某局点 SecPath F1070(V7)防火墙双主组网CPU忽高忽低经验案例分析

IRF 会话 zhiliao_Eu03A 2018-09-30 发表

组网及说明

现场有两台F1070(V7)防火墙做了IRF，使用的双主组网。防火墙的版本为7.1.064, Release 9323P18
。

问题描述

现场使用的防火墙irf双主组网，反馈查看CPU利用率间隔一小段时间会升高到50%以上，呈现规律性忽高忽低。

```
<Changde-ZHDJ-F1070-IRF>dis cpu history
100%|
 95%|
 90%|
 85%|
 80%|
 75%|
 70%|
 65%|
 60%|
 55%|
 50%| #     #     #    ##    #     #     #
 45%| ##    #     ##    ##    ##    ###   ##
 40%| ##    ###   ###   ##    ###   ###   ###
 35%|####   ###   ###   ####  ###   ###   ###
 30%|####   ####  ####  ####  ####  #####  ####
 25%|####  #####  #####  #####  #####  #####  #####
 20%|#####  ######  #####  ######  ######  #####  ######
 15%|##### #######  #######  ######  ######  #######  #######
 10%|###### #######  #######  #######  #######  #######  #######  #
  5%|#################################################################
```

过程分析

1、 查看防火墙会话数只有1000条左右，多次查看cpu发现cpu波动主要由转发进程引起。

```
<Changde-ZHDJ-F1070-IRF> display process cpu slot 1
CPU utilization in 5 secs: 3.8%; 1 min: 3.2%; 5 mins: 33.8%
  JID    5Sec     1Min     5Min   Name
  171    0.0%     0.0%     0.0%   [kdrvcp0]
  172    0.0%     0.0%     0.0%   [kdrvcp1]
  173    2.9%     2.8%     0.9%   [kdrvdp2]
  174    2.9%     2.7%     0.9%   [kdrvdp3]
  175    3.0%     2.9%     1.0%   [kdrvdp4]
  176    3.1%     2.9%     1.0%   [kdrvdp5]
  177    3.0%     2.9%     1.0%   [kdrvdp6]
  178    3.1%     2.9%     1.0%   [kdrvdp7]
  179    3.1%     2.9%     1.0%   [kdrvdp8]
  180    2.9%     2.9%     1.0%   [kdrvdp9]
  181    3.1%     2.9%     1.0%   [kdrvdp10]
  182    2.9%     3.0%     0.9%   [kdrvdp11]
  183    3.1%     3.0%     0.9%   [kdrvdp12]
  184    3.1%     3.0%     0.9%   [kdrvdp13]
  185    3.1%     2.9%     0.9%   [kdrvdp14]
  186    3.0%     2.8%     0.9%   [kdrvdp15]
```

2、经过分析原因是DNS请求报文在slot1上（这个是主会话），备份到slot2上，此时DNS应答报文在slot2上，并命中之前备份的会话，导致备会话的DNS老化时间切成1s；主会话因为只有单向命中老化时间比较大，由于备会话老化时间为1s，要老化了，就会向主会话所在的slot1一直发老化查询消息，主会话因为没老化，但是备会话老化时间为1s，就会一直发，频繁的发老化查询消息，导致堆叠口流量比较大，cpu上升。

解决方法

让现场将DNS的老化时间改为5s问题解决（默认1s），更改DNS老化时间的命令是session aging-time application dns 5。