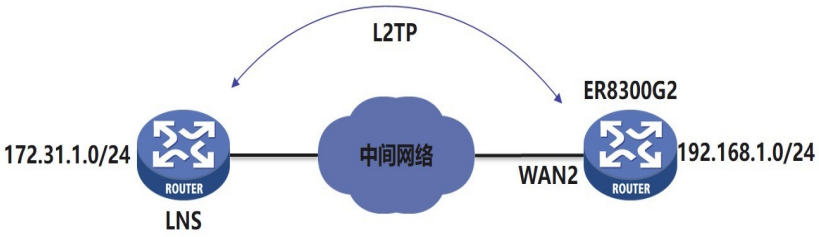
ER8300G2作为L2TP客户端访问LNS内网不通问题经验案例

L2TP VPN 郭昊 2019-01-03 发表

组网及说明



ER8300G2设备作为L2TP客户端，对应公网口为WAN2。

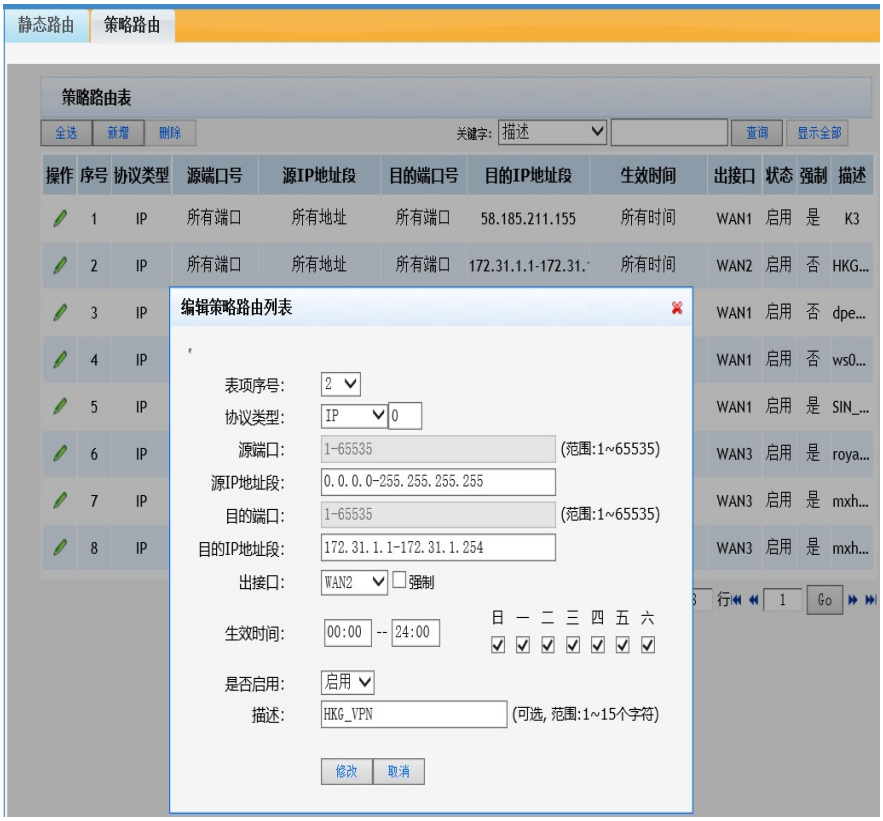
问题描述

L2TP可以正常拨号，拨上后ER8300G2的内网192.168.1.0/24无法访问LNS侧的内网172.31.1.0/24。

过程分析

192.168.1.0/24访问172.31.1.0/24时，在ER8300G2的内网口抓包，发现有192.168.1.1 ping 172.31.1.1的ping request，没有回来的reply。ER8300G2的外网口抓包，发现本端发出的icmp报文，没有封装L2TP，只有IP头。

之后查看设备配置，发现设备上配置了策略路由，将目的地址为172.31.1.0/24的报文，发到WAN2口去了。这种情况下，设备不会进行L2TP封装，直接将IP包从WAN2发出去了，这样私网IP头的报文在公网上不通。



这个现象可以理解为，设备拨L2TP后，会生成一个l2tp0的虚拟口，如果策略路由将报文发到WAN2，没有进l2tp0，就没有正确封装L2TP头。

解决方法

删除设备上与L2TP业务地址重叠的策略路由后正常。