一、开始

Comware V7 盒式防火墙目前应用诸多局点，其中防火墙丢包问题较为普遍，丢包主要现象是 ping 测试延迟丢包、访问业务卡顿等。Comware V7 防火墙有多个转发核，默认正常情况下是单转发核处理流量报文，如果出现 CPU 高和单个转发核高的情况都会导致丢包现象。此外各个型号防火墙的会话规格不同，应保证设备的会话在规格内，超过了规格也会产生丢包问题。针对目前 Comware V7 防火墙的丢包问题，主要从以下几个方面来排查定位：查看 CPU 状态是否异常、查看转发核是否存在单核打满、查看历史会话是否异常、查看 Top-statistics 是否存在异常的源 IP 地址等。

二、流程图相关操作说明

1、查看 CPU 状态是否正常

CPU，称为中央控制器，是一块超大规模的集成电路，是一台网络设备的运算核心（Core）和控制核心，对于 NGFW 系列产品的 CPU，所有的流量都需要上到 CPU 处理，因此 CPU 的性能和状态影响设备的转发性能，NGFW 盒式防火墙的 CPU 状态可以通过以下命令查看。

命令：display cpu summary slot X（X 代表设备在 IRF 中的成员编号）

display cpu history slot X（X 代表设备在 IRF 中的成员编号）

display cpu control-plane slot X（X 代表设备在 IRF 中的成员编号）

display cpu data-plane slot X （X 代表设备在 IRF 中的成员编号）

例如：使用命令 display cpu summary 可查看最近 5 秒、1 分钟、5 分钟的 CPU 占用情况。

```
<H3C>display cpu summary
Slot CPU       Last 5 sec        Last 1 min        Last 5 min
1    0         85%                86%               85%
2    0         0%                 1%                1%
```

使用 display cpu history 命令显示最近 60 个采样点的 CPU 值，以坐标的形式显示 CPU 历史利用率信息，如下：

```
<H3C>display cpu history slot 1
100%|
95%|
 90%|
 85%|####
 80%|####
 75%|####
 70%|####
 65%|####
 60%|####  #
 55%|####  #
 50%|####  #
 45%|####  ##
 40%|####  ##
 35%|####  ##
 30%|####  ##
 25%|##### ##
 20%|##### ##
 15%|##### ##
 10%|##### ##
  5%|##### ##
    ------------------------------------------------------------
              10        20        30        40        50        60
                       cpu-usage  (Slot  1  CPU  0)  last  60  minutes
    (SYSTEM)
```

使用命令 display cpu control-plane 查看控制平面 CPU 利用率的统计信息，如下：

```
<H3C>display cpu control-plane
Slot 1 CPU 0 CPU usage:
      18% in last 5 seconds
      18% in last 1 minute
      18% in last 5 minutes
Slot 2 CPU 0 CPU usage:
      17% in last 5 seconds
      16% in last 1 minute
      17% in last 5 minutes
```

使用命令 display cpu data-plane slot X （X 代表设备在 IRF 中的成员编号）查看数据平面 CPU 利用率的统计信息。

```
<H3C>display cpu data-plane
Slot 1 CPU 0 CPU usage:
       85% in last 5 seconds
       86% in last 1 minute
       85% in last 5 minutes
Slot 2 CPU 0 CPU usage:
       0% in last 5 seconds
       0% in last 1 minute
       0% in last 5 minutes
```

2、是否开启策略加速

NGFW V7 防火墙从 D022 分支开始使用的都是安全策略，安全策略加速是默认开启的，D022 之前的分支版本使用的是域间策略，域间策略策略加速默认是不开启的。在对基于会话的业务报文（如 NAT、ASPF 等）进行规则匹配时，通常只对首个报文进行匹配以加快报文的处理速度，但这有时并不足以解决报文匹配的效率问题。例如，当有大量用户同时与设备新建连接时，需要对每个新建连接都进行规则匹配，如果对象策略内包含有大量规则，那么这个匹配过程将很长，这会导致用户建立连接时间超长，CPU 会增高，从而影响设备新建连接的性能如延迟丢包等现象。

对象策略加速功能则可以解决上述问题，当对包含大量规则的对象策略使能了加速功能之后，其规则匹配速度将大大提高，从而提高了设备的转发性能以及新建连接的性能，通过命令行进行查看对象策略组是否激活。

```
[H3C]display object-policy accelerate summary ip
Object-policy ip test
```

