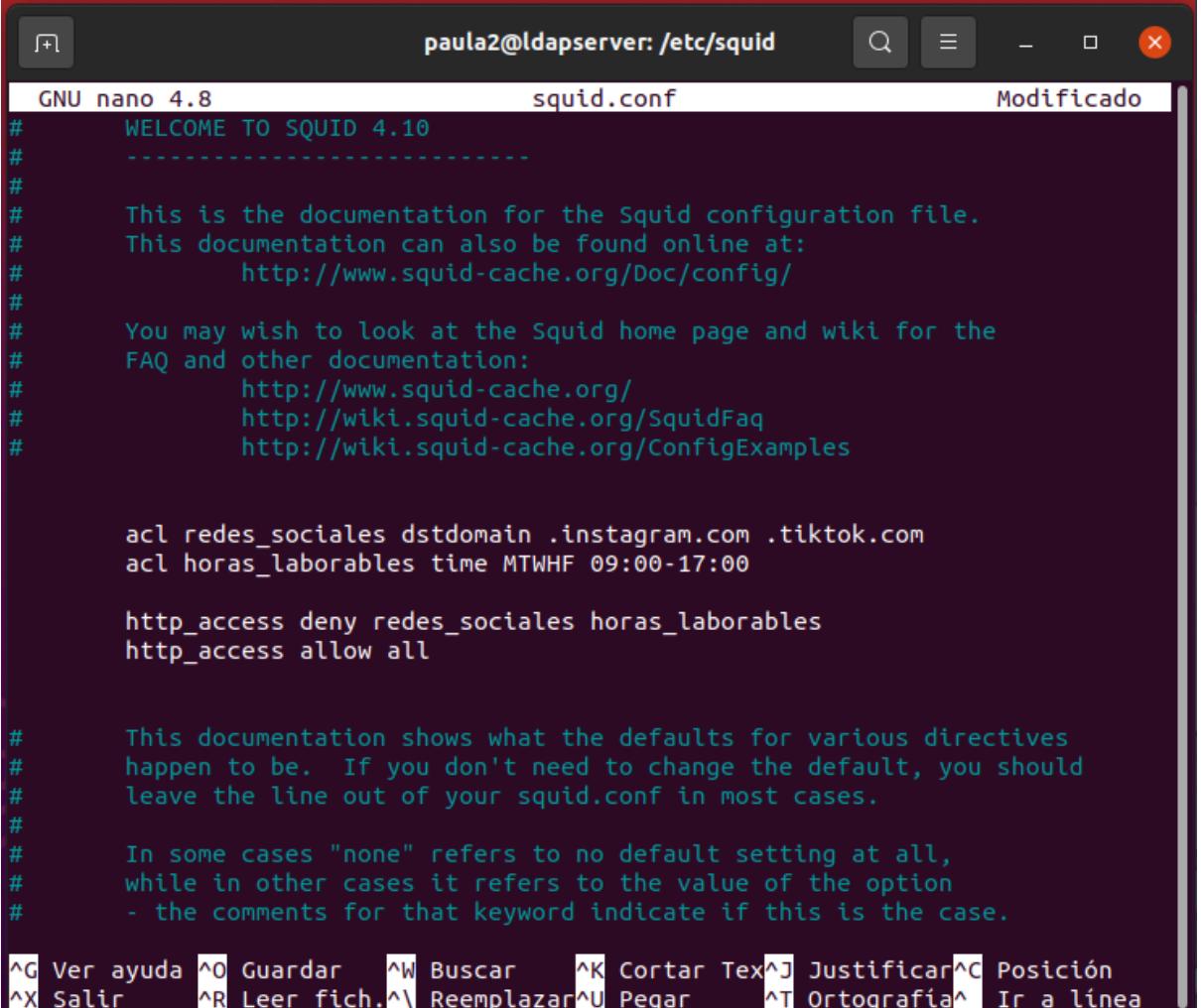




No me deja por lo que mi ACL funciona

2º Horario pedido para la práctica.

Ahora que he comprobado que denegar acceso por horario funciona, voy a configurar la ACL de nuevo pero con el horario pedido en el enunciado.



