



iNode拨SSLVPN提示隧道建立失败问题

iNode

iMC

SSL VPN

连辉

2021-09-30 发表

组网及说明

不涉及。手机端iNode拨号正常，

问题描述

现场测试发下，手机端iNode拨号正常，拨号后能正常访问内网，win10 PC iNode拨号提示隧道建立失败。

过程分析

收集手机iNode日志和PC端iNode日志分析，发现手机iNode拨号交互过程正常，而PC端iNode日志No desslvpn.xxxxxx.log中提示IP分配失败。

```
[2021-09-28 23:08:33] [Dbg] [b98] CsslHttpOper::recvRespData HTTP/1.1 551 Alloc IP Failed
Server: SSLVPN-Gateway/7.0
Content-Length: 0

[2021-09-28 23:08:33] [Dbg] [b98] CsslClient::getVpnAllocParam receiving data success.
[2021-09-28 23:08:33] [Err] [b98] CsslClient::getVpnAllocParam the response is not OK.
[2021-09-28 23:08:33] [Err] [b98] CsslClient::configVirtNetwork failed to get VPN parameters.
[2021-09-28 23:08:33] [Warn] [b98] CsslClient::conn2Remote failed to build the SSL VPN network.
[2021-09-28 23:08:33] [Err] [b98] CsslVpnMgr::startConnSpecial failed to connect the remote gateway, return code: 1
[2021-09-28 23:08:33] [Warn] [b98] CsslVpnMgr::connProcessNotify 建立VPN隧道失败。
[2021-09-28 23:08:33] [Dbg] [b98] CHttpsAuth::doLogout start do logout...
```

此报错是防火墙返回给iNode的，通常是防火墙配置问题，需要检查防火墙上的配置，检查sslvpn context主要配置，发现没什么问题，手机端可以正常拨号，也从侧面说明了这一点。

```
sslvpn ip address-pool SSLVPN地址池 [redacted]
#
sslvpn gateway SSLVPNSX
ip address [redacted] port 4433
service enable
#
sslvpn context SSLVPN
gateway SSLVPNSX
ip-tunnel interface SSLVPN-AC1
ip-tunnel address-pool SSLVPN地址池 mask 255.255.255.0
ip-tunnel dns-server primary [redacted]
ip-route-list FWNW
include [redacted] 255.255.224.0
ip-route-list XNJ
include [redacted]
policy-group SSLVPN资源组
filter ip-tunnel acl 3999
ip-tunnel access-route force-all
ip-tunnel access-route ip-route-list FWNW
ip-tunnel address-pool SSLVPN地址池 mask 255.255.255.0
service enable
..
```

此时注意到，context中并未配置aaa domain，也就是用的本地用户进行的认证，查看本地用户的配置，发现只有2个本地用户，其中一个用户明显多一条policy-group的配置

```
local-user admin class manage
password hash $h$6$XIP8QTY9Lk7MHVS6$vf8B1X2n4Je2pztdrPaGGUtcOW
service-type ssh telnet terminal https
authorization-attribute user-role level-3
authorization-attribute user-role network-admin
authorization-attribute user-role network-operator
#
local-user [redacted] 162 [redacted] class network
password cipher $c$3$uCVIsYex+mBbPLTRmACoXX414q4xjzYpv8KP
service-type advpn
service-type ike
service-type ipoe
service-type lan-access
service-type portal
service-type ppp
service-type sslvpn
authorization-attribute user-role network-operator
authorization-attribute sslvpn-policy-group SSLVPN资源组
#
local-user [redacted] 423 [redacted] class network
password cipher $c$3$+JHrRfVLEIS3uJNck7m99X+qXc1KkINx8hrn
service-type advpn
service-type ike
service-type ipoe
service-type lan-access
service-type portal
service-type ppp
service-type sslvpn
authorization-attribute user-role network-operator
```

进一步查看手机端正常的iNode日志，发现果然正常的用户是用162的账号上线的，而win10客户端是

用423账号上线的

解决方法

确认是本地用户配置的问题，增加policy-group的配置后，拨号正常

