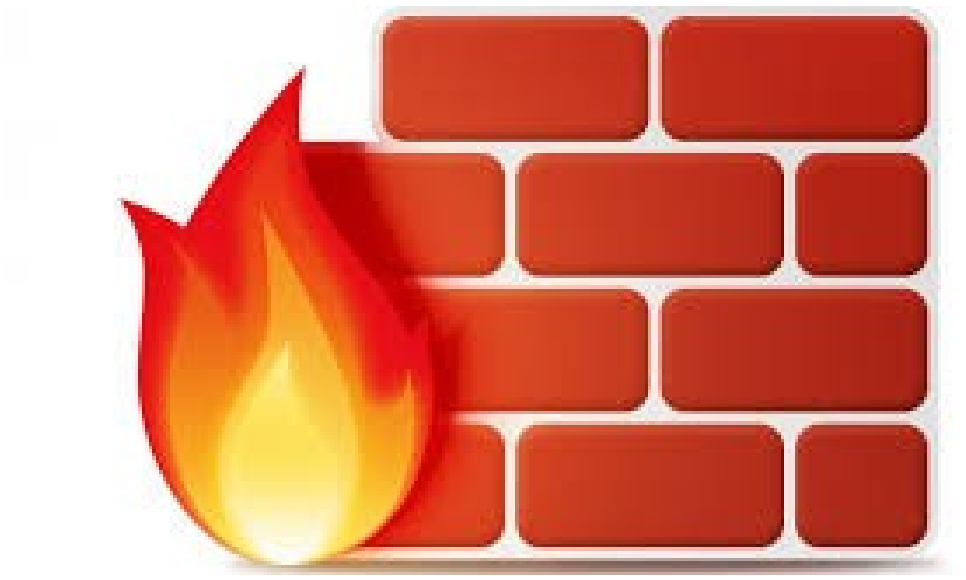
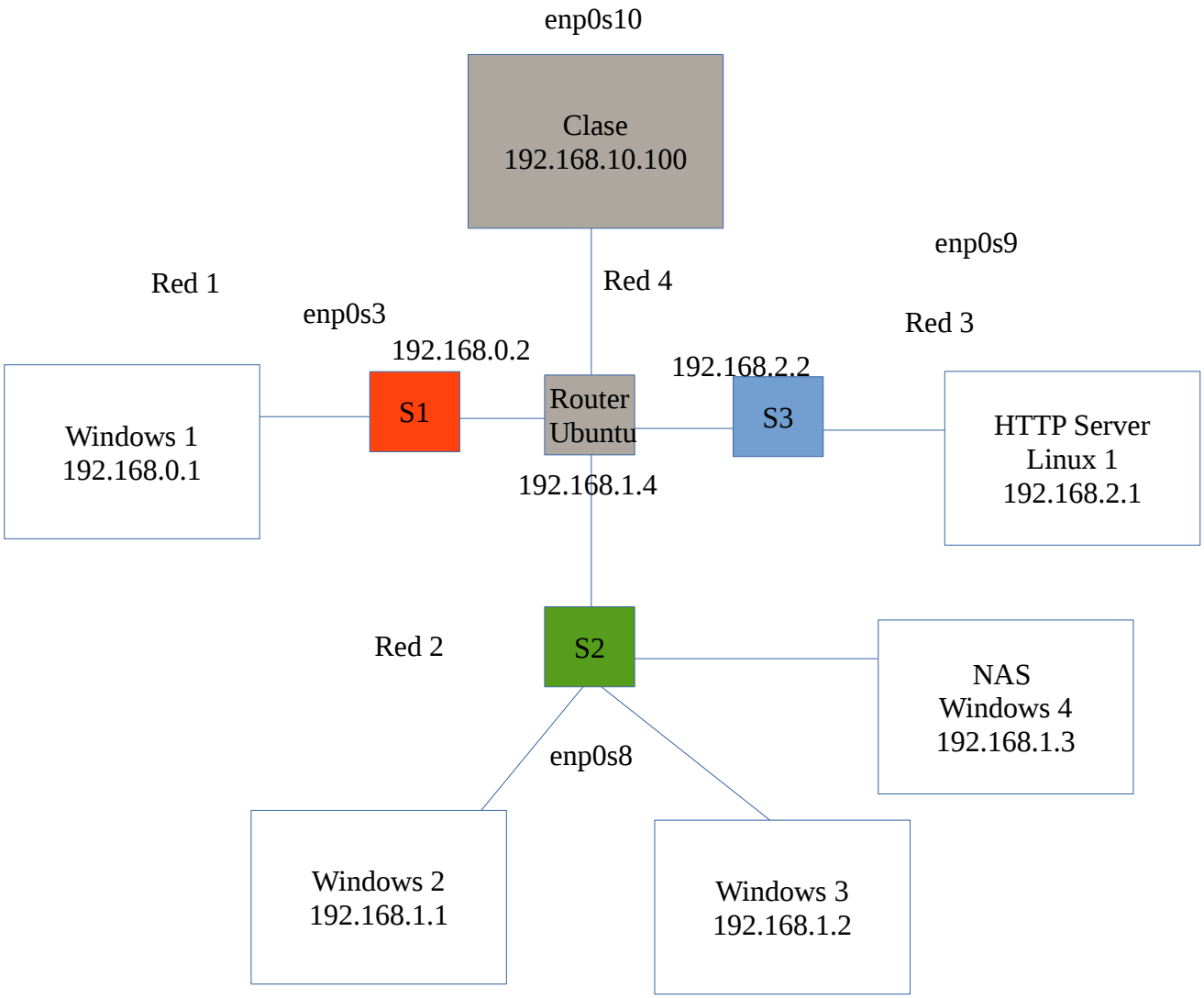
FIREWALL



