某局点F1030防火墙直连ping不通的经验案例

域间策略/安全域 VRF 李聪 2018-09-25 发表

组网及说明

无

问题描述

某局点防火墙直连ping不通对方的路由器设备，同时查看会话也是没有相应的会话生成。接下来针对此问题进行分析。

过程分析

1、检查设备的配置

通过搜集现场设备的配置信息如下：

```
#
interface GigabitEthernet1/0/8
port link-mode route
ip binding vpn-instance test  //接口绑定了vpn实例
ip address 12.12.12.12 255.255.255.0
#
security-zone name Trust
import interface GigabitEthernet1/0/8


security-policy ip
rule 3 name test
 action pass
 source-zone local
 destination-zone trust
```

2、原因分析

经过分析，如果防火墙的接口绑定了vpn实例。那么安全策略在处理报文的时候，安全策略规则里面需要配置相关的vrf实例参数，对指定的vpn实例报文有效。安全策略修改配置之后如下：

```
security-policy ip
rule 3 name test
 action pass
  vrf test  //需要在安全策略里面也指定策略生效的vpn实例
 source-zone local
 destination-zone trust
```

解决方法

通过修改安全策略配置对指定的vpn实例报文生效，防火墙报文转发问题解决。