

EJERCICIOS DE SQUID

♦ 1. Verificar instalación de Squid

Este ejercicio lo haremos individual, y después en grupo, de manera que el equipo se conectará al proxy de uno de los compañeros.

En Kali ya suele venir en los repositorios. Comprueba:

squid -v

```
~/Documents/box > squid -v
Squid Cache: Version 7.1
Service Name: squid
Debian GNU/Linux 13 (trixie)
configure options: '--build=x86_64-linux-gnu' '--prefix=/usr' '--sysconfdir=/etc/squid' '--localisedir=/usr/share/squid' '--infodir=${prefix}/share/info' '--sysconfdir=/etc/squid' '--disable-silent-rules' '--libdir=${prefix}/lib/x86_64-linux-gnu' '--disable-dependency-tracking' 'BUILDCC=gcc' 'BUILDCCFLAGS=-g -O2' 'PROTECTOR=strong' '-fstack-clash-protection -Wformat'
```

Si no está instalado:

sudo apt update

sudo apt install squid -y

```
~/Doc/Ejercicios_seguridad_informatica_2025 main > sudo apt install squid
Installing:
  squid

Installing dependencies:
  libcap3  squid-common  squid-langpack

Suggested packages:
  resolvconf
```

♦ 2. Iniciar y habilitar el servicio

```
sudo systemctl start squid
```

```
sudo systemctl enable squid
```

```
sudo systemctl status squid
```

Debe quedar en estado **active (running)**.

```
~/Documents/box > sudo systemctl start squid

~/Documents/box > sudo systemctl enable squid
Synchronizing state of squid.service with SysV service script with /usr/lib/systemd/systemd-sysv-install enable squid
Executing: /usr/lib/systemd/systemd-sysv-install enable squid
Created symlink '/etc/systemd/system/multi-user.target.wants/squid.service' → '/usr/lib/systemd/system/squid.service'.

~/Documents/box > sudo systemctl status squid
● squid.service - Squid Web Proxy Server
   Loaded: loaded (/usr/lib/systemd/system/squid.service; enabled; preset: disabled)
   Active: active (running) since Wed 2025-10-01 12:16:00 CEST; 19s ago
 Invocation: 0752ee56ed9746268e64e25718fe704c
    Docs: man:squid(8)
  Main PID: 5669 (squid)
    Tasks: 4 (limit: 6870)
  Memory: 17.8M (peak: 18.3M)
     CPU: 110ms
   CGroup: /system.slice/squid.service
           └─5669 /usr/sbin/squid --foreground -sYC
             └─5674 "(squid-1)" --kid squid-1 --foreground -sYC
               └─5675 "(logfile-daemon)" /var/log/squid/access.log
                 └─5676 "(pinger)"
```

♦ 3. Configuración básica del proxy

El archivo principal es:

Sudo nano /etc/squid/squid.conf

En este fichero puedes ajustar:

- Puerto de escucha (por defecto 3128):

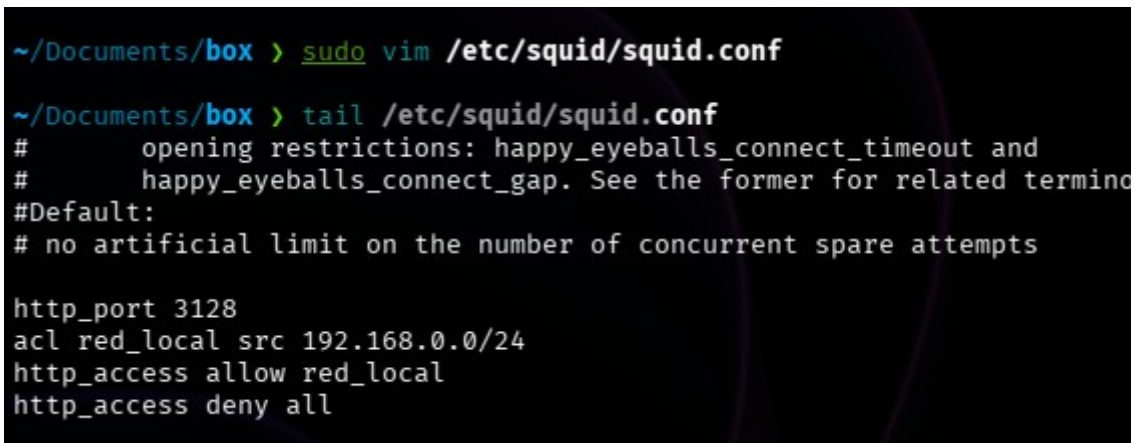
http_port 3128

- Permitir acceso desde tu red local (ejemplo 192.168.56.0/24 en VirtualBox):

