

# Configuración de Squid como Proxy Transparente en Entorno Linux

---

Informe técnico

Configuración de Squid como proxy transparente en entorno Linux

Autor: Anónimo

## Índice

1. Introducción
2. Pasos realizados
3. Problemas encontrados y soluciones aplicadas
4. Verificación final del funcionamiento
5. Conclusión
6. Fuentes

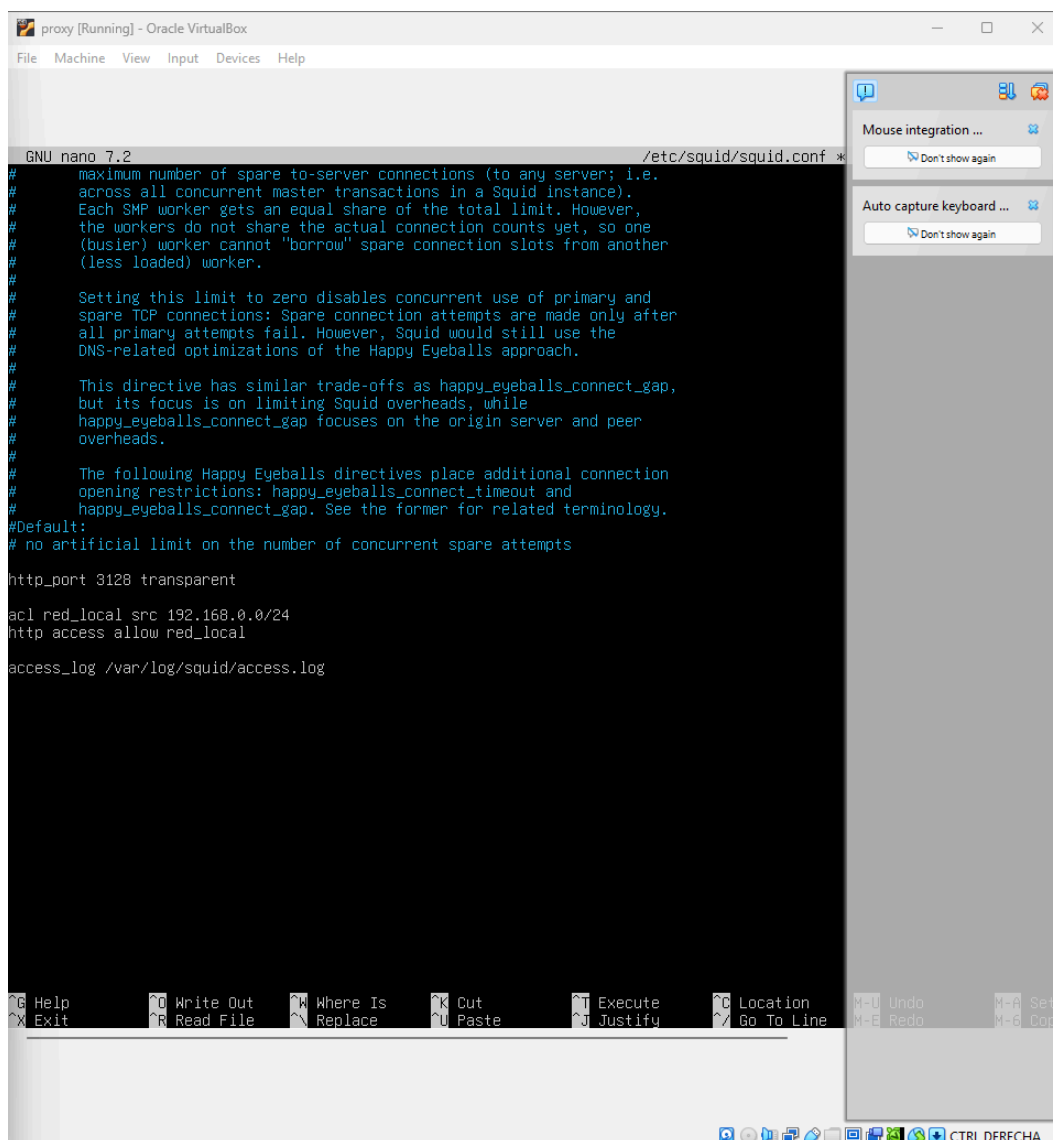
## 1. Introducción

En el presente informe se documenta el proceso de instalación, configuración y validación de un servidor proxy transparente utilizando Squid en un entorno basado en Ubuntu Server. Squid actúa como intermediario entre los clientes de la red local y los servidores web externos, registrando y filtrando el tráfico HTTP y HTTPS.

## 2. Pasos realizados

A continuación se describen los pasos realizados durante el proceso, acompañados de capturas de pantalla que ilustran cada etapa.

