

Trabajo ASIS1

Patricia Briones Yus | 735576

Germán Garcés Latre | 757024

Red interna 1: 192.168.57.0/24

Red interna 2: 192.168.58.0/24

Red interna 3: 192.168.56.0/24

[Configuración] Debian1

Antes de encender la máquina, configurar las interfaces de red:

- NAT (enp0s3)
- Red interna 1 (enp0s8)
- Red interna 2 (enp0s9)
- Host-OnlyNetwork (enp0s10)

Modificar el fichero `/etc/network/interfaces` con las siguientes líneas:

```
# red interna 1
allow-hotplug enp0s8
iface enp0s8 inet static
address 192.168.57.1
netmask 255.255.255.0

# red interna 2
allow-hotplug enp0s9
iface enp0s9 inet static
address 192.168.58.1
netmask 255.255.255.0

# Ruta para acceder a la red interna 3
up route add -net 192.168.59.0 netmask 255.255.255.0 gw 192.168.58.6 dev
enp0s9

# red host-only
allow-hotplug enp0s10
iface enp0s10 inet static
```

```
address 192.168.56.5
netmask 255.255.255.0
```

Instalar paquete `isc-dhcp-server` y modificamos el fichero donde se definen las interfaces `/etc/default/isc-dhcp-server` añadiendo al final:

```
INTERFACES="enp0s9"
```

En el fichero `/etc/sysctl.conf` descomentar la linea:

```
net.ipv4.ip_forward=1
```

Crear `firewall` en `/etc/network/if-up.d` con el siguiente contenido:

```
#!/bin/sh

# Se activa el enrutamiento
echo "1" >/proc/sys/net/ipv4/ip_forward
iptables -F
iptables -P INPUT DROP
iptables -P FORWARD DROP

# Bloquear pings del host
iptables -A INPUT -i enp0s10 -p icmp --icmp-type echo-request -j REJECT

iptables -A INPUT -j LOG --log-prefix "netfilter-drop: "
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -i enp0s3 -p ALL -j ACCEPT

# Permite solo el trafico al servidor web en debian2 y al servidor ssh en
debian5
iptables -A FORWARD -d 192.168.59.5 -p tcp --dport 22 -j ACCEPT
iptables -A FORWARD -d 192.168.57.2 -p tcp --dport 80 -j ACCEPT

# Permite todo el tráfico intranet, y todo el tráfico de salida
iptables -A FORWARD -i enp0s8 -p ALL -j ACCEPT
iptables -A FORWARD -i enp0s9 -p ALL -j ACCEPT
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -i enp0s10 -p ALL -j ACCEPT
iptables -A INPUT -i enp0s3 -p ALL -j ACCEPT
iptables -A INPUT -i enp0s8 -p ALL -j ACCEPT
iptables -A INPUT -i enp0s9 -p ALL -j ACCEPT
```

```
iptables -A INPUT -i enp0s10 -p ALL -j ACCEPT
iptables -A OUTPUT -j ACCEPT

# Previene el acceso a los nodos desde el exterior
iptables -t nat -A POSTROUTING -s 192.168.57.0/24 -o enp0s3 -j MASQUERADE
iptables -t nat -A POSTROUTING -s 192.168.58.0/24 -o enp0s3 -j MASQUERADE
iptables -t nat -A POSTROUTING -o enp0s10 -j MASQUERADE

# Permitir que desde fuera y desde la red Host Only se pueda acceder al
servidor ssh
iptables -t nat -A PREROUTING -i enp0s3 -p tcp --dport 22 -j DNAT --to
192.168.59.5:22
iptables -t nat -A PREROUTING -i enp0s10 -p tcp --dport 22 -j DNAT --to
192.168.59.5:22

# Permitir que la red Host Only tenga acceso al servidor Apache (HTTP y HTTPS)
iptables -t nat -A PREROUTING -i enp0s10 -p tcp --dport 80 -j DNAT --to
192.168.57.2:80
iptables -t nat -A PREROUTING -i enp0s10 -p tcp --dport 443 -j DNAT --to
192.168.57.2:443
```

Este script se ejecutará al iniciar los servicios de red de `debian1`.

