



# Proyecto

## Ciberseguridad

CONFIGURACIÓN DE  
PROXY SQUID



ISMAEL VELÁZQUEZ CHÁVEZ

## Tabla de contenido

1.	INTRODUCCIÓN .....	3
2.	ESCENARIO DE LA PRÁCTICA .....	3
3.	INSTALACIÓN DE PROXY SQUID .....	6
4.	CONFIGURACIÓN POR DEFECTO DE SQUID .....	8
5.	DEFINICIÓN Y USO DE LAS ACL.....	10
6.	VERIFICACIÓN DEL FUNCIONAMIENTO DEL PROXY .....	13
7.	CONFIGURACIÓN BÁSICA DEL PROXY .....	14
8.	REGISTROS (LOGS) EN SQUID .....	16
9.	BLOQUEO DE DOMINIOS.....	17
10.	ORDEN Y FUNCIONAMIENTO DE LAS ACL .....	20
11.	BLOQUEO MEDIANTE EXPRESIONES REGULARES.....	22
12.	BLOQUEO POR DÍAS Y HORARIOS .....	23
13.	PERSONALIZACIÓN DEL MENSAJE DE ERROR.....	24
14.	AUTENTICACIÓN DE USUARIOS.....	27
15.	VERIFICACIÓN DEL FUNCIONAMIENTO DE LA CACHÉ.....	30
16.	CONFIGURACIÓN DE LA CACHÉ.....	31
17.	USO DE LISTAS PÚBLICAS DE BLOQUEO DE DOMINIOS .....	32
	Conclusiones .....	¡Error! Marcador no definido.

## 1. INTRODUCCIÓN

En el contexto actual de conectividad constante y uso masivo de internet, las organizaciones requieren mecanismos eficaces para controlar el tráfico de red, garantizar la seguridad de los usuarios y optimizar el consumo de recursos. Uno de los enfoques más utilizados para lograr estos objetivos es la implementación de servidores proxy, siendo SQUID una de las herramientas más robustas y versátiles en entornos Linux.

Este proyecto tiene como finalidad instalar, configurar y administrar un servidor proxy SQUID, explorando desde su puesta en marcha hasta la aplicación de políticas de control de acceso (ACL), autenticación de usuarios y filtrado de contenido. A lo largo del desarrollo, se abordarán aspectos clave como la gestión de la caché, la personalización de mensajes de error, el bloqueo de dominios y expresiones regulares, así como la integración de listas públicas para reforzar el filtrado web.

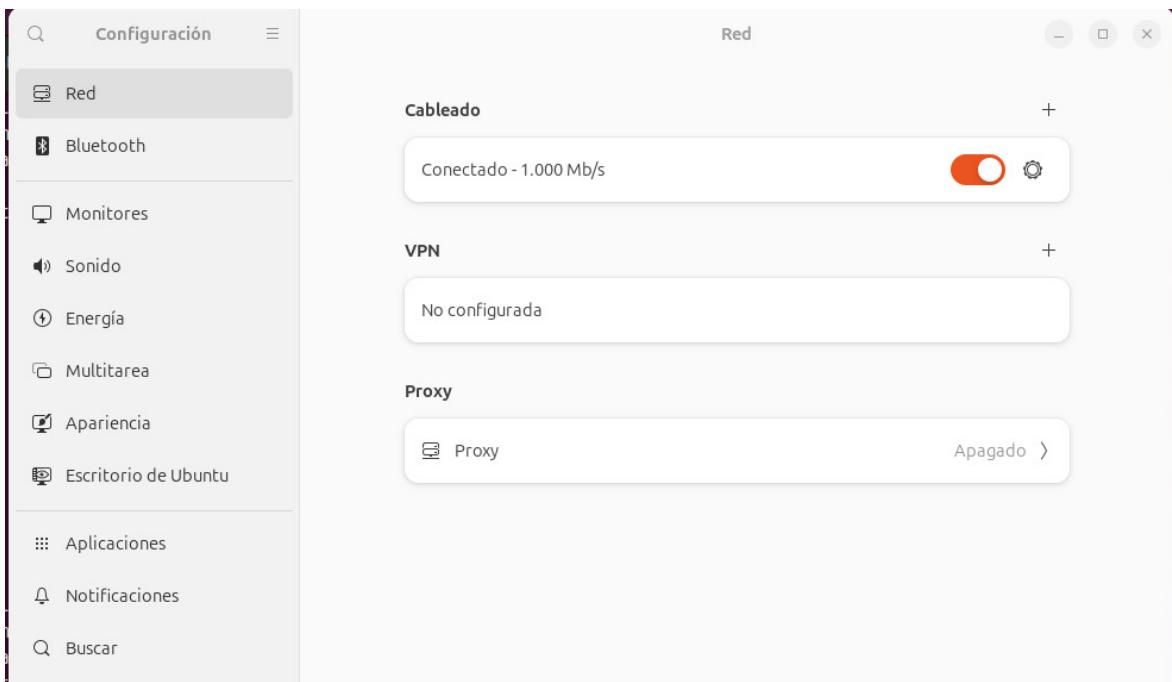
Mediante esta práctica se busca proporcionar una base sólida en la administración de proxies, permitiendo comprender su funcionamiento, utilidad en redes corporativas y su papel como herramienta de seguridad y optimización del ancho de banda.

## 2. ESCENARIO DE LA PRÁCTICA

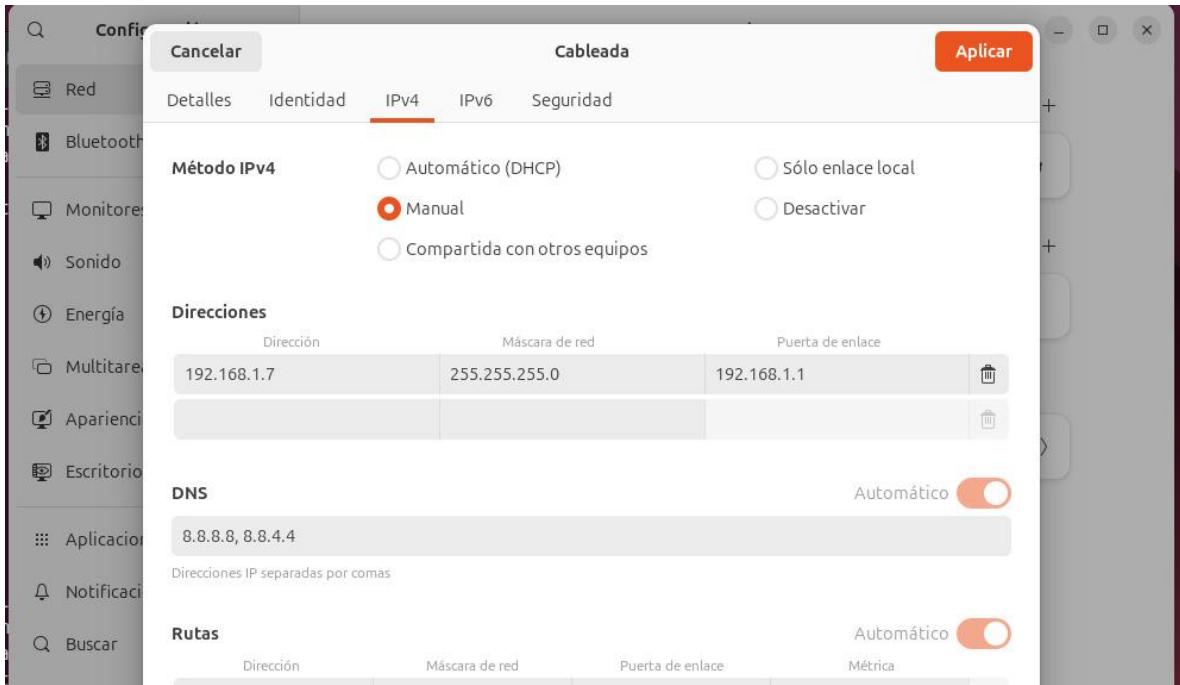
Para empezar, ejecutaremos una serie de comandos que son ejecutados en la terminal de Linux, en este caso la distribución a utilizar será Ubuntu versión: ()�.

Configuraciones previas: dirección ip estática

Acceso a configuración y luego a Red:



Accedemos a configuración y posterior a ello en ipv4



Llenamos los campos para convertir nuestra dirección ip en estática, seleccionando la dirección, mascara de red y puerta de enlace. Llenamos también el apartado de DNS. Aplicamos los cambios. Una vez hecho los cambios, verificamos que los cambios estén ejecutados y Comenzamos. Continuamos.

#### Instalación de servidor SSH

- Conexión SSH al servidor : ssh usuario@direccion\_ip

Este comando inicia una conexión remota segura (SSH) al servidor con IP, usando el usuario de la maquina indicada, dicho comando permite administrar la máquina de forma remota desde otra computadora o terminal

```
ismaelvelazquez@ismaelvelazquez-VirtualBox:~$ ssh ismaelvelazquez@192.168.1.7
The authenticity of host '192.168.1.7 (192.168.1.7)' can't be established.
ED25519 key fingerprint is SHA256:FpcS7YsuzR/neS6w9IPryMpc1u0ItZkZLYDrsw4kMSY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.7' (ED25519) to the list of known hosts.
ismaelvelazquez@192.168.1.7's password:
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.11.0-26-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

El mantenimiento de seguridad expandido para Applications está desactivado

Se pueden aplicar 0 actualizaciones de forma inmediata.

Active ESM Apps para recibir futuras actualizaciones de seguridad adicionales.
Vea https://ubuntu.com/esm o ejecute «sudo pro status»


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.
```

- Actualizar la lista de paquetes: sudo apt-get update

Dicho comando permite actualizar el índice de paquetes disponibles desde los repositorios configurados en el sistema. No instala, solo permite actualizar la información de los paquetes.

- Instalar servidor SSH: sudo apt-get install openssh-server

Instala el servidor SSH en la máquina (si este no se encuentra instalado). Dicho comando se que otros dispositivos puedan conectarse vía SSH a esta máquina.

Tras haber ejecutado los comandos de ssh revisamos por medio de nmap:

Nmap es una herramienta que permite escanear redes con el objetivo de encontrar dispositivos, puertos abiertos y servicios en ejecución.

