Squid

Introducción

El término en ingles «Proxy» tiene un significado muy general y al mismo tiempo ambiguo, aunque invariablemente se considera un sinónimo del concepto de «Intermediario». Se suele traducir, en el sentido estricto, como delegado o apoderado (el que tiene el que poder sobre otro).

En informática, el término *Proxy* hace referencia a un programa o dispositivo que realiza una acción en representación de otro.

Definición de Proxy

Un Servidor Intermediario (Proxy) se define como una máquina que ofrece un servicio de red que consiste en permitir a los clientes realizar conexiones de red indirectas hacia otros servicios de red.

En su forma más pura, se trata de una máquina dual-homed, es decir, conectada a dos redes, pero que no tiene capacidad de enrutamiento.

El Proxy reserva un espacio de Disco de longitud variable, al que se denominará caché.

Funcionamiento

Por una de las interfaces, el proxy recibe una petición de un host cliente.

El software toma una de estas peticiones, y lo siguiente que hace es buscar en la caché, para ver si ya existe una copia de la página u objeto que está solicitando el cliente:

- ✓ Si ya existe, solo toma esa copia existente en el disco duro, y se la envía al cliente solicitante.

- ✓ Si no existe dicha copia, el Proxy tiene que bajar aquel contenido de Internet, para poder enviárselo al cliente. En este caso, además de hacer dicho envío, se encarga de añadir este nuevo objeto, página o archivo a la caché para su posterior uso.

Funcionamiento

Un Proxy permite a otros equipos conectarse a una red de forma indirecta a través de él. Cuando un equipo de la red desea acceder a una información o recurso, es realmente el Proxy quien realiza la comunicación y a continuación traslada el resultado al equipo inicial. En unos casos esto se hace así porque no es posible la comunicación directa y en otros casos porque el Proxy añade una funcionalidad adicional, como puede ser la de mantener los resultados obtenidos (por ejemplo una página Web) en una cache que permita acelerar sucesivas consultas coincidentes.

Pasos de Funcionamiento

El cliente se conecta hacia un Servidor Intermediario (Proxy). El cliente solicita una conexión, fichero u otro recurso disponible en un servidor distinto.

El servidor Intermediario (Proxy) proporciona el recurso ya sea conectándose hacia el servidor especificado o sirviendo éste desde un caché.

En algunos casos el Servidor Intermediario (Proxy) puede alterar la solicitud del cliente o bien la respuesta del servidor para diversos propósitos.

Ventajas de un Proxy

- Control: Sólo el intermediario hace el trabajo real, por tanto se pueden limitar y restringir los derechos de los usuarios, y dar permisos sólo al Proxy.

- Velocidad: Si varios clientes van a pedir el mismo recurso, el Proxy puede hacer caché: guardar la respuesta de una petición para darla directamente cuando otro usuario la pida.

- Filtrado: El Proxy puede negarse a responder algunas peticiones si detecta que están prohibidas.

- Modificación: Como intermediario que es, un Proxy puede falsificar información, o modificarla siguiendo un algoritmo.

Desventajas de un Proxy

- Abuso: Usuarios ajenos que desean navegar anónimamente.
- Carga: Un Proxy ha de hacer el trabajo de muchos usuarios.
- Intromisión: Es un paso más entre origen y destino, y algunos usuarios pueden no querer pasar por el Proxy. Y menos si hace de caché y guarda copias de los datos.
- Incoherencia: Si hace de caché, es posible que se equivoque y dé una respuesta antigua cuando hay una más reciente en el recurso de destino.
- Irregularidad: El hecho de que el Proxy represente a más de un usuario da problemas en muchos servicios, en concreto los que requieren una comunicación directa entre 1 emisor y 1 receptor.

Instalar Squid

Para instalar squid en una distribución derivada de debian, como ubuntu, basta con hacer:

sudo apt-get install squid

Configuración de Squid

Para hacer esto se añadirán y/o modificaran algunas líneas al fichero de configuración del Squid, cuya ruta es:

/etc/squid/squid.conf

squid.conf viene muy documentado. Antes de seguir, échale un vistazo. Es común hacer una copia de seguridad del fichero inicial, y crear uno vacío con solo los argumentos necesarios.

