

# 知 sslvpn只有一个本地用户能访问资产

SSL VPN 李瑞 2021-11-10 发表

## 组网及说明

IP接入, 标准组网, 本地用户

#### 问题描述

客户反馈，现场所有用户都能正常登录，但是只有第一个拨入的用户能访问内网资源

## 过程分析

关键配置:

### # acl advanced 3000

```
rule 0 permit ip source 192.168.68.2 0.0.0.128 destination 10.0.0.0 0.255.255.255
rule 20 permit ip source 192.168.68.2 0.0.0.128 destination 192.168.68.0 0.0.0.255
```

```
# sslvpn ip address-pool sslpool 192.168.68.130 192.168.68.250
```

```
# sslvpn context context2
```

```
gateway sslgate
```

```
ip-tunnel interface SSLVPN-AC20
```

```
ip-tunnel address-pool sslpool mask 255.255.255.128
```

```
ip-route-list route
```

```
include 10.0.0.0 255.0.0.0
```

```
include 192.168.68.0 255.255.255.0
```

```
policy-group zygroup
```

```
filter ip-tunnel acl 3000
```

```
ip-tunnel access-route
```

```
ip-route-list route service enable
```

## 解决方法

测试发现是现场的反掩码写错，按照错误的反掩码计算，0.0.0.128的符合地址只有192.168.68.2和192.168.68.30，由于sslvpn地址池是按照IP地址的大小从最小开始分配的，所以会导致现场只有第一个被分配了192.168.68.30的PC访问内网资源

需要现场修改反掩码为0.0.0.255才能包含130~250地址池的地址

