MSR3640路由器映射ssl vpn服务不成功经验案例

NAT SSL VPN GRE VPN 孙兆强 2019-07-25 发表

组网及说明

防火墙在内网提供ssl vpn服务，MSR3640做nat server映射ssl vpn端口。

问题描述

现场pc连接公网拨ssl vpn正常，客户移动定制平板通过4G网络无法拨成功。

过程分析

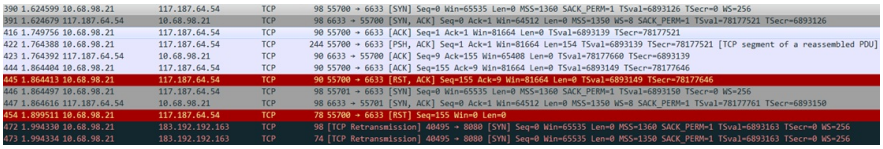
1、查看路由器nat server配置

nat server protocol tcp global 117.187.64.xx 6633 inside 10.10.112.21 443

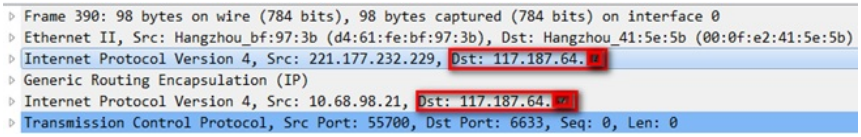
PC能拨号成功说明MSR3640映射配置及FW的ssl vpn配置均没问题。

2、移动平板拨号时在路由器上查看nat会话dis nat session destination-ip 117.187.64.xx verbose无任何会话信息，且FW上未抓包任何相关报文。pc拨号时有nat会话。怀疑是移动平板拨号时报文没发到路由器。

3、移动平板拨号时接口抓包查看，报文已发过来，但从报文结构看，移动平板是先与MSR3640路由器建立GRE，拨ssl vpn的流量封装在GRE里面。



第一个SYN报文展开如下，内层目的地址和外侧目的地址相同，均为路由器公网口地址。



有TCP协商和重传报文且无nat会话，说明路由器公网口nat没生效，路由器回复了tcp协商报文。

4、路由的处理逻辑是，在公网口对报文只做一次处理，先处理GRE封装，nat server没生效。GRE解封装后内层报文在Tunnel口处理。

解决方法

在路由器GRE的Tunnel口做nat server

nat server protocol tcp global 117.187.64.xx 6633 inside 10.10.112.21 443