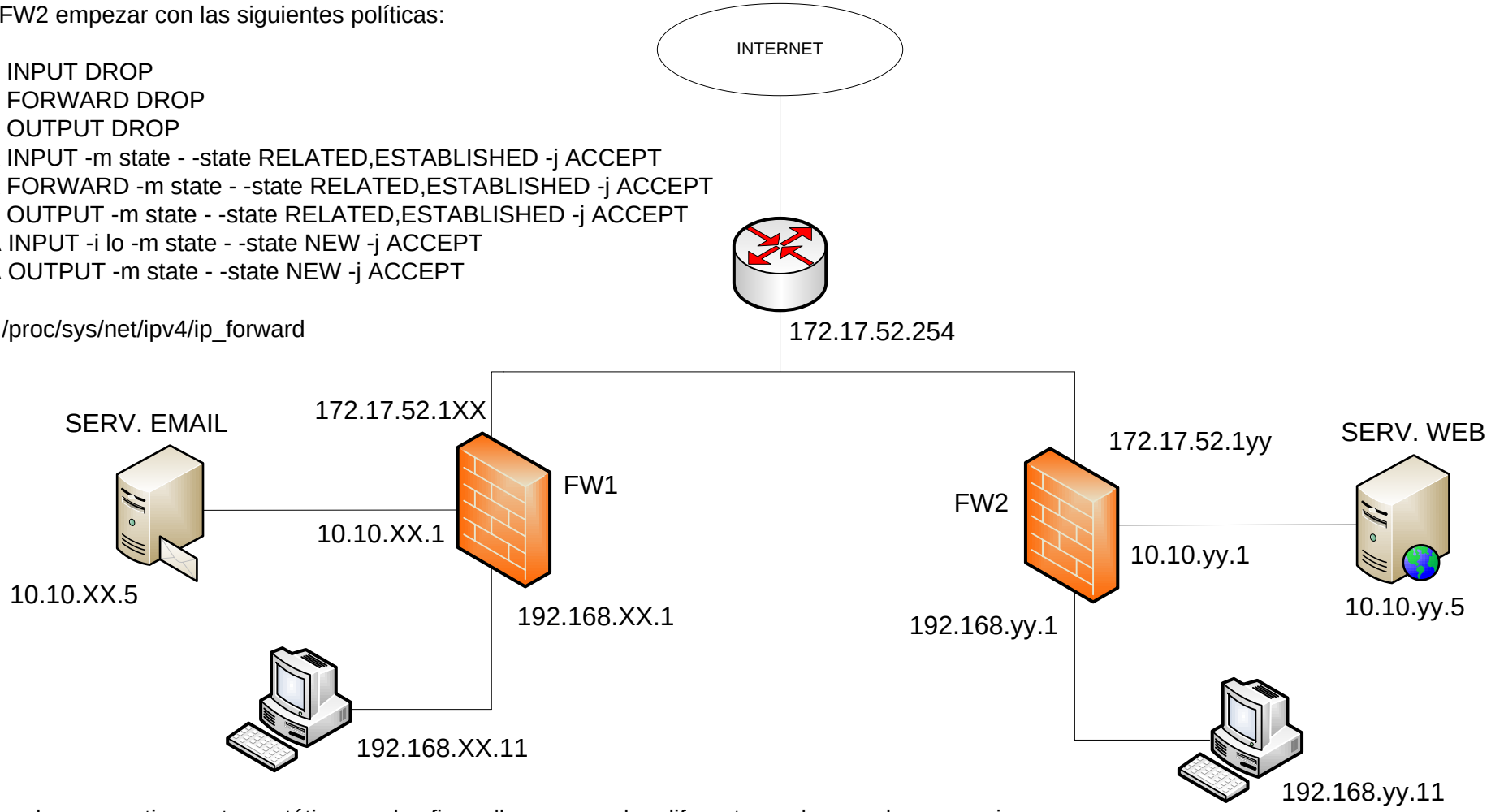
En FW1 y FW2 empezar con las siguientes políticas:

```
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT DROP
iptables -A INPUT -m state - -state RELATED,ESTABLISHED -j ACCEPT
iptables -A FORWARD -m state - -state RELATED,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -m state - -state RELATED,ESTABLISHED -j ACCEPT
Iptables -A INPUT -i lo -m state - -state NEW -j ACCEPT
Iptables -A OUTPUT -m state - -state NEW -j ACCEPT

echo “1” > /proc/sys/net/ipv4/ip_forward
```



1. Agregar las respectivas rutas estáticas en los firewalls para que las diferentes redes puedan comunicarse:

```
En FW1:  route  add  -net  10.10.yy.0   netmask  255.255.255.0  gw  172.17.52.1yy
         route  add  -net  192.168.yy.0 netmask  255.255.255.0  gw  172.17.52.1yy
En FW2:  route  add  -net  10.10.xx.0   netmask  255.255.255.0  gw  172.17.52.1xx
         route  add  -net  192.168.xx.0 netmask  255.255.255.0  gw  172.17.52.1xx
```

2. Las máquinas en las redes 192.168.xx.0/24 y 192.168.yy.0/24 deberán tener acceso a Internet a los protocolos:
   HTTP, HTTPS, DNS, ICMP (Ping)

3. Las máquinas en las redes 192.168.xx.0/24 y 192.168.yy.0/24 deberán tener acceso a ICMP (Ping) y SSH a sus respectivos Firewalls

4. Las máquinas en las redes 192.168.xx.0/24 y 192.168.yy.0/24 deberán tener acceso a ICMP (Ping) tanto al servidor EMAIL como al WEB; solamente SMTP, POP3 e IMAP4 al servidor EMAIL y solamente HTTP y HTTPS al servidor WEB.

5. Los servidores EMAIL y WEB deberán tener acceso únicamente a Internet y no se deberá permitir ningún otro tipo de conexión.