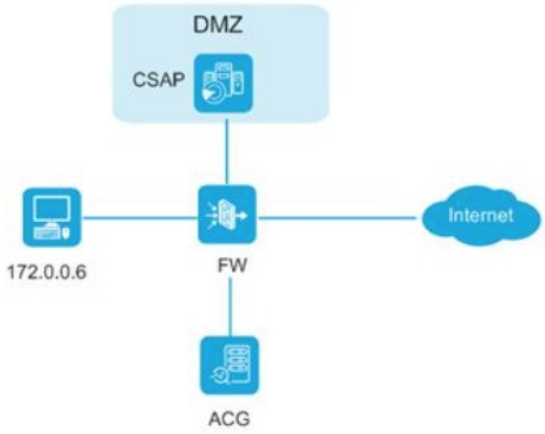
CSAP联动ACG注意事项

日志采集器 **孔梦龙** 2021-11-04 发表

组网及说明



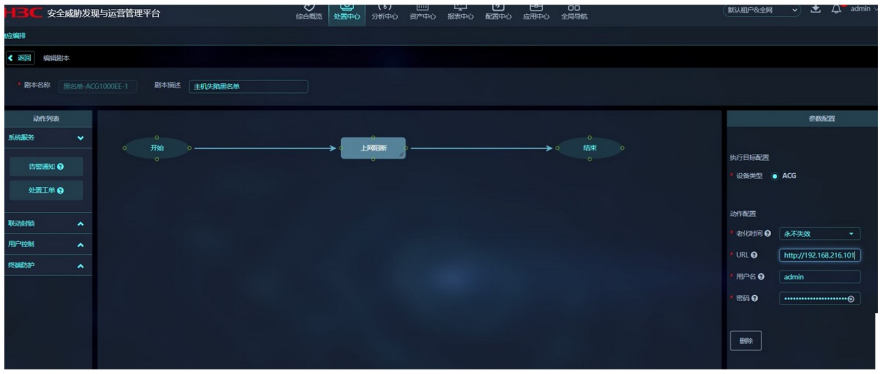
配置的链接参考。https://www.h3c.com/cn/d_202109/1472323_30005_0.htm#_Toc83824921

配置步骤

本案例只说明细节部分：

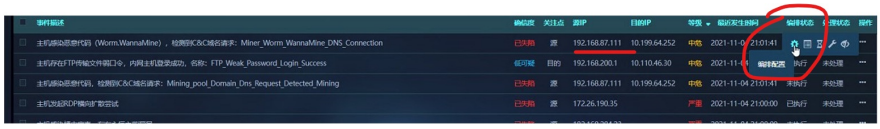
（1）下发的时间需要CSAP上事先存在的事件，这个可以现场伪造几个。

（2）43P04之前的版本在配置下面的URL时候，不用带端口，默认使用80端口，需要ACG上的HTTP的端口也是80；P05以后的版本可以写端口，AVG上也可以使用自定义的端口。



（3）CSAP上实现存在有未处理的危险时间

（4）选择是个事件，假设IP192.168.87.11（图中），然后下发之前的剧本




处理中
已处理
总数
已失期
高可疑
低可疑
严重
0
0
0
145
17
9,147
131
编排配置
* 剧本
请选择
请输入剧本名称
黑名单-ZSZL-FW5060-BJ-2
黑名单-YZL-FW5060-BJ-1

配置关键点