D032 新版本分支中安全策略加速功能默认开启，且不能手动关闭，如下几种情况会导致安全策略加速功能失效。

（1）激活安全策略规则加速功能时，内存资源不足会导致安全策略加速失效。

若安全策略规则中指定的 IP 地址对象组中包含排除地址和通配符掩码，则会导致安全策略加速功能失效。

（2）安全策略加速失效后，设备无法对报文进行快速匹配，但是仍然可以进行原始的慢速匹配。

（3）为使新增或修改的规则可以对报文进行匹配，必须激活这些规则的加速功能。

（4）激活安全策略规则的加速功能时比较消耗内存资源，不建议频繁激活加速功能。建

议在所有安全策略规则配置和修改完成后，统一执行 accelerate enhanced enable 命令。

（5）若安全策略规则中指定的 IP 地址对象组中包含用户或用户组，则此条安全策略规则失效，将无法匹配任何报文。

（6）安全策略规则中引用对象的内容发生变化后，也需要重新激活该规则的加速功能。

例如，对象组中包含排除地址和通用符掩码会导致加速失败，新版本中会报如下日志：

```
%May 24 08:19:21:458 2019   FJFZ-PC-WGWL-FW-F5000M-SJ5FB
SECP/4/SECP_ACCELERATE_NOT_SUPPORT: Failed to accelerate IPv4 security-
policy. Reason: An IP address object group is configured with excluded
IP addresses for rule 105 of policy.
```

3、开启策略加速

D022 分支版本不自动加速，如果因为没有开启策略加速导致 CPU 高，可以通过如下命令行开启策略加速。

```
[H3C]security-policy ip
[H3C-security-policy-ip]accelerate enhanced enable
```

4、是否存在单核打满的情况

NGFW V7 防火墙有多个转发核同时工作处理报文，多核处理方式有两种，一种是逐包转发，一种是逐流转发。逐包转发性能高，基于报文处理，将报文依次发送到不同的 CPU 进行处理，但是不保证报文的处理顺序，可能会有乱序的风险；逐流转发性能低于逐流转发，基于流处理，设备可以基于五元组划分流，将五元组相同的一条流分配到同一个 CPU 进行处理，处理过程保证先进先出，V7 设备默认是逐流转发，如果单核被打满后设备转发性能会受到影响。

查看单核状态用 display process cpu | include kdr 命令，如下：

```
[H3C]display process cpu | include kdrvdp
       169      0.0%      0.0%      0.0%    [kdrvBoardTsk0]
       170      0.0%      0.0%      0.0%    [kdrvcp0]
       171      0.0%      0.0%      0.0%    [kdrvcp1]
       172      0.0%      0.0%      0.0%    [kdrvdp2]
       173      0.0%      0.0%      0.0%    [kdrvdp3]
       174      0.0%      0.0%      0.0%    [kdrvdp4]
       175      6.0%      6.0%      6.0%    [kdrvdp5]
       176      0.0%      0.0%      0.0%    [kdrvdp6]
       177      0.0%      0.0%      0.0%    [kdrvdp7]
       178      0.0%      0.0%      0.0%    [kdrvdp8]
       179      0.0%      0.0%      0.0%    [kdrvdp9]
       180      0.0%      0.0%      0.0%    [kdrvdp10]
       181      0.0%      0.0%      0.0%    [kdrvdp11]
       182      0.0%      0.0%      0.0%    [kdrvdp12]
       183      0.0%      0.0%      0.0%    [kdrvdp13]
       184      0.0%      0.0%      0.0%    [kdrvdp14]
       185      0.0%      0.0%      0.0%    [kdrvdp15]
```

前 2 个 vcpu 为控制核，负责管理和控制表项生成，后面 14 个转发 vcpu 处理业务。CPU 利用率 100 为极限，100/16=6.3%，单核到了这个数值就表明单核被打满了，此时需要查看会话是否异常。

5、修改转发模式

如果出现设备单核打满情况，之前为逐流处理方式，可以通过更改为逐包方式后再查看单核是否还存在被打满情况。

用命令行去更改设备转发模式，如下：

```
[H3C]forwarding policy ?
  per-flow    Per-flow forwarding
  per-packet  Per-packet forwarding
```

6、查看会话是否异常

NGFW V7 防火墙针对每个型号都有会话规格，超过了会话规格，设备转发性能会受到影响，可能会产生丢包，命令行可以查看会话并发与新建会话量如下：

```
[H3C]display session statistics summary
Slot Sessions  TCP       UDP       Rate      TCP rate  UDP rate
1    6      21589      485         0/s       0/s       0/s
2    6        2         4          0/s       0/s       0/s
```

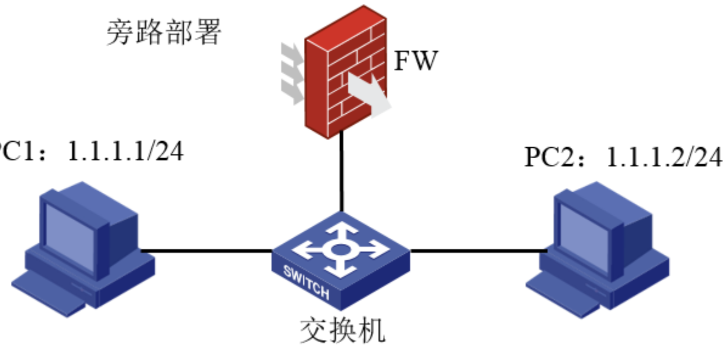
如果会话异常，则要查看 Top-statistics 统计，是否有单个源 IP 地址异常的情况；如果会话

