UT05: Instalación y configuración de servidores proxy – 3) Informe Squid de configuraciones y aplicaciones.

Nombre: Francisco Jesús García – Uceda Díaz - Albo

Curso: 2º ASIR.

Índice

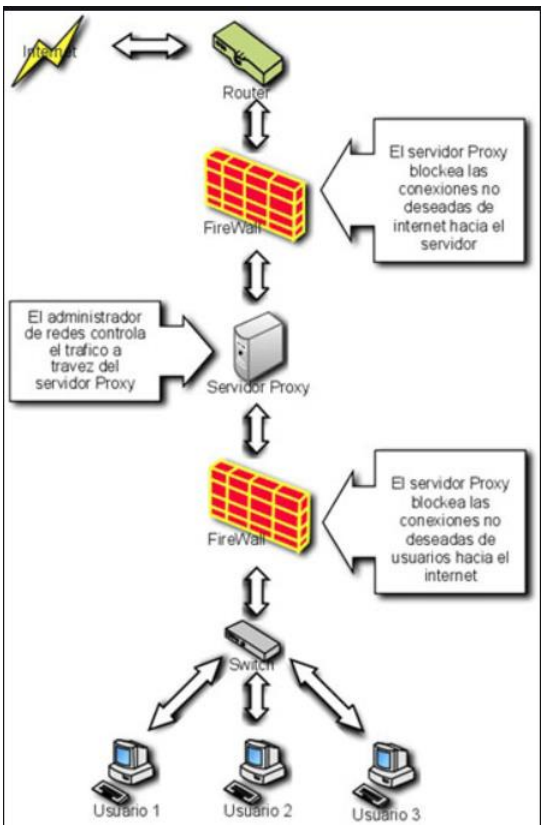
Introducción

En esta práctica aprenderemos distintas configuraciones y aplicaciones sobre Squid. Veremos configuraciones de Squid en modo transparente e inverso y aprenderemos sobre aplicaciones como DansGuardian y Servidor ICAP y su relación con el Proxy Squid.

3. Realizar un informe para:

a) configurar el servidor Proxy "Squid" en modo transparente.

Un proxy transparente combina un servidor proxy con NAT de manera que las conexiones son enrutadas dentro del proxy sin configuración por parte del cliente, y habitualmente sin que el propio cliente conozca de su existencia.



Lo primero será realizar un backup de nuestro fichero de configuración de Squid por si lo necesitamos restaurar. Para hacer el backup simplemente lo copiamos:

```
root@debian:/home/franciscojesus# cd /etc/squid/
root@debian:/etc/squid# cp squid.conf squid.conf.bak
```

Vamos a configurar nuestro Proxy con las siguientes políticas:

- Puerto Squid: http_port 3128 transparent

```
Abrir                                                    *squid.conf
                                                         /etc/squid
#                       In seconds; idle is the initial time before TCP starts
#                       probing the connection, interval how often to probe, and
#                       timeout the time before giving up.
#
#          require-proxy-header
#                       Require PROXY protocol version 1 or 2 connections.
#                       The proxy_protocol_access is required to whitelist
#                       downstream proxies which can be trusted.
#
#       If you run Squid on a dual-homed machine with an internal
#       and an external interface we recommend you to specify the
#       internal address:port in http_port. This way Squid will only be
#       visible on the internal address.
#
#

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

Configuramos también las siguientes reglas de IPTables. Activamos el IP FORWARDING en el servidor y hacemos que todo lo que salga desde la LAN hacia el exterior por el puerto 80 y 443 lo reenvie al 3218 de localhost para cachear. En este punto radica la "Magia" del proxy transparente donde los usuarios no deberán tocar nada en sus navegadores para navegar a través del Proxy Web. Esto es transparente para el usuario y no necesita hacer configuraciones especiales en su equipo:

echo 1 > /proc/sys/net/ipv4/ip_forward

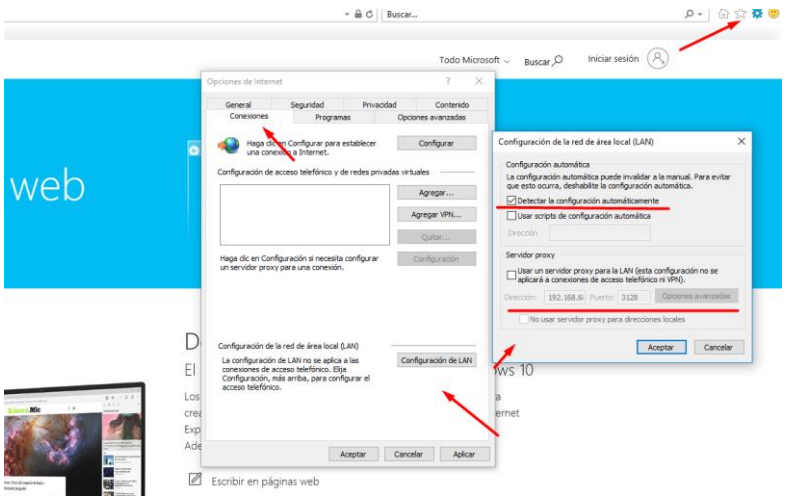
iptables -t nat -A PREROUTING -p tcp -s 172.27.1.0/24 --dport 80 -j REDIRECT --to-port 3128

iptables -t nat -A PREROUTING -p tcp -s 172.27.1.0/24 --dport 443 -j REDIRECT --to-port 3128

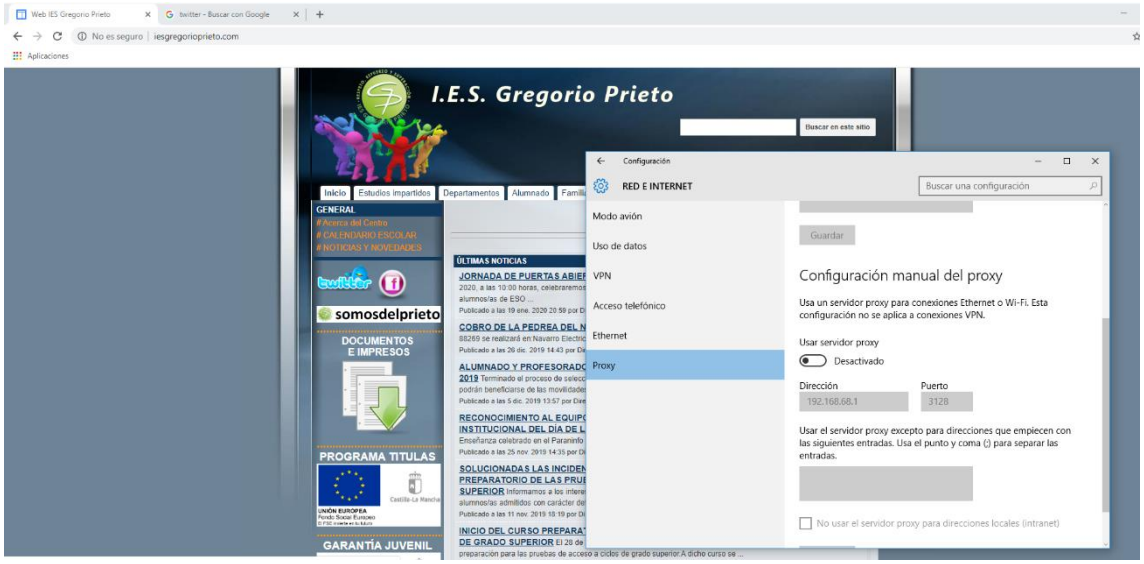
iptables -t nat -A POSTROUTING -s 172.27.1.0/24 -d 0.0.0.0/0 -o eth0 -j MASQUERADE

