某局点F1000-AI-55(V7) sslvpn拨号成功后无法访问内网资源

SSL VPN　刘文粟　2023-07-31 发表

问题描述

现场SSL VPN用户能正常拨号，但是无法访问内外资源

过程分析

查看配置，内网的资源已经放通

```
sslvpn context ctxip
 gateway gw
 ip-tunnel interface SSLVPN-AC1
 ip-tunnel address-pool vp1 mask 255.255.255.0
 ip-route-list rt1
  include 10.0.0.0 255.0.0.0
  include 172.16.0.0 255.240.0.0
  include 192.168.0.0 255.255.0.0
 policy-group rp1
  filter ip-tunnel acl 3500
  ip-tunnel access-route ip-route-list rt1
 default-policy-group rp1
 service enable
```

检查两边路由表都正常

安全策略都放通了

于是再次检查配置，发现内网口配置了策略路由

正好匹配了内网的地址

```
#
interface GigabitEthernet1/0/15
port link-mode route
ip policy-based-route pbr
#
#
policy-based-route pbr permit node 10
if-match acl 3005
apply next-hop xxx.xxx.xxx.xxx
#

#
acl advanced 3005
rule 5 permit ip source 172.16.0.0 0.0.0.255
#
```

解决方法

这个PBR里加一个deny的节点，把去往sslvpn网段的流量deny