某局点防火墙冗余组切换后不通的经验案例

冗余组 张腾 2022-05-29 发表

组网及说明

2台F1000-AI-55防火墙做IRF，采用冗余组主备方式。

防火墙版本：Release 8860P18

问题描述

防火墙进行主备切换测试，发现切换后业务不通

过程分析

1、
防火墙下行冗余口reth10成员接口如下
#
interface Reth10
description DOWN-Link-AH_DMZ_H00_CS01:vlan-intface1000
ip address 172.16.200.6 255.255.255.248
member interface Route-Aggregation1 priority 100
member interface Route-Aggregation2 priority 80
进行主备切换流量从一框切换到二框后冗余组和冗余口状态如下：
[AH_DMZ_H00_FW01]display reth interface Reth 10
Reth10 :
  Redundancy group : DMZ
  Member   Physical status   Forwarding status   Presence status
  RAGG1   DOWN   Inactive   Normal
  RAGG2   UP   Active   Normal
[AH_DMZ_H00_FW01]display redundancy group
Redundancy group DMZ (ID 1):
  Node ID   Slot   Priority   Status   Track weight
  1   Slot1   100   Secondary   -765
  2   Slot2   80   Primary   255

Preempt delay time remained   : 0   sec
Preempt delay timer setting   : 60   sec
Remaining hold-down time   : 0   sec
Hold-down timer setting   : 1   sec
Manual switchover request   : No

Member interfaces:
    Reth1   Reth2   Reth10

Node 1:
  Track info:
    Track   Status   Reduced weight   Interface
    1   Negative   255   GE1/0/2
    2   Negative   255   GE1/0/3
    3   Negative   255   GE1/0/14
    4   Negative(Faulty) 255   GE1/0/15
Node 2:
  Track info:
    Track   Status   Reduced weight   Interface
    11   Positive   255   GE2/0/2
    12   Positive   255   GE2/0/3
    13   Positive   255   GE2/0/14
    14   Positive   255   GE2/0/15
2、此时用测试终端去ping防火墙reth10口地址，发现防火墙上没会话。通过debug ip packet发现报文未上到防火墙。排查交换机侧发现交换机学不到防火墙reth10口的ARP信息，交换机侧debug如下，未收到ARP回包：
Ping 172.16.200.6 (172.16.200.6): 56 data bytes, press CTRL+C to break
*Apr 1 22:53:04:083 2013 AH_DMZ_H00_CS01 ARP/7/ARP_SEND: Sent an ARP message, operation: 1, sender MAC: 642f-c759-b160, sender IP: 172.16.200.1, target MAC: 0000-0000-0000, target IP: 172.16.200.6
*Apr 1 22:53:05:914 2013 AH_DMZ_H00_CS01 ARP/7/ARP_SEND: Sent an ARP message, operation: 1, sender MAC: 642f-c759-b160, sender IP: 172.16.200.1, target MAC: 0000-0000-0000, target IP: 172.16.200.6
Request time out
*Apr 1 22:53:06:282 2013 AH_DMZ_H00_CS01 ARP/7/ARP_SEND: Sent an ARP message, operation: 1, sender MAC: 642f-c759-b160, sender IP: 172.16.200.1, target MAC: 0000-0000-0000, target IP: 172.16.200.6

Request time out

*Apr 1 22:53:08:483 2013 AH_DMZ_H00_CS01 ARP/7/ARP_SEND: Sent an ARP message, operation: 1, sender MAC: 642f-c759-b160, sender IP: 172.16.200.1, target MAC: 0000-0000-0000, target IP: 172.16.200.6

Request time out

解决方法

3、在防火墙侧查看ARP信息发现，防火墙可以学到交换机的ARP信息：

将BFD MAD检测配置在三层聚合口下

<AH_DMZ_H00_FW01>display arp

Type: S-Static D-Dynamic O-Openflow R-Rule I-Invalid

IP address MAC address VLAN/VSI name Interface/Link ID Aging Type

115.233.206.241 ac4e-9165-8103 -- Reth1 12 D

60.12.5.89 20f1-7c96-b63e -- Reth2 20 D

172.16.200.1 642f-c759-b160 -- Reth10 20 D

192.168.0.2 2c16-dba6-70c9 -- MGE1/0/0 19 D

4、用防火墙去ping对端设备172.16.200.1，此时查看会话发现会话报文是从1框发出去的，但实际上1框的冗余口成员接口聚合口1是处于DOWN的状态。

Reth2 UP UP 60.12.5.90 UP_to_LianTong-200M-360DCA0

Reth10 UP UP 172.16.200.6 DOWN-Link-AH_DMZ_H00_CS01:v

Reth19 DOWN DOWN --

RAGG1 DOWN DOWN -- DOWN_Link_AH_DMZ_H00_CS01:B

RAGG2 UP UP -- DOWN_Link_AH_DMZ_H00_CS01:B

Vlan2000 UP UP 1.1.1.1 BFD-VLAN

[AH_DMZ_H00_FW01]display session table ipv4 source-ip 172.16.200.6 verbose

Slot 1:

Initiator:

Source IP/port: 172.16.200.6/28839

Destination IP/port: 172.16.200.1/2048

DS-Lite tunnel peer: -

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

Protocol: ICMP(1)

Inbound interface: InLoopBack0

Source security zone: Local

Responder:

Source IP/port: 172.16.200.1/28839

Destination IP/port: 172.16.200.6/0

DS-Lite tunnel peer: -

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

Protocol: ICMP(1)

Inbound interface: Reth10

Source security zone: Trust

State: ICMP_REQUEST

Application: ICMP

Rule ID: 5

Rule name: 6

Start time: 2022-04-12 16:05:10 TTL: 41s

Initiator->Responder: 5 packets 420 bytes

Responder->Initiator: 0 packets 0 bytes

Total sessions found: 1

Slot 2:

Initiator:

Source IP/port: 172.16.200.6/28839

Destination IP/port: 172.16.200.1/2048

DS-Lite tunnel peer: -

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

Protocol: ICMP(1)

Inbound interface: InLoopBack0

Source security zone: Local

Responder:

Source IP/port: 172.16.200.1/28839

Destination IP/port: 172.16.200.6/0

DS-Lite tunnel peer: -

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

Protocol: ICMP(1)
Inbound interface: Reth10
Source security zone: Trust
State: INACTIVE
Application: ICMP
Rule ID: 5