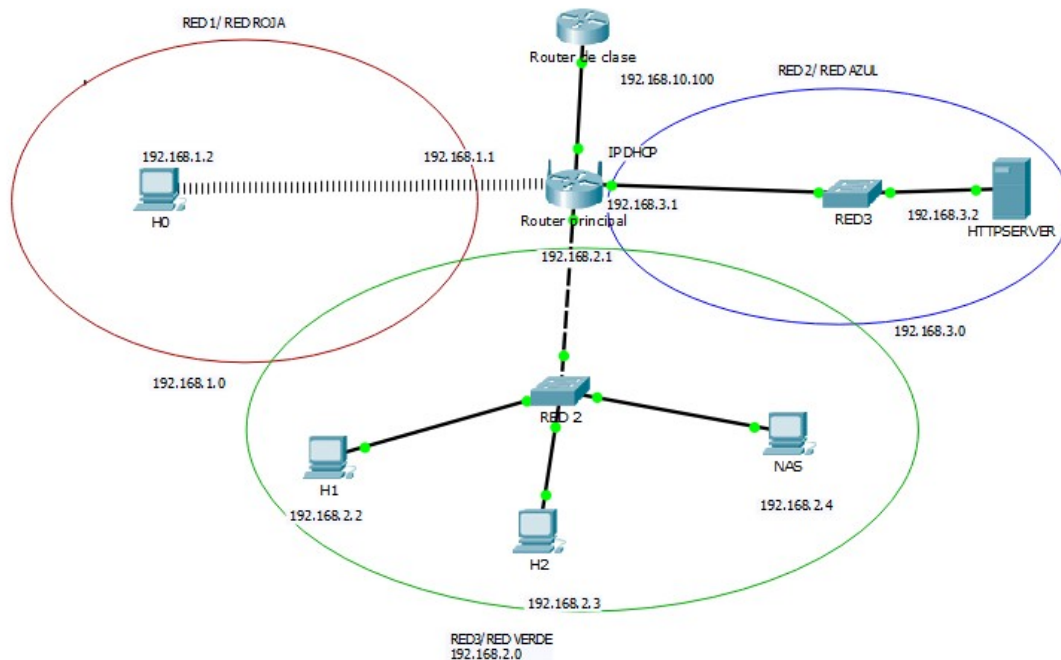


# **Trabajo Firewall de router**

**Por:  
Antonio Quiles Sempere**

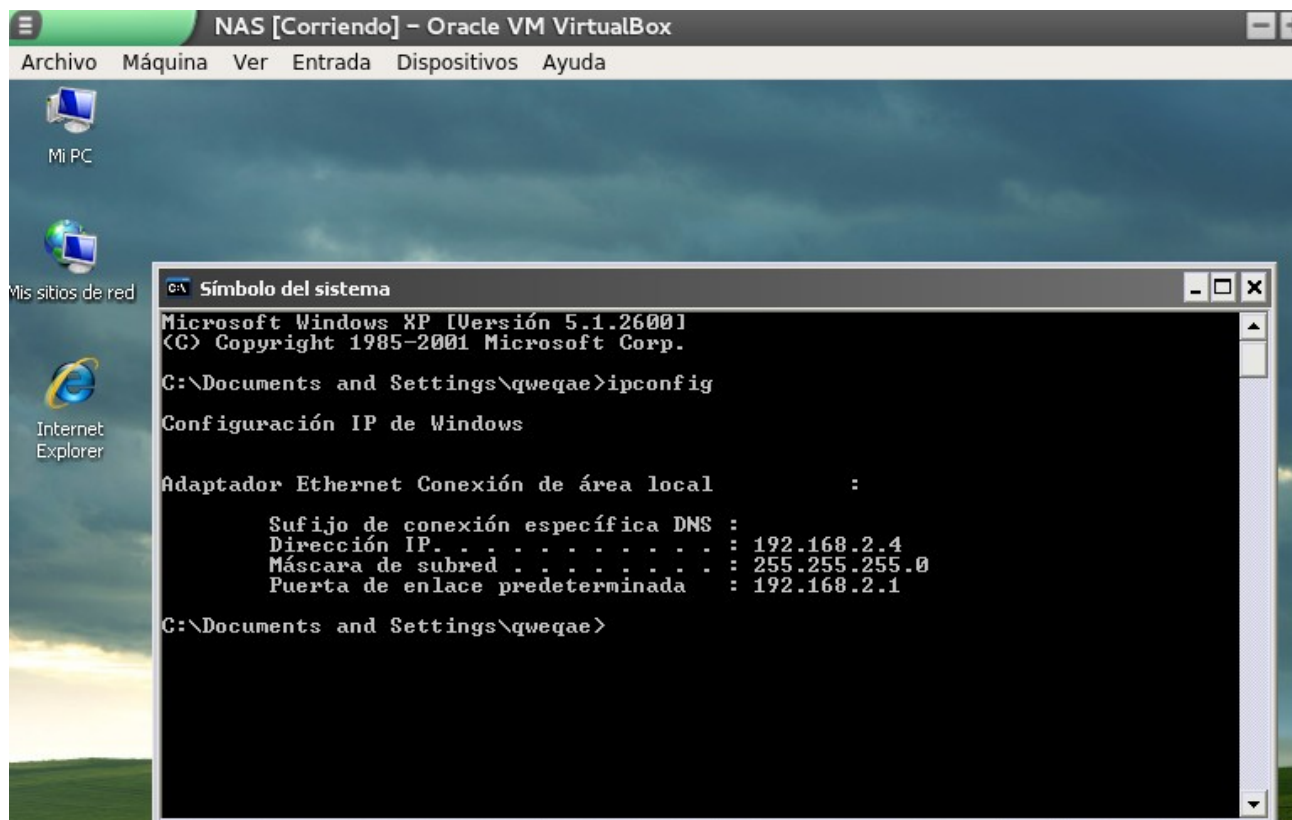