```
franciscojesus@debian: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
root@debian:/etc/squid# echo 1 > /proc/sys/net/ipv4/ip_forward
root@debian:/etc/squid# iptables -t nat -A PREROUTING -p tcp -s 172.27.1.0/24 --dport 80 -j REDIRECT --to-port 3128
root@debian:/etc/squid# iptables -t nat -A PREROUTING -p tcp -s 172.27.1.0/24 --dport 443 -j REDIRECT --to-port 3128
root@debian:/etc/squid# iptables -t nat -A POSTROUTING -s 172.27.1.0/24 -d 0.0.0.0/0 -o eth0 -j MASQUERADE
root@debian:/etc/squid#
```

En los equipos clientes, la ventaja de usar Squid en Modo Transparente es que no debemos configurar la dirección de nuestro proxy, ya que esto se hará de forma automática y de forma transparente en el Proxy gracias a IPTables:



Tendremos de igual manera correcta conexión aplicándose el filtrado.



b) configurar el servidor Proxy “Squid” en modo inverso (reverse) reverse.

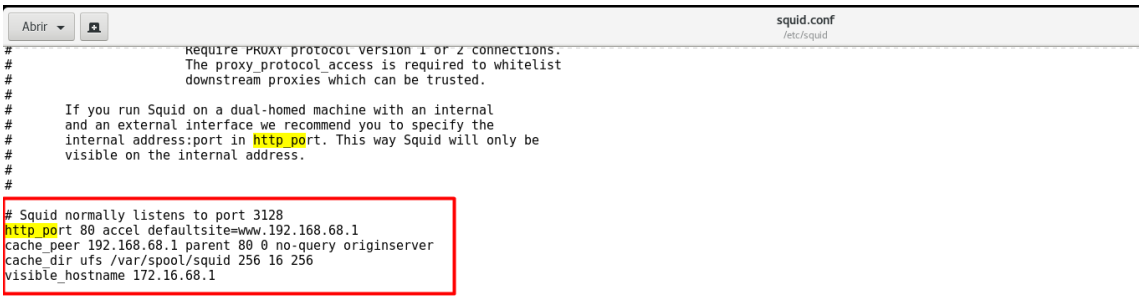
Un proxy inverso es un tipo de servidor proxy que recupera recursos en nombre de un cliente desde uno o más servidores. Estos recursos son entonces regresados al cliente como si se originaran en el propio servidor Web.

Básicamente un proxy inverso es un servidor proxy-caché "al revés". Es un servidor proxy que, en lugar de permitirles el acceso a Internet a usuarios internos, permite a usuarios de Internet acceder indirectamente a determinados servidores internos.

El servidor de proxy inverso es utilizado como un intermediario por los usuarios de Internet que desean acceder a un sitio web interno al enviar sus solicitudes indirectamente. Con un proxy inverso, el servidor web está protegido de ataques externos directos, lo cual fortalece la red interna.

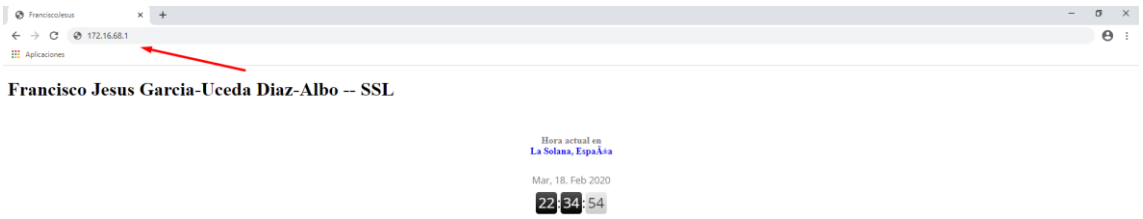
Vamos al archivo squid.conf y realizamos las siguientes configuraciones.

