一、开始

内存利用率高是防火墙最常见的问题之一，首先通过 display memory 查看设备内存是否在正常范围，如果内存占用很高，可以从会话、是否开启 DPI、防火墙内存释放机制、是否存在内存泄露的已知问题等方面入手。会话方面主要看是否存在大量半连接会话、 是否存在会话长连接、会话并发是否超过设备规格等；防火墙是否开启了 DPI，如 IPS、URL 过滤、数据库过滤、文件过滤、防病毒等；防火墙的内存释放机制一般是达到一级告警门限会自动释放；是否存在内存泄露主要是查看版本说明书。具体排查方详见以下步骤。

二、流程图相关操作说明：

1.查看内存利用率

命令：display memory

举例：一般情况内存使用率建议不高于 70%，如果持续高于 70%超过 3 小时，即内存剩余率持续小于 30%，或者内存突然升高，需要关注。

```
<F1070>dis memory
Memory statistics are measured in KB:
Slot 1:
             Total        Used        Free      Shared     Buffers      Cached
FreeRatio
Mem:         8142380     3390072     4752308           0       14680     1237992
69.1%
-/+ Buffers/Cache:    2137400    6004980
Swap:           0           0           0
```

2. 查看是否存在内存泄露的已知问题

请确认现场版本，并查阅版本说明书确认。

3. 将设备升级至官网最新版本

如果现场版本过老，请升级版本至官网最新版本。

4. 是否存在会话长连接或者会话并发超规格

如果误配会话长连接，最极端的情况是配置了会话永不老化，将会导致会话永不释放，持续消耗设备内存，最终导致内存耗尽。如果现场已经没有相业务，但是会话却一直在，可以看一下现场是否开启了会话长连接。如果现场存在会话长连接，请在相应视图下将相应的会话长连接关闭掉，各个视图下会话长连接配置命令如下：

```
session persistent aging-time  （安全策略视图下）
session aging-time（安全策略视图下）
session persistent acl xxxx aging-time 命令用来配置长连接会话规则。（全局视图下）
session  aging-time  application 命令用来设置应用层协议或应用的会话老化时间。（全局视图下）
session aging-time state 命令用来设置各协议状态的会话老化时间。（全局视图下）
```

例如以下配置会使得会话永不老化或者老化时间过长：

```
Security-policy ip
rule 3 name 80
  action pass
  logging enable
  counting enable
  source-zone Untrust
  destination-zone Trust
  destination-ip-host 1.1.1.1
  session persistent aging-time 0
rule 2 name 78
  action pass
  logging enable
  counting enable
  source-zone Untrust
  destination-zone Trust
  destination-ip-host 1.1.1.1
  session aging-time 2000000
```

通过以下命令查看设备当前并发会话是否超过设备规格：

```
[F1070_IRF]display session statistics
Slot 1:
Current sessions: 18
          TCP sessions:                    3
          UDP sessions:                   14
         ICMP sessions:                    1
       ICMPv6 sessions:                    0
     UDP-Lite sessions:                    0
         SCTP sessions:                    0
         DCCP sessions:                    0
        RAWIP sessions:                    0

          DNS sessions:                    3
          FTP sessions:                    0
          GTP sessions:                    0
         H323 sessions:                    0
         HTTP sessions:                    1
```