The screenshot shows a terminal window titled "paula2@ldapserver: /etc/squid". The window contains the squid.conf configuration file for Squid 4.10. The file includes documentation on how to use the configuration, defines access control lists (acl) for social media domains and work hours, and specifies rules for access. It also contains comments about default settings and notes on the "none" keyword. At the bottom, there are nano editor key bindings.

```
GNU nano 4.8          squid.conf          Modificado
#
# WELCOME TO SQUID 4.10
#
#-----#
#
# This is the documentation for the Squid configuration file.
# This documentation can also be found online at:
#     http://www.squid-cache.org/Doc/config/
#
# You may wish to look at the Squid home page and wiki for the
# FAQ and other documentation:
#     http://www.squid-cache.org/
#     http://wiki.squid-cache.org/SquidFaq
#     http://wiki.squid-cache.org/ConfigExamples
#
# acl redes_sociales dstdomain .instagram.com .tiktok.com
# acl horas_laborables time MTWHF 09:00-17:00
#
# http_access deny redes_sociales horas_laborables
# http_access allow all
#
# This documentation shows what the defaults for various directives
# happen to be. If you don't need to change the default, you should
# leave the line out of your squid.conf in most cases.
#
# In some cases "none" refers to no default setting at all,
# while in other cases it refers to the value of the option
# - the comments for that keyword indicate if this is the case.
#
^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar Tex^J Justificar^C Posición
^X Salir      ^R Leer fich.^\\ Reemplazar^U Pegar      ^T Ortografía^_ Ir a línea
```

Así el horario queda de nueve de la mañana a las cinco de la tarde en vez de a las doce como puse para poder probar, se hace un reload y un start y ya estaría funcionando.

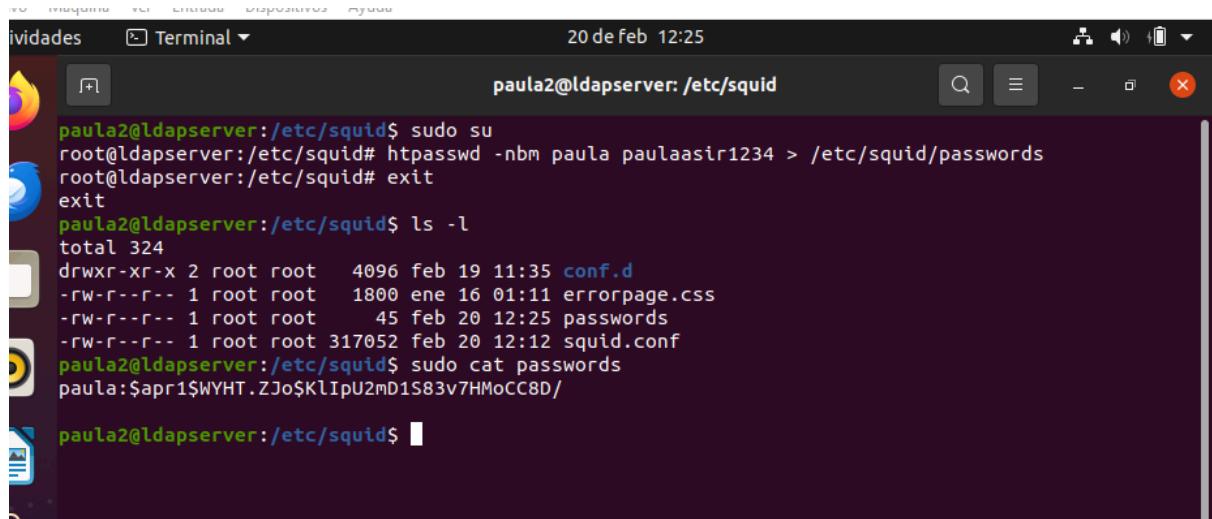
Apartado 3: Autenticación de squid con NCSA

Voy a utilizar la página facilitada por el profesor para realizar esta parte:

<https://wiki.squid-cache.org/ConfigExamples/Authenticate/Ncsa>

Tengo que crear el archivo y el usuario con su contraseña.

El comando htpasswd -c -nbm /etc/squid/passwords username password me está dando problema ya que -c y -n están entrando en conflicto, voy a usar la siguiente estructura:



