

知 M9000系列防火墙web页面无法产生黑名单日志经验案例

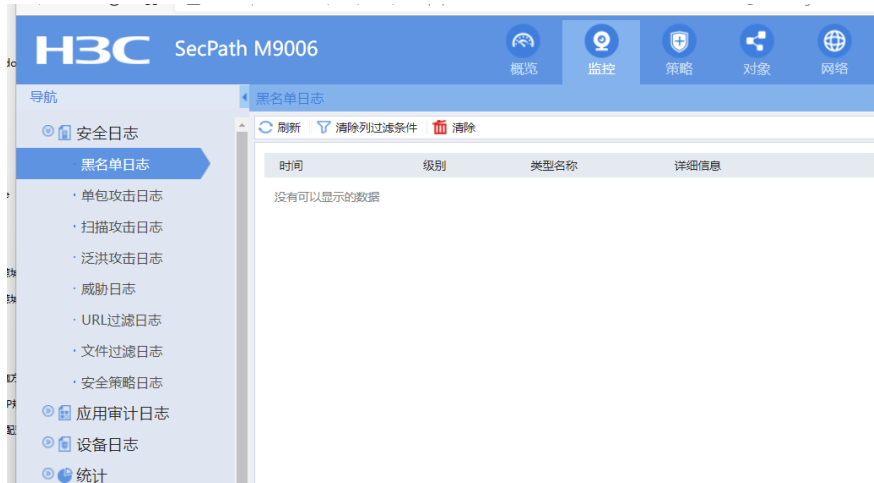
WEB管理 Syslog日志 葛松炜 2022-01-28 发表

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。

The screenshot shows the 'Attack Prevention Log' configuration page. On the left is a navigation menu with 'Attack Prevention Log' selected. The main area has two sections: 'Log Type' and 'Blacklist Log'.

Log Type: Radio buttons for 'System Log' (selected) and 'Fast Log'. A red warning message states: '开启系统日志可能会对设备性能产生影响，建议开启快速日志。' (Enabling system logs may affect device performance, it is recommended to enable fast logs.) Below are two checked checkboxes: 'Single packet attack prevention log aggregation output' and 'Enable blacklist log function'. An 'Apply' button is present.

Blacklist Log: Three input fields with ranges: 'Log buffer zone limit' (1024, range 0-1024), 'Log file storage limit' (1, range 1-10 MB), and 'Log file usage warning threshold' (80, range 0-100%). An 'Apply' button is at the bottom.

Log List: A table showing log entries with columns for time, level, type, and details.

时间	级别	类型名称	详细信息
122-01-21 16:31:23	notification	Delete IPv4 blacklist	SrcIPAddr(1003)=11.25.23.44; SndDSLiteTunnelPeer(1041)=; RcvVPNInstance(1042)=; Reason(1056)=Configuration.
122-01-21 16:30:48	notification	Add IPv4 blacklist	SrcIPAddr(1003)=11.25.23.44; SndDSLiteTunnelPeer(1041)=; RcvVPNInstance(1042)=; TTL(1055)=; Reason(1056)=Configura

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。

