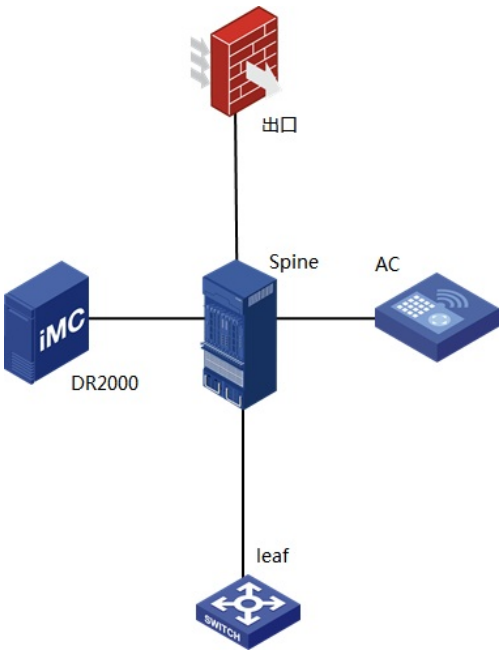
某局点 S10506 vxlan隧道流量做认证，无法匹配策略路由经验案例

策略路由 VXLAN **单畅** 2019-03-23 发表

组网及说明

组网如下：



问题描述

匹配ACL的是终端地址，tracert下一跳不对，终端练192.168.120.1的地址都不能ping通，

1.无线启用了两个SSID，其中一个SSID是再本地ADCampus上做认证，是正常的，

2.新建一个VSI3058地址是10.117.0.1的VXLAN地址需要设置策略路由下一跳到192.168.120.2上，测试发现策略路由匹配不正常 acl 3000 policy aaa

```
#
interface Vsi-interface3508
 ip binding vpn-instance vpn-default
 ip address 10.117.x.x 255.255.0.0
 mac-address 0000-0000-0001
 local-proxy-arp enable
 ip policy-based-route aaa
 distributed-gateway local
#
policy-based-route aaa permit node 5
 if-match acl 3000
 apply next-hop 192.168.120.2
#
```

过程分析

1、查询设备单板硬件表项，策略路由下发正常。

2. 策略路由使流量从vpn-default转发到公网出去。对于ping过程，会存在两个问题：对端出口设备不一定有到本设备私网的路由，icmp回复报文在本设备不能上送平台。这样均会导致不能ping通。

3. 现网需求是匹配acl的终端到另一个认证服务器进行认证。可以配置路由策略的同时，将设备出接口与VSI3508在同一个vpn内，并将路由发布到对端设备。

解决方法

将设备出接口与VSI3508在同一个vpn内，并将路由发布到对端设备问题解决。