

PRACTICA IPTABLES

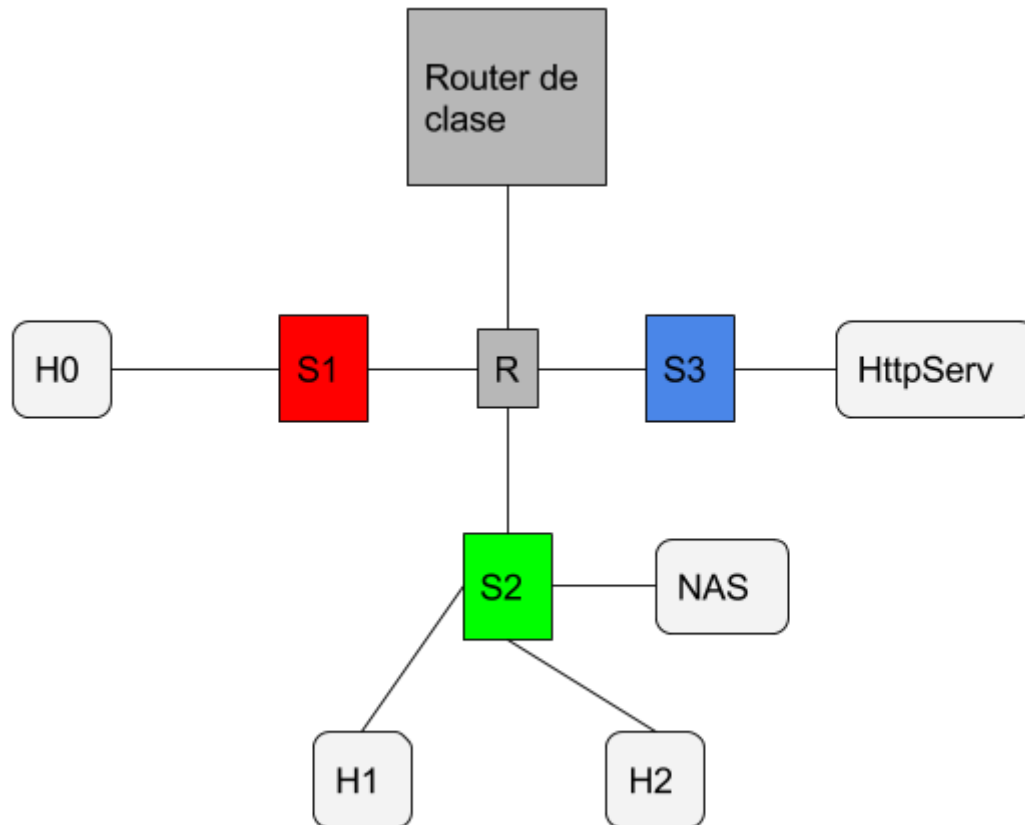
Vamos a crear una red donde hay

Red Roja: Es una red wifi y por lo tanto no segura.

Red verde: Es la red interna de la empresa, es una red fiable. Aquí se encuentran los trabajadores y un NAS.

Red azul: Es una red donde hay servidores http públicos.

Me he guiado del siguiente esquema para esta práctica.



He creado las maquinas H0 → en mi caso lo he llamado wifi, H1, H2, Servidor http y el Router.
Con las siguientes IPs:

H0 → 10.0.1.1

H1 → 10.0.2.1

H2 → 10.0.2.2

Servidor http → 10.0.3.1

Y el router →

enp0s3 → Bridge

enp0s8 → 10.0.1.100

enp0s9 → 10.0.2.100

enp0s10 → 10.0.3.100

Maquinas instaladas



Lo primero que voy a hacer, ya he puesto a todos en la red que les corresponde y voy a ver si se conectan correctamente.

