

## 知 某局点SecPath F1030(V7) 出口更改公网IP之后直连不通

NAT

孔德飞

2020-04-07 发表

### 组网及说明

终端---接入SW---核心SW---F1030（冗余主备）出口（reth10）---运营商。

### 问题描述

两台F1030冗余主备做出口，现场要对出口公网IP进行更改，但是更改之后直连不通。

### 过程分析

1.远程发现设备一直报地址冲突，是因为reth10的下一跳是1.1.1.2，而reth10又存在如下配置“nat server global 1.1.1.2 inside 10.1.1.1”，nat server的全局地址是响应ARP的，所以会造成地址冲突。  
Duplicate address 1.1.1.2 on interface GigabitEthernet1/0/1, sourced from 28ae-a8a1-0206

2.现场在reth10下增加“nat server protocol tcp global 1 24.88.70.x 8443 inside 172.16.93.1xx 443 reversible”时，设备一直报如下冲突  
The specified local addresses can't partly overlap with an existing addresses.  
发现现场存在如下配置：

```
intf ace reht1
 nat server global 10.93.174.x inside 172.16.93.1xx reversible
```

因为在reth1口下存在如下配置，因为reversible所以需要反向转换，reth1口的配置代表反向172.16.93.1xx的所有端口到10.93.174.x的所有端口的转换，此时若再增加“nat server protocol tcp global 124.88.70.x 8443 inside 172.16.93.1xx 443 reversible”，将会造成本地地址冲突的报错，因为同一个inside IP地址不可能同时转换为两个global ip地址。

### 解决方法

- 1.更改nat server的global地址不与下一跳冲突；
- 2.更改nat server的global地址不与已经存在的nat server reversible冲突，即同一个inside地址不能对应两个不同的global地址。