

Practica de firewall

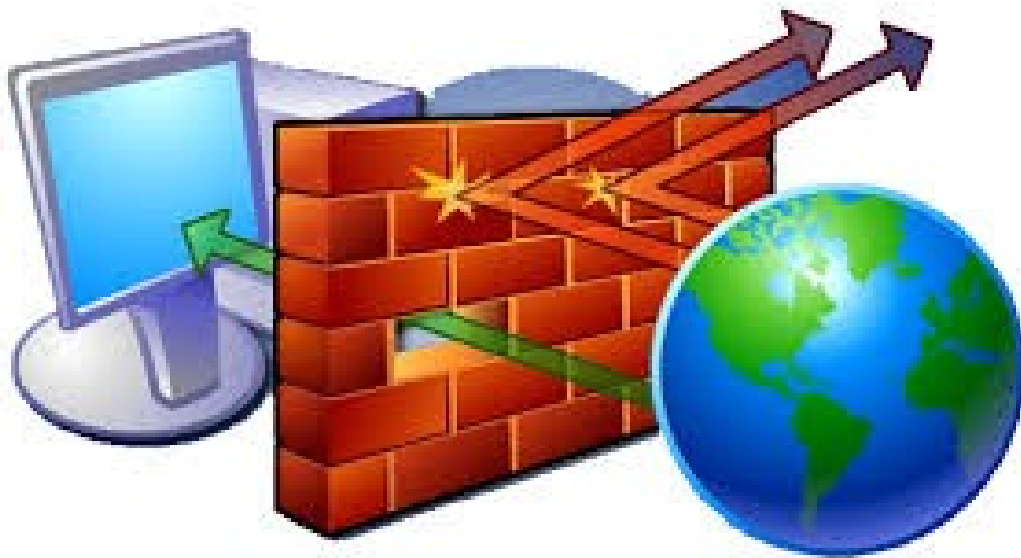
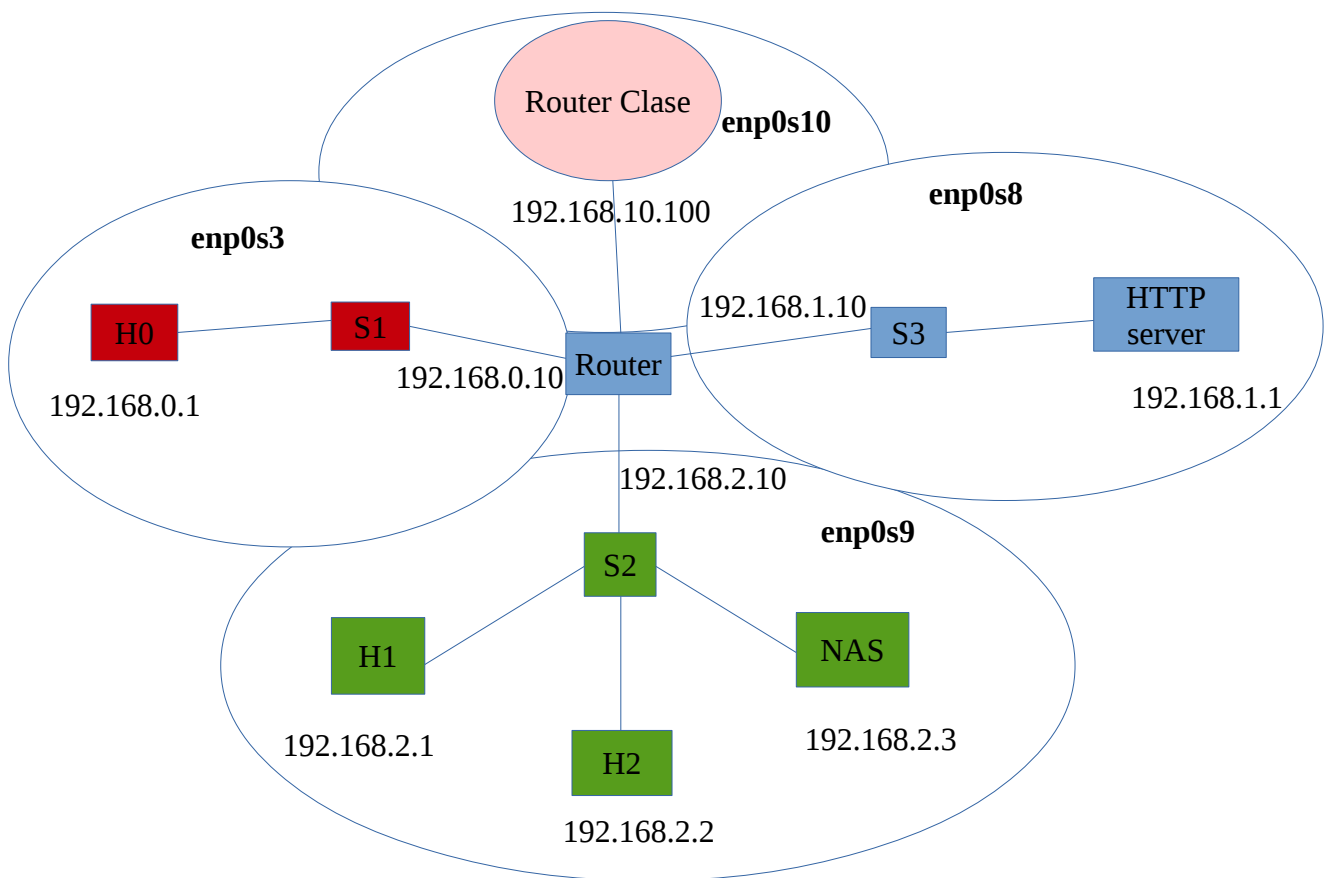