防火墙设备的会话并发数可以参考 DMP 的市场规格列表。

5. 取消会话长连接或者、更换更高性能的设备

假如现场存在会话长连接或者会话并发超规格，可以取消会话长连接或者更换更高性能的设备。

6.是否存在大量半连接会话

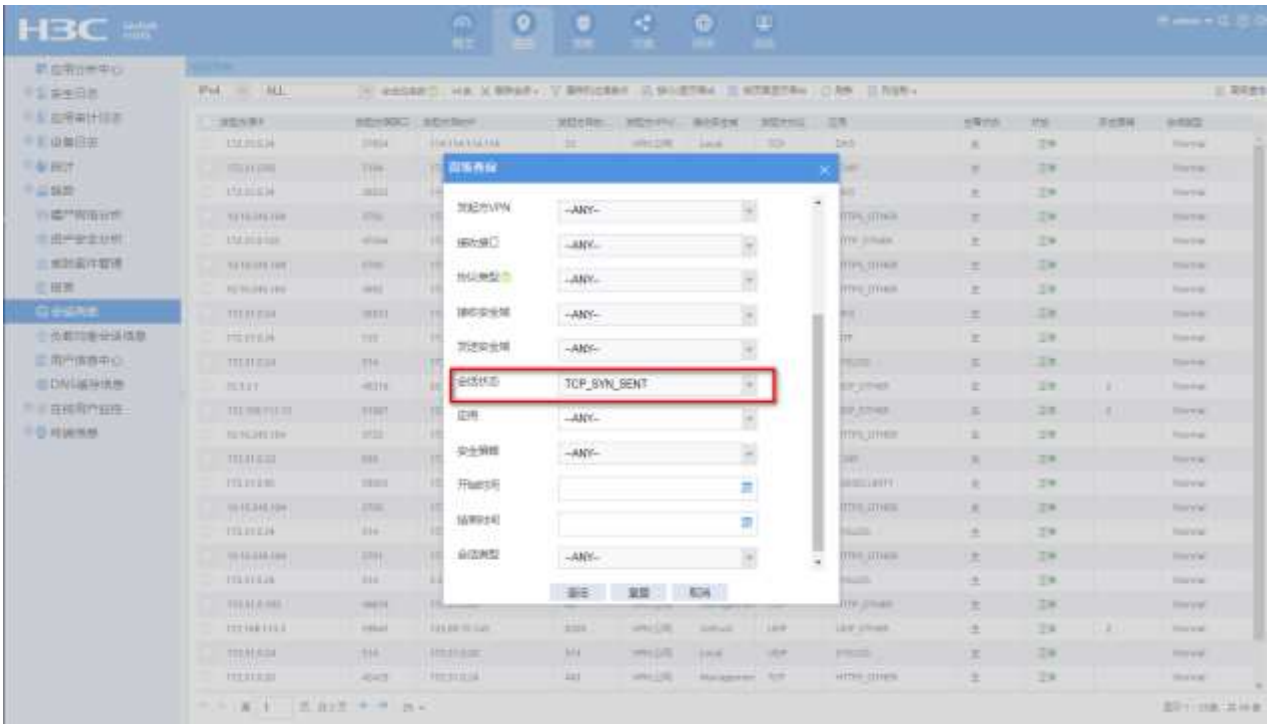
如果设备存在大量半连接会话，会持续在设备上创建会话，耗费设备内存，此时需要使用安全策略阻断异常会话。

命令：display session table verbose

例如：通过命令查看多条详细会话信息，受到 SYN Flood 攻击的设备会话有如下特点：会话状态 SYN，一般目的 IP 比较固定，大多数情况是内部的服务器，反向可能没有回包。

```
[h3c]display session table verbose
Initiator:
  Source IP/Port : 255.91.195.14/26851
  Dest IP/Port   : 115.239.230.214/7444
  VPN-Instance/VLAN ID/VLL ID:
Responder:
  Source IP/Port : 115.239.230.214/7444
  Dest IP/Port   : 255.91.195.14/26851
  VPN-Instance/VLAN ID/VLL ID:
Pro: TCP(6)     App: unknown           State: SYN
Start time: 2013-04-18 03:35:46  TTL: 0s
Root                      Zone(in):Untrust
                          Zone(out):Trust
Received packet(s)(Init): 1 packet(s) 40 byte(s)
Received packet(s)(Reply): 0 packet(s) 0 byte(s)
Initiator:
  Source IP/Port : 137.114.132.16/25480
  Dest IP/Port   : 115.239.230.214/7444
  VPN-Instance/VLAN ID/VLL ID:
Responder:
  Source IP/Port : 115.239.230.214/7444
  Dest IP/Port   : 137.114.132.16/25480
  VPN-Instance/VLAN ID/VLL ID:
Pro: TCP(6)     App: unknown           State: SYN
Start time: 2013-04-18 03:36:04  TTL: 1s
Root                      Zone(in):
                          Zone(out):
Received packet(s)(Init): 1 packet(s) 40 byte(s)
Received packet(s)(Reply): 0 packet(s) 0 byte(s)
```