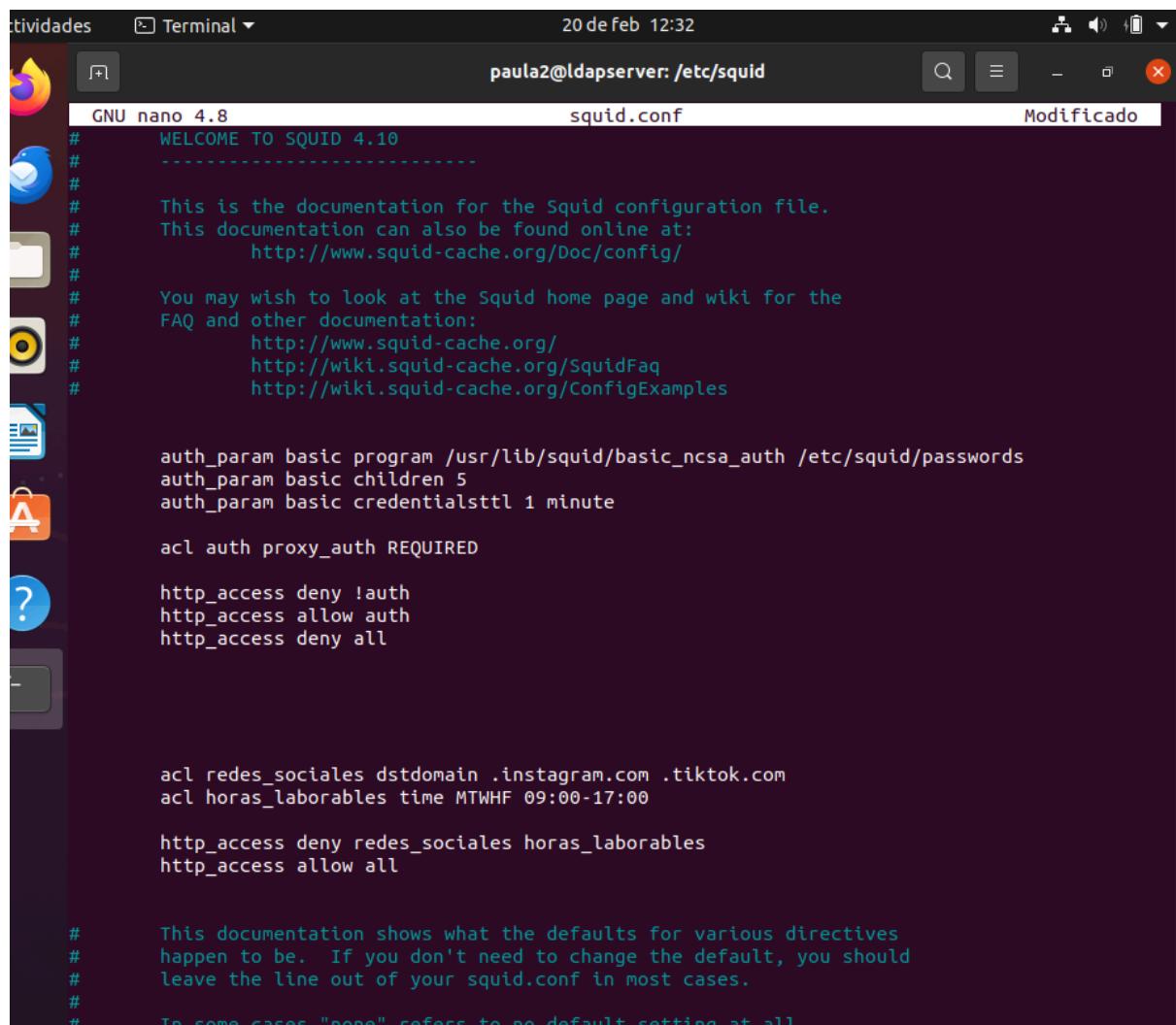
The screenshot shows a terminal window titled "Terminal" with the command line "paula2@ldapserver: /etc/squid". The user runs "htpasswd -nbm paula paulaasir1234 > /etc/squid/passwords" to create a password entry. Then, they exit the root shell with "exit". Finally, they run "ls -l" to show the contents of the directory, which includes files like "conf.d", "errorpage.css", "passwords", and "squid.conf". They then use "sudo cat passwords" to view the contents of the password file, which shows the hashed password "paula:\$apr1\$WYHT.ZJo\$KlIpU2mD1S83v7HMoCC8D/".

```
paula2@ldapserver:/etc/squid$ sudo su
root@ldapserver:/etc/squid# htpasswd -nbm paula paulaasir1234 > /etc/squid/passwords
root@ldapserver:/etc/squid# exit
paula2@ldapserver:/etc/squid$ ls -l
total 324
drwxr-xr-x 2 root root 4096 feb 19 11:35 conf.d
-rw-r--r-- 1 root root 1800 ene 16 01:11 errorpage.css
-rw-r--r-- 1 root root 45 feb 20 12:25 passwords
-rw-r--r-- 1 root root 317052 feb 20 12:12 squid.conf
paula2@ldapserver:/etc/squid$ sudo cat passwords
paula:$apr1$WYHT.ZJo$KlIpU2mD1S83v7HMoCC8D/

paula2@ldapserver:/etc/squid$
```

tengo que recordar este usuario y contraseña ya que lo usaré posteriormente para poder acceder a los sitios web.

