修改IPS某一个缺省动作后不生效，新日志显示仍然命中老的default策略

IPS防攻击 李瑞 2024-08-21 发表

组网及说明

串联部署

告警信息

不涉及

问题描述

防火墙单独例外一个IPS特征，使其动作从缺省的放行改为drop但是不生效

配置如下

```
rule 14 name Trust_Untrust_14_IPv4
 action pass
 profile 14_IPv4
 source-zone Trust
 source-zone Local
 destination-zone Untrust
 source-ip 办公内网
#
app-profile 14_IPv4
ips apply policy ips mode protect
data-filter apply policy default
url-filter apply policy 办公内网---公网
file-filter apply policy default
anti-virus apply policy default mode protect
waf apply policy default mode protect
apt apply policy default
#
ips policy ips
object-dir server client
action block-source drop permit reset
severity-level low medium high critical
status enabled disabled
signature override pre-defined 46406 enable drop logging capture
... ...
```

过程分析

远程debug测试，发现流量能正常命中调用了自定义ips的安全策略，但是刷新web界面的ips日志，发现新增日志还是命中的defalut的ips策略

后查看会话，发现新会话的创建时间是未来时间，确定是防火墙时间问题导致web界面显示的日志是老日志，给管理员带来了无法命中修改后的配置的错觉。

原理：web是以PC时间为准，所以web界面搜索出来的最新日志都是前一天的日志（即以PC时间转换成标准格林威治时间去设备上搜索，但是设备的时间是未来时间，所以格林威治的时间搜出来的日志就是过去的老日志）

解决方法

修改防火墙时间为标准时间后恢复