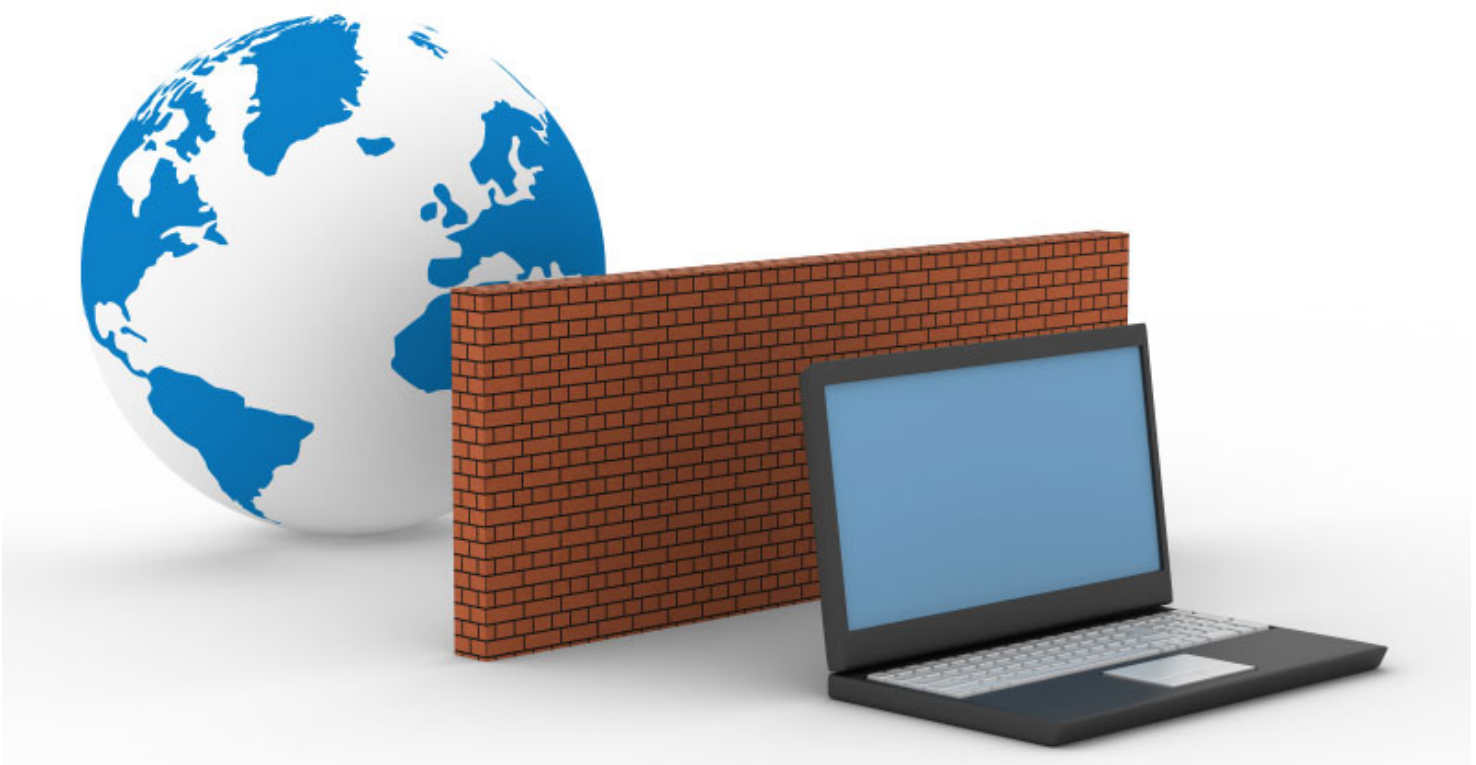