### 2.1 Instalación y actualización del sistema



The screenshot shows a terminal window titled 'proxy [Running] - Oracle VM VirtualBox'. The terminal is running the GNU nano 7.2 editor, editing the file /etc/squid/squid.conf. The configuration file content is as follows:

```
GNU nano 7.2 /etc/squid/squid.conf
# maximum number of spare to-server connections (to any server; i.e.
# across all concurrent master transactions in a Squid instance).
# Each SMP worker gets an equal share of the total limit. However,
# the workers do not share the actual connection counts yet, so one
# (busier) worker cannot "borrow" spare connection slots from another
# (less loaded) worker.
#
# Setting this limit to zero disables concurrent use of primary and
# spare TCP connections: Spare connection attempts are made only after
# all primary attempts fail. However, Squid would still use the
# DNS-related optimizations of the Happy Eyeballs approach.
#
# This directive has similar trade-offs as happy_eyeballs_connect_gap,
# but its focus is on limiting Squid overheads, while
# happy_eyeballs_connect_gap focuses on the origin server and peer
# overheads.
#
# The following Happy Eyeballs directives place additional connection
# opening restrictions: happy_eyeballs_connect_timeout and
# happy_eyeballs_connect_gap. See the former for related terminology.
#Default:
# no artificial limit on the number of concurrent spare attempts

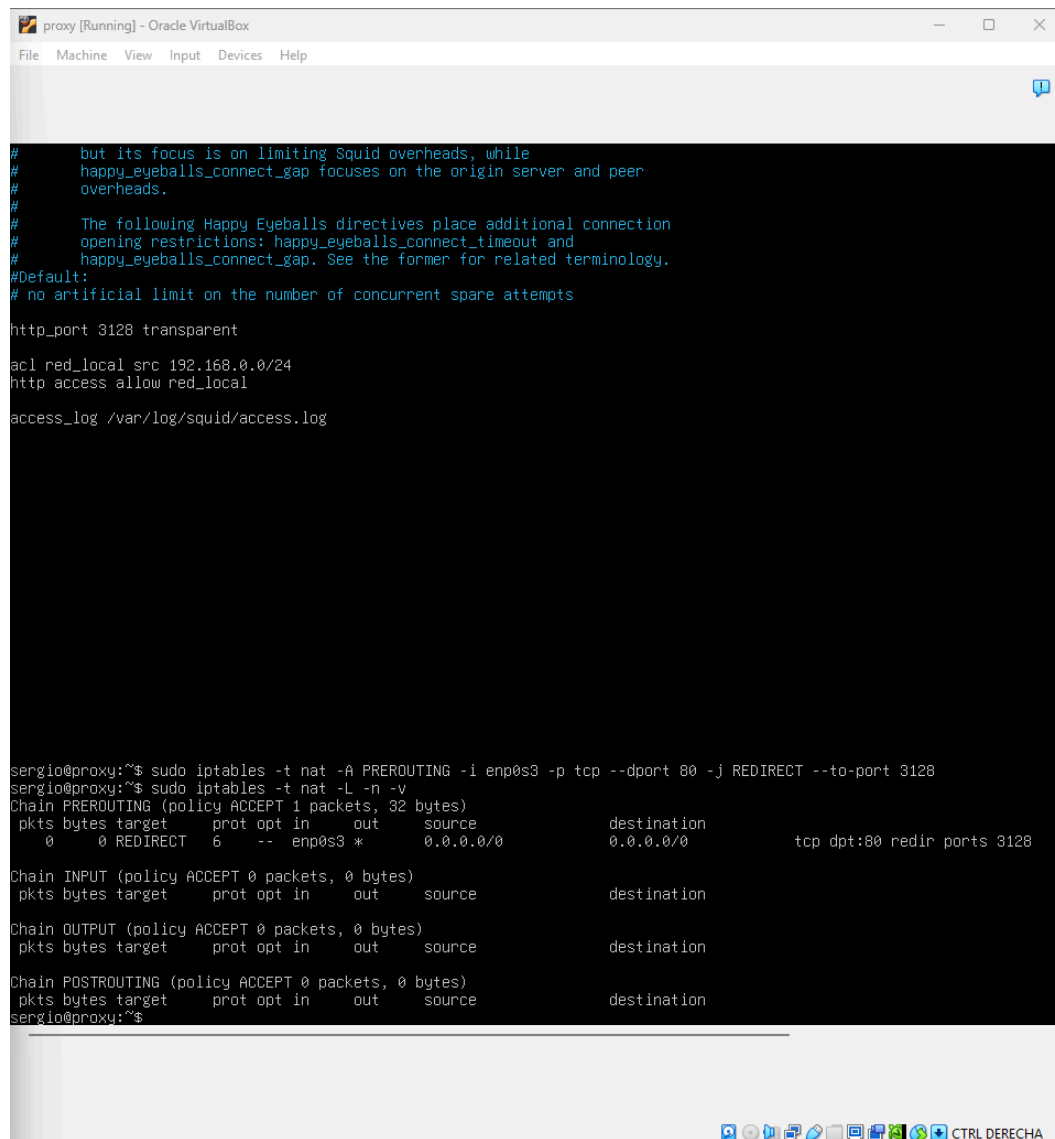
http_port 3128 transparent

acl red_local src 192.168.0.0/24
http access allow red_local

access_log /var/log/squid/access.log
```

The terminal window also displays a menu bar with various options: Help, Exit, Write Out, Read File, Where Is, Replace, Cut, Paste, Execute, Justify, Location, Go To Line, Undo, Redo, Set, Copy. The bottom of the window shows a taskbar with icons for the terminal, file manager, and other applications, along with the text 'CTRL DERECHA'.

