

Conexiones fallan desde LAN pero funcionan desde WAN

Introducción

Resumen rápido de un problema que rompía WireGuard y RustDesk al acceder desde LAN con dominios públicos. La solución fue más simple de lo esperado, pero no tan obvia si no conoces cómo funciona OpenWrt.

“ ⚠ Este fue **mi caso concreto**. Dependiendo de la configuración de cada red o router, el comportamiento puede variar.

Problema

Desde la red local (LAN), al acceder a servicios expuestos mediante redirección de puertos (DNAT) usando el dominio público o la IP WAN del router, la conexión fallaba.

Ejemplo: `mi.dominio.net:51820` no funcionaba desde LAN, pero sí desde fuera (móvil con datos).

Causa

OpenWrt tiene activado por defecto el loopback NAT para las reglas DNAT (también llamado *reflection*), lo que permite acceder desde LAN usando la IP pública del router.

Pero si el loopback usa como origen la IP **interna** del router (`192.168.X.X`), algunos servicios lo rechazan, porque esperan que la conexión venga de una IP pública (como haría cualquier cliente externo real).

Solución aplicada

En el panel LuCI, dentro de la sección de redirección de puertos:

1. Mantener activado el **NAT loopback** (reflection).
 2. Cambiar el parámetro "**IP de origen del bucle de retorno**" de:
 - Dirección IP interna
 - a Dirección IP externa
-

¿Qué hace esto?

- Obliga al router a simular el tráfico como si viniera realmente del exterior (usando su IP pública).
 - Así, los servicios como WireGuard o RustDesk no lo rechazan.
 - Se evita tener que hacer apaños como hijack DNS, split-horizon o reglas extra de firewall.
-

Resultado

- ✓ WireGuard conecta sin problemas desde LAN usando el dominio externo.
 - ✓ RustDesk también funciona correctamente desde dentro.
 - ✓ No hizo falta tocar reglas, ni montar DNS especial ni nada raro.
-

Resumen rápido

- Fallo al acceder desde LAN usando dominios públicos con redirección de puertos.
 - Loopback NAT activado, pero usaba IP interna como origen.
 - Cambio a IP externa como origen: todo arreglado.
 - Solución limpia sin DNS ni reglas extra.
-

Notas personales

No hacía falta desactivar el loopback, ni liarse con split-DNS. El fallo fue por no fijarse en la IP de origen del loopback.

Referencias

- [Documentación de OpenWrt sobre el firewall para mas información.](#)
-

Revision #1

Created 2025-06-14 17:56:04 UTC by Juan Francisco

Updated 2025-12-22 20:20:18 UTC by Juan Francisco