

知 防火墙本地发出的报文如果发出接口是IRF备上的接口那么会话无法同步

会话同步 会话 李瑞 2022-05-17 发表

组网及说明

IRF组网

告警信息

无告警

#### 问题描述

防火墙本地发出的报文如果发出接口是IRF备上的接口那么会话无法同步。

本地发出的报文例如NQA探测、LB的探测报文，如果报文的正向出口是IRF备的物理口，那么这个会话无法同步到IRF的主墙上。

## 过程分析

debug看有如下的回显

... ..

Session entry was created.

\*May 17 09:57:23:293 2022 F1070-IRF SESSION/7/BACKUP: -Context=1;

Tuple5(ERROR): 33.33.33.1/18568-->33.33.33.32/2048(ICMP(1))

Hot-backup restoration: **Failed to process the added IPFS cache conflict**

查看会话，IRF的主Slot1上没有会话：

<F1070-IRF>dis session table ipv4 destination-ip 33.33.33.32 protocol icmp source-port 18568 ver

Slot 1:

Total sessions found: 0

Slot 2:

Initiator:

Source IP/port: 33.33.33.1/18568

Destination IP/port: 33.33.33.32/2048

DS-Lite tunnel peer: -

VPN instance/VLAN ID/Inline ID: -/-

Protocol: ICMP(1)

Inbound interface: InLoopBack0

Source security zone: Local

Responder:

Source IP/port: 33.33.33.32/18568

Destination IP/port: 33.33.33.1/0

DS-Lite tunnel peer: -

VPN instance/VLAN ID/Inline ID: -/-

Protocol: ICMP(1)

Inbound interface: GigabitEthernet2/0/13

Source security zone: Trust

State: ICMP\_REPLY

Application: ICMP

Rule ID: 1012

Rule name: pass

Start time: 2022-05-17 09:57:22 TTL: 3s

Initiator->Responder: 1 packets 128 bytes

Responder->Initiator: 1 packets 128 bytes

Total sessions found: 1

## 解决方法

属于防火墙的限制，无法解决

规避方法：配置报文的出接口为逻辑口即可（将单个物理口加入聚合口也可以）

