M9000系列防火墙web页面无法产生黑名单日志经验案例

WEB管理 Syslog日志 **葛松炜** 2022-01-28 发表

组网及说明

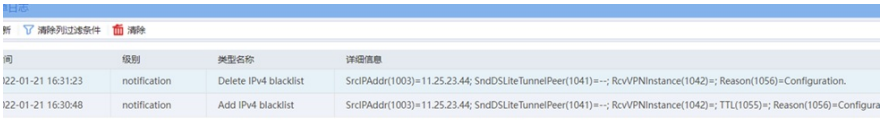
不涉及

问题描述

客户现场使用版本为R9141P42的M9006配置黑名单，在web页面安全防护下配置黑名单地址，测试黑名单功能已生效，无法访问到黑名单地址，但是监控中始终没有命中黑名单的相关日志产生。

过程分析

建议客户在web页面日志设置---攻击防范日志内开启黑名单日志记录功能，并且配置为系统日志的输出方式，配置后测试发现增加和删除黑名单可以生成黑名单日志，但是命中黑名单进行阻断时仍然不会产生日志。



拿实验室版本为R9153P2412的M9006和R9345P2416的F1030测试，只要完成黑名单配置并开启黑名单全局使能，并且配置为输出系统日志，命中黑名单都是可以在web页面产生命中日志的，但是logbuffer里没有，判断黑名单日志是不会产生到log中，所以客户现场M9K的安全策略日志虽然较多，但因为web页面的黑名单日志不从logbuffer内读取，并不会影响黑名单日志的产生

解决方法

后续经产品线确认，D032版本防火墙不支持在web页面显示黑名单阻断日志，需要升级到D045之后版本，建议现场将M9006升级至当前官网最新的R9153P3003版本。