Manual de Redireccionamiento de Puertos en Proxmox

Escenario de Red

- **Subred del centro:** 10.10.13.0/24
- **IP de Proxmox:** 10.10.13.202
- **IP del Servidor (Web, NFS y VPN):** 10.10.16.2 (dentro de una VLAN en Proxmox)

Paso 1: Configurar el Redireccionamiento de Puertos con iptables

1.1 Habilitar el reenvío de paquetes en el kernel

Ejecutamos el siguiente comando para asegurarnos de que el reenvío de paquetes está activado:

```
sudo echo "net.ipv4.ip_forward=1" >> /etc/sysctl.conf
sudo sysctl -p
```

1.2 Configurar iptables en Proxmox

Ejecutamos los siguientes comandos para redirigir los puertos desde Proxmox (10.10.13.202) hacia el servidor (10.10.16.2):

Redirigir HTTP (80) y HTTPS (443) para el servidor web:

```
sudo iptables -t nat -A PREROUTING -i vmbr0 -p tcp --dport 80 -j DNAT
--to-destination 10.10.16.2:80
sudo iptables -t nat -A PREROUTING -i vmbr0 -p tcp --dport 443 -j DNAT
--to-destination 10.10.16.2:443
```

Redirigir el tráfico SSH (22) hacia el servidor:

```
sudo iptables -t nat -A PREROUTING -i vmbr0 -p tcp --dport 2222 -j DNAT
--to-destination 10.10.16.2:22
```

(De esta forma, para conectarnos por SSH desde fuera usaremos el puerto 2222 en Proxmox).

Redirigir el puerto del servidor NFS (2049):

```
sudo iptables -t nat -A PREROUTING -i vmbr0 -p tcp --dport 2049 -j DNAT
--to-destination 10.10.16.2:2049
```

Redirigir el puerto de la VPN (1194 UDP, el puerto de nuestra utilidad VPN, OpenVPN):

```
sudo iptables -t nat -A PREROUTING -i vmbr0 -p udp --dport 1194 -j DNAT
--to-destination 10.10.16.2:1194
```

Hacer NAT para permitir el tráfico de vuelta:

```
sudo iptables -t nat -A POSTROUTING -s 10.10.16.2 -o vmbr0 -j MASQUERADE
```

1.3 Guardar las reglas de iptables

Para que los cambios sean permanentes, guardamos las reglas (opcional):

```
sudo apt install iptables-persistent
sudo netfilter-persistent save
sudo netfilter-persistent reload
```

Paso 2: Verificar la Configuración

Para comprobar que las reglas están aplicadas correctamente:

```
sudo iptables -t nat -L -n -v
```

Para probar la conectividad desde una máquina externa:

```
curl http://10.10.13.202
```

Para probar SSH:

```
ssh -p 2222 usuario@10.10.13.202
```

Inciso

Siguiendo estos pasos, hemos configurado el redireccionamiento de puertos en Proxmox, asegurando que los servicios del servidor sean accesibles externamente mediante la IP de Proxmox. Además, hemos implementado el soporte para VLANs y garantizado la persistencia de las reglas de iptables tras reinicios del sistema. Con esta configuración, podemos gestionar los accesos de manera eficiente y segura. Asimismo y para facilitar futuros cambios en el servidor Proxmox, hemos decidido implementar un script que se ejecutará automáticamente al encenderse el servidor con todas estas reglas, garantizando que si en algún momento se desea hacer algún cambio o hay algo que no funciona bien, podamos corregir dichos cambios e inconvenientes. He aquí el script utilizado:

```
#!/bin/bash

# Definir variables
PROXMOX_IP="10.10.13.202"
SERVER_IP="10.10.16.2"

# Habilitar el reenvío de paquetes
echo "Habilitando el reenvío de paquetes..."
echo 1 > /proc/sys/net/ipv4/ip_forward
sysctl -w net.ipv4.ip_forward=1

# Limpiar reglas previas
iptables -t nat -F
iptables -F

# Configurar NAT (masquerade) para permitir tráfico entre VLANs
iptables -t nat -A POSTROUTING -o vmbr0 -j MASQUERADE

# Redirigir puertos de Proxmox a la máquina del servidor
# HTTP (80)
iptables -t nat -A PREROUTING -p tcp --dport 80 -d $PROXMOX_IP -j DNAT
--to-destination $SERVER_IP:80
iptables -A FORWARD -p tcp -d $SERVER_IP --dport 80 -m state --state
NEW,ESTABLISHED,RELATED -j ACCEPT

# HTTPS (443)
iptables -t nat -A PREROUTING -p tcp --dport 443 -d $PROXMOX_IP -j DNAT
--to-destination $SERVER_IP:443
```

```
iptables -A FORWARD -p tcp -d $SERVER_IP --dport 443 -m state --state
NEW,ESTABLISHED,RELATED -j ACCEPT

# SSH (22)
iptables -t nat -A PREROUTING -p tcp --dport 2222 -d $PROXMOX_IP -j DNAT
--to-destination $SERVER_IP:22
iptables -A FORWARD -p tcp -d $SERVER_IP --dport 22 -m state --state
NEW,ESTABLISHED,RELATED -j ACCEPT

# OpenVPN (1194/udp)
sudo iptables -t nat -A PREROUTING -i vmbr0 -p udp --dport 1194 -j DNAT
--to-destination 10.10.16.2:1194

# Bloquear tráfico entre VLAN 10 y VLAN 20
iptables -A FORWARD -i vmbr0.10 -o vmbr0.20 -j DROP
iptables -A FORWARD -i vmbr0.20 -o vmbr0.10 -j DROP

# Guardar reglas para que persistan tras reinicio
#apt install -y iptables-persistent
#netfilter-persistent save

# Mostrar reglas aplicadas
iptables -t nat -L -n -v
echo "Reglas aplicadas correctamente."
```