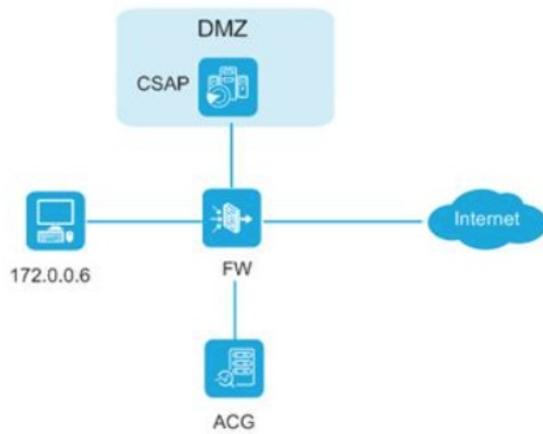


知 CSAP联动ACG注意事项

日志采集器 孔梦龙 2021-11-04 发表

组网及说明



配置的连接参考。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。



基础配置

实时保存配置 关 (注：仅对WEB配置生效)

管理员唯一性检查 关

管理员双因子认证 关 (注：仅对https配置生效) UKey管理软件 UKey客户端软件

最大登录尝试次数 * (1-5)

登录失败阻断间隔 * (10-3600秒)

页面超时时间 * (1-480分钟)

Web在线管理员 * (1-20)

管理员认证方式 本地认证 外部认证

HTTPS端口 *

HTTP端口 *

TELNET端口 *

SSH端口 *

密码周期 天 (1-180)

- (3) CSAP上实现存在有未处理的危险时间

事件描述	源IP	目标IP	等级	危险时间	处理状态	操作
主机弱口令事件 (Worm/WannaMine), 检测IC&C域名请求: Miner_Worm_WannaMine_DNS_Connection	192.168.87.111	10.199.64.252	中危	2021-11-04 21:01:41	未执行	未处理
主机弱口令事件 (Worm/WannaMine), 内网主机登录成功, 名称: FTP_Weak_Password_Login_Success	192.168.200.1	10.110.46.30	中危	2021-11-04 21:01:41	未执行	未处理
主机弱口令事件 (Worm/WannaMine), 检测IC&C域名请求: Mining_pool_Domain_Dns_Request_Detected_Mining	192.168.87.111	10.199.64.252	中危	2021-11-04 21:01:41	未执行	未处理
主机弱口令事件 (Worm/WannaMine), 检测IC&C域名请求: Mining_pool_Domain_Dns_Request_Detected_Mining	172.26.190.35		严重	2021-11-04 21:00:00	已执行	未处理
主机弱口令事件 (Worm/WannaMine), 存在本机之漏洞	192.168.204.23		严重	2021-11-04 21:00:00	未执行	未处理
主机弱口令事件 (Worm/WannaMine), 存在本机之漏洞	10.234.31.136		严重	2021-11-04 21:00:00	已执行	未处理

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

事件描述	源IP	目标IP	等级	危险时间	处理状态	操作
主机弱口令事件 (Worm/WannaMine), 检测IC&C域名请求: Miner_Worm_WannaMine_DNS_Connection	192.168.87.111	10.199.64.252	中危	2021-11-04 21:01:41	未执行	未处理
主机弱口令事件 (Worm/WannaMine), 内网主机登录成功, 名称: FTP_Weak_Password_Login_Success	192.168.200.1	10.110.46.30	中危	2021-11-04 21:01:41	未执行	未处理
主机弱口令事件 (Worm/WannaMine), 检测IC&C域名请求: Mining_pool_Domain_Dns_Request_Detected_Mining	192.168.87.111	10.199.64.252	中危	2021-11-04 21:01:41	未执行	未处理
主机弱口令事件 (Worm/WannaMine), 检测IC&C域名请求: Mining_pool_Domain_Dns_Request_Detected_Mining	172.26.190.35		严重	2021-11-04 21:00:00	已执行	未处理
主机弱口令事件 (Worm/WannaMine), 存在本机之漏洞	192.168.204.23		严重	2021-11-04 21:00:00	未执行	未处理
主机弱口令事件 (Worm/WannaMine), 存在本机之漏洞	10.234.31.136		严重	2021-11-04 21:00:00	已执行	未处理

处理中	已处理	忽略	已关闭	高可疑	低可疑	严重
0	0	0	145	17	9,147	131

配置关键点	IP	目标IP
Worm:Win32/Miner, 检测回C/C域名请求: Miner_Worm_WannaM...	92.168.87.111	10.199.64.252
2021/09/14/72323_30005_0.htm#.Toc838249	92.168.200.1	10.110.46.30
端口命令, 内网主机登录成功, 名称: FTP_Weak_Password_Login_Suc...	92.168.87.111	10.199.64.252
检测回C/C域名请求: Mining_pool_Dns_Request_Detected,	72.26.190.35	
黑名单	92.168.204.23	
黑名单-YSZL-FW5060-BJ-2		
黑名单-YZL-FW5060-BJ-1		

编排配置

副本

请选择

请输入副本名称

- 黑名单-ZSZL-FW5060-BJ-2
- 黑名单-YZL-FW5060-BJ-1