acl red_local src 192.168.56.0/24

http_access allow red_local

http_access deny all



```
~/Documents/box > sudo vim /etc/squid/squid.conf
~/Documents/box > tail /etc/squid/squid.conf
#      opening restrictions: happy_eyeballs_connect_timeout and
#      happy_eyeballs_connect_gap. See the former for related termino
#Default:
# no artificial limit on the number of concurrent spare attempts

http_port 3128
acl red_local src 192.168.0.0/24
http_access allow red_local
http_access deny all
```

- (Opcional) Definir cache/logs:

Ya vienen preconfigurados en /var/spool/squid y /var/log/squid/.

Después de cambios:

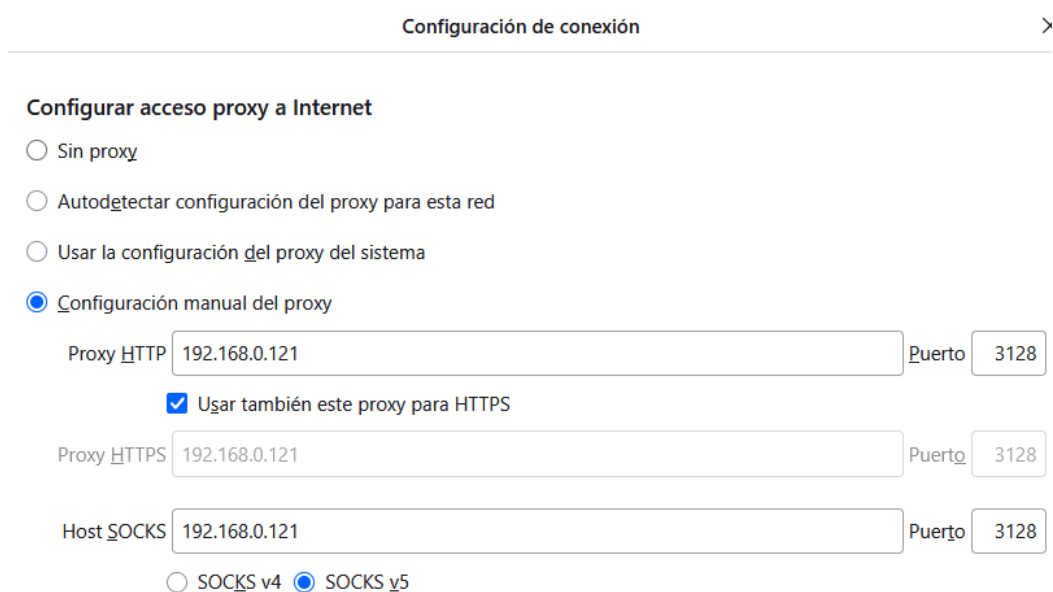
sudo systemctl restart squid

♦ 4. Configurar el cliente (para “usar” el proxy)

Ahora, cualquier cliente (otro Linux, Windows, navegador, etc.) debe apuntar a **la IP de tu máquina virtual + puerto 3128**.

Ejemplos:

- En navegador (Firefox/Chrome):
 - Configuración → Proxy manual →
 - HTTP Proxy: 192.168.56.101 (IP de la VM Kali)
 - Puerto: 3128
 - Usar este proxy para todo protocolo.



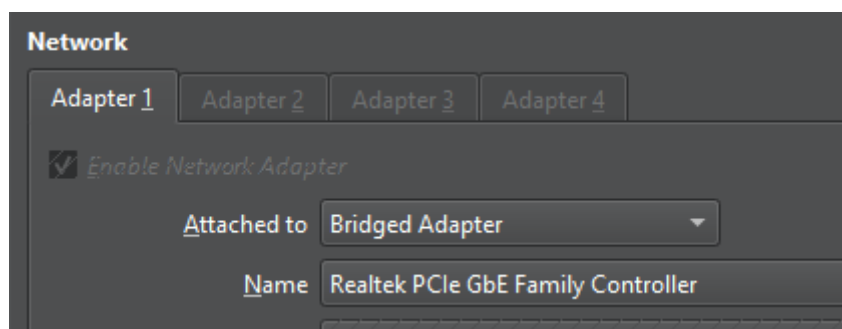
- En Linux (temporal):

export http_proxy="http://192.168.56.101:3128"

export https_proxy="http://192.168.56.101:3128"

- En Windows (red → configuración de proxy manual):
 - **Servidor proxy: 192.168.56.101:3128.**

(Asegúrate de que la red de tu VM está en modo **Bridged** o **Host-only** para que el cliente pueda verla).