Ahora voy a modificar el archivo de configuración y añado las líneas que podemos encontrar en la página que he mostrado antes



The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "Terminal" and the command line shows "paula2@ldapserver: /etc/squid". The window content is the "squid.conf" configuration file for Squid 4.10. The file includes documentation for the Squid configuration file, instructions for basic authentication, and specific rules for social media access during work hours. The terminal window has a dark theme and is part of the Unity interface.

```
GNU nano 4.8          squid.conf          Modificado
# WELCOME TO SQUID 4.10
#
# This is the documentation for the Squid configuration file.
# This documentation can also be found online at:
#     http://www.squid-cache.org/Doc/config/
#
# You may wish to look at the Squid home page and wiki for the
# FAQ and other documentation:
#     http://www.squid-cache.org/
#     http://wiki.squid-cache.org/SquidFaq
#     http://wiki.squid-cache.org/ConfigExamples

auth_param basic program /usr/lib/squid/basic_ncsa_auth /etc/squid/passwords
auth_param basic children 5
auth_param basic credentialsttl 1 minute

acl auth proxy_auth REQUIRED

http_access deny !auth
http_access allow auth
http_access deny all

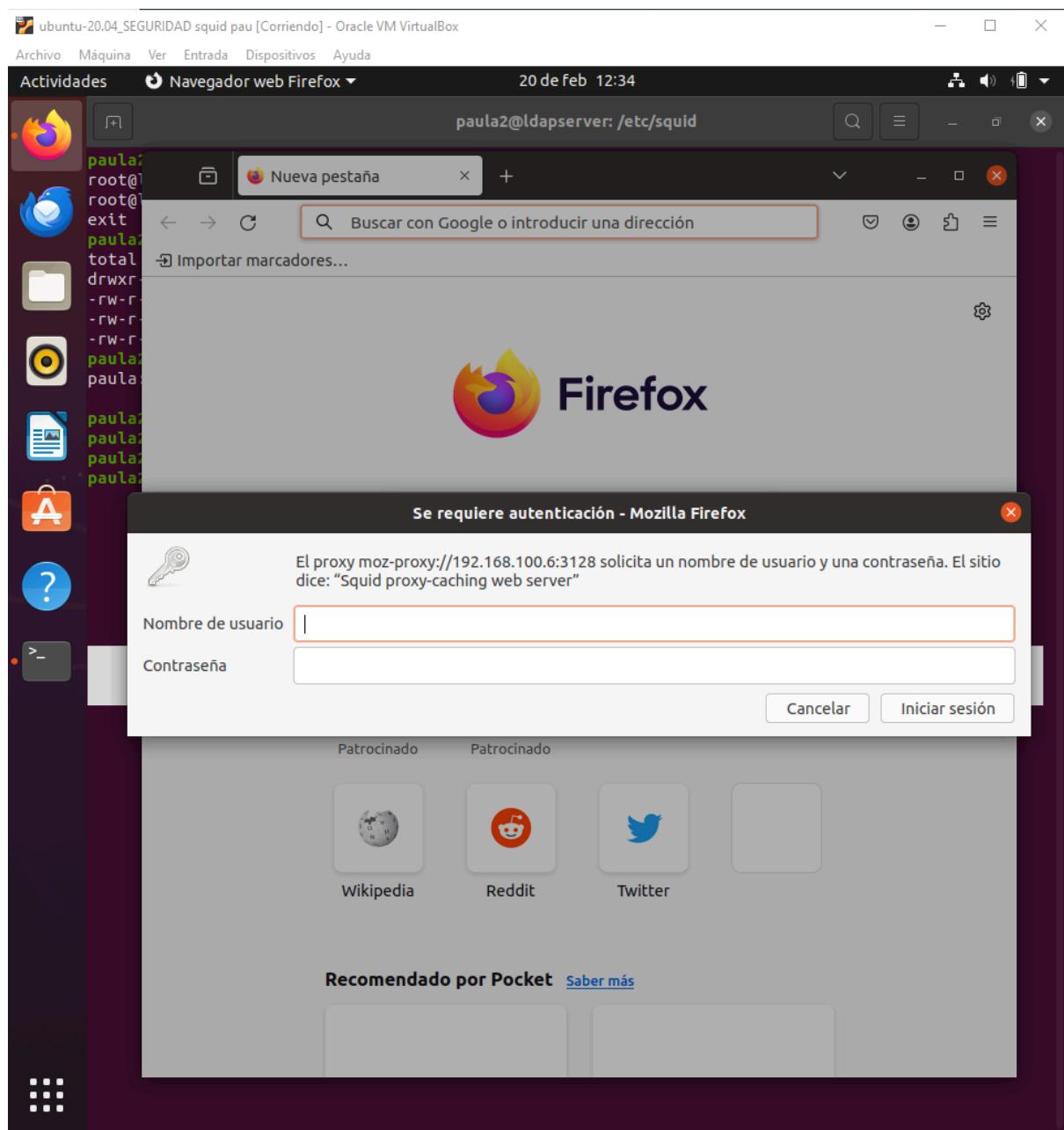
acl redes_sociales dstdomain .instagram.com .tiktok.com
acl horas_laborables time MTWHF 09:00-17:00

http_access deny redes_sociales horas_laborables
http_access allow all

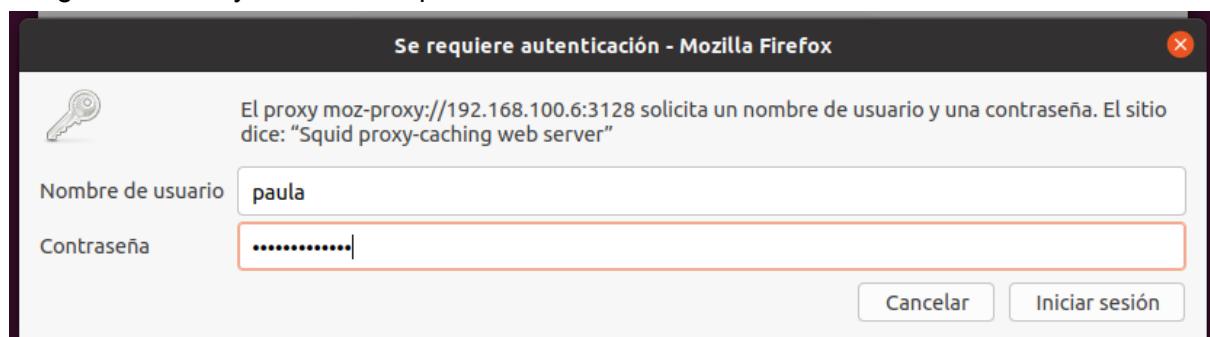
#
# This documentation shows what the defaults for various directives
# happen to be. If you don't need to change the default, you should
# leave the line out of your squid.conf in most cases.
#
# To some cases "none" refers to no default setting at all
```

