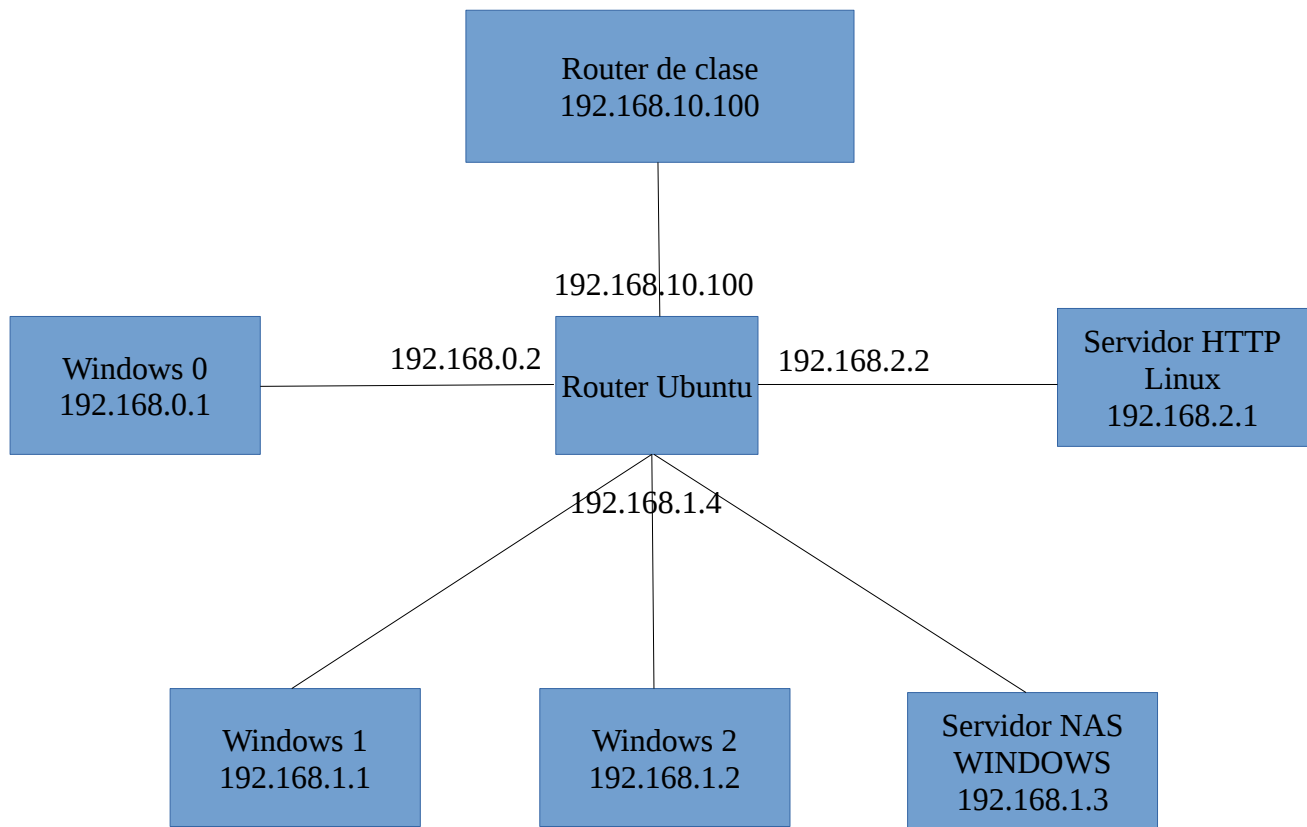


PRÁCTICA DE FIREWALL



Rubén Irles Esclapez
2ºG SMR 2016/2017
IES SEVERO OCHOA



Primero de todo, vamos al router ubuntu y tenemos que activar el FORWARD de forma permanente.