Realizado por: Francisco José Llopis García
2º G SMR


enp0s10
Clase
192.168.10.100
enp0s9
Red 1
Red 4
Red 3
enp0s3
192.168.0.2
192.168.2.2
Windows 1
192.168.0.1
S1
Router
Ubuntu
S3
HTTP Server
Linux 1
192.168.2.1
192.168.1.4
Red 2
S2
NAS
Windows 4
192.168.1.3
enp0s8
Windows 2
192.168.1.1
Windows 3
192.168.1.2

Activar FORWARD de forma permanente en /etc/sysctl.conf. Descomentar net.ipv4.ip_forward=1

```
#
# /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
                                [ 60 líneas leídas ]
^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.
```

Script de iptables

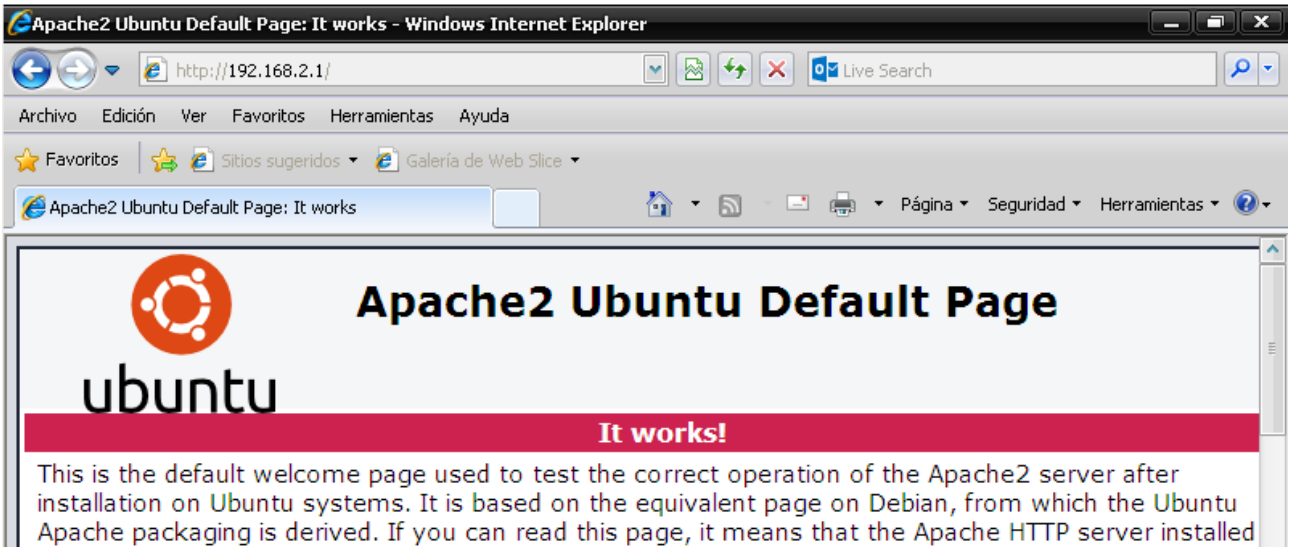
```
 GNU nano 2.5.3                 Archivo: iptables.sh

#!/bin/bash

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


iptables -P FORWARD DROP
iptables -P INPUT DROP
iptables -P OUTPUT DROP
```

```
# Activamos el NAT para poder comunicarnos con el router de clase
iptables -t nat -A POSTROUTING -o enp0s10 -j MASQUERADE

# Aqui permitimos el tráfico desde la red roja hacia Internet
iptables -A FORWARD -i enp0s3 -o enp0s10 -j ACCEPT

# Aqui permitimos el trafico 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

# Permitimos el trafico de cualquier red hacia la red roja
iptables -A FORWARD -o enp0s3 -j ACCEPT

# Permitimos el trafico hacia la red verde solo si a pedido de antes
iptables -A FORWARD -m state --state RELATED,ESTABLISHED -o enp0s8 -j ACCEPT

# Permite el trafico desde la maquina 192.168.1.1 en la red verde a la red azul por los puertos 20,$
iptables -A FORWARD -s 192.168.1.1 -o enp0s9 -p tcp --dport 20 -j ACCEPT
iptables -A FORWARD -s 192.168.1.1 -o enp0s9 -p tcp --dport 21 -j ACCEPT
iptables -A FORWARD -s 192.168.1.1 -o enp0s9 -p tcp --dport 22 -j ACCEPT

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

# Permite el trafico de internet hacia la red verde
iptables -A FORWARD -i enp010 -o enp0s8 -j ACCEPT

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

# Permite el trafico de internet hacia la red azul solo 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
```

