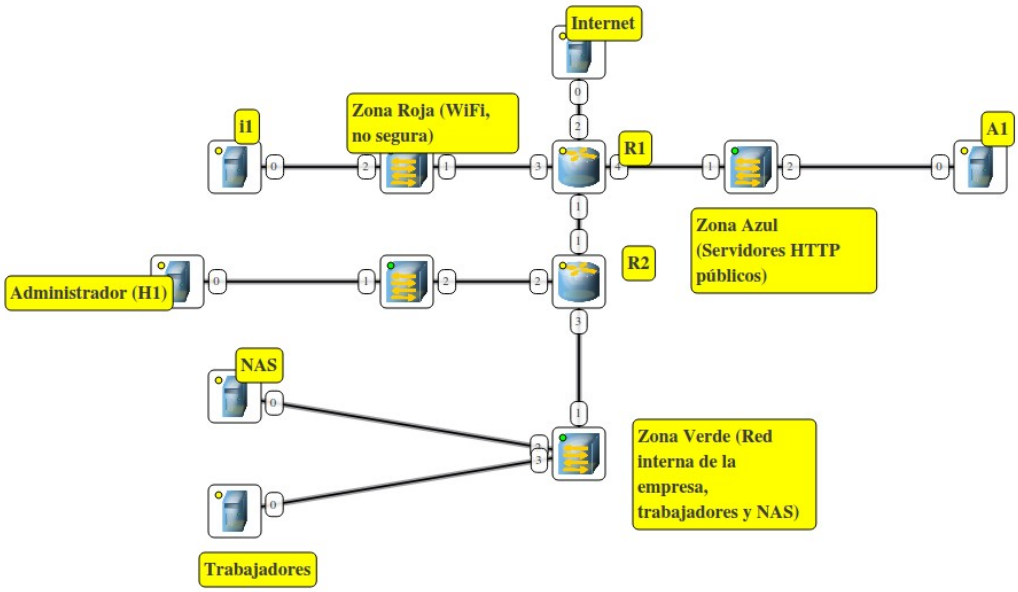
Práctica de Firewall

INDICE

1.- Diagrama de la red

En esta practica he elegido otro modelo de configurar la red pedida para la practica ya que este modo en mi opinión es más seguro



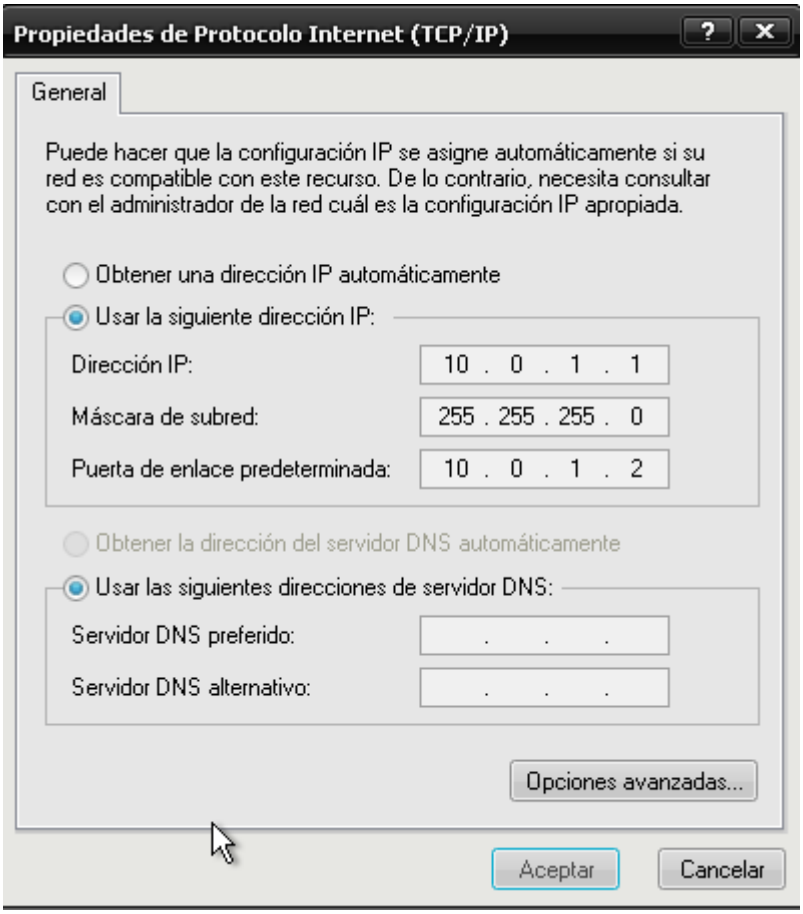
Aqui muestro una tabla donde indico la configuración de las interfaces y sus IP's de la red que he utilizado para guiarme mejor a la hora de hacer la práctica

I1	E0 → 10.0.0.1
R1	E1 → 172.168.100.1
	E2 → (Internet)
	E3 → 10.0.0.2
	E4 → 10.0.1.2
A1	E0 → 10.0.1.1
H1	E0 → 192.168.0.1
R2	E1 → 172.168.100.2
	E2 → 192.168.0.2
	E3 → 192.168.1.3
NAS	E0 → 192.168.1.1
Trabajadores	E0 → 192.168.1.2

