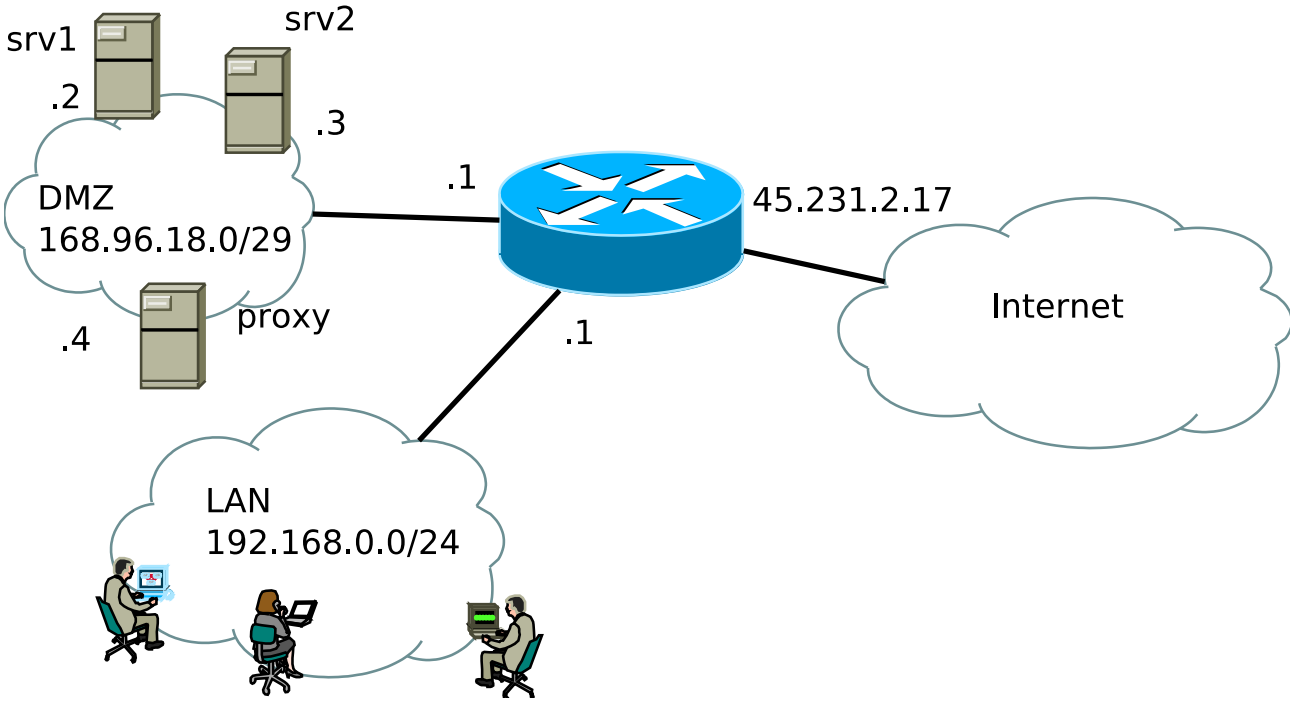
Ejercicio Firewall 20241107

En la red de la figura, ambos servidores tienen servicio DNS (53 TCP y UDP), el srv1 tiene aparte WWW (puertos 80 y 443 tcp), y el serv2 es servidor de correo y MX, ofreciendo los protocolos SMTP de transferencia y envio respectivamente (25, 587,465 TCP), POPs (TCP 995) e IMAPs (TCP 993). El servidor proxy web, atiende a los clientes de la LAN en el puerto 3128 TCP



Diseñe las reglas del firewall de tal manera de cumplir las siguientes especificaciones

LAN: los clientes de la LAN, solo pueden consultar DNS (TCP/UDP 53) a los servidores de la DMZ, no a los de Internet. Para navegar, solo pueden hacerlo a través del servidor proxy. Por lo tanto se les prohiben los accesos DNS y Web directos al exterior. Al resto de los servicios externos se puede acceder. Tener en cuenta que el servidor proxy necesita acceder a la web en nombre de los clientes.
Los clientes de la LAN solo pueden acceder a los puertos necesarios de los servidores de la DMZ (SMTP, IMAPs, POPs, WEB, DNS) pero nada más.

