某局点SecPath F1000-AK110内存过高问题处理经验案例

应用审计 内存 刘资瑜 2019-03-29 发表

组网及说明

不涉及

问题描述

现场反馈SecPath F1000-AK110防火墙设备内存82%，但是CPU利用率及flash均在正常范围内。现场版本Ess 9524P13。

过程分析

通过查看display version发现，现场设备内存大小只有1G： DDR3 SDRAM Memory 1008M bytes
通过查看display process memory 发现如下进程占用较高：
125 40 59888 32 388 ifmgr
140 12668 34864 44 8188 comsh
181 560 88924 0 6956 xmlcfgd
499 360 40148 92 14792 dpid
519 676 106828 52 34564 ntopd
4067022 8 44676 84 12996 iked
可以看到，dpid进程是由于设备开启了DPI存在的，comsh是命令行进程，xmlcfgd是Web配置文件进程。
查看与DPI相关的配置包括app-profile，url过滤策略，拉起了DPI的进程，但是现场并未在安全策略中调用，和现场沟通是之前配置过这些策略，后由于一些原因删掉了在策略中调用的命令，但是dpid进程并未结束。
让现场全局开启inspect bypass，但是发现内存占用还是很高。

解决方法

已经让现场全局开启inspect bypass但是故障仍旧，原因是这个命令确实可以关闭DPI，但是不一定可以彻底截止dpid进程。因此需要将保存dpi进程信息的startup.mdb这个文件删除，并且需要重启设备才能生效。需要注意，一旦进行这个操作，设备如果更新过特征库，特征库将会回滚到出厂版本。
1G内存设备建议尽量不要开启DPI功能，可能会导致设备内存过高。