 # sudo mv squid.conf squid.conf.bak

 # sudo touch squid.conf

Squid.conf

Esta es una configuración válida para un proxy.

```
http_port 8080
access_log /var/log/squid/access.log
cache_log /var/log/squid/cache.log
cache_store_log /var/log/squid/store.log
acl all src 0.0.0.0/0.0.0.0
acl yo src 127.0.0.1/32
http_access allow yo
http_access deny all
```

Introducimos esta Configuración y luego configuramos firefox para que utilice 127.0.0.1 como proxy.

Squid.conf

- http_port 3128

Este es el puerto que Squid utiliza para escuchar las solicitudes de los clientes. El puerto por defecto es el 3128, pero el 8080 también suele utilizarse. Si lo desea, puede especificar varios números de puerto separados por espacios.

Squid.conf

- cache_access_log /var/log/squid/access.log
- cache_log /var/log/squid/cache.log
- cache_store_log /var/log/squid/store.log

Estas tres entradas especifican las rutas en las que Squid registra todas sus acciones. Normalmente no es necesario realizar ningún cambio. Si Squid experimenta una carga de uso intensa, puede que resulte útil distribuir el caché y los archivos de registro en varios discos.

Squid.conf

- ACLs

Squid proporciona listas de acceso para controlar el acceso al alterno. Las ACL son listas con reglas que se procesan de forma secuencial. Las listas ACL deben definirse antes de proceder a su uso.

Algunas listas ACL, como all y localhost, están predefinidas.

Squid.conf

- acl <nombre_acl> <tipo> <datos>

<nombre_acl> puede elegirse arbitrariamente.

- <tipo> selecciona el tipo de lista de acceso (src, time, srcdomain, dstdomain, url_regex...).
- <datos> depende del tipo de ACL individual y también puede leerse desde un archivo, por ejemplo mediante nombres de hosts, direcciones IP o direcciones URL.

ejemplos:

```
acl misusuarios srcdomain .midominio.com

acl profesores src 192.168.1.0/255.255.255.0

acl alumnos src 192.168.7.0-192.168.9.0/255.255.255.0

acl horadelalmuerzo time MTWHF 12:00-15:00
```

Squid.conf

- Tipos de ACL
  - Src o dst: hace referencia a una ip o dirección de red.

acl red_local src "/etc/squid/ip_permitidas"

acl red_local src 192.168.1.0/24

acl google_es dst 216.239.0.0/24

  - Time: permite denegar conexiones dentro de un rango horario.

acl horario_laboral time M T W H F 8:00-15:00

acl horario time 18:00-21:00

  - Srcdomain o dstdomain: permite denegar conexiones a un determinado sitio.

acl google_com dstdomain google.com

  - Urlregex: permite identificar sitios web según cierto patrón. También se puede importar definiciones de sitios desde un fichero externo.

acl sitios_prohibidos url_regex "/etc/squid/sitios_prohibidos"

acl pincha_google url_regex -i ^ftp://.\.pdf$*

Acl ficheros_prohibidos urlpath_regex .pdf$ .mp3$ .zip$

  - Port: permite identificar un puerto de aplicación

acl puertos_SSL port 443 563

Además de estos tipos hay muchos más

Squid.conf

- http_access (allow | deny) <nombre_acl>

Para que una ACL sea efectiva hay que aplicarla mediante http_access.

Se puede permitir o denegar el acceso mediante los valores deny (Denegar) y allow (Permitir).

Las cláusulas http_access se procesarán de arriba a abajo, por lo que es muy importante el orden.