```
http_port 80 accel defaultsite=www.192.168.68.1
cache_peer 192.168.68.1 parent 80 0 no-query originserver
cache_dir ufs /var/spool/squid 256 16 256
visible_hostname 192.168.68.1
```

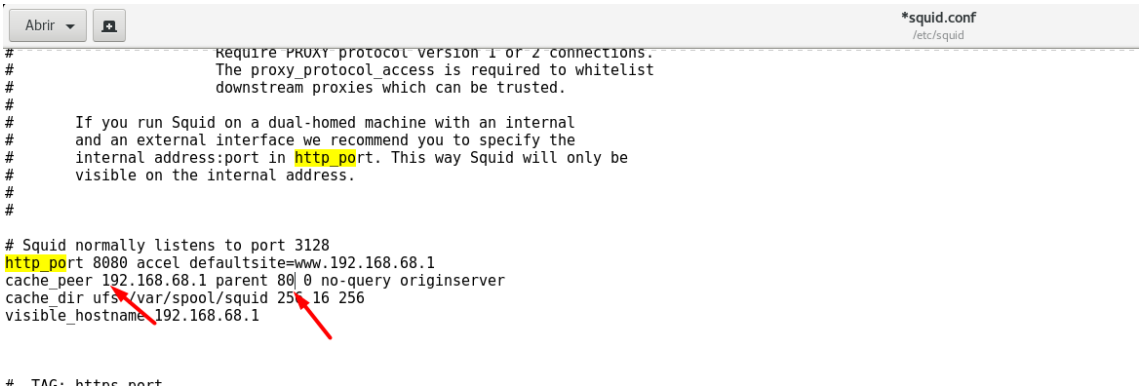


Entramos desde Internet **(usaré mi proyecto de SAD para ello, para entrar en la red interna desde mi equipo real)** y veremos cómo es el proxy quien se encarga de gestionar esa conexión y redirigirla a dicha dirección IP configurada de manera transparente para mí.

Vemos cómo funciona y Squid redirige automáticamente la petición web hacía dicho servido web (mi servidor Debian que use para las prácticas de Apache). Todo de manera transparente para el usuario.



Podemos hasta intercambiar puertos.

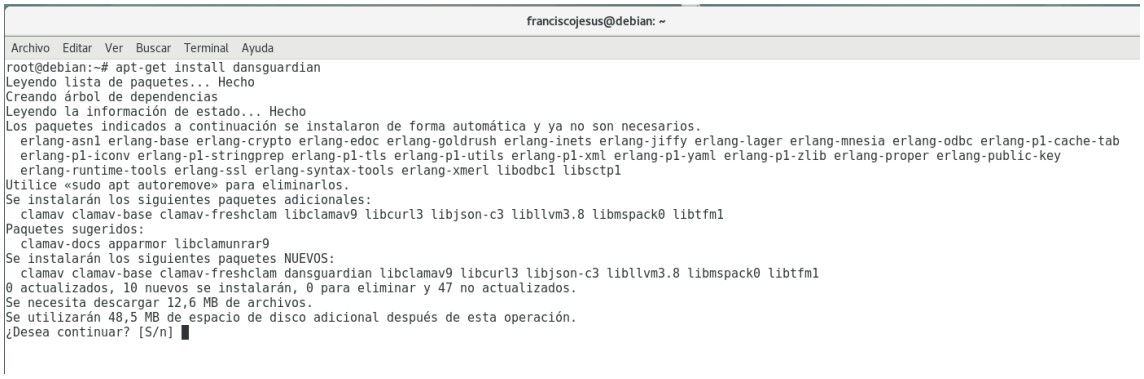


c) “Squid” + DansGuardian” http://dansguardian.org

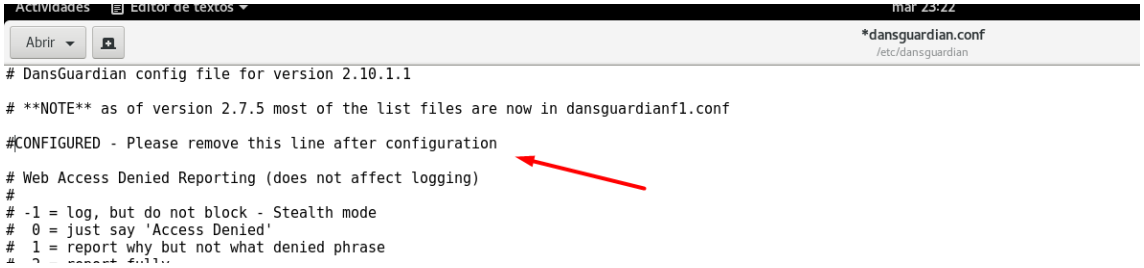
DansGuardian es un software de filtro de contenido diseñado para controlar el acceso a sitios web. Incluye un filtro de virus, importante en sistemas Windows, es usado principalmente en instituciones de educación, gobierno y empresas. Se caracteriza por su alto grado de flexibilidad y adaptación de la implementación

DansGuardian se sitúa o actúa entre el navegador cliente y el proxy, interceptando y modificando la comunicación entre ambos. De esta forma facilita la tarea de filtrado de páginas visitadas por el usuario desde el equipo cliente, cuya utilización puede ser de especial interés en el aula e incluso en el propio domicilio.

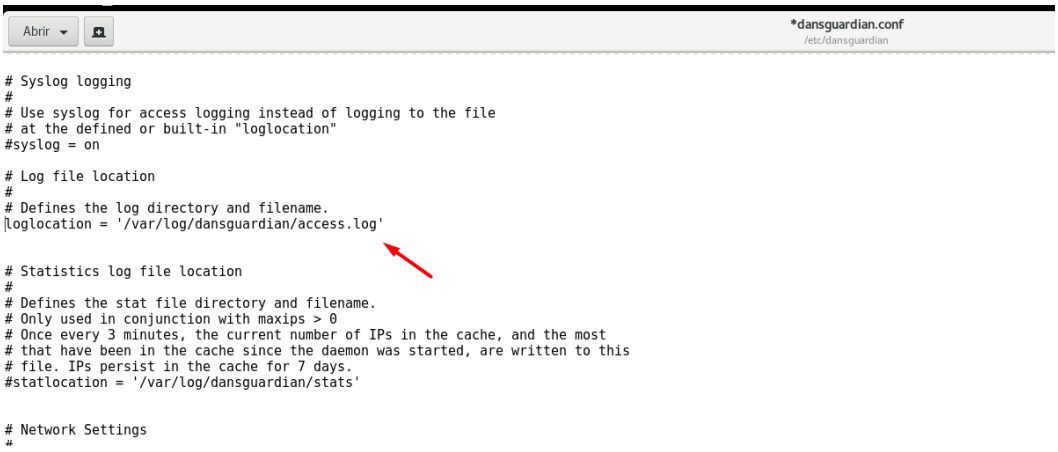
Instalamos DansGuard.



Editamos su archivo de configuración. En la línea donde dice UNCONFIGURED la dejamos CONFIGURE o comentamos toda la línea con #. Esto se hace para que el servicio pueda arrancar.



Descomentaremos la siguiente línea para poder ver los logs de DansGuardian.



Realizaremos las últimas configuraciones especificando el puerto en caso de ser otro o el puerto que filtrará las conexiones.

