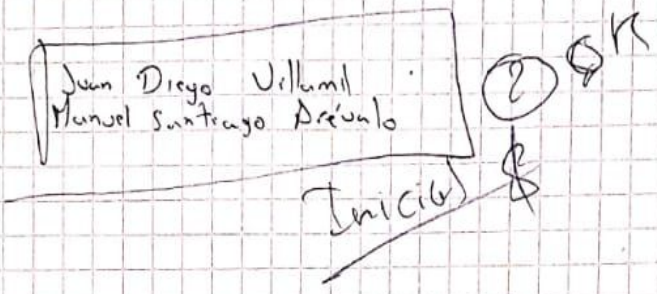
Laboratorio # 3



01-04-2019

Proxy Server

Seguridad de la informacion

1. Filtro web
2. control de acceso
3. control de throughput

INFORME LABORATORIO

SERVIDOR PROXY

MANUEL SANTIAGO ARÉVALO CORREDOR

JUAN DIEGO VILLAMIL OSORIO

UNIVERSIDAD EL BOSQUE

FACULTAD DE INGENIERÍA

PROGRAMA DE INGENIERÍA DE SISTEMAS

BOGOTA D.C.

2019

CONTENIDO

INTRODUCCIÓN

La información es lo más preciado para las empresas, y mantener esta segura se vuelve la prioridad número uno, es por ello que estas optan por restringir la salida a internet de los equipos que se encuentran dentro en la compañía esto con el fin de evitar ataques desde internet y la salida de la información por parte de los usuarios. Una de las maneras más comunes para llevar a cabo este bloqueo de fuga de información es mediante un proxy, cuyo objetivo es bloquear la salida de internet de las máquinas que se encuentran en la infraestructura, permitiendo dicha salida únicamente si se pasa por el equipo proxy. Durante el desarrollo de este laboratorio veremos una forma de configuración de un servidor proxy con el fin de restringir la navegación hacia internet de los equipos que se encuentran dentro de nuestra VLAN.

MARCO TEÓRICO

Para realizar este laboratorio se utilizaron diferentes herramientas, una de ellas fue una máquina virtual, este es un software el cual sirve para simular un sistema operativo y se pueden ejecutar aplicativos como si se tratase de uno normal, en ella se implementó un servidor el cual es un equipo, virtual o físico, encargado de proporcionar servicios a los clientes que le realizan las peticiones, en estos servidores se pueden instalar diferentes aplicaciones y desplegar páginas de internet las cuales serían accesibles desde internet si se desea, un ejemplo de lo que se puede instalar allí son proxys, estos son intermediarios des las peticiones de recursos que hace un cliente a un servidor, esto permite tener un control del tráfico que está generando el cliente con lo que se puede mejorar la seguridad ya que se pueden bloquear paginas especificas o contenido que no se quiere tener acceso.

MATERIALES Y MÉTODOS

Para el desarrollo de este laboratorio, se utilizaron diversos materiales y herramientas, debido a que el laboratorio en parte se hizo presencial se adjuntan estos implementos también. Se utilizaron los siguientes:

1. 2 computadores con Windows 7
2. Cables de red
3. Virtual Box
4. 1 máquinas virtual con SO Ubuntu Server.
5. Squid.

PROCEDIMIENTO

Para el desarrollo del laboratorio es preciso seguir el diagrama de red Figura 1 donde se muestra, esto nos proporciona una visión acerca de la comunicación de las máquinas.