## 2.2 Instalación de Squid



```
proxy [Running] - Oracle VirtualBox
File Machine View Input Devices Help

# but its focus is on limiting Squid overheads, while
# happy_eyeballs_connect_gap focuses on the origin server and peer
# overheads.
#
# The following Happy Eyeballs directives place additional connection
# opening restrictions: happy_eyeballs_connect_timeout and
# happy_eyeballs_connect_gap. See the former for related terminology.
#Default:
# no artificial limit on the number of concurrent spare attempts

http_port 3128 transparent

acl red_local src 192.168.0.0/24
http access allow red_local

access_log /var/log/squid/access.log

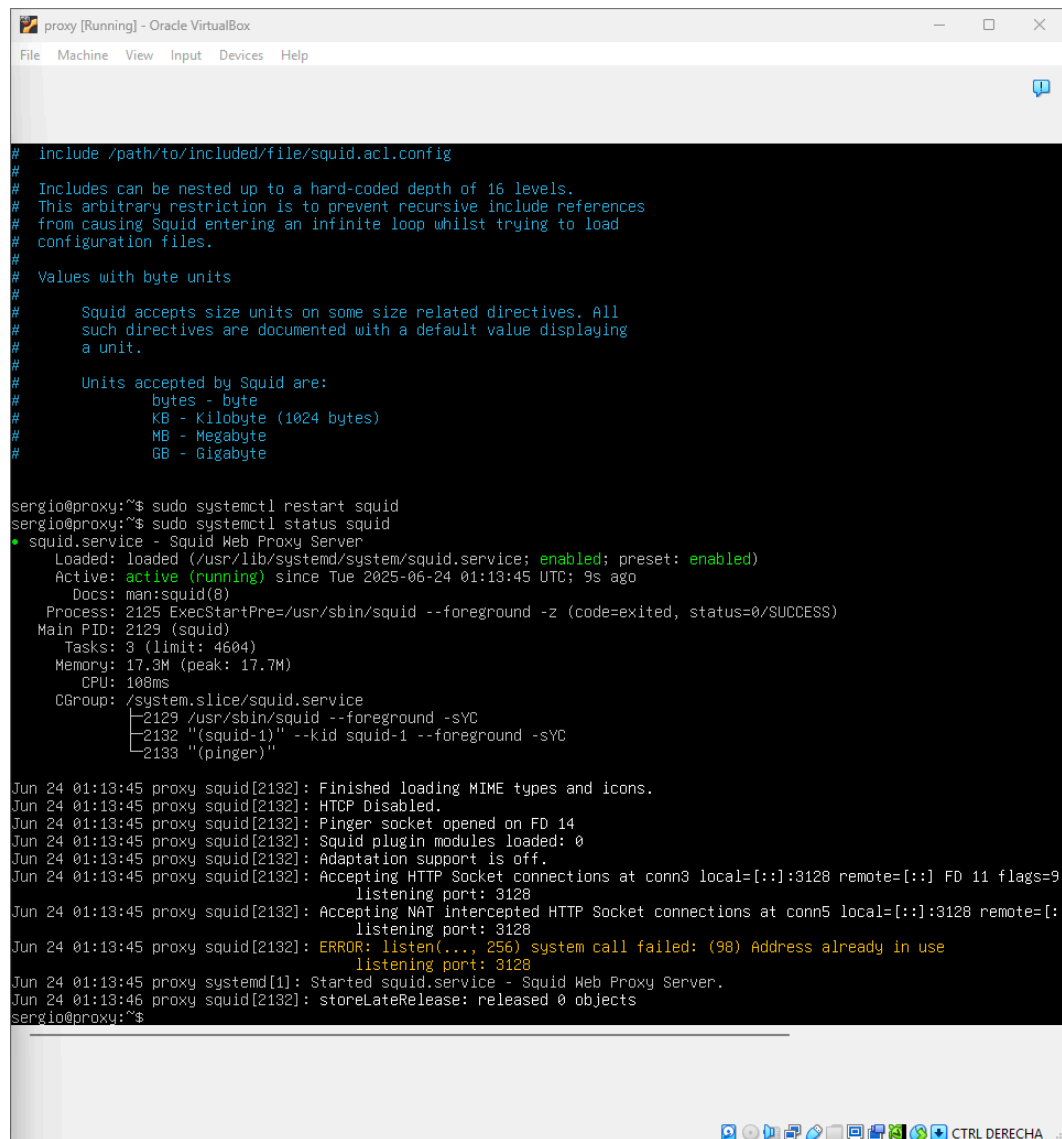
sergio@proxy:~$ sudo iptables -t nat -A PREROUTING -i enp0s3 -p tcp --dport 80 -j REDIRECT --to-port 3128
sergio@proxy:~$ sudo iptables -t nat -L -n -v
Chain PREROUTING (policy ACCEPT 1 packets, 32 bytes)
 pkts bytes target     prot opt in     out     source            destination
    0      0 REDIRECT    6     --  enp0s3 *          0.0.0.0/0         tcp dpt:80 redir ports 3128

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source            destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source            destination

Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source            destination
sergio@proxy:~$
```