Para hacer esto, tenemos que ir al fichero: `/etc/sysctl.conf` y cambiamos la línea que está marcada

en la siguiente imagen

```
GNU nano 2.5.3          Archivo: /etc/sysctl.conf

#
# /etc/sysctl.conf - Configuration file for setting system variables
# See /etc/sysctl.d/ for additional system variables.
# See sysctl.conf (5) for information.
#

#kernel.domainname = example.com

# Uncomment the following to stop low-level messages on console
#kernel.printk = 3 4 1 3

#####3
# Functions previously found in netbase
#

# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1

# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1

# Uncomment the next line to enable packet forwarding for IPv6
# Enabling this option disables Stateless Address Autoconfiguration
# based on Router Advertisements for this host

^G Ver ayuda  ^O Guardar   ^W Buscar    ^K Cortar Text^J Justificar  ^C Posición   ^Y Pág. ant.
^X Salir      ^R Leer fich.^_ Reemplazar  ^U Pegar txt  ^T Ortografía ^_ Ir a línea  ^U Pág. sig.
```

Una vez que hayamos hecho esto, tenemos que crear las reglas de iptables para permitir o denegar todo el tráfico de nuestra red.

Como son muchas reglas, utilizaremos un script, y de esta forma solamente lo ejecutaremos y ya lo tendremos todo configurado.