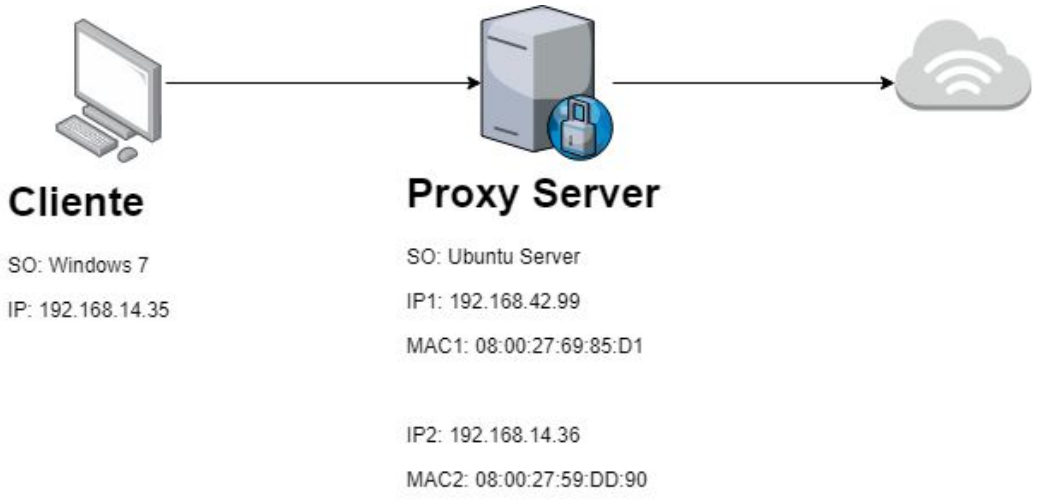


Figura 1. Diagrama de red

Una vez hecho el diagrama de red se procede a descargar virtual box con el fin de crear nuestra máquina virtual, una vez instalado virtual box creamos una máquina virtual con SO Ubuntu server el cual debemos instalar y seguir las indicaciones que se muestran en la ventana. Luego de esto, debemos instalar la instrucción apt-get descargar squid como vemos en la Figura 3 ya que este será nuestro servidor proxy y el que se configurará para dar internet a la otra máquina. Una vez finalizado este proceso, la instalación, procedemos a configurar Squid como se observa en la Figura 3 y Figura 4.

```
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

user@localhost:~$ apt -get -y update && apt-get -y install squid
E: No tiene sentido la opción de línea de órdenes «g» [de -get] combinada con las otras opciones.
user@localhost:~$ sudo apt-get update
[sudo] password for user:
Obj:1 http://archive.ubuntu.com/ubuntu cosmic InRelease
Des:2 http://archive.ubuntu.com/ubuntu cosmic-updates InRelease [88,7 kB]
Des:3 http://archive.ubuntu.com/ubuntu cosmic-backports InRelease [74,6 kB]
Des:4 http://archive.ubuntu.com/ubuntu cosmic-security InRelease [88,7 kB]
Des:5 http://archive.ubuntu.com/ubuntu cosmic/main Translation-en [513 kB]
Des:6 http://archive.ubuntu.com/ubuntu cosmic/main Translation-es [364 kB]
Des:7 http://archive.ubuntu.com/ubuntu cosmic/restricted Translation-en [3.888 B]
Des:8 http://archive.ubuntu.com/ubuntu cosmic/restricted Translation-es [1.960 B]
Des:9 http://archive.ubuntu.com/ubuntu cosmic/universe Translation-es [1.259 kB]
Des:10 http://archive.ubuntu.com/ubuntu cosmic/universe Translation-en [5.063 kB]
Des:11 http://archive.ubuntu.com/ubuntu cosmic/multiverse Translation-en [113 kB]
Des:12 http://archive.ubuntu.com/ubuntu cosmic/multiverse Translation-es [74,9 kB]
Des:13 http://archive.ubuntu.com/ubuntu cosmic-updates/main Translation-en [103 kB]
Des:14 http://archive.ubuntu.com/ubuntu cosmic-updates/restricted Translation-en [2.192 B]
Des:15 http://archive.ubuntu.com/ubuntu cosmic-updates/universe Translation-en [85,2 kB]
Des:16 http://archive.ubuntu.com/ubuntu cosmic-updates/multiverse Translation-en [1.620 B]
Des:17 http://archive.ubuntu.com/ubuntu cosmic-backports/universe Translation-en [1.268 B]
Des:18 http://archive.ubuntu.com/ubuntu cosmic-security/main Translation-en [55,8 kB]
Des:19 http://archive.ubuntu.com/ubuntu cosmic-security/restricted Translation-en [2.192 B]
Des:20 http://archive.ubuntu.com/ubuntu cosmic-security/universe Translation-en [37,9 kB]
Des:21 http://archive.ubuntu.com/ubuntu cosmic-security/multiverse Translation-en [1.620 B]
Descargados 7.935 kB en 24s (327 kB/s)
Leyendo lista de paquetes... Hecho
user@localhost:~$
```

Figura 2. Instalación Squid

```
  GNU nano 2.9.8                                squid.conf

#Indicamos el puerto que usaremos para el proxy
http_port 3128

#La memoria cache que utilizaremos para almacenar las url
#Tenemos que indicar que son MB
cache_mem 100 MB

#Ubición del directorio del spool
cache_dir ufs /var/spool/squid 150 16 256

#Declaremos la variable de red local con los datos de nuestra LAN
#Usamos la máscara de 24 bits (255.255.255.0)
acl red_local src 192.168.14.36/24

#Declaramos el localhost
acl localhost src 127.0.0.1/32
#acl password proxy_auth REQUIRED
#Declaramos la expresión regulat de URL (url_regex)
acl def_prohibidas url_regex "/etc/squid/bloqueos/prohibidas"

#Decimos que la variable 'all' son todas las redes 'all'
acl all src all
#Damos acceso a la web a nuestra máquina y la red local
#http_access allow localhost
#http_access allow red_local !def_prohibidas
#http_access deny all


auth_param basic program /usr/lib/squid/basic_ncsa_auth /etc/squid/users
auth_param basic children 30
auth_param basic realm PROXY Seguridad

                              [ Read 36 lines ]
^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos    M-U Undo
^X Exit      ^R Read File  ^\ Replace   ^U Uncut Text ^T To Spell  ^_ Go To Line M-E Redo
```

