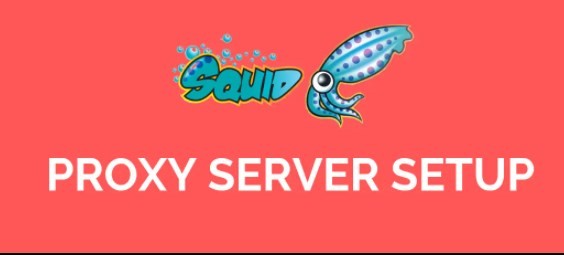
Cómo configurar su propio servidor proxy gratuito usando Squid Proxy



# Servidor proxy gratuito usando Squid Proxy

En algunas ocasiones deberemos configurar un servidor web proxy. Podremos hacerlos a través de uan API como webmin, pero en este caso debemos de usar **Squid**3.

El servidor proxy **Squid** se adapta mejor para la creación de un servidor proxy de reenvío o caché. Es un servidor proxy de reenvío de código abierto con muchas funcionalidades. Está siendo utilizado por muchas empresas como proxy de reenvío o caché.

Indice

1. Servidor proxy gratuito con **Squid** Proxy
2. Configuración de proxy de **Squid**
   1. Puerto proxy de **Squid**
   2. Proxy de conectividad a Internet
   3. Configurar la autenticación de **Squid** Proxy
   4. Bloqueo de sitios web mediante **Squid** Proxy
   5. Uso del proxy **Squid**
3. Conclusión

# Servidor proxy gratuito con Squid Proxy

En esta tarea se explicará el proceso paso a paso para configurar un servidor proxy gratuito utilizando **Squid** Proxy en el servidor Ubuntu más reciente.

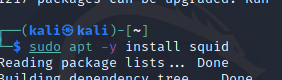
Siga los pasos que se indican a continuación para un servidor proxy que funcione.

**Paso 1**: inicie sesión en el servidor y actualice la lista de paquetes.

sudo apt update

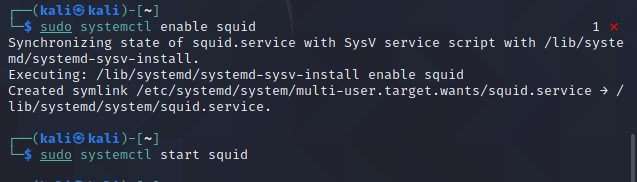
**Paso 2:** Instale el servidor **Squid** Proxy.

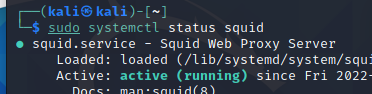
sudo apt -y install **Squid**



**Paso 3:** Inicie y habilite el servicio **Squid** para que se inicie en el arranque del sistema.

sudo systemctl start **Squid**

sudo systemctl enable **Squid**



**Paso 4:** Verifique el estado del servicio de **Squid**. Debería estar viendo el estado "activo".

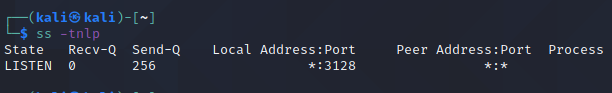
sudo systemctl state **Squid**

# Puerto proxy de Squid

Por defecto, **Squid** se ejecuta en el puerto 3128 Puedes comprobarlo usando el siguiente comando.

netstat –tnlp

ss –tnlp



Ahora tenemos un servidor proxy **Squid** en funcionamiento. El siguiente paso importante es configurar el proxy **Squid** según sus necesidades.

# Configuración de proxy de Squid

Si está configurando el proxy **Squid** para su entorno de producción, debe asegurarse de que todas las configuraciones del proxy estén establecidas según sus necesidades.

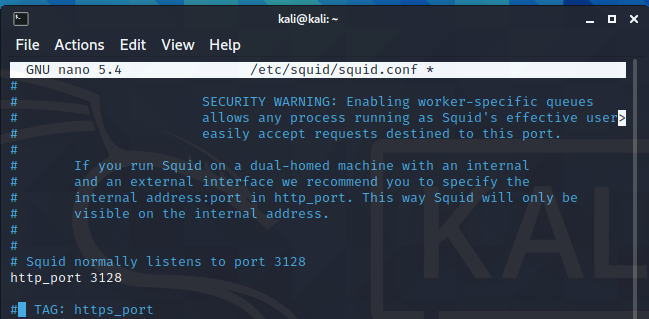
La configuración principal del proxy **Squid** está en */etc/squid/squid.conf*

# Puerto proxy de Squid

Por defecto, el proxy de **Squid** se ejecuta en el puerto 3128. Asegúrese de permitir 3128 en las reglas de su cortafuegos.