Para este caso usaremos este nmap para averiguar que puertos se encuentran en servicio activo:  
el comando a usar ahora es:

```
ismaelvelazquez@ismaelvelazquez-VirtualBox:~$ nmap localhost
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-08 14:49 CST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00022s latency).

Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
631/tcp   open  ipp

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
```

Para verificar si esta activo el servidor ssh se usa:

```
ismaelvelazquez@ismaelvelazquez-VirtualBox:~$ systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: enabled)
  Active: active (running) since Sun 2025-06-08 14:49:33 CST; 9min ago
    TriggeredBy: ● ssh.socket
    Docs: man:sshd(8)
           man:sshd_config(5)
  Process: 4798 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
 Main PID: 4800 (sshd)
   Tasks: 1 (limit: 3472)
  Memory: 2.1M (peak: 3.4M)
    CPU: 209ms
   CGroup: /system.slice/ssh.service
           └─4800 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

jun 08 14:49:33 ismaelvelazquez-VirtualBox systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
jun 08 14:49:33 ismaelvelazquez-VirtualBox sshd[4800]: Server listening on :: port 22...
jun 08 14:49:33 ismaelvelazquez-VirtualBox systemd[1]: Started ssh.service - OpenBSD Secure Shell server...
```

¿Por qué es importante ejecutar un servidor ssh y para qué sirve en este proyecto?

Secure Shell es un protocolo seguro que permite acceder a otra máquina a través de una red. Usando un cifrado para proteger la comunicación entre el cliente y el servidor. Para este caso es importante por varias razones, permitiendo administrar el servidor remotamente, desde otra máquina sin necesidad de tener acceso físico. Es de gran utilidad ya que por ejemplo se está trabajando desde una máquina anfitriona (host) y un servidor está en una máquina virtual. Una de las grandes ventajas en este caso, es que es fácil de instalar y configurar SQUID, permitiendo editar archivos de configuración, y reiniciar servicios desde la terminal remota. El uso de SSH permite usar una propia terminal, para gestionar el servidor.

### 3. INSTALACIÓN DE PROXY SQUID

Para esta sección utilizaremos comandos relevantes

- Actualizaciones: sudo apt-get update

permite actualizar paquetes en caso de ser necesario. Permitiendo usar las versiones más recientes.

- Instalacion del servidor proxy SQUID: sudo apt-get install squid

el cual es un proxy cache para la web que permite filtrar el contenido y mejora el rendimiento de navegación, este comando permite descargarlo e instalarlo.

```
ismaelvelazquez@ismaelvelazquez-VirtualBox:~$ sudo apt-get install squid
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no
son necesarios.
  libllvm17t64 python3-netifaces
Utilice «sudo apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes adicionales:
  libdbi-perl libecap3 squid-common squid-langpack
Paquetes sugeridos:
  libmldb-perl libnet-daemon-perl libsql-statement-perl squidclient squid-cgi
  squid-purge resolvconf smbclient winbind
Se instalarán los siguientes paquetes NUEVOS:
```

- Verificacion de versión: squid –v

Permite verificar la versión instalada de squid, una de las funciones es que permite detectar si la versión se instaló correctamente.

```
Squid Cache: Version 6.10
Service Name: squid
Ubuntu linux
configure options: '--build=x86_64-linux-gnu' '--prefix=/usr' '--includedir=${prefix}/include' '--mandir=${prefix}/share/man' '--infodir=${prefix}/share/info'
```

- Ayuda: squid –h

Muestra una lista de opciones de ayuda y parámetros disponibles para el comando squid. Siendo esta una guía rápida desde la terminal.

- Verificar estado: service squid status

verifica si esta cuenta o con errores o está activo o inactivo.

```
ismaelvelazquez@ismaelvelazquez-VirtualBox:~$ service squid status
● squid.service - Squid Web Proxy Server
   Loaded: loaded (/usr/lib/systemd/system/squid.service; enabled; preset: en>
   Active: active (running) since Sun 2025-06-08 15:45:21 CST; 1min 53s ago
     Docs: man:squid(8)
  Process: 4706 ExecStartPre=/usr/sbin/squid --foreground -z (code=exited, st>
 Main PID: 4710 (squid)
    Tasks: 4 (limit: 3472)
   Memory: 17.8M (peak: 18.3M)
      CPU: 207ms
     CGroup: /system.slice/squid.service
             └─4710 /usr/sbin/squid --foreground -sYC
                 ├─4713 "(squid-1)" --kid squid-1 --foreground -sYC
                 ├─4714 "(logfile-daemon)" /var/log/squid/access.log
                 └─4715 "(pinger)"

jun 08 15:45:21 ismaelvelazquez-VirtualBox squid[4713]: Using Least Load store >
jun 08 15:45:21 ismaelvelazquez-VirtualBox squid[4713]: Set Current Directory to >
jun 08 15:45:21 ismaelvelazquez-VirtualBox squid[4713]: Finished loading MIME t>
jun 08 15:45:21 ismaelvelazquez-VirtualBox squid[4713]: HTCP Disabled.
jun 08 15:45:21 ismaelvelazquez-VirtualBox squid[4713]: Pinger socket opened on >
jun 08 15:45:21 ismaelvelazquez-VirtualBox squid[4713]: Squid plugin modules lo>
```

#### 4. CONFIGURACIÓN POR DEFECTO DE SQUID

Para la configuración tenemos los siguientes comandos:

Para empezar accedemos a la ruta de squid:

```
ismaelvelazquez@ismaelvelazquez-VirtualBox:~$ cd etc/squid
bash: cd: etc/squid: No existe el archivo o el directorio
ismaelvelazquez@ismaelvelazquez-VirtualBox:~$ cd /etc/squid
ismaelvelazquez@ismaelvelazquez-VirtualBox:/etc/squid$ ls
conf.d  errorpage.css  squid.conf
ismaelvelazquez@ismaelvelazquez-VirtualBox:/etc/squid$ ls -l
total 356
drwxr-xr-x 2 root root  4096 jun  8 15:45 conf.d
-rw-r--r-- 1 root root  1791 sep  9 2024 errorpage.css
-rw-r--r-- 1 root root 352677 sep  9 2024 squid.conf
ismaelvelazquez@ismaelvelazquez-VirtualBox:/etc/squid$ S
```

Para comenzar con la configuración básica: ejecutamos los siguientes comandos:

- Respaldo: sudo cp /etc/squid/squid.conf /etc/squid/squid.conf.backup

Copia el archivo de configuración original de Squid y crea una copia de seguridad. Sirve para tener un respaldo antes de hacer cambios.

```
ismaelvelazquez@ismaelvelazquez-VirtualBox:/etc/squid$ sudo cp squid.conf squid.conf.backup
ismaelvelazquez@ismaelvelazquez-VirtualBox:/etc/squid$ ls -l
total 704
drwxr-xr-x 2 root root    4096 jun  8 15:45 conf.d
-rw-r--r-- 1 root root    1791 sep  9  2024 errorpage.css
-rw-r--r-- 1 root root 352677 sep  9  2024 squid.conf
-rw-r--r-- 1 root root 352677 jun  8 15:57 squid.conf.backup
ismaelvelazquez@ismaelvelazquez-VirtualBox:/etc/squid$
```

- Edición de archivo: sudo vim /etc/squid/squid.conf

Permite abrir el archivo de configuración usando el editor vim con permisos de super usuario.

- Configuraciones activas: :g/^s\*#/d

Elimina todas las líneas que son comentarios, sirve para limpiar el archivo y ver solo las configuraciones activas.

- Fuera líneas en blanco: :g/^\$/d

En vim, elimina todas las líneas en blanco del archivo. Ayuda a tener un archivo más limpio y ordenado

- Guardar cambios: :wq

Guardar (write) y salir (quit) del archivo. Guarda los cambios hechos al archivo de configuración.

```
ismaelvelazquez@ismaelvelazquez-VirtualBox:/etc/squid
```

```
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 deny manager
http_access allow localhost
http_access deny to_localhost
http_access deny to_linklocal
include /etc/squid/conf.d/*.conf
http_access deny 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 \/(Packages|Sources)(|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims
refresh_pattern \/Release(|\.pgg)$ 0 0% 0 refresh-ims
refresh_pattern \/InRelease$ 0 0% 0 refresh-ims
refresh_pattern \/(Translation-.*)(|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims
refresh_pattern .               0      20%    4320
:wq
```

- Archivos adicionales: include /etc/squid/conf.d/\*

Incluye todos los archivos adicionales de configuración ubicados en: /etc/squid/conf.d/

Aquí ubicaremos cada uno de los ficheros relevantes para configuraciones en el futuro

- **Puert:** en el que escuchará el proxy Squid.

El puerto 3128 es el puerto por defecto que utiliza Squid para recibir solicitudes HTTP.

## 5. DEFINICIÓN Y USO DE LAS ACL

Hay dos componentes diferentes: ACL y listas de acceso. Una lista de acceso consta de una acción de permitir o denegar seguida de una serie de elementos de ACL.

Al cargar el archivo de configuración, Squid procesa todas las líneas de acl (directivas) en la memoria como pruebas que se pueden realizar contra cualquier solicitud transacción. Los tipos de pruebas se describen en la siguiente sección ACL Elementos. Por sí solas, estas pruebas no hacen nada. Por ejemplo; La palabra "Domingo" coincide con un día de la semana, pero no indica qué día de la semana que estás leyendo esto.

Para procesar una transacción se utiliza otro tipo de línea. A medida que cada La acción de procesamiento debe tener lugar en la ejecución para probar qué acción o se van a producir limitaciones para la transacción. Los tipos de cheques son: descrito en la siguiente sección Listas de acceso, seguido de detalles de cómo Los cheques operan.

### Tipos de ACL disponibles

- **src:** direcciones IP de origen (cliente)
- **dst:** direcciones IP de destino (servidor)
- **myip:** la dirección IP local de la conexión de un cliente
- **arp:** Coincidencia de direcciones Ethernet (MAC)
- **srcdomain:** nombre de dominio de origen (cliente)
- **dstdomain:** nombre de dominio de destino (servidor)
- **srcdom\_regex:** patrón de expresión regular de origen (cliente) cotejo
- **dstdom\_regex:** patrón de expresión regular de destino (servidor) cotejo
- **src\_as:** número del Sistema Autónomo de origen (cliente)
- **dst\_as:** número del Sistema Autónomo de destino (servidor)
- **peername:** etiqueta de nombre asignada al cache\_peer donde se solicita se espera que se envíe.
- **Hora:** hora del día y día de la semana
- **url\_regex:** Coincidencia de patrones de expresiones regulares de URL
- **urlpath\_regex:** coincidencia de patrones de expresiones regulares URL-path, omite el protocolo y el nombre de host
- **Puerto:** número de puerto de destino (servidor)