Figura 3. Configuración Squid 1

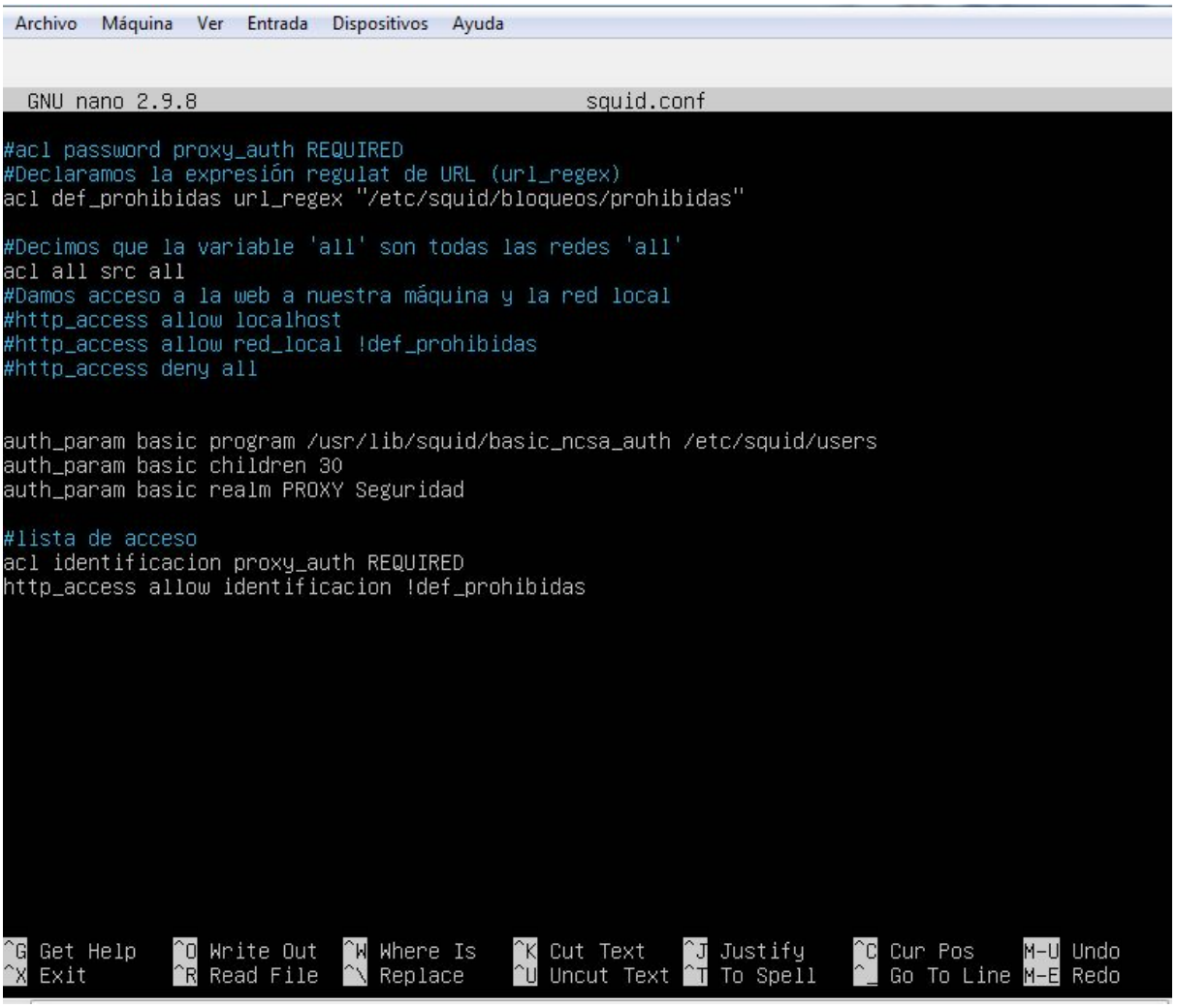


Figura 4. Configuración Squid 2

Después de tener configurado Squid, debemos confirmar que desde la MV se le este proporcionando internet a la otra máquina, para ello debemos confirmar y asignar las ips a las tarjetas de red Figura 5. esto con el fin de poder determinar los segmentos en los cuales se colocara la ip del equipo que navegara por medio del proxy.

Teniendo configuradas las tarjetas de red debemos cambiar las ip en la máquina cliente, para que se encuentre en el mismo segmento que la tarjeta de red 2 de la MV, con ello se obliga a pasar por el proxy para que desde la otra tarjeta de red se le proporcione el internet con la configuración que tenga Squid (el proxy).

