TP-LINK®

TP-LINK安全审计
系统入门指南

声明

目录

目录 II

第 1 章 系统简介 1

第 2 章 系统安装 3

第 3 章 设备对接 7

3.1 路由器对接步骤（TL-ER3220G 为例） 7

3.1.1 行为审计模块设置记录到系统日志 7

3.1.2 行为日志发送到服务器 9

3.1.3 系统日志发送至服务器 9

3.2 防火墙对接步骤（TL-FW6600 为例） 10

3.2.1 设置安全配置文件 10

3.2.2 设置安全策略记录日志 11

3.2.3 系统日志发送至服务器 11

3.2.4 设置审计配置文件 12

3.2.5 设置审计策略 13

3.2.6 审计日志发送至服务器 14

3.3 服务器所接入的 TP-LINK 设备端 14

第 4 章 系统功能介绍 15

4.1 首页 15

4.2 日志 17

4.3 统计报表 18

4.3.1 日志统计 18

4.3.2 流量统计 19

4.3.3 策略命中统计 20

第 5 章 系统 21

5.1 数据库管理与备份 21

5.2 日志屏蔽规则 22

5.3 设备鉴权 22

第 6 章 FAQ 24

第1章 系统简介

TP-LINK 安全审计系统是运行在 Windows 服务器系统上的集成软件，可用于 TP-LINK 商用路由器和防火墙设备的日志对接，以及对日志信息进行统计分析和报表输出。TP-LINK 安全审计系统集日志审计、统计报表、系统管理于一体，通过安全审计，实时监控网络安全运行状态，解决网络安全问题，做到事前预警，未雨绸缪；事中控制，运筹帷幄；事后审计，及时改进。

软件特性：

1. 支持防火墙审计日志、路由审计日志、流量日志等多种日志管理方式，能够总览网络设备的安全状况、运行状况；

2. 支持日志的详细记录，如：记录每一次网络连接消耗的上行/下行流量、记录管理员登录并操作的详细内容、记录网络内策略命中情况、显示连接到服务器的设备连接和断开的历史记录；