量不大，则要看下接口 ARP 是否达到限速值。

7、接口 ARP 是否达到限速值

防火墙为了保护 ARP 进程软件上存在接口 ARP 限速，如果触发了 ARP 限速，会导致该 ARP 请求报文被丢弃，从而产生丢包的现象。

如下为某局点 ARP 限速导致丢包案例，防火墙旁路部署，防火墙采用二层聚合口与交换机对接，组网运行一段时间出现丢包现象，在防火墙与交换机互联的接口进行抓包分析，发现故障时服务器一直在发送 ARP 请求，但防火墙没有发送 ARP 应答报文。



Debug 发现有大量的 ARP 广播报文上送防火墙，ARP 报文速率超过了限速值，因此后续报文会产生丢包。

```
*May  5 18:22:17:686 2019 HF-F5040-BJCLOUD MACFW/7/MACFW_ERROR: -Context=1;
Frame discarded: ARP packet rate limit exceeded.

*May  5 18:22:17:687 2019 HF-F5040-BJCLOUD MACFW/7/MACFW_ERROR: -Context=1;
Frame discarded: ARP packet rate limit exceeded.

*May  5 18:22:17:687 2019 HF-F5040-BJCLOUD MACFW/7/MACFW_ERROR: -Context=1;
Frame discarded: ARP packet rate limit exceeded.

*May  5 18:22:17:687 2019 HF-F5040-BJCLOUD MACFW/7/MACFW_ERROR: -Context=1;
Frame discarded: ARP packet rate limit exceeded.

*May  5 18:22:17:687 2019 HF-F5040-BJCLOUD MACFW/7/MACFW_ERROR: -Context=1;
Frame discarded: ARP packet rate limit exceeded.

*May  5 18:22:17:687 2019 HF-F5040-BJCLOUD MACFW/7/MACFW_ERROR: -Context=1;
Frame discarded: ARP packet rate limit exceeded.

*May  5 18:22:17:687 2019 HF-F5040-BJCLOUD MACFW/7/MACFW_ERROR: -Context=1;
Frame discarded: ARP packet rate limit exceeded.
```

8、更改组网

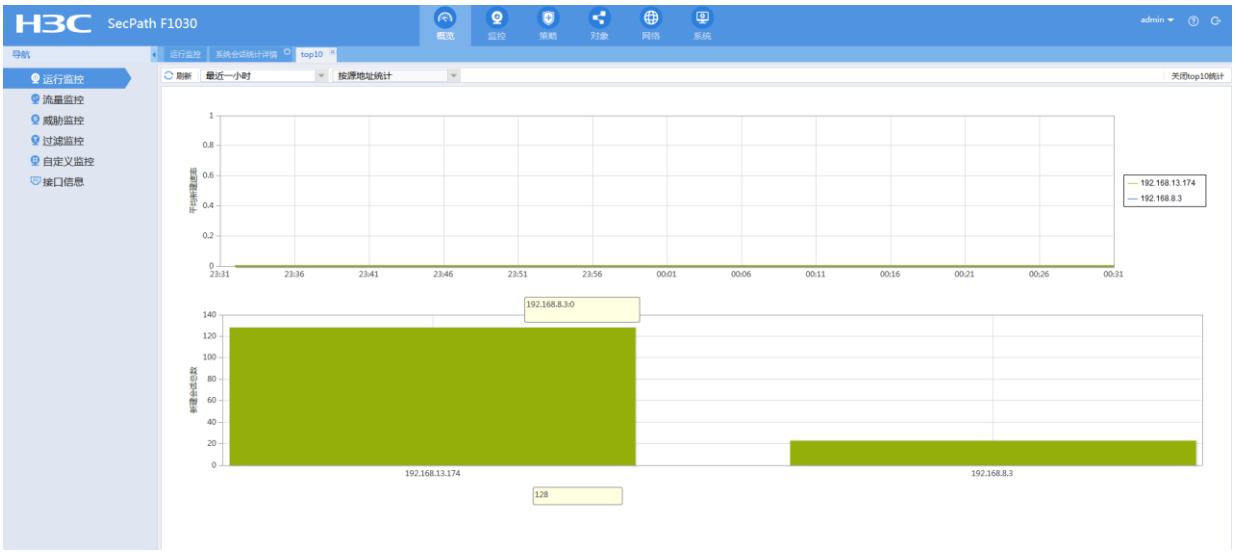
针对这种情况需要修改组网，创建聚合子接口，将 Vlan-interface 改成三层聚合子接口，因为二层聚合接口的环境是属于 MAC 软转，ARP 有限速，改为三层聚合口后，是三层转发，对于 ARP 报文规格上没有限制。