## Diagrama de la red de la empresa:

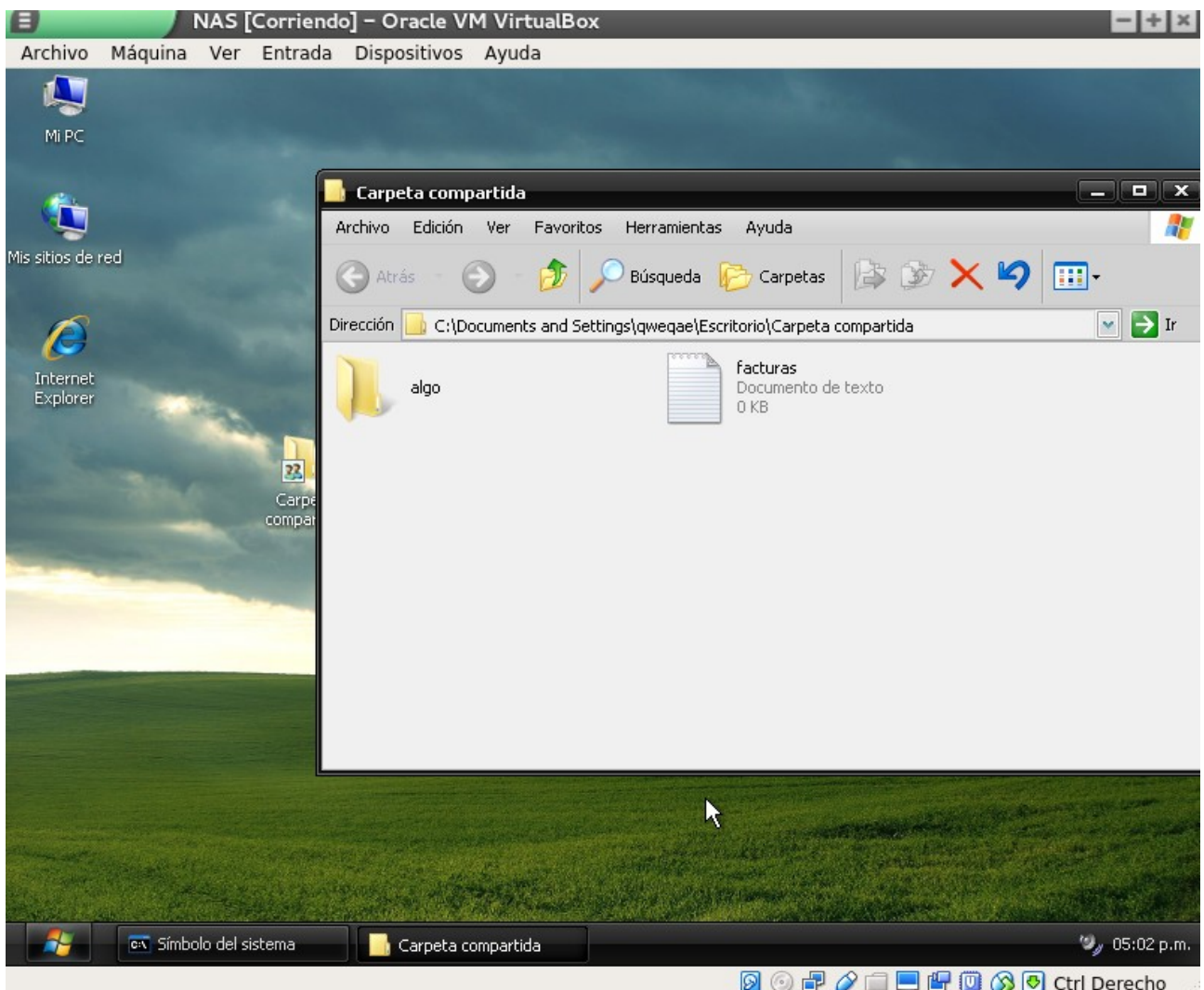


## IP y funcionamiento del NAS