```
Abrir
# once every 3 minutes, the current number of IPs in the cache, and the most
# that have been in the cache since the daemon was started, are written to this
# file. IPs persist in the cache for 7 days.
#statlocation = '/var/log/dansguardian/stats'


# Network Settings
#
# the IP that DansGuardian listens on.  If left blank DansGuardian will
# listen on all IPs.  That would include all NICs, loopback, modem, etc.
# Normally you would have your firewall protecting this, but if you want
# you can limit it to a certain IP. To bind to multiple interfaces,
# specify each IP on an individual filterip line.
filterip = 192.168.68.1

# the port that DansGuardian listens to.
filterport = 8080

# the ip of the proxy (default is the loopback - i.e. this server)
proxyip = 127.0.0.1

# the port DansGuardian connects to proxy on
proxyport = 3128

# Whether to retrieve the original destination IP in transparent proxy
# setups and check it against the domain pulled from the HTTP headers.
#
# Be aware that when visiting sites which use a certain type of round-robin
```

Reiniciamos y comprobamos que funcione.

```
franciscojesus@debian: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
● dansguardian.service - LSB: dansguardian configuration
   Loaded: loaded (/etc/init.d/dansguardian; generated; vendor preset: enabled)
   Active: active (running) since Tue 2020-02-18 23:38:10 CET; 2s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 5780 ExecStart=/etc/init.d/dansguardian start (code=exited, status=0/SUCCESS)
Main PID: 5785 (dansguardian)
    Tasks: 11 (limit: 4915)
   CGroup: /system.slice/dansguardian.service
           ├─5785 /usr/sbin/dansguardian
           ├─5786 /usr/sbin/dansguardian
           ├─5787 /usr/sbin/dansguardian
           ├─5788 /usr/sbin/dansguardian
           ├─5789 /usr/sbin/dansguardian
           ├─5790 /usr/sbin/dansguardian
           ├─5791 /usr/sbin/dansguardian
           ├─5792 /usr/sbin/dansguardian
           ├─5793 /usr/sbin/dansguardian
           ├─5794 /usr/sbin/dansguardian
           └─5795 /usr/sbin/dansguardian
```

Con los pasos anteriores ya tenemos configurado DANSGUARDIAN con SQUID, los cuales por defecto filtran contenido relacionado con pornografía, páginas de drogas, entre otros.

Modificamos el archivo /etc/dansguardian/listst/bannedphraselist

Dentro de éste, se agregan las palabras o frases que deseemos bloquear; en este caso estaremos bloqueando el contenido que se relacione con las palabras: oso, perro

```
Abrir
*bannedphraselist
/etc/dansguardian/lists
# BANNEDPHRASELIST - INSTRUCTIONS FOR USE
#
# To block any page with the word "sex".
# < sex >

