某局点F5000-AI-15（V7）白名单不生效问题处理经验案例

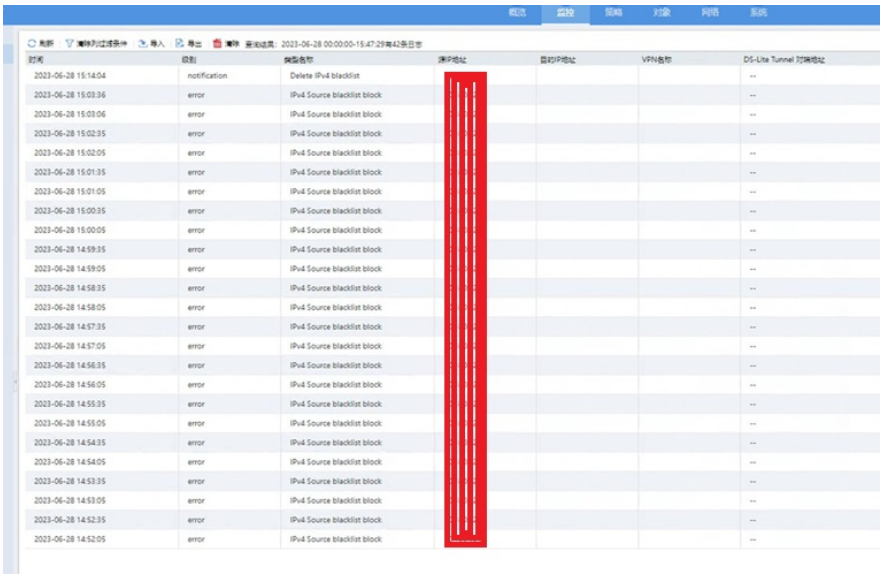
攻击防范 IPS防攻击 刁勇 2023-08-31 发表

组网及说明

组网不涉及

问题描述

某个IP被识别进黑名单了，因此想通过白名单放通，配置完成后发现未生效，在黑名单里依旧可以看到这个IP的记录



过程分析

查看白名单配置：

whitelist global enable

blacklist logging enable

whitelist object-group ������

object-group ip address ������

0 network host address 10.X.X.X

object 0 description ��。�����

10 network range 10.X.X.X 10.X.X.X

object 10 description DNS

中文部分是乱码，怀疑未生效，修改成拼音：

blacklist global enable

whitelist global enable

blacklist logging enable

whitelist object-group ceshi

object-group ip address ceshi

security-zone HeXin

0 network host address 10.X.X.X

object 0 description ceshi

10 network range 10.X.X.X 10.X.X.X

object 10 description DNS

20 network host address 10.X.X.X

object 20 description lousao

测试依旧不行：

解决方法

白名单属于攻击防范模块，而命中IPS特征规则的黑名单属于IPS模块，两者是互不干涉的

针对现场场景，可以通过如下设置，将想要的源地址放白

1．新建安全策略，加上想放通的源地址

2．新建配置文件，针对想要放通的IPS规则，动作为允许

3．安全策略调用新建的IPS配置文件，并且将该策略放到最前