### IP del nas:



## Carpeta compartida del NAS:



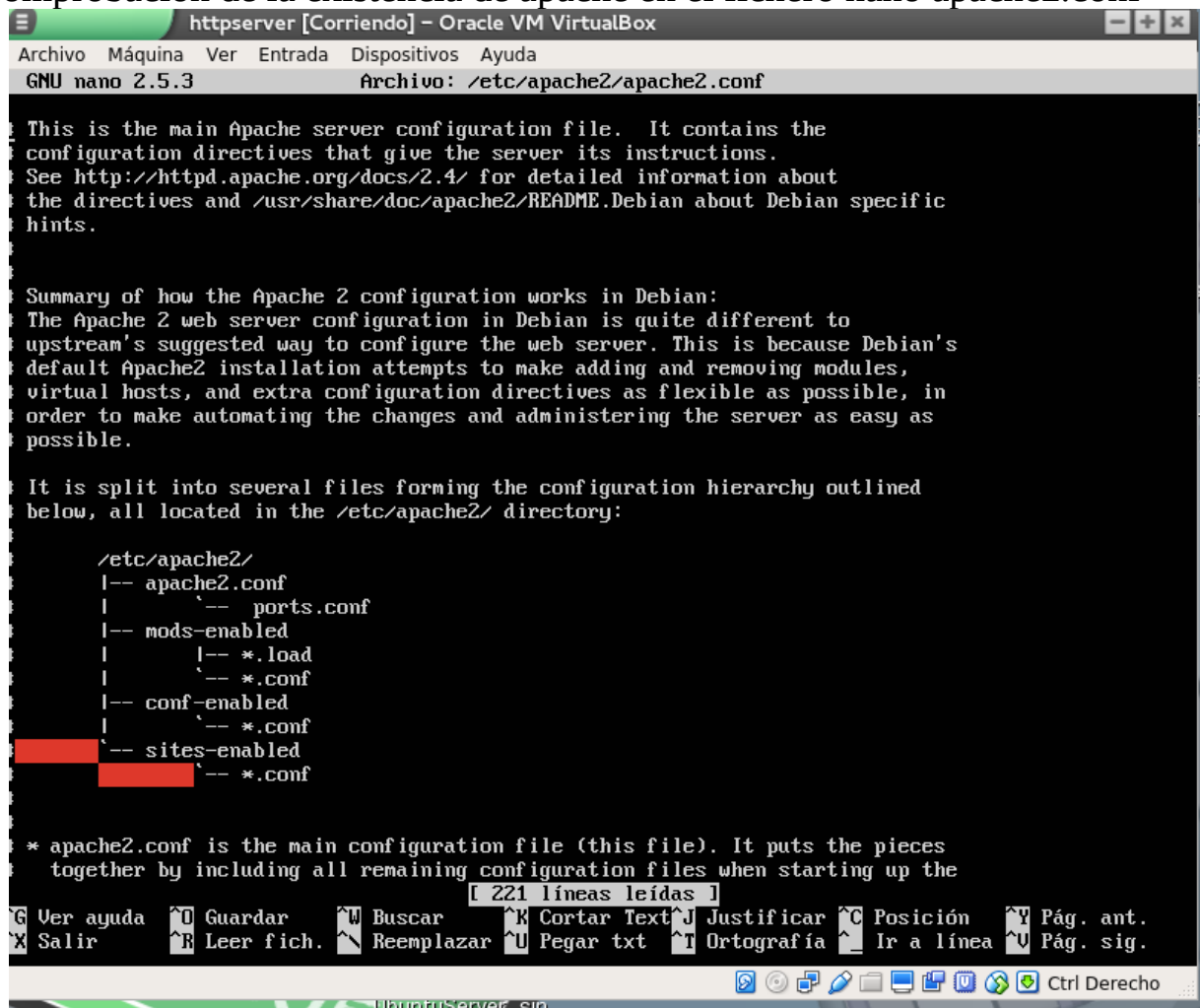
# IP y funcionamiento del servidor http:

IP del servidor http:

```
httpserver@httpserver:~$ ifconfig
emp0s3  Link encap:Ethernet  direcciónHW 08:00:27:4f:d1:7c
        Direc. inet:192.168.3.2  Difus.:192.168.3.255  Másc:255.255.255.0
        Dirección inet6: fe80::a00:27ff:fe4f:d17c/64 Alcance:Enlace
        ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST MTU:1500 Métrica:1
        Paquetes RX:39 errores:0 perdidos:0 overruns:0 frame:0
        Paquetes TX:84 errores:0 perdidos:0 overruns:0 carrier:0
        colisiones:0 long.colaTX:1000
        Bytes RX:8364 (8.3 KB)  TX bytes:7252 (7.2 KB)

lo      Link encap:Bucle local
        Direc. inet:127.0.0.1  Másc:255.0.0.0
        Dirección inet6: ::1/128 Alcance:Anfitrión
        ACTIVO BUCLE FUNCIONANDO MTU:65536 Métrica:1
        Paquetes RX:160 errores:0 perdidos:0 overruns:0 frame:0
        Paquetes TX:160 errores:0 perdidos:0 overruns:0 carrier:0
        colisiones:0 long.colaTX:1
        Bytes RX:11840 (11.8 KB)  TX bytes:11840 (11.8 KB)
```

Comprobación de la existencia de apache en el fichero nano apache2.conf



```
httpserver [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
GNU nano 2.5.3      Archivo: /etc/apache2/apache2.conf

This is the main Apache server configuration file.  It contains the
configuration directives that give the server its instructions.
See http://httpd.apache.org/docs/2.4/ for detailed information about
the directives and /usr/share/doc/apache2/README.Debian about Debian specific
hints.

Summary of how the Apache 2 configuration works in Debian:
The Apache 2 web server configuration in Debian is quite different to
upstream's suggested way to configure the web server. This is because Debian's
default Apache2 installation attempts to make adding and removing modules,
virtual hosts, and extra configuration directives as flexible as possible, in
order to make automating the changes and administering the server as easy as
possible.

It is split into several files forming the configuration hierarchy outlined
below, all located in the /etc/apache2/ directory:

/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf

* apache2.conf is the main configuration file (this file). It puts the pieces
together by including all remaining configuration files when starting up the

[ 221 líneas leídas ]
Ver ayuda  Guardar  Buscar  Cortar Text  Justificar  Posición  Pág. ant.
Salir  Leer fich.  Reemplazar  Pegar txt  Ortografía  Ir a línea  Pág. sig.
UbuntuServer sin
```