9、查看会话 Top-statistics 是否异常

如果会话存在异常，首先需要开启 top 会话统计 session top-statistics enable，然后查看 Top-statistics 是否存在会话异常的源 IP 地址，可以通过命令行 display session top-statistics last-1-hour 查看最近一小时的会话量。

```
[H3C]display session top-statistics last-1-hour
Counting by source addresses:
No.       Source address                                Sessions
1         172.31.0.24                                   16360001
Counting by destination addresses:
No.       Destination address                           Sessions
1         10.72.66.36                                   636
```

Web 上通过【概览】—【运行监控】—【查看 top10 统计】路径查看。



10、将异常的源 IP 加入黑名单

如上排行 Top 1 的会话量在最近一小时达到了一千六百多万的会话，查看此 IP 地址是一个监控服务器，正常情况下此 IP 地址会话量很少，因此可以判定收到了攻击，产生了大量的攻击报文，导致会话量突高，可以通过把异常会话的源 IP 地址加入黑名单的方式来暂时规避攻击，命令行可以通过全局和安全域下两种方式加入黑名单。

```
[H3C]blacklist global enable                    //开启全局黑名单
[H3C]blacklist ip 172.31.0.24
[H3C]security-zone name test
[H3C-security-zone-test]blacklist enable        //开启安全域黑名单
[H3C]blacklist ip 172.31.0.24
```

在 Web 上可以通过【策略】—【安全防护】—【黑名单】如下路径来添加全局黑名单，或者通过【策略】—【安全防护】—【安全域】路径来开启添加安全域黑名单。

11、查看是否属于硬件性能丢包

如果设备会话量很大，且没有异常的攻击流量，正常情况下高峰期出口流量很大，可能是达到了设备性能瓶颈，此时需要查看 DMP 上对应的 NGFW 产品市场规格表，判断会话量和适用带宽是否超过阈值，如果超过的话建议更换性能更高的设备。

可以在 probe 视图下通过 display hardware internal xlp poe para slot X 命令收集信息提供给工程师分析是否存在硬件性能丢包。

```
[H3C-probe]display hardware internal xlp poe para slot 1
POE POE_DISTR_CLASS_DROP_CNT:
POE_DISTR_C280_DROP_CNT : 0x0
POE_DISTR_C281_DROP_CNT : 0x0
POE_DISTR_C282_DROP_CNT : 0xf2fab14a
POE_DISTR_C283_DROP_CNT : 0x294c05a4
POE POE_DISTR_CLASS_DROP_CNT:
POE_DISTR_C280_DROP_CNT : 0x0
POE_DISTR_C281_DROP_CNT : 0x0
POE_DISTR_C282_DROP_CNT : 0x5e2e8a
POE_DISTR_C283_DROP_CNT : 0x605f83
```

通过 display system internal ip packet-drop statistics slot X 查看设备是否存在分片重组失败报文丢包，观察 virtual fragment reassembly failed 参数对应数值如果存在过大，则证明存在分片失败丢包。

防火墙处理大包的能力有限，如果正常业务中存在大量大包，需要修改运营商网关接口上的 TCP MSS 的值使得通过防火墙插卡的报文不要分片，以提升防火墙的处理性能。

```
[H3C-probe]display system internal ip packet-drop statistics slot 1
Slot 1:
IPv4 packets dropping statistics:
  Drop orignal paket after fragmentation:                          0
  Match blackhole FIB:                                          0
  Interface forbids forwarding broadcast packets:                    0
 …
    Interface network status down:                                21020
  Unknown FIB forwarding type:                                  0
  Drop layer 2 broadcast and multicast packets:                     1500
  Unknown protocol type:                                        0
  IP version error:                                               0
  IP header length error:                                         0
  Packet length less than that claimed in IP header:                    0
  Invalid destination IP address:                                   0
  IP options processing error:                                    0
  IP checksum error:                                             0
  Fragments in queue for virtual reassembly reach the limit:            0
  Virtual fragment reassembly failed:                           3258917
  Dropped by control plane policing:                              0
  Expand packet buffer failed:                                    0
  Packet buffer error:                                           0
  Invalid fragment flag:                                          0
  Packet length claimed in IP header larger than 65535 bytes:           0
  Source or destination ip is loopback but not local:                   0
```

12、更换高性能设备

例如 F1020 设备的混合包吞吐量为 1G，但是高峰期流量超过了 1G，这时候如果产生丢包卡顿就跟设备性能有关，需要更换高性能的设备。