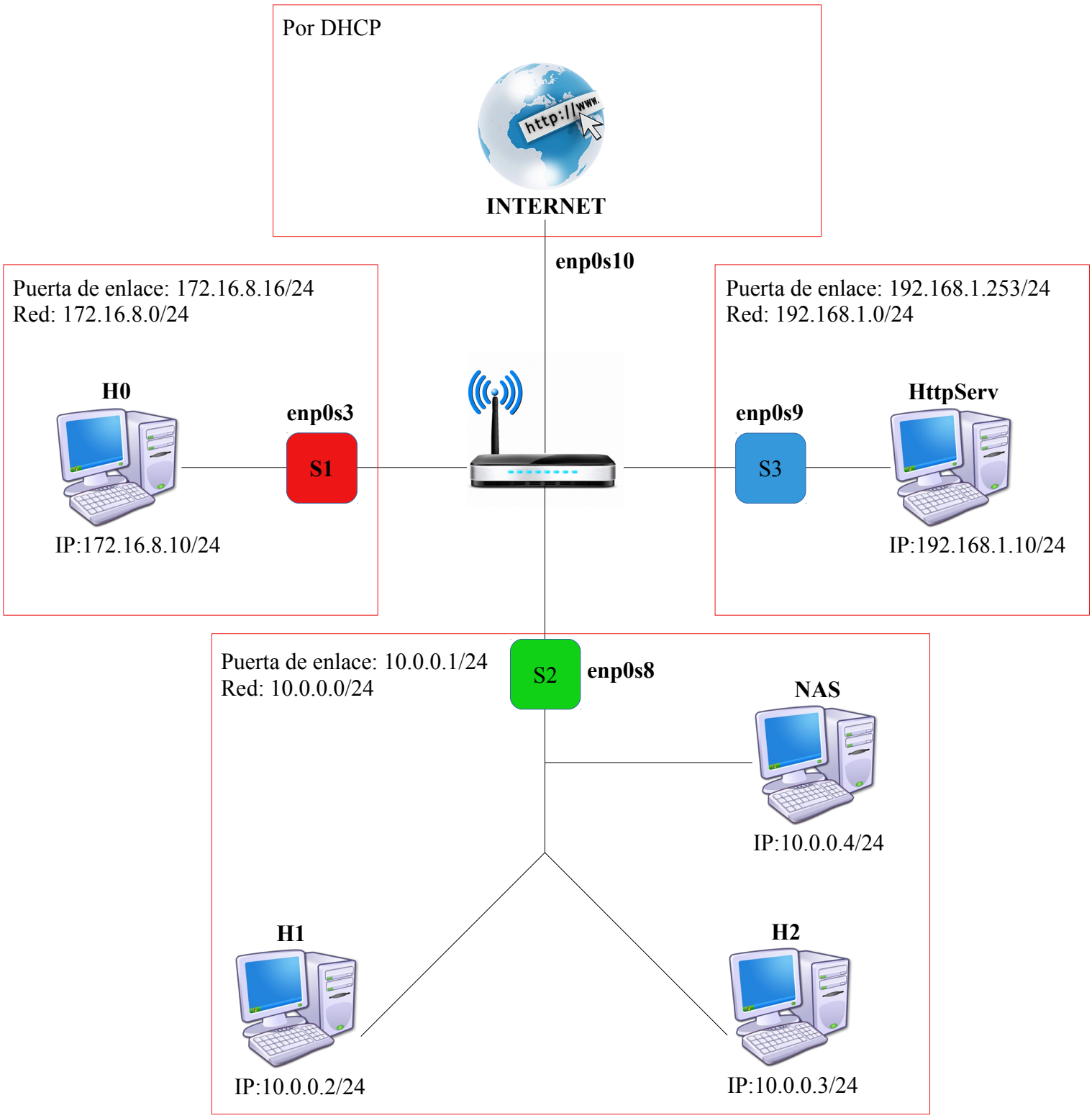
Practica final
Firewall