♦ 5. Ver logs de uso

Cada vez que un cliente use el proxy, quedará registrado:

`tail -f /var/log/squid/access.log`

```
~/Documents/box > sudo tail -f /var/log/squid/access.log
sudo tail -f /var/log/squid/cache.log
1759314590.852    0 192.168.0.65 TCP_DENIED/403 3905 CONNECT www.google.com:443 - HIER_NONE/- text/html
1759314591.061    0 192.168.0.65 TCP_DENIED/403 3905 CONNECT www.google.com:443 - HIER_NONE/- text/html
1759314591.278    0 192.168.0.65 TCP_DENIED/403 3905 CONNECT www.google.com:443 - HIER_NONE/- text/html
1759314661.940    0 127.0.0.1 NONE_NONE/000 0 - error:transaction-end-before-headers - HIER_NONE/- -
1759314661.940    0 127.0.0.1 NONE_NONE/000 0 - error:transaction-end-before-headers - HIER_NONE/- -
1759314697.424   20 192.168.0.65 TCP_DENIED/403 3908 CONNECT ads.mozilla.org:443 - HIER_NONE/- text/html
1759314713.202 170882 127.0.0.1 TCP_TUNNEL/200 7399 CONNECT contile.services.mozilla.com:443 - HIER_DIRECT/34.36.137.203 -
1759314713.203 170883 127.0.0.1 TCP_TUNNEL/200 2348 CONNECT spocs.getpocket.com:443 - HIER_DIRECT/34.36.137.203 -
1759314763.682    0 127.0.0.1 NONE_NONE/000 0 - error:transaction-end-before-headers - HIER_NONE/- -
1759314763.682    0 127.0.0.1 NONE_NONE/000 0 - error:transaction-end-before-headers - HIER_NONE/- -
1759314798.129   20 192.168.0.65 TCP_DENIED/403 3905 CONNECT www.google.com:443 - HIER_NONE/- text/html
1759314810.557    0 192.168.0.65 TCP_DENIED/403 3905 CONNECT www.google.com:443 - HIER_NONE/- text/html
```

♦ 6. Probar funcionamiento

En el cliente, abre un navegador con proxy activado y entra en una web.

Si funciona:

- La página cargará **a través del proxy Squid**.
- En los logs de Kali (/var/log/squid/access.log) verás la petición registrada.



```
~/Documents/box > sudo tail -f /var/log/squid/access.log
1759316349.523    0 192.168.0.65 TCP_DENIED/403 3905 CONNECT www.google.com:443 - HIER_NONE/- text/html
1759316349.686    0 192.168.0.65 TCP_DENIED/403 3905 CONNECT www.google.com:443 - HIER_NONE/- text/html
1759316349.804    0 192.168.0.65 TCP_DENIED/403 3905 CONNECT www.google.com:443 - HIER_NONE/- text/html
1759316350.372   20 192.168.0.65 TCP_DENIED/403 3902 CONNECT www.google.es:443 - HIER_NONE/- text/html
1759316409.603    0 192.168.0.65 NONE_NONE/000 0 - error:transaction-end-before-headers - HIER_NONE/- -
1759316409.603    0 192.168.0.65 NONE_NONE/000 0 - error:transaction-end-before-headers - HIER_NONE/- -
1759316460.355    0 127.0.0.1 NONE_NONE/400 3737 - / - HIER_NONE/- text/html
1759316460.448    0 127.0.0.1 TCP_HIT/200 13022 GET http://kali:3128/squid-internal-static/icons/SN.png - HIER_NON
E/- image/png
1759316460.470    0 127.0.0.1 NONE_NONE/400 3759 - /favicon.ico - HIER_NONE/- text/html
1759316490.575  109 127.0.0.1 TCP_MISS/200 1190 POST http://o.pki.goog/wr2 - HIER_DIRECT/142.250.200.131 applicati
on/ocsp-response
1759316506.451   21 192.168.0.65 TCP_DENIED/403 3944 CONNECT merino.services.mozilla.com:443 - HIER_NONE/- text/ht
ml
1759316506.451   20 192.168.0.65 TCP_DENIED/403 3908 CONNECT ads.mozilla.org:443 - HIER_NONE/- text/html
1759316506.451   21 192.168.0.65 TCP_DENIED/403 3908 CONNECT ads.mozilla.org:443 - HIER_NONE/- text/html
1759316527.233 170286 127.0.0.1 TCP_TUNNEL/200 7394 CONNECT contile.services.mozilla.com:443 - HIER_DIRECT/34.36.137
.203 -
1759316527.235 170288 127.0.0.1 TCP_TUNNEL/200 2348 CONNECT spocs.getpocket.com:443 - HIER_DIRECT/34.36.137.203 -
1759316530.034   193 127.0.0.1 TCP_TUNNEL/200 1477 CONNECT safebrowsing.googleapis.com:443 - HIER_DIRECT/172.217.17
1.202 -
1759316553.597  62943 127.0.0.1 TCP_TUNNEL/200 1035732 CONNECT www.google.com:443 - HIER_DIRECT/142.250.184.4 -
1759316570.199    0 192.168.0.65 TCP_DENIED/403 3905 CONNECT www.google.com:443 - HIER_NONE/- text/html
1759316573.818    0 192.168.0.65 TCP_DENIED/403 3902 CONNECT www.google.es:443 - HIER_NONE/- text/html
```