Ping de la maquina wifi al ruter

```
Haciendo ping a 10.0.1.100 con 32 bytes de datos:
Respuesta desde 10.0.1.100: bytes=32 tiempo<1m TTL=64
Respuesta desde 10.0.1.100: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 10.0.1.100:
    Paquetes: enviados = 2, recibidos = 2, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

Ping de la maquina servidor http al ruter

```
C:\Documents and Settings\h1>ping 10.0.3.100

Haciendo ping a 10.0.3.100 con 32 bytes de datos:

Respuesta desde 10.0.3.100: bytes=32 tiempo<1m TTL=64
Respuesta desde 10.0.3.100: bytes=32 tiempo<1m TTL=64
Respuesta desde 10.0.3.100: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 10.0.3.100:
    Paquetes: enviados = 3, recibidos = 3, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

Ping de h2 a ruter

```
Haciendo ping a 10.0.2.100 con 32 bytes de datos:
Respuesta desde 10.0.2.100: bytes=32 tiempo<1m TTL=64
Respuesta desde 10.0.2.100: bytes=32 tiempo<1m TTL=64
Respuesta desde 10.0.2.100: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 10.0.2.100:
    Paquetes: enviados = 3, recibidos = 3, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms
Control-C
```

Una vez que todo conecta correctamente ahora tenemos que ver como conseguir acceso a internet
Crearemos un fichero para configurar las iptables de golpe así nos va a ser mucho mas comodo. Y lo ejecutamos con: **bash nuestro_script**

```
iptables -F
iptables -t nat -F
iptables -X
iptables -t nat -X

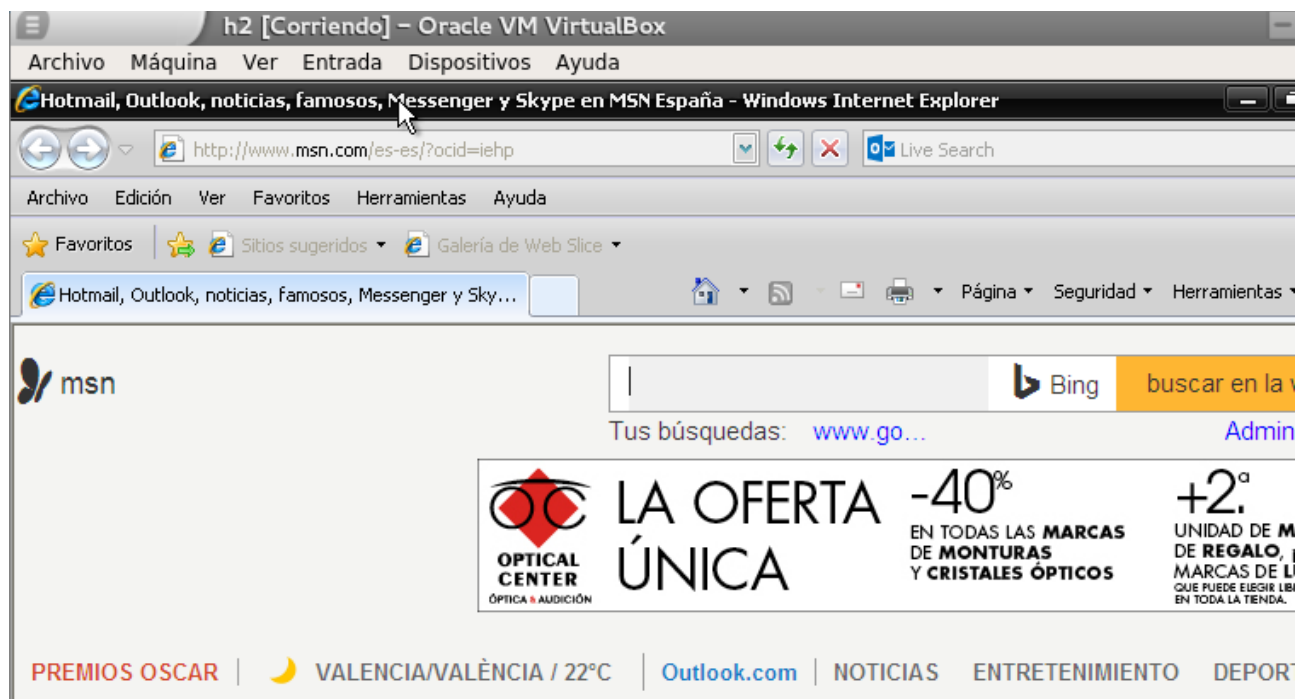
echo "Aplicando reglas de redireccionamiento"

echo 1 > /proc/sys/net/ipv4/ip_forward

#Políticas
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -P INPUT ACCEPT

#Dans y Masquerade
iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE
```