La última entrada siempre debe ser http_access deny all o lo dejaremos pasar todo.

http_access allow localhost

http_access deny all

Squid.conf

- Existen multitud de argumentos en squid.conf, pero es imposible conocerlos todos. Algunos que pueden ser útiles.
  - cache_mem
  - cache_dir
  - cache_effective_user y cache_effective_group
  - dns_nameservers
  - cache_peer

Squid.conf

- cache_mem 8 MB

  Esta entrada define la cantidad de memoria que puede emplear Squid para las respuestas más frecuentes y las activas. El valor por defecto es 8 MB. Este valor no especifica el uso total de memoria de Squid, por lo que es posible que el uso real sea superior.

Squid.conf

- cache_dir ufs /var/cache/squid/ 100 16 256

La entrada cache_dir define el directorio del disco en el que se almacenan todos los objetos.

Los números del final indican el espacio máximo en disco que debe utilizarse en MB y el número de directorios de primer y segundo nivel.

El parámetro indica ufs indica el algoritmo de lectura/escritura en disco. Además de ufs están aufs, diskd, coss y null.

Los valores por defecto implican 100 MB de espacio ocupado en disco por el directorio /var/cache/squid y la creación de 16 subdirectorios en él, cada uno de los cuales contiene 256 subdirectorios adicionales.

Cambiar los valores de subdirectorios puede relentizar el sistema.

Squid.conf

- Cache_effective_user y cache_effective_group

cache_effective_user proxy

cache_effective_group proxy

- De este modo indicamos el usuario que utiliza squid para ejecutar sus procesos. De este modo evitamos que un usuario puedo acceder a los recursos gesionados por squid.

En ubuntu, squid utiliza el usuario proxy por defecto, por lo que en principio no habrá que usarlos. En cualquier caso, comprueba que el proceso squid se ejecuta bajo el usuario proxy y que los directorios caché son propiedad de proxy.

sudo ps aux | grep proxy

ls -lah /var/spool/squid

Squid.conf

- dns_nameservers 127.0.0.1 80.58.32.33

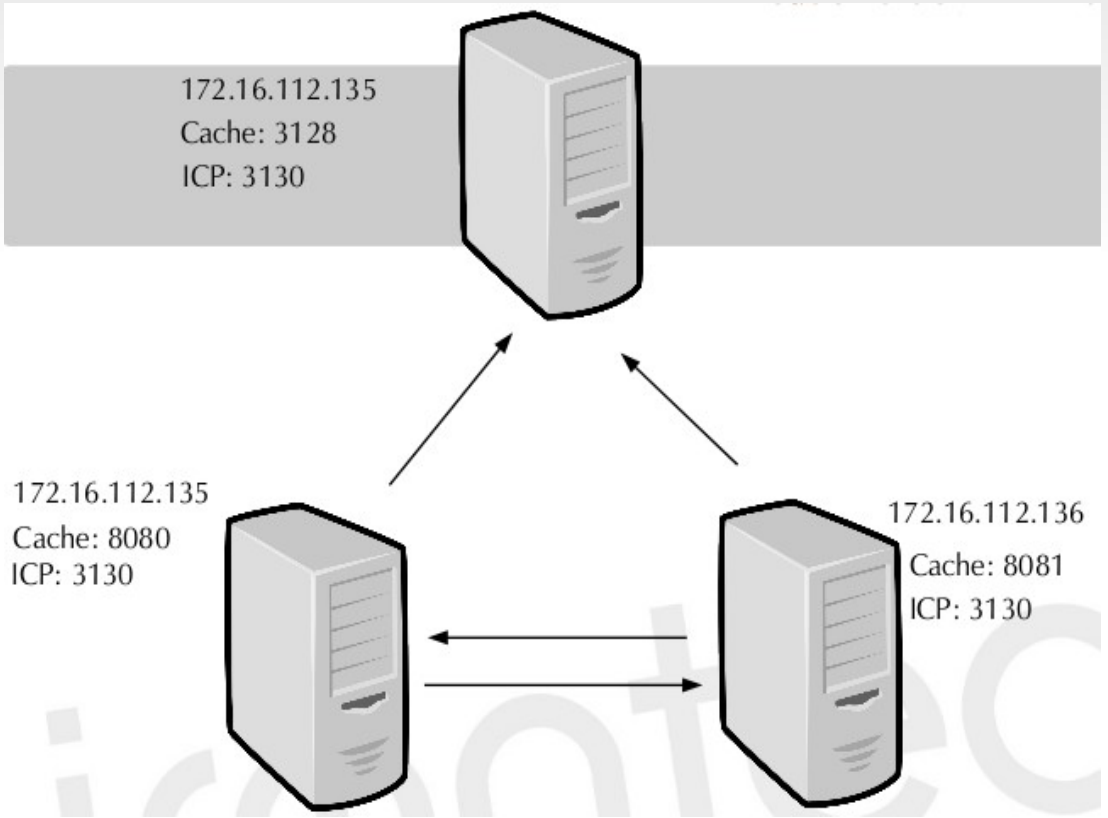
Podemos definir los servidores DNS que utilizará el proxy para resolver nombres.

