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 stat</f1070>	memory istics are	e measured i	n KB:			
Slot 1.	iberes ar	measarear				
5100 1.	Total	Used	Free	Shared	Buffers	Cached
FreeRatio						
Mem:	8142380	3390072	4752308	0	14680	1237992
69.1%						
-/+ Buffers	/Cache:	2137400 6	004980			
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]dis	splay session s	tatistics	
Slot 1:			
Current sessio	ons: 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
                        Zone(in):Untrust
Root
                        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
                        Zone(in):
Root
                        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:

C#0=#0												
新生司書	Pol All	(i) east	COLHA: X SPAR	VIV BHICK	B.F. (5, 593)	THA 1 11 107	(#2284)	ORN DIMEN				(第
在将来计11 年	100550	101000	apriler.	- Milener-	Marrie .	BORSK :	anteria l	100	5975	1750	31284	9.132
山甸田田田	LALINE H	1004	THE PLACEMENT		white	- Lond		Dedi		24		Invest
mat /	The second	THE	THE REAL PROPERTY.					x 200		28		Investigation of the second
18.20	etenisie	-10000	1.0					10.0		120		Terra.
C With series	ALL REAL PROPERTY.	174	2012/2/174	-ARY-		- 9		TTPS, STITUS		20.		100700
11-2-2-041	L'Maigine.	-104	10000	-BMV-				free pression.	12	29.		10010
#21日前中国1月	1010010101	100	THE REAL PROPERTY.					TTPS_STORE		38.		-
11.21	10100-000		NU.RSC 1	ANDY		17		TTPE D'MARK	2	39.		Server.
	TILITIE		IN BORSH	~ANS-		10						1000
法通知管理法法规	C PERSON	111	Ph. manual					277	12	39.		Transfer .
THE BAC	TEALERA		100×304	-AND-		35		1000	1.5	18.		Terror.
DNUEBHK	10.117	-0.111	自然状态	TCP_SVN	SENT	1		an other	- 12	10.	1.60	Incide
RICROTHE	111 100 111 11		11 24	197		317	- 1	10,000	.5	28.		The second
100000	NUNCHED IN		100					ITTPS_UITEER	12	- 28.		transa.
			安土的田	-ANY-		2		240				Sec.
	rearran	1000	HE FRANK			-		ACCOUNTS AND A		38.		Torral.
	10-15.345.104	1.000	100					itter, annes		28		Tory of
	ITLITEI+	104-1	PERSONAL PROPERTY			1		Martin I	+	24		(and a second
	1012244.000	13794	0/2/852	-ANY-		10		othe stress	12	28		inches.
	TRATES.	in c		1 Contraction of the local sectors of the local sec		1000111		and the second second	+	124		Towns.
	101.AL.0.000	-0414	110	9.6	2.0	656	-	ine prian	12	38		The year's
	TTT ING I IS A	- estad	CALLSO TO LAR	ana :	units.	and a	100	Law private	+	28	0.81	(included)
	111.11.0.04	1214	100.01.000	344	man	1000	100	PROFESSION		2.0		terri and
		4943	deres and	101	-	-	100	witten chinem	-	- 29		the second

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:

HBC III					9	0 0		•											
104488	2100																		
6186	10.484-10.8	10 H H H	89 - PE- 0	Bri GBa	R(1) - 21	1 (2 2 H) 1 - Berl		er . 16, 101, 64	0.0399								100.000	10.10.0	4 2,4091
- MECLANIF	TORMENTR SPEEDOACH	AND OWNER	1 842 2118	NO. WRITER	*****	ORCHAN BET	RE INCOM	TR DAN	CE -74	14. WE		***	-						
CAUSER .	1.10	3111	Probate .	- 10	10 000	915	Revenu-	88	30		1972	7	18	-	4785	98		Berlint.	8598
T B D emm											this place	Т							
12.941	1.00										20 pelod	L		-					
TRADE!				. 77				-	-		Jul and a di	Ľ				1.2	775	1.5	
A MIRINAT											UR-minde 201 minute	н							
# A MERNAE	1.144		1.1.0	1914	4	149	44	A.44		-	_				24	10	111	10.0	
1 BLOMBIT	#111	**	40	-	1.4	40	**	Arre	40	-					-		-		
13.41元年2月	11445		-	1.014		-	-	- 27	-	-			1846		-	-			
10 作用口由	0.44			814		-		-		-					-		100	1.8.1	
CARSING CARSEN																			

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 stat:	y memory istics are	e measured	in KB:						
5107 1.	Total	Used	Free	Shared	Buffers	Cached			
FreeRatio	10041	obeu	1100	bildred	Durrerb	ouonou			
Mem:	4027996	3775260	252736	0	0	415908			
9.6%									
-/+ Buffers/	/Cache:	3359352	668644						
Swap:	0	0	0						
<pre>%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</pre>									

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/Characterist

ic_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"。

HBC the		0 2	0 4	9 0		H+9.0 P
N H BEAR	C DR A RECEIVE					
Castile	608	No. 1	Accession 1	Talanta	Denders	81
0.0.用时数性	Ampion	ward .	1001-01-00		All landsom	ALL PROPERTY AND
▲ E 155 km	Disance .	1.108	2010-12-20	-		8214 (1014 (1118)
IT IL HERICE	Distance .	6.000	2010 13.22			127901007010000
*D-000#	10104028	100	394.03			The start was
ELINERO.	101.00000000	1446	(9849-19.01			221-0 (201-0 (MAR))
NEERU	64.00%24	(4.1)	((0000-10.00)			DEFE DEFE MARK
2-21	reakos					para anna pala
C License El R	WARRANTING	1.0.0				STATISTICS INCOME

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:										
	Т	otal	Used	Free	Shared					
Buffers	Cached	FreeRatio								
Mem:	4028220	3843828	184392		0					
3124	342132	7.2%	1							
-/+ Buffers/C	Cache: 3498	572 52	9648							

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 norma1、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