<oso>,<perro>,<sex>

#
# To block any page with words that contain the string "sex". (ie. sexual)
# <sex>
```

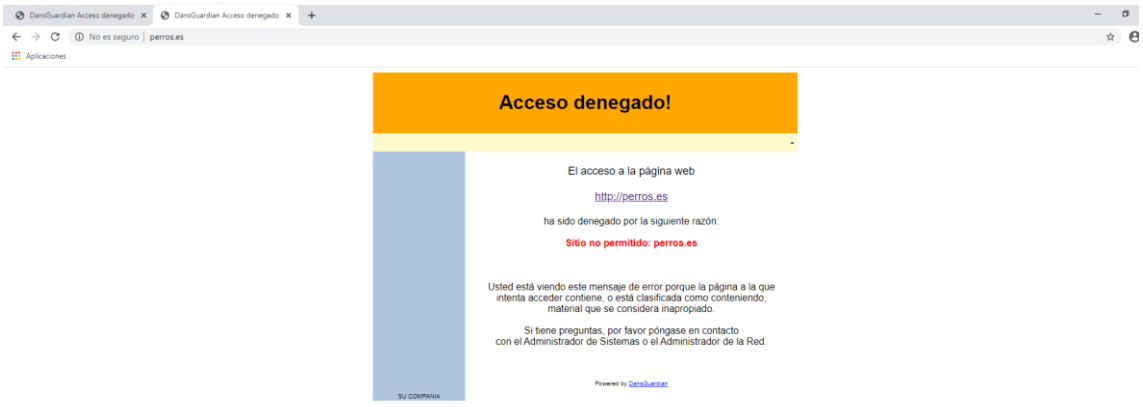
NOTA: Es importante que, si queremos un mejor filtrado, seamos específicos con las diferentes formas de poner una palabra dentro de los indicadores <> ya que, por ejemplo, <oso> filtrará solamente la palabra 'oso'; < oso> filtrará frases que terminen con 'oso'; <oso > filtrará frases que comiencen con 'oso' y < oso > filtrará frases que contengan en medio la palabra 'oso'. (La diferencia radica en poner o no y dónde, el carácter de espacio).

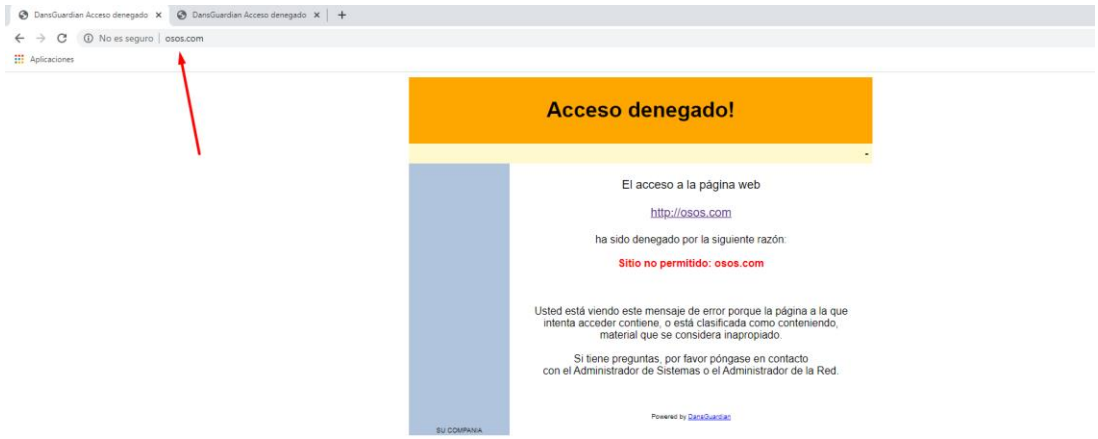
De esta forma, tenemos configurado DANSGUARDIAN y SQUID. Sólo nos queda hacer unas pruebas para verificar que las configuraciones hayan quedado correctamente aplicadas.

Lo primero que haremos es redirigir le tráfico del puerto 3128 al 8080 para así poder filtrar el tráfico mediante DansGuard. Gracias a esto no tendremos que tocar nada en los clientes.

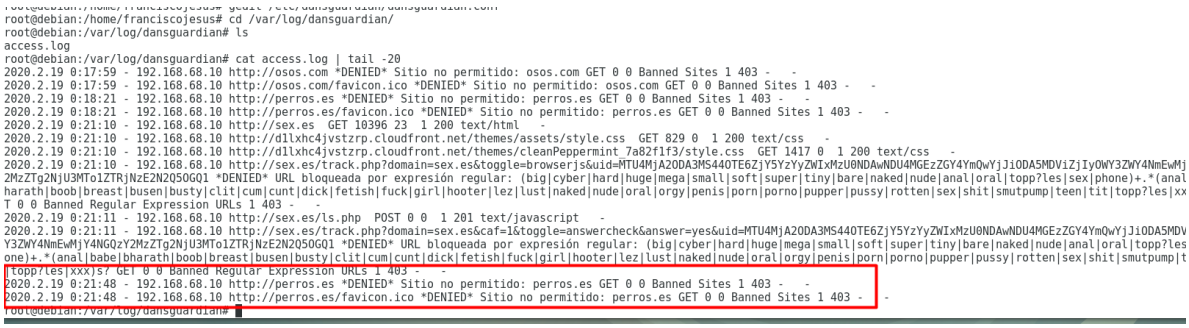
```
iptables -t nat -A PREROUTING -i enp0s8 -s 192.168.2.0/24 -d 0.0.0.0/0.0.0.0 -p tcp --dport 80 -j REDIRECT --to-port 3128

iptables -t nat -A PREROUTING -i enp0s8 -s 192.168.2.0/24 -d 0.0.0.0/0.0.0.0 -p tcp --dport 433 -j REDIRECT --to-port 3128