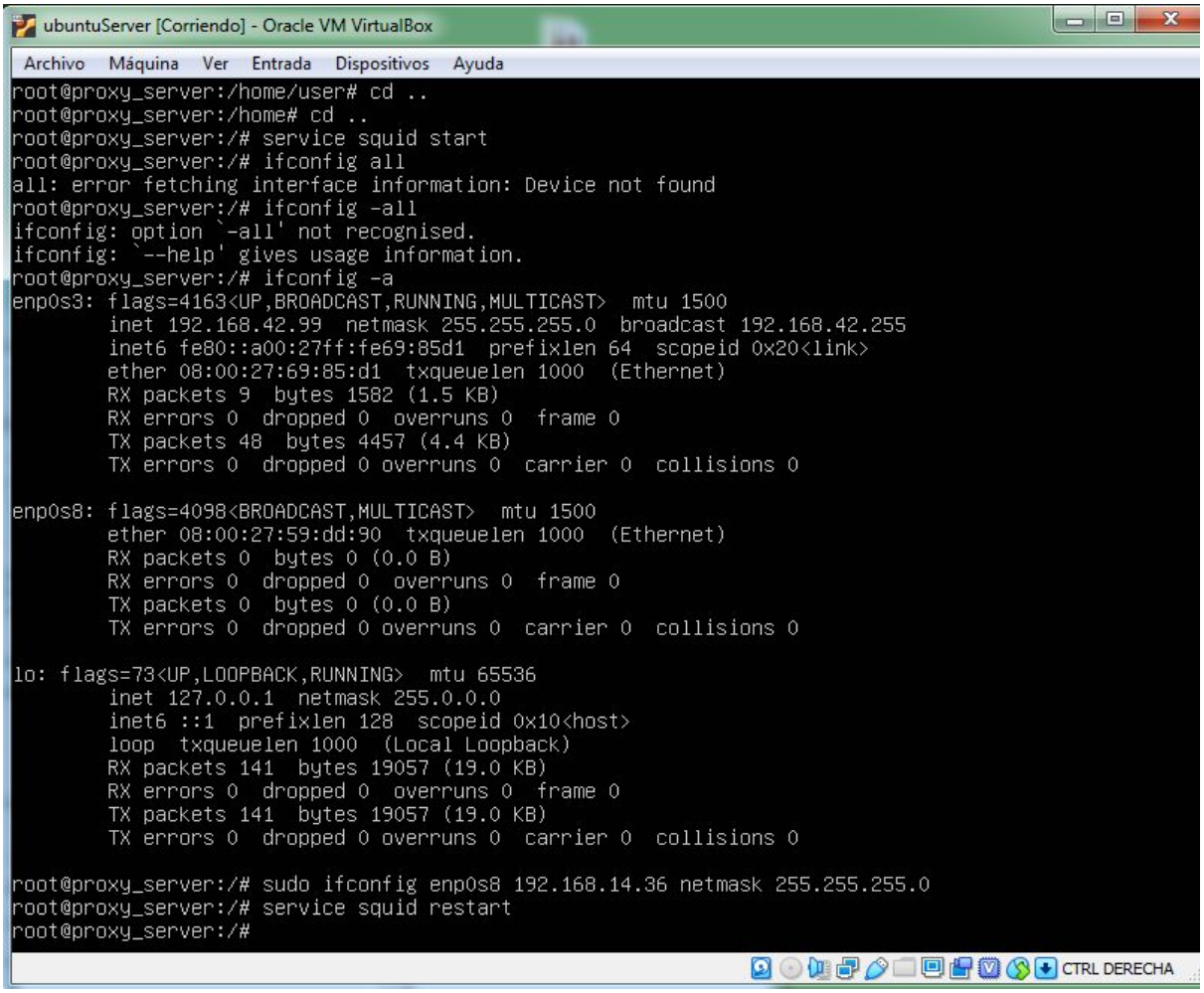


Figura 5. Tarjetas de red

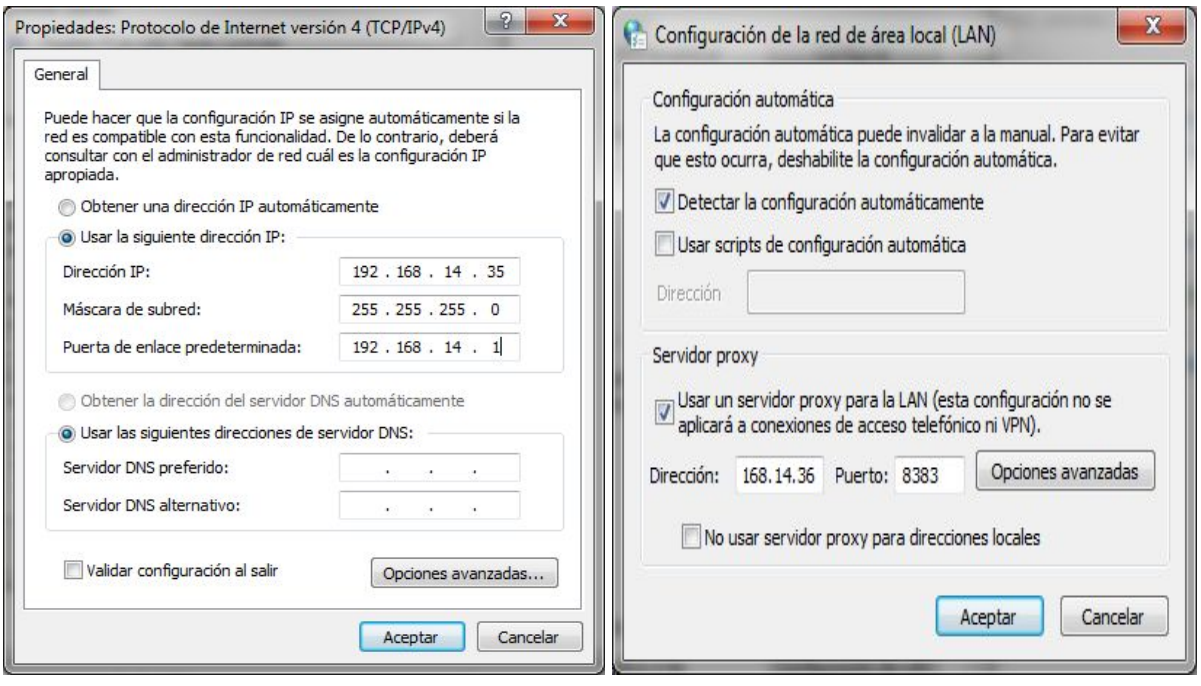


Figura 6. Configuración IPs

Ya configurada nuestra red y confirmado que permite navegar en la máquina cliente, debemos configurar las páginas que vamos a bloquear, en este caso creamos un archivo con unas palabras, entonces, las páginas que contengan estas palabras en sus rutas serán bloqueadas. Sin embargo, también podemos bloquear el acceso a internet por medio de usuario y contraseña, para ello debemos instalar Apache Figura 7.

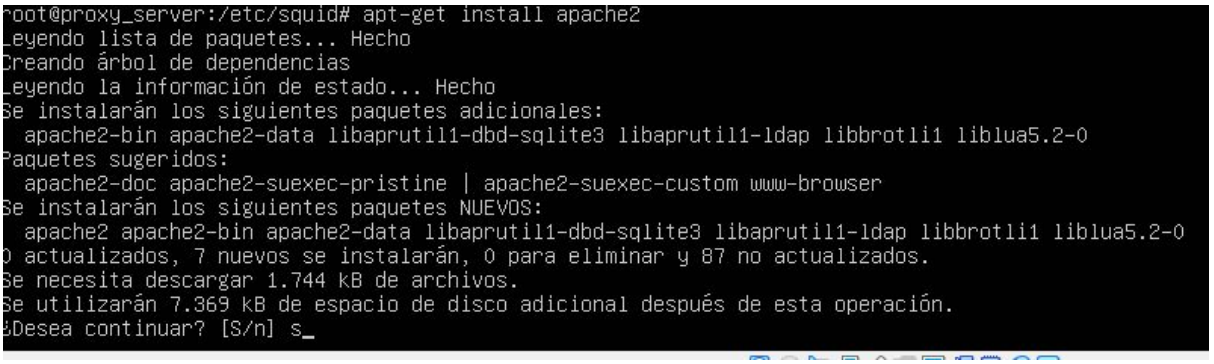


Figura 7. Instalación apache

Una vez instalado el Apache procedemos a crear los usuarios que darán acceso a internet, para ello ejecutamos el comando que se ilustra en la Figura 8 y se le asigna la contraseña, para confirmar