某局点AC CPU利用率高问题经验案例

wlan接入 协议报文限速 SNMP 樊昊 2015-07-29 发表

某客户反馈我司LSQ1WCMD0设备CPU使用率过高，导致无法正常配置，网管平台持续报警。

CPU高

通过一线反馈现场AC配置，以及现场情况，近期现场做过的变更。现场最近测试WSM系统，看到task中AGENT进程占用了较多CPU。

#

snmp-agent

snmp-agent local-engineid 800063A20380F62ED4486F

snmp-agent community read public

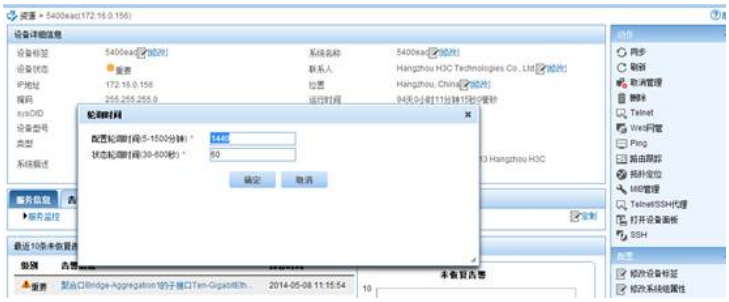
snmp-agent community write private

snmp-agent sys-info version all

snmp-agent target-host trap address udp-domain 202.38.193.215 params securityname public v2c

#

于是先安排现场对WSM组件进行优化，在iMC管理页面，打开设备的详细信息页面，在详细页面的右边一栏中，查看设备轮询参数为多少。



1. 无线终端轮询周期设置为30分钟

方法：在iMC服务器的安装目录下，找到imc/server/conf/qvdm_wlan.conf，先备份“qvdm_wlan.conf”文件，查看原文件中“StaPollIntv”字段。

优化之后CPU有所下降AGNT进程占用CPU控制在15左右，观察一段时间后，又出现CPU占用到100%的情况，隐藏命令模式，查看task:

发现：[AC-master-hidecmd]dis cpu task

===== Current CPU usage info =====

CPU Usage Stat. Cycle: 8 (Second)

CPU Usage : 100%

CPU Usage Stat. Time : 2015-06-25 15:39:42

CPU Usage Stat. Tick : 0x64b(CPU Tick High) 0xe070e7cb(CPU Tick Low)

Actual Stat. Cycle : 0x0(CPU Tick High) 0x20a32455(CPU Tick Low)

TaskName CPU Runtime(CPU Tick High/CPU Tick Low)

CTLT 0% 0/ 15bc2

TICK 1% 0/ 6cfa90

STMR 3% 0/ 14aaecb

IPCT 0% 0/ daa6d

DrTC 0% 0/ 20d244

MCIN	0%	0/	10e20
IPCB	0%	0/	18235f
RPCQ	0%	0/	154110
VP	0%	0/	42e
ADJ6	0%	0/	ccc3
IPCM	0%	0/	1a29c
INFO	0%	0/	66e
DEV	0%	0/	b0af7
SOCK	0%	0/	81c7e
ADJ4	0%	0/	27ba9
SFLW	0%	0/	384a8
ACL	0%	0/	489a3
LAGG	0%	0/	1a1a5
MSTP	0%	0/	19b2a
LLDP	0%	0/	15f92
PTMT	2%	0/	db993f
PTTP	3%	0/	1093128
ARP	14%	0/	4d8f59e
IP	0%	0/	15e60c
NQA	0%	0/	c84f6
FSLH	0%	0/	152d3
FSLR	0%	0/	5c7b5
NTPT	0%	0/	18357
VTYD	0%	0/	924dc
DHCC	0%	0/	991b
DHCP	6%	0/	1fb9c50
DHP6	2%	0/	ceda8b
ND	7%	0/	27179aa
AGNT	17%	0/	5b56e8a
TRAP	0%	0/	1095
DT1X	3%	0/	107337a
ACM	2%	0/	ae859c
LS	0%	0/	88e37
RDSO	0%	0/	a8a15
RDS	0%	0/	3e7f3c
SC	1%	0/	556af2
IKE	0%	0/	32a8ef
MACA	4%	0/	150fd58
WAPI	0%	0/	9f13a
PSEC	0%	0/	2360a
ULOG	0%	0/	b0e2c
STND	0%	0/	23527
ROUT	0%	0/	13e14d
WMAC	4%	0/	186db48
WIDS	0%	0/	6c9fb
WRRM	0%	0/	6e49a

