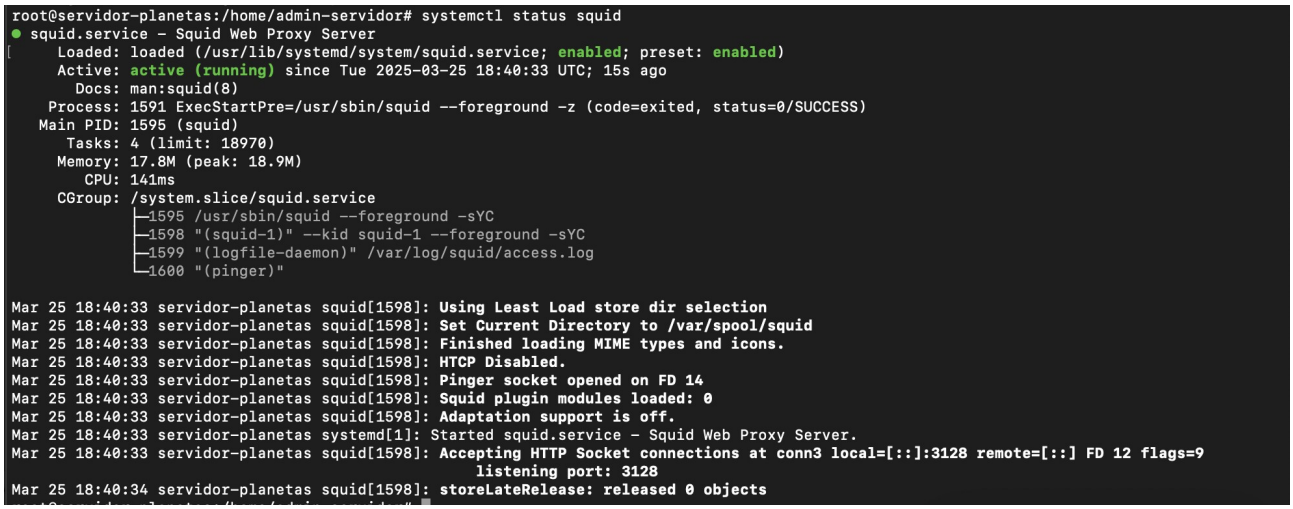
Instalación y configuración del servidor proxy

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



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

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 estableces 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 almanenará 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

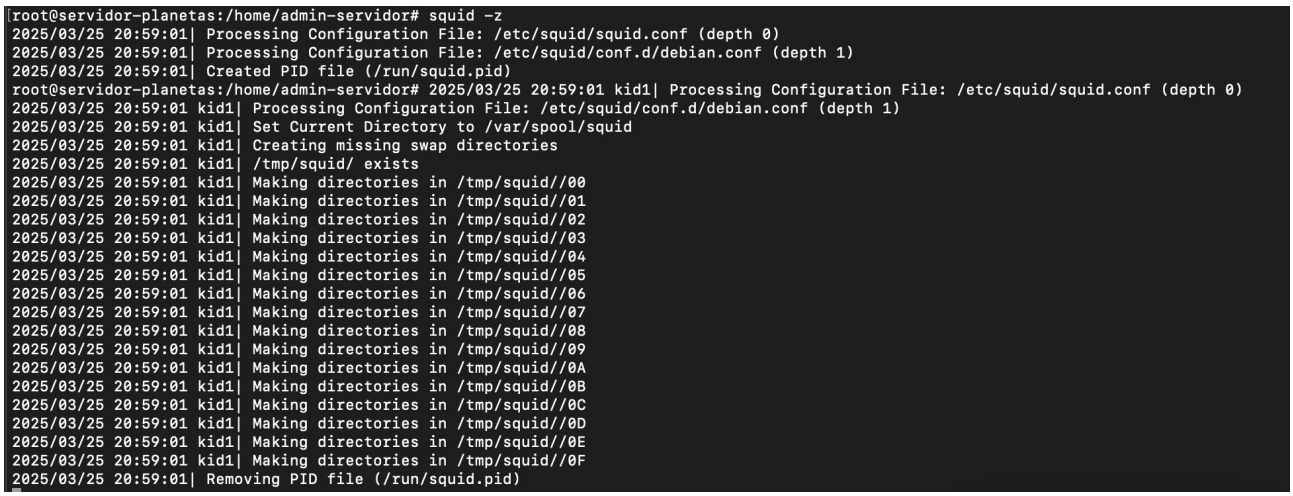
·Ruta de acceso al archivo de configuración de squid:

- ·/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



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