3. 支持日志统计，展示指定时间内各类的日志数量；流量统计，记录设备流量与源 IP 流量的 Top5 排行；策略命中统计，记录策略命中数量的 Top5 排行；

4. 支持自动/手动备份日志数据，按需选择备份保存时间、周期和地址，也可进行数据库导入与清空，满足不同应用场景和用户的数据管理需求；

5. 支持日志屏蔽规则，支持按不同的规则屏蔽日志如：日志级别、类型、关键字等；

6. 支持设备鉴权管理，开启后只接受白名单设备上的日志；

7. 支持用户安全证书，根据用户获得的证书，匹配相应的系统功能；

8. 支持统一权限管理，按需添加管理人员和操作人员；

9. 适配防火墙，增加威胁日志、URL 日志、内容日志、邮件过滤日志信息及相应的统计信息。

第2章 系统安装

安装之前，请确认以下几点：

1) 已从官网下载 TP-LINK 安全审计系统。

2) 管理主机已正确连接至本地网络中。

3) 管理主机已正确安装有线网卡及该网卡的驱动程序。

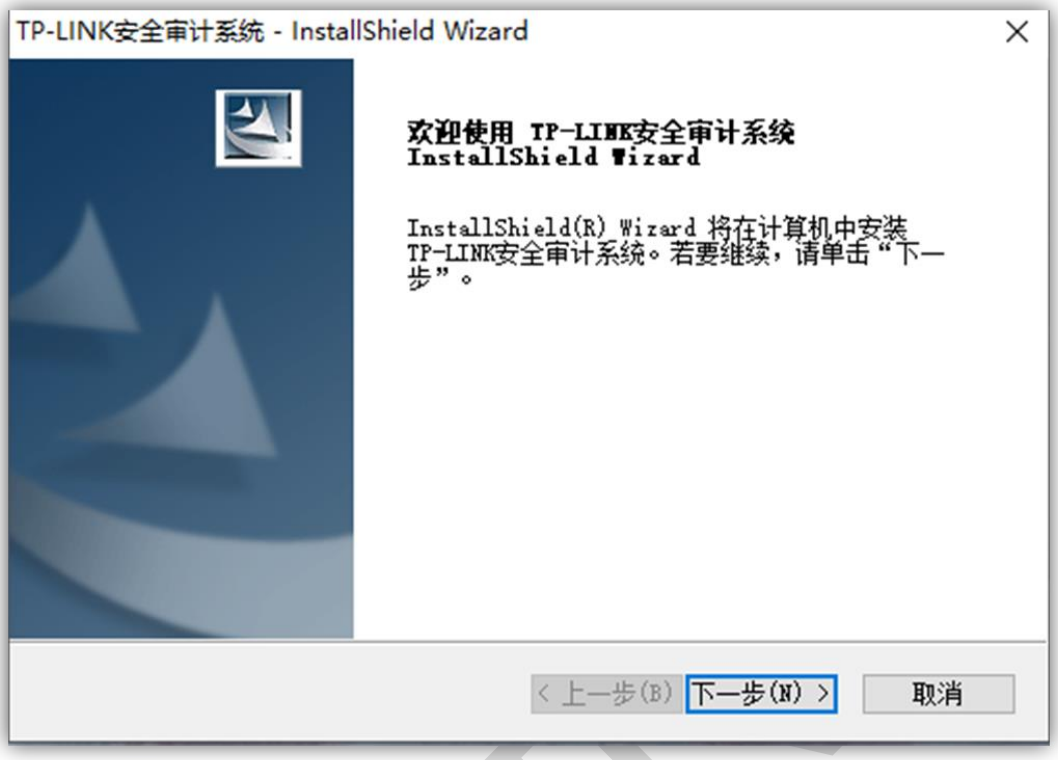
4) 管理主机建议硬件配置 i3 处理器以上，内存 16GB 或以上，操作系统应为 Windows7/8/10(64bit)。

