

# 知 防火墙如何删除威胁日志？

其他 Syslog日志 罗浩 2022-01-18 发表

## 问题描述

客户咨询如何删除防火墙上的威胁日志，在web界面上没有相关删除的选项



威胁日志列表

删除 导出Excel 清除过滤条件 日志聚合配置 前一天 后一天 查询结果: 2021-12-01 00:00:00-23:59:59有1532条日志

查询: (开始时间: 2021-12-01 00:00:00, 结束时间: 2021-12-15 18:43:48)

查看	时间	威胁类型	威胁ID	威胁名称	严重级别	源安全区域	目的安全区域	源IP地址	目的IP地址	应用	协议	内容安全策略
	2021-12-01 23:58:04	入侵防御	9206	WEB服务器...	低	Trust	Untrust	172.16.17.70	112.65.69.11	360通用	TCP	all-ips
	2021-12-01 23:56:52	入侵防御	19278	针对攻击中...	中	Trust	Untrust	172.16.12.92	114.114.11...	dns	UDP	all-ips
	2021-12-01 23:56:52	入侵防御	19278	针对攻击中...	中	Trust	Untrust	172.16.12.92	8.8.8.8	dns	UDP	all-ips
	2021-12-01 23:54:07	入侵防御	9206	WEB服务器...	低	Trust	Untrust	172.16.12.1...	112.65.69.11	360通用	TCP	all-ips
	2021-12-01 23:53:10	入侵防御	19278	针对攻击中...	中	Trust	Untrust	172.16.12.92	114.114.11...	dns	UDP	all-ips
	2021-12-01 23:53:10	入侵防御	19278	针对攻击中...	中	Trust	Untrust	172.16.12.92	8.8.8.8	dns	UDP	all-ips
	2021-12-01 23:51:43	入侵防御	25440	过时的验证...	低	Trust	Untrust	172.16.20.1...	111.206.20...	https	TCP	all-ips
	2021-12-01 23:47:08	入侵防御	25440	过时的验证...	低	Trust	Untrust	172.16.20.1...	180.97.104...	https	TCP	all-ips
	2021-12-01 23:41:42	入侵防御	25440	过时的验证...	低	Trust	Untrust	172.16.20.1...	111.206.20...	https	TCP	all-ips
	2021-12-01 23:41:26	入侵防御	19278	针对攻击中...	中	Trust	Untrust	172.16.12.92	8.8.8.8	dns	UDP	all-ips
	2021-12-01 23:41:26	入侵防御	19278	针对攻击中...	中	Trust	Untrust	172.16.12.92	114.114.11...	dns	UDP	all-ips
	2021-12-01 23:39:32	入侵防御	25440	过时的验证...	低	Trust	Untrust	172.16.20.1...	180.97.104...	https	TCP	all-ips
	2021-12-01 23:38:42	入侵防御	9206	WEB服务器...	低	Trust	Untrust	172.16.14.25	112.65.69.11	360通用	TCP	all-ips
	2021-12-01 23:38:33	入侵防御	19278	针对攻击中...	中	Trust	Untrust	172.16.12.92	114.114.11...	dns	UDP	all-ips

第 1 页, 共 62 页 每页显示条数 25 显示 1 - 25条, 共

#### 解决方法

如果威胁日志存到硬盘的话，那只能格式化硬盘（此操作十分危险，请谨慎操作）；没加硬盘的话，web界面威胁日志读取的是Ntop数据库存储的位置，设备重启后就看不到相关日志。

