某局点经过F1080 NAT转发之后，内网用户L2tp VPN 拨号失败问题

L2TP VPN 刘文峰 2019-11-30 发表

组网及说明

无

问题描述

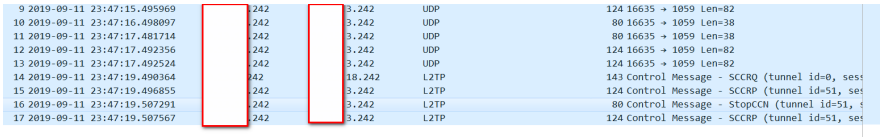
某局点采用我司F1080替换家用路由器做出口设备做NAT，替换完之后，内网能正常访问外网，但是内网用户去L2tp 拨号公网的华为路由器发现L2tp 无法拨号成功，如果把电脑连接接在外网或者把F1080换成家用路由器就可以拨号成功，怀疑还是F1080问题导致。

过程分析

1. 在外网口开启和关闭NAT ALG 都无法解决。
2. 设备外网口只配置了NAT转换，并无其他特殊配置，安全策略也都是内外都放通了。

```
interface GigabitEthernet1/0/3
 port link-mode route
 description To_NewNongHe
 ip address x.x.x.x 255.255.255.240
 mirroring-group 1 mirroring-port both
 nat outbound 3002
```

3. 对比正常的抓包和不正常的抓包，发现是华为设备回应了stopccn，但是如果不过我们设备就正常，怀疑还是设备问题导致华为设备回应了stopccn报文。



9	2019-09-11 23:47:15.495969	.242	3.242	UDP	124	16635 → 1059 Len=82
10	2019-09-11 23:47:16.498097	.242	3.242	UDP	80	16635 → 1059 Len=38
11	2019-09-11 23:47:17.481714	.242	3.242	UDP	80	16635 → 1059 Len=38
12	2019-09-11 23:47:17.492356	.242	3.242	UDP	124	16635 → 1059 Len=82
13	2019-09-11 23:47:17.492524	.242	3.242	UDP	124	16635 → 1059 Len=82
14	2019-09-11 23:47:19.490364	242	18.242	L2TP	143	Control Message - SCCRQ (tunnel id=0, ses
15	2019-09-11 23:47:19.496855	.242	3.242	L2TP	124	Control Message - SCCRP (tunnel id=51, se
16	2019-09-11 23:47:19.507291	.242	3.242	L2TP	80	Control Message - StopCCN (tunnel id=51,
17	2019-09-11 23:47:19.507567	.242	3.242	L2TP	124	Control Message - SCCRP (tunnel id=51, se

解决方法

后续建议客户配置NAT static 测试，发现配置之后，能够拨号成功，怀疑是在NAT outbound 转换时由于端口号问题导致。

最终让客户在全局配置NAT mapping-behavior endpoint-independeng mapping 之后问题解决。

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。