- **myport**: número de puerto local al que se conectó el cliente
- **myportname**: etiqueta de nombre asignada al puerto de escucha de Squid que cliente conectado a
- **Proto**: Protocolo de transferencia (http, FTP, etc)
- **method**: Método de solicitud HTTP (get, post, etc.)
- **http\_status**: estado de respuesta HTTP (200 302 404, etc.)
- **Navegador**: coincidencia de patrones de expresiones regulares en la solicitud encabezado user-agent
- **referer\_regex**: coincidencia de patrones de expresiones regulares en el Solicitud de encabezado http-referer
- **ident**: coincidencia de cadena en el nombre del usuario
- **ident\_regex**: coincidencia de patrones de expresiones regulares en el archivo nombre
- **proxy\_auth**: autenticación de usuarios a través de procesos externos
- **proxy\_auth\_regex**: coincidencia de patrones de expresión regular en el usuario Autenticación a través de procesos externos
- **snmp\_community**: Coincidencia de cadenas de la comunidad SNMP
- **maxconn**: un límite en el número máximo de conexiones de un dirección IP de cliente único
- **max\_user\_ip**: un límite en el número máximo de direcciones IP El usuario puede iniciar sesión desde
- **req\_mime\_type**: coincidencia de patrones de expresión regular en el request content-type encabezado
- **req\_header**: coincidencia de patrones de expresión regular en una solicitud Contenido del encabezado
- **rep\_mime\_type**: coincidencia de patrones de expresiones regulares en el Responder (contenido descargado) encabezado de tipo de contenido. Esto solo es utilizable en la Directiva http\_reply\_access, no en http\_access.
- **rep\_header**: coincidencia de patrones de expresiones regulares en una respuesta Contenido del encabezado. Esto solo se puede usar en el http\_reply\_access directiva, no http\_access.
- **Externo**: Búsqueda a través de un ayudante de ACL externo definido por external\_acl\_type
- **user\_cert**: hacer coincidir con los atributos de un certificado SSL de usuario
- **ca\_cert**: hacer coincidir con los atributos de un usuario que emite CA SSL certificado

- **ext\_user**: coincidir en el campo user= devuelto por el asistente de ACL externo definido por external\_acl\_type
- **ext\_user\_regex**: coincidencia de patrones de expresión regular en user= Campo devuelto por el ayudante de ACL externo definido por external\_acl\_type

## Listas de acceso

Hay una serie de listas de acceso diferentes:

- [\*\*http\\_access\*\*](#): Permite que los clientes HTTP (navegadores) accedan al puerto HTTP. Este es el Lista de control de acceso principal.
- [\*\*http\\_reply\\_access\*\*](#): Permite que los clientes HTTP (navegadores) reciban la respuesta a su pedir. Esto restringe aún más los permisos otorgados por [\*\*http\\_access\*\*](#), y está diseñado principalmente para usarse junto con rep\_mime\_type [\*\*ACL\*\*](#) para bloquear Diferentes tipos de contenido.
- [\*\*icp\\_access\*\*](#): Permite que las cachés vecinas consulten su caché con ICP.
- [\*\*miss\\_access\*\*](#): Permite que ciertos clientes reenvíen errores de caché a través de su caché. Esto restringe aún más los permisos otorgados por [\*\*http\\_access\*\*](#), y está destinado principalmente a ser utilizado para reforzar las relaciones entre hermanos Al denegar que los hermanos reenvíen errores de caché a través de su caché.
- [\*\*caché\*\*](#): Define respuestas que no se deben almacenar en caché.
- [\*\*url\\_rewrite\\_access\*\*](#): Controla qué solicitudes se envían a través del grupo de redirecciónamiento.
- [\*\*ident\\_lookup\\_access\*\*](#): Controla qué solicitudes necesitan una búsqueda de Ident.
- [\*\*always\\_direct\*\*](#): Controla qué solicitudes siempre se deben reenviar directamente a servidores de origen.
- [\*\*never\\_direct\*\*](#): Controla qué solicitudes nunca deben reenviarse directamente al origen Servidores.
- [\*\*snmp\\_access\*\*](#): Controla el acceso del cliente SNMP a la memoria caché.
- [\*\*broken\\_posts\*\*](#): Define las solicitudes para las que squid anexa un CRLF adicional después de POST cuerpos de mensaje según lo requieran algunos servidores de origen rotos.
- [\*\*cache\\_peer\\_access\*\*](#): Controla qué solicitudes se pueden reenviar a un vecino determinado ([\*\*cache\\_peer\*\*](#)).
- [\*\*htcp\\_access\*\*](#): Controla qué equipos remotos pueden realizar solicitudes HTCP.
- [\*\*htcp\\_clr\\_access\*\*](#): Controla qué equipos remotos pueden realizar solicitudes HTCP CLR.
- [\*\*request\\_header\\_access\*\*](#): Controla qué encabezados de solicitud se eliminan cuando se infringe HTTP protocolo.

- [reply\\_header\\_access](#): Controla qué encabezados de respuesta se eliminan de la entrega al cliente al violar el protocolo HTTP.
- [delay\\_access](#): Controla qué solicitudes se manejan con qué [retraso piscina](#)
- [icap\\_access](#): (reemplazado por [adaptation\\_access](#) en [Squid-3.1](#)) Qué solicitudes se pueden enviar a un servidor ICAP en particular.
- [adaptation\\_access](#): Qué solicitudes se pueden enviar a un filtro ICAP o eCAP en particular servicio.
- [log\\_access](#): Controla qué solicitudes se registran. Esto es global y anula Listas de acceso a archivos específicas anexadas a las directivas [access\\_log](#).

Una lista de control de acceso que ayuda a permitir o denegar solicitudes de clientes hacia recursos web, teniendo en cuenta alguno criterios como IP de origen, Puerto de destino Nombre de dominio, horarios. Es necesario entender dos conceptos fundamentales, los componentes de una ACL, la cual se define usando palabras clave acl seguida del nombre de la lista, el tipo y el argumento. Colocaremos un ejemplo simple: acl localnet src 10.0.0.0/8

Localnet = nombre de la ACL, src= tipo, 10.0.0.0/8 = argumento

El segundo componente consta de las listas de acceso, las cuales refieren a que acción se van a realizar con las ACL, ya sea permitir (allow) o denegar (deny) un ejemplo básico es: http\_access allow localnet.

Al momento de definir la sintaxis es la siguiente acl <nombre> <tipo> <valor>

Y al momento de aplicar la política:

http\_access allow|deny <nombre>

## 6. VERIFICACIÓN DEL FUNCIONAMIENTO DEL PROXY

Una vez entendido conceptos fundamentales acerca de lo que son las listas de control de acceso. Procedemos a verificar el funcionamiento de squid. Utilizando Curl,

CURL: basado en sistemas Unix. Es una abreviatura de client URL, comandos diseñados para funcionar como una forma de verificar la conectividad de las URL. Y como una gran herramienta para transferir datos. Permite enviar datos hacia o desde un servidor sin interacción del usuario utilizando la biblioteca libcurl. Curl, también puede usarse para solucionar problemas de conexión. Es compatible con muchos de los protocolos tales como http, https, gtp, ftps, imap, imapspop, pops. Por mencionar algunos. Su sintaxis básica es: curl [options] [url] El uso más simple de curl es mostrar el contenido de una página.

Para este caso: utilizaremos una sintaxis como la siguiente:

curl -x http:// 192.168.1.41:3128 -I <http://www.google.com/> puede solicitar o colocarse usuario y contraseña.

-x pasa un servidor proxy a curl

-I solo muestra la info del documento.

```
ismaelvelazquez@ismaelvelazquez-VirtualBox:~$ curl -x http://192.168.1.7:3128 -I http://www.google.com/
HTTP/1.1 403 Forbidden
Server: squid/6.10
Mime-Version: 1.0
Date: Mon, 09 Jun 2025 04:28:17 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 3536
X-Squid-Error: ERR_ACCESS_DENIED 0
Vary: Accept-Language
Content-Language: en
Cache-Status: ismaelvelazquez-VirtualBox
Via: 1.1 ismaelvelazquez-VirtualBox (squid/6.10)
Connection: keep-alive
```

También utilizaremos una extensión denominada FoxyProxy, esta es una herramienta de administración de proxys avanzada, que reemplaza totalmente la limitada funcionalidad de proxis nativa de Firefox. FoxyProxy automatiza el proceso manual de modificar los parámetros de las propiedades de Conexión de FireFox. El cambio de servidor proxy es dependiente de la pagina a cargar y las reglas de selección definidas por el usuario.



## 7. CONFIGURACIÓN BÁSICA DEL PROXY

Para la siguiente sección procedemos a configurar squid.

- Creamos el fichero de reglas, con el comando: `sudo nano /etc/squid/conf.d/myrules.conf`

abrimos el editor con permisos de superusuario, creando el archivo myrules.conf en la carpeta de configuración de Squid.

- Creamos archivo ACL: `acl miredlocal src 192.168.1.0/24`

Define una acl (Access control list) de nombre miredlocal, el elemento de src implica que se aplica a todos los dispositivos de la red local de dirección ip con mascara de subred de 24 bits, permitiendo agrupar dispositivos bajo una sola regla para controlar su acceso.

- Acceso a internet: http\_access allow miredlocal

Permite que la ACL miredlocal tenga acceso a Internet mediante el proxy Squid.

- Actualización: service squid reload

Recarga el servicio de Squid para aplicar los cambios. Es útil cuando se ha modificado los archivos de configuración sin detener el servicio.

- Reconfiguración de archivos actualizados: sudo squid -k reconfigure

```
ismaelvelazquez@ismaelvelazquez-VirtualBox: $ sudo nano /etc/squid/conf.d/myrules.conf
[sudo] contraseña para ismaelvelazquez:
ismaelvelazquez@ismaelvelazquez-VirtualBox: $ sudo squid -k reconfigure
2025/06/10 00:11:08| Processing Configuration File: /etc/squid/squid.conf (depth 0)
2025/06/10 00:11:08| Processing Configuration File: /etc/squid/conf.d/debian.conf (depth 1)
2025/06/10 00:11:08| Processing Configuration File: /etc/squid/conf.d/myrules.conf (depth 1)
2025/06/10 00:11:08| Set Current Directory to /var/spool/squid
ismaelvelazquez@ismaelvelazquez-VirtualBox: $ curl -x http://192.168.1.7:3128 -I http://www.google.com
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-Yf5g98P9hjxviHdPdMJSHw' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http://report-uri https://csp.withgoogle.com/csp/gws/other-hp
P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info."
Date: Tue, 10 Jun 2025 06:12:34 GMT
Server: gws
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN
Expires: Tue, 10 Jun 2025 06:12:34 GMT
Cache-Control: private
Set-Cookie: AEC=AVh_V2j3VA5mslROKf9l3xfJ7VycIBYDtveEAwqovPkkrQUmyuVj8uj_VjM; expires=Sun, 07-Dec-2025 06:12:34 GMT; path=/; domain=.google.com; Secure; HttpOnly; SameSite=lax
Set-Cookie: NID=524=oGuEQNzHR6bkVeRTobnKdQ9q9a3ovtIo9tFnU0RMGSNa2wrWFOnawelcfrXPXljUDQ8ltSG4obeQTMnoDeOefN3PTKCLc2_tWoNLiok0kV7uborUPl06w14JLJA6MC4utNFKrJdqCxyVUUcSAF5_20nXHJHuHIIKdBJDjhQ2jkMx6k1HZ4qiFYGN9CCaVT88XjHdzC79yyUIw; expires=Wed, 1
```

Internet Protocol, es un identificador único asignado a cada dispositivo que se conecta a una red, permitiendo así la comunicación entre ellos

#### ESTRUCTURA:

intervalo de direcciones IP inicio hasta una dirección final. El protocolo IP se encarga de la asignación de direcciones IP en una red, asegurando así la comunicación entre dispositivos conectados. Expertos en redes como Vint Cerf, considerado uno de los padres de Internet, y estudios como el de la IEEE (Instituto de Ingenieros Eléctricos y Electrónicos) han contribuido significativamente al desarrollo de estándares y buenas prácticas en la configuración de rangos de direcciones IP.