## Capturas del script en el router:

```
GNU nano 2.5.3 Archivo: script

#!/bin/bash

echo 1 >/proc/sys/net/ipv4/ip_forward
#Reiniciar
iptables -F
iptables -X
iptables -Z

iptables -t mangle -F
iptables -t mangle -X
iptables -t mangle -Z

#Políticas
iptables -P FORWARD DROP
iptables -P INPUT DROP
iptables -P OUTPUT DROP

#Hacer nat en postrouting
iptables -t nat -A POSTROUTING -o enp0s10 -j MASQUERADE

#De la red 1 a la red 3
iptables -A FORWARD -i enp0s3 -o enp0s9 -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -i enp0s3 -o enp0s9 -p udp --dport 80 -j ACCEPT
#De la red 1 a internet
iptables -A FORWARD -o enp0s3 -j ACCEPT
iptables -A FORWARD -i enp0s3 -o enp0s10 -j ACCEPT
#De la red 2 a internet
iptables -A FORWARD -m state --state RELATED,ESTABLISHED -i enp0s10 -o enp0s8 -j ACCEPT
iptables -A FORWARD -i enp0s8 -o enp0s10 -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -i enp0s8 -o enp0s10 -p tcp --dport 443 -j ACCEPT
iptables -A FORWARD -i enp0s8 -o enp0s10 -p tcp --dport 53 -j ACCEPT

iptables -A FORWARD -i enp0s8 -o enp0s10 -p tcp --dport 443 -j ACCEPT
iptables -A FORWARD -i enp0s8 -o enp0s10 -p tcp --dport 53 -j ACCEPT
iptables -A FORWARD -i enp0s8 -o enp0s10 -p udp --dport 80 -j ACCEPT
iptables -A FORWARD -i enp0s8 -o enp0s10 -p udp --dport 443 -j ACCEPT
iptables -A FORWARD -i enp0s8 -o enp0s10 -p udp --dport 53 -j ACCEPT

#De la red 2 a la red 3
iptables -A FORWARD -m state --state RELATED,ESTABLISHED -i enp0s9 -o enp0s8 -j ACCEPT
iptables -A FORWARD -i enp0s8 -o enp0s9 -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -i enp0s8 -o enp0s9 -p udp --dport 80 -j ACCEPT
#Administrador de la red 2 a la red 3
iptables -A FORWARD -s 192.168.2.2 -o enp0s9 -j ACCEPT

#De la red 3 a internet
iptables -A FORWARD -m state --state RELATED,ESTABLISHED -i enp0s10 -o enp0s9 -j ACCEPT
iptables -A FORWARD -i enp0s9 -o enp0s10 -j ACCEPT

#Administrador de la red 2 al router
iptables -A INPUT -s 192.168.2.2 -p tcp --dport 22 -j ACCEPT
iptables -A INPUT -s 192.168.2.2 -p udp --dport 22 -j ACCEPT
iptables -A OUTPUT -d 192.168.2.1 -j ACCEPT

#proxy squid
iptables -t nat -A PREROUTING -i enp0s3 -p tcp --dport 80 -j REDIRECT --to-port 8080
iptables -t nat -A PREROUTING -i enp0s8 -p tcp --dport 80 -j REDIRECT --to-port 8080
iptables -t nat -A PREROUTING -i enp0s9 -p tcp --dport 80 -j REDIRECT --to-port 8080

#Dejar paso a input y output para dansguardian
iptables -A INPUT -p tcp --dport 8080 -j ACCEPT
iptables -A INPUT -p udp --dport 8080 -j ACCEPT
iptables -A OUTPUT -p tcp --sport 8080 -j ACCEPT
iptables -A OUTPUT -p udp --sport 8080 -j ACCEPT
```

Instalación del squid:

Para demostrar el squid, he hecho capturas en webmin:

