web更改某一策略的IPS/AV等DPI配置，其他策略也会一起更改

域间策略/安全域 IPS防攻击 AV防病毒 URL过滤 数据过滤 聂骋 2023-01-04 发表

组网及说明

不涉及

告警信息

无

告警信息

问题描述

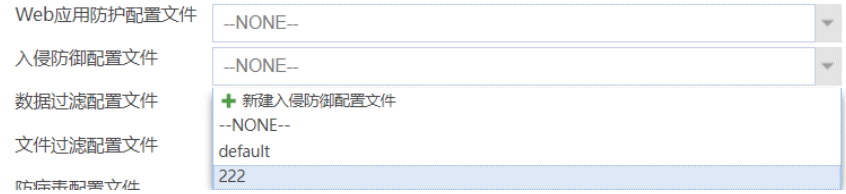
web更改某一策略的IPS/AV等DPI配置，其他策略也会一起更改

过程分析

这个问题是由于web和命令行混配导致的。具体原因如下
对于IPS/AV规则，命令行的操作逻辑是配置app-profile，然后策略下调用。

```
app-profile ips_add_av
ips apply policy default mode protect
rule 3 name test
  description tset
  action pass
profile ips_add_av
```

但是web界面是没有app-profile这一层的，web界面看到的是直接IPS/AV，选择后web自动创建app-profile和策略下调用profile。比如下图，web是直接选择default策略，但是命令行，default是在app-profile下调用的。



这种情况下，web界面需要更改IPS/AV，逻辑就不只是删除策略下的profile，还需要删除app-profile，因为web本身是每个rule一个profile。但是现场应该是命令行操作的，许多策略调用的是相同的profile和app-profile，这就导致web删除app-profile，那其他策略也会收到影响，因为调用的内容没了。这就是批量删除的原因。

批量增加的原因是现场去web操作的时候，web删除了全局的app-profile，但是策略下的profile只删除操作的这一条策略的。
从命令行看就是如下状态，

```
rule 2 name test111
  action pass
  profile ips_add_av
rule 3 name test
  description tset
  action pass
  profile ips_add_av
```

变成

```
rule 2 name test111
  action pass
  profile ips_add_av
rule 3 name test
  description tset
  action pass
```

rule3删除了，但是rule2还会保留profile的配置，这种情况下，重新操作rule2去添加IPS/AV，那么设备就直接生成同名的app-profile ips_add_av，所以其他本身调用同名profile的，就会批量恢复。
综上，现场批量删除是因为web操作删除了app-profile，批量恢复是因为web重新增加了app-profile。
这个情况出现是因为web和命令行逻辑不一样，而现场同个模块出现web和命令行混配导致。同个模块是不能混配的。

解决方法

想恢复的话，可以写个脚本删除所有策略下的profile配置，刷入设备。后续就只用web操作，就不会出现这种情况。