#### TIPOS DE RANGO DE DIRECCIONES IP

Rango de direcciones IP públicas: Estas direcciones son únicas en internet y se utilizan para identificar dispositivos de manera global. Se asignan por entidades como la Internet Assigned Numbers Authority (IANA) y suelen ser utilizadas en servidores web, correos electrónicos, entre otros.

Rango de direcciones IP privadas: Estas direcciones se reservan para uso interno en redes privadas y no están destinadas a ser enruteadas a través de internet. Son comúnmente usadas en redes domésticas y empresariales, permitiendo la conexión de múltiples dispositivos de forma local

Rango de direcciones IP **estáticas**: En este tipo de rango, las direcciones IP no cambian y se asignan manualmente a cada dispositivo de la red. Son ideales para servidores, impresoras o dispositivos que requieren una dirección fija y constante.

Rango de direcciones IP **dinámicas**: Las direcciones IP dinámicas se asignan automáticamente a los dispositivos mediante un servidor DHCP (Dynamic Host Configuration Protocol). Este método es conveniente para redes en las que se conectan y desconectan dispositivos con frecuencia.

## CÓMO CONFIGURAR UN RANGO DE DIRECCIONES IP

- Identificar el **tipo de red**: Antes de establecer un rango de direcciones IP, es crucial determinar si se trata de una red local (LAN) o una red pública (WAN).
- Determinar el **rango de direcciones**: Define el rango de direcciones IP disponibles para asignar a los **dispositivos de la red**. Esto se hace estableciendo **una dirección IP inicial y una dirección IP final dentro de un rango específico**.
- Configuración del **enrutador o switch**: Accede a la configuración del **dispositivo de red (router o switch)** y asigna el **rango de direcciones IP definido anteriormente**. Es importante asegurarse de que no haya **conflictos de direcciones dentro de la red**.
- Reserva de **direcciones estáticas**: Para dispositivos que siempre necesitan la misma dirección IP, como servidores o impresoras de red, considera reservar direcciones estáticas dentro del **rango definido para evitar asignaciones automáticas**.
- Pruebas de conectividad: Una vez configurado el rango de direcciones IP, realiza pruebas de **conectividad para verificar que los dispositivos puedan comunicarse entre sí** correctamente.

## 8. REGISTROS (LOGS) EN SQUID

- Ubicación de logs: ls /var/log/squid/

Lista los archivos de registro generados por Squid. El comando accede a la ruta donde se guardan los logs.

```
ismaelvelazquez@ismaelvelazquez-VirtualBox:/var/log/squid$ ls -l
total 68
-rw-r----- 1 proxy proxy 10575 jun 10 00:14 access.log
-rw-r----- 1 proxy proxy 52170 jun 10 23:59 cache.log
ismaelvelazquez@ismaelvelazquez-VirtualBox:/var/log/squid$
```

- Actividad en tiempo real: sudo tail -f /var/log/squid/access.log

Tail -f muestra las últimas líneas del archivo y sigue mostrando nuevas líneas a medida que se agregan. Para comandos de esta índole se necesitan permisos de superusuario y leer estos logs. Access.log es el archivo donde Squid registra las peticiones de los clientes.

En el archivo acces.log, se generan los registros de acceso a internet que se realizan a través del proxy squid incluyen fecha y hora, dirección ip del cliente, método http, url solicitada, código de estado http, tamaño de la respuesta y tiempo de la respuesta,

```

ismaelvelazquez@ismaelvelazquez-VirtualBox: $ ssh ismaelvelazquez@192.168.1.7
ismaelvelazquez@192.168.1.7's password:
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.11.0-26-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/pro

El mantenimiento de seguridad expandido para Applications está desactivado

Se pueden aplicar 7 actualizaciones de forma inmediata.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

Active ESM Apps para recibir futuras actualizaciones de seguridad adicionales.
Vea https://ubuntu.com/esm o ejecute "sudo pro status"

Last login: Sun Jun  8 14:15:40 2025 from 192.168.1.7
ismaelvelazquez@ismaelvelazquez-VirtualBox: $ sudo tail -f /var/log/
lib/ local/ lock/ log/
ismaelvelazquez@ismaelvelazquez-VirtualBox: $ sudo tail -f /var/log/squid/access.log
[sudo] contraseña para ismaelvelazquez:
Lo siento, pruebe otra vez.
[sudo] contraseña para ismaelvelazquez:
1749536055.148 82 192.168.1.7 TCP_MISS/200 1042 POST http://o.pki.goog/we2 - HIER_DIRECT/192.178.56.163 application/ocsp-response
1749536055.825 119 192.168.1.7 TCP_MISS/200 1042 POST http://o.pki.goog/we2 - HIER_DIRECT/192.178.56.163 application/ocsp-response
1749536078.972 23458 192.168.1.7 TCP_TUNNEL/200 7093 CONNECT play.google.com:443 - HIER_DIRECT/192.178.52.206 -
1749536078.972 23594 192.168.1.7 TCP_TUNNEL/200 9676 CONNECT ogads-pa.clients6.google.com:443 - HIER_DIRECT/192.178.52.170 -
1749536078.972 25624 192.168.1.7 TCP_TUNNEL/200 5618 CONNECT csp.withgoogle.com:443 - HIER_DIRECT/192.178.56.209 -
1749536078.972 24165 192.168.1.7 TCP_TUNNEL/200 9491 CONNECT ogads-pa.clients6.google.com:443 - HIER_DIRECT/192.178.52.170 -
1749536078.972 26003 192.168.1.7 TCP_TUNNEL/200 1571 CONNECT incoming.telemetry.mozilla.org:443 - HIER_DIRECT/34.120.208.123 -
1749536078.972 26974 192.168.1.7 TCP_TUNNEL/200 138076 CONNECT www.google.com:443 - HIER_DIRECT/192.178.56.36 -
1749536078.972 27548 192.168.1.7 TCP_TUNNEL/200 6250 CONNECT encrypted-tbn0.gstatic.com:443 - HIER_DIRECT/172.217.4.174 -
1749536078.972 29436 192.168.1.7 TCP_TUNNEL/200 19088 CONNECT www.google.com:443 - HIER_DIRECT/192.178.56.36 -

```

- Tipos de archivos importantes: son acces.logs, cache.log

Siendo el primero respuestas de las peticiones de clientes. Y el segundo son los mensajes de error de configuración. Access.log muestra las solicitudes http de los clientes, como que sitio visitaron, fecha y estado. Siendo muy útil para el análisis de tráfico y auditoría. Cache.log Registra mensajes de error del sistema Squid, advertencias o problemas de configuración, es clave cuando algo falla en el proxy

## 9. BLOQUEO DE DOMINIOS

Para la sección de bloqueo de dominios, se implementara de dos maneras: la primera con argumentos directos en Acl y la segunda es usando un archivo de texto externo

- Argumentos directos: acl filtro\_rrss dstdomain .facebook.com .instagram.com

La palabra clave acl permite crear una regla de acceso, seguido de filtro\_rrss el cual indica el nombre personalizado de la acl seguido de dstdomain, el cual indica que se va a filtrar por dominio de destino (sitios web a los que el cliente intenta acceder). Los argumentos siguientes, indican los dominios que se van a bloquear, el punto inicial indica que también aplica a subdominios, como www.facebook.com o m.facebook.com.

- Detener acceso: http\_access deny filtro\_rrss

La primera parte indica que se deniega el acceso y filtro\_rrss se refiere al nombre de la ACL definida anteriormente. Esto bloquea el acceso a los sitios listados.

```

GNU nano 7.2                                     /etc/squid/conf.d/myrules.conf
#Crear ACL para nuestra red local
acl miredlocal src 192.168.1.0/24

#Crear ACL con webs de rss con argumentos
acl filtro_rss dstdomain .facebook.com .instagram.com

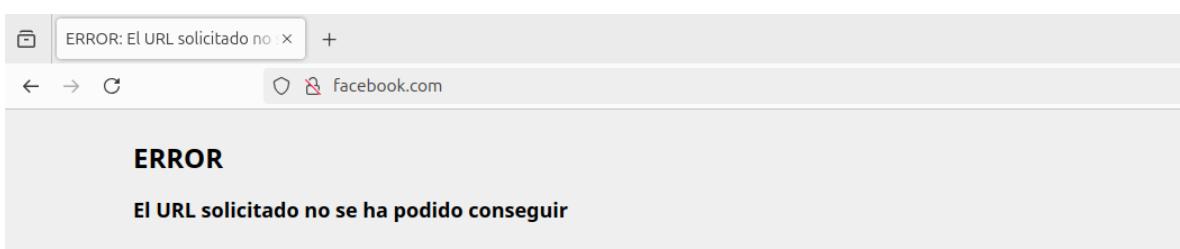
#Denegar acceso a acl a elementos acl
http_access deny filtro_rss

#Permitir navegación Web para dicha ACL
http_access allow miredlocal

[ 12 líneas escritas ]
^C Ayuda      ^O Guardar     ^W Buscar      ^K Cortar      ^T Ejecutar    ^C Ubicación   M-U Deshacer   M-A Poner marca M-] A llave
^X Salir      ^R Leer fich.  ^\ Reemplazar  ^U Pegar       ^J Justificar  ^/ Ir a linea   M-E Rehacer    M-G Copiar     ^Q Buscar atrás
ismaelvelazquez@ismaelvelazquez-VirtualBox:~$ sudo nano /etc/squid/conf.d/myrules.conf
ismaelvelazquez@ismaelvelazquez-VirtualBox:~$ sudo squid -k reconfigure
2025/06/12 00:32:00| Processing Configuration File: /etc/squid/squid.conf (depth 0)
2025/06/12 00:32:00| Processing Configuration File: /etc/squid/conf.d/debian.conf (depth 1)
2025/06/12 00:32:00| Processing Configuration File: /etc/squid/conf.d/myrules.conf (depth 1)
2025/06/12 00:32:00| Set Current Directory to /var/spool/squid
ismaelvelazquez@ismaelvelazquez-VirtualBox:~$ sudo nano /etc/squid/conf.d/myrules.conf
ismaelvelazquez@ismaelvelazquez-VirtualBox:~$ curl -x http://192.168.1.7:3128 -I http://www.google.com
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-4EAFrAmRxpmjxDIxMHeeQ' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http://report-uri https://csp.withgoogle.com/csp/gws/other-hp
P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info."
Date: Thu, 12 Jun 2025 06:33:28 GMT
Server: gws
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN
Expires: Thu, 12 Jun 2025 06:33:28 GMT
Cache-Control: private
Set-Cookie: AEC=AVh_V2gdIxvhXbpfxjT8z4y1ZMX_jnfM8unVzqZZdDjBdrjfKldzha-T0; expires=Tue, 09-Dec-2025 06:33:28 GMT; path=/; domain=.google.com; Secure; HttpOnly; SameSite=lax
Set-Cookie: NID=524-PMN4gflKLcp8xrIWdTBRxF52grjxWzyTgdGoyUjIwEDPSNYe03Hu6WI6tpb044ucH4MGLiHxohAXFziIJVECakPuQQzH5nwdsCEnbgiuvmthU6G5l5x4o2mJl-G2vYdtcS7my_050w0ZZ_ZtIJKH8twpGI0IVGj9nfrxioQKOCTyvxh4hdn9eqy1DAT2EDoNzl89F5ew; expires=Fri, 12-Dec-2025 06:33:28 GMT; path=/; domain=.google.com; HttpOnly
Cache-Status: ismaelvelazquez-VirtualBox; detail=mismatch
Via: 1.1 ismaelvelazquez-VirtualBox (squid/6.10)
Connection: keep-alive

ismaelvelazquez@ismaelvelazquez-VirtualBox:~$ curl -x http://192.168.1.7:3128 -I http://www.facebook.com
HTTP/1.1 403 Forbidden
Server: squid/6.10
Mime-Version: 1.0
Date: Thu, 12 Jun 2025 06:33:46 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 3542
X-Squid-Error: ERR_ACCESS_DENIED 0
Vary: Accept-Language
Content-Language: en
Cache-Status: ismaelvelazquez-VirtualBox
Via: 1.1 ismaelvelazquez-VirtualBox (squid/6.10)
Connection: keep-alive

