

# Instalación y configuración del servidor proxy

## Instalación de SQUID

Procedemos a instalar el servicio de proxy mediante el software “squid” disponible en los repositorios de Ubuntu mediante el siguiente comando:

`apt install squid`

Posteriormente comprobamos que se esta ejecutando correctamente

```
root@servidor-planetas:/home/admin-servidor# 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 2025-03-25 18:40:33 UTC; 15s ago
     Docs: man:squid(8)
   Process: 1591 ExecStartPre=/usr/sbin/squid --foreground -z (code=exited, status=0/SUCCESS)
  Main PID: 1595 (squid)
    Tasks: 4 (limit: 18970)
   Memory: 17.8M (peak: 18.9M)
      CPU: 141ms
   CGroup: /system.slice/squid.service
           └─1595 /usr/sbin/squid --foreground -sYC
             └─1598 "(squid-1)" --kid squid-1 --foreground -sYC
               └─1599 "(logfile-daemon)" /var/log/squid/access.log
                 └─1600 "(pinger)"

Mar 25 18:40:33 servidor-planetas squid[1598]: Using Least Load store dir selection
Mar 25 18:40:33 servidor-planetas squid[1598]: Set Current Directory to /var/spool/squid
Mar 25 18:40:33 servidor-planetas squid[1598]: Finished loading MIME types and icons.
Mar 25 18:40:33 servidor-planetas squid[1598]: HTCP Disabled.
Mar 25 18:40:33 servidor-planetas squid[1598]: Pinger socket opened on FD 14
Mar 25 18:40:33 servidor-planetas squid[1598]: Squid plugin modules loaded: 0
Mar 25 18:40:33 servidor-planetas squid[1598]: Adaptation support is off.
Mar 25 18:40:33 servidor-planetas systemd[1]: Started squid.service - Squid Web Proxy Server.
Mar 25 18:40:33 servidor-planetas squid[1598]: Accepting HTTP Socket connections at conn3 local=[::]:3128 remote=[::] FD 12 flags=9
                                         listening port: 3128
Mar 25 18:40:34 servidor-planetas squid[1598]: storeLateRelease: released 0 objects
```

## Modificación de parámetros de configuración

### Establecimiento de lista de control de acceso “localnet”

En primer lugar modificaremos el archivo de configuración de squid para indicarle cual va a ser la dirección de red, que en este caso es la red 172.20.0.0/26:

· Ruta de acceso al archivo de configuración de squid:

`·/etc/squid/squid.conf`

```
# Example rule allowing access from your local networks.
# Adapt to list your (internal) IP networks from where browsing
# should be allowed
acl localnet src 172.20.0.0/26                # RFC 1918 Red corporativa Planetas S.A. (LAN)
```

## Verificación de puerto a la escucha

Ahora comprobaremos en el fichero de configuración en que puerto por defecto el servidor proxy estará a la escuchar

· Ruta de acceso al archivo de configuración de squid:

·/etc/squid/squid.conf

```
# Squid normally listens to port 3128
http_port 3128
```

Lo vamos a mantener en el puerto por defecto

## Creación de archivo de paginas no autorizadas

Para no tener que modificar el archivo de configuración cada vez que queramos modificar las paginas web a las que no se permite el acceso desde la red corporativa, vamos a crear un archivo que contenga las URL de las paginas no autorizadas:

·Ruta del archivo que contiene las URL no autorizadas:

·/etc/squid/urls\_no\_autorizadas

```
GNU nano 7.2 /etc/squid/urls_no_autorizadas *
shein
es.shein
shein.com
facebook
facebook.com
facebook.es
instagram
instagram.com
instagram.es
tiktok
tiktok.es
tiktok.com
```

He añadido estas url de momento para realizar pruebas de funcionamiento en “equipo-cliente”

## Modificación de listas de control de acceso y establecimiento de reglas

Para modificar el control de acceso a paginas web, debemos establecer listas de controles de acceso dentro del archivo de configuración. Vamos a realizar una configuración básica que deniegue el acceso a las URL indicadas en el archivo creado en el paso anterior y habilitar el acceso a internet a conexiones provenientes de nuestra red corporativa (localnet)

· Ruta de acceso al archivo de configuración de squid:

· /etc/squid/squid.conf

```
#Listas de control de acceso personalizadas para Planetas S.A.  
acl no_aut url_regex "/etc/squid/urls_no_autorizadas"  
  
#Reglas personalizadas para Planetas S.A.  
http_access deny no_aut  
http_access allow localnet
```

## Habilitado de cacheado

Para habilitar la cache, previamente vamos a crear el directorio donde se almacenará el archivo de cache de squid.