que el usuario haya sido creado de forma exitosa debemos abrir el archivo “users” y en seguida mostrará el nombre del usuario que fue creado.

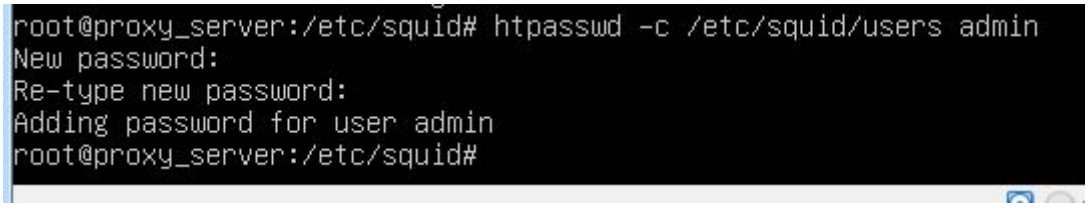


Figura 8. Creación usuarios

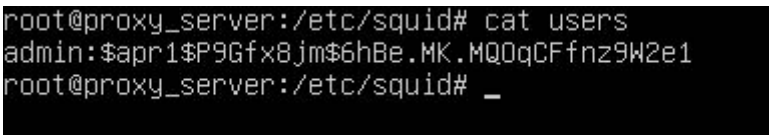


Figura 9. Verificación usuario

Por último iniciamos el servicio con el comando “service squid start”.

RESULTADOS

En cuanto implementamos las configuraciones del squid para el bloqueo de ciertas páginas web encontramos que, en primer lugar las páginas sin certificado de seguridad, nuestro proxy las bloquea como se observa en la Figura 10 y Figura 11, en estas vemos que la solicitud no se ha podido completar pues el squid le da acceso denegado, así mismo vemos la versión del proxy con hora y fecha en la que se hizo la solicitud, ilustrado en la Figura 12