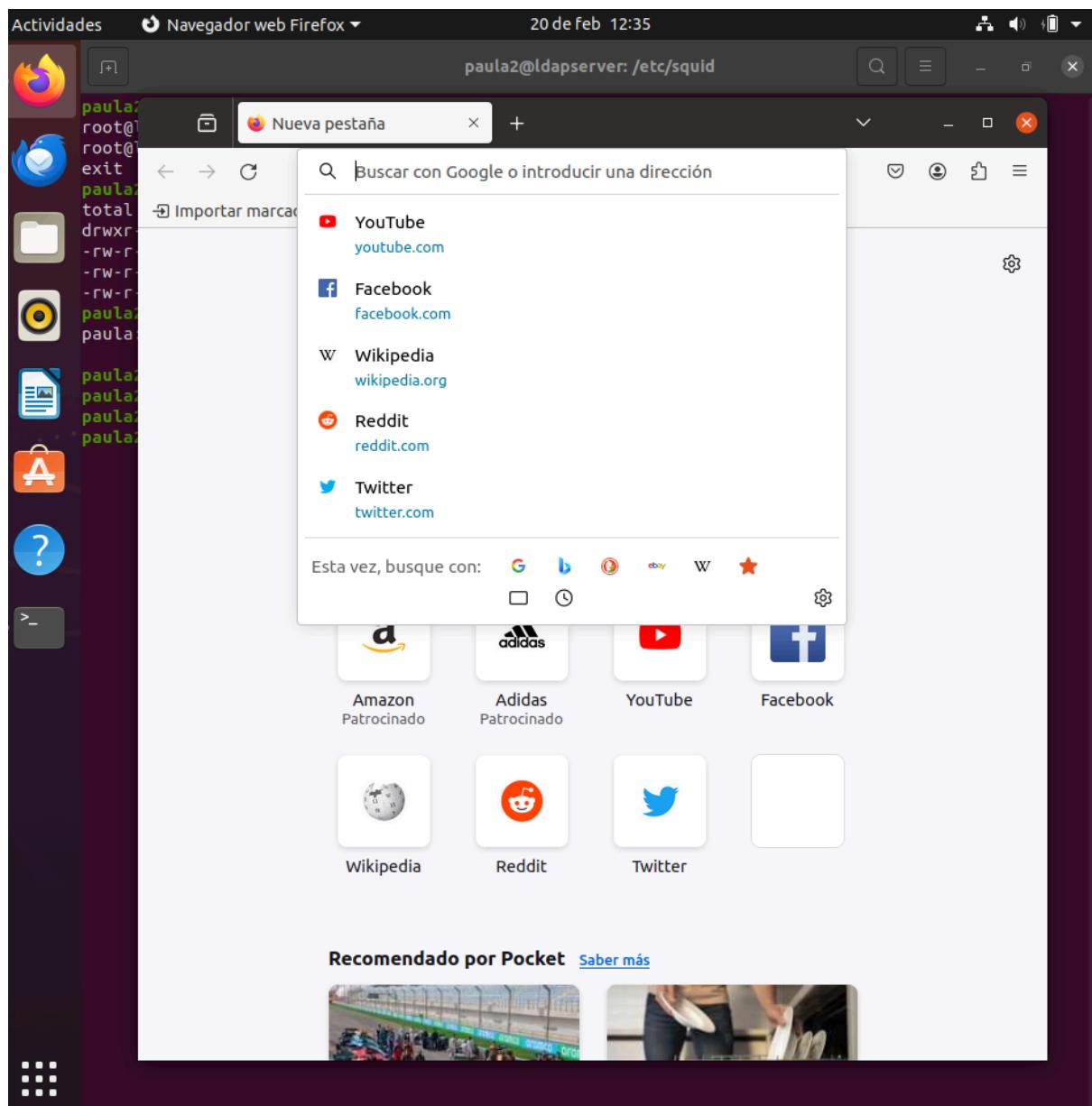
Después de guardar esta configuración, hago un reload y un restart.