· Directorio donde se almacenará el archivo de caché de squid:

· /tmp/squid

Ahora vamos a incluir la opción de uso de cache en el archivo de configuración de squid

· Ruta de acceso al archivo de configuración de squid:

· /etc/squid/squid.conf

```
#Caché  
cache_dir ufs /tmp/squid/ 5000 16 256
```

Tras esto, habilitamos el uso de cache por parte de squid mediante el comando:

· squid -z

```
root@servidor-planetis:/home/admin-servidor# squid -z
2025/03/25 20:59:01| Processing Configuration File: /etc/squid/squid.conf (depth 0)
2025/03/25 20:59:01| Processing Configuration File: /etc/squid/conf.d/debian.conf (depth 1)
2025/03/25 20:59:01| Created PID file (/run/squid.pid)
root@servidor-planetis:/home/admin-servidor# 2025/03/25 20:59:01 kid1| Processing Configuration File: /etc/squid/squid.conf (depth 0)
2025/03/25 20:59:01 kid1| Processing Configuration File: /etc/squid/conf.d/debian.conf (depth 1)
2025/03/25 20:59:01 kid1| Set Current Directory to /var/spool/squid
2025/03/25 20:59:01 kid1| Creating missing swap directories
2025/03/25 20:59:01 kid1| /tmp/squid/ exists
2025/03/25 20:59:01 kid1| Making directories in /tmp/squid//00
2025/03/25 20:59:01 kid1| Making directories in /tmp/squid//01
2025/03/25 20:59:01 kid1| Making directories in /tmp/squid//02
2025/03/25 20:59:01 kid1| Making directories in /tmp/squid//03
2025/03/25 20:59:01 kid1| Making directories in /tmp/squid//04
2025/03/25 20:59:01 kid1| Making directories in /tmp/squid//05
2025/03/25 20:59:01 kid1| Making directories in /tmp/squid//06
2025/03/25 20:59:01 kid1| Making directories in /tmp/squid//07
2025/03/25 20:59:01 kid1| Making directories in /tmp/squid//08
2025/03/25 20:59:01 kid1| Making directories in /tmp/squid//09
2025/03/25 20:59:01 kid1| Making directories in /tmp/squid//0A
2025/03/25 20:59:01 kid1| Making directories in /tmp/squid//0B
2025/03/25 20:59:01 kid1| Making directories in /tmp/squid//0C
2025/03/25 20:59:01 kid1| Making directories in /tmp/squid//0D
2025/03/25 20:59:01 kid1| Making directories in /tmp/squid//0E
2025/03/25 20:59:01 kid1| Making directories in /tmp/squid//0F
2025/03/25 20:59:01| Removing PID file (/run/squid.pid)
```

Al finalizar este proceso squid ya esta haciendo uso de cache

## Modificaciones en equipo clientes

Para establecer el uso del servidor proxy corporativo en el sistema del equipo cliente debemos ejecutar los siguientes comandos o incluirlos en un script y ejecutarlo:

```
echo "http_proxy=http://172.20.0.1:3128" | sudo tee -a /etc/environment
```

```
echo "https_proxy=http://172.20.0.1:3128" | sudo tee -a /etc/environment
```

Posteriormente añadiremos estos comandos en una automatización mediante el software Ansible si me da tiempo a llegar a implementar esa mejora

## Pruebas en “equipo-cliente”

Accedemos a uno de los sitios establecidos como no autorizados para comprobar el correcto funcionamiento del servidor proxy



El servidor proxy rechaza las conexiones a las paginas establecidas como no autorizadas