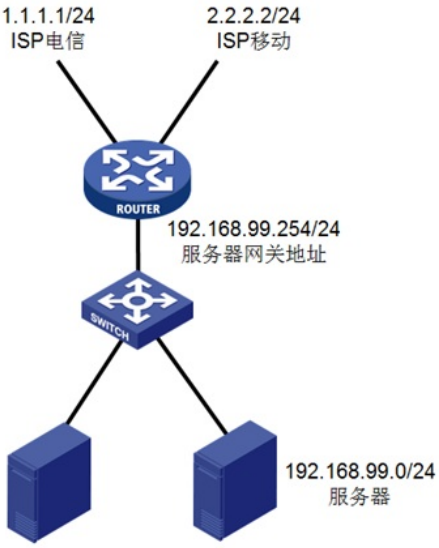
某局点MSR3620路由器做SSL VPN终端可以拨号但是无法正常访问内网的经验案例

SSL VPN 叶靖 2019-06-26 发表

组网及说明

现场购买了一台V7版本的MSR3620路由器作为公网出口设备，内网服务器的网关在路由器上，另外现场有两条运营商链路，分别为移动和电信，现在要在电信的链路接口上配置IP方式接入的SSL VPN。



问题描述

现场按照官网的配置指导完成相关配置之后，终端从公网可以正常拨入SSLVPN，但是拨入成功之后，终端无法正常访问内网服务器，但是可以正常ping通路由器上内网服务器的网关地址。

过程分析

终端可以正常拨号，但是无法正常访问内网的服务器。我们需要排查以下几点问题：

1、 从路由器上能否正常访问到内网服务器，确保内网服务器正常及网络可达

现场测试直接从路由器上ping内网服务器是可以正常访问的

2、是否正确为SSL VPN终端添加了到内网的路由

```
#
sslvpn context sslvpn
 gateway jwzxsslvpn domain domainip
 ip-tunnel interface SSLVPN-AC1
 ip-tunnel address-pool pool100 mask 255.255.255.0
 ip-route-list networkmanage
  include 192.168.99.0 255.255.255.0（正常引用了路由列表，添加了到内网服务器的路由）
policy-group sslvpn
  filter ip-tunnel acl 3999
  ip-tunnel access-route ip-route-list networkmanage
 service enable
```

现场在排查了以上几点发现均为正常，最后发现，由于现场是双运营商出口链路，为了使得流量负载，现场在路由器的内网口上配置了策略路由，匹配源地址为内网服务器192.168.99.0/24网段的流量，使得这部分流量在访问外网时可以走电信链路出去。

```
policy-based-route Internet permit node 5
 if-match acl 3100
 apply next-hop 1.1.1.1.

acl advanced 3100
 description Nat_outbound-dianxin
 rule 10 permit ip source 192.168.99.0 0.0.0.255
```

但是在这个问题中，内网服务器给SSL VPN终端的回包也会匹配上内网口配置的策略路由，最后走电信链路出去，实际上，内网服务器给SSL VPN终端的回包应该匹配设备自动创建的目的地址为SSL VPN终端网段的直连路由走SSLVPN-AC接口出去。

```
Destination/Mask   Proto   Pre Cost      NextHop         Interface
192.168.98.0/24    Direct  0   0         192.168.98.254  SSLVPN-AC100
```

解决方法

修改策略路由，添加节点，优先匹配内网服务器回给SSL VPN终端的报文，使得这部分流量根据路由表进行转发

```
policy-based-route Internet permit node 1
 if-match acl 3101

acl advanced 3101
 description neiwang-ssl
 rule 10 permit ip source 192.168.99.0 0.0.0.255 destination 192.168.98.0 0.0.0.255
```

添加配置如上，添加一个更小的节点，动作不需要配置，使得内网服务器回给SSL VPN终端的报文根据直连路由进行转发。