```



Se encontró el siguiente error al intentar recuperar la dirección URL: <http://facebook.com/>

#### Acceso Denegado

La configuración de control de acceso evita que su solicitud sea permitida en este momento. Por favor, póngase en contacto con su proveedor de servicios si cree que esto es incorrecto.  
Su administrador del caché es [webmaster](#).

Para la segunda forma:

- Uso de fichero: acl filtro\_rrss dstdomain "/etc/squid/usuarios-denegados"

Se colocan los dominios en un archivo externo para este caso usuarios-denegados. Esto es de utilidad si hay muchos dominios a bloquear, ya que permite mantener limpio el archivo principal de configuración.

- Contenido del fichero: cat /etc/squid/usuarios-denegados

El comando muestra el contenido del archivo que contiene los dominios a bloquear.

Para esta sección se crea una regla de acceso basada en dominios, sebloquea el acceso a dichos dominoos y se muestra el contenido del archivo con los dominios bloqueados.

El orden de las listas de acceso influye en el resultado.

```
GNU nano 7.2                               /etc/squid/conf.d/myrules.conf
#Crear ACL para nuestra red local
acl miredlocal src 192.168.1.0/24

#Crear ACL con webs de rrss con argumentos
#acl filtro_rrss dstdomain .facebook.com .instagram.com

#Crear ACL con webs de RRSS con fichero
acl filtro_rrss dstdomain "/etc/squid/usuarios-denegados"

#Denegar acceso a acl a elementos acl
http_access deny filtro_rrss

#Permitir navegación Web para dicha ACL
http_access allow miredlocal
```

```

ismaelvelazquez@ismaelvelazquez-VirtualBox:~$ sudo nano /etc/squid/conf.d/myrules.conf
[sudo] contraseña para ismaelvelazquez:
ismaelvelazquez@ismaelvelazquez-VirtualBox:~$ cd /etc
ismaelvelazquez@ismaelvelazquez-VirtualBox:/etc$ cd squid
ismaelvelazquez@ismaelvelazquez-VirtualBox:/etc/squid$ sudo dominios-denegados
sudo: dominios-denegados: orden no encontrada
ismaelvelazquez@ismaelvelazquez-VirtualBox:/etc/squid$ sudo nano dominios-denegados
ismaelvelazquez@ismaelvelazquez-VirtualBox:/etc/squid$ sudo squid -k reconfigure
2025/06/12 14:41:55| Processing Configuration File: /etc/squid/squid.conf (depth 0)
2025/06/12 14:41:55| Processing Configuration File: /etc/squid/conf.d/debian.conf (depth 1)
2025/06/12 14:41:55| Processing Configuration File: /etc/squid/conf.d/myrules.conf (depth 1)
2025/06/12 14:41:55| Set Current Directory to /var/spool/squid
ismaelvelazquez@ismaelvelazquez-VirtualBox:/etc/squid$ sudo nano dominios-denegados
ismaelvelazquez@ismaelvelazquez-VirtualBox:/etc/squid$ sudo squid -k reconfigure
2025/06/12 14:43:36| Processing Configuration File: /etc/squid/squid.conf (depth 0)
2025/06/12 14:43:36| Processing Configuration File: /etc/squid/conf.d/debian.conf (depth 1)
2025/06/12 14:43:36| Processing Configuration File: /etc/squid/conf.d/myrules.conf (depth 1)
2025/06/12 14:43:36| Set Current Directory to /var/spool/squid
ismaelvelazquez@ismaelvelazquez-VirtualBox:/etc/squid$ curl -x http://192.168.1.7:3128 -I http://www.facebook.com

HTTP/1.1 403 Forbidden
Server: squid/6.10
Mime-Version: 1.0
Date: Thu, 12 Jun 2025 20:43:46 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 3542
X-Squid-Error: ERR_ACCESS_DENIED 0
Vary: Accept-Language
Content-Language: en
Cache-Status: ismaelvelazquez-VirtualBox

```

ⓘ https://m.facebook.com/reel/724560806718532/?referral\_source=native\_in\_feed\_unit

## El servidor proxy está rechazando las conexiones

Ha ocurrido un error al conectar con m.facebook.com.

- Compruebe la configuración de proxy para asegurarse de que es correcta.
- Contácte con su administrador de red para asegurarse de que el servidor proxy está funcionando.

[Reintentar](#)

## 10. ORDEN Y FUNCIONAMIENTO DE LAS ACL

Hay una serie de listas de acceso diferentes:

- **http\_access**: Permite que los clientes HTTP (navegadores) accedan al puerto HTTP. Este es el Lista de control de acceso principal.
- **http\_reply\_access**: Permite que los clientes HTTP (navegadores) reciban la respuesta a su pedir. Esto restringe aún más los permisos otorgados por **http\_access**, y está diseñado

principalmente para usarse junto con rep\_mime\_type ACL para bloquear Diferentes tipos de contenido.

- **icp\_access:** Permite que las cachés vecinas consulten su caché con ICP.
- **miss\_access:** Permite que ciertos clientes reenvíen errores de caché a través de su caché. Esto restringe aún más los permisos otorgados por http\_access, y está destinado principalmente a ser utilizado para reforzar las relaciones entre hermanos Al denegar que los hermanos reenvíen errores de caché a través de su caché.
- **caché:** Define respuestas que no se deben almacenar en caché.
- **url\_rewrite\_access:** Controla qué solicitudes se envían a través del grupo de redirecciónamiento.
- **ident\_lookup\_access:** Controla qué solicitudes necesitan una búsqueda de Ident.
- **always\_direct:** Controla qué solicitudes siempre se deben reenviar directamente a servidores de origen.
- **never\_direct:** Controla qué solicitudes nunca deben reenviarse directamente al origen Servidores.
- **snmp\_access:** Controla el acceso del cliente SNMP a la memoria caché.
- **broken\_posts:** Define las solicitudes para las que squid anexa un CRLF adicional después de POST cuerpos de mensaje según lo requieran algunos servidores de origen rotos.
- **cache\_peer\_access:** Controla qué solicitudes se pueden reenviar a un vecino determinado (cache\_peer).
- **htcp\_access:** Controla qué equipos remotos pueden realizar solicitudes HTCP.
- **htcp\_clr\_access:** Controla qué equipos remotos pueden realizar solicitudes HTCP CLR.
- **request\_header\_access:** Controla qué encabezados de solicitud se eliminan cuando se infringe HTTP protocolo.
- **reply\_header\_access:** Controla qué encabezados de respuesta se eliminan de la entrega al cliente al violar el protocolo HTTP.
- **delay\_access:** Controla qué solicitudes se manejan con qué retraso piscina
- **icap\_access:** (reemplazado por adaptation\_access en Squid-3.1) Qué solicitudes se pueden enviar a un servidor ICAP en particular.
- **adaptation\_access:** Qué solicitudes se pueden enviar a un filtro ICAP o eCAP en particular servicio.
- **log\_access:** Controla qué solicitudes se registran. Esto es global y anula Listas de acceso a archivos específicas anexadas a las directivas access\_log.

Las listas de acceso se comprueban en orden. La búsqueda termina cuando una regla coincide. Existe una regla por defecto http\_access deny all si no encuentra ninguna coincidencia, se niega el acceso por defecto. Es una medida de seguridad, nada pasa a menos que el usuario lo permita. En el manejo de configuraciones de squid esta presente la lógica de evaluación: que implica que todos los elementos de una entrada ACL son OR y todos los elementos de una regla utilizan AND.

Si cualquier condición de ACL se cumple, la ACL se considera verdadera. Todas las involucradas en la regla deben cumplirse para que se permita o se niegue el acceso.

http\_access allow|deny acl AND acl AND ...

OR

```
http_access allow|deny acl AND acl AND ...
```

OR

Se pueden encadenar varias reglas con allow o deny y cada una puede tener multiples condiciones. Dentro de una misma línea: los ACL's se relacionan con un AND. Por otro lado se evalúan como alternativas como si fuera un or implícito entre reglas

## 11. BLOQUEO MEDIANTE EXPRESIONES REGULARES

Una expresión regular se define como una secuencia de caracteres que define un patrón de búsqueda en una cadena de texto. Dicho esto, implementaremos este tipo de conceptos en nuestras próximas configuraciones

- Especificación: sudo nano block-exp

Permite crear un archivo con permisos de superusuario usando el editor nano, dentro de, se escribirán las palabras clave o expresiones regulares que se desee bloquear.