CWMS 0% 0/ 2b8d3

LWPS 19% 0/ 659e863

WVB 0% 0/ 1739d

WBKP 0% 0/ 5d852

IACT 0% 0/ 14c01

WBNJ 0% 0/ 5e54c

IFNT 0% 0/ 1f230

FTMT 0% 0/ b54d5

FTMC 0% 0/ 8d05b

au0 1% 0/ 610448

CPU占用到100%。

其中ARP占用较多，现场有ARP攻击的可能性，于是开启防止ARP攻击功能：

anti-attack enable

anti-attack protocol arp enable

anti-attack protocol arp flow-threshold 30

配置ARP有所下降。

LWAPP进程较高，查看配置，发现现场热备没有启用单独vlan，且热备心跳时间没有按照公告修改为2000，该处ARP攻击会导致AC热备心跳断开，进而进一步触发了AP主备切换，大量的AP频繁切换，上线下线，进一步加剧了CPU高的问题。并且该处发现主备AP配置不同。

于是修改心跳间隔为2000，且设置单独的vlan，同时修改主备配置保证同步。

#

hot-backup enable domain 1

hot-backup vlan 651

hot-backup hellointerval 2000

#

这些配置修改之后：

1. arp攻击目前通过总限速和流限速已经防住；

2. 在处理完arp攻击，并开启ap冷备，此时arp任务下降，ap没有出现链路切换，仍然出现cpu卡顿，但此时不会出现cpu 100%告警，各种任务的利用率都比较正常，没有明显偏高的情况。

但是观察几天之后，又发现CPU利用率告警。进一步分析，发现与IP v6相关。

通过对送控制平面报文历史记录进行观察，发现在开启ipv6后，default类型报文送控制平面流量不稳定，有时会大量增加。如下加粗部分，

关闭ipv6后，default流量会明显减小，每分钟也就几百pps。

idx proto date rx drop delta

4205 default 15:16:05 06/30/2015 21352183 27630461 4349

4206 default 15:17:05 06/30/2015 21356470 27630461 4287

4207 default 15:18:05 06/30/2015 21361561 27630461 5091

4208 default 15:19:05 06/30/2015 21366239 27630461 4678

4209 default 15:20:06 06/30/2015 21372084 27630461 5845

4210 default 15:21:06 06/30/2015 21376956 27630461 4872

4211 default 15:22:07 06/30/2015 21382793 27630461 5837

4212 default 15:23:13 06/30/2015 21405013 27765054 22220

4213 default 15:24:17 06/30/2015 21414698 27767319 9685

4214 default 15:25:21 06/30/2015 21424383 27770837 9685

4215 default 15:26:29 06/30/2015 21432832 27785073 8449

4216 default 15:27:36 06/30/2015 21447483 28022393 14651

4217 default 15:28:44 06/30/2015 21466325 28042212 18842

4218 default 15:29:51 06/30/2015 21477051 28056607 10726

4219 default 15:30:59 06/30/2015 21487600 28062556 10549

4220 default 15:32:05 06/30/2015 21502073 28071997 14473

4221 default 15:33:12 06/30/2015 21512462 28088208 10389

4222 default 15:34:19 06/30/2015 21521168 28101223 8706

4223 default 15:35:26 06/30/2015 21537726 28126847 16558

4224 default 15:36:29 06/30/2015 21540521 28130720 2795

4225 default 15:37:29 06/30/2015 21541408 28130720 887

4226 default 15:38:29 06/30/2015 21541835 28130720 427

通过对default类型细分查看到出现了大量mid(0x11) type(0x00000002)类型消息，这种消息与ipv6有关。

[AC-master-hidecmd]fpl-diag showcpufcdefault

start .....