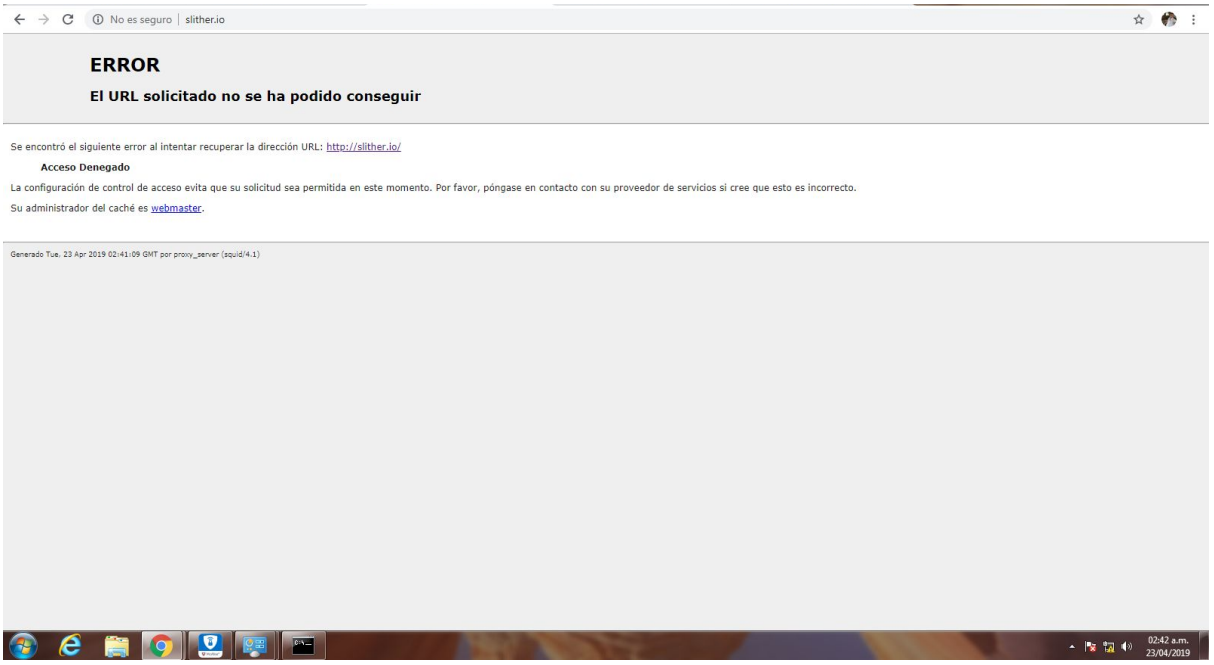


Figura 10 Bloqueo HTTP

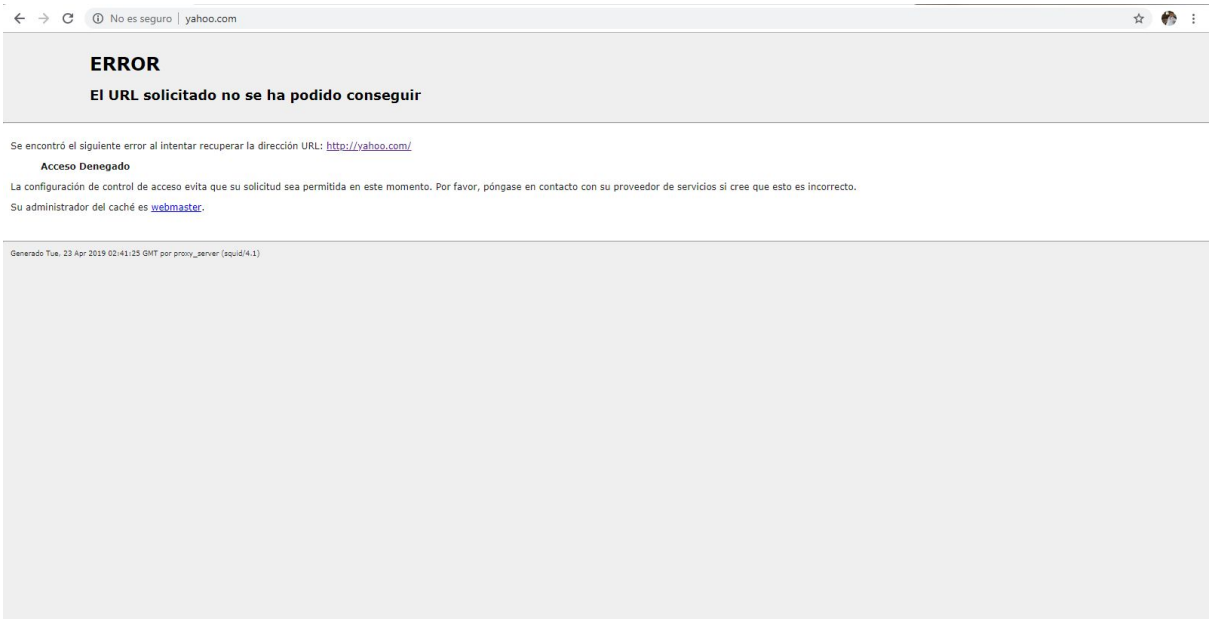


Figura 11 Bloqueo HTTP

Figura 12 Version Squid

Según nuestras configuraciones del servidor proxy, bloqueamos las paginas que contuvieran "youtube", "facebook" o "el tiempo" dentro de su dominio, por lo que cualquier sitio web que traiga consigo estos textos será bloqueado como se muestra en la Figura 13

