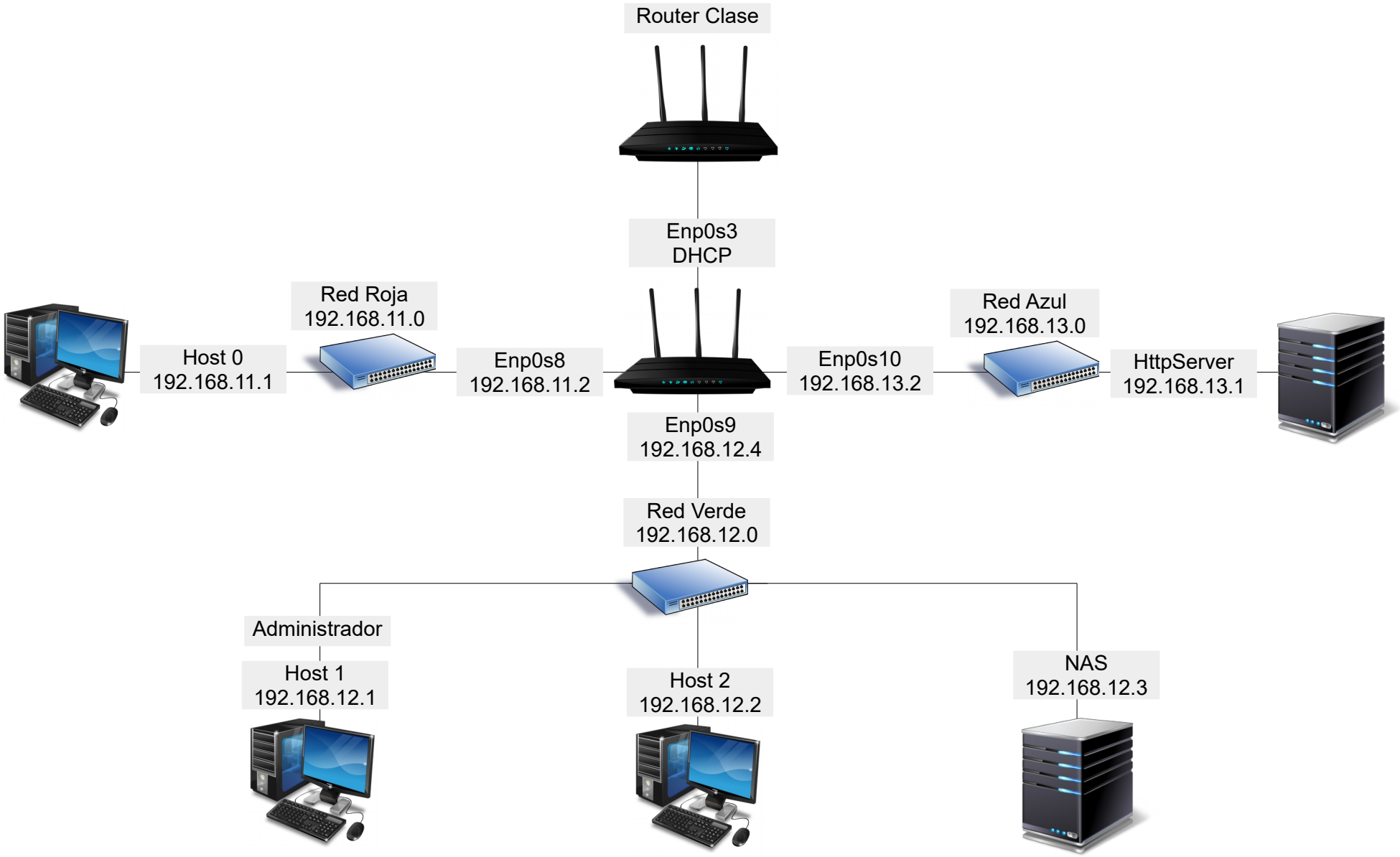
Práctica Final de Firewall

Morgana Morales Sagasta, 2º SMR G
IES Severo Ochoa, 2016/17

ÍNDICE

Diseño de Red



Script

```
 GNU nano 2.5.3                  Archivo: iptables.sh

#!/bin/bash

clear

#Configurar como router
echo 1 > /proc/sys/net/ipv4/ip_forward

#Limpiar filter, 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

#Denegar conexiones
iptables -P FORWARD ACCEPT
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT

#Activar nat para comunicarnos con el router de clase
iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE

#Permitir el tráfico de la red roja hacia internet
iptables -A FORWARD -i enp0s8 -o enp0s3 -j ACCEPT

#Permitir el tráfico desde la red roja hacia el HTTP en la red azul solo por el puerto 80
iptables -A FORWARD -i enp0s8 -o enp0s10 -p tcp --dport 80 -j ACCEPT

#Permitir todo el tráfico hacia la red roja (XP Sin seguridad)
iptables -A FORWARD -o enp0s8 -j ACCEPT

#Permitir el tráfico a la red verde solo si esta lo ha pedido (Windows y NAS)
iptables -A FORWARD -m state --state RELATED,ESTABLISHED -o enp0s9 -j ACCEPT

#Permitir que el ordenador 192.168.12.1 pueda acceder a la red azul (HTTP)
iptables -A FORWARD -s 192.168.12.1 -i enp0s10 -p tcp --dport 20 -j ACCEPT
iptables -A FORWARD -s 192.168.12.1 -i enp0s10 -p tcp --dport 21 -j ACCEPT
iptables -A FORWARD -s 192.168.12.1 -i enp0s10 -p tcp --dport 22 -j ACCEPT