Prueba de que va:



Ahora que hemos comprobado que funciona internet lo que vamos a hacer es proteger nuestras red privada y nuestro servidor http. He creado las siguientes reglas:

```
GNU nano 2.5.3 Archivo: cortafuegos.sh

iptables -F
iptables -t nat -F
iptables -X
iptables -t nat -X

echo "Aplicando reglas de redireccionamiento"

echo 1 > /proc/sys/net/ipv4/ip_forward

#Políticas
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
iptables -P INPUT DROP

#Dns y Masquerade
iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE
#iptables -t nat -A PREROUTING -s 192.168.3.0/24 -p tcp --dport 80 -j REDIRECT --to-port 8080

#wifi
iptables -A FORWARD -i enp0s8 -o enp0s3 -j ACCEPT
iptables -A FORWARD -o enp0s8 -j ACCEPT

#servidor http
iptables -A FORWARD -p tcp -m multiport --dports 80,443 -o enp0s10 -j ACCEPT
iptables -A FORWARD -p udp -m multiport --dports 80,443 -o enp0s10 -j ACCEPT
iptables -A FORWARD -p tcp -m multiport --dports 20,21 -i enp0s9 -o enp0s10 -s 13.0.0.2 -j ACCEPT
iptables -A FORWARD -p tcp -m multiport --dports 20,21 -i enp0s10 -o enp0s9 -s 13.0.0.2 -j ACCEPT
iptables -A FORWARD -p tcp -m multiport --dports 80,443 -o enp0s3 -j ACCEPT

#red trabajo
iptables -A FORWARD -p tcp -i enp0s9 -o enp0s3 -j ACCEPT
iptables -A FORWARD -o enp0s9 -m state --state ESTABLISHED,RELATED -j ACCEPT
[ 36 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 Corrector ^_ Ir a línea ^U Pág. sig.
```

Su continuación:

```
#servidor http
iptables -A FORWARD -p tcp -m multiport --dports 80,443 -o enp0s10 -j ACCEPT
iptables -A FORWARD -p udp -m multiport --dports 80,443 -o enp0s10 -j ACCEPT
iptables -A FORWARD -p tcp -m multiport --dports 20,21 -i enp0s9 -o enp0s10 -s 13.0.0.2 -j ACCEPT
iptables -A FORWARD -p tcp -m multiport --dports 20,21 -i enp0s10 -o enp0s9 -s 13.0.0.2 -j ACCEPT
iptables -A FORWARD -p tcp -m multiport --dports 80,443 -o enp0s3 -j ACCEPT

#red trabajo
iptables -A FORWARD -p tcp -i enp0s9 -o enp0s3 -j ACCEPT
iptables -A FORWARD -o enp0s9 -m state --state ESTABLISHED,RELATED -j ACCEPT
#Acceso al ruter
iptables -A INPUT -i enp0s9 -s 13.0.0.2 -j ACCEPT
```

Lo ejecutamos con bash y comprobamos que no nos da errores.

```
r0R:~$ sudo bash cortafuegos.sh
Aplicando reglas de redireccionamiento
r0R:~$ _
```

Aquí instalando apache en la maquina del servidor nos hemos dado cuenta de que no se puede instalar porque es una maquina xp, he creado un linux con la misma configuración.

Y aquí la comprobacion desde la maquina del ADM que va apache2.