Además, puede cambiar el puerto 3128 predeterminado a un puerto personalizado editando la siguiente configuración en el archivo s*quid.conf.*

http\_puerto 3128

**

# Proxy de conectividad a Internet

El caso de uso principal para la mayoría de nosotros es conectarnos a Internet a través de un servidor proxy.

Si desea conectarse a Internet a través de su proxy, debe configurar las ACL (Lista de control de acceso) en su configuración de **Squid**.

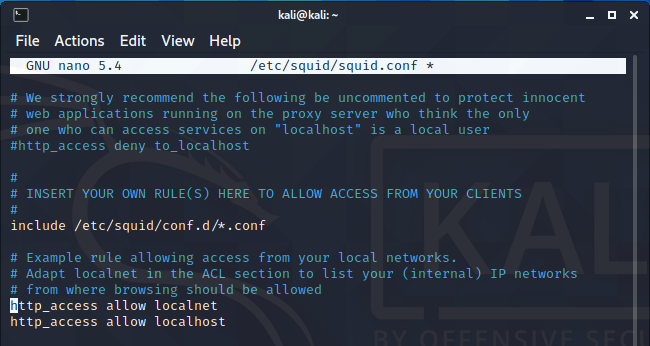
# Habilite las ACL de Squid para la conectividad a Internet

De forma predeterminada, se denegarán todas las conexiones entrantes al servidor proxy. Necesitamos habilitar algunas configuraciones para que el servidor **Squid** acepte conexiones de otros hosts.

Abra el archivo */etc/squid/squid.conf.*

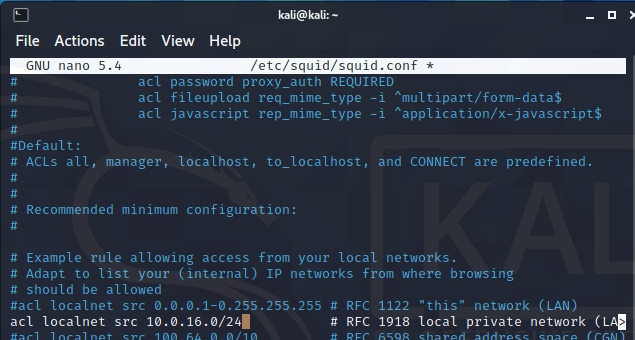
nano */etc/squid/squid.conf*

Busque la entrada http\_access allow localnet en el archivo. Por defecto, estará comentado. Descoméntalo.



El siguiente paso es agregar ACL al archivo de configuración de **Squid** /etc/**Squid**/**Squid**.conf. ACL para red local tiene el siguiente formato.

acl localnet src [fuente-ip-rango]



Puede incluir en la lista blanca los rangos de IP de origen de la siguiente manera:

1. IP única [49.205.220.161]

2. Un rango de IP [0.0.0.1-0.255.255.255]

3. Rango CIDR [10.0.0.0/28]

Según sus requisitos, puede agregar la red local acl. Por ejemplo, en nuestro caso de uso incluimos la dirección de mi equipo

acl localnet src 10.0.16.100

Si desea incluir en la lista blanca el rango CIDR de sus redes privadas, puede tener la ACL como la siguiente. Normalmente, este tipo de casos de uso se presenta cuando configura una red virtual para su organización.

acl localnet src 10.0.16.0/254

Nota: Puede agregar su ACL en el archivo de configuración debajo de las ACL predeterminadas. Si busca todas las ACL, encontrará la sección predeterminada de ACL. Si especifica un rango privado de CIDR, asegúrese de que el proxy esté en la misma red privada.



Aquí está la ACL que agregué a mi servidor **Squid**.