Giorgi Megutnishvili
7 de Marzo 2016
IES Severo Ochoa, 2-SMRG

Diagrama de red



Primero activamos el forwarding

Para poder hacerlo vamos en el fichero **/etc/sysctl.conf**
 # nano /etc/sysctl.conf

Script de Iptables (te lo pegue con paint para que se vea más xD)

```
 GNU nano 2.5.3                  Archivo: iptables.sh

#!/bin/bash

# Limpiar y borrar los Iptables
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 OUTPUD DROP
iptables -P INPUT DROP
iptables -P FORWARD DROP

# Para enmascarar, necesitamos esto para poder tener el internet
iptables -t nat -A POSTROUTING -o enp0s10 -j MASQUERADE

# S1 red wifi(enp0s10) no segura, la primera linea es para aceptar todo lo que se pida por wifi que
# le permita salir en internet(enp0s3)
# y en la segunda línea le decimos que todo lo que salga por internet(enp0s3) que lo acepte.
iptables -A FORWARD -i enp0s3 -o enp0s10 -j ACCEPT
iptables -A FORWARD -o enp0s3 -j ACCEPT

# S2 Servidor red interna de empresa(red fiable/enp0s8) todo lo que salga de red interna y
# vaya al internet(enp0s10) lo aceptamos, pero del internet que devuelva solamente
# lo relacionado y establecido(esto se hace para que solamente nos llegue la información
# que hayamos pedido).
# Todo lo que vaya de la red interna(enp0s8) al http(enp0s9) lo aceptamos
# y al reves todo lo que vaya desde el servidor http a red interna lo permitimos.
# abrimos el puerto 22 para un ip en especifico en la red interna para poder usar ssh
# en protocolos tcp y udp para que deje salir y entrar por el ip 10.0.0.2 (admin/H1)
# Abrimos el puerto 21 para FTP en los 2 lados tambien para el ip 10.0.0.2
iptables -A FORWARD -i enp0s8 -0 enp0s10 -j ACCEPT_
iptables -A FORWARD -i enp0s10 -o enp0s8 -m state --state RELATED,ESTABLISHED

iptables -A FORWARD -i enp0s8 -o enp0s9 -j ACCEPT
iptables -A FORWARD -i enp0s9 -o enp0s8 -J ACCEPT

iptables -A FORWARD -s 10.0.0.2 -o enp0s9 -p tcp --dport 22 -j ACCEPT
iptables -A FORWARD -s 10.0.0.2 -o enp0s9 -p udp --dport 22 -j ACCEPT
iptables -A FORWARD -i enp0s9 -d 10.0.0.2 -p tcp --dport 22 -j ACCEPT
iptables -A FORWARD -i enp0s9 -d 10.0.0.2 -P udp --dport 22 -j ACCEPT
iptables -A FORWARD -s 10.0.0.2 -o enp0s9 -p tcp --dport 21 -j ACCEPT
iptables -A FORWARD -s 10.0.0.2 -o enp0s9 -p udp --dport 21 -j ACCEPT
iptables -A FORWARD -i enp0s9 -d 10.0.0.2 -p tcp --dport 21 -j ACCEPT
iptables -A FORWARD -i enp0s9 -d 10.0.0.2 -P udp --dport 21 -j ACCEPT

