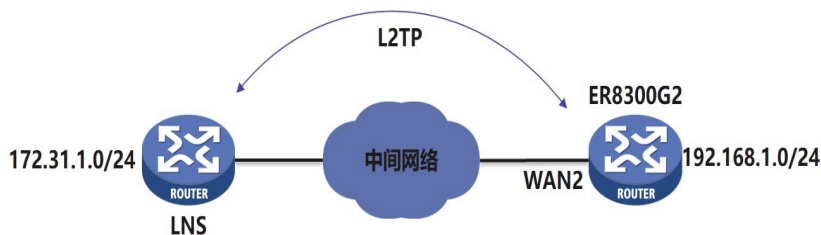


知 ER8300G2作为L2TP客户端访问LNS内网不通问题经验案例

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头的报文在公网不通。

静态路由 策略路由

策略路由表

全选 新增 删除 关键字: 描述 查询 显示全部

操作	序号	协议类型	源端口号	源IP地址段	目的端口号	目的IP地址段	生效时间	出接口	状态	强制	描述
	1	IP	所有端口	所有地址	所有端口	58.185.211.155	所有时间	WAN1	启用	是	K3
	2	IP	所有端口	所有地址	所有端口	172.31.1.1-172.31.1.254	所有时间	WAN2	启用	否	HKG...
	3	IP						WAN1	启用	否	dpe...
	4	IP						WAN1	启用	否	ws0...
	5	IP						WAN1	启用	是	SIN...
	6	IP						WAN3	启用	是	roya...
	7	IP						WAN3	启用	是	mxh...
	8	IP						WAN3	启用	是	mxh...

编辑策略路由列表

表项序号: 2

协议类型: IP 0

源端口: 1-65535 (范围:1~65535)

源IP地址段: 0.0.0.0-255.255.255.255

目的端口: 1-65535 (范围:1~65535)

目的IP地址段: 172.31.1.1-172.31.1.254

出接口: WAN2 强制

生效时间: 00:00 -- 24:00 日 一 二 三 四 五 六

是否启用: 启用

描述: HKG_VPN (可选, 范围:1~15个字符)

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。