

# INSTALACIÓN DE PROXY EN LINUX CON SQUID

---



---

SEGURIDAD INFORMÁTICA  
JUAN CARLOS NAVIDAD GARCÍA

## 1. Instalación de Squid:

Instalaremos **Squid** con el siguiente comando:

```
jnav@jnav-vbox:~$ sudo apt-get install squid
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
libdbi-perl libcap3 squid-common squid-langpack
```

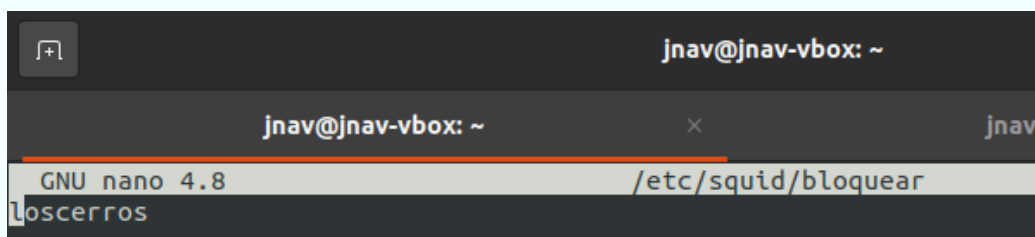
## 2. Creación de la lista negra en Squid:

Lo primero que haremos, será crear un archivo que contendrá la lista de **direcciones que nuestro Proxy va a denegar el acceso al cliente**. Para tenerlo más controlado, lo crearemos dentro del directorio **/etc/squid** y lo nombraremos como queramos.

Por ejemplo, yo lo he llamado **"bloquear"**:

```
jnav@jnav-vbox:~$ sudo nano /etc/squid/bloquear
[sudo] contraseña para jnav:
```

Con introducir simplemente el **nombre básico de la página** basta, no hace falta introducir el dominio completo, en mi caso, he bloqueado la página de **Los Cerros**:



### 3. Configuración de Squid:

Para configurar **Squid**, nos iremos a su **archivo de configuración**, el cual es **/etc/squid/squid.conf**.

Lo primero que haremos será asignar a nuestro **servidor Proxy** nuestra dirección **IP** con las líneas:

- **http\_access allow localnet**
- **http\_access src <ip>**

```
GNU nano 4.8 /etc/squid/squid.conf Modificado
#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
include /etc/squid/conf.d/*

# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
#http_access allow localnet
http_access allow all
http_access allow localnet
acl localnet src 192.168.103.55
# And finally deny all other access to this proxy
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

^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar Tex ^J Justificar ^C Posición
^X Salir ^R Leer fich. ^\ Reemplazar ^U Pegar ^T Ortografía ^_ Ir a línea
```

Posteriormente, volveremos a añadir nuestra dirección **IP** de la misma manera y debajo añadiremos la línea que permitirá a **Squid bloquear las páginas** que hemos especificado en el fichero de **lista negra** que hemos creado anteriormente, la línea sería:

- **acl <nombre de la lista negra> dstdomain "<directorio de la lista negra>"**

```
GNU nano 4.8 /etc/squid/squid.conf
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
acl CONNECT method CONNECT

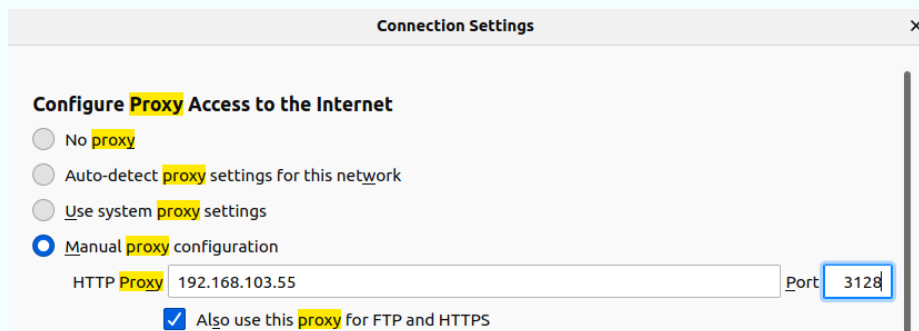
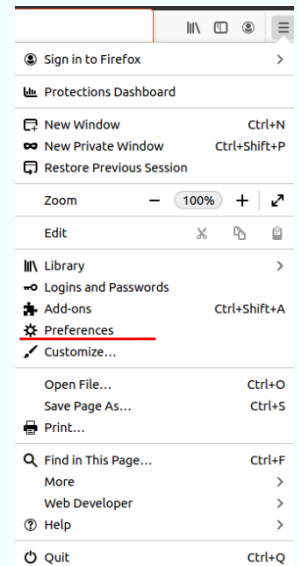
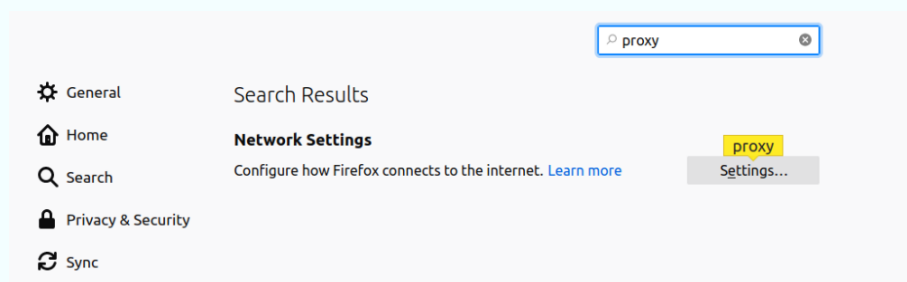
acl red local src 192.168.103.55
acl bloquear dstdomain "/etc/squid/bloquear"
```

## 4. Comprobación de funcionamiento:

Por último, comprobaremos si funciona o no, para eso nos iremos al **cliente** y añadiremos nuestro **servidor proxy** a la configuración de **red** o a la configuración del **navegador**.

En mi caso, la he añadido en la **configuración del navegador Firefox**:

Nos iremos a **Preferencias → Buscaremos Proxy → Ajustes → Configuración manual del proxy** → Añadimos la **IP** y el **puerto** por defecto de **Squid** que es el **3128**:



Si todo está configurado correctamente podríamos navegar por Internet como de normal, pero no podríamos acceder a la página que se encuentra en la **lista negra**, nos debería de salir un mensaje de que el **servidor proxy rechaza la conexión**:

