

知 防火墙透明桥模式下，放通策略全通，业务正常，放通明细策略，部分业务异常

域间策略/安全域 会话 张春光 2023-10-16 发表

问题描述

透明桥模式下，放通策略全通，业务正常，放通明细策略，部分业务异常

过程分析

- 1、全通策略下，客户侧ping 穿越防火墙测试，正常，但是防火墙无法抓到包
- 2、策略精细化后，客户侧ping穿越防火墙测试，不通，防火墙无法抓到包
- 3、抓包查看防火墙流量发现有mpls流量产生，精细化查看后发现ospf、bgp、ldp协议互通

解决方法

针对相关协议（包括ospf协议、bgp协议、bfd协议、ldp-tcp/udp646、ldp-tcp/udp749）进行放通后业务正常

ping无法抓包的原因是，ping包中封装了mpls的外层标签，无法抓包；