#Accesos a S3 Servidor HTTP(enp0s9)
#Solamente dejare que entren y salgan por unos puertos necesarios para un servidor. Que son: 80,
# 443,53. Necesitamos estos puertos para que las personas puedan navegar por nuestro servidor
# Dejare que accedan por esos puertos desde el internet y desde nuestro wifi asi que hare
# entradas y salidas desde nuestro servidor(enp0s9) a internet(enp0s10) y wifi(enp0s3) y al reves.
# Pondre los 2 protocolos tcp y udp para que no de problemas a la hora de acceder.
iptables -A FORWARD -i enp0s9 -o enp0s10 -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -i enp0s9 -o enp0s10 -p tcp --dport 443 -j ACCEPT
iptables -A FORWARD -i enp0s9 -o enp0s10 -p tcp --dport 53 -j ACCEPT
iptables -A FORWARD -i enp0s9 -o enp0s10 -p udp --dport 80 -j ACCEPT
iptables -A FORWARD -i enp0s9 -o enp0s10 -p udp --dport 443 -j ACCEPT
iptables -A FORWARD -i enp0s9 -o enp0s10 -p udp --dport 53 -j ACCEPT
##
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
iptables -A FORWARD -i enp0s10 -o enp0s9 -p tcp --dport 53 -j ACCEPT
iptables -A FORWARD -i enp0s10 -o enp0s9 -p udp --dport 80 -j ACCEPT
```

```
iptables -A FORWARD -i enp0s10 -o enp0s9 -p udp --dport 443 -j ACCEPT
iptables -A FORWARD -i enp0s10 -o enp0s9 -p udp --dport 53 -j ACCEPT
##
iptables -A FORWARD -i enp0s3 -o enp0s9 -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -i enp0s3 -o enp0s9 -p tcp --dport 443 -j ACCEPT
iptables -A FORWARD -i enp0s3 -o enp0s9 -p tcp --dport 53 -j ACCEPT
iptables -A FORWARD -i enp0s3 -o enp0s9 -p udp --dport 80 -j ACCEPT
iptables -A FORWARD -i enp0s3 -o enp0s9 -p udp --dport 443 -j ACCEPT
iptables -A FORWARD -i enp0s3 -o enp0s9 -p udp --dport 53 -j ACCEPT
##
iptables -A FORWARD -i enp0s9 -o enp0s3 -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -i enp0s9 -o enp0s3 -p tcp --dport 443 -j ACCEPT
iptables -A FORWARD -i enp0s9 -o enp0s3 -p tcp --dport 53 -j ACCEPT
iptables -A FORWARD -i enp0s9 -o enp0s3 -p udp --dport 80 -j ACCEPT
iptables -A FORWARD -i enp0s9 -o enp0s3 -p udp --dport 443 -j ACCEPT
iptables -A FORWARD -i enp0s9 -o enp0s3 -p udp --dport 53 -j ACCEPT


#Squid proxy transparente
iptables -t nat -A OUTPUT -o enp0s10 -p tcp --dport 80 -j DNAT --to-destination 127.0.0.1:3128

#Dansguardian
iptables -t nat -A PREROUTING -o enp0s10 -p tcp --dport 80 -j DNAT --to-destination 127.0.0.1:8080
```