iptables -t nat -A PREROUTING -i enp0s8 -p tcp --dport 3128 -j REDIRECT --to-port 8080
```

enp0s8 es la red interna de mi equipo actúa de firewall. Podemos ver que si buscamos ahora el link que hemos puesto para bloquear DansGuard lo bloquea correctamente.



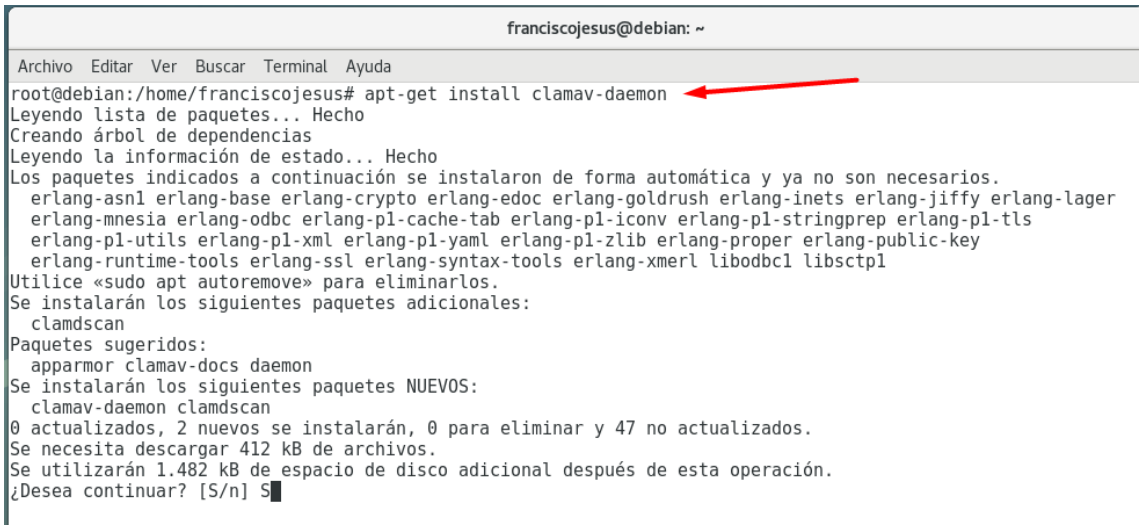


Podemos ver en los logs de DansGuardian como bloquea correctamente a los clientes.

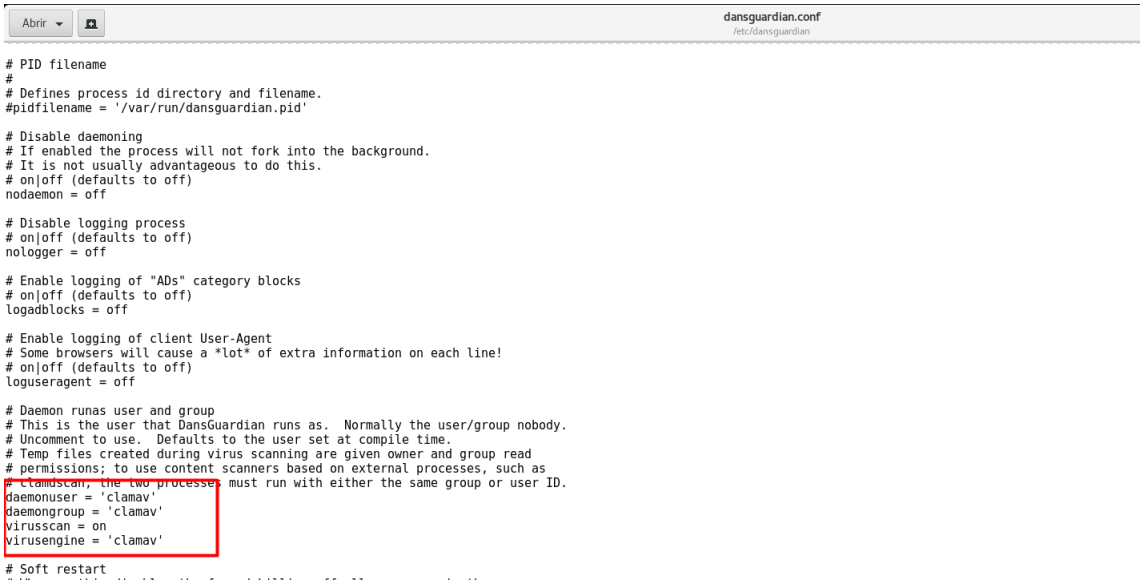


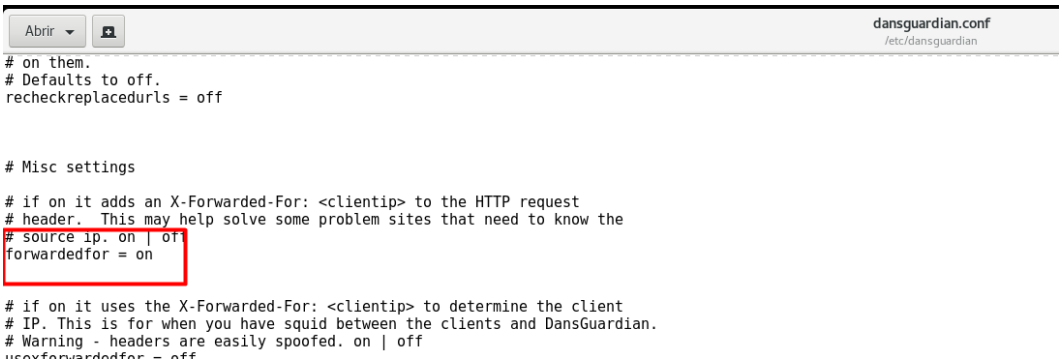
El siguiente paso es algo maravilloso. Configuraremos DansGuard para usar un antivirus y así detectar amenazas de manera online para mayor seguridad del cliente.

Lo primero que haremos es instalar clamav-daemon, será el antivirus que usemos.

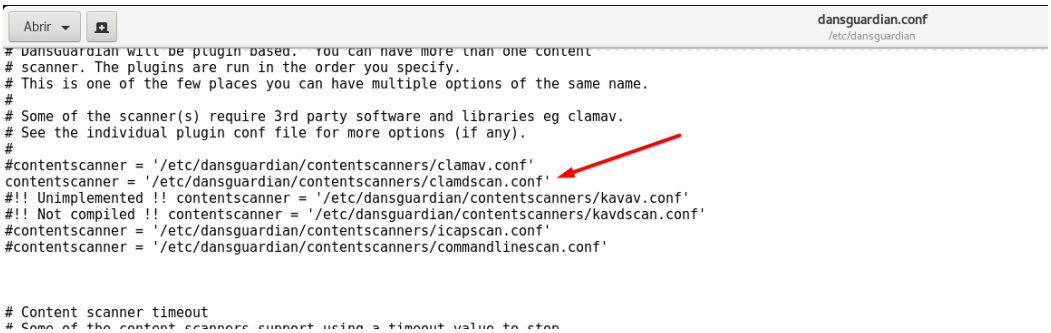


Una vez realizado esto vamos a */etc/dansguardian/dansguardian.conf* y lo configuraremos para usar el antivirus.





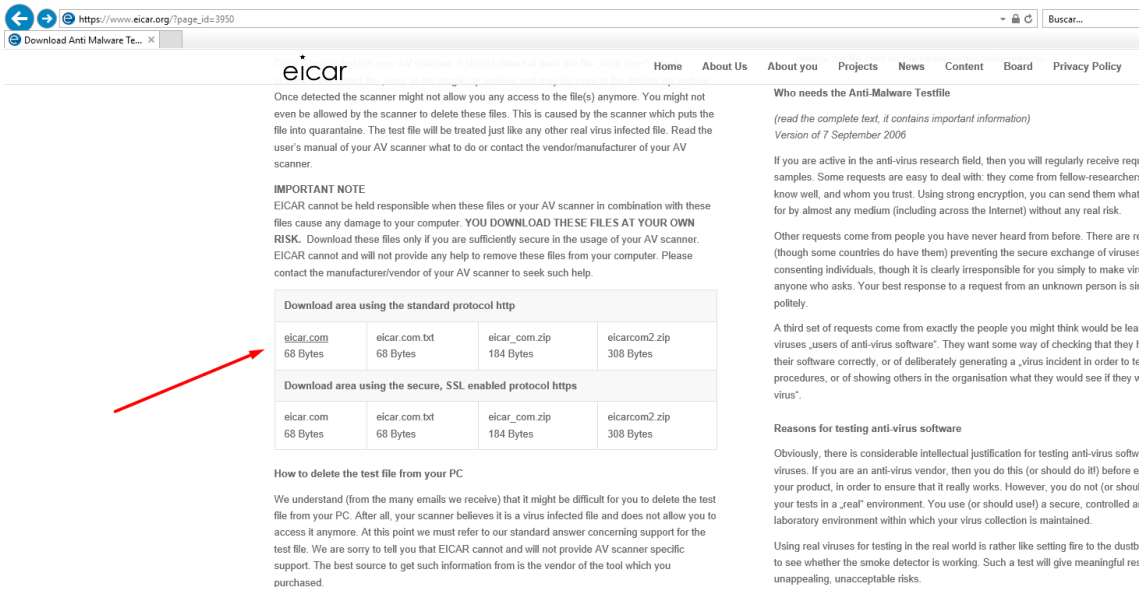
Descomentamos la siguiente línea.



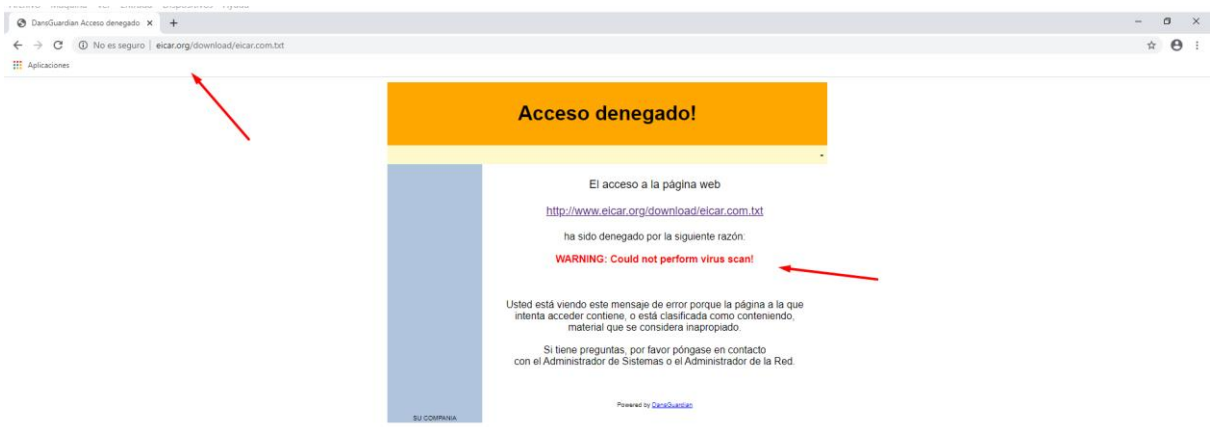
Una vez realizado esto y teniendo el Proxy Squid activo y DansGuardian activo volvemos al cliente y podemos empezar a buscar, podemos ver como graciosamente DansGuardian detecta la página principal de Internet Explorer como un virus.

Voy a la página de EICAR, para quien no se acuerde, la prueba EICAR es una prueba sirve para probar la respuesta de los programas antivirus en un equipo.