## 2.3 Configuración del archivo squid.conf

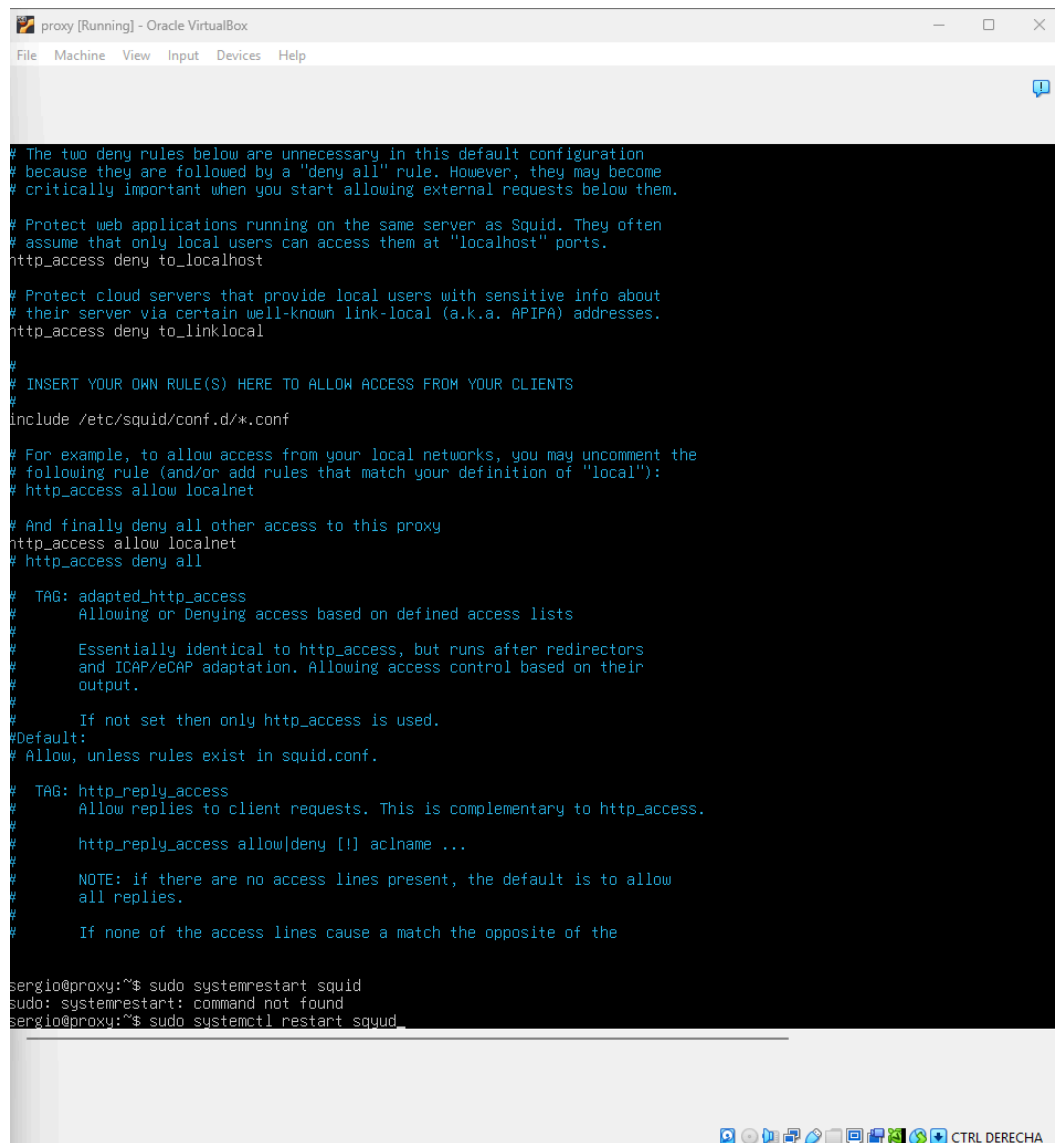


```
# include /path/to/included/file/squid.acl.config
#
# Includes can be nested up to a hard-coded depth of 16 levels.
# This arbitrary restriction is to prevent recursive include references
# from causing Squid entering an infinite loop whilst trying to load
# configuration files.
#
# Values with byte units
#
#     Squid accepts size units on some size related directives. All
#     such directives are documented with a default value displaying
#     a unit.
#
#     Units accepted by Squid are:
#         bytes - byte
#         KB - Kilobyte (1024 bytes)
#         MB - Megabyte
#         GB - Gigabyte

sergio@proxy:~$ sudo systemctl restart squid
sergio@proxy:~$ sudo systemctl status squid
• squid.service - Squid Web Proxy Server
   Loaded: loaded (/usr/lib/systemd/system/squid.service; enabled; preset: enabled)
   Active: active (running) since Tue 2025-06-24 01:13:45 UTC; 9s ago
     Docs: man:squid(8)
   Process: 2125 ExecStartPre=/usr/sbin/squid --foreground -z (code=exited, status=0/SUCCESS)
   Main PID: 2129 (squid)
      Tasks: 3 (limit: 4604)
     Memory: 17.3M (peak: 17.7M)
        CPU: 106ms
    CGroup: /system.slice/squid.service
            └─2129 /usr/sbin/squid --foreground -sYC
              └─2132 "(squid-1)" --kid squid-1 --foreground -sYC
                └─2133 "(pinger)"

Jun 24 01:13:45 proxy squid[2132]: Finished loading MIME types and icons.
Jun 24 01:13:45 proxy squid[2132]: HTTP Disabled.
Jun 24 01:13:45 proxy squid[2132]: Pinger socket opened on FD 14
Jun 24 01:13:45 proxy squid[2132]: Squid plugin modules loaded: 0
Jun 24 01:13:45 proxy squid[2132]: Adaptation support is off.
Jun 24 01:13:45 proxy squid[2132]: Accepting HTTP Socket connections at conn3 local=[::]:3128 remote=[::] FD 11 flags=9
                                listening port: 3128
Jun 24 01:13:45 proxy squid[2132]: Accepting NAT intercepted HTTP Socket connections at conn5 local=[::]:3128 remote=[::]
                                listening port: 3128
Jun 24 01:13:45 proxy squid[2132]: ERROR: listen(.... 256) system call failed: (98) Address already in use
                                listening port: 3128
Jun 24 01:13:45 proxy systemd[1]: Started squid.service - Squid Web Proxy Server.
Jun 24 01:13:46 proxy squid[2132]: storeLateRelease: released 0 objects
sergio@proxy:~$
```