mid(0x11) type(0x00000002): 1346937

mid(0x11) type(0x00000004): 114024

mid(0x17) type(0x00000001): 548903

mid(0x19) type(0x00000000): 6

mid(0x43) type(0x00000001): 113531

mid(0xf1) type(0x00000001): 821649

end .....

这种消息有两个事件触发：

1） 数据平面IPv6转发过程中，在使能了重定向功能的前提下，如果发现入接口等于出接口，并且报文的源地址和接口地址在同一网段；

2） 数据平面IPv6转发过程中，如果遇到一些需要发送ICMP6错误报文的情形。 （这一点就是以往出现hop limit攻击的问题导致cpu高，已经通过undo ipv6 hoplimit-expires解决）

只有可能是第一个原因引起，该现象出现肯定是开启了ipv6 redirects enable，且网络中出现了大量触发redirect回应的报文，不排除是有这方面攻击.

根据default报文监控，在开启ipv6时，即使cpu未出现卡顿的情况下， mid(0x11) type(0x00000002)消息速率就达到了100pps左右。在cpu开始出现卡顿，通过default历史记录看该消息类型达到了300pps以上。

大量的消息上送控制平面导致驱动消息接收处理任务任务繁忙，该任务不受平面监控，因此看不到有task高。

这么多的重定向报文肯定是不正常，怀疑网络中还是存在这中redirect攻击，目前没有办法查看该消息的攻击源，和处理hop limit攻击一样，可以通过关闭redirect功能解决。

关闭redirect功能后，该消息类型不再存在，业务正常，slave长ping master4万余包没有出现问题。

[AC-master]undo ipv6 redirects

[AC-master-hidecmd]fpl-diag clearcpufcdefault

[AC-master-hidecmd]fpl-diag showcpufcdefault

start .....

mid(0x11) type(0x00000004): 8

mid(0x17) type(0x00000001): 7

mid(0x43) type(0x00000001): 4

end .....

[AC-master-hidecmd]fpl-diag showcpufcdefault

start .....

mid(0x11) type(0x00000004): 14

mid(0x17) type(0x00000001): 13

mid(0x43) type(0x00000001): 7

进行以上调整后CPU恢复正常。

附：IP v6 redirect攻击

当主机启动时，它的路由表中可能只有一条到缺省网关的缺省路由。当满足一定的条件时，缺省网关会向源主机发送ICMPv6重定向消息，通知主机选择更好的下一跳进行后续报文的发送（与IPv4的ICMP重定向消息的功能相同）。

设备在满足下列条件时会发送对主机重定向的ICMPv6重定向报文：

接收和转发数据报文的接口是同一接口；//本例AC 收到此类报文

被选择的路由本身没有被ICMPv6重定向报文创建或修改过；

被选择的路由不是缺省路由；

被转发的IPv6数据报文中不包含路由扩展头。

1. WSM组件未优化，按照公告优化；

2. arp攻击，arp任务高，配置防ARP攻击

anti-attack enable

anti-attack protocol arp enable

anti-attack protocol arp flow-threshold 30

3 AC出现cpu卡顿，不响应命令，长时间ping不通

4. 热备vlan未独立，并综合问题2）和3）导致AC发生主、备切换、回切，ap重关联，client重新上下线再次加剧cpu负担，达到100%；设置独立vlan，加大hello间隔

hot-backup enable domain 1

hot-backup vlan 651

hot-backup hellointerval 2000

5.开启了ipv6 redirects enable,现场存在攻击，关闭该功能：

ipv6 redirects enable

undo ipv6 redirects