Squid+Iptables

Carolina Alvarado Chavarría
B40246

Resumen—

Index Terms—proxy, firewall, caché, ACL, puerto, proxy transparente, tráfico de red, servidor web.

El presente proyecto se realizó con el proposito de ampliar los conocimientos propios de Linux y al mismo tiempo el utilizar los conocimientos ya adquiridos anteriormente. Se trabajará con redes, la terminal de linux, repositorios, editores de texto entre otros. Se realizó una investigación acerca de la configuración de tanto squid como iptables. Se logró la configuración de squid en un navegador web y se intentó su configuración como proxy transparente.

1. Marco Teórico

El presente proyecto se basa en la utilización y configuración de la aplicación Squid junto con Iptables. Squid es un servidor proxy para la web con caché que soporta protocolos HTTP, HTTPS, FTP, entre otros (Squid-cache.org, 2013). Es necesario saber que un proxy funciona como un intermediario entre los clientes y servidores web. El proxy brinda acceso a la web a personas que se encuentran en subredes cerradas y que solo pueden acceder al internet a través de un firewall (Luotonen, A., 1994). El proxy no modifica los pedidos de los clientes sino que facilita la comunicación brindando más rapidez en las respuestas por medio del caché. El proxy también puede funcionar como filtro entre la comunicación en caso que existan reglas predeterminadas de acceso a servidores web.

El proxy puede funcionar como un proxy transparente. Un proxy de intercepción o proxy transparente funciona interceptando las solicitudes de los clientes o redirigiendolas a uno más servidores proxy sin configurar los clientes HTTP en los equipos clientes, o sin el conocimiento de los clientes (Saini, K., 2011. p.240). Para obtener un proxy transparente es necesario configurar el firewall de red para utilizarlo cómo monitor de seguridad del mismo. Un firewall o cortafuegos es un dispositivo de seguridad de red que monitorea el tráfico de red -entrante y saliente- y decide si permite o bloque tráfico específico en función de un conjunto definido de reglas de seguridad (Cisco, s.f.).

En el sistema operativo de Linux se utiliza la herramienta Iptables para configurar el firewall. Iptables es una herramienta que permite la filtración de paquetes, traducción de direcciones de red entre otras configuraciones de red (Netfilter, s.f.). Iptables es parte del entorno de trabajo del software Netfilter, el cuál se encuentra dentro del kernel de Linux a partir de la Linux 2.4.x. Es por medio de la combinación del software Squid y la herramienta Iptables de Netfilter que se puede configurar un proxy transparente.

El uso de Squid optimiza el flujo de datos entre clientes y servidores, además el uso de caché permite ahorrar ancho de banda mejorando la experiencia de navegación del usuario. (Saini, K., 2011. p.8). Por otro lado Iptables permite utilizar el proxy Squid como un proxy transparente lo cual permite que para el uso del proxy no se deba de configurar cada cliente haciendo el proceso más ágil. Squid es de los proxies más utilizados en sistemas Linux por lo que el aprender sus funciones resulta importante para las personas que deseen obtener más conocimiento acerca de redes y su configuración es importante si se busca tener los mayores beneficios al navegar la red o al poseer servidores web.

La configuración de Squid también necesita el conocimiento de diferentes conceptos. Squid necesita saber en que puerto de red debe de escuchar para realizar sus procesos. Un puerto de red permite a las aplicaciones compartir recursos sin interferir uno con otro. Las computadoras y routers automaticamente manejan el tráfico de red a traves de puertos de red virtuales (Mitchell, B. 2013). Los ACL o “access control lists” son los elementos básico

en la configuración de un proxy. Por medio de estos squid decide si realizar o no una transacción solicitada, pueden ser acl's rápidos o lentos dependiendo de los prefijos que se utilicen en la página de configuración (Saini, K. 2011. p.92). Es por medio de estas listas de control que el proxy sabe que paginas o direcciones ip el administrador desea bloquear y además si la conexión esta definida como segura. El caché que realiza squid es para hacer más rápido el proceso de conexión, siendo caché el guardar la información de paginas web para no tener que acceder directamente a ellas para obtenerla. Una función importante de la configuración de squid es la del registro, esencialmente es un registro de las acciones realizadas, peticiones o usuarios por medio de documentos (Saini, K. 2011. p.66). El log puede funcionar para encontrar errores en el tráfico de datos o acceso.

Por otro lado Iptables tiene una configuración en forma de tablas, las tablas se dividen en cadenas y en estas cadenas se encuentran las reglas del firewall definidas por el usuario. Las tablas que se encuentran en Iptables son: raw, filter, nat, mangle y security. Cada una de estas tablas poseen sus propias cadenas por ejemplo las de filter son INPUT, OUTPUT y FORWARD. Dentro de cada una de esas cadenas se pueden registrar o configurar reglas a seguir conforme a la distribución y filtración de paquetes (Iptables, s.f).