## 2.4 Aplicación de reglas iptables para redirección del tráfico HTTP/HTTPS



```
proxy [Running] - Oracle VirtualBox
File Machine View Input Devices Help

# The two deny rules below are unnecessary in this default configuration
# because they are followed by a "deny all" rule. However, they may become
# critically important when you start allowing external requests below them.

# Protect web applications running on the same server as Squid. They often
# assume that only local users can access them at "localhost" ports.
http_access deny to_localhost

# Protect cloud servers that provide local users with sensitive info about
# their server via certain well-known link-local (a.k.a. APIPA) addresses.
http_access deny to_linklocal

#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
include /etc/squid/conf.d/*.conf

# For example, to allow access from your local networks, you may uncomment the
# following rule (and/or add rules that match your definition of "local"):
# http_access allow localnet

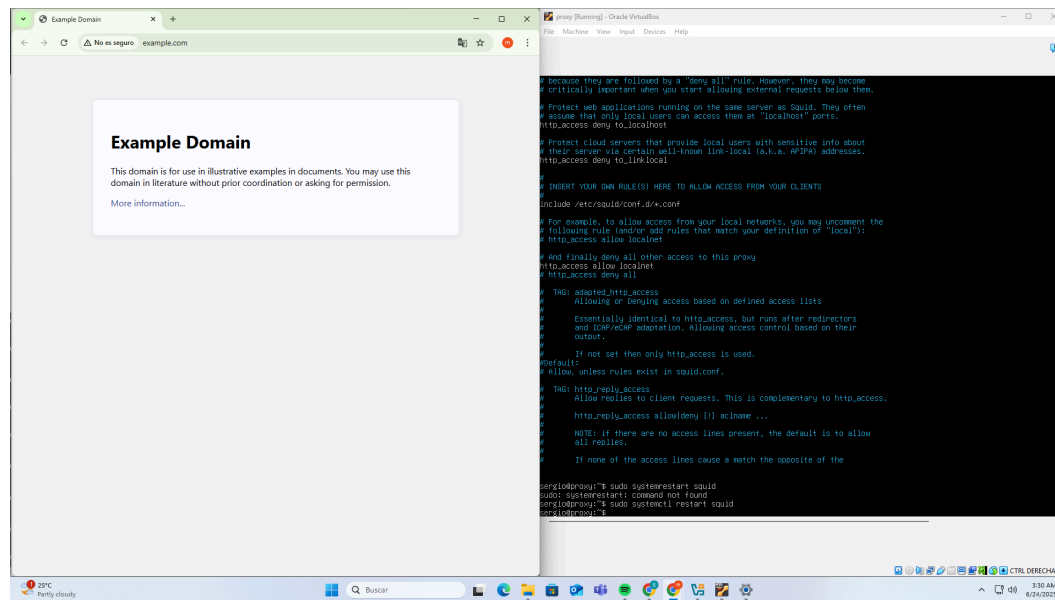
# And finally deny all other access to this proxy
http_access allow localnet
# http_access deny all

# TAG: adapted_http_access
#   Allowing or Denying access based on defined access lists
#
#   Essentially identical to http_access, but runs after redirectors
#   and ICAP/eCAP adaptation. Allowing access control based on their
#   output.
#
#   If not set then only http_access is used.
#Default:
# Allow, unless rules exist in squid.conf.

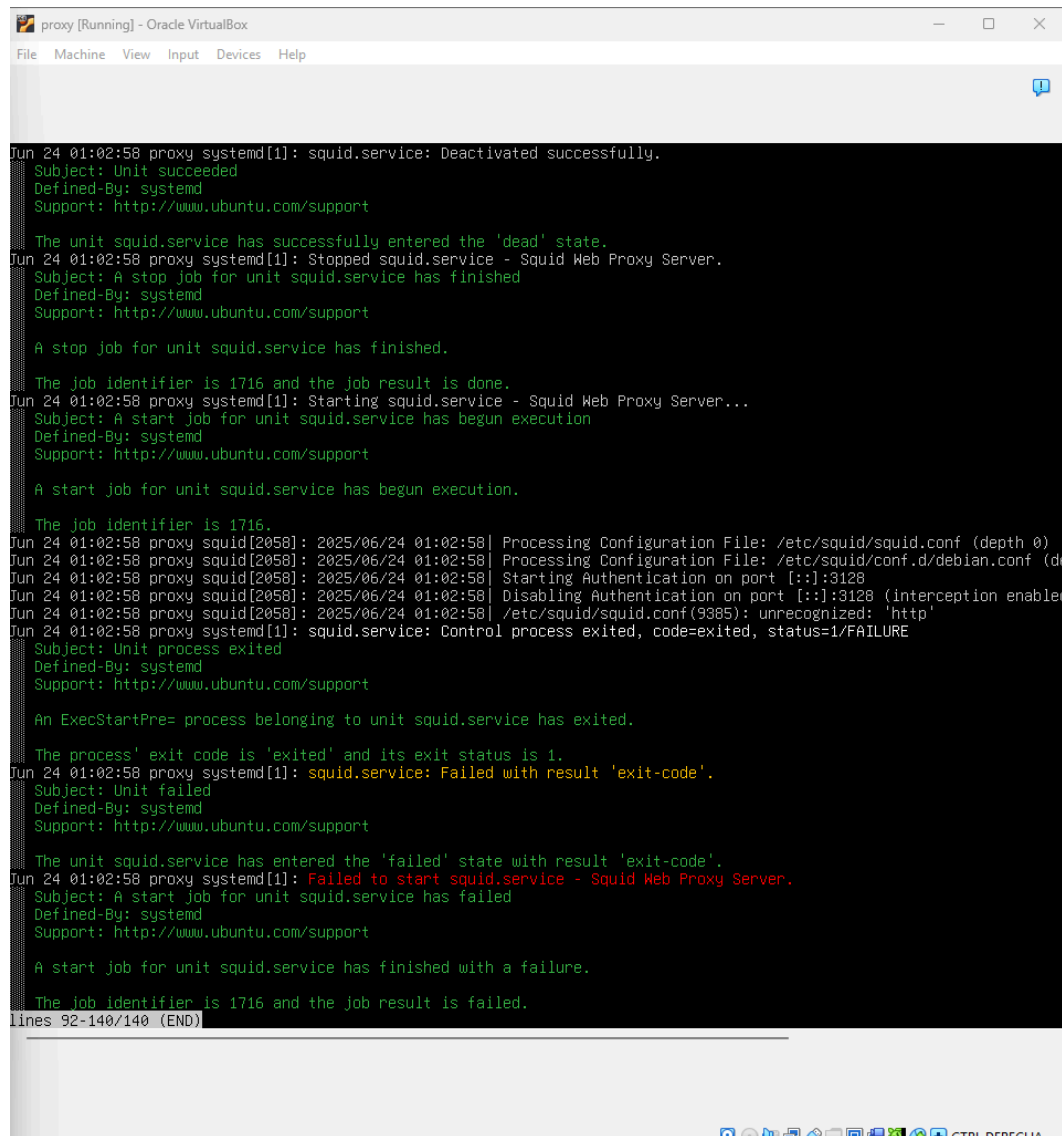
# TAG: http_reply_access
#   Allow replies to client requests. This is complementary to http_access.
#
#   http_reply_access allow|deny [!] aclname ...
#
#   NOTE: if there are no access lines present, the default is to allow
#   all replies.
#
#   If none of the access lines cause a match the opposite of the

sergio@proxy:~$ sudo systemctl restart squid
sudo: systemctl: command not found
sergio@proxy:~$ sudo systemctl restart squid
```

