Prácticas con ***squid***

Sobre una máquina virtual Linux con dos tarjetas de red, una en modo puente y la otra como red interna para dar servicio a otras máquinas virtuales que harán de clientes en esa red interna, instala y configura *squid*. Por supuesto también puedes usar GNS3 (recomendado). Al principio se trata de hacer una configuración mínima de *squid*, que permita navegar desde un navegador sito en la red interna. Puedes encontrar multitud de tutoriales en Internet de instalación y configuración mínima. Es un tema muy trillado y nada complejo.

Lee atentamente y haz las pruebas que hay en el libro para conocer al máximo los potenciales de ***squid***.

Cuando hagas las diversas actividades, ten en cuenta las siguientes cuestiones:

1. **autentificación de usuarios en Squid3 y ACLs**

Para que funcione la autenticación de usuarios BASIC hay que seguir los pasos del libro y añadir la siguiente línea:

http_access allow passwd

Además utiliza esta línea:

auth_param basic program /usr/lib/squid3/basic_ncsa_auth /etc/squid3/claves

Si añadimos listas de control de acceso hay que tener en cuenta el orden en el que se procesan, de forma que si primero ponemos una línea http_access allow all antes del línea http_access deny... el resultado será que no se llegarán a tener en cuenta las línea que deniegan. Por ejemplo para tener autenticación de usuarios y dominios prohibidos pondremos algo parecido a lo siguiente:

```
acl nowebs dstdomain "/etc/squid3/nowebs"
http_access deny nowebs
acl passwd proxy_auth REQUIRED
http_access allow passwd
http_access allow all
```

sin embargo no funciona ni la autenticación ni los dominios prohibidos si ponemos:

```
http_access allow all
acl nowebs dstdomain "/etc/squid3/nowebs"
http_access deny nowebs
acl passwd proxy_auth REQUIRED
http_access allow passwd
```

2. Proxy transparente

Para que el Proxy funcione en modo transparente, además del comando de iptables, debemos indicarlo con las siguientes líneas (la segunda permite el puerto 8080 en modo normal):

```
http_port 3128 transparent
http_port 8080
```

NOTA: el proxy transparente no funciona con la autenticación de usuarios

Haz capturas de todas las pruebas realizadas. Verifica tanto los accesos permitidos como los denegados.

A continuación realiza los siguientes ejercicios, pruébalos y haz capturas como de costumbre. Investiga en el fichero de configuración original *squid.conf*, en el *man* o en Internet cómo hacerlos.

1. Deniega las conexiones a todos los equipos en horario de 18:00 a 21:00 horas. Permite el resto.
2. Deniega las conexiones a todos los equipos en horario de 20:00 a 9:00 horas, así como los fines de semana. Permite el resto.
3. Deniega el acceso a un equipo con una IP determinada. El resto de IPs deben estar permitidas.
4. Restringe el acceso a todo el contenido con extensión .mp3 u otra extensión que puedas probar.
5. Restringe el acceso a todo el contenido con extensión .mp3 (u otra) en horario de 9:00 a 14:00 horas.
6. Deniega el acceso a una serie de sitios de Internet en un horario a tu elección. Permite el resto.
7. Deniega el acceso a una serie de sitios de Internet en un horario a tu elección desde algunas IPs. Permite el resto.