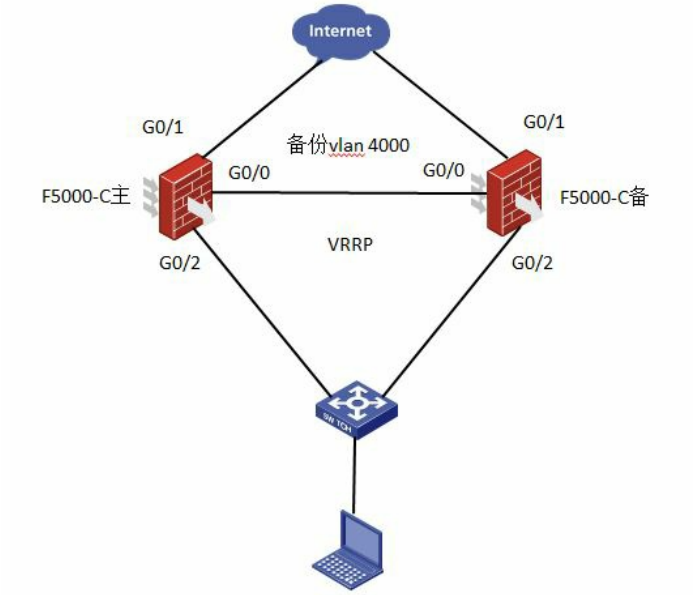
F5000-C(V5)防火墙配置nqa检测在双机热备组网中会话同步问题案例分析

BFD/NQA/TRACK/接口组联动 双机热备 李聪 2016-09-26 发表



一、 组网：

如图所示，两台防火墙F5000-C对内配置了vrrp，同时两台防火墙都配置双机热备。目前遇到主防火墙上面的会话量643个，但是备机上面确只有16个，会话量不一致，差距太大。

本案例涉及的防火墙的型号为SecPath F5000-C(V5)，版本为H3C SecPath F5000-C-CMW520-R3811P05。

二、 原因分析：

接下来从客户配置、以及会话方面进行分析。

1. 检查配置

1.1下面为主防火墙上面的配置：

```
#
nqa entry admin test  //这部分为主防火墙上面的nqa的配置。
 type icmp-echo
  destination ip 11.7.132.102  //检测的目的ip地址。
  frequency 5000
  history-record enable
  history-record number 10
  next-hop 11.7.132.102
  probe count 10
  probe timeout 500
#
 nqa schedule admin test start-time now lifetime forever  //# 启动ICMP-echo测试操作。
#
 dhbk enable backup-type symmetric-path  //# 使能双机热备业务备份功能，且支持对称路径。
 dhbk interface GigabitEthernet0/0 vlan 4000  //备份vlan是vlan 4000
 dhbk configuration-backup master synchronization  //配置为主设备并且开启配置同步功能。
#
```

session synchronization enable //开启会话同步的功能。

1.2下面为备防火墙上面的配置：

#

dhbk enable backup-type symmetric-path //# 使能双机热备业务备份功能，且支持对称路径。

dhbk interface GigabitEthernet0/0 vlan 4000 //备份vlan是vlan 4000

#

session synchronization enable //开启会话同步的功能。

1.3 检查以及分析配置

从以上的配置我们看出双机热备部分的配置没有问题，其中还有vrrp的配置也检查过没有问题，通过dis vrrp的状态都是正常的，主设备就是master的状态，内设备是backup的状态。检查双机热备的状态，通过dis dhbk status查看双机热备状态：

display dhbk status

Stateful failover: Enabled

Backup type: Symmetric path

Current state: Synchronized //发现双机热备是同步的状态，并且主备上面都是同步的，说明双机热备成功了。

Current port:

  GigabitEthernet0/0

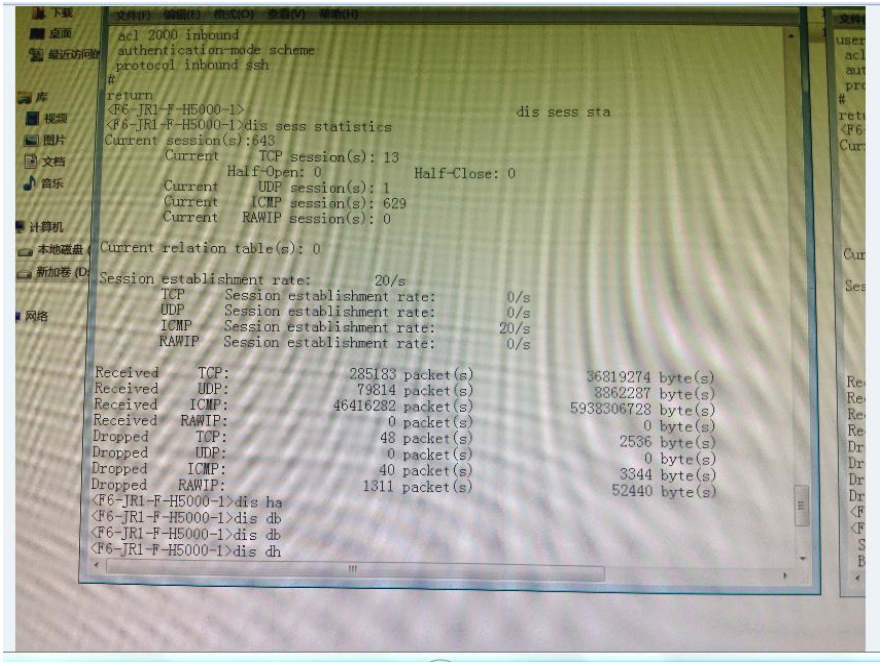
VLAN ID: 4000

2. 分析原因

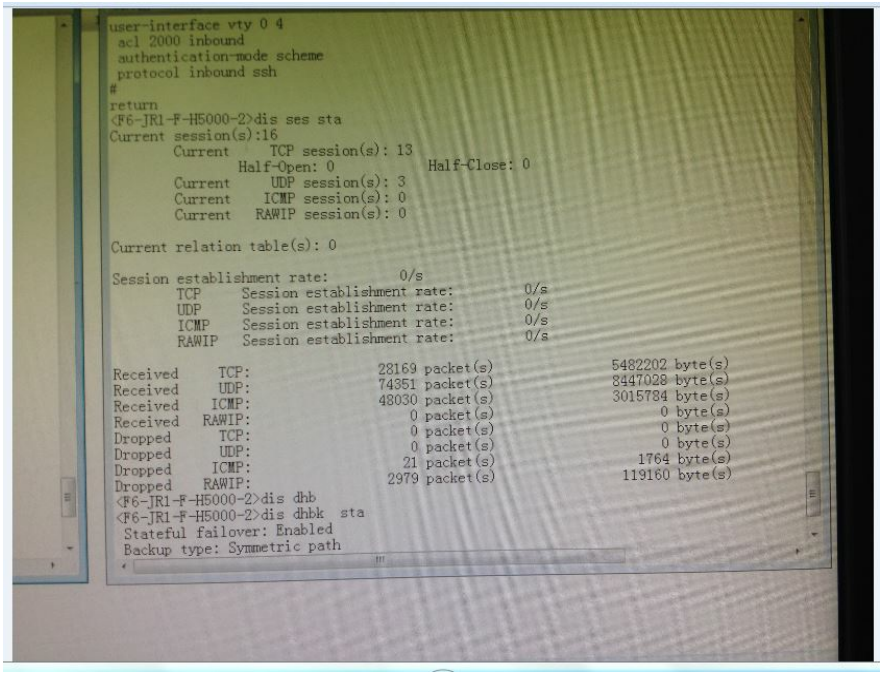
从以上的配置分析我们看到vrrp以及双机热备的状态是没有问题的，因此我们需要对同步会话进行分析看看是不是会话的问题。

2.1 通过display session statistics查看会话统计信息。

以下是主防火墙上面的会话截图信息：



以下是备防火墙上面的会话截图信息：



从以上主防火墙的会话统计看出会话数量为643个，tcp会话数量为13个，icmp会话数量为629个。备防火墙的会话统计看出会话数量为16个，tcp会话数量为13个，icmp会话数量为0个。我们发现tcp会话倒是一样的，但是icmp会话异常。

同时我们通过查看主防火墙上面的会话信息发现icmp的会话的目的地址基本都是nqa配置中的目的地址，但是备防火墙上面并没有配置nqa。因此我们怀疑是不是nqa的原因，接下来进行解释。

2.2 双机热备的防火墙对icmp会话同步的机制

根据和产品工程师那边了解，主防火墙主机本地始发和到本地的icmp会话是不会同步到备机的。本案例中主防火墙配置了nqa检测，nqa检测发包是设备作为源去ping目的地址的，因此是由主防火墙本地发起的ping的icmp会话，这个会话是不会被同步到备机上面的。

三、 解决办法：

通过以上的分析，我们总结了以下几点：

1．防火墙在配置双机热备的情况下，建议主备防火墙配置一致，并且需要开启配置同步功能、会话同步。

2．配置了双机热备的vlan，需要保证vlan放通，这样双机热备才能正常建立。

3．本案例的结论就是主防火墙主机本地始发和到本地的icmp会话是不会同步到备机的。因此，看到类似的问题不必怀疑是防火墙问题。