- Contenido de larchivo: torrent , crack

Se indica que se bloquearán todas las URLs que contengan las palabras torrent o crack esto es util para bloquear sitios relacionados con descargas ilegales o software pirata.

- ACL con expresiones regulares: acl block-exp url\_regex "/etc/squid/block-exp"

Establecer una ACL de nombre block-exp del tipo url\_regex, lo que indica que se basa en expresiones regulares además de añadir la fuente, que contiene las palabras clave.

```
GNU nano 7.2 /etc/squid/conf.d/myrules.conf
#Crear ACL para nuestra red local
acl miredlocal src 192.168.1.0/24

#Crear ACL con webs de rrss con argumentos
#acl filtro_rrss dstdomain .facebook.com .instagram.com
#Crear ACL con webs de RRSS con fichero
acl filtro_rrss dstdomain "/etc/squid/ dominios-denegados"

#Acl con expresiones regulares
acl block_exp url_regex "/etc/squid/block-exp

http_access deny block_exp

#Denegar acceso a acl a elementos acl
http_access deny filtro_rrss

#Permitir navegación Web para dicha ACL
http_access allow miredlocal

[ 19 líneas leídas ]
^G Ayuda      ^O Guardar   ^W Buscar   ^K Cortar   ^T Ejecutar  ^C Ubicación
^X Salir      ^R Leer fich. ^\ Reemplazar ^U Pegar    ^J Justificar ^/ Ir a linea
```

- Denegando navegación: http\_access deny block-exp

Si una URL solicitada coincide con la ACL block-exp, se le niega el acceso. Cualquier página cuya URL contenga torrent o crack será bloqueada por Squid.



```
ismaelvelazquez@ismaelvelazquez-VirtualBox: ~
GNU nano 7.2          block-exp
torrent
crack
```

- Comprobando funcionamiento Curl: curl -x http://user:password192.168.1.41:3128 -I <http://www.crackstation.com/>

Se implementa para probar si el bloqueo está funcionando. Nuevamente curl, indica la herramienta de consola para hacer peticiones web, luego de eso se indica que se usara un proxy Squid, en este caso. Con usuario, contraseña, ip del servidor squid, puerto por defecto en -I solicita las cabeceras HTTP la url del final es el sitio de prueba al contener la palabra crack, debe ser bloqueado. Si todo esta bien configurado, el sitio será bloqueado por el proxy, y curl no mostrará cabeceras, en cambio habrá un mensaje de rechazo o timeout.

```
ismaelvelazquez@ismaelvelazquez-VirtualBox:/etc/squid$ sudo squid -k reconfigure
2025/06/16 01:42:39| Processing Configuration File: /etc/squid/squid.conf (depth 0)
2025/06/16 01:42:39| Processing Configuration File: /etc/squid/conf.d/debian.conf (depth 1)
2025/06/16 01:42:39| Processing Configuration File: /etc/squid/conf.d/myrules.conf (depth 1)
2025/06/16 01:42:39| Set Current Directory to /var/spool/squid
ismaelvelazquez@ismaelvelazquez-VirtualBox:/etc/squid$ curl -x http://192.168.1.7:3128 -I http://www.crackstation.com
HTTP/1.1 403 Forbidden
Server: squid/6.10
Mime-Version: 1.0
Date: Mon, 16 Jun 2025 07:42:46 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 3554
X-Squid-Error: ERR_ACCESS_DENIED 0
Vary: Accept-Language
Content-Language: en
Cache-Status: ismaelvelazquez-VirtualBox
Via: 1.1 ismaelvelazquez-VirtualBox (squid/6.10)
Connection: keep-alive

ismaelvelazquez@ismaelvelazquez-VirtualBox:/etc/squid$
```

## 12. BLOQUEO POR DÍAS Y HORARIOS

En pocas palabras es una restricción por horarios. Al denegarlo de esta manera permite hacer uso más racional del ancho de banda con el que se dispone. ACL time, en pocas palabras está basado en definir restricciones de acceso basadas en horario y días de la semana.

- Se describe por días y horario de trabajo: acl WORKING time MTWTF 08:30-17:30

Se crea el acl working, se indica el tipo de acl trabaja con días y horarios, representando con iniciales los días de la semana e indicando el horario permitido en este ejemplo, se describe el caso de que dicha ACL será válida solo en días laborales y horario laboral.

- Denegar navegación fuera del horario laboral: http\_access deny !WORKING

El símbolo de exclamación niega la condición. En este caso significa Denegar el acceso cuando No se cumpla la condición WORKING. Fuera del horario laboral y los días indicados la navegación se bloquea. El comando date, permite mostrar fecha y hora del sistema, útil para verificar si está uno dentro o fuera del horario establecido.

The terminal window shows the following command and its output:

```
ismaelvelazquez@ismaelvelazquez-VirtualBox:~$ sudo nano block-exp
ismaelvelazquez@ismaelvelazquez-VirtualBox:~$ sudo squid -k reconfigure
2025/06/16 14:43:53| Processing Configuration File: /etc/squid/squid.conf (depth 0)
2025/06/16 14:43:53| Processing Configuration File: /etc/squid/conf.d/debian.conf (depth 1)
2025/06/16 14:43:53| Processing Configuration File: /etc/squid/conf.d/myrules.conf (depth 1)
2025/06/16 14:43:53| Set Current Directory to /var/spool/squid
ismaelvelazquez@ismaelvelazquez-VirtualBox:~$ sudo nano /etc/squid/conf.d/myrules.conf
ismaelvelazquez@ismaelvelazquez-VirtualBox:~$ sudo squid -k reconfigure
2025/06/16 14:51:56| Processing Configuration File: /etc/squid/squid.conf (depth 0)
2025/06/16 14:51:56| Processing Configuration File: /etc/squid/conf.d/debian.conf (depth 1)
2025/06/16 14:51:56| Processing Configuration File: /etc/squid/conf.d/myrules.conf (depth 1)
2025/06/16 14:51:56| Set Current Directory to /var/spool/squid
ismaelvelazquez@ismaelvelazquez-VirtualBox:~$ curl -x http://192.168.1.7:3128 -I
HTTP/1.1 403 Forbidden
Server: squid/6.10
Date: Mon, 16 Jun 2025 20:53:43 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 3536
X-Squid-Error: ERR_ACCESS_DENIED
Vary: Accept-Language
Content-Language: en
Cache-Status: Ismaelvelazquez-VirtualBox
Via: 1.1 ismaelvelazquez-VirtualBox (squid/6.10)
Connection: keep-alive
```

The browser window shows an error message: "El servidor proxy está" (The proxy server is) and "Ha ocurrido un error al conectar con www.google.com". It includes troubleshooting steps: "Compruebe la configuración de proxy para ase" and "Contacte con su administrador de red para ase".

### 13. PERSONALIZACIÓN DEL MENSAJE DE ERROR

Este tipo de configuración permite orientar al usuario cuando este visualice el mensaje de error. Dentro de este archivo se podrá modificar el menaje de error que quiere que el usuario visualice.

- Identificación de archivos: ls /usr/share/squid/errors/

Indica la dirección de los directorios por idioma.

```
ismaelvelazquez@ismaelvelazquez-VirtualBox:~$ cat /usr/share/squid/errors/Spanish/ERR_ACCESS_DENIED
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<html><head>
<meta type="copyright" content="Copyright (C) 1996-2021 The Squid Software Foundation and contributors">
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>ERROR: El URL solicitado no se ha podido conseguir</title>
<style type="text/css"><!--
  body
  :lang(fa) { direction: rtl; font-size: 100%; font-family: Tahoma, Roya, sans-serif; float: right; }
  :lang(he) { direction: rtl; }
  --></style>
</head><body id="%c">
<div id="titles">
<h1>ERROR</h1>
<h2>El URL solicitado no se ha podido conseguir</h2>
</div>
<hr>
```

- Mensaje de error: sudo nano /usr/share/squid/errors/Spanish/ERR\_BLOCKED\_RRSS

Abre o crea un archivo nuevo de error personalizado para cuando se bloqueen las redes Sociales. El nombre de archivo puede ser cualquiera, pero debe seguir el formato y estar en el directorio correcto.

- Contenido del archivo: ERR\_BLOCKED\_RRSS

Este archivo esta escrito en HTML, que será interpretado por el navegador como una pagina de error:

```
<HTML>
<HEAD>
<TITLE>ERROR: Página Web Bloqueada</TITLE>
</HEAD>
<BODY>
<H1>Esta página Web ha sido bloqueada debido a la política de la empresa</H1>
<P>No se permite el acceso a las Redes Sociales</P>
<P>Para más información contactar con nosotros:</P>
<UL>
<LI>Phone: 555-12435 (ext 44)</LI>
<LI>Email: helpdesk@chevere.com</LI>
</UL>
</BODY>
</HTML>
```

```
ismaelvelazquez@ismaelvelazquez-VirtualBox: $ cat /usr/share/squid/errors/Spanish/ERR_BLOCKED_RRSS~
<HTML>
<HEAD>
<TITLE>ERROR: Página Web Bloqueada</TITLE>
</HEAD>
<BODY>
<H1>Esta página Web ha sido bloqueada debido a la política de la empresa</H1>
<P>No se permite el acceso a las Redes Sociales</P>
<P>Para más información contactar con nosotros:</P>
<UL>
<LI>Phone: 11111 (ext 44)</LI>
<LI>Email: helpdesk@chevere.com</LI>
</UL>
</BODY>
</HTML>
```

- Como usarlo: deny\_info ERR\_BLOCKED\_RRSS filtro\_rrss

Se debe vincular este archivo a una regla deny\_inf. Esto le indica a Squid si se aplica la denegación filtro\_rrss, se debe mostrar la página ERR\_BLOCKED\_RRSS

- Definir el directorio de mensajes de error: error\_directory  
/usr/share/squid/errors/Spanish
- Aplicar un mensaje a un elemento ACL: deny\_info ERR\_BLOCKED\_RRSS filtro\_rrss