En las siguientes capturas de pantalla veremos el script creado con líneas comentadas a modo de explicación para saber que hace cada comando introducido.

```
GNU nano 2.5.3 Archivo: iptables.sh

#!/bin/bash

clear

#Limpiamos el filter, la nat y mangle.
iptables -F
iptables -X
iptables -Z
iptables -t nat -F
iptables -t nat -X
iptables -t nat -Z
iptables -t mangle -F
iptables -t mangle -X
iptables -t mangle -Z

#Denegamos todas las conexiones
iptables -P FORWARD DROP
iptables -P INPUT DROP
iptables -P OUTPUT DROP

#Activar nat para comunicarnos con el router de clase
iptables -t nat -A POSTROUTING -o enp0s10 -j MASQUERADE

#Permitir el tráfico de la red roja hacia internet
iptables -A FORWARD -i enp0s3 -o enp0s10 -j ACCEPT

#Permitir el tráfico desde la red roja hacia el HTTP en la red verde solo por el puerto 80
iptables -A FORWARD -i enp0s3 -o enp0s9 -p tcp --dport 80 -j ACCEPT

#Permitir todo el tráfico hacia la red roja (XP sin seguridad)
iptables -A FORWARD -o enp0s3 -j ACCEPT

^G Ver ayuda  ^O Guardar   ^W Buscar    ^K Cortar Text^J Justificar ^C Posición  ^Y Pág. ant.
^X Salir      ^R Leer fich.^_ Reemplazar  ^U Pegar txt  ^T Corrector ^_ Ir a línea  ^U Pág. sig.
```

```
GNU nano 2.5.3 Archivo: iptables.sh

iptables -P INPUT DROP
iptables -P OUTPUT DROP

#Activar nat para comunicarnos con el router de clase
iptables -t nat -A POSTROUTING -o enp0s10 -j MASQUERADE

#Permitir el tráfico de la red roja hacia internet
iptables -A FORWARD -i enp0s3 -o enp0s10 -j ACCEPT

#Permitir el tráfico desde la red roja hacia el HTTP en la red verde solo por el puerto 80
iptables -A FORWARD -i enp0s3 -o enp0s9 -p tcp --dport 80 -j ACCEPT

#Permitir todo el tráfico hacia la red roja (XP sin seguridad)
iptables -A FORWARD -o enp0s3 -j ACCEPT

#Permitir el tráfico a la red verde solo si ésta lo ha pedido (Windows y NAS)
iptables -A FORWARD -m state --state RELATED,ESTABLISHED -o enp0s8 -j ACCEPT