Probaremos primeramente si detecta la página eicar.com, esta página lo que te hace es descargar un .exe llamado eicar.exe que es el falso virus.



Vemos como nos bloquea correctamente la página eicar.com, protege correctamente evitando descargar el archivo eicar.exe. Podemos observar cómo nos avisa que la página es un virus.



Funciona correctamente en cualquier otro navegador.

d) “Squid” + Servidor ICAP (Internet Content Adaptation Protocol).

El Protocolo de Adaptación de Contenidos de Internet (o ICAP) es un protocolo de red abierto y público, originado para la redirección de contenidos con fines de filtrado y conversión.

Permite el uso de antivirus, filtrado de contenidos, traducción dinámica de páginas, inserción automática de anuncios, compresión de HTML, etc. Los servicios basados en ICAP tienen dos posibilidades de implantación, dependiendo de si la redirección al servidor de filtrado se realiza inmediatamente después de la solicitud del cliente (modo “request”) o tras la respuesta del servidor de destino (modo “response”). Normalmente se asocia el filtrado de acceso al modo solicitud y el filtrado de contenido al modo respuesta. ICAP permite una nueva clase de servicios al permitir que los propietarios de sitios ofrezcan aplicaciones Web más cercanas al usuario.

Squid trae incorporado su propio servidor ICAP. Configuramos el archivo de configuración de Squid para usar ICAP.