5) 为保证更好地体验Web页面显示效果，请将显示器的分辨率调整到1024×768或以上。

安装方法如下：

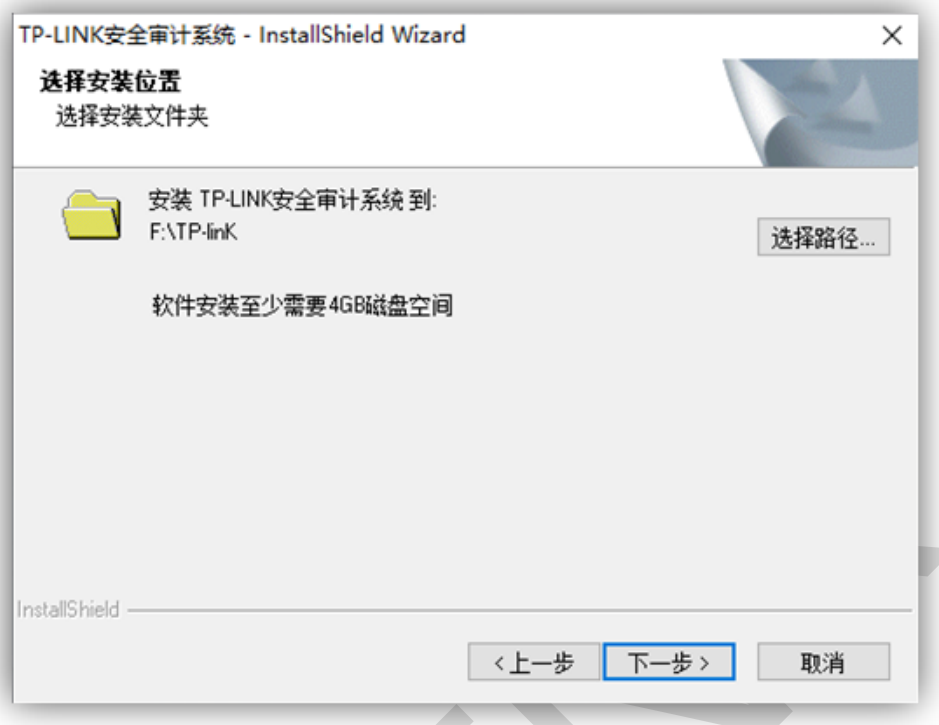
1) 双击 TP-LINK 安全审计系统安装软件。

2) 根据安装向导进行安装：



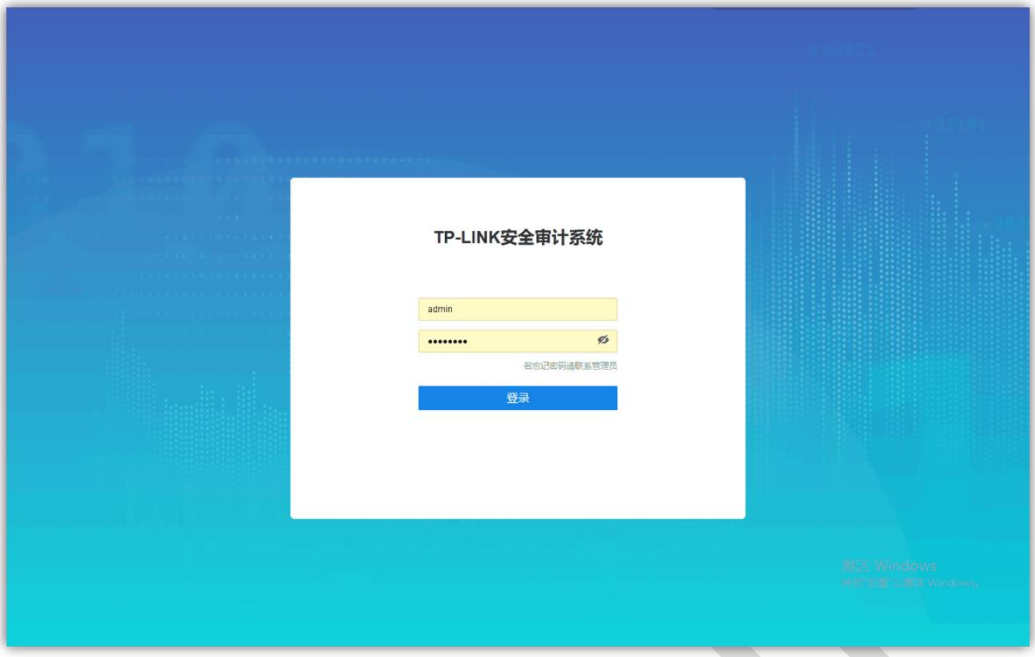
注意：

- 软件安装至少需要 4GB 磁盘空间，请保证磁盘空间充足；
- 安装路径不应包含,./'":;!@#$%等特殊字符，否则程序可能无法启动；
- 建议不要安装在 C 盘,随着日志数量的增多,软件所占体积会非常大；