#Permitir que el ordenador 192.168.1.1 pueda acceder a la red azul (HTTP)
iptables -A FORWARD -s 192.168.1.1 -i enp0s9 -p tcp --dport 20 -j ACCEPT
iptables -A FORWARD -s 192.168.1.1 -i enp0s9 -p tcp --dport 21 -j ACCEPT
iptables -A FORWARD -s 192.168.1.1 -i enp0s9 -p tcp --dport 22 -j ACCEPT

#Permitir el tráfico de la red verde a internet
iptables -A FORWARD -i enp0s8 -o enp0s10 -j ACCEPT

#Permitir el tráfico de internet hacia la red verde
iptables -A FORWARD -i enp0s10 -o enp0s8 -j ACCEPT

#Permitir el tráfico de la red azul a internet
iptables -A FORWARD -i enp0s9 -o enp0s10 -j ACCEPT

^G Ver ayuda  ^O Guardar   ^W Buscar    ^K Cortar Text^J Justificar ^C Posición  ^Y Pág. ant.
^X Salir      ^R Leer fich.^_ Reemplazar  ^U Pegar txt  ^T Corrector ^_ Ir a línea  ^U Pág. sig.
```

```
GNU nano 2.5.3          Archivo: iptables.sh

#Permitir que el ordenador 192.168.1.1 pueda acceder a la red azul (HTTP)
iptables -A FORWARD -s 192.168.1.1 -i enp0s9 -p tcp --dport 20 -j ACCEPT
iptables -A FORWARD -s 192.168.1.1 -i enp0s9 -p tcp --dport 21 -j ACCEPT
iptables -A FORWARD -s 192.168.1.1 -i enp0s9 -p tcp --dport 22 -j ACCEPT

#Permitir el tráfico de la red verde a internet
iptables -A FORWARD -i enp0s8 -o enp0s10 -j ACCEPT

#Permitir el tráfico de internet hacia la red verde
iptables -A FORWARD -i enp0s10 -o enp0s8 -j ACCEPT

#Permitir el tráfico de la red azul a internet
iptables -A FORWARD -i enp0s9 -o enp0s10 -j ACCEPT

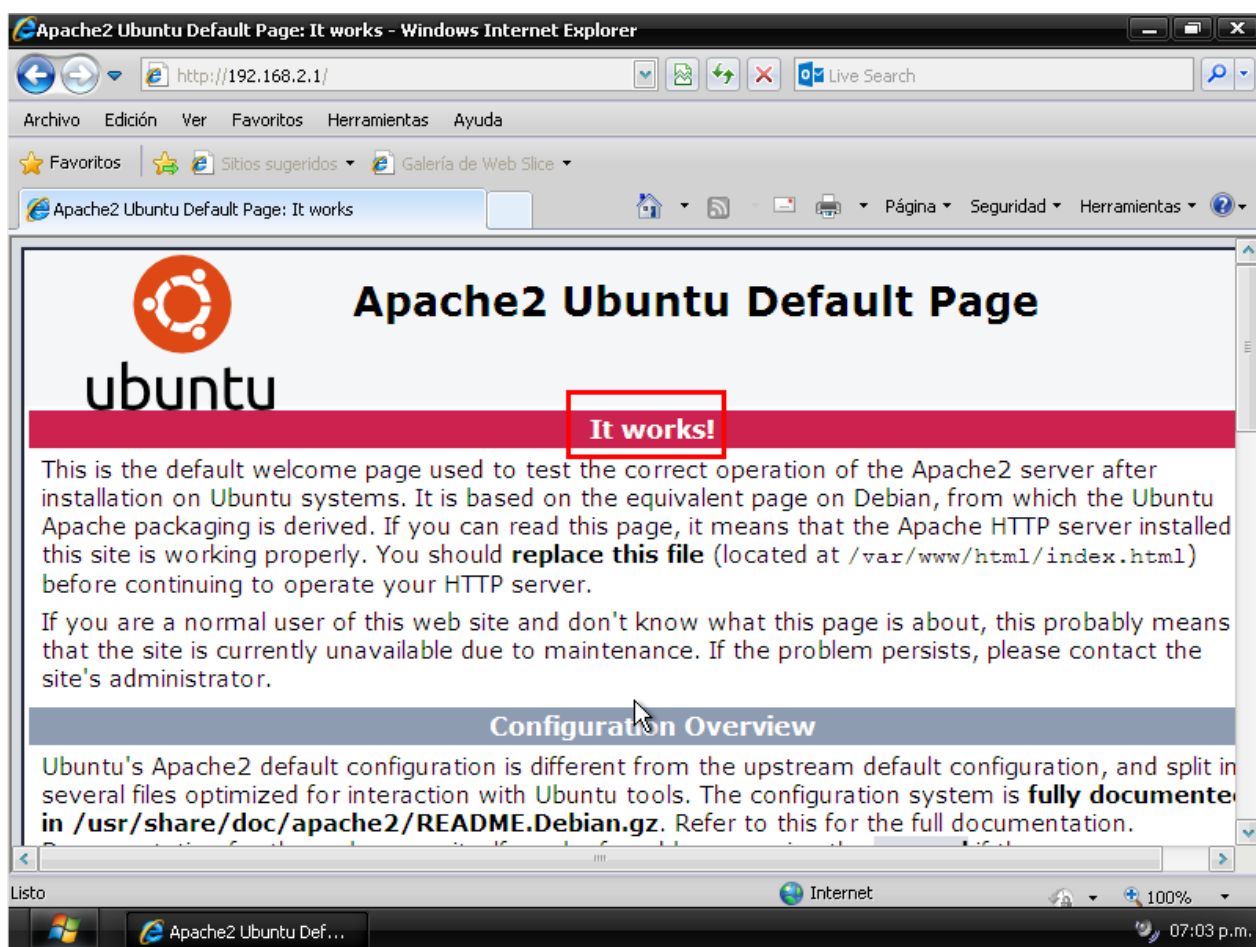
#Permitir el tráfico de internet hacia la red azul pero sólo por los puertos 80 y 443
iptables -A FORWARD -i enp0s10 -o enp0s9 -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -i enp0s10 -o enp0s9 -p tcp --dport 443 -j ACCEPT

^G Ver ayuda  ^O Guardar    ^W Buscar     ^K Cortar Text^J Justificar  ^C Posición   ^Y Pág. ant.
^X Salir      ^R Leer fich. ^_ Reemplazar  ^U Pegar txt  ^T Corrector  ^_ Ir a línea  ^U Pág. sig.
```