```
icap_enable on

icap_service service_req reqmod_precache 1 icap://127.0.0.1:1344/request

icap_class class_req service_req

icap_access class_req allow all

icap_service service_resp respmod_precache 0 icap://127.0.0.1:1344/response

icap_class class_resp service_resp

icap_access class_resp allow all
```

```
#
#       Remove from squid.conf to inherit the current ulimit setting.
#
#       Note: Changing this requires a restart of Squid. Also
#       not all I/O types supports large values (eg on Windows).
#Default:
# Use operating system limits set by ulimit.


icap_enable on

icap_service service_req reqmod_precache 1 icap://127.0.0.1:1344/request
icap_class class_req service_req
icap_access class_req allow all

icap_service service_resp respmod_precache 0 icap://127.0.0.1:1344/response
icap_class class_resp service_resp
icap_access class_resp allow all
```

*Error con c-icap y squid 3.5 en Debian 9 y 10: Según los foros oficiales de Red-Hat, c-icap falla en la versión de squid 3.4 - 3.5 que es la que actualmente uso. He intentado solucionarlo y toda solución que provee internet no he conseguido que funcione. Básicamente nunca arranca c-icap.

icap support has been disabled on squid 3.5.20-2.el7

Updated January 25 2018 at 9:21 AM - English

Issue

The icap support has been disabled on squid 3.5.20-2. The previous version, squid-3.3.8-26.el7_2.4 has configured with '--enable-icap-client' option but it has changed to '--disable-icap-client' on squid 3.5.20-2.el7.

Raw

```
# squid -v
Squid Cache: Version 3.5.20
Service Name: squid
configure options:  '--build=x86_64-redhat-linux-gnu' '--host=x86_64-redhat-linux-gnu' '--program-prefix=' '--prefix=/usr' '--exec-
prefix=/usr' '--bindir=/usr/bin' '--sbindir=/usr/sbin' '--sysconfdir=/etc' '--datadir=/usr/share' '--includedir=/usr/include' '--
libdir=/usr/lib64' '--libexecdir=/usr/libexec' '--sharedstatedir=/var/lib' '--mandir=/usr/share/man' '--infodir=/usr/share/info' '--disable-
strict-error-checking' '--exec_prefix=/usr' '--libexecdir=/usr/lib64/squid' '--localstatedir=/var' '--datadir=/usr/share/squid' '--
sysconfdir=/etc/squid' '--with-logdir=$(localstatedir)/log/squid' '--with-pidfile=$(localstatedir)/run/squid.pid' '--disable-dependency-
tracking' '--enable-eui' '--enable-follow-x-forwarded-for' '--enable-auth' '--enable-auth-basic=DB,LDAP,MSNT-multi-
domain,NCSA,NIS,PAM,POP3,RADIUS,SASL,SMB,SMB_LM,getpwnam' '--enable-auth-ntlm=smb_lm,fake' '--enable-auth-digest=file,LDAP,eDirectory' '--
enable-auth-negotiate=kerberos' '--enable-external-acl-helpers=file_userip,LDAP_group,time_quota,session,unix_group,wbinfo_group' '--enable-
cache-digests' '--enable-cachemgr-hostname=localhost' '--enable-delay-pools' '--enable-epoll' '--enable-ident-lookups' '--enable-linux-
netfilter' '--enable-removal-policies=heap,lru' '--enable-snmp' '--enable-ssl-crtd' '--enable-storeio=aufs,diskd,ufs' '--enable-wccpv2' '--
enable-esi' '--enable-ecap' '--with-aio' '--with-default-user=squid' '--with-dl' '--with-openssl' '--with-pthreads' '--disable-arch-native'
'--disable-icap-client' 'build_alias=x86_64-redhat-linux-gnu' 'host_alias=x86_64-redhat-linux-gnu' 'CFLAGS=-O2 -g -pipe -Wall -Wp,-
D_FORTIFY_SOURCE=2 -fexceptions -fstack-protector-strong --param=ssp-buffer-size=4 -grecord-gcc-switches   -m64 -mtune=generic -fpie'
'LDFLAGS=-Wl,-z,relro  -pie -Wl,-z,relro -Wl,-z,now' 'CXXFLAGS=-O2 -g -pipe -Wall -Wp,-D_FORTIFY_SOURCE=2 -fexceptions -fstack-protector-
strong --param=ssp-buffer-size=4 -grecord-gcc-switches   -m64 -mtune=generic -fpie'
'PKG_CONFIG_PATH=:/usr/lib64/pkgconfig:/usr/share/pkgconfig'
```

It was enabled on squid 3.3.8-26.el7_2.4.