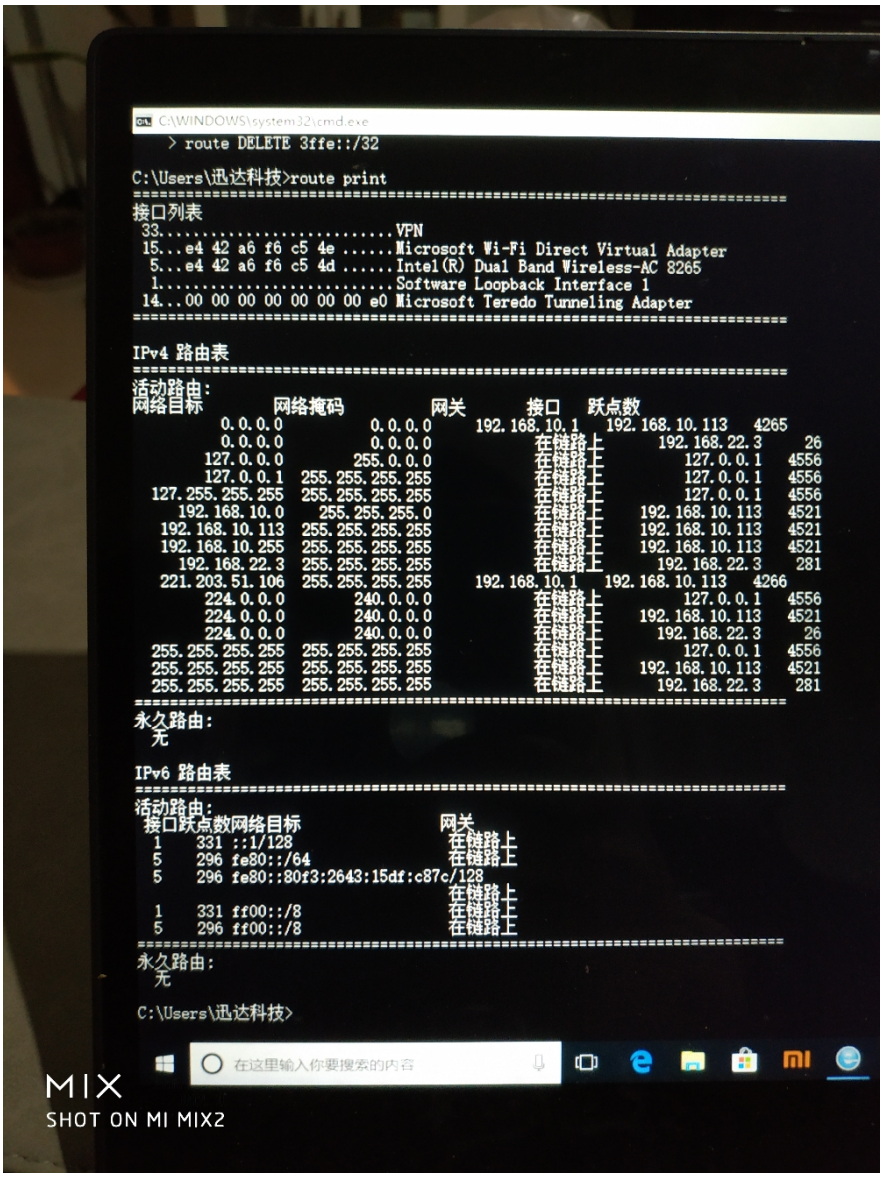
l2tp拨号总部成功后经ipsec访问分部

刘银川 2018-01-24 发表

客户平时出差，通过l2tp拨号访问总部，上网方式为PPPOE拨号。总部是固定IP上网，分部是PPPOE拨号上网，总部与分部间已经建立了野蛮模式的ipsec vpn，现在客户要达成访问分部私网的需求。

由于客户与分部均为PPPOE拨号上网，一般的vpn均不能满足直接访问的需求，可以通过ipsec访问域名来实现。但由于分部数量众多，操作繁琐，于是想到可以利用现网环境来满足需求。当客户与总部建立起l2tp vpn后，会自动生成一条优先级最高的默认路由，指向总部VT接口。那么只需要在已有的ipsec vpn的感兴趣流中匹配到l2tp和分部私网的地址，便可以实现从总部经ipsec访?问分部的目的。



在总部与分部的ipsec感兴趣流中加入l2tp和分部私网的地址，由于总部是模板的方式，所以要先由分部触发ipsec流，在总部生成一条源为l2tp目的为分部私网的ipsec sa。当客户访问分部私网时，会将请求包发给总部，总部匹配到ipsec感兴趣流，会与分部之间建立起对应的ipsec vpn，然后分部通过vpn与客户建立连接

关键配置:

总部:

```
acl advanced 3001
 rule 5 deny ip source 192.168.22.0 0.0.0.255 destination 192.168.0.0 0.0.0.255   //nat穿越
acl advanced 3010
 rule 5 permit ip source 192.168.22.0 0.0.0.255 destination 192.168.0.0 0.0.0.255
//ipsec中放通l2tp到分部私网的acl
```

分部:

```
acl number 3001
 rule 5 permit ip source 192.168.20.0 0.0.0.255 destination 192.168.22.0 0.0.0.255
//ipsec中放通分部私网到l2tp的acl
acl number 3010
```

rule 5 deny ip source 192.168.20.0 0.0.0.255 destination 192.168.22.0 0.0.0.255 //nat穿越

1、由于ipsec是野蛮模式，所以需要分部主动触发，但这样就要求每次访问总部前都要分部先触发，过于繁琐。可以在总部建一个环回口，地址为l2tp的网段，然后在分部长连接该地址（NTP或NQA协议，活学活用），保证ipsec隧道不老化。这样客户只要拨号到总部便可以随时随地访问分部，简便快捷。

（参考案例：11145）

2、在遇到类似问题时，建议根据客户的需求及现网环境找出最简单有效的解决方法，不要墨守成规，只用学到的东西生搬硬套。