Ahora tenemos que instalar el apache2 en nuestro servidor http

```
root@ubuntu:/home/perico# sudo apt-get install apache2
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
apache2 ya está en su versión más reciente (2.4.18-2ubuntu3.1).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 130 no actualizados.
root@ubuntu:/home/perico#
```

Y comprobamos que funciona conectándonos desde una máquina xp



Volvemos al router ubuntu y instalamos el squid y el dansguardian:

```
root@ubuntu:/home/perico# apt-get install squid dansguardian
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
dansguardian ya está en su versión más reciente (2.10.1.1-5.1build1).
squid ya está en su versión más reciente (3.5.12-1ubuntu7.3).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 90 no actualizados.
root@ubuntu:/home/perico# _
```

Ahora tenemos que entrar en el archivo de configuración “/etc/squid/squid.conf”

Y buscar http_acces deny all para encontrar las siguientes líneas que hemos de modificar como se ve en la imagen de la siguiente página:

```
GNU nano 2.5.3 Archivo: /etc/squid/squid.conf

# We strongly recommend the following be uncommented to protect innocent
# web applications running on the proxy server who think the only
# one who can access services on "localhost" is a local user
#http_access deny to_localhost
#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
#http_access allow localnet
#http_access allow localhost

acl redroja src 192.168.0.0/24
acl redverde src 192.168.1.0/24
acl redazul src 192.168.2.0/24

acl bad_url dstdomain /etc/squid/bad-sites.acl

# And finally deny all other access to this proxy

http_access deny bad_url
http_access allow redroja
http_access allow redverde
http_access allow redazul

http_access deny all

# TAG: adapted_http_access

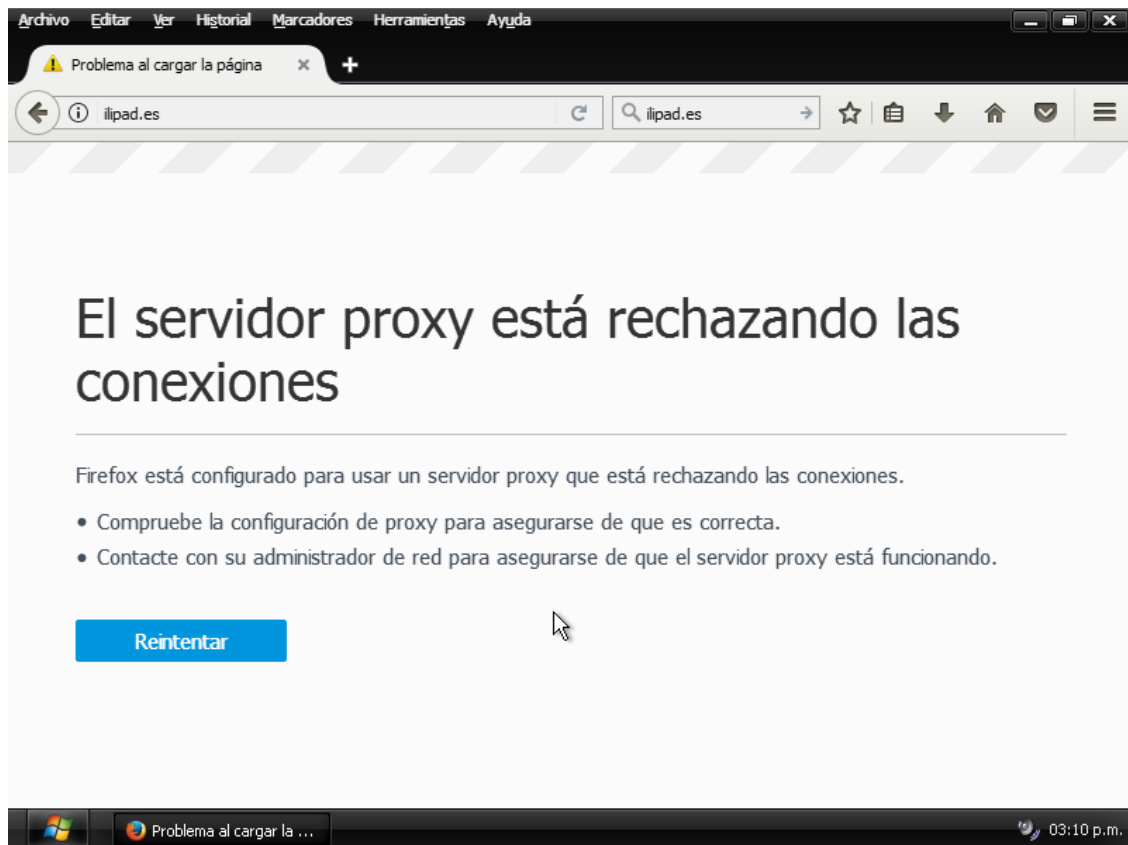
root@ubuntu:/home/perico#
```

Después tenemos que crear el fichero bad-sites.acl y añadimos las páginas a las que no queremos permitir el acceso como se ve en la imagen:

```
GNU nano 2.5.3 Archivo: bad-sites.acl

.msn.com
.ilipad.es

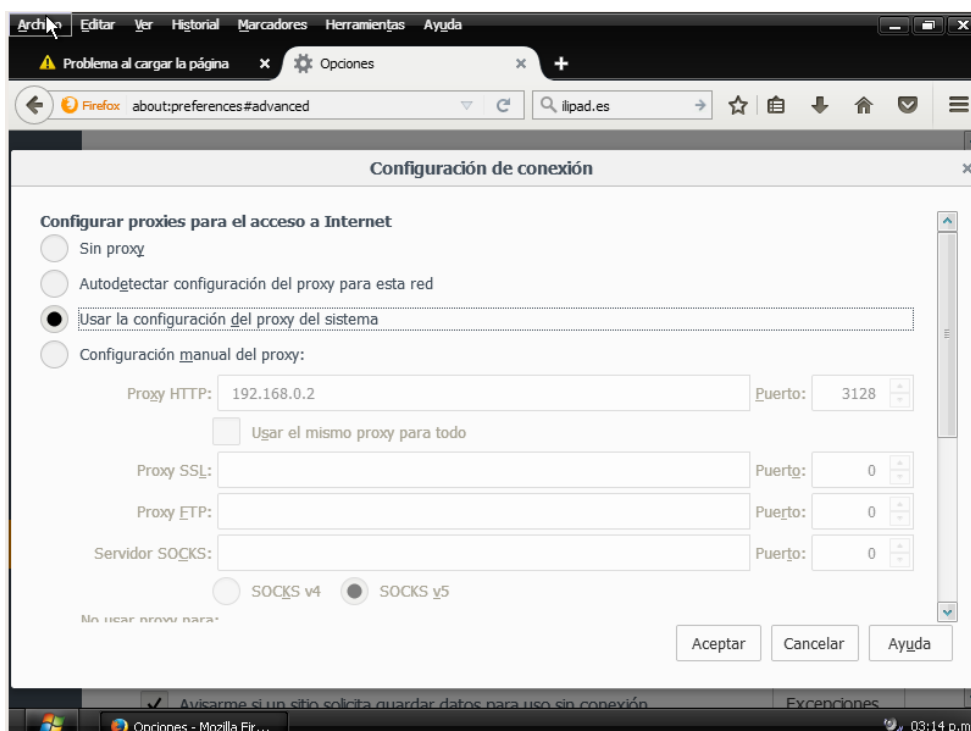
root@ubuntu:/etc/squid# _
```



