

# 知 某局点F5010 BFD检测安全域及安全策略问题

BFD 域间策略/安全域 孔德飞 2020-03-10 发表

## 组网及说明

不涉及

## 问题描述

- F5030上的BFD检测口vlan4090没有加入到安全域，也没有配置相应的安全策略，在设备上查看bfd verbose状态却是normal

```
interface Vlan-interface4090
description BFD-MAD
mad bfd enable
mad ip address 1.1.1.1 255.255.255.252 member 1
mad ip address 1.1.1.2 255.255.255.252 member 2
```

- 防火墙插卡上的BFD检测口是Route-Aggregation64，Route-Aggregation64加入到安全域并配置了相

应的安全策略，安全策略中打开了计数功能，但是在  
WEB界面上没有看到命中次数  
interface Route-Aggregation64  
mad bfd enable  
mad ip address 1.1.1.5 255.255.255.252 member 1  
mad ip address 1.1.1.6 255.255.255.252 member 2

```
security-zone name Trust
import interface FortyGigE1/0/2
import interface FortyGigE1/0/3
import interface FortyGigE2/0/2
import interface FortyGigE2/0/3
import interface Reth2
import interface Reth2.37
import interface Reth2.38
import interface Reth2.39
import interface Route-Aggregation64
```

```
rule 1022 name Local-to-Trust-MAD_detect
action pass
counting enable
source-zone Local
destination-zone Trust
service bfd-echo
service bfd-control
service bfd-control-multipoint
rule 1023 name Trust-to-Local-MAD_detect
action pass
counting enable
source-zone Trust
destination-zone Local
service bfd-echo
service bfd-control
service bfd-control-multipoint
```

Local...	Local	Local	IPv4	102:	Any	Any	bfd-ei	Any	允许	0	0.008	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Trust...	Trust	Local	IPv4	102:	Any	Any	bfd-ei	Any	允许	0	0.008	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

## 过程分析

BFD接口未加入安全域以及配置相应的安全策略，但是查看的BFD状态却是normal；

BFD接口加入安全域以及相应的安全策略，安全策略中配置了计数功能，WEB界面上却看不到命中次数；

通过以上现象分析安全策略未生效，于是向研发进一步确认，现场版本（该版本（R8524P24）以及之后的版本）mad bfd流量不走安全业务点，所以安全策略对bfd流量无感知。

## 解决方法

R8524P24版本以及之后的版本由于安全策略对BFD流量无感知，所以在配置IRF MAD BFD检测的时候，可以不用将BFD接口加入安全域以及配置相应的安全策略。