Instalación y configuración Squid y dansguardian

Primero lo instalamos
 # apt-get install squid dansguardian

Squid

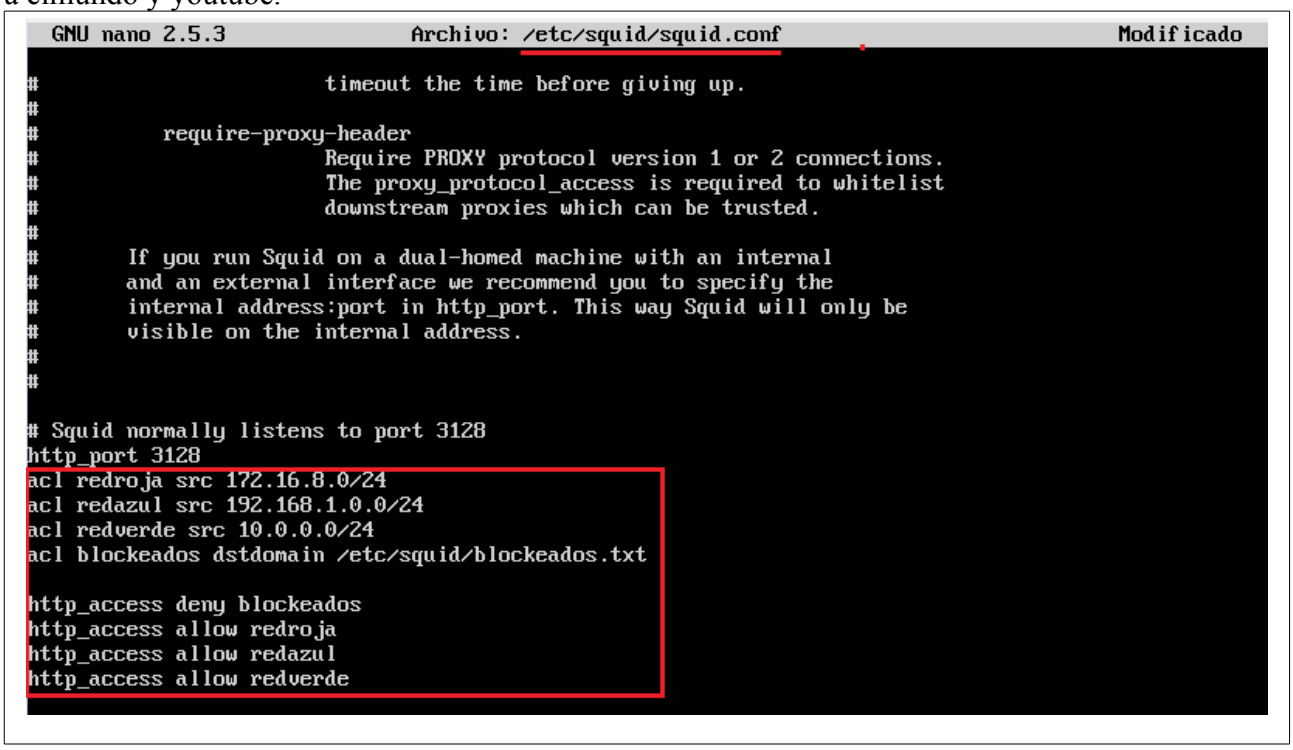
Ahora editamos el fichero **/etc/squid/squid.conf**
 # nano /etc/squid/squid.conf

Primero he creado un fichero para blockear ciertas páginas que no quiero que accedan mis usuarios.
Le llamaré **blockeados.txt**

```
 GNU nano 2.5.3                Archivo: blockeados.txt                    Modificado

www.elmundo.es
www.youtube.com
```

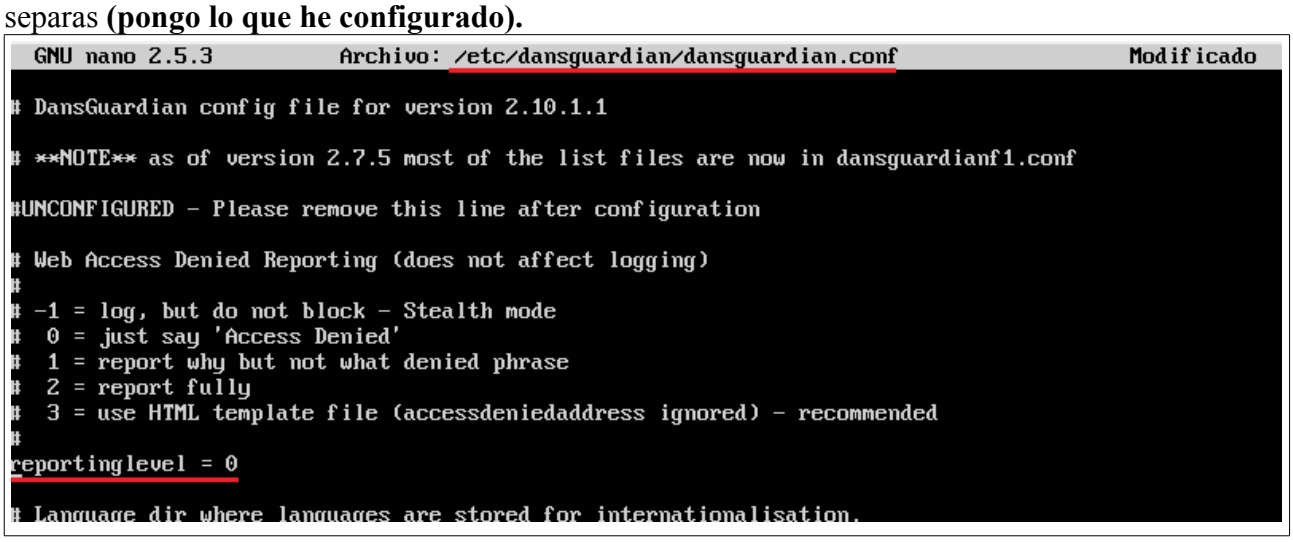
Y ahora ya le puse los 3 redes que tengo roja,azul y verde y blockeados para que no puedan acceder a elmundo y youtube.