#Permitir el tráfico de la red verde a internet
iptables -A FORWARD -i enp0s3 -o enp0s9 -j ACCEPT

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

#Permitir el tráfico de internet hacia la red azul
iptables -A FORWARD -i enp0s3 -o enp0s10 -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -i enp0s3 -o enp0s10 -p tcp --dport 443 -j ACCEPT

#Squid transparente
iptables -t nat -A PREROUTING -i enp0s8 -p tcp --dport 80 -j REDIRECT --to-port 3128
```

Configuración de Red en el Router

```
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto enp0s3
iface enp0s3 inet dhcp

auto enp0s8
iface enp0s8 inet static
        address 192.168.11.2
        netmask 255.255.255.0
        network 192.168.11.0
        broadcast 192.168.11.255

auto enp0s9
iface enp0s9 inet static
        address 192.168.12.4
        netmask 255.255.255.0
        network 192.168.12.0
        broadcast 192.168.12.255

auto enp0s10
iface enp0s10 inet static
        address 192.168.13.2
        netmask 255.255.255.0
        network 192.168.13.0
```

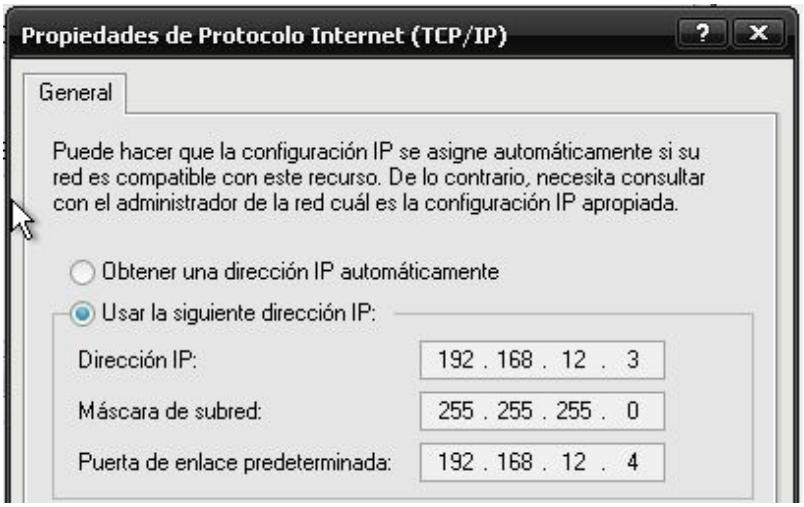
```
auto enp0s9
iface enp0s9 inet static
        address 192.168.12.4
        netmask 255.255.255.0
        network 192.168.12.0
        broadcast 192.168.12.255

auto enp0s10
iface enp0s10 inet static
        address 192.168.13.2
        netmask 255.255.255.0
        network 192.168.13.0
        broadcast 192.168.13.255
```