Se pueden definir varios servidores DNS.

Squid.conf

- Cache_peer

Squid permite crear jerarquías de cachés. Puede haber proxys-cachés padres y hermanos. Si establecemos una jerarquía padre-hijo (parent), el padre debe proporcionar el objeto pedido tanto si está en la caché como si no lo está.



Squid.conf

- HERMANO 1.

icp_port 3130

puerto icp

cache_peer 172.16.112.131 parent 3128 3130 default

definimos cache padre. Puerto proxy 3128 y puerto icp 3130

cache_peer 172.16.112.136 sibling 8081 3130 proxy-only

definimos cache hermano. Puerto proxy 8081 y puerto icp 3130

icp_access allow all

permitimos acceso icp a todos

Default: en caso de duda, usar este vecino.
Proxy-only: no almacenar en caché la respuesta de este vecino

Squid.conf

- HERMANO 2.

icp_port 3130

puerto icp

cache_peer 172.16.112.131 parent 3128 3130 default

definimos cache padre. Puerto proxy 3128 y puerto icp 3130

cache_peer 172.16.112.135 sibling 8081 3130 proxy-only

definimos cache hermano. Puerto

proxy 8081 y puerto icp 3130 icp_access allow all

permitimos acceso icp a todos

Squid.conf

- PADRE

icp_port 3130

puerto icp

icp_access allow all

permitimos acceso icp a todos

Squid.conf

- También podemos limitar el acceso al proxy mediante usuario y contraseña.
- Si tenemos un controlador de dominio, podemos autenticar contra él.
- Nosotros de momento, utilizarmenos la autenticación de Apache.

Squid.conf

$ touch /etc/squid/squid_passwd

$ chmod 644 /etc/squid/squid_passwd; chown proxy:proxy /etc/squid/squid_passwd

$ htpasswd /etc/squid/squid_passwd www

New password:

Re-type new password:

Adding password for user www

$ locate ncsa_auth

/usr/lib/squid/ncsa_auth

Opción alternativa

acl autorizado ident mauri
http_access allow autorizado

Usuarios del sistema.

Hay que Añadir en squid.conf:

auth_param basic program /usr/lib/squid/ncsa_auth /etc/squid/squid_passwd

acl **ncsa_users** proxy_auth REQUIRED

acl **business_hours** time M T W H F 9:00-17:00

http_access allow **ncsa_users business_hours**

Squid.conf

- Proxy transparente
- Un proxy transparente no requiere la configuración de firefox. Para conseguir un proxy transparente hacen falta dos cosas:
  - En squid.conf
    - http_port 3128 transparent
  - En iptables

(página siguiente)

Squid+iptables

iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 -j REDIRECT --to-port 3128

iptables -A INPUT -m state --state NEW,ESTABLISHED,RELATED -i eth1 -p tcp --dport 3128 -j ACCEPT

iptables -A OUTPUT -m state --state NEW,ESTABLISHED,RELATED -o eth0 -p tcp --dport 80 -j ACCEPT

iptables -A INPUT -m state --state ESTABLISHED,RELATED -i eth0 -p tcp --sport 80 -j ACCEPT

iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -o eth1 -p tcp --sport 80 -j ACCEPT