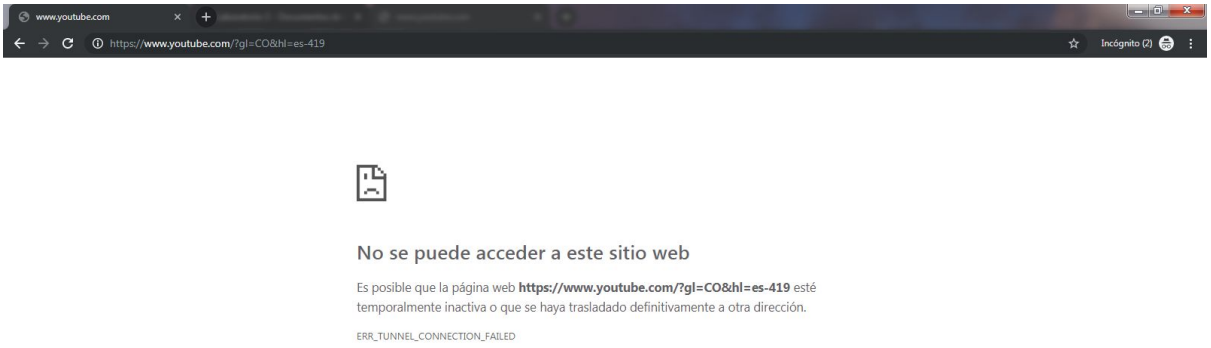


Figura 13 Bloqueo del Proxy

De igual manera cuando ingresamos al archivo de logs de squid vemos el bloqueo que realiza el proxy sobre dicha página, denegando la conexión que se intenta hacer, esto lo vemos en la Figura 14 donde niega el servicio de conexión a la pagina www.facebook.com o en el caso de la imagen que se ve en la Figura 15 donde se niega también la conexión hacia www.eltiempo.com, estos bloqueos lo hace por el protocolo TCP, visualizando esta transacción en los logs como TCP_DENIED.

```
1556590301.727      0 192.168.14.35 TCP_DENIED/403 4039 CONNECT connect.facebook.net:443 - HIER_NONE
/- text/html
1556590489.085    863 192.168.14.35 TCP_TUNNEL/200 65099 CONNECT connect.facebook.net:443 seguridad
HIER_DIRECT/157.240.6.23 -
1556590491.337   2248 192.168.14.35 TCP_TUNNEL/200 925 CONNECT www.facebook.com:443 seguridad HIER_D
IRECT/157.240.6.35 -
1556590526.199  26473 192.168.14.35 TCP_TUNNEL/200 762 CONNECT www.facebook.com:443 seguridad HIER_D
IRECT/157.240.6.35 -
1556590568.226  41659 192.168.14.35 TCP_TUNNEL/200 1390 CONNECT www.facebook.com:443 seguridad HIER_
DIRECT/157.240.6.35 -
1556590568.228  68499 192.168.14.35 TCP_TUNNEL/200 185983 CONNECT connect.facebook.net:443 seguridad
 HIER_DIRECT/157.240.6.23 -
1556591331.544      0 192.162.35.23 TCP_DENIED/403 4094 CONNECT www.facebook.com:443 seguridad HIER_
NONE/- text/html
1556591331.630      0 192.162.35.23 TCP_DENIED/403 4094 CONNECT www.facebook.com:443 seguridad HIER_
NONE/- text/html
1556591336.678      0 192.162.35.23 TCP_DENIED/403 4094 CONNECT www.facebook.com:443 seguridad HIER_
NONE/- text/html
1556591369.958      1 192.162.35.23 TCP_DENIED/403 4094 CONNECT www.facebook.com:443 seguridad HIER_
NONE/- text/html
root@proxy_server:/var/log/squid# _
```

Figura 14 Logs www.facebook.com

```
1556590286.163      1 192.168.14.35 TCP_DENIED/403 4045 CONNECT embed.eltiempo.digital:443 - HIER_NO
NE/- text/html
1556590286.214      0 192.168.14.35 TCP_DENIED/403 4027 CONNECT www.eltiempo.com:443 - HIER_NONE/- t
ext/html
1556590286.241      1 192.168.14.35 TCP_DENIED/403 4045 CONNECT embed.eltiempo.digital:443 - HIER_NO
NE/- text/html
1556590286.244      0 192.168.14.35 TCP_DENIED/403 4027 CONNECT www.eltiempo.com:443 - HIER_NONE/- t
ext/html
1556590376.397      2 192.168.14.35 TCP_DENIED/403 4027 CONNECT www.eltiempo.com:443 - HIER_NONE/- t
ext/html
1556590376.401      1 192.168.14.35 TCP_DENIED/403 4045 CONNECT embed.eltiempo.digital:443 - HIER_NO
NE/- text/html
1556590376.454      0 192.168.14.35 TCP_DENIED/403 4027 CONNECT www.eltiempo.com:443 - HIER_NONE/- t
ext/html
1556590376.477      3 192.168.14.35 TCP_DENIED/403 4045 CONNECT embed.eltiempo.digital:443 - HIER_NO
NE/- text/html
1556590376.491      1 192.168.14.35 TCP_DENIED/403 4027 CONNECT www.eltiempo.com:443 - HIER_NONE/- t
ext/html
root@proxy_server:/var/log/squid#
```