WEB 界面可以通过以下方式查看：



7.使用安全策略阻断异常会话

假设现场存在大量半连接会话，可以使用安全策略阻断异常会话。

8.是否开启了 DPI

如果设备上开启了入侵防御功能，设备性能减半，所以与未开启入侵防御相比，会加重内存的消耗，可以通过查看设备配置，看一下设备上是否存在 IPS、文件过滤、URL 过滤、防病毒等配置。

以 F1070 为例，WEB 界面查看方式如下，其中安全策略规则 ID 为 0 的都是调用了默认策略：

对应的命令行查看方式如下：

```
[H3C]display security-policy ip
security-policy ip
 rule 0 name all
  action pass
  counting enable
  profile 0_IPv4

[H3C]display current-configuration configuration app-profile
app-profile 0_IPv4
 ips apply policy default mode protect
 data-filter apply policy default
 url-filter apply policy default
 file-filter apply policy default
 anti-virus apply policy default mode protect
 waf apply policy default mode protect
 apt apply policy default
```

9.关闭 DPI 或者使用跟高性能的设备

DPI 功能在 2G 以上设备才支持，如果现场设备内存在 2G 左右，并且拥有 2 个以上的授权，并且升级了最新特征库，可能导致基础内存就很高，因此如果现场存在此情况，请现场关闭 DPI 或者更换更高性能的设备。

10.是否错用大小病毒库

对于防火墙，如果要使用防病毒功能，必须及时更新病毒库，如果防火墙的内存小于 8G，需要使用小库，大于或等于 8G 可以使用大库。

<H3C>system

[H3C]probe

[H3C-probe]display system internal version

H3C SecPath F1000-AK108 V900R005B03D632SP35

Comware V700R001B64D032SP35

R9333P22 及以上的版本内存 8G 及以上设备且设备存储介质 1G 以上升大库 。如果内存 8G 以下设备或存储介质是小于 1G，只支持升级小库。如，有些 F5040 的 cf 卡是 256M，虽然

内存高于 8G 但是不能升级大库。

实验室使用设备 F1000-AK145，版本 R9333P21，内存 4G，在没有任何流量的情况下。

升级完大库之后，设备出现内存告警门限。

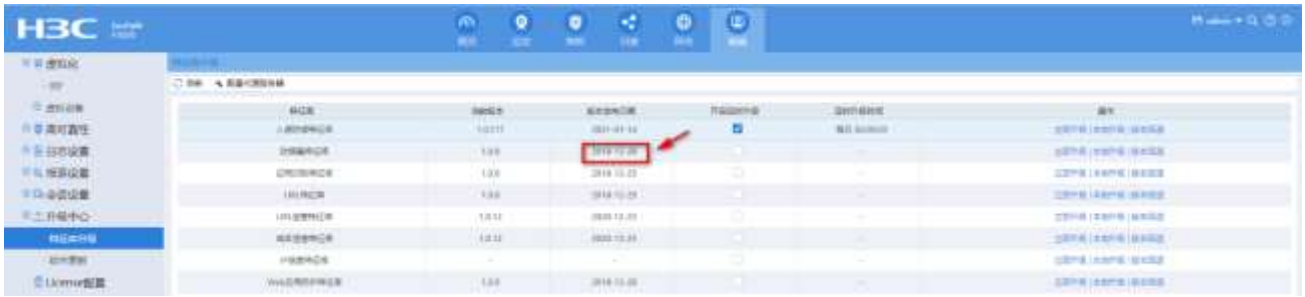
```
[H3C]display memory
Memory statistics are measured in KB:
Slot 1:
             Total        Used        Free      Shared     Buffers      Cached
FreeRatio
Mem:         4027996     3775260      252736           0           0      415908
9.6%
-/+ Buffers/Cache:    3359352     668644
Swap:              0           0           0


%Sep 28 16:25:28:079 2020 OA_6F_H3C_F1030_9.1 DIAG/1/MEM_EXCEED_THRESHOLD: -
Context=1; Memory minor threshold has been exceeded.
%Sep 28 16:25:28:218 2020 OA_6F_H3C_F1030_9.1 DIAG/1/MEM_BELOW_THRESHOLD: -
Context=1; Memory usage has dropped below minor threshold
```

