某局点 SecPath F1000-AK125(V7) 结合IMC做ssl vpn后，拨号获取地址后无法ping通内网口，2分钟后inode会自动掉线问题排查案例

SSL VRF **方志伟** 2019-06-27 发表

组网及说明

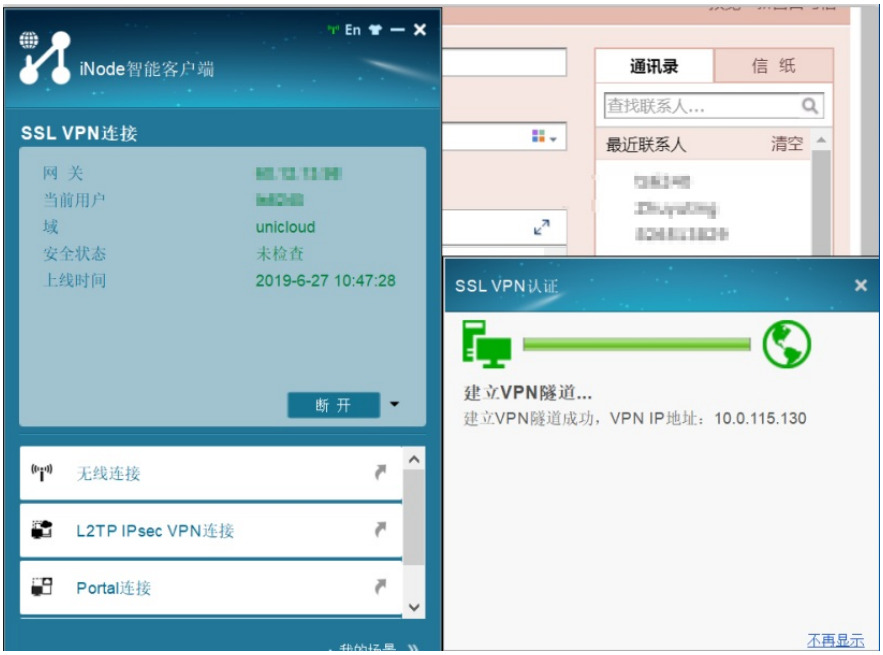
现场设备：公网口 GEx/x/x，IP地址为x.x.x.x 安全域 Untrust

AC口 interface SSLVPN-AC10，IP地址为x.x.x.x ，所在安全域 ywunTrust。

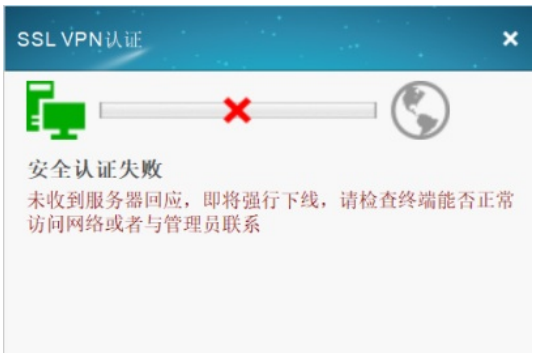
内网口为x口，**公网口和AC口都绑定了vpn实例vrf1。**

问题描述

现场配置后终端拨号能成功，能获取私网地址，但是无法ping通AC口，也无法ping通内网的认证服务器。然后ssl vpn认证成功后，过2分钟左右，会自动掉线，详细记录截图在下面



下线提示信息



过程分析

查看sslvpn实例相关配置

```
#
sslvpn context unicloud
 vpn-instance vrf1
 gateway unicloud domain unicloud
 ip-tunnel interface SSLVPN-AC10
 ip-tunnel address-pool uni mask 255.255.255.224
 ip-tunnel dns-server primary 114.114.114.114
 ip-route-list uni
  include 10.0.0.0 255.0.0.0
 policy-group unicloud
  filter ip-tunnel acl 3997
  ip-tunnel access-route ip-route-list uni
 default-policy-group unicloud
 aaa domain unicloud
```

service enable
#
acl advanced 3997
rule 0 permit ip vpn-instance vrf1
#
相关路由
#
ip route-static vpn-instance vrf1 10.0.6.0 24 Tunnel25　　//相关vpn实例路由也已添加
#
安全策略也放通了
#
security-policy ip
rule 39 name irf1-any
 action pass
 vrf vrf1
 source-zone Untrust
rule 40 name ywirf-any
 action pass
 vrf vrf1
 source-zone ywunTrust

解决方法

此时再次仔细查看版本说明书与官网说明，发现如下说明
配置SSL VPN访问控制策略时，需要注意：
引用的ACL规则中不能存在VPN实例，否则该规则不能生效

现场ACL规则中去除vpn实例后，该故障现象消失