#Defecto:

# Las ACL all, manager, localhost y to\_localhost están predefinidas.

#

#

# Configuración mínima recomendada:

#

acl localnet src 49.205.45.67

# Regla de ejemplo que permite el acceso desde sus redes locales.

# Adáptese para enumerar sus redes IP (internas) desde donde navega

# Debería ser permitido

#acl localnet src 10.0.0.0/8 # RFC1918 posible red interna

#acl localnet src 172.16.0.0/12 # RFC1918 posible red interna

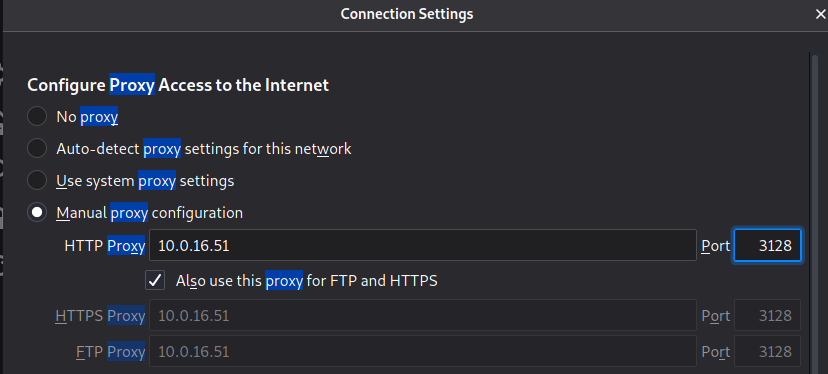
#acl localnet src 192.168.0.0/16 # RFC1918 posible red interna

#acl localnet src fc00::/7 # RFC 4193 rango de red privada local

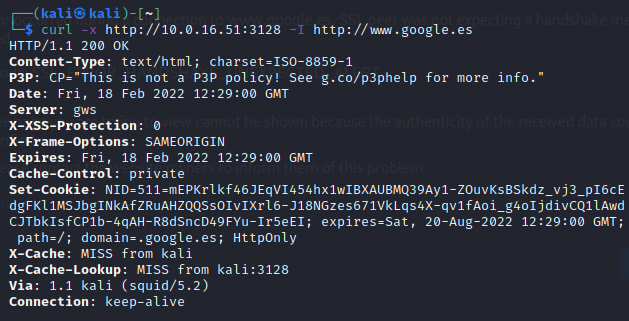
#acl localnet src fe80::/10 # RFC 4291 máquinas de enlace local (conectadas directamente)

# Probar la conectividad del proxy

Para probar la conectividad proxy para Internet desde su fuente de ACL especificada, puede usar la siguiente sintaxis de comando curl whi ch debería devolver un código de respuesta 200 OK.



curl -x http://[TU-PROXY-IP]:3128 -I [http://google.com](http://google.com/) A la salida le gustaría lo siguiente.



* ~ curl -x http://134.209.77.172:3128 -I [http://www.google.com](http://www.google.com/)

HTTP/1.1 200 OK

Date: Sun, 24 Mar 2019 07:21:26 GMT

Expires: -1

Cache-Control: private, max-age=0

Content-Type: text/html; charset=ISO-8859-1

P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info." Server: gws

X-XSS-Protection: 1; mode=block X-Frame-Options: SAMEORIGIN

Set-Cookie: 1P\_JAR=2019-03-24-07; expires=Tue, 23-Apr-2019 07:21:26 GMT; path=/; domain=.google.com

Set-Cookie: NID=164=QUlqgO1t2- LesVjVjqd0RqBXPUh3QMutuw31xovrIC4EXZOYF5KSpvmDuIORnkm2EvinnZRzqWwG6Lb hWR-lb11HpiHQZczfWPN2HuT9FZjaLO\_z0ku1qk0N- IWOv2W5l4XparkWr8kusyUPw3jBHGgtoB\_gECW4VqUiPvK5H98; expires=Mon, 23- Sep-2019 07:21:26 GMT; path=/; domain=.google.com; HttpOnly

Accept-Ranges: none Vary: Accept-Encoding

X-Cache: MISS from crunch-proxy

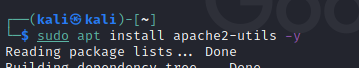
X-Cache-Lookup: MISS from crunch-proxy:3128 Via: 1.1 crunch-proxy (squid/3.5.27) Connection: keep-alive

# Configurar la autenticación de Squid Proxy

El método anterior permitiría el uso de proxy anónimo. Para evitar esto, puede configurar la autenticación de proxy utilizando un nombre de usuario y una contraseña.

