

Unknown Title



Conversación con Gemini

Estoy haciendo esto "Router OpenWRT

Conectar Ethernet1 a la nube NAT y Ethernet0 a un switch. El resto de las interfaces no están configurada la IP.

No pide

contraseña, no se la configures. Solo usa "ip a".

Si quisieras

configurarlo, puedes hacerlo por el terminal ("Buena suerte, jeje").

Mejor usa

túneles: Pon un "webtermi-winbox" en el diagrama. Conéctalo a la LAN del router. Después configura un contenedor o VM en Proxmox y úsalos para conectarlo.

```
ssh -p 22 root@10.2.7.62 -R 10.2.7.50:1080:192.168.1.1:80 -fN
```

```
ssh -p 22 "usuario"@"pc_con_acceso" -R
```

```
"pc_con_acceso":1080:"pc_del_diagrama":80 -fN
```

Comprueba en "pc_con_acceso" que está escuchando por el puerto:

```
ss -ltnp | grep 1080
```

Tiene que salir algo así:

Si ves 0.0.0.0:1080 o 10.2.7.62:1080 = está escuchando en la interfaz

pública y podrás conectarte desde otra máquina a 10.2.7.62:1080.

Si aparece 127.0.0.1:1080 solo está ligado a localhost — entonces solo

desde el propio 10.2.7.62 podrás usar curl http://127.0.0.1:1080.

Ahora puedes poner la ip del pc_con_acceso en el navegador así:

```
http://10.2.7.62:1080
```

" y tengo este problema "Si aparece 127.0.0.1:1080 solo está ligado a localhost — entonces solo

desde el propio 10.2.7.62 podrás usar curl http://127.0.0.1:1080." Como solucionarlo?



El problema que describes, donde el **reenvío de puerto remoto SSH** solo se enlaza a 127.0.0.1:1080 (localhost) en el pc_con_acceso (en tu ejemplo 10.2.7.62), significa que el túnel solo es accesible desde la propia máquina que estableció la conexión SSH (10.2.7.62).

Para que otros dispositivos en la red puedan acceder al túnel a través de la IP pública o de red del pc_con_acceso (es decir, 10.2.7.62:1080), necesitas que el **servidor SSH** en pc_con_acceso permita que el puerto reenviado se enlace a **todas las interfaces** (a 0.0.0.0:1080).

Solución: Modificar la Configuración SSH

La solución más común y segura implica un cambio en el archivo de configuración del servidor SSH (sshd) en el pc_con_acceso (10.2.7.62).

1. **Edita el archivo de configuración de SSH:** Abre el archivo de configuración del demonio SSH (sshd_config) en el pc_con_acceso. Esto generalmente se hace con un editor de texto con privilegios de superusuario:

```
sudo nano /etc/ssh/sshd_config
```

2. Añade o Descomenta la Directiva: Asegúrate de que la siguiente directiva esté presente y **no esté comentada** (sin # al inicio). Si no está, añádela:

```
GatewayPorts yes
```

- **GatewayPorts yes** indica al servidor SSH (sshd) que permita el reenvío de puertos remotos para enlazar a direcciones no locales (como 0 . 0 . 0 . 0), haciéndolo accesible desde fuera de la máquina.

3. Reinicia el Servicio SSH: Despues de modificar el archivo, debes reiniciar el servicio para que el cambio surta efecto:

```
sudo systemctl restart sshd
# 0 a veces:
# sudo service sshd restart
```

Verificación

1. Vuelve a establecer el túnel: Una vez reiniciado el servicio SSH en pc_con_acceso, ejecuta de nuevo tu comando de túnel SSH desde tu máquina:

```
ssh -p 22 root@10.2.7.62 -R 10.2.7.50:1080:192.168.1.1:80 -fN
```

(Nota: El 10.2.7.50 en el comando es la IP de la interfaz en pc_con_acceso a la que deseas que se enlace. Si quieres que se enlace a **todas las interfaces**, puedes usar 0.0.0.0 o, más comúnmente, **omitar la IP** y solo poner el puerto: -R 1080:192.168.1.1:80).

2. Comprueba el enlace nuevamente en pc_con_acceso: Ejecuta el comando ss de nuevo:

```
ss -ltnp | grep 1080
```

Ahora deberías ver que el servicio está escuchando en 0 . 0 . 0 . 0 :1080 (todas las interfaces) o 10 . 2 . 7 . 62 :1080 (la interfaz pública/de red específica), lo que te permitirá acceder desde otras máquinas usando la IP http://10.2.7.62:1080.

¿Te gustaría que te ayude a verificar si tienes el archivo de configuración SSH correcto en tu sistema?

C

Gemini puede cometer errores, incluso sobre personas, así que verifica sus respuestas. [Tu privacidad y GeminiSe abre en una ventana nueva](#)