Si se activa la ACL llamada filtro\_rrss (por ejemplo, al intentar visitar redes sociales), Entonces Squid mostrará el mensaje HTML definido en ERR\_BLOCKED\_RRSS.

```
GNU nano 7.2                               /etc/squid/conf.d/myrules.conf
#Fichero de configuracion
error_directory /usr/share/squid/errors/Spanish

#Crear ACL para nuestra red local
acl miredlocal src 192.168.1.0/24

#Crear ACL con webs de rrss con argumentos
#acl filtro_rrss dstdomain .facebook.com .instagram.com
#Crear ACL con webs de RRSS con fichero
acl filtro_rrss dstdomain "/etc/squid/dominios-denegados"

#Acl con expresiones regulares a prohibir
acl block-exp url_regex "/etc/squid/block-exp"

#Crear ACL por fecha y hora de trabajo
#acl WORKING time MTWTF 08:30-17:30

#denegar navegacion por horarios
#http_access deny !WORKING

#denegar navegacion al elemento acl
http_access deny block-exp
```

```
GNU nano 7.2                               /etc/squid/conf.d/myrules.conf
acl filtro_rrss dstdomain "/etc/squid/dominios-denegados"

#Acl con expresiones regulares a prohibir
acl block-exp url_regex "/etc/squid/block-exp"

#Crear ACL por fecha y hora de trabajo
#acl WORKING time MTWTF 08:30-17:30

#denegar navegacion por horarios
#http_access deny !WORKING

#denegar navegacion al elemento acl
http_access deny block-exp

#Denegar acceso a acl a elementos acl
http_access deny filtro_rrss

#Permitir navegación Web para dicha ACL
http_access allow miredlocal

#Aplicar mensaje a un elemento ACL
deny_info ERR_BLOCKED_RRSS filtro_rrss
```

- Comprobar con curl: curl -x http:// 192.168.1.7:3128 -I <http://www.google.com/>  
Este comando debe funcionar sin error si Google no está bloqueado.

```

ismaelvelazquez@ismaelvelazquez-VirtualBox:~$ curl -x http://192.168.1.7:3128 -I http://www.facebook.com
HTTP/1.1 403 Forbidden
Server: squid/6.10
Mime-Version: 1.0
Date: Mon, 16 Jun 2025 22:07:23 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 49
X-Squid-Error: ERR_BLOCKED_RRSS 0
Cache-Status: ismaelvelazquez-VirtualBox
Via: 1.1 ismaelvelazquez-VirtualBox (squid/6.10)
Connection: keep-alive

ismaelvelazquez@ismaelvelazquez-VirtualBox:~$ curl -x http://192.168.1.7:3128 -I http://www.crackstation.com
HTTP/1.1 403 Forbidden
Server: squid/6.10
Mime-Version: 1.0
Date: Mon, 16 Jun 2025 22:07:40 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 3610
X-Squid-Error: ERR_ACCESS_DENIED 0
Cache-Status: ismaelvelazquez-VirtualBox
Via: 1.1 ismaelvelazquez-VirtualBox (squid/6.10)
Connection: keep-alive

```

#### 14. AUTENTICACIÓN DE USUARIOS

La autenticación de usuarios en Squid consta de un proceso para ver quien puede acceder a internet a través del servidor proxy.

- Herramientas de utilidades: sudo apt-get install apache2-utils

Instala un conjunto de utilidades que incluye htpasswd, herramienta necesaria para crear archivos con usuarios y contraseñas cifradas.

```

0 actualizados, 3 nuevos se instalarán, 0 para eliminar y 11 no actualizados.
Se necesita descargar 297 kB de archivos.
Se utilizarán 907 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] S
Des:1 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 libapr1t64 amd64 1.7.2-3.1ubuntu0.1 [108 kB]
Des:2 http://archive.ubuntu.com/ubuntu noble/main amd64 libaprutil1t64 amd64 1.6.3-1.1ubuntu7 [91,9 kB]
Des:3 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 apache2-utils amd64 2.4.58-1ubuntu8.6 [97,2 kB]
Descargados 297 kB en 2s (141 kB/s)
Seleccionando el paquete libapr1t64:amd64 previamente no seleccionado.
(Leyendo la base de datos ... 176225 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../libapr1t64_1.7.2-3.1ubuntu0.1_amd64.deb ...
Desempaquetando libapr1t64:amd64 (1.7.2-3.1ubuntu0.1) ...
Seleccionando el paquete libaprutil1t64:amd64 previamente no seleccionado.
Preparando para desempaquetar .../libaprutil1t64_1.6.3-1.1ubuntu7_amd64.deb ...
Desempaquetando libaprutil1t64:amd64 (1.6.3-1.1ubuntu7) ...
Seleccionando el paquete apache2-utils previamente no seleccionado.
Preparando para desempaquetar .../apache2-utils_2.4.58-1ubuntu8.6_amd64.deb ...
Desempaquetando apache2-utils (2.4.58-1ubuntu8.6) ...
Configurando libapr1t64:amd64 (1.7.2-3.1ubuntu0.1) ...
Configurando libaprutil1t64:amd64 (1.6.3-1.1ubuntu7) ...
Configurando apache2-utils (2.4.58-1ubuntu8.6) ...
Procesando disparadores para man-db (2.12.0-4build2) ...
Procesando disparadores para libc-bin (2.39-0ubuntu8.4) ...

```

- Fichero de usuario y contraseñal: sudo htpasswd -c /etc/squid/squid\_password hugo

-c crea el archivo **squid\_password** la primera vez. No se debe usar cuando se agregan mas usuarios, El sistema pedirá el nombre para ese usuario.

- Más usuarios: sudo htpasswd /etc/squid/squid\_password mart

Se añade este usuario al archivo ya creado. No se usa -c pues no se desea sobrescribir el archivo.

- Comprobar el contenido de fichero: cat squid\_password

Muestra el contenido cifrado del archivo. No revela la contraseña, sin embargo puedes ver usuarios registrados.

```
ismaelvelazquez@ismaelvelazquez-VirtualBox:/etc/squid$ ls /usr/lib/squid
basic_db_auth      basic_smb_auth.sh          ext_time_quota_acl      ntlm_smb_lm_auth
basic_fake_auth    cert_tool                  ext_unix_group_acl    pinger
basic_getpwnam_auth digest_file_auth        ext_wbinfo_group_acl  security_fake_certverify
basic_ldap_auth    digest_ldap_auth         helper-mux             storeid_file_rewrite
basic_ncsa_auth    diskd                     log_db_daemon         unlinkd
basic_pam_auth     ext_file_userip_acl       log_file_daemon       url_fake_rewrite
basic_pop3_auth    ext_kerberos_ldap_group_acl negotiate_kerberos_auth   url_fake_rewrite.sh
basic_radius_auth  ext_ldap_group_acl       negotiate_kerberos_auth_test
basic_sasl_auth    ext_session_acl          negotiate_wrapper_auth
basic_smb_auth     ext_sql_session_acl      ntlm_fake_auth
ismaelvelazquez@ismaelvelazquez-VirtualBox:/etc/squid$
```

- Archivo ejecutable: sudo find / -name basic\_ncsa\_auth | grep basic\_ncsa\_auth

Busca el ejecutable necesario para que Squid pueda autenticar a los usuarios con el archivo squid\_password. Basic\_ncsa\_auth suele estar en la ruta de squid ya sea lib o lib6.

- Probar usuarios: /usr/lib/squid/basic\_ncsa\_auth /etc/squid/squid\_password

Ejecutamos manualmente el programa de autenticación para verificar si los usuarios y contraseñas están funcionando correctamente. Ejemplo: hugo 1234-> O,K si es correcto ERRO si es incorrecto.

- Ubicación del programa autenticación y archivo: auth\_param basic program /usr/lib/squid/basic\_ncsa\_auth /etc/squid/squid\_password

Se usa el programa basic\_ncsa\_auth que autentica contra un archivo de contraseñas. Se le pasa el archivo /etc/squid/squid\_password que contiene los usuarios y contraseñas.

- Mensaje de muestra como solicitud de autenticación: auth\_param basic realm Autenticación de Usuarios de Squid

Para este comando el texto aparece en la ventana del navegador cuando pide usuario y contraseña. Indica al usuario por qué se solicita autenticarse

- Login:: auth\_param basic children 5

Procesos en paralelo de autenticación

- Tiempo: auth\_param basic credentialsttl 2 hours

Credenciales del usuario se guardarán durante 2 horas para este caso. Terminado ese lapso de tiempo, el usuario deberá volver a autenticarse.

```

GNU nano 7.2                                     squid.conf *
#Ubicación del programa autenticación y archivo
auth_param basic program /usr/lib/squid/basic_ncsa_auth /etc/squid/squid_password
#Mensaje de muestra
auth_param basic realm Autenticación de Usuarios de Squid
#Login
auth_param basic children 5
#Procesos en paralelo de autenticación
auth_param basic credentialsttl 2 hours

```

Hay una sección y es la configuración de reglas:

- ACL de usuarios autenticados: acl usuarios proxy\_auth REQUIRED

Proxy\_auth REQUIRED indica que el acceso solo será permitido si el usuario se ha autenticado correctamente.

- Acceso HTTP: http\_access allow usuarios

Solo los usuarios autenticados definidos en la ACL tendrán permitido el acceso a la red a través del proxy.

```

ismaelvelazquez@ismaelvelazquez-VirtualBox:/etc/squid$ sudo squid -k reconfigure
2025/06/16 21:25:19| Processing Configuration File: /etc/squid/squid.conf (depth 0)
2025/06/16 21:25:19| Processing Configuration File: /etc/squid/conf.d/debian.conf (depth 1)
2025/06/16 21:25:19| Processing Configuration File: /etc/squid/conf.d/myrules.conf (depth 1)
2025/06/16 21:25:20| Set Current Directory to /var/spool/squid
ismaelvelazquez@ismaelvelazquez-VirtualBox:/etc/squid$ curl -x http://192.168.1.7:3128 -I http://www.google.com
HTTP/1.1 407 Proxy Authentication Required
Server: squid/6.10
Mime-Version: 1.0
Date: Tue, 17 Jun 2025 03:26:25 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 3552
X-Squid-Error: ERR_CACHE_ACCESS_DENIED 0
Vary: Accept-Language
Content-Language: en
Proxy-Authenticate: Basic realm="Autenticación de Usuarios de Squid"
Cache-Status: ismaelvelazquez-VirtualBox
Via: 1.1 ismaelvelazquez-VirtualBox (squid/6.10)
Connection: keep-alive