**Paso 1:** Instale las utilidades de apache.

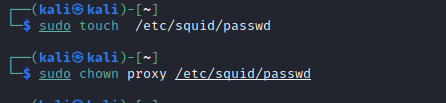
sudo apt install apache2-utils- y



**Paso 2:** Cree un archivo passwd y cambie la propiedad a un usuario proxy.

sudo touch /etc/squid/passwd

sudo chown proxy /etc/squid/passwd



**Paso 3:** Cree un usuario llamado proxy usando el siguiente comando. Le pedirá una contraseña. Proporcione una contraseña segura.

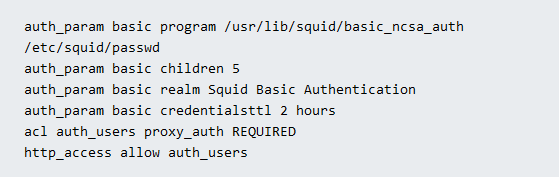
sudo htpasswd /etc/squid/passwd proxy

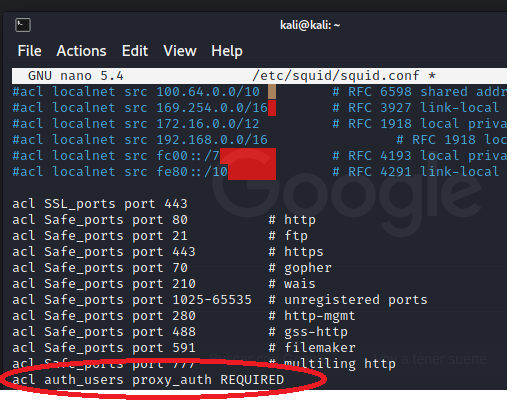


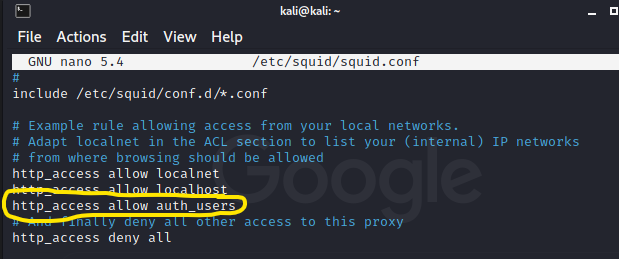
**Paso 4:** Abra el archivo *squid.conf.*

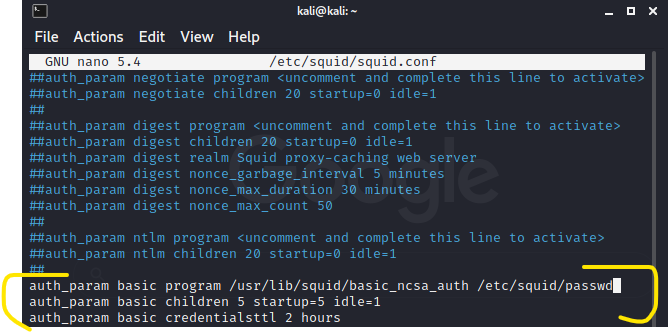
sudo nano /etc/squid/squid.conf

**Paso 5:** Agregue el siguiente contenido al archivo.









**Paso 6:** reinicie el servidor **Squid** para que se realicen los cambios.

sudo systemctl reiniciar squid

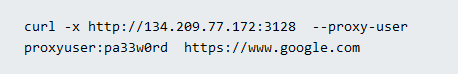
# Probar la autenticación de proxy de Squid

Pruebe la autenticación de proxy de **Squid** usando curl. Puede utilizar la siguiente sintaxis.



curl -x http://[IP-servidor-squid]:3128 --proxy-user proxy:[contraseña-proxy] https://[www.google.com](http://www.google.com/)

Por ejemplo,



curl -x http://10.0.16.100:3128 --proxy-user proxy:pa33w0rd https://[www.google.com](http://www.google.com/) Verá el siguiente error si los detalles de autenticación no se pasan correctamente.



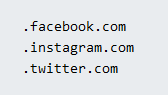
# Bloqueo de sitios web mediante Squid Proxy

Otro caso de uso clave de un proxy **Squid** es bloquear el acceso a ciertos sitios web. En esta sección, veremos los pasos para configurar una lista de bloqueo de sitios web.

**Paso 1:** Cree un archivo de lista de bloqueo llamado proxy-block-list.acl

sudo nano /etc/**squid**/proxy-block-list.acl

**Paso 2:** Agregue los sitios web que tiene que bloquear al archivo como se muestra a continuación.



.facebook.com

.instagram.com

.twitter.com

Nota: asegúrese de que no tiene ningún

por encima de la regla de la lista de bloqueo.

Tendrá prioridad y la lista de bloqueo no funcionará.

**Paso 3:** Abra el archivo de configuración de **Squid**.

sudo nano /etc/squid/squid.conf

**Paso 4:** agregue las siguientes líneas sobre las ACL que hemos agregado en los pasos anteriores.

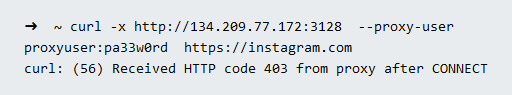
acl bad\_urls dstdomain "/etc/squid/proxy-block-list.acl" http\_access denegar bad\_urls

**Paso 5:** reinicie el servidor squid.

sudo systemctl restart squid

# Pruebe los sitios web bloqueados de Squid

Ahora, si intenta acceder a los sitios web que están en la lista de bloqueo, obtendrá un error 403 como se muestra a continuación.



* ~ curl -x http://10.0.16.100:3128 --proxy-user proxy:pa33w0rd https://instagram.com

Respuesta del proxy de sitio bloquedo:

curl: (56) Recibió el código HTTP 403 del proxy después de CONECTAR

# Uso del proxy Squid

Puede usar el proxy **Squid** de las siguientes formas:

* + Para la navegación web: Puede usar el punto final del proxy **Squid** como su proxy de navegador. Cada navegador tiene su propia configuración de proxy. Puede agregar la IP del proxy, el puerto y los detalles de autenticación si están habilitados.
  + Para aplicaciones: Si tiene aplicaciones que se ejecutan en una red privada y desea conectarse a Internet para llamadas específicas, puede usar el extremo del proxy para enrutar ese tráfico de Internet saliente.
  + Para bloqueo del acceso no deseado a sitios web: Las organizaciones usan un servidor proxy para limitar el acceso a ciertos sitios web no deseados.

# Conclusión

**Squid** proxy ofrece una variedad de soluciones como proxy de reenvío. Es el mejor software de servidor proxy gratuito. Su implementación depende de su arquitectura y diseño.

# Ejercicio: Configurar Squid como proxy no transparente con autenticación básica (NCSA).

Una star-up llamada Faiser tiene 3 personas trabajando, todos tienen ordenador, y todos ellos deben de estar conectados en las horas de trabajo.

Los tres empleados ( Director. operario e informático) tienen un ordenador disponible en su puesto de trabajo. Están preocupados y quiere limitar los lugares web visitables, pero no las revistas de cine con información necesaria para su trabajo.

Charles Pfizer, el dueño de la start-up te contrata para que demuestres como **Squid** proxy instalado y configurado en la red de la empresa puede realizar esa tarea con las siguientes condiciones:

1. Las direcciones IP de los 3 trabajadores son 10.0.3.16, 10.0.3.17, 10.0.3.18 serán de tipo A con su máscara 24.
2. No tienen permitida el acceso a las web <https://www.astrazeneca.es/>ni <https://www.modernatx.com/>, pero sí a las revistas de alto nivel científico: [http://www.nature.com/,](http://www.nature.com/) dos siglos de publicación de la revista nature la califican como la mejor revista científica del mundo. Es ciencia "pura y dura". Británica. Y <http://www.aaas.org/>la revista Science de la Academia Americana para el Avance de la Ciencia. Publica contenidos biomédicos (y de ciencia en general) que todavía no tienen aplicación clínica, pero de donde surgen los grandes avances de la medicina. Es una especie de versión americana de Nature.
3. Por otra parte, todos los usuarios tendrán su usuario y contraseña para navegar, y deberán configurar sus navegadores ( al menos tres navegadores diferentes) con el proxy que estará en la dirección previa a la de difusión de la subred que escojas. Los usuarios son: Charles Pfizer, como jefe, Albert Bourla, como operario y Charles F. Erhart, como informático.

Inventa los usuarios y contraseñas seguras para cada uno de ellos teniendo en cuenta sus nombre y demuestra que se puede conectar usando su usuario y contraseña.