Ahora escribimos transparent después del puerto 3128

```
GNU nano 2.5.3          Archivo: /etc/squid/squid.conf          Modificado
#
#       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
#
# TAG: https_port
# Note: This option is only available if Squid is rebuilt with the
#       --with-openssl
#
# Usage:  [ip:]port cert=certificate.pem [key=key.pem] [model] [options...]
#
# The socket address where Squid will listen for client requests made
# over TLS or SSL connections. Commonly referred to as HTTPS.
#
# This is most useful for situations where you are running squid in
# accelerator mode and you want to do the SSL work at the accelerator level.
#
# You may specify multiple socket addresses on multiple lines,
#
# Ver ayuda  Guardar  Buscar  Cortar Text  Justificar  Posición  Pág. ant.
# Salir      Leer fich. Reemplazar  Pegar txt  Ortografía  Ir a línea  Pág. sig.
```


Volvemos a dejar la configuración del proxy del XP en "usar la configuración del proxy del sistema"



Ahora configuramos el dansguardian modificando el fichero de configuración /etc/dansguardian/dansguardian.conf

```
GNU nano 2.5.3      Archivo: /etc/dansguardian/dansguardian.conf      Modificado
# DansGuardian config file for version 2.10.1.1
# **NOTE** as of version 2.7.5 most of the list files are now in dansguardianf1.conf
# INCONFIGURED - Please remove this line after configuration
# Web Access Denied Reporting (does not affect logging)
#
# -1 = log, but do not block - Stealth mode
# 0 = just say 'Access Denied'
# 1 = report why but not what denied phrase
# 2 = report fully
# 3 = use HTML template file (accessdeniedaddress ignored) - recommended
#
reportinglevel = 0
#
# The HTML dir where languages are stored for internationalisation.
# The HTML template within this dir is only used when reportinglevel
# is set to 3. When used, DansGuardian will display the HTML file instead of
# using the perl cgi script. This option is faster, cleaner
# and easier to customise the access denied page.
# The language file is used no matter what setting however.
#
languagedir = '/etc/dansguardian/languages'
# language to use from languagedir.
language = 'spanish'
# Logging Settings
#
# 0 = none 1 = just denied 2 = all text based 3 = all requests
loglevel = 2
^G Ver ayuda  ^O Guardar  ^W Buscar  ^K Cortar Text  ^J Justificar  ^C Posición  ^Y Pág. ant.
^X Salir      ^R Leer fich.  ^E Reemplazar  ^U Pegar txt  ^T Ortografía  ^I Ir a línea  ^U Pág. sig.
```

```
GNU nano 2.5.3      Archivo: /etc/dansguardian/dansguardian.conf      Modificado

# Statistics log file location
#
# Defines the stat file directory and filename.
# Only used in conjunction with maxips > 0
# 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 = 127.0.0.1

# the port that DansGuardian listens to.
filterport = 127.0.0.1

# 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

^G Ver ayuda  ^O Guardar   ^W Buscar    ^K Cortar Text^J Justificar  ^C Posición   ^Y Pág. ant.
^X Salir      ^R Leer fich.^_ Reemplazar  ^U Pegar txt  ^T Ortografía ^_ Ir a línea  ^V Pág. sig.
```