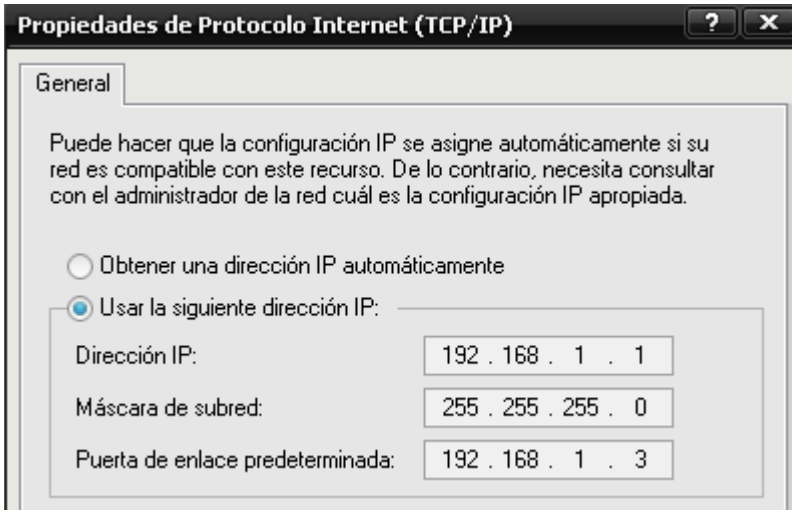
2.-Configuración de HTTP y NAS

Como para esta practica he utilizado una configuración diferente al del resto esta tiene. En un principio que asegurarnos que tienen las IP que hemos indicado en la tabla y asegurarnos que tenemos desactivado el firewall de Windows para que no nos de problemas más adelante.

Captura de i1, que en nuestro caso es HTTP.



Captura de la configuración de red de NAS



3.- Script

Para que la práctica sea mas fácil a la hora de indicar las rutas de encaminamiento que falten en los routers y para configurar la iptables hemos un utilizado un script en cada máquina virtual

Configuración del script de r1

```
 GNU nano 2.5.3                    Archivo: script.sh

##Para enrutar
echo 1 > /proc/sys/net/ipv4/ip_forward

##Tablas de enrutamiento
route add -net 192.168.0.0 netmask 255.255.255.0 gw 172.168.100.2
route add -net 192.168.1.0 netmask 255.255.255.0 gw 172.168.100.2

##A partir de este comentario comienzan las iptables
echo -n Aplicando reglas de Firewall

##Borrado de reglas
iptables -F
iptables -X
iptables -Z
iptables -t nat -F

##Reglas por defecto
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

##Para que el ruter haga NAT
iptables -t nat -A POSTROUTING -o enp0s8 -j MASQUERADE

##El trafico se dirigido al proxy squid
iptables -t nat -A PREROUTING -i enps0s8 -p tcp --dport 80 -j REDIRECT --to-port 3128
```

```
##Iptables de Red Roja y de wifi
iptables -A FORWARD -i enp0s9 -o enp0s10 -p tcp -m multiport --dports 80,443,53 -j ACCEPT
iptables -A FORWARD -i enp0s9 -o enp0s8 -p tcp -m multiport --dports 80,443,53 -j ACCEPT

iptables -A FORWARD -i enp0s9 -o enp0s10 -p udp -m multiport --dports 80,443,53 -j ACCEPT
iptables -A FORWARD -i enp0s9 -o enp0s8 -p udp -m multiport --dports 80,443,53 -j ACCEPT

##Iptables de Red Azul y HTTP
iptables -A FORWARD -i enp0s10 -p tcp -m multiport --dports 80,443,53 -j ACCEPT
iptables -A FORWARD -i enp0s10 -p udp -m multiport --dports 80,443,53 -j ACCEPT
iptables -A FORWARD -i enp0s10 -m state --state ESTABLISHED,RELATED -j ACCEPT

##INTERNET
iptables -A FORWARD -i enp0s8 -j ACCEPT

##Iptables de Red Verde
iptables -A FORWARD -i enp0s3 -j ACCEPT
```

Configuración del script r2

```
##Para enrutar
echo 1 > /proc/sys/net/ipv4/ip_forward

##Tablas de enrutamiento
route add default gw 172.168.100.1
route add -net 10.0.0.0 netmask 255.255.255.0 gw 172.168.100.1
route add -net 10.0.1.0 netmask 255.255.255.0 gw 172.168.100.1
route add -net 192.168.3.0 netmask 255.255.255.0 gw 172.168.100.1

##A partir de este comentario comienzan las iptables
echo -n Aplicando reglas de Firewall

##Borrado de reglas
iptables -F
iptables -X
iptables -Z
iptables -t nat -F

##Reglas por defecto
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
```

```
##Red Azul-Configuracion R1
iptables -A FORWARD -i enp0s3 -p tcp -m multiport --dports 80,443,53 -j ACCEPT
iptables -A FORWARD -i enp0s3 -p udp -m multiport --dports 80,443,53 -j ACCEPT

iptables -A FORWARD -i enp0s3 -m state --state ESTABLISHED,RELATED -j ACCEPT

##Red Verde
iptables -A FORWARD -i enp0s9 -p tcp -m multiport --dports 80,443,53 -j ACCEPT
iptables -A FORWARD -i enp0s9 -p udp -m multiport --dports 80,443,53 -j ACCEPT

iptables -A FORWARD -i enp0s9 -m state --state ESTABLISHED,RELATED -j ACCEPT

##Administrador
iptables -A FORWARD -i enp0s8 -j ACCEPT
```

4.- Instalación y configuración de Squid

Para instalar el squid debemos de escribir **sudo apt-get install squid**

```
root@r1:/home/r1# apt-get install squid
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
squid ya está en su versión más reciente (3.5.12-1ubuntu7.3).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 91 no actualizados.
root@r1:/home/r1# _
```

Y ahora deberemos de dirigirnos al fichero de configuración de squid y en la línea **“http_port 3128”** escribir **transparent**

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

5.- Instalación de dansguardian

Por último instalaremos dansguaridan y utilizaremos el comando **apt-get install dansguardian**

```
root@r1:/home/r1# apt-get install 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).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 91 no actualizados.
```