Instalación Apache2

```
root@r0:/home/r0# 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.
```

Comprobar que la red roja tiene acceso al apache del HTTP Server



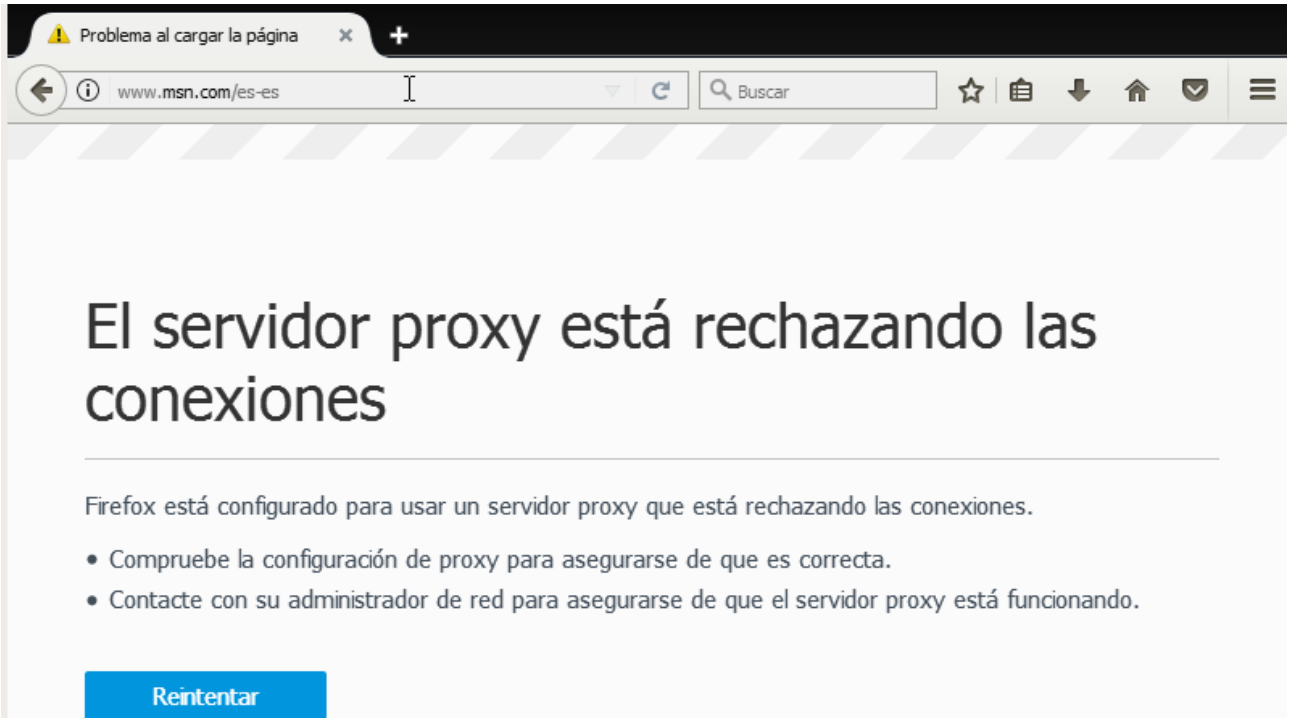
Instalación Squid y Dansguardian

```
r0@r0:~$ sudo 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.
r0@r0:~$
```

Entramos en el archivo de configuración de squid (/etc/squid/squid.conf) y añadimos las lineas de acl y http.

```
#
# 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
```

```
 GNU nano 2.5.3                Archivo: /etc/squid/bad-site.acl

.ilipad.es
.msn.com
.google.es
```



Para hacer a squid tranparente modificamos en /etc/squid/squid.conf la linea de http_port 3128 añadiéndole transparent al final.

Y añadimos al scrit una linea.

```
iptables -A FORWARD -s 192.168.1.1 -o enp0s9 -p tcp --dport 20 -j ACCEPT
iptables -A FORWARD -s 192.168.1.1 -o enp0s9 -p tcp --dport 21 -j ACCEPT
iptables -A FORWARD -s 192.168.1.1 -o enp0s9 -p tcp --dport 22 -j ACCEPT

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

# Permite el trafico de internet hacia la red verde
iptables -A FORWARD -i enp010 -o enp0s8 -j ACCEPT

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

# Permite el trafico de internet hacia la red azul solo 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

#Squid Transparente
iptables -t nat -A PREROUTING -i enp0s3 -p tcp --dport 80 -j REDIRECT --to-port 3128
```

Por ultimo el Dansguardian entramos a /etc/dansguardian/dansguadian.conf y modificamos las lineas

reportinglevel = 0

language = ’spanish’

loglocation = ‘/var/log/dansguardian/access.log’ (Descomentar)

filterip = 127.0.0.1

filterport = 8080

proxyip = 127.0.0.1

proxyport = 3128

```
# 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 = 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
```