Al meterme a firefox me abre esta pestaña de login



Pongo el usuario y contraseña que creé anteriormente





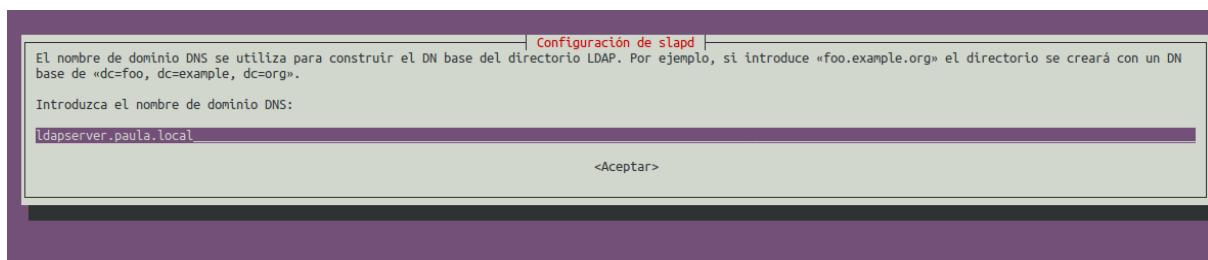
Una vez he metido las credenciales ya puedo usar mi navegador

Apartado 4: Autenticación de squid con LDAP

Para poder realizar este apartado será necesario tener un servidor de LDAP funcionando, en mi caso ya tengo ldap instalado

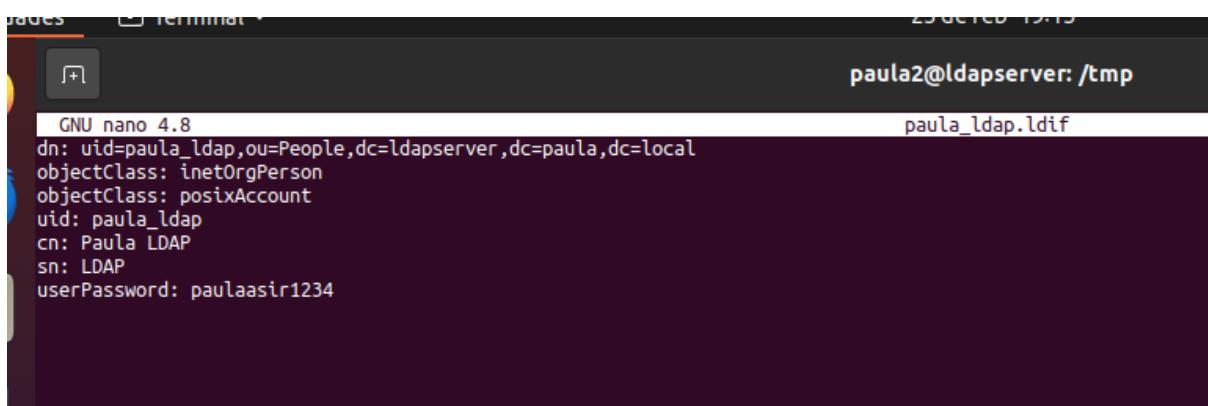
```
paula2@ldapserver:~$ sudo apt-get install slapd ldap-utils
[sudo] contraseña para paula2:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
ldap-utils ya está en su versión más reciente (2.4.49+dfsg-2ubuntu1.10).
slapd ya está en su versión más reciente (2.4.49+dfsg-2ubuntu1.10).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 4 no actualizados.
paula2@ldapserver:~$
```

con este comando: sudo dpkg-reconfigure slapd voy a hacer la configuración necesaria, así se va a llamar (tanto el servidor como el dominio)