3) 安装完成后，桌面会出现 TP-LINK 安全审计系统的快捷方式图标，双击该图标，开启安全审计系统。

系统默认账号密码为 admin/123456，通过此账号密码可以登录安全审计系统。

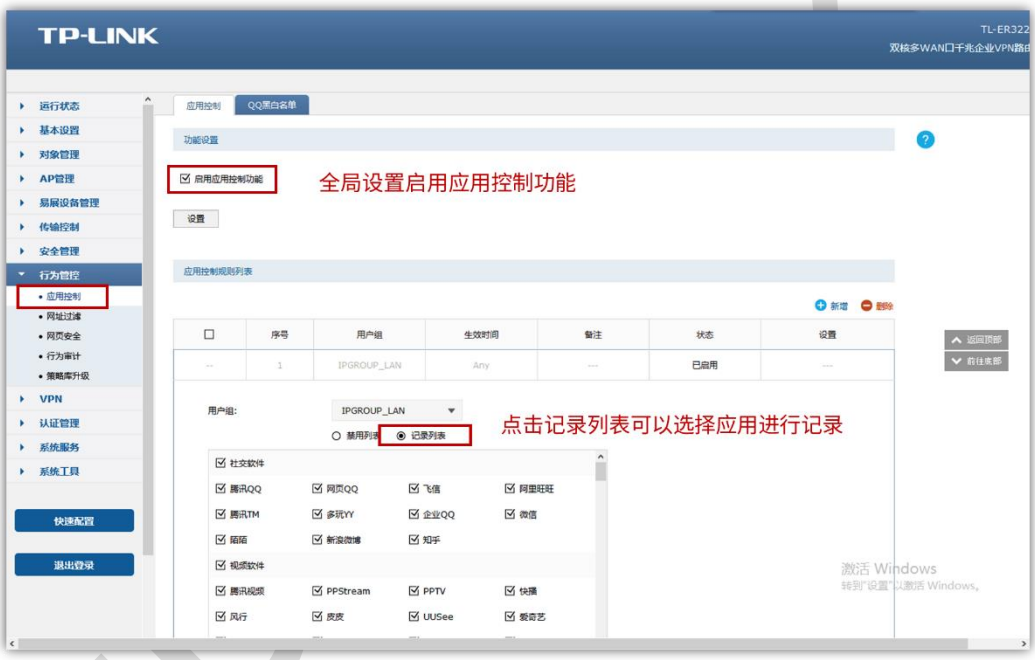


第3章 设备对接

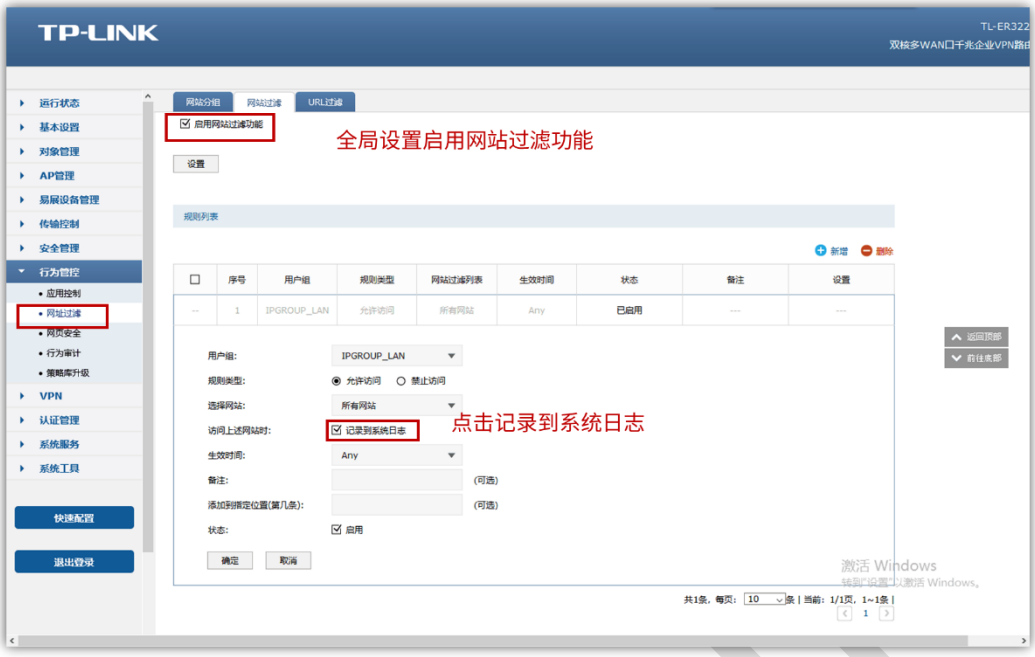
