

知 V7 IPS设备的安全日志模块存储路径及web显示问题

Syslog日志 刘宏宇 2019-10-29 发表

问题描述

V7 IPS设备的安全日志模块存储路径及web显示问题

解决方法

安全日志模块中下列标红的几个日志随系统日志先存在logbuffer里，web上也能读取到，但是重启后logbuffer清空了，web上读取不到，执行logfile save命令后可以手动将日志文件缓冲区中的内容全部保存到日志文件。威胁日志（AV/IPS）等会存放在数据库内，重启后也无法在web看到。

	日志类别	存储目录	文件大小限制（达到限制后如何处理）	WEB显示（是否有条数限制）	是否可以自动保存，保存周期是否可以自定义	重启后是否可以查看之前的日志
安全日志	黑名单日志	随系统日志	随系统日志	无	随系统日志	随系统日志
	单包攻击日志	随系统日志	随系统日志	无	随系统日志	随系统日志
	扫描攻击日志	随系统日志	随系统日志	无	随系统日志	随系统日志
	泛洪攻击日志	随系统日志	随系统日志	无	随系统日志	随系统日志
	威胁日志（AV/IPS）	/	10000 每 context	数据库内数据全部返回	否	否
	URL过滤日志					
	文件过滤日志					
安全策略日志						