Cambiar los permisos y hacerlo ejecutable con `chmod 766 /etc/network/if-up.d/firewall && chmod +x /etc/network/if-up.d/firewall`

[Configuración] Debian2

Antes de encender la máquina, configurar las interfaces de red:

- Red interna 1 (`enp0s3`)

Modificar el fichero `/etc/network/interfaces` con las siguientes líneas:

```
# red interna 1
allow-hotplug enp0s3
iface enp0s3 inet static
address 192.168.57.2
netmask 255.255.255.0
gateway 192.168.57.1
```

Instalar el paquete `nginx`.

[Configuración] Debian3

Antes de encender la máquina, configurar las interfaces de red:

- Red interna 2 (enp0s3)

Modificar el fichero `/etc/network/interfaces` con las siguientes líneas:

```
# red interna 2
allow-hotplug enp0s3
iface enp0s3 inet dhcp

# Ruta para acceder a la red interna 3
up ip route add 192.168.59.0/24 via 192.168.58.6 dev enp0s3
```

[Configuración] Debian4

Antes de encender la máquina, configurar las interfaces de red:

- Red interna 2 (enp0s3)

Modificar el fichero `/etc/network/interfaces` con las siguientes líneas:

```
# red interna 2
allow-hotplug enp0s3
iface enp0s3 inet dhcp
```

[Configuración] Debian5

Antes de encender la máquina, configurar las interfaces de red:

- Red interna 3 (enp0s3)

Modificar el fichero `/etc/network/interfaces` con las siguientes líneas:

```
# red interna 3
allow-hotplug enp0s3
iface enp0s3 inet static
address 192.168.59.5
```

```
netmask 255.255.255.0
gateway 192.168.59.6
```

Instalar paquete `openssh-server` y ejecutar `systemctl enable ssh` para que se inicie en el arranque del sistema.

[Configuración] Debian6

Antes de encender la máquina, configurar las interfaces de red:

- Red interna 2 (`enp0s3`)
- Red interna 3 (`enp0s8`)

Modificar el fichero `/etc/network/interfaces` con las siguientes líneas:

```
# red interna 2
allow-hotplug enp0s3
iface enp0s3 inet static
address 192.168.58.6
netmask 255.255.255.0
gateway 192.168.58.1

# red interna 3
allow-hotplug enp0s8
iface enp0s8 inet static
address 192.168.59.6
netmask 255.255.255.0
```

En el fichero `/etc/sysctl.conf` descomentar la linea:

```
net.ipv4.ip_forward=1
```

Crear `firewall` en `/etc/network/if-up.d` con el siguiente contenido:

```
#!/bin/sh

# activar el enrutamiento
echo "1" >/proc/sys/net/ipv4/ip_forward

iptables -F
```

```
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -A INPUT -j LOG --log-prefix "netfilter-drop: "
iptables -A FORWARD -i enp0s3 -p ALL -j ACCEPT
iptables -A FORWARD -i enp0s8 -p ALL -j ACCEPT
iptables -A INPUT -i enp0s3 -p ALL -j ACCEPT
iptables -A INPUT -i enp0s8 -p ALL -j ACCEPT
iptables -A OUTPUT -j ACCEPT
iptables -t nat -A POSTROUTING -s 192.168.59.0/24 -o enp0s3 -j MASQUERADE
```

Este script se ejecutará al iniciar los servicios de red de `debian1`.

Cambiar los permisos y hacerlo ejecutable con `chmod 766 /etc/network/if-up.d/firewall && chmod +x /etc/network/if-up.d/firewall`

[Problemas] Debian1

- No se conseguía que `iptables` bloqueara las peticiones `icmp echo request`. Se vió que no estábamos dando un orden adecuado a las reglas por lo que algunas sobrescribían a otras.

[Problemas] Todas las máquinas

- Se tuvo que cambiar los servidores por defecto de las máquinas ya que estos no tenían conectividad, se usaron los [servidores DNS de google](#).

[Pruebas]

- ☑ Todas las máquinas debían `X` deberán verse entre sí mediante `ping`, y deben ver a Host (pero Host no las verá mediante `ping`).
- ☑ Todas las máquinas debían `X` se deben poder conectar a Internet (a través de `debian1`)
- ☑ Todas las máquinas (incluida Host) deben poder conectarse al servidor `ssh` en `debian5`
- ☑ Desde Host, con un navegador se debe poder conectar al servidor web en `debian1`, y verse la página web que se instala por defecto, o la que se ponga.