堆叠场景下NGFW开启会话同步功能后会话不一致问题

会话同步 outbound链路负载均衡 孔凡安 2023-05-11 发表

组网及说明

不涉及

告警信息

不涉及

问题描述

某局点两台NGFW堆叠主备部署，下行为Reth接口，上行为二层跨框聚合配置最大选中数，业务实际是主备部署。
运行过程中发现主备设备会话数目不一致，差别较大。
设备也已经开启了会话同步功能。

```
[H3C-F1000-AK135]disp se sta su
Slot Sessions  TCP       UDP       Rate      TCP rate  UDP rate
1    146718    142107    4545      4816/s    4718/s    95/s
2    148       85        35        33/s      29/s      1/s
```

```
#
 session synchronization enable
 session synchronization dns http
#
```

过程分析

查看slot 2的会话，备份的会话基本都是一些本地发出或者到本机的会话。

```
<H3C-F1000-AK135>disp session ta ipv4 sl 2 ver
Slot 2:
Initiator:
  Source      IP/port: 221.12.166.112/6606
  Destination IP/port: 221.12.1.227/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: InLoopBack0
  Source security zone: Local
Responder:
  Source      IP/port: 221.12.1.227/6606
  Destination IP/port: 221.12.166.112/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: Vlan-interface4012
  Source security zone: Untrust
State: INACTIVE
Application: ICMP
Rule ID: 3
Rule name: 1
Start time: 2023-05-02 11:58:32  TTL: 212s
Initiator->Responder:            0 packets          0 bytes
Responder->Initiator:            0 packets          0 bytes

Initiator:
  Source      IP/port: 113.12.181.168/9356
  Destination IP/port: 115.221.240.66/57413
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: UDP(17)
  Inbound interface: Dialer1
  Source security zone: Untrust
Responder:
  Source      IP/port: 115.221.240.66/57413
  Destination IP/port: 113.12.181.168/9356
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: UDP(17)
  Inbound interface: InLoopBack0
  Source security zone: Local
State: INACTIVE
Application: GENERAL_UDP
Rule ID: 4
Rule name: 2
Start time: 2023-05-06 15:04:48  TTL: 276s
Initiator->Responder:            0 packets          0 bytes
Responder->Initiator:            0 packets          0 bytes

Initiator:
  Source      IP/port: 183.167.205.250/52803
  Destination IP/port: 115.221.240.66/26881
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: Dialer1
  Source security zone: Untrust
Responder:
```

解决方法

开启虚服务器的会话扩展信息备份功能

```
  Source      IP/port: 115.221.240.66/26881
  Destination IP/port: 183.167.205.250/52803
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: InLoopBack0
  Source security zone: Local
State: INACTIVE
Application: GENERAL_TCP
Rule ID: 4
Rule name: 2
Start time: 2023-05-06 15:05:09  TTL: 298s
Initiator->Responder:           0 packets         0 bytes
Responder->Initiator:           0 packets         0 bytes
Initiator:
  Source      IP/port: 49.234.25.245/49399
  Destination IP/port: 115.221.240.66/1234
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: UDP(17)
  Inbound interface: Dialer1
  Source security zone: Untrust
Responder:
  Source      IP/port: 115.221.240.66/1234
  Destination IP/port: 49.234.25.245/49399
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: UDP(17)
  Inbound interface: InLoopBack0
  Source security zone: Local
State: INACTIVE
Application: GENERAL_UDP
Rule ID: 4
Rule name: 2
Start time: 2023-05-06 15:04:47  TTL: 276s
Initiator->Responder:           0 packets         0 bytes
Responder->Initiator:           0 packets         0 bytes
```

对比 slot1大部分都是转发的报文。

```
<H3C-F1000-AK135>disp session ta ipv4 ver
Slot 1:
Initiator:
  Source      IP/port: 192.168.20.124/57721
  Destination IP/port: 192.168.200.57/8080
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: Reth12
  Source security zone: Trust
Responder:
  Source      IP/port: 192.168.200.57/8080
  Destination IP/port: 115.221.240.66/8104
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: Dialer1
  Source security zone: Untrust
State: TCP_SYN_SENT
Application: GENERAL_TCP
Rule ID: 1
Rule name: trust_untrsut
Start time: 2023-05-06 15:07:57  TTL: 20s
Initiator->Responder:           2 packets         104 bytes
```

connection-sync enable命令用来开启虚服务器的会话扩展信息备份功能。

undo connection-sync enable命令用来关闭虚服务器的会话扩展信息备份功能。

【命令】

connection-sync enable

undo connection-sync enable

【缺省情况】

虚服务器的会话扩展信息备份功能处于关闭状态。

【视图】

虚服务器视图

【缺省用户角色】

network-admin

mdc-admin

vsys-admin

【使用指导】

HTTP类型的虚服务器不支持本命令。

【举例】

开启IP类型的虚服务器vs3的会话扩展信息备份功能。

```
<Sysname>system-view
[Sysname] virtual-server vs3 type ip
[Sysname-vs-ip-vs3] connection-sync enable
```

Responder - Initiator: 0 packets 0 bytes