DMZ: Los servidores de la DMZ tienen acceso total a Internet pero no a la LAN. Desde el exterior, se puede acceder los servicios DNS, WEB y al servicio SMTP de transferencia (solo TCP 25) de los servidores correspondientes.

Utilizar NAT solo en los casos en que sea indispensable (se evaluará)

Solución

```
#! /usr/bin/bash
# Nota: eth0=LAN, eth1=DMZ, eth2=INTERNET
LAN=192.168.0.0/24
WEB=168.96.18.2
MAIL=168.96.18.3
PROXY=168.96.18.4
I=/sbin/iptables

# Politica por omisión de FORWARD (es decir lo que no matchee ninguna regla)
$I -P FORWARD DROP

# Reglas de estado (por omisión la tabla es FILTER)
$I -A FORWARD -m state --state INVALID -j DROP
$I -A FORWARD -m state --state ESTABLISHED, RELATED -j ACCEPT
#

# Accesos de los clientes de la LAN a la DMZ (tomo tanto la ip de origen como la
interfaz)
# Permiso desde la LAN al WEB y DNS TCP
$I -t filter -A FORWARD -m multiport -s $LAN -d $WEB -p tcp --dports 53,80,443 \
       -i eth0 -j ACCEPT
# Acceso al DNS de srv1 y srv2 por UDP
for J in $WEB $MAIL ; do
       $I -t filter -A FORWARD  -s $LAN -d $J -p udp --dport 53 \
              -i eth0 -j ACCEPT
done
# Acceso a servidor de mail (SMTP, SMTS cliente, POP3s, IMAPs, DNS x TCP
$I -t filter -A FORWARD -m multiport -s $LAN -d $MAIL -p tcp \
       --dports 25,587,465,993,995,53-i eth0 -j ACCEPT
# Acceso desde la LAN al PROXY
$I -t filter -A FORWARD -s $LAN -d $PROXY -p tcp –dport 3128 \
       -i eth0 -j ACCEPT
# Evito que desde la LAN se acceda a más puertos de los servidores
$I -A FORWARD -i eth0 -o eth1 -j REJECT

# Resto de los servicios externos
# Empiezo por lo que no tienen permitido salir a Internet
$I -A FORWARD -s $LAN -i eth0 -p tcp -o eth2 -m multiport \
--dports 53,80,443 -j REJECT
# Consulta DNS x UDP al exterior no permitida
$I -A FORWARD -s $LAN -i eth0 -p udp -o eth2 --dport 53 -j REJECT
# El resto si
$I -A FORWARD -s $LAN -i eth0 -o eth2 -j ACCEPT


# DMZ no accede a LAN
$I -A FORWARD  -i eth1 -o eth0 -j REJECT

# Pero si a Internet
$I -A FORWARD  -i eth1 -o eth2 -j ACCEPT

# Internet a DMZ
# Acceso a DNS x UDP
$I -A FORWARD -i eth2 -p udp --dport 53 -d $WEB -j ACCEPT
$I -A FORWARD -i eth2 -p udp --dport 53 -d $MAIL -j ACCEPT
# Acceso a WEB
$I -A FORWARD -i eth2 -d $WEB -p tcp -m multiport --dports 53,80,443 \
       -j ACCEPT
#Acceso a MAIL
$I -A FORWARD -i eth2 -d $MAIL -p tcp -m multiport --dports 53,25 \
       -j ACCEPT
# Como tiene POLICY DROP no hace falta bloquear Internet → LAN

# Reglas de NAT

# DMZ no requiere NAT en éste caso.
# LAN si
$I -t nat -A POSTROUTING -i eth0 -s $LAN -o eth2 -j SNAT --to 45.231.2.17
```