## 2.5 Verificación del estado del servicio Squid



## 2.6 Revisión del funcionamiento del proxy mediante acceso web y registro en logs



```
Jun 24 01:02:58 proxy systemd[1]: squid.service: Deactivated successfully.
Subject: Unit succeeded
Defined-By: systemd
Support: http://www.ubuntu.com/support

The unit squid.service has successfully entered the 'dead' state.
Jun 24 01:02:58 proxy systemd[1]: Stopped squid.service - Squid Web Proxy Server.
Subject: A stop job for unit squid.service has finished
Defined-By: systemd
Support: http://www.ubuntu.com/support

A stop job for unit squid.service has finished.

The job identifier is 1716 and the job result is done.
Jun 24 01:02:58 proxy systemd[1]: Starting squid.service - Squid Web Proxy Server...
Subject: A start job for unit squid.service has begun execution
Defined-By: systemd
Support: http://www.ubuntu.com/support

A start job for unit squid.service has begun execution.

The job identifier is 1716.
Jun 24 01:02:58 proxy squid[2058]: 2025/06/24 01:02:58| Processing Configuration File: /etc/squid/squid.conf (depth 0)
Jun 24 01:02:58 proxy squid[2058]: 2025/06/24 01:02:58| Processing Configuration File: /etc/squid/conf.d/debian.conf (depth 1)
Jun 24 01:02:58 proxy squid[2058]: 2025/06/24 01:02:58| Starting Authentication on port [::]:3128
Jun 24 01:02:58 proxy squid[2058]: 2025/06/24 01:02:58| Disabling Authentication on port [::]:3128 (interception enabled)
Jun 24 01:02:58 proxy squid[2058]: 2025/06/24 01:02:58| /etc/squid/squid.conf(9385): unrecognized: 'http'
Jun 24 01:02:58 proxy systemd[1]: squid.service: Control process exited, code=exited, status=1/FAILURE
Subject: Unit process exited
Defined-By: systemd
Support: http://www.ubuntu.com/support

An ExecStartPre= process belonging to unit squid.service has exited.

The process' exit code is 'exited' and its exit status is 1.
Jun 24 01:02:58 proxy systemd[1]: squid.service: Failed with result 'exit-code'.
Subject: Unit failed
Defined-By: systemd
Support: http://www.ubuntu.com/support

The unit squid.service has entered the 'failed' state with result 'exit-code'.
Jun 24 01:02:58 proxy systemd[1]: Failed to start squid.service - Squid Web Proxy Server.
Subject: A start job for unit squid.service has failed
Defined-By: systemd
Support: http://www.ubuntu.com/support

A start job for unit squid.service has finished with a failure.

The job identifier is 1716 and the job result is failed.
lines 92-140/140 (END)
```