Figura 15 Logs www.eltiempo.com

Como segundo punto, realizamos en la configuración del proxy la creación de un usuario con su respectiva contraseña para que al usuario final se le bloquee la navegación si no es ingresada la contraseña, de igual manera se mantiene el bloqueo del punto anterior en donde se le bloquea la navegación con cierto texto en el dominio. El bloqueo con usuario y contraseña lo podemos ver en la Figura 16, donde se evidencia en el pop up el nombre del proxy (seguridad) y la solicitud del usuario y contraseña para poder navegar.

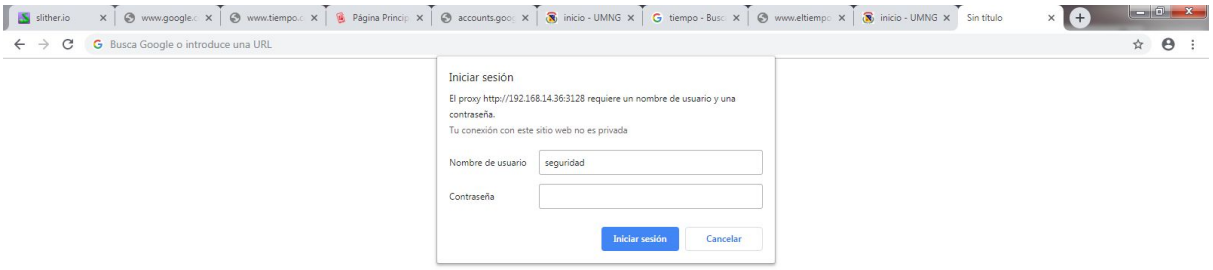


Figura 16 bloqueo con usuario

En cuanto a la configuración del throughput, dentro del archivo de configuración del squid se agregaron las líneas que se ven en la Figura 17, cuyo objetivo es limitar las conexiones simultáneas que pueden tener los usuarios hacia el proxy y su respectiva salida a internet, bloqueando de esta manera aquellas conexiones que sobrepasen la cantidad acordada.

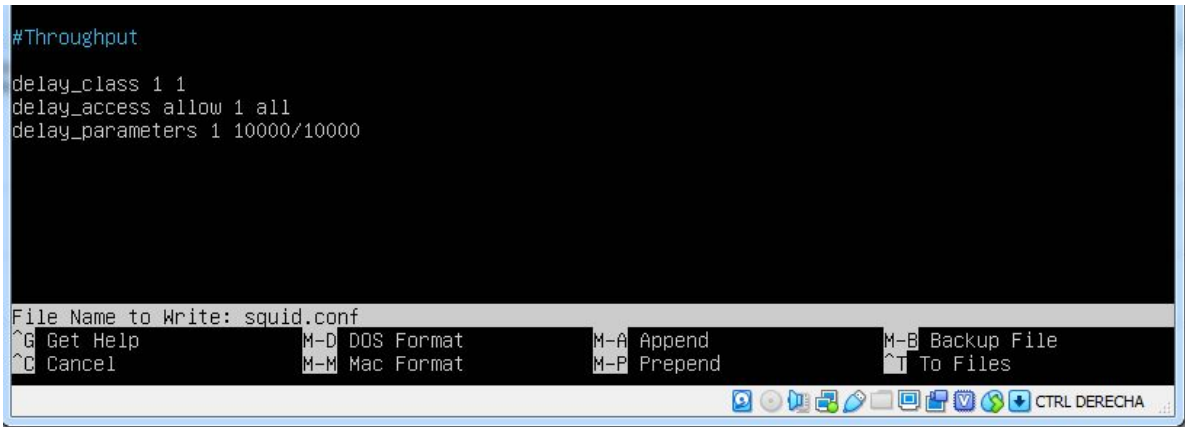


Figura 17. Bloqueo throughput

CONCLUSIONES

Para una correcta implementación de un proxy es de vital importancia definir de manera correcta las redes ya que si no se hace, puede ser inútil el proxy que hagamos ya que la máquina externa podría llegar sin ningún filtro a internet. Además, dependiendo la forma en la que se bloquee el acceso se debe tener cuidado, debido a que se pueden estar bloqueando páginas útiles para los usuarios.

Además de las restricciones de acceso, un proxy nos permite capturar toda la información del tráfico que se está generando por el uso de las máquinas cliente, esto ayuda en tener un control acerca de cómo se esta usando la red y así poder tomar más medidas y en casos específicos.

REFERENCIAS

https://www.xataka.com/especiales/maquinas-virtuales-que-son-como-funcionan-y-como-utilizarlas

Instalar apt-get http://www.kacharreando.com/ubuntu/configurar-proxy-squid/

Instalando squid
https://www.ochobitshacenunbyte.com/2014/02/18/configurar-proxy-para-nuestra-pequena-empresa-o-red-domestica-con-squid/