En general mediante adecuadas configuraciones de squid como iptables es posible crear las limitaciones deseadas en el uso de los servidores web.

2. Procedimiento y Uso

El proyecto se divide en dos procedimientos principales los cuáles son:

1. Configurar Squid para que trabaje como un proxy en la computadora.
2. Configurar Iptables y establecer el proxy transparente.

2.1. Configuración de Squid

Antes de realizar la configuración de squid es necesario instalar la aplicación. Se utilizó el paquete disponible en el repositorio. El cúal es squid3.

```
caro@Link:~/Documents$ sudo apt-get install squid3
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  squidclient squid-cgi squid-purge resolvconf smbclient ufw winbindd
The following NEW packages will be installed:
  squid3
0 upgraded, 1 newly installed, 0 to remove and 44 not upgraded.
Need to get 0 B/2,068 kB of archives.
After this operation, 6,577 kB of additional disk space will be used.
Selecting previously unselected package squid3.
(Reading database ... 170663 files and directories currently installed.)
Preparing to unpack .../squid3_3.4.8-6+deb8u4_amd64.deb ...
Unpacking squid3 (3.4.8-6+deb8u4) ...
Processing triggers for systemd (215-17+deb8u6) ...
Processing triggers for man-db (2.7.0.2-5) ...
Setting up squid3 (3.4.8-6+deb8u4) ...
Creating Squid HTTP proxy 3.x spool directory structure
2017/04/25 22:19:29 kid1| Set Current Directory to /var/spool/squid3
2017/04/25 22:19:29 kid1| Creating missing swap directories
2017/04/25 22:19:29 kid1| No cache_dir stores are configured.
Processing triggers for systemd (215-17+deb8u6) ...
caro@Link:~/Documents$
```

Una vez instalado es necesario configurarlo esto se hace editando el documento de texto del paquete que se encuentra en /etc/squid3/squid.conf". Se verificó que squid escuchará en el puerto 3128. Además se habilitaron las instrucciones que establecen el directorio para el caché además de su tamaño.

```
Squid normally listens to port 3128
http_port 3128
```

En cuanto a la configuración de paginas a bloquear se realizó haciendo un archivo donde se escribieron las palabras o direcciones a negar.

```
 GNU nano 2.2.6                File: prohibidas

yahoo.com
live
pelis24.comm
```

Para prohibir esa lista se utilizó la siguiente dirección en el texto de configuración de squid:

```
#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
visible_hostname Link
acl bloqueadas url_regex "/etc/squid3/prohibidas"
```

En el archivo de configuración también se deben incluir las direcciones ip que tienen acceso al proxy además de direcciones del tipo refresh pattern, cache_mem, cache_dir y las direcciones que determinan los puertos seguros. La configuración predeterminada de squid ya viene con muchas de las instrucciones necearias pero igual es necesario agregar instrucciones especificas referentes a la red que se utiliza. En general el archivo de configuración básico se ve como el siguiente:

```
http_port 3128

refresh_pattern ^ftp:
refresh_pattern ^gopher:
refresh_pattern -i (/cgi-bin/|\?
refresh_pattern .

acl localnet src 10.0.0.0/8
acl localnet src 172.16.0.0/12
acl localnet src 192.168.0.0/16
acl localnet src fc00::/7
acl localnet src fe80::/10

acl SSL_ports port 443

acl Safe_ports port 80
acl Safe_ports port 21
acl Safe_ports port 443
acl Safe_ports port 70
acl Safe_ports port 210
acl Safe_ports port 1025-65535
acl Safe_ports port 280
acl Safe_ports port 488
acl Safe_ports port 591
acl Safe_ports port 777

acl CONNECT method CONNECT

http_access deny !Safe_ports
http_access deny CONNECT !SSL_po
http_access allow localhost mana
http_access deny manager
http_access allow localnet
http_access allow localhost
http_access deny all
```

Finalmente se configuró en el navegador Firefox la utilización del proxy por medio de la ip de red.

