某局点ER5200G2路由器做LNS侧设备时,外网终端L2TP VPN接入无法访问 内网终端问题排查

L2TP VPN **徐猛** 2018-06-05 发表

组网及说明

不涉及

某局点现场配置了L2TP VPN,使用我司的ER5200G2设备做为网络中的LNS设备,L2TP隧道正 常建立,LAC侧内网终端使用PPP的方式获取地址,且能够获取地址成功。但是出现了一个奇怪的现 象,LAC侧终端能够访问通LNS侧内网终端的内网网关,但是无法ping通内网终端。

过程分析

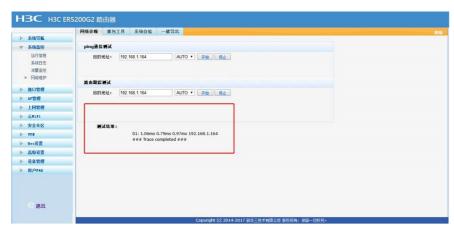
1.开始怀疑LNS侧内网终端是不是因为没有配置网关,从而导致LAC侧终端的ping报文到了LNS侧 终端后,LNS侧终端回包时出现问题。但是现场检查,LNS侧内网终端均正确的配置了网关信息。 2.让现场收集了ER5200G2的相应的配置信息。







> 系统导航	网络诊断 抓包工具 系统自检 一號写出	秋1
w 系统监控	ping通信测试	
运行信息 系统日志	目的地址: 192.168.1.164 AUTO ▼ 开绘 停止	
流量溢控		
> 网络维护	新由聚森剌试	
≫ 接口管理	目的地址: AUTO ▼ 开始 停止	
➢ AP管理		
上同管理		
> Zviri		
> 安全专区	测试结果:	
> VPM	PING 192.168.1.164: 56 data bytes, press CTRL_C to break	
≫ Qou设置	Reply from 192.168.1.164: bytes=56 Sequence=1 ttl=64 time=0.4 ms Reply from 192.168.1.164: bytes=56 Sequence=2 ttl=64 time=0.3 ms	
> 高級设置	Reply from 192.168.1.164: bytes=56 Sequence=3 ttl=64 time=0.8 ms	
没备管理	Reply from 192.168.1.164: bytes=56 Sequence=4 ttl=64 time=0.6 ms 192.168.1.164 ping statistics	
> 用户YAQ	4 packets transmitted,	
	4 padets received, Ofu padets loss ginna, e 0.3(0.5/10.8 ms round-trip impli-ayelina = 0.3(0.5/10.8 ms ### Offu completed ###	
三 源出		



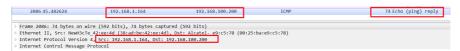
根据现场发来的L2TP相关配置,检查后并未发现L2TP配置存在问题。

3.让现场进行LAC侧终端ping测试LNS侧下联终端,同时在ER5200G2的LAN口和WAN口进行抓包。 抓包后发现:

在设备的WAN口处可以看到经过L2TP封装的,由LAC侧终端地址192.168.100.200到LNS侧终端地址192.168.1.164的ping报文,类型为ping请求报文。同时外层封装使用的公网地址为:源地址119.1 35.100.155,目的地址14.23.98.58,使用L2TP隧道协议封装。



但是查看回包时发现了问题,在查看由LNS侧终端地址192.168.1.164发给LAC侧终端地址192.168.1.00.200的ping回应报文时,发现该回应报文并未经过L2TP封装就被从WAN口发了出来。



由于之前现场描述,LAC侧终端能够ping通对端LNS侧内网的网关,且在我司ER设备上对于本地始发的报文是不会匹配策略路由的,回包不会受策略路由配置影响。于是怀疑现场的ER5200G2路由器上是不是因为配置了策略路由,从而在LAC侧终端ping测试对端LNS侧内网的终端时,导致内网终端回包匹配了策略路由,而并未发给L2TP的隧道接口进行封装。

解决方法

现场检查设备的策略路由配置,发现客户之前自行配置了策略路由,与之前的预想原因一致,让现场工程师修改策略路由配置后,问题解决。