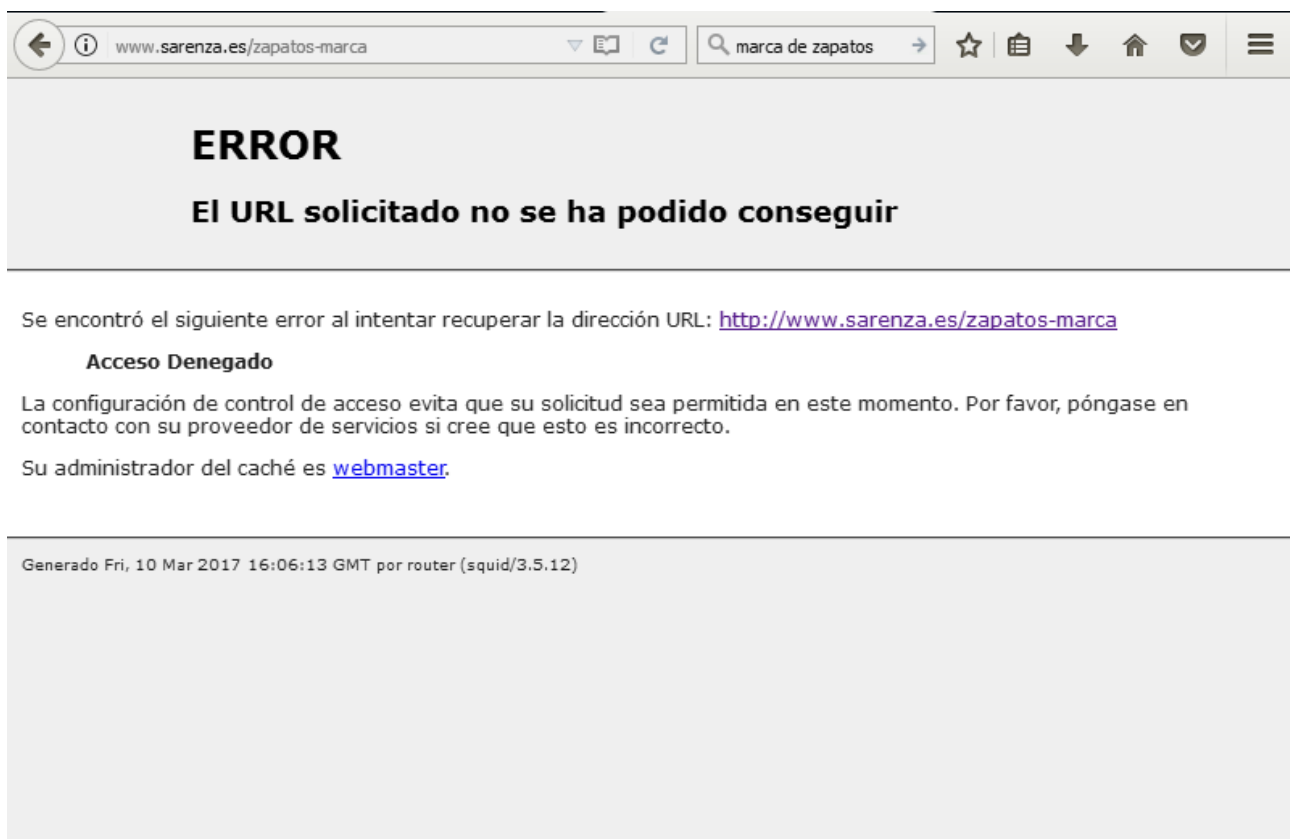
Name	Type	Matching..
SSL_ports	URL Port	443
Safe_ports	URL Port	80
Safe_ports	URL Port	21
Safe_ports	URL Port	443
Safe_ports	URL Port	70
Safe_ports	URL Port	210
Safe_ports	URL Port	1025-65535
Safe_ports	URL Port	280
Safe_ports	URL Port	488
Safe_ports	URL Port	591
Safe_ports	URL Port	777
CONNECT	Request Method	CONNECT
red_roja	Client Address	192.168.1.0/24
red_verde	Client Address	192.168.2.0/24
red_azul	Client Address	192.168.3.0/24
cosasprohibidas	URL Path Regexp	marca compra

	Action	ACLs	Move
<input type="checkbox"/>	Deny	!Safe_ports	↓
<input type="checkbox"/>	Deny	CONNECT !SSL_ports	↓ ↑
<input type="checkbox"/>	Allow	localhost manager	↓ ↑
<input type="checkbox"/>	Deny	manager	↓ ↑
<input type="checkbox"/>	Allow	localhost	↓ ↑
<input type="checkbox"/>	Deny	cosasprohibidas	↓ ↑
<input type="checkbox"/>	Allow	red_roja	↓ ↑
<input type="checkbox"/>	Allow	red_azul	↓ ↑
<input type="checkbox"/>	Allow	red_verde	↓ ↑
<input type="checkbox"/>	Deny	all	↑
Add proxy restriction			

Ahora lo he puesto modo transparente en el fichero nano squid.conf:

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

Y nos bloquea la página:



Instalación del dansguardian:

En el fichero de configuración de dansguardian, comentamos esta linea

```
#UNCONFIGURED - Please remove this line after configuration
```

En el mismo fichero de configuración especificamos el puerto en el que trabaja dansguardian, la ip y el puerto del proxy (squid) .

```
# 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
```