3.1 路由器对接步骤（TL-ER3220G 为例）

3.1.1 行为审计模块设置记录到系统日志

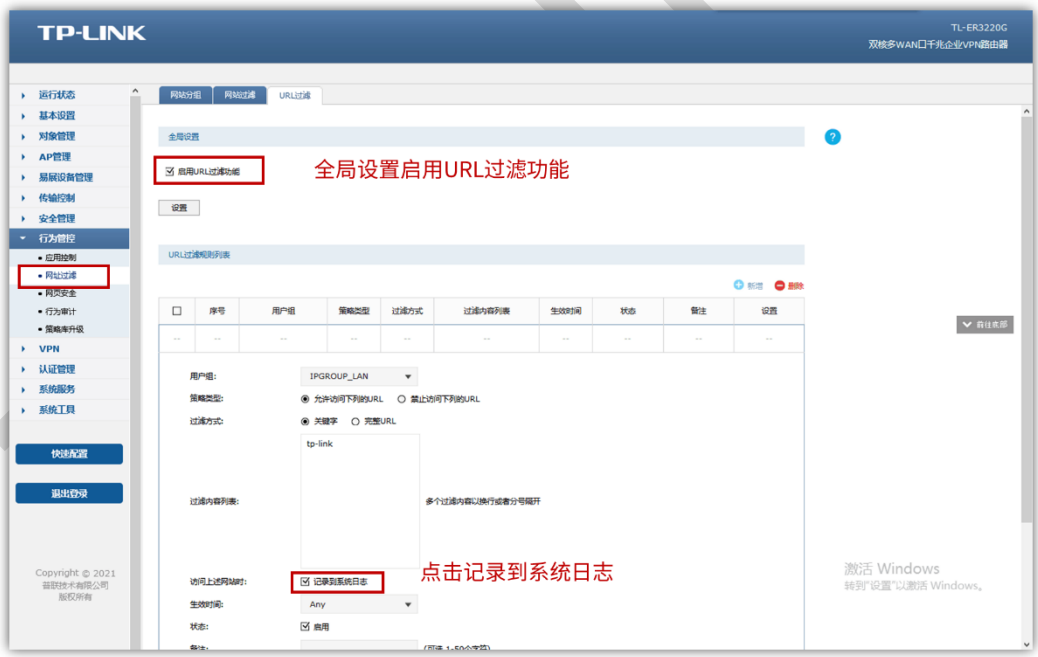
应用控制：



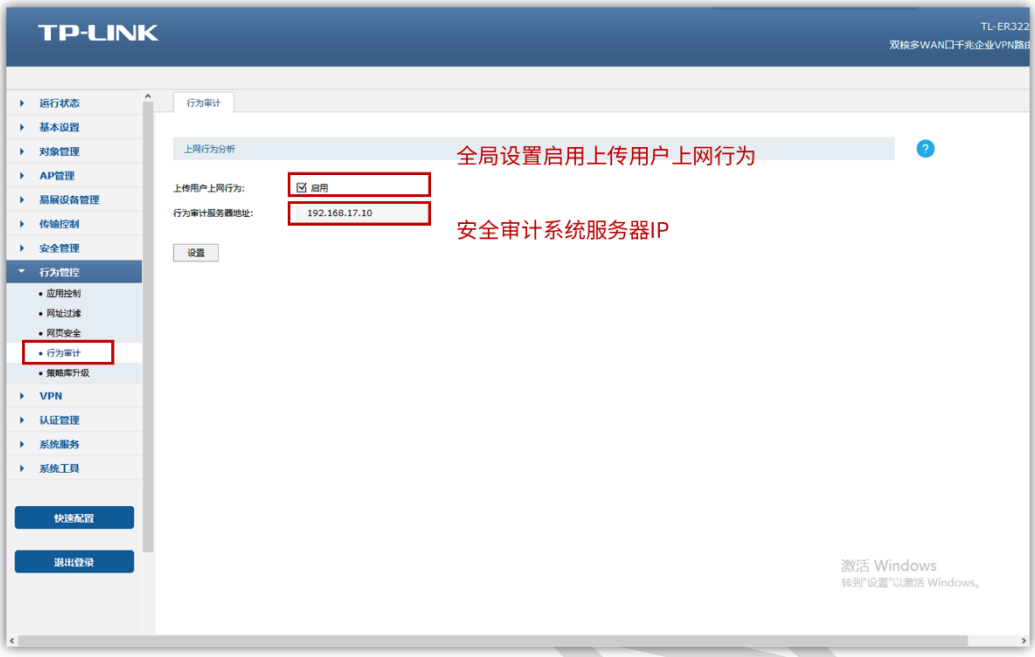
网址过滤：


TP-LINK
全局设置启用网站过滤功能
点击记录到系统日志

URL 过滤：