## 3. Problemas encontrados y soluciones aplicadas

Durante la configuración se identificaron diversos errores relacionados con la resolución de nombres, conectividad y carga del archivo de configuración. Todos fueron solucionados revisando la red, corrigiendo el hostname y aplicando correctamente los comandos iptables. Se adjuntan a continuación capturas de los errores y su resolución.



```
proxy [Running] - Oracle VirtualBox
File Machine View Input Devices Help

#
# The following Happy Eyeballs directives place additional connection
# opening restrictions: happy_eyeballs_connect_timeout and
# happy_eyeballs_connect_gap. See the former for related terminology.
#Default:
# no artificial limit on the number of concurrent spare attempts

http_port 3128 transparent

acl red_local src 192.168.0.0/24
http access allow red_local

access_log /var/log/squid/access.log

sergio@proxy:~$ sudo iptables -t nat -A PREROUTING -i enp0s3 -p tcp --dport 80 -j REDIRECT --to-port 3128
sergio@proxy:~$ sudo iptables -t nat -L -n -v
Chain PREROUTING (policy ACCEPT 1 packets, 32 bytes)
 pkts bytes target    prot opt in     out     source            destination
    0      0 REDIRECT    6  --  enp0s3 *      0.0.0.0/0         0.0.0.0/0         tcp dpt:80 redir ports 3128

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source            destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source            destination

Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source            destination
sergio@proxy:~$ sudo systemctl restart squid
Job for squid.service failed because the control process exited with error code.
See "systemctl status squid.service" and "journalctl -xeu squid.service" for details.
sergio@proxy:~$
```

```
proxy [Running] - Oracle VirtualBox
File Machine View Input Devices Help

Jun 24 01:09:19 proxy systemd[1]: squid.service: Failed with result 'exit-code'.
Subject: Unit failed
Defined-By: systemd
Support: http://www.ubuntu.com/support

The unit squid.service has entered the 'failed' state with result 'exit-code'.
Jun 24 01:09:19 proxy systemd[1]: Failed to start squid.service - Squid Web Proxy Server.
Subject: A start job for unit squid.service has failed
Defined-By: systemd
Support: http://www.ubuntu.com/support

A start job for unit squid.service has finished with a failure.

The job identifier is 1824 and the job result is failed.
Jun 24 01:10:35 proxy systemd[1]: Starting squid.service - Squid Web Proxy Server...
Subject: A start job for unit squid.service has begun execution
Defined-By: systemd
Support: http://www.ubuntu.com/support

A start job for unit squid.service has begun execution.

The job identifier is 2041.
Jun 24 01:10:35 proxy squid[2108]: 2025/06/24 01:10:35| Processing Configuration File: /etc/squid/squid.conf (depth 0)
Jun 24 01:10:35 proxy squid[2108]: 2025/06/24 01:10:35| /etc/squid/squid.conf(1): unrecognized: 'WELCOME'
Jun 24 01:10:35 proxy squid[2108]: 2025/06/24 01:10:35| Processing Configuration File: /etc/squid/conf.d/debian.conf (depth 0)
Jun 24 01:10:35 proxy squid[2108]: 2025/06/24 01:10:35| Starting Authentication on port [::]:3128
Jun 24 01:10:35 proxy squid[2108]: 2025/06/24 01:10:35| Disabling Authentication on port [::]:3128 (interception enabled)
Jun 24 01:10:35 proxy systemd[1]: squid.service: Control process exited, code=exited, status=1/FAILURE
Subject: Unit process exited
Defined-By: systemd
Support: http://www.ubuntu.com/support

An ExecStartPre= process belonging to unit squid.service has exited.

The process' exit code is 'exited' and its exit status is 1.
Jun 24 01:10:35 proxy systemd[1]: squid.service: Failed with result 'exit-code'.
Subject: Unit failed
Defined-By: systemd
Support: http://www.ubuntu.com/support

The unit squid.service has entered the 'failed' state with result 'exit-code'.
Jun 24 01:10:35 proxy systemd[1]: Failed to start squid.service - Squid Web Proxy Server.
Subject: A start job for unit squid.service has failed
Defined-By: systemd
Support: http://www.ubuntu.com/support

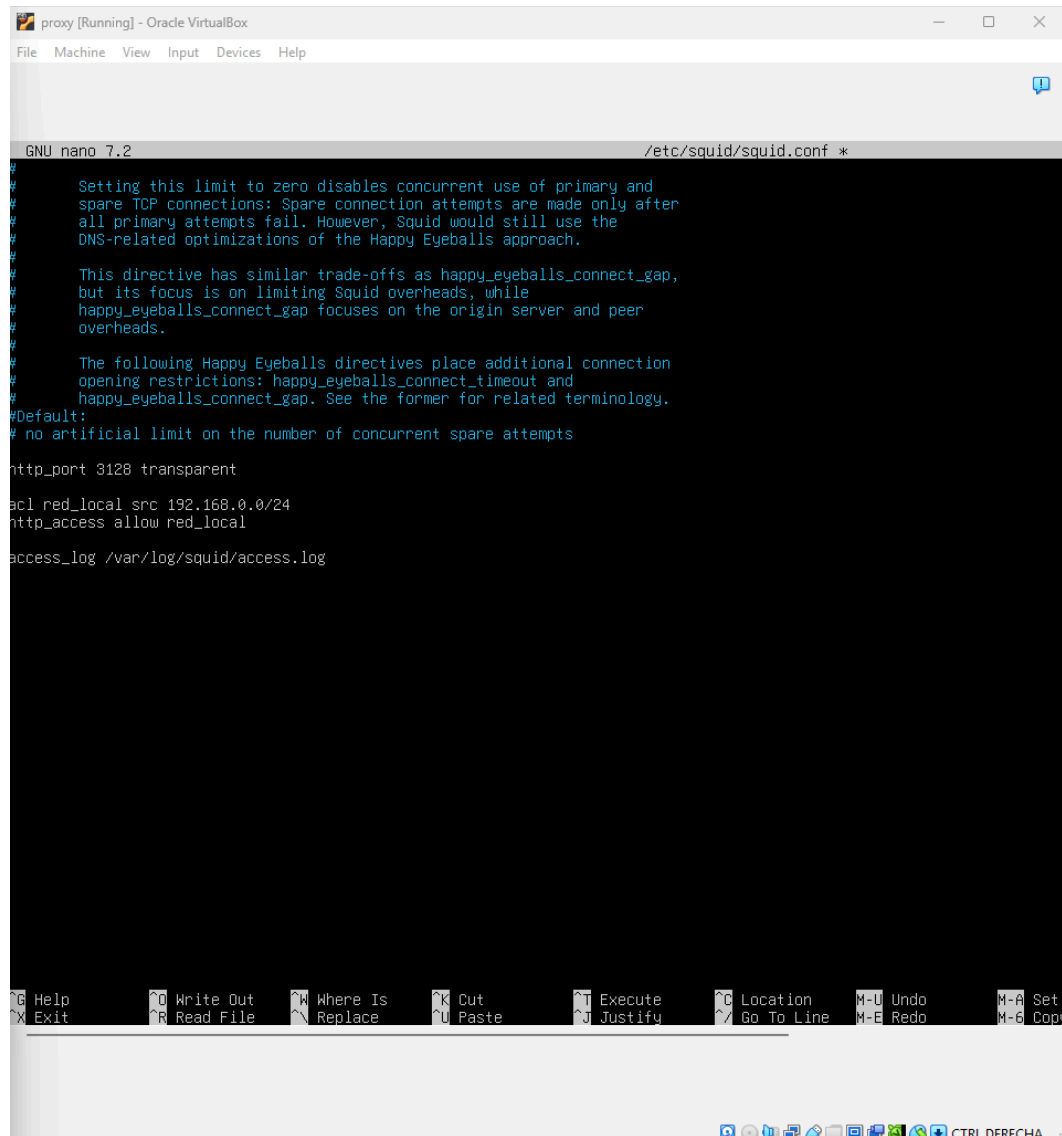
A start job for unit squid.service has finished with a failure.

The job identifier is 2041 and the job result is failed.
lines 162-210/210 (END)
```

```
proxy [Running] - Oracle VirtualBox
File Machine View Input Devices Help

GNU nano 7.2 /etc/squid/squid.conf *
10 6.10
# -----
#
# 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/
#   https://wiki.squid-cache.org/SquidFaq
#   https://wiki.squid-cache.org/ConfigExamples
#
# 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.
#
# Configuration options can be included using the "include" directive.
# Include takes a list of files to include. Quoting and wildcards are
# supported.
#
# For example,
# include /path/to/included/file/squid.acl.config
#
# Includes can be nested up to a hard-coded depth of 16 levels.
# This arbitrary restriction is to prevent recursive include references
# from causing Squid entering an infinite loop whilst trying to load
# configuration files.
#
# Values with byte units
#
# Squid accepts size units on some size related directives. All
# such directives are documented with a default value displaying
# a unit.
#
# Units accepted by Squid are:
#   bytes - byte
#   KB - Kilobyte (1024 bytes)
#   MB - Megabyte
#   GB - Gigabyte
#
[ To suspend, type ^T^Z ]
G Help      ^O Write Out  ^K Where Is   ^K Cut        ^T Execute    ^O Location  M-U Undo    M-A Set
X Exit      ^R Read File  ^N Replace   ^U Paste      ^J Justify    ^_ Go To Line M-E Redo    M-G Copy

CTRL DERECHA
```



