某局点 SecPath F1080(V7) L2TP无法拨入经验案例

L2TP VPN 关萌 2019-11-30 发表

组网及说明

拓扑： 局点（华为系列路由器）-----专线-----F1080防火墙-------终端
用户使用我司F1080替换原来一款家用路由器，替换完成后发现，L2TP排号不成功。

问题描述

当前把F1080防火墙替换原来的普通路由器替换，L2TP使用的是微软自带的连接工具，接上防火墙ping测试正常，L2TP无法拨号成功， 专线接回原来路由器可以拨号成功，原来的路由是是一台很普通的家用路由器上面也没有相关的策略 。

过程分析

从收集信息看，拨号时可以看到用户的会话。F1080上只做了nat outbound，用户L2TP拨号流量只经过了NAT outbound。流量流经防火墙时也做了NAT alg。还是无法正常拨号成功。
于是通过抓包分析，通过抓包分析，LNS收到SCCRQ报文后，LNS重定向到端口209796 从20796回复报文到FW时，匹配不到原来会话，也没有NAT。我们的NAT无限转，报文回来时，源端口变化，匹配不到原来NAT会话。原始报文是UDP的1701端口。

```
> Frame 516: 124 bytes on wire (992 bits), 124 bytes captured (992 bits)
> Ethernet II, Src: [illegible]
> Internet Protocol [illegible]
> User Datagram Protocol, Src Port: 20796, Dst Port: 1080
> Layer 2 Tunneling Protocol
```

解决方法

通过以上信息分析，可以配置下面命令解决。
nat mapping-behavior命令用来配置PAT方式出方向动态地址转换的模式。
undo nat mapping-behavior命令用来恢复缺省情况。
【命令】 nat mapping-behavior endpoint-independent [acl { ipv4-acl-number | name ipv4-acl-name }] undo nat mapping-behavior endpoint-independent
【缺省情况】 PAT出方向动态方式地址转换的模式为Address and Port-Dependent Mapping。
【视图】 系统视图 【缺省用户角色】 network-admin mdc-admin
【参数】 acl：指定ACL的编号或名称，用于控制需要遵守指定地址转换模式的报文范围。 ipv4-acl-number：ACL的编号，取值范围为2000～3999。 name ipv4-acl-name：ACL的名称，为1～63个字符的字符串，不区分大小写，必须以英文字母a～z或A～Z开头。为避免混淆，ACL的名称不允许使用英文单词all。
【使用指导】 PAT方式出方向动态地址转换支持两种模式：
·Endpoint-Independent Mapping（不关心对端地址和端口的转换模式）：只要是来自相同源地址和源端口号的报文，不论其目的地址是否相同，通过PAT映射后，其源地址和源端口号都被转换为同一个外部地址和端口号，该映射关系会被记录下来并生成一个EIM表项；并且NAT网关设备允许外部网络的主机通过该转换后的地址和端口来访问这些内部网络的主机。这种模式可以很好的支持位于不同NAT网关之后的主机间进行互访。
· Address and Port-Dependent Mapping（关心对端地址和端口的转换模式）：对于来自相同源地址和源端口号的报文，若其目的地址和目的端口号不同，由于相同的源地址和源端口号不要求被转换为相同的外部地址和端口号，所以通过PAT映射后，相同的源地址和源端口号通常会被转换成不同的外部地址和端口号。并且NAT网关设备只允许这些目的地址对应的外部网络的主机才可以通过该转换后的地址和端口来访问这些内部网络的主机。这种模式安全性好，但是不便于位于不同NAT网关之后的主机间进行互访。