Configuración en el HttpServer

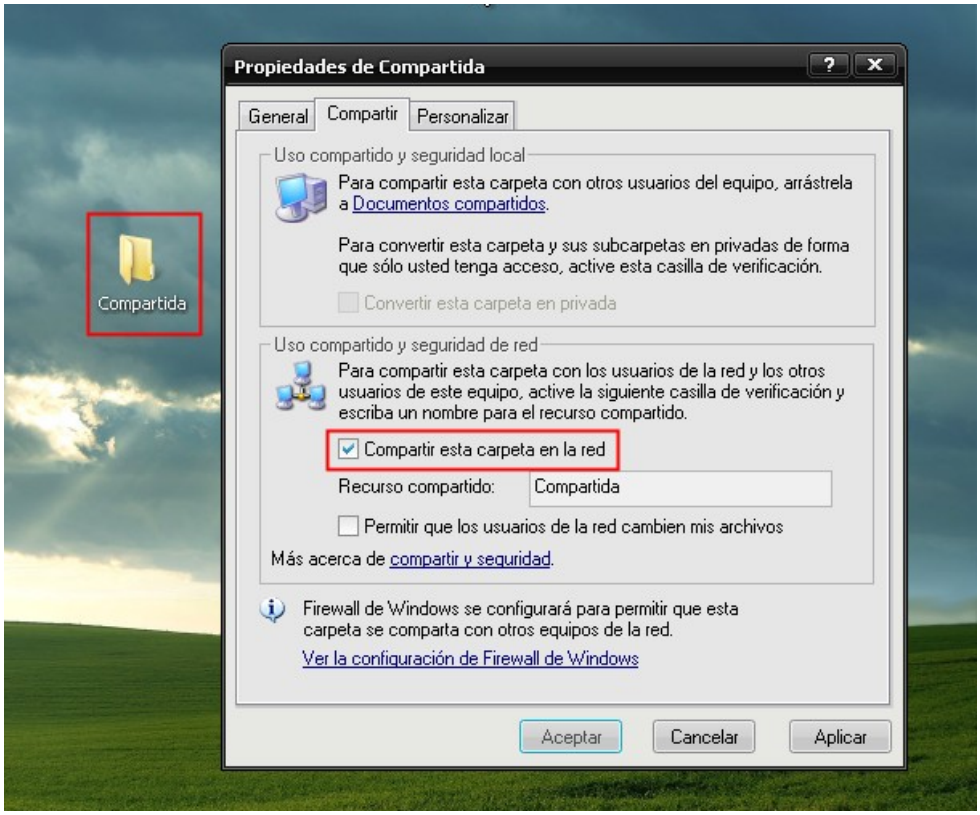
```
r@R:~$ ifconfig
enp0s3    Link encap:Ethernet  direcciónHW 08:00:27:c3:46:c1
          Direc. inet:192.168.13.1  Difus.:192.168.13.255  Másc:255.255.255.0
          Dirección inet6: fe80::a00:27ff:fec3:46c1/64 Alcance:Enlace
          ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST  MTU:1500  Métrica:1
          Paquetes RX:0 errores:0 perdidos:0 overruns:0 frame:0
```

```
r@R:~$ sudo apt-get install apache2
[sudo] password for r:
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 132 no actualizados.
r@R:~$
```

Configuración del NAS



Creamos una carpeta donde compartiremos información y le damos clic derecho → propiedades. Seleccionamos la opción de compartir y escribimos el nombre de la carpeta. Como resultado aparecerá la carpeta con un icono como vemos a la derecha:



Configuración de Squid transparente

```
 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 192.168.11.0/24
acl redverde src 192.168.12.0/24
acl redazul src 192.168.13.0/24

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

# And finally deny all other access to this proxy

http_acces deny bad_url
http_acces allow redroja
http_acces allow redverde
http_acces allow redazul_
```

```
#       If you run Squid on a dual-homed machine with an interna
#       and an external interface we recommend you to specify th
#       internal address:port in http_port. This way Squid will
#       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 t
#       --with-openssl
#
```

Restricciones:

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

.google.es
.ilipad.es_
```

Configuración de Dansguardian