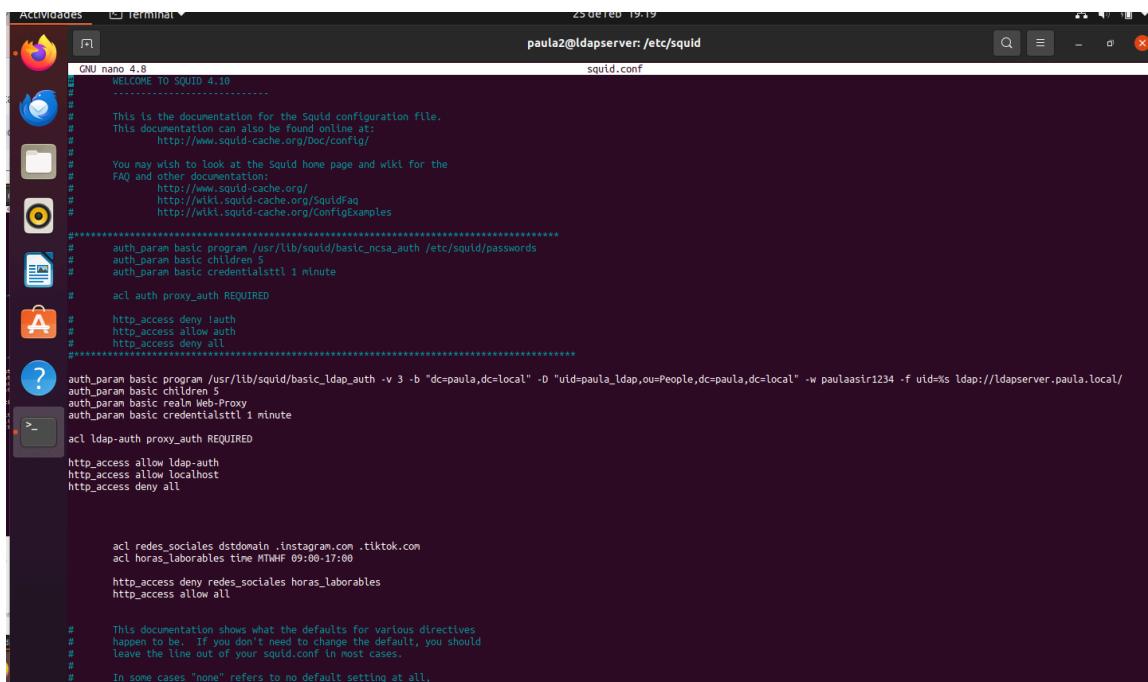
Voy a crear un usuario dentro de mi servicio de LDAP para poder usar esas credenciales

De esta forma tendré al usuario paula_ldap:



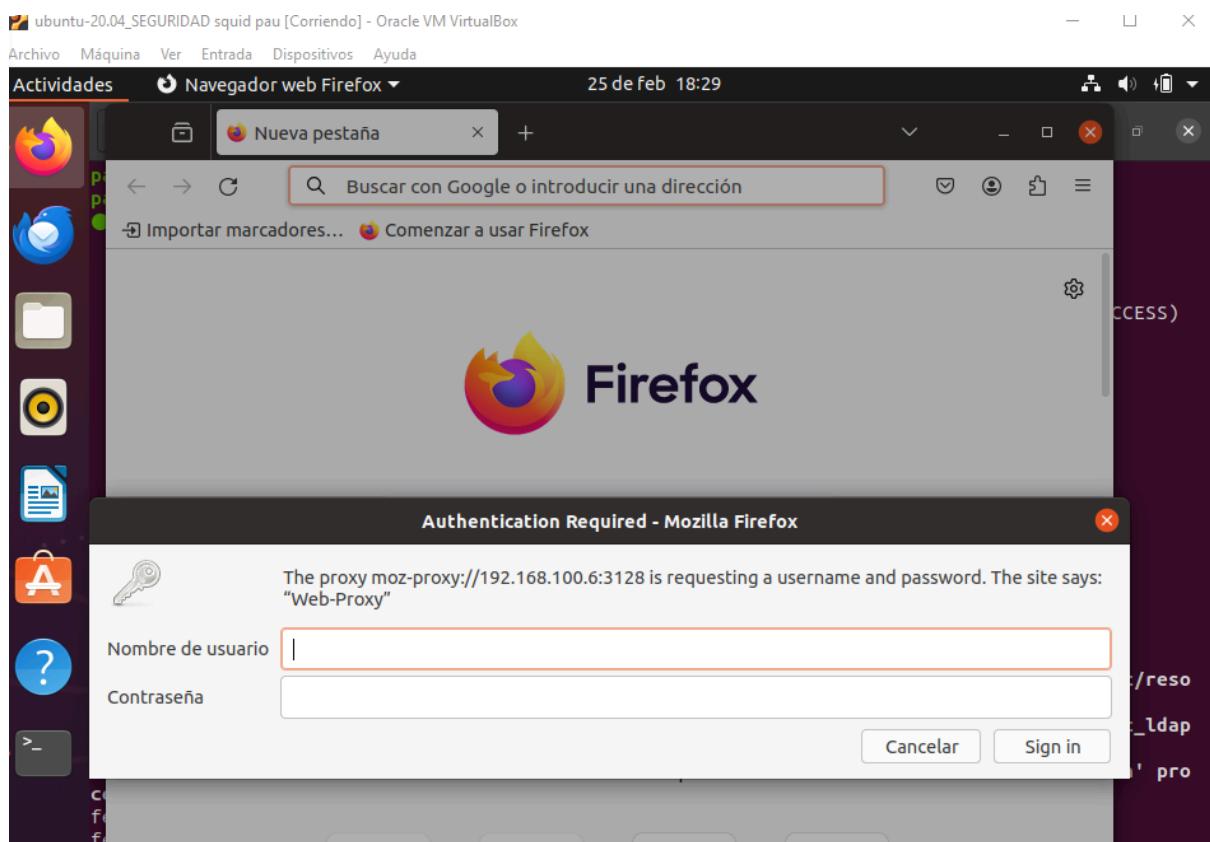
```
GNU nano 4.8
dn: uid=paula_ldap,ou=People,dc=ldapserver,dc=paula,dc=local
objectClass: inetOrgPerson
objectClass: posixAccount
uid: paula_ldap
cn: Paula LDAP
sn: LDAP
userPassword: paulaasir1234
```