Dansguardian

Editamos el archivo **/etc/dansguardian/dansguardian.conf**
#nano etc/dansguardian/dansguardian.conf

Los siguientes solamente los escribo ya que tendría que tomar varías fotos porque van en zonas separas **(pongo lo que he configurado).**

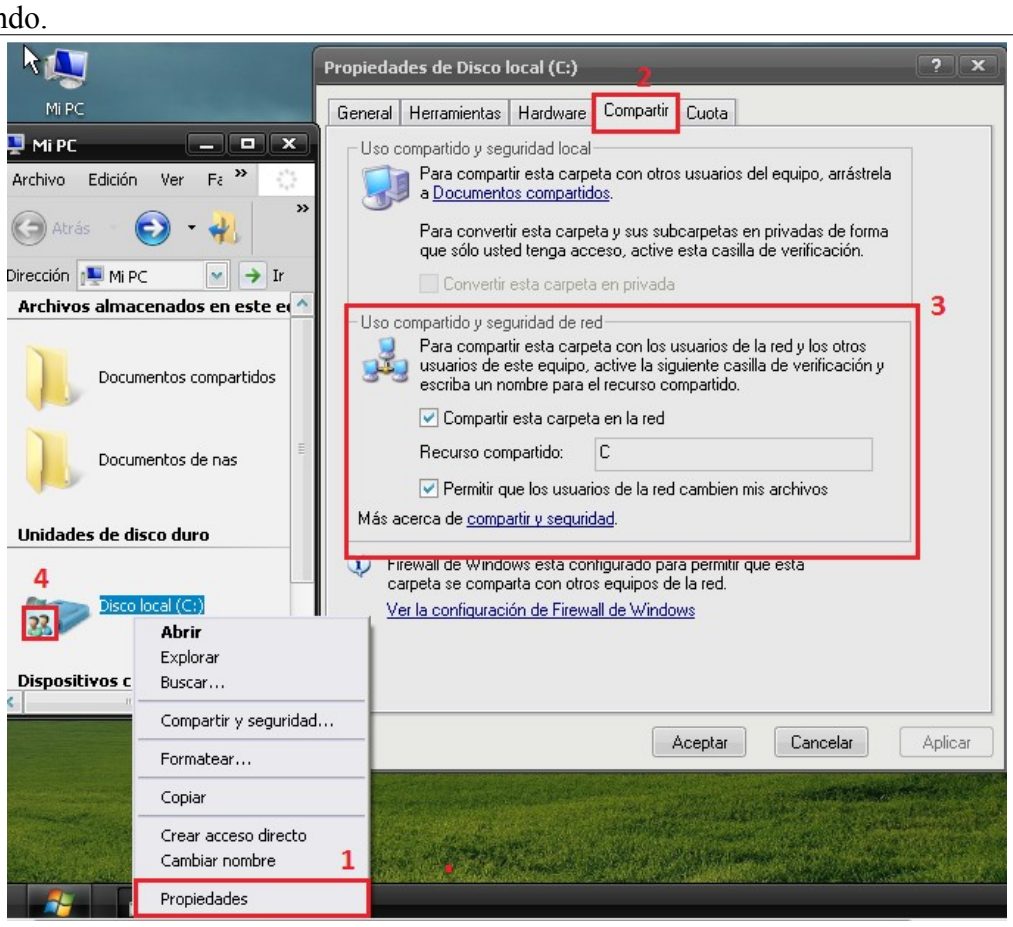


Los cambiamos asi:
reportinglevel = 0
language = 'spanish'
filterip = 127.0.0.1
filterport = 8080
proxyip = 127.0.0.1

