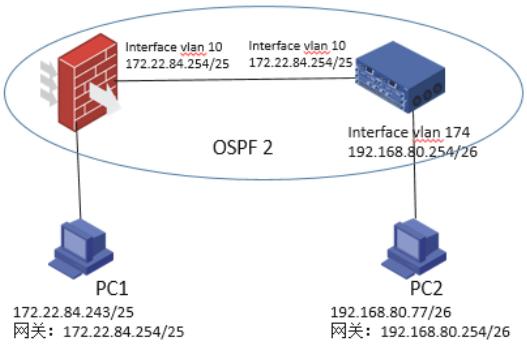
某局点SecPath F1050与7503E串联路由学习正常但内网不能互访问题经验案例

OSPF 静态路由 会话 **刘资瑜** 2018-12-19 发表

组网及说明



组网如上图所示，F1050与7503E之间运行OSPF，1050下联终端PC1的网关是vlan10的虚接口地址，75E下联终端PC2的网关是vlan174接口地址。

问题描述

现场反馈PC1和PC2不能互通，但是防火墙可以访问到PC2。PC1可以访问7503E的互联口，但是不能ping 通PC2的网关地址。

过程分析

通过查看，F1050和7503E的路由表及OSPF LSDB发现路由没有问题，因此进行以下操作：

1、在防火墙上查看会话，发现只有发包并没有回包

```
Initiator:
  Source      IP/port: 172.22.84.243/1
  Destination IP/port: 192.168.80.77/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: Vlan-interface10
  Source security zone: Trust
Responder:
  Source      IP/port: 192.168.80.77/1
  Destination IP/port: 172.22.84.243/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: Vlan-interface10
  Source security zone: Trust
State: ICMP_REQUEST
Application: ICMP
Start time: 2018-12-18 12:52:50  TTL: 59s
Initiator->Responder:          136 packets       8160 bytes
Responder->Initiator:            0 packets          0 bytes
```

2、在7503E上做流统发现，交换机上行口及下行口出入方向的收发包都正常

3、由于现场是测试环境，因此将F1030替换为一台交换机，发现可以ping 通

4、将PC1的网关改为同网段的75E的接口地址172.22.84.254，发现PC1和PC2可以互访

仔细分析发现，在防火墙上存在来回路径不一致的问题

PC1的网关为1030和75E的互联口地址时，访问PC2的流量走向如下：PC1-int vlan10-1030下行口-75E上行口....

PC2的回包流量走向如下：其他-75E上行口-PC1

这是由于75E发现目标网段和自己属于同一个二层，因此直接将报文发给PC1，因此匹配不上防火墙会话，会被防火墙ASPF策略丢掉，查看防火墙会话时才会发现没有回包。

解决方法

因此给出现场三种解决方案：

1、将PC1的网关下移到75E的上行口

2、在防火墙上使用命令**session state-machine mode loose** 配置会话状态为宽松模式

3、更改组网，将PC1重新划分到另外一个网段，配置另外一个interface vlan接口作为网关