

某局点F1070终端使用inode 拨号L2tp over ipsec 不成功问题处理经验案例

L2TP over IPsec VP

刘文峰 2020-04-11 发表

组网及说明

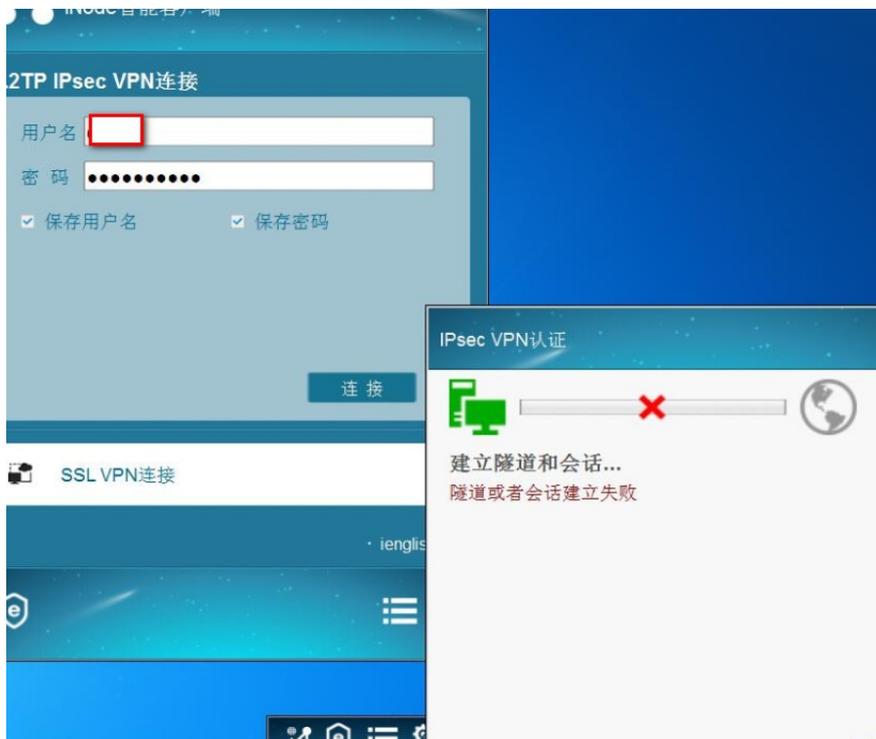
组网:



问题描述

某局点采用F1070做L2tp over ipsec, 设备部署在内网, 出口为其他路由器, 外网已把L2tp 和IPsec 端口都做了映射, 配置完成之后, 发现终端使用inode 无法拨号成功, 提示建立隧道或会话失败, 具体看下图:





过程分析

远程到设备上调试发现，dis ike sa 和dis ipsec sa 都已建立成功，但是dis l2tp tunnel 看隧道状态是Wait-connect，怀疑是l2tp 出了问题，但是在终端上如果取消ipsec，单独拨l2tp是发现可以拨号成功，并且获取地址，感觉l2tp 的配置也没有问题。

关键配置：

```
interface Virtual-Template2
  ppp authentication-mode pap
  ppp ipcp dns
  remote address pool 2
  ip address 192.
ipsec transform-set vpn_IPv4_20
  esp encryption-algorithm des-cbc
  esp authentication-algorithm md5
#
ipsec policy-template inode 10
  transform-set vpn_IPv4_20 1 2 3 5 6
  local-address x
  ike-profile x
ipsec policy vpn 5 isakmp template inode
l2tp-group 3 mode lns
  allow l2tp virtual-template 2 remote x
  undo tunnel authentication
  tunnel name vpn2
#
l2tp enable
ike profile vpn_IPv4_20
keychain vpn_IPv4_20
exchange-mode aggressive
local-identity fqdn x
match remote identity fqdn xx
proposal 1 2 3 4 5 10
#
ike proposal 1
  encryption-algorithm aes-cbc-128
  dh group2
  authentication-algorithm md5
#
ike proposal 2
  encryption-algorithm 3des-cbc
  dh group2
```

```
authentication-algorithm md5
#
ike proposal 3
encryption-algorithm 3des-cbc
dh group2
#
ike proposal 4
encryption-algorithm aes-cbc-256
dh group2
#
ike proposal 5
dh group2
#
ike proposal 10
#
ike keychain vpn_IPv4_20
pre-shared-key address 0.0.0.0 0.0.0.0 key cipher $c$3$Oa263eXaf5cEm8O3bFrVKk/S1Xl7aj2LQw
==
#
```

解决方法

从测试结果来说，l2tp 和 ipsec 的配置应该都没问题，怀疑可能是inode设置问题，但是inode 上 ipsec 的设置应该没问题，dis ike sa 和 ipsec sa 都有，怀疑是inode 上的l2tp 设置问题，分析当前组网，由于Ins 在内网，按照l2tp over ipsec 的原理，内层是l2tp 报文，外层是ipsec 报文，所以inode 上设置的话，ipsec 地址为公网地址，Ins的地址为内网地址，修改之后，重新拨号，问题解决。