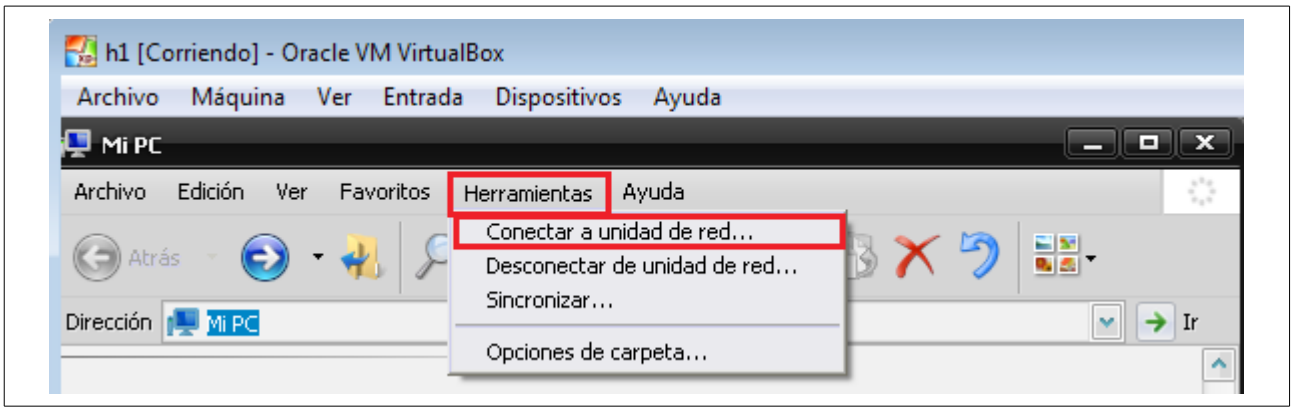
proxyport = 3128
Esto lo descomentamos
loglocation = '/var/log/dansguardian/access.log'

NAS

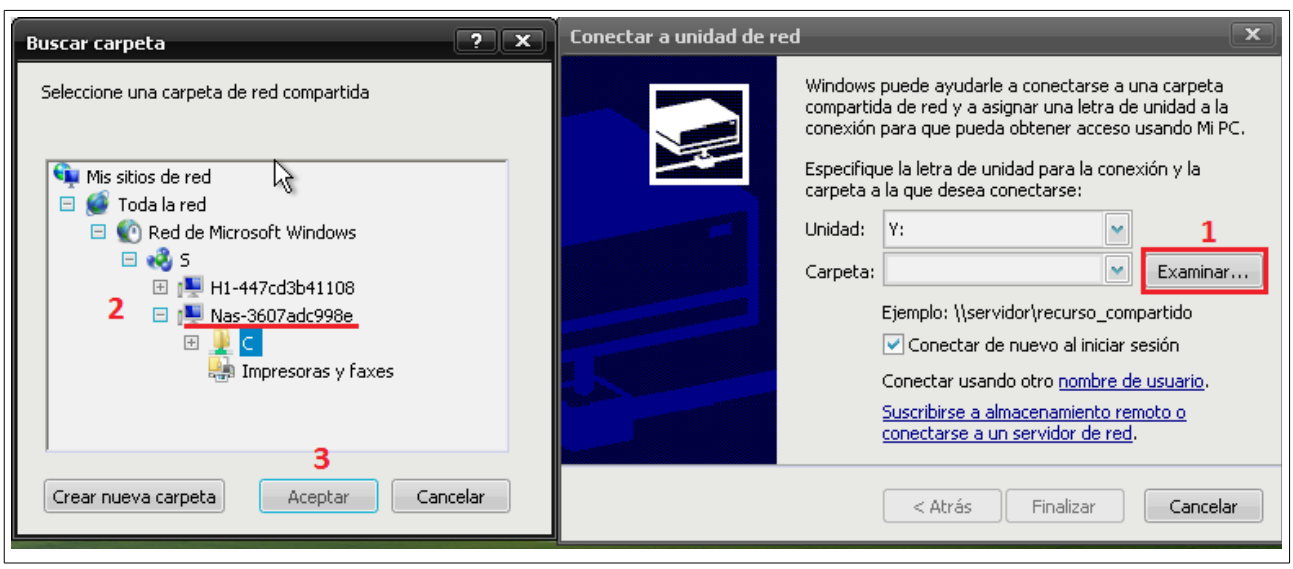
Yo voy a compartir mi disco C a los usuarios de mi RED para poder hacerlo debemos hacer los siguientes pasos:
1. Click derecho sobre lo que queremos compartir y le damos a propiedades.
2. Nos vamos a Compartir.
3. Marcamos las 2 casillas que nos aparecen en la siguiente imagen.
4. Cuando terminemos de compartir el disco nos aparecera con este icono de que se esta compartiendo.