The screenshot shows a terminal window titled "proxy [Running] - Oracle VirtualBox". Inside the terminal, the nano 7.2 text editor is open, editing the file "/etc/squid/squid.conf". The editor's status bar at the bottom indicates "GNU nano 7.2" and the file path. The configuration file content is as follows:

```
#
# Setting this limit to zero disables concurrent use of primary and
# spare TCP connections: Spare connection attempts are made only after
# all primary attempts fail. However, Squid would still use the
# DNS-related optimizations of the Happy Eyeballs approach.
#
# This directive has similar trade-offs as happy_eyeballs_connect_gap,
# but its focus is on limiting Squid overheads, while
# happy_eyeballs_connect_gap focuses on the origin server and peer
# overheads.
#
# The following Happy Eyeballs directives place additional connection
# opening restrictions: happy_eyeballs_connect_timeout and
# happy_eyeballs_connect_gap. See the former for related terminology.
#Default:
# no artificial limit on the number of concurrent spare attempts
http_port 3128 transparent
acl red_local src 192.168.0.0/24
http_access allow red_local
access_log /var/log/squid/access.log
```

The nano editor's bottom status bar shows various keyboard shortcuts: ^G Help, ^X Exit, ^O Write Out, ^R Read File, ^W Where Is, ^N Replace, ^K Cut, ^U Paste, ^T Execute, ^J Justify, ^C Location, ^\_ Go To Line, ^M-U Undo, ^M-E Redo, ^M-A Set, ^M-G Cop. The system tray at the bottom right of the window includes icons for network, volume, and other system utilities, along with the text "CTRL DERECHA".

## 4. Verificación final del funcionamiento

Se verificó el correcto funcionamiento de Squid mediante la ejecución de pruebas de navegación en clientes de la red local. Los accesos se registraron correctamente en los logs del sistema, confirmando la operatividad del proxy transparente.

## 5. Conclusión

El objetivo del ejercicio fue alcanzado con éxito, dejando configurado un servidor Squid funcional en modo transparente, capaz de redirigir y registrar el tráfico HTTP/HTTPS desde la red local hacia el exterior. El uso de reglas iptables y el ajuste de la configuración en squid.conf fueron fundamentales en este proceso. La verificación final confirmó la efectividad de la solución implantada.

## 6. Fuentes

- Squid Cache Wiki. (2024). \*Squid Configuration Manual\*.  
<https://wiki.squid-cache.org/ConfigExamples>
- Ubuntu Documentation. (2024). \*Squid - Ubuntu Wiki\*.  
<https://help.ubuntu.com/community/Squid>
- Iptables Tutorial. (2023). \*Configuring iptables for Transparent Proxy\*.  
<https://www.netfilter.org>