可以通过查看 AV 特征库发布日期来判断设备使用的特征库是大库还是小库。

http://www.h3c.com/cn/Products___Technology/Products/IP_Security/Characteristic_Service_Area/

以 F1070 为例，可以在“系统---升级中心---特征库升级处查看 AV 特征库发布时间”。



11. 请使用正确的特征库

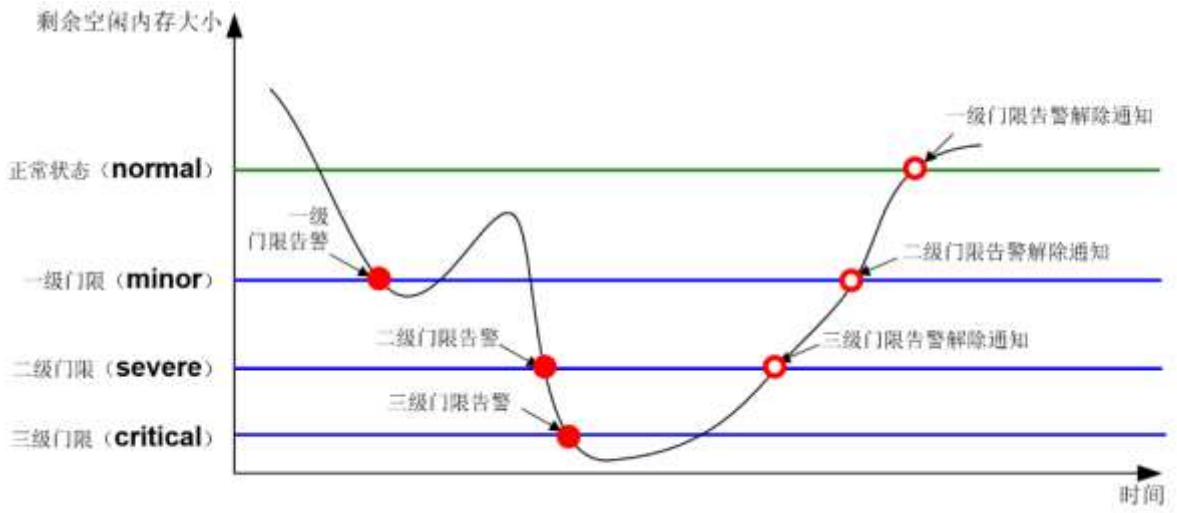
如果现场错误使用了 AV 特征库，请现场使用正确的 AV 特征库。

12. 是否 cache 占用比较多

内存 cache 占用过多，达到一级告警门限会自动释放内存。比如 cached 占了内存总量的 30%以上，可以持续观察一段时间。

```
[H3C]display memory
Memory statistics are measured in KB:
•Slot 1:
                          Total           Used           Free        Shared
     Buffers       Cached     FreeRatio
Mem:              4028220      3843828        184392                 0
   3124       342132               7.2%
-/+ Buffers/Cache:     3498572       529648
```

内存释放机制为：当前设备内存释放机制是，当剩余内存小于 normal 值，会触发 cache 和 buffer 占用的内存释放。



假设现场剩余内存为 283M，normal 值为 235M，可以调整为 500M，当剩余内存低于设置的这个值会自动释放 Buffers/Cache。

可以通过以下命令调整 normal、一级门限、二级门限、三级门限值分别为 4000MB、3000MB、2000MB 与 1000MB。

命令：*memory-threshold slot 1 cpu 0 minor 3000 severe 2000 critical 1000 normal 4000*

三. 拨打热线 400-810-0504 寻求帮助

如果进行以上排查依然不能解决，请收集设备诊断以及以下信息并且拨打 400。

1. display session statistics
2. display session top-statistics last-1-hour
3. display session table verbose