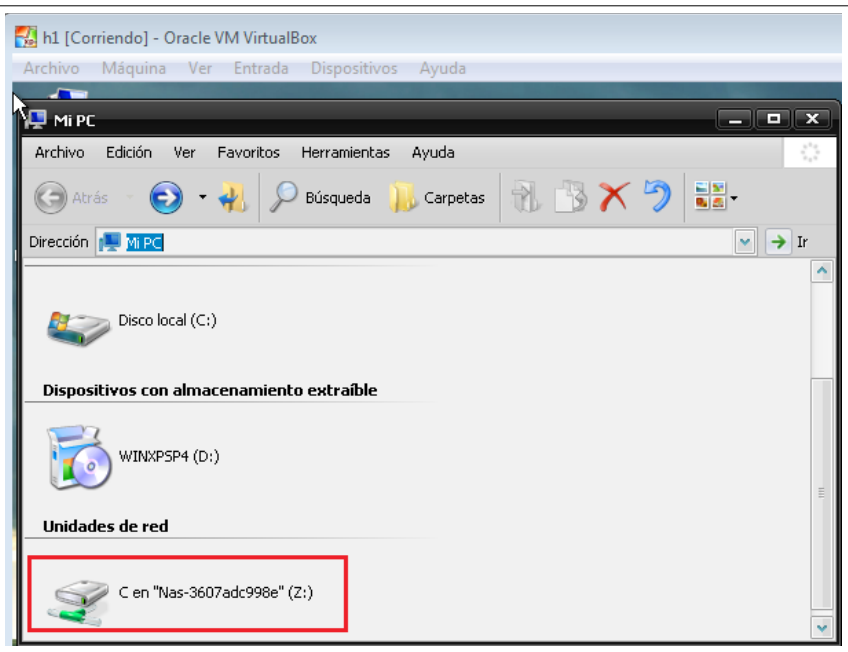
Ahora para poder verlo hare una prueba en otro ordenador H1, entramos en Mi PC o en cualquier carpeta y le damos a **herramientas -> Conectar a unidad de red**



Le damos a **Examinar y** como vemos en la ventana de la izquierda nos sale la **máquina Nas y si lo desplegamos** dentro nos aparece el **disco C** que hemos compartido antes **lo marcamos** y le damos a **Aceptar**



Como vemos se ha compartido el **Disco C,** nos aparece en Mi PC.



Instalación Apache en Servidor HTTP

Para instalarlo ponemos:
 # sudo apt-get install apache2

Esta parte no la he podido seguir porque en mi casa no me daba internet por red interna y ya no queria desconfigurar nada para solamente instalar apache puede que luego me crease mas problemas.