



SecBlade防火墙插卡来回路径不一致导致业务中断

一、组网：

某单位与总部互连，走的是2M和8M链路，正常情况下视频会议走2M链路，生产业务走8M链路，互为备份。防火墙与总部这端走的OSPF，S95E与防火墙插卡走的静态路由，并将静态路由引入到OSPF中。两台防火墙之间走的是三层转发和静态路由。

二、问题描述：

现在从8M切换到2M链路后，能够ping通相关服务的ip地址，但无法访问生产业务和视频会议。

三、过程分析：

遇到上述问题，我们可以做如下测试：

1、首先，这个问题是主备链路切换后导致的，很自然地就会想到链路是否有切换到备份链路上。这样，我们就在总部和分部的终端分别做trace测试，来确定是否切换到备份链路上，测试结果如下：

总部—>MSR50-2—>FW-2—>S95E-2—>分部

分部—>S95E-1—>FW-1—>FW-2—>MSR50-2—>总部

2、从测试1结果来看，数据流来回路径不一致。这时，我们就需要在经过的设备上去查看具体的路由，确认导致这种问题产生的路由信息是何种路由协议形成的（如OSPF、BGP、OSPF的外部路由，静态路由等等），进而查看相关路由配置是否正确。

测试结果如下：

在S95E-1上观察到：去往总部终端的路路由是由静态路由决定的，下一跳为FW-1；

在FW-1上观察到：去往总部终端的路路由是由静态路由决定的，下一跳为FW-2；

在FW-2上观察到：去往分部终端的路路由是由静态路由决定的，下一跳为S9512-E；

这样的话，就形成了来回路径不一致。

3、因为经过的设备有防火墙，还要查看在防火墙上是否有相应业务的会话（防火墙是基于会话表转发数据的），测试结果如下：

在FW-1没有相应业务的会话，因为在回来的路径上没有经过FW-1，这样会话就没有建立起来。

四、解决方法：

针对以上分析，给出以下解决方案：

1、在两块防火墙插卡上开启双机热备功能进行会话同步，并选择支持非对称路径；

原因：开启双机热备功能，同步两台防火墙之间的会话信息，主备链路切换后，业务不会中断。

在来回路径不一致的情况下：（以TCP业务为例）

1>如果选择不支持非对称路径，只有当TCP会话达到established状态（即稳定状态），才会将整个会话信息同步到备防火墙上，TCP SYN报文经过FW-1，开始创建一个双向会话，而SYN_ACK报文经过的是FW-2,不能匹配到相应的会话，就会被丢弃，从而会话就建立不起来，业务就不会通。

2>如果选择支持非对称路径，SYN报文经过FW-1，FW-1会将这条会话信息同步到FW-2上，当SYN_ACK报文到达FW-2时，就会匹配到相应的会话，并且将这些会话信息同步到FW-1上，当ACK报文经过FW-1时，也能匹配到相应的会话，此时，TCP连接也就建立起来了，同时也会将这些会话信息同步到FW-2，从而两台防火墙的会话信息就同步了，业务报文也就能正常转发了。

2、将S9512E与防火墙插卡之间走OSPF，取代静态路由，并调整相应的cost值，这样能够很好地避免来回路径不一致。

原因：OSPF是动态路由协议，通过SFP算法计算出最短路径，只要cost值设置合理，就不会人为地造成来回路径不一致。

五、注意事项：

1、一般核心设备之间不建议走静态路由，尽量走动态路由协议。

2、防火墙插卡的GE口不建议做三层转发，一般用作双机热备的心跳互连接口或网管接口。