Diagrama de la empresa



- Para instalar el servidor HTTP pondremos lo siguiente:

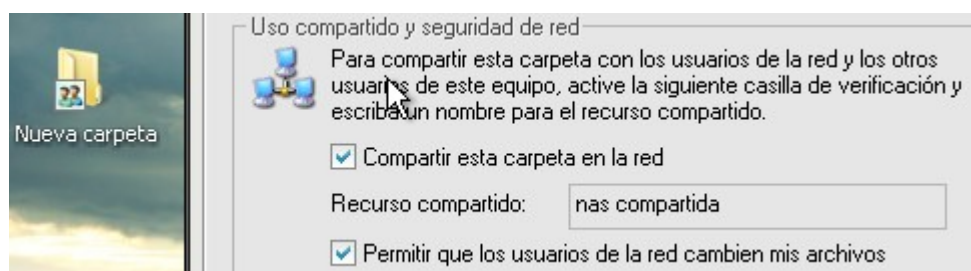
sudo apt-get install apache2

y empezará la instalación. Esta es su configuración de red:

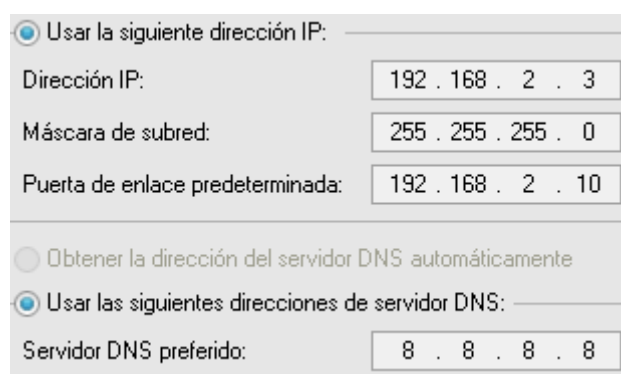
```
GNU nano 2.2.6      Archivo: /etc/network/interfaces
# interfaces(5) file used by ifup(8) and ifdown(8)
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
    network 192.168.1.0
    netmask 255.255.255.0
    address 192.168.1.1
    broadcast 192.168.1.255
    gateway 192.168.1.10
    dns-nameservers 8.8.8.8
```

- Para tener el NAS, instalaremos windows xp, y compartiremos una carpeta en nuestra red.



Esta es su configuración de red



SCRIPT

```
#!/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
```

```
# __Políticas__

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

```
# __Configuracion__

#Aqui se activa el NAT para ir al router de fuera de la red
iptables -t nat -A POSTROUTING -o enp0s10 -j MASQUERADE
```

```
# __Red roja__

#Aceptamos desde la red roja hacia internet
iptables -A FORWARD -i enp0s3 -o enp0s10 -j ACCEPT

#Permitimos de la red roja a serv.http por el puerto 80
iptables -A FORWARD -i enp0s3 -o enp0s8 -p tcp --dport 80 -j ACCEPT

#Permitimos que todo entre en la red roja
iptables -A FORWARD -o enp0s3 -j ACCEPT
```

```
# __Red verde__

#Dejamos pasar solo si ya ha habido comunicacion
iptables -A FORWARD -m state --state RELATED,ESTABLISHED -o enp0s9 -j ACCEPT

#dejamos comunicarse la red verde con http por el puerto 80
iptables -A FORWARD -i enp0s9 -o enp0s8 -p tcp --dport 80 -j ACCEPT

#Dejamos comunicarse a h2 con http por los puertos 20,21,22
iptables -A FORWARD -s 192.168.2.2 -o -enp0s8 -p tcp --dport 22 -j ACCEPT
iptables -A FORWARD -s 192.168.2.2 -o -enp0s8 -p tcp --dport 21 -j ACCEPT
iptables -A FORWARD -s 192.168.2.2 -o -enp0s8 -p tcp --dport 20 -j ACCEPT

#Deja pasar datos de la red verde hacia internet
iptables -A FORWARD -i enp0s9 -o enp0s10 -j ACCEPT

#Deja pasar datos de internet a la red verde
iptables -A FORWARD -i enp0s10 -o enp0s9 -j ACCEPT
```

```
# Red azul

#Deja pasar datos de la red azul a internet
iptables -A FORWARD -m state --state RELATED,ESTABLISHED -i enp0s10 -o enp0s8 -j ACCEPT
iptables -A FORWARD -i enp0s8 -o enp0s10 -j ACCEPT

#Solo deja pasar datos de internet a serv.http por el puerto 80 y 443
iptables -A FORWARD -i enp0s10 -o enp0s8 -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -i enp0s10 -o enp0s8 -p tcp --dport 443 -j ACCEPT
```

Instalas squid

sudo apt-get install squid

Y en /etc/squid haces sudo nano squid.conf

y pones al final de http_port 3128 **transparent**

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

Instalas dansguardian

sudo apt-get install dansguardian