2.2. Configuración de Iptables

Primero se realizó la instalación del paquete Iptables para poder manejar las tablas y reglas.

```
caro@Link:~/Documents$ sudo apt-get install iptables
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  iptables
0 upgraded, 1 newly installed, 0 to remove and 44 not upgraded.
Need to get 277 kB of archives.
After this operation, 3,642 kB of additional disk space will be used.
Get:1 http://mirrors.ucr.ac.cr/debian/ jessie/main iptables amd64 1.4.21-2+b1 [277 kB]
Fetched 277 kB in 1s (158 kB/s)
Selecting previously unselected package iptables.
(Reading database ... 170587 files and directories currently installed.)
Preparing to unpack .../iptables_1.4.21-2+b1_amd64.deb ...
Unpacking iptables (1.4.21-2+b1) ...
Processing triggers for man-db (2.7.0.2-5) ...
Setting up iptables (1.4.21-2+b1) ...
Processing triggers for libc-bin (2.19-18+deb8u7) ...
caro@Link:~/Documents$
```

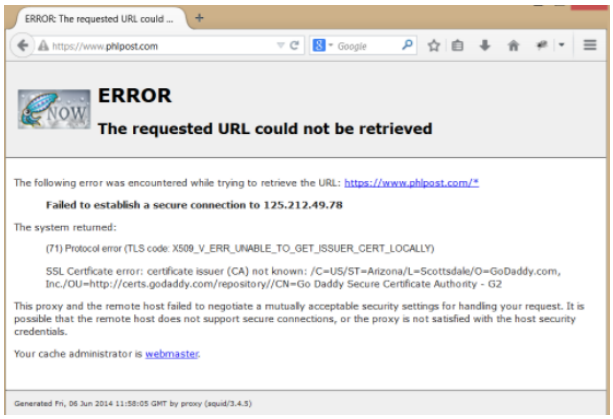
La dirección a usar para hacer que el tráfico del puerto 8080 se redirige al puerto 3128 que es donde se encuentra escuchando Squid es:

iptables -t nat -A PREROUTING -i eth0 -p tcp –dport 80 -j REDIRECT –to-port 3128

Esta dirección funciona para que se pueda trabajar squid como un proxy transparente.

3. Justificación de Resultados

En la implementación del proyecto sí se logró que el proxy squid funcionará en un navegador (firefox) mediante la configuración del proxy en el mismo. Al hacer esto e intentar ingresar a las paginas configuradas como prohibidas se obtuvo el mensaje de error de squid como se puede observar:



En cuanto a la implementación de iptables para convertir el proxy a uno transparente no se logró. Se cambio la configuración de squid para que funcionara como transparente. Se utilizó la dirección descrita anteriormente y también se realizó con pequeñas modificaciones como poner la dirección ip especifica pero al enlistar las reglas de iptables no aparecía enlistada y al ingresar al navegador web no se bloquearon las paginas necesarias sin que se configurará el proxy determinado en las preferencias. Lo anterior principalmente se da debido a la falta de conocimiento de Iptables. Es posible que sean necesarias más instrucciones para poder modificar una tabla de iptables o que fuera necesario habilitar la opción de squid transparente desde la compilación del programa. Es también necesario tomar en consideración los problemas con la tarjeta de red de la computadora que se utilizó. Se intentó realizar todos los procesos por medio de la red ethernet pero sí se utilizó el wifi defectuoso en ocasiones.

En general la configuración e implementación de squid brindó conocimiento acerca de los proxys y al mismo tiempo permitió ampliar el conocimiento de redes. Iptables permitió comprender el funcionamiento de los firewalls además de las divisiones de su estrcutura.

4. RECOMENDACIONES

- Realizar una copia del archivo de configuración de squid para poder volver a la configuración predeterminada en caso de cometer algún error.
- Leer con anterioridad las especificaciones de squid e iptables para saber que significa cada instrucción que se utiliza.
- Si es posible utilizar el proxy como transparente debido a que puede ahorrar procesos y tiempo.
- Utilizar el proxy Squid a cualquier proxy para reducir el uso de ancho de banda, mejorar la velocidad de carga de páginas y tener un registro de la actividad.
- Si se es dueño de una red utilizar Squid para manejar las reglas de acceso de cada cliente a las misma.

5. BIBLIOGRAFÍA

Archlinux (s.f). *Iptables*. [wiki] Recuperado de https://wiki.archlinux.org/index.php/iptables

Cisco (s.f). *¿Qué es un firewall?*. Recuperado de http://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html

Luotonen, A. & Altis, K. (Abril 1994). *World-Wide Web Proxies*. Computer Networks and ISDN Systems, pp. 147-154.

Mitchell, B. (Marzo 2017). *Computer ports and their role in computer networking*. Lugar de publicación: Lifewire. Recuperado de https://www.lifewire.com/computer-port-usage-817366

Netfilter (s.f). *The netfilter.org project*. Recuperado de http://www.netfilter.org/

Saini, K. (2011). *Squid Proxy Server 3.1: Beginner's Guide.*. Packt Publishing.

Squid-chache.org. (Mayo 2013). *squid: Optimising Web Delivery*. Recuperado de http://www.squid-cache.org/