Una vez hecho esto, me meto en el archivo de configuración de squid y escribo las siguientes líneas:

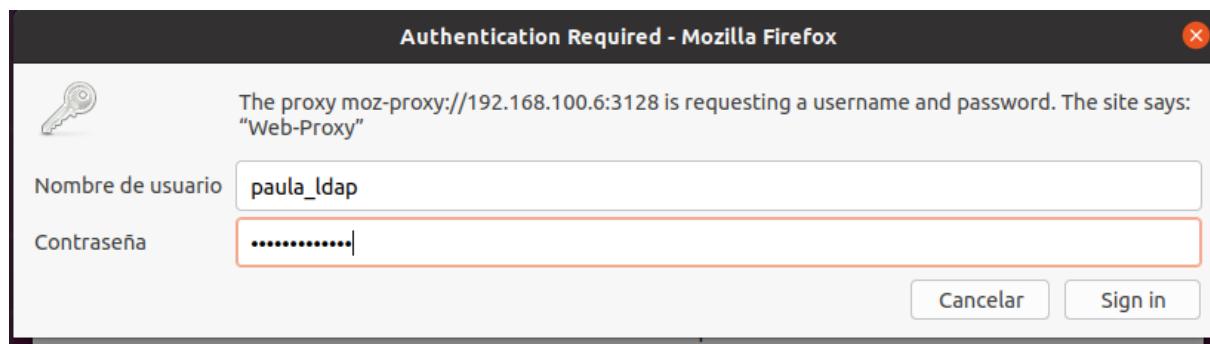


```
GNU nano 4.8
WELCOME TO SQUID 4.10
-----
# This is the documentation for the Squid configuration file.
# This documentation can also be found online at:
#   http://www.squid-cache.org/doc/config/
#
# You may wish to look at the Squid home page and wiki for the
# FAQ and other documentation:
#   http://www.squid-cache.org/
#   http://wiki.squid-cache.org/SquidFAQ
#   http://wiki.squid-cache.org/ConfigExamples
#
#-----#
# auth_param basic program /usr/lib/squid/basic_ncsa_auth /etc/squid/passwords
# auth_param basic children 5
# auth_param basic credentialssttl 1 minute
#
# acl auth proxy_auth REQUIRED
#
#   http_access deny !auth
#   http_access allow auth
#   http_access deny all
#-----#
auth_param basic program /usr/lib/squid/basic_ldap_auth -v 3 -b "dc=paula,dc=local" -D "uid=paula_ldap,ou=People,dc=paula,dc=local" -w paulaasir1234 -f uid=%s ldap://ldapserver.paula.local/
auth_param basic children 5
auth_param basic realm Web-Proxy
auth_param basic credentialssttl 1 minute
#
acl ldap-auth proxy_auth REQUIRED
#
http_access allow ldap-auth
http_access allow localhost
http_access deny all
#
#
#-----#
# acl redes_sociales dstdomain .instagram.com .tiktok.com
# acl horas_laborables time MTWTF 09:00-17:00
#
# http_access deny redes_sociales horas_laborables
# http_access allow all
#
#-----#
# This documentation shows what the defaults for various directives
# happen to be. If you don't need to change the default, you should
# leave the line out of your squid.conf in most cases.
#
# In some cases "none" refers to no default setting at all,
```

Abro mi navegador y me sale una pestaña paraloguearse



meto mis credenciales



No me está funcionando, he verificado todo pero mi servidor de ldap no está funcionando correctamente y por eso no me funciona la autenticación, no sé cómo solucionarlo

Apartado 5: URL Github

https://kixsab.github.io/kixsab/seuridad_paula/index.html