```

### Ejemplo con autenticación

En esta configuración podemos controlar el proxy Squid mediante autenticación básica, gestionando quien puede navegar y por cuanto tiempo se mantiene las sesiones activas

```
ismaelvelazquez@ismaelvelazquez-VirtualBox:~$ curl -x http://lily:1234@192.168.1.7:3128 -I http://www.google.com
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-zV00x6lmjJPlnykscJndqA' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http;;report-uri https://csp.withgoogle.com/csp/gws/other-hp
P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info."
Date: Tue, 17 Jun 2025 05:48:17 GMT
Server: gws
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN
Expires: Tue, 17 Jun 2025 05:48:17 GMT
Cache-Control: private
Set-Cookie: AEC=AVh_V2gBjq0jceBAKdFtJMayAWXJADW2yKhCryT0ZiiYfK1JnCtG_t89RFU; expires=Sun, 14-Dec-2025 05:48:17 GMT; path=/; domain=.google.com; Secure; HttpOnly; SameSite=lax
Set-Cookie: NID=524=bkbeZC9FB0B2dmWuJDPv7H70FdNbbL7UgspQckp2AKSA7ifiEArDAsrTTGxvJPVFAxPxGP8kxU2oa0uVtstuhz5YcJWv9Xkx3OMZYe19J52cFtg0B1BoHA7otKd-sbYVxlFnvtFpom1dK3vlpBPuXzTjgL-25D-4FHM_TfyKD7h1GprJr15RGjn0vnndrDuhDLsGsRbbQ; expires=Wed, 17-Dec-2025 05:48:17 GMT; path=/; domain=.google.com; HttpOnly
Cache-Status: ismaelvelazquez-VirtualBox;detail=mismatch
Via: 1.1 ismaelvelazquez-VirtualBox (squid/6.10)
Connection: keep-alive

ismaelvelazquez@ismaelvelazquez-VirtualBox:~$ curl -x http://lily:1234@192.168.1.7:3128 -I http://www.facebook.com
HTTP/1.1 403 Forbidden
Server: squid/6.10
Mime-Version: 1.0
Date: Tue, 17 Jun 2025 05:48:40 GMT
Content-Type: text/html;charset=utf-8
Content-Length: 3593
X-Squid-Error: ERR_ACCESS_DENIED 0
Vary: Accept-Language
Content-Language: en
Cache-Status: ismaelvelazquez-VirtualBox
Via: 1.1 ismaelvelazquez-VirtualBox (squid/6.10)
Connection: keep-alive
```

## 15. VERIFICACIÓN DEL FUNCIONAMIENTO DE LA CACHÉ

Un proxy cache se sitúa entre la máquina del usuario y otra red. Actúa como elemento de separación y como cache para acelerar el acceso a páginas web o restringir acceso a contenidos.

La zona cache es una parte de la memoria RAM que almacena una copia de los datos a los que se accederá con frecuencia. Esto reduce el tiempo de acceso ya que el acceso a la RAM es más rápido que el disco duro.

- Cliente de squid: sudo apt install squidclient

El comando instala la herramienta squidclient, que es una herramienta que permite comunicar con squid para obtener estadísticas, estado del servicio y otras funciones administrativas. Permite comprobar el estado del cache, validar el funcionamiento de Squid y obtener información útil para diagnóstico o monitoreo.

- estadísticas del proxy Squid: squidclient mgr:info

Conecta al servicio Squid y solicita información detallada del sistema mediante la interfaz de administración interna. Esto permite mostrar consultas de estadísticas como ejemplo tenemos el uso de cache, tiempo de actividad cantidad de peticiones servidas, estado de conexiones.

```

ismaelvelazquez@ismaelvelazquez-VirtualBox:~$ sudo apt install squidclient
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
  libllvm17t64 python3-netifaces
Utilice «sudo apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes NUEVOS:
  squidclient
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 47 no actualizados.
Se necesita descargar 50,9 kB de archivos.
Se utilizarán 175 kB de espacio de disco adicional después de esta operación.
Des: http://archive.ubuntu.com/ubuntu noble-updates/universe amd64 squidclient amd64 6.10-0ubuntu0.24.04.1 [50,9 kB]
Descargados 50,9 kB en 1s (97,8 kB/s)
Seleccionando el paquete squidclient previamente no seleccionado.
(Leyendo la base de datos ... 176275 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../squidclient_6.10-0ubuntu0.24.04.1_amd64.deb ...
Desempaquetando squidclient (6.10-0ubuntu0.24.04.1) ...
Configurando squidclient (6.10-0ubuntu0.24.04.1) ...
Procesando disparadores para man-db (2.12.0-4build2) ...
ismaelvelazquez@ismaelvelazquez-VirtualBox:~$ squidclient mgr:info
HTTP/1.1 200 OK
Server: squid/6.10
Mime-Version: 1.0
Date: Tue, 17 Jun 2025 05:57:10 GMT
Content-Type: text/plain; charset=utf-8
Expires: Tue, 17 Jun 2025 05:57:10 GMT
Last-Modified: Tue, 17 Jun 2025 05:57:10 GMT
Cache-Control: no-cache, no-store
Cache-Status: ismaelvelazquez-VirtualBox;detail=mismatch
Via: 1.1 ismaelvelazquez-VirtualBox (squid/6.10)
Connection: close

Squid Object Cache: Version 6.10
Build Info: Ubuntu linux
Service Name: squid
Start Time:   Tue, 17 Jun 2025 05:40:43 GMT
Current Time: Tue, 17 Jun 2025 05:57:10 GMT
Connection information for squid:
  Number of clients accessing cache:      2
  Number of HTTP requests received:       2
  Number of ICP messages received:        0
  Number of ICP messages sent:           0
  Number of queued ICP replies:          0
  Number of HTCP messages received:       0
  Number of HTCP messages sent:          0
  Request failure ratio:    0.00
  Average HTTP requests per minute since start:  0.1
  Average ICP messages per minute since start:  0.0
  Select loop called: 2122 times, 465.441 ms avg
Cache information for squid:
  Hits as % of all requests:      5min: 0.0%, 60min: 0.0%
  Hits as % of bytes sent:        5min: -0.0%, 60min: -0.0%
  Memory hits as % of hit requests: 5min: 0.0%, 60min: 0.0%
  Disk hits as % of hit requests: 5min: 0.0%, 60min: 0.0%
  Storage Swap size:             0 KB
  Storage Swap capacity:         0.0% used, 0.0% free
  Storage Mem size:              212 KB
  Storage Mem capacity:          0.1% used, 99.9% free
  Mean Object Size:              0.00 KB
  Requests given to unlinkd:     0
Median Service Times (seconds) 5 min 60 min:
  HTTP Requests (All): 0.00000 0.02742
  Cache Misses: 0.00000 0.00000
  Cache Hits: 0.00000 0.00000
  Near Hits: 0.00000 0.00000
  Not-Modified Replies: 0.00000 0.00000
  DNS Lookups: 0.00000 0.02683
  ICP Queries: 0.00000 0.00000
Resource usage for squid:

```

## 16. CONFIGURACIÓN DE LA CACHÉ

- Cache del disco: cache\_dir ufs /var/spool/squid 100 16 256

Define donde almacenara en disco los archivos en cache. Se define una cache en disco además de eso se indica el tipo de almacenamiento, (Unix File System) es el método indicado para guardar

archivos de cache en la estructura de carpetas. Es importante definir el tamaño máximo en megabytes(MB). 100 para este caso. Es importante además definir el número de carpetas de primer nivel que se crean dentro del directorio de cache, y asignar también el número de subcarpetas de segundo nivel dentro de cada carpeta de primer nivel. En general este comando permite hacer un mejor manejo de archivos y evitar que haya demasiados en un solo directorio lo que provoca ralentización de acceso y escritura.

- Cache de memoria: `cache_mem 512 MB`

Permite definir el tamaño del cache en memoria RAM. Para este caso se usa como referencia 512 de RSAM para almacenar objetos en cache. Esto permite responder mas rápido a solicitudes sin tener que ir al disco. En pocas palabras se le dice a Squid cuanto de espacio usar en disco y memoria. Como organizar los archivos de forma eficiente. Donde los datos cacheados para mejorar el rendimiento.

## 17. USO DE LISTAS PÚBLICAS DE BLOQUEO DE DOMINIOS

- Lista publica de dominios github: `wget -q -N https://raw.githubusercontent.com/maravento/blackweb/master/blackweb.tar.gz && cat blackweb.tar.gz* | tar xzf -`

El comando permite descargar archivos de dominio prohibido, como `blackweb.txt`, descomprimidos y listos para usarse

- ACL indicando la dirección del fichero: `acl blackweb dstdomain "/home/redesplus/blackweb.txt"`

Creamos una ACL denominada `blackweb`, la cual filtra por dominio de destino, la ruta indica el archivo que contiene los dominios que desean bloquear.

- Denegación de acceso: `http_access deny blackweb`

Bloquea todo acceso a los dominios que aparecen en la ACL `blackweb`. En pocas palabras se descarga una lista publica de sitios no deseados. La acl detecta el intento de acceso a esos dominios. Esto bloquearía el acceso a cualquier sitio listado allí.

```
ismaelvelazquez@ismaelvelazquez-VirtualBox:~$ curl -x http://192.168.1.7:3128 -I http://www.crackstation.com
HTTP/1.1 403 Forbidden
Server: squid/6.10
Mime-Version: 1.0
Date: Wed, 18 Jun 2025 00:38:31 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 3554
X-Squid-Error: ERR_ACCESS_DENIED 0
Vary: Accept-Language
Content-Language: en
Cache-Status: ismaelvelazquez-VirtualBox
Via: 1.1 ismaelvelazquez-VirtualBox (squid/6.10)
Connection: keep-alive
```

BlackWeb como se ha descrito anteriormente, es un proyecto que recolecta y unifica listas de bloqueo de dominio público, de sitios que incluyen pornografía, venta de drogas y malware spyware. Este tipo de herramientas solo es un mecanismo básico de control de acceso que permite a través de la misma elementos comunes como direcciones de correo, usuarios, contraseñas y demás, excepto los elementos mencionados en un párrafo anterior. A dichos elementos se les deniega el acceso.

#### CONCLUSIONES

- El uso de ACL permite un control granular de tráfico, en pocas palabras por medio de los ACL es posible bloquear o permitir acceso a sitios específicos según políticas corporativas, usuarios, grupos, horarios o tipos de contenido, fortaleciendo la seguridad y el cumplimiento.
- La autenticación de usuarios fortalece la seguridad y el control del acceso la autenticación con basic\_ncsa\_auth garantiza que solo los usuarios autorizados puedan usar el proxy, lo que permite auditorias más precisas y evita el uso no controlado de servicio.
- Es posible limitar y controlar el uso de sitios no deseados, bloqueando con el uso de listas públicas como blackweb, se reducen riesgos de productividad baja, fuga de datos y exposición a contenidos inapropiados o peligrosos.
- La verificación con herramientas como curl y squidclient permite validar el funcionamiento del proxy, permitiendo comprobar de forma práctica si las políticas y restricciones implementadas en Squid están funcionando como se espera.
- Un factor clave es la configuración de la cache como mejora de rendimiento de red. Al ajustar parámetros como cache\_dir y cache\_mem, se optimiza el uso del ancho de banda y se acelera el acceso a recursos ya visitados, lo que resulta en una experiencia de navegación más fluida para los usuarios.
- El uso de listas públicas de bloqueo facilita la administración de seguridad, integra fuentes externas confiables, como es nuestro caso blackweb, que ahorra tiempo al administrador y mantiene actualizadas las políticas de bloqueo frente a nuevos dominios peligrosos.
- La modularidad de Squid permite su adaptación a distintos entornos organizacionales, para pequeñas, medianas o grandes redes, permitiendo políticas personalizadas sin necesidad de herramientas costosas.