Nota

Podemos probar con

curl -x http://192.168.10.109:3128 <http://example.com>

El cliente hay que configurarlo en Windows,

```
~/Documents/box > curl -x http://localhost:3128 http://www.google.com -I 16s
HTTP/1.1 200 OK
Content-Type: text/html; charset=ISO-8859-1
Content-Security-Policy-Report-Only: object-src 'none';base-uri 'self';script-src 'nonce-dtugibPG3iYIdBzU3f2lrw' 'st
rict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/g
ws/other-hp
Date: Wed, 01 Oct 2025 10:58:32 GMT
Server: gws
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN
Expires: Wed, 01 Oct 2025 10:58:32 GMT
Cache-Control: private
Set-Cookie: AEC=AaJma5vmMV049gDTMybRLs9FcgvqlgBC6NfnjkaNzOxhvzq6qlMYcwsMA84; expires=Mon, 30-Mar-2026 10:58:32 GMT;
path=/; domain=.google.com; Secure; HttpOnly; SameSite=lax
Cache-Status: kali;detail=mismatch
Via: 1.1 kali (squid/7.1)
Connection: keep-alive
```



```

~/Documents/box > sudo tail -f /var/log/squid/access.log
1759317133.349 20 192.168.0.65 TCP_DENIED/403 3896 CONNECT youtube.com:443 - HIER_NONE/- text/html
1759317134.032 0 192.168.0.65 TCP_DENIED/403 3896 CONNECT youtube.com:443 - HIER_NONE/- text/html
1759317134.272 0 192.168.0.65 TCP_DENIED/403 3896 CONNECT youtube.com:443 - HIER_NONE/- text/html
1759317134.456 0 192.168.0.65 TCP_DENIED/403 3896 CONNECT youtube.com:443 - HIER_NONE/- text/html
1759317171.583 108 ::1 TCP_MISS/200 736 HEAD http://www.google.com/ - HIER_DIRECT/216.58.209.68 text/html
1759317221.337 20 192.168.0.65 TCP_DENIED/403 314 HEAD http://www.google.com/ - HIER_NONE/- text/html
1759317253.081 0 127.0.0.1 NONE_NONE/000 0 - error:transaction-end-before-headers - HIER_NONE/- -
1759317253.081 0 127.0.0.1 NONE_NONE/000 0 - error:transaction-end-before-headers - HIER_NONE/- -
1759317398.341 270992 127.0.0.1 TCP_TUNNEL/200 22073 CONNECT widget-mediator.zopim.com:443 - HIER_DIRECT/52.30.
9 -
1759317398.341 139689 127.0.0.1 TCP_TUNNEL/200 7387 CONNECT contile.services.mozilla.com:443 - HIER_DIRECT/34.3
.203 -
1759317779.704 108 192.168.0.65 TCP_TUNNEL/200 11392 CONNECT encrypted-tbn0.gstatic.com:443 - HIER_DIRECT/14
.184.14 -
1759317788.966 0 192.168.0.121 NONE_NONE/400 3741 - / - HIER_NONE/- text/html
1759317788.967 0 192.168.0.65 TCP_MISS/400 3804 GET http://192.168.0.121:3128/ - HIER_DIRECT/192.168.0.121
/html
1759317788.989 0 192.168.0.65 TCP_HIT/200 13022 GET http://kali:3128/squid-internal-static/icons/SN.png -
NONE/- image/png
1759317789.031 0 192.168.0.65 TCP_MISS_ABORTED/000 0 GET http://192.168.0.121:3128/favicon.ico - HIER_DIRE
2.168.0.121 -
1759317789.031 0 192.168.0.121 NONE_NONE_ABORTED/400 309 - /favicon.ico - HIER_NONE/- text/html
1759317833.102 380 192.168.0.65 TCP_MISS/200 1042 GET http://example.com/ - HIER_DIRECT/23.220.75.232 text/h
1759317833.317 189 192.168.0.65 TCP_MISS/404 1711 GET http://example.com/favicon.ico - HIER_DIRECT/23.220.75
text/html

```

DENEGAR ACCESO A WEBS

```

~/Doc/Ejercicios_seguridad_informatica_2025/p/squid main ↵3 > cat reglas.conf | grep -v "#"
acl bloqueadas dstdomain "/etc/squid/bloqueadas.txt"
http_access deny bloqueadas

acl red_local src 192.168.0.0/23
http_access allow red_local

http_access deny all

```

```

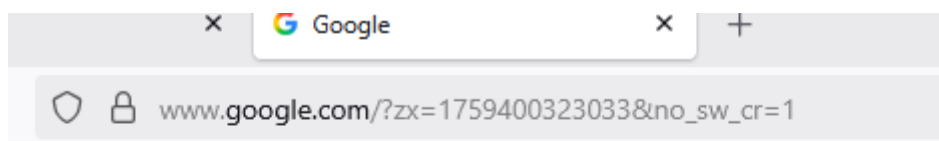
~/Doc/Ejercicios_seguridad_informatica_2025/p/squid main ↵3 > cat bloqueadas.txt | grep -v "#"
.facebook.com
.youtube.com
.tiktok.com

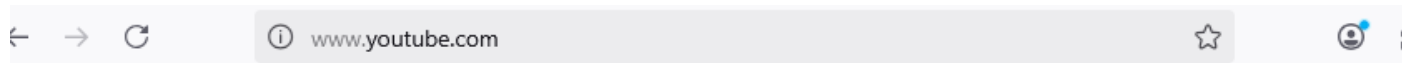
```

```

local
~/Doc/Ejercicios_seguridad_informatica_2025/p/squid main f3 > grep -v "^#" /etc/squid/squid.conf | grep -v "^$"
include /etc/squid/reglas.conf
acl localnet src 0.0.0.1-0.255.255.255 # RFC 1122 "this" network (LAN)
acl localnet src 10.0.0.0/8 # RFC 1918 local private network (LAN)
acl localnet src 100.64.0.0/10 # RFC 6598 shared address space (CGN)
acl localnet src 169.254.0.0/16 # RFC 3927 link-local (directly plugged) machines
acl localnet src 172.16.0.0/12 # RFC 1918 local private network (LAN)
acl localnet src 192.168.0.0/16 # RFC 1918 local private network (LAN)
acl localnet src fc00::/7 # RFC 4193 local private network range
acl localnet src fe80::/10 # RFC 4291 link-local (directly plugged) machines
acl SSL_ports port 443
acl Safe_ports port 80 # http
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
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost manager
http_access allow localhost
http_access allow to_localhost
http_access allow to_linklocal
include /etc/squid/conf.d/*.conf
http_access allow all
http_port 3128
coredump_dir /var/spool/squid
refresh_pattern ^ftp: 1440 20% 10080
refresh_pattern -i (/cgi-bin/|\?) 0 0% 0
refresh_pattern . 0 20% 4320
acl sitios_bloqueados dstdomain "/etc/squid/bloqueados.txt"
http_access deny sitios_bloqueados

```





El servidor proxy está rechazando las conexiones

Firefox está configurado para usar un servidor proxy que está rechazando las conexiones.

Código de error: 403 Forbidden