

知 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






时间	级别	消息内容	源IP地址	目标IP地址	VPN名称	DS-Lite Tunnel 归属地址
2023-06-28 15:14:04	notification	Delete IPv4 blacklist				--
2023-06-28 15:03:36	error	IPv4 Source blacklist block				--
2023-06-28 15:03:06	error	IPv4 Source blacklist block				--
2023-06-28 15:02:35	error	IPv4 Source blacklist block				--
2023-06-28 15:02:05	error	IPv4 Source blacklist block				--
2023-06-28 15:01:35	error	IPv4 Source blacklist block				--
2023-06-28 15:01:05	error	IPv4 Source blacklist block				--
2023-06-28 15:00:35	error	IPv4 Source blacklist block				--
2023-06-28 15:00:05	error	IPv4 Source blacklist block				--
2023-06-28 14:59:35	error	IPv4 Source blacklist block				--
2023-06-28 14:59:05	error	IPv4 Source blacklist block				--
2023-06-28 14:58:35	error	IPv4 Source blacklist block				--
2023-06-28 14:58:05	error	IPv4 Source blacklist block				--
2023-06-28 14:57:35	error	IPv4 Source blacklist block				--
2023-06-28 14:57:05	error	IPv4 Source blacklist block				--
2023-06-28 14:56:35	error	IPv4 Source blacklist block				--
2023-06-28 14:56:05	error	IPv4 Source blacklist block				--
2023-06-28 14:55:35	error	IPv4 Source blacklist block				--
2023-06-28 14:55:05	error	IPv4 Source blacklist block				--
2023-06-28 14:54:35	error	IPv4 Source blacklist block				--
2023-06-28 14:54:05	error	IPv4 Source blacklist block				--
2023-06-28 14:53:35	error	IPv4 Source blacklist block				--
2023-06-28 14:53:05	error	IPv4 Source blacklist block				--
2023-06-28 14:52:35	error	IPv4 Source blacklist block				--
2023-06-28 14:52:05	error	IPv4 Source blacklist block				--

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 HeKin

0 network host address 10.X.X.X

object 0 description ceshi

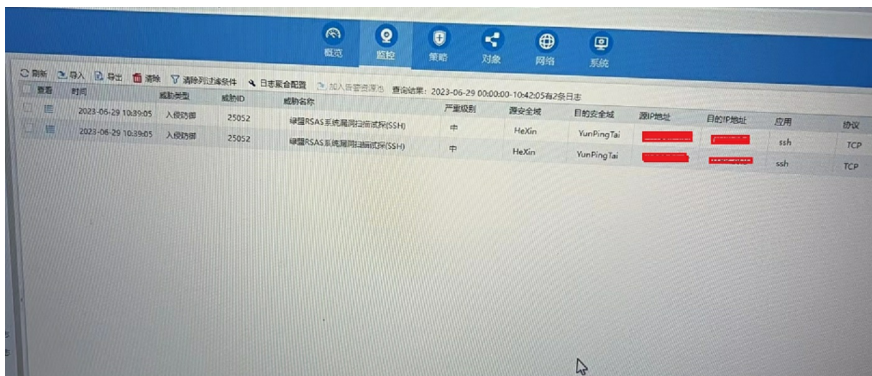
10 network range 10.X.X.X 10.X.X.X

object 10 description DNS

20 network host address 10.X.X.X

object 20 description lousao

测试依旧不行：



时间	威胁类型	威胁ID	威胁名称	严重级别	源安全域	目的安全域	源IP地址	目的IP地址	应用	协议
2023-06-29 10:39:05	入侵防御	25052	入侵PSAS系统漏洞攻击(SSH)	中	HeKin	YunPingTai	[REDACTED]	[REDACTED]	ssh	TCP
2023-06-29 10:39:05	入侵防御	25052	入侵PSAS系统漏洞攻击(SSH)	中	HeKin	YunPingTai	[REDACTED]	[REDACTED]	ssh	TCP

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

