

## 知 MSR3620在使用INODE客户端拨入L2TP OVER IPSEC时需要取消上传客户端版本号

L2TP VPN IPsec VPN 刘嘉炜 2019-03-29 发表

### 组网及说明

无

### 问题描述

客户使用INODE软件登录L2TP OVER IPSEC时提示PPP协商超时，排查配置发现IPSEC已经可以正常建立。但是客户端单独使用WINDOWS客户端L2TP VPN却可以拨号成功。

### 过程分析

配置：

```
ipsec transform-set 1
esp encryption-algorithm 3des-cbc
esp authentication-algorithm md5
#
ipsec policy-template newvpn 1
transform-set 1
local-address 10.*.*.138
ike-profile newvpn
#
ike profile newvpn
keychain 11
local-identity fqdn ct-center
exchange-mode aggressive    \IKE协商模式没有设置
match remote identity fqdn newvpn
match remote identity fqdn newvpn1
match remote identity fqdn newvpn2
match remote identity fqdn newvpn3
match remote identity fqdn newvpn4
match remote identity fqdn newvpn5
match remote identity fqdn newvpn6
match remote identity address 0.0.0.0 0.0.0.0    \补充此命令
match local address 10.*.*.138
proposal 1
#
ike keychain 11
pre-shared-key address 0.0.0.0 0.0.0.0 key cipher $c$3$AN6dG1frG97zT0oMdyQ==
#
ike proposal 1
#
ike identity fqdn ct-center
#
interface Virtual-Template1
ppp authentication-mode chap domain system
remote address pool 1
ip address 10.*.*.49 255.255.255.248
#
local-user hhgnsyh6 class network
password cipher $c$3$iffa5QQ3KukwhA==
service-type ppp
authorization-attribute user-role network-operator
#
l2tp-group 1 mode lns
allow l2tp virtual-template 1
undo tunnel authentication
tunnel name LNS
#
l2tp enable
查看IPSEC VPN建立情况，发现IPSEC VPN已经正常建立连接，并生成安全联盟：
IPsec policy: policy1
```

Sequence number: 102

Mode: Template

-----

Tunnel id: 2

Encapsulation mode: tunnel

Perfect Forward Secrecy:

Inside VPN:

Extended Sequence Numbers enable: N

Traffic Flow Confidentiality enable: N

Path MTU: 1444

Tunnel:

local address: 10.200.251.138

remote address: 172.27.79.9

Flow:

sour addr: 10.200.251.138/255.255.255.255 port: 1701 protocol: udp

dest addr: 172.27.79.9/255.255.255.255 port: 0 protocol: udp

<ZYNX\_MSR3640\_4G\_VPN>dis ike sa

Connection-ID	Remote	Flag	DOI
---------------	--------	------	-----

-----

184	172.27.79.9	RD	IPsec
-----	-------------	----	-------

既然PPP报错于是debug PPP从中寻找问题原因，发现客户端发送challenge No. 1报文后PPP提示认证失败。

%Mar 23 15:49:21:305 2019 ZYNX\_MSR3640\_4G\_VPN IFNET/3/PHY\_UPDOWN: Physical state on the interface Virtual-Access0 changed to up.

%Mar 23 15:49:21:321 2019 ZYNX\_MSR3640\_4G\_VPN IFNET/5/LINK\_UPDOWN: Line protocol state on the interface Virtual-Access0 changed to up.

\*Mar 23 15:49:24:403 2019 ZYNX\_MSR3640\_4G\_VPN PPP/7/CHAP\_EVENT\_0:

PPP Event:

Virtual-Access0 CHAP Challenge TimeOut Event

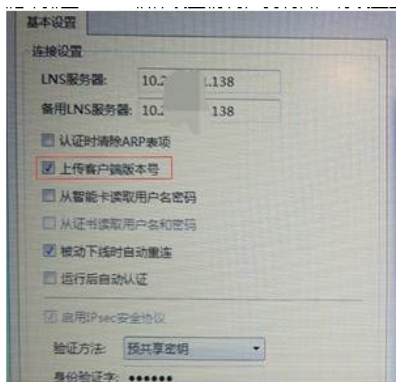
State SendChallenge , Retransmit = 1

\*Mar 23 15:49:24:404 2019 ZYNX\_MSR3640\_4G\_VPN PPP/7/AUTH\_ERROR\_0:

PPP Error:

Virtual-Access0 CHAP: Send challenge No. 1 !

随即排查INODE软件设置情况，发现客户有设置上传客户端版本号。取消上传客户端版本号后L2TP VPN协商通过。



## 解决方法

INODE软件默认情况下上传客户端版本号是开启的，主要是配合IMC EAD组件限制INODE客户端版本功能。因为没有EAD的配合所以需要L2TP OVER IPSEC或者L2TP配置中取消INODE上传客户端版本号选项。