

Proxy SQUID

A.D.G.

Monta en un servidor linux un proxy squid:

```
andreidaniel@asir:~$ sudo apt install squid
andreidaniel@asir:~$ sudo apt install net-tools
andreidaniel@asir:~$ sudo netstat -apn | grep squid
tcp6      0      0  ::::3128                :::*                    LISTEN      48809/(squid-1)
udp       0      0  0.0.0.0:37734            0.0.0.0:*              48809/(squid-1)
udp6      0      0  :::33235                :::*                   48809/(squid-1)
udp6      0      0  :::1:42653              :::1:36213             ESTABLISHED 48809/(squid-1)
unix  2      [ ]          DGRAM      CONNECTED    80653         48807/squid
unix  3      [ ]          STREAM     CONNECTED    81153         48809/(squid-1)
unix  2      [ ]          DGRAM      CONNECTED    81146         48809/(squid-1)
```

Hacemos una copia de seguridad por si a caso:

```
andreidaniel@localhost:/etc/squid$ sudo cp squid.conf DEFAULTsquid.conf
```

```
andreidaniel@localhost:/etc/squid$ sudo nano squid.conf
```

Luego de modificar el squid.conf, crear los archivos de palabras para las prohibiciones, hacemos que se ejecute el servicio al iniciar la máquina del Ubuntu, y forzamos el arranque con start para probarlo. Comprobamos con status:

```
andreidaniel@localhost:/etc/squid$ sudo systemctl enable squid
Synchronizing state of squid.service with SysV service script with /lib/systemd/systemd-sysv-ins
tall.
Executing: /lib/systemd/systemd-sysv-install enable squid
andreidaniel@localhost:/etc/squid$ sudo systemctl start squid
andreidaniel@localhost:/etc/squid$ sudo systemctl status squid
● squid.service - Squid Web Proxy Server
   Loaded: loaded (/lib/systemd/system/squid.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2023-02-08 00:44:41 CET; 47s ago
     Docs: man:squid(8)
  Main PID: 3007 (squid)
    Tasks: 4 (limit: 2227)
   Memory: 15.6M
      CPU: 276ms
   CGroup: /system.slice/squid.service
           └─3007 /usr/sbin/squid --foreground -sYC
             └─3009 "(squid-1)" --kid squid-1 --foreground -sYC
               └─3010 "(logfile-daemon)" /var/log/squid/access.log
                 └─3011 "(pinger)"

feb 08 00:44:41 localhost.localdomain squid[3009]: Using Least Load store dir selection
feb 08 00:44:41 localhost.localdomain squid[3009]: Set Current Directory to /var/spool/squid
feb 08 00:44:41 localhost.localdomain squid[3009]: Finished loading MIME types and icons.
feb 08 00:44:41 localhost.localdomain squid[3009]: HTTP Disabled.
feb 08 00:44:41 localhost.localdomain squid[3009]: Pinger socket opened on FD 14
feb 08 00:44:41 localhost.localdomain squid[3009]: Squid plugin modules loaded: 0
feb 08 00:44:41 localhost.localdomain squid[3009]: Adaptation support is off.
feb 08 00:44:41 localhost.localdomain squid[3009]: Accepting HTTP Socket connections at conn3 l
feb 08 00:44:41 localhost.localdomain systemd[1]: Started Squid Web Proxy Server.
feb 08 00:44:42 localhost.localdomain squid[3009]: storeLateRelease: released 0 objects
lines 1-24/24 (END)
```

y copiamos la configuración que tienes anotada en el aula.

Servidor:

**Lubuntu Proxy SQUID** (Base enlazada para Lub...)
Apagada

**Red**
Adaptador 1: Intel PRO/1000 MT Desktop (Red interna, «ProxySQUID»)
Adaptador 2: Intel PRO/1000 MT Desktop (Adaptador puente, «Intel(R) Wi-Fi 6 AX200 160MHz #2»)

La red interna tiene el: Modo promiscuo: Permitir todo

```
andreidaniel@asir:~$ sudo apt-get install apache2-utils para usar htpasswd
```

Cliente:

**Lubuntu Cliente** (Base enlazada para Lubuntu Cl...)
Apagada

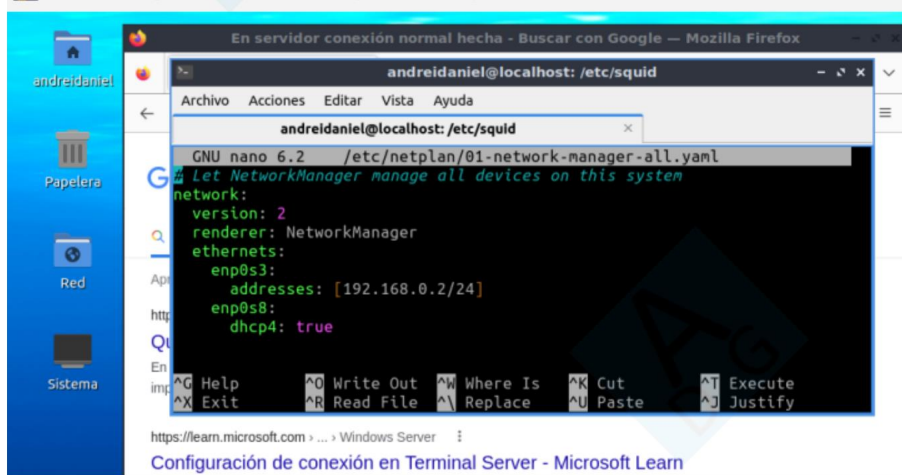
**Red**
Adaptador 1: Intel PRO/1000 MT Desktop (Red interna, «ProxySQUID»)

Se debe configurar de la siguiente forma:

--> acceso normal a internet (**PARA EL CLIENTE A TRAVÉS DEL ADAPTADOR PUENTE DEL SERVIDOR**):

Servidor:

Lubuntu Proxy SQUID (Base enlazada para Lubuntu y Lubuntu Flask) [Corriendo] - Oracle VM VirtualBox

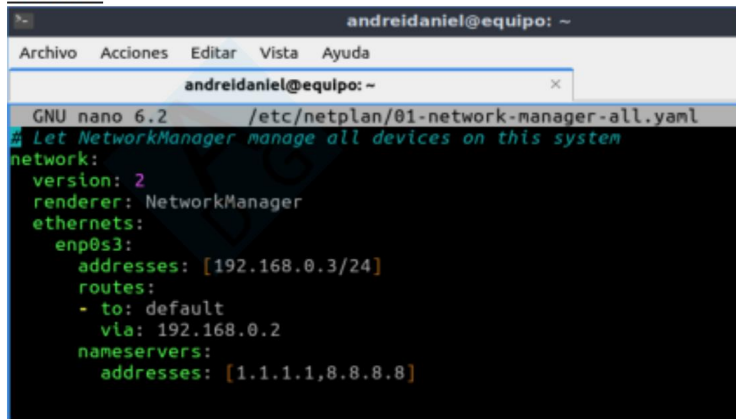


```
andrei@daniel@localhost: /etc/squid
GNU nano 6.2 /etc/netplan/01-network-manager-all.yaml
Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: NetworkManager
  ethernet:
    enp0s3:
      addresses: [192.168.0.2/24]
      dhcp4: true
Help Write Out Where Is Cut Execute
Exit Read File Replace Paste Justify

https://learn.microsoft.com > ... > Windows Server
Configuración de conexión en Terminal Server - Microsoft Learn
```

```
andrei@daniel@localhost:/etc/squid$ sudo su && echo 1 > /proc/sys/net/ipv4/ip_forward
root@localhost:/etc/squid# iptables -F
root@localhost:/etc/squid# iptables -A FORWARD -j ACCEPT
root@localhost:/etc/squid# iptables -t nat -A POSTROUTING -s 192.168.0.0/24 -o enp0s8 -j MASQUERADE
```

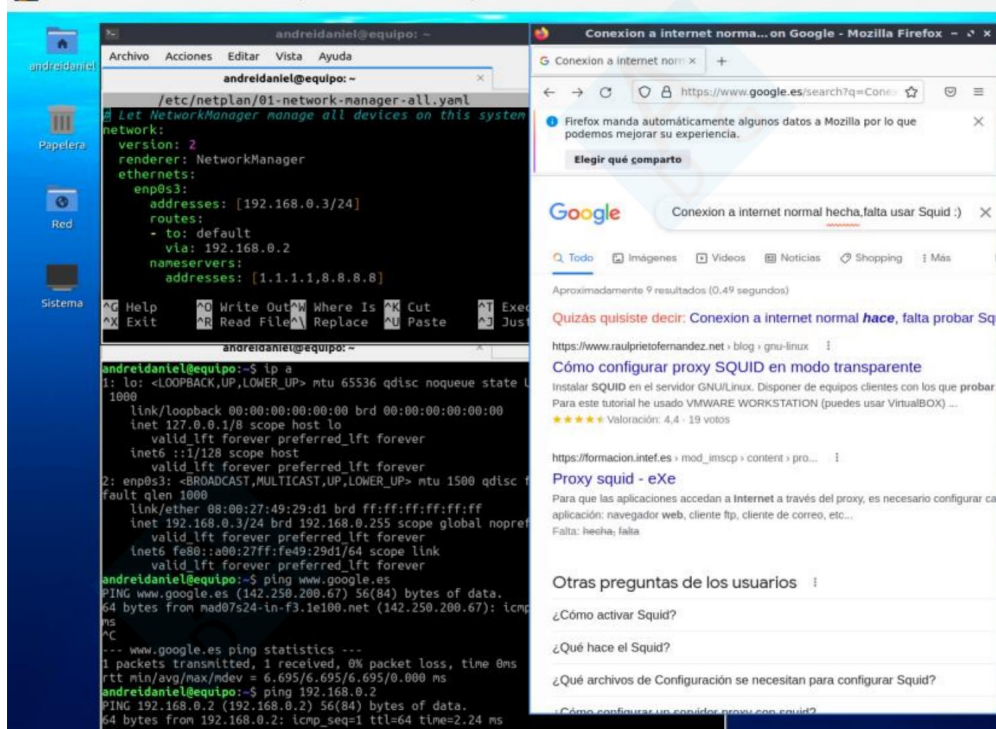
Cliente:



```
andrei@daniel@equipo: ~
GNU nano 6.2 /etc/netplan/01-network-manager-all.yaml
Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: NetworkManager
  ethernet:
    enp0s3:
      addresses: [192.168.0.3/24]
      routes:
        - to: default
          via: 192.168.0.2
      nameservers:
        addresses: [1.1.1.1, 8.8.8.8]
```

Acceso normal a Internet para el **Cliente** que tiene sólo una Red Interna logrado:

Lubuntu Cliente (Base enlazada para Lubuntu Cliente y Lubuntu Cliente clonar) [Corriendo]...



```
andrei@daniel@equipo: ~
GNU nano 6.2 /etc/netplan/01-network-manager-all.yaml
Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: NetworkManager
  ethernet:
    enp0s3:
      addresses: [192.168.0.3/24]
      routes:
        - to: default
          via: 192.168.0.2
      nameservers:
        addresses: [1.1.1.1, 8.8.8.8]

andrei@daniel@equipo:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state L
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc f
    link/ether 08:00:27:49:29:d1 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.3/24 brd 192.168.0.255 scope global nopref
        valid_lft forever preferred_lft forever
    inet6 fe80::a0:27ff:fe49:29d1/64 scope link
        valid_lft forever preferred_lft forever
andrei@daniel@equipo:~$ ping www.google.es
PING www.google.es (142.250.200.67) 56(84) bytes of data.
64 bytes from nad07s24-in-f3.1e100.net (142.250.200.67): icmp
ms
--- www.google.es ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/ndev = 6.695/6.695/6.695/0.000 ms
andrei@daniel@equipo:~$ ping 192.168.0.2
PING 192.168.0.2 (192.168.0.2) 56(84) bytes of data.
64 bytes from 192.168.0.2: icmp_seq=1 ttl=64 time=2.24 ms
```

profe – profe

```
andreidaniel@asir:~$ sudo su
root@asir:/home/andreidaniel# htpasswd -bc /etc/squid/users profe profe
Adding password for user profe
```

nombre – nombre

```
root@asir:/etc/squid# htpasswd -b /etc/squid/users andrei andrei
Adding password for user andrei
```

--> usuarios que acceden al [proxy](#): El mensaje sea "SQUID GAME de ASIR"

--> Prohibiciones

--> tiene que conectarse con uno de los usuarios

--> No puede entrar a ninguna red social

--> No puede entrar a máquinas que sean de soccer, deportes, tenis

--> No pueden entrar a as.com

--> No pueden entrar a eldiario.es

Se debe entregar:

Captura/s de la configuración de prohibiciones

```
GNU nano 6.2 squid.conf
# WELCOME TO SQUID 5.2
# -----
auth_param basic program /usr/lib/squid/basic_ncsa_auth /etc/squid/users
auth_param basic children 30
auth_param basic realm SQUID GAME de ASIR
acl identificacion proxy_auth REQUIRED

acl RedesSociales url_regex -i "/etc/squid/RedesSociales_bloqueadas"
http_access deny RedesSociales

acl Deportes url_regex -i "/etc/squid/Deportes_bloqueados"
http_access deny Deportes

acl As dstdomain www.As.com
http_access deny As

acl ElDiario dstdomain www.ElDiario.es
http_access deny ElDiario

http_access allow identificacion
#
# This is the documentation for the Squid configuration file.
# This documentation can also be found online at:
# http://www.squid-cache.org/Doc/config/
```

Captura de archivos externos si se han utilizado

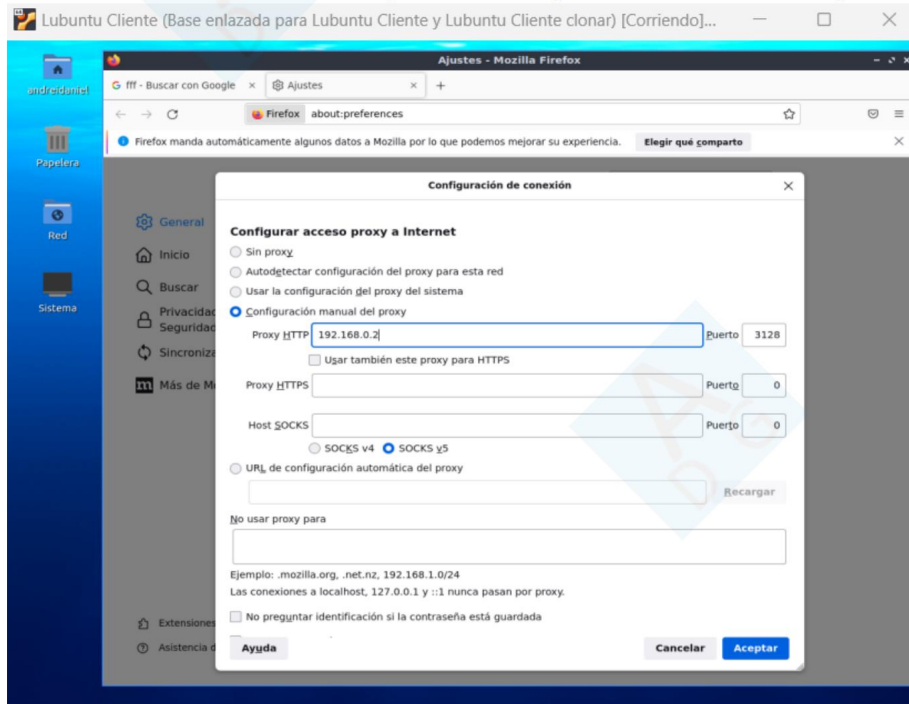
```
GNU nano 6.2 /etc/squid/users
profe:$apr1$acLg2lB4$97GVvT1fNVreG5XrVJ.vo.
andrei:$apr1$R0e99NwH$Qx50s10TIh343Ln7ZQ0dB1

/etc/squid/RedesSociales_bloqueadas *
facebook
instagram
linkedin
twitter
youtube
tiktok

/etc/squid/Deportes_bloqueados *
soccer
deportes
tenis
```


Captura de poner proxy en el navegador de un ordenador de la red

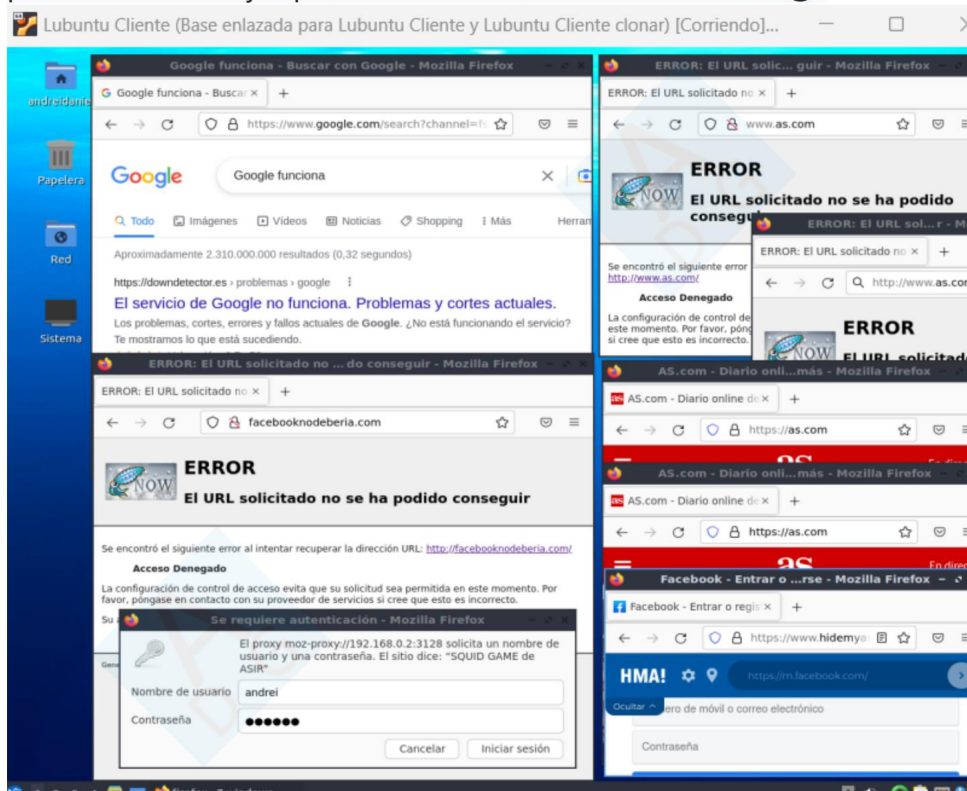
Mozilla Firefox: Botón menú > Ajustes > Configuración de Red > Configuración > Configuración manual del proxy >



Captura entrando a la pantalla de login desde un ordenador de la red

Captura entrando a una página bloqueada

Como se puede observar: En Google accedemos. En facebooknodeberia no por incluir "facebook" en la dirección. En "www.as.com" no porque lo establecimos así, sin embargo si no se añaden más formas de escribirla podrán acceder ya que sólo detecta si se incluye "www.as.com" en la dirección. Igualmente podríamos hacer más trampeos y usar un proxy desde otro proxy 😊 y lograríamos acceder, por ejemplo a Facebook (se supone que ya puede uno usar <http://facebook.com>, www.facebook.com, <https://facebook.com>, <http://www.facebook.com>, <https://www.facebook.com>, facebook.com, facebook.es, hastaestadefacebookquenoexiste.com y no permitiría el acceso, pero usando un proxy más en el cliente podemos acceder ya que cambia la URL sin incluir facebook 😊):



Lubuntu Cliente (Base enlazada para Lubuntu Cliente y Lubuntu Cliente clonar) [Corriendo]...

Facebook - Entrar o registrarse - Mozilla Firefox

Facebook - Entrar o regis...

← → ↻ <https://www.hidemypass-freeproxy.com/proxy/es-es/aHR0cHM6Ly93d3cuZmFjZWJyb2suY291LTlw>

HIDE my ASS!
Proxy web

<https://m.facebook.com/>

Prueba de la VPN gratuita

Entrar

[¿Has olvidado la contraseña?](#)

[Crear cuenta nueva](#)

Español (España)
Polski
Italiano
Deutsch

English (UK)
Français (France)
Português (Brasil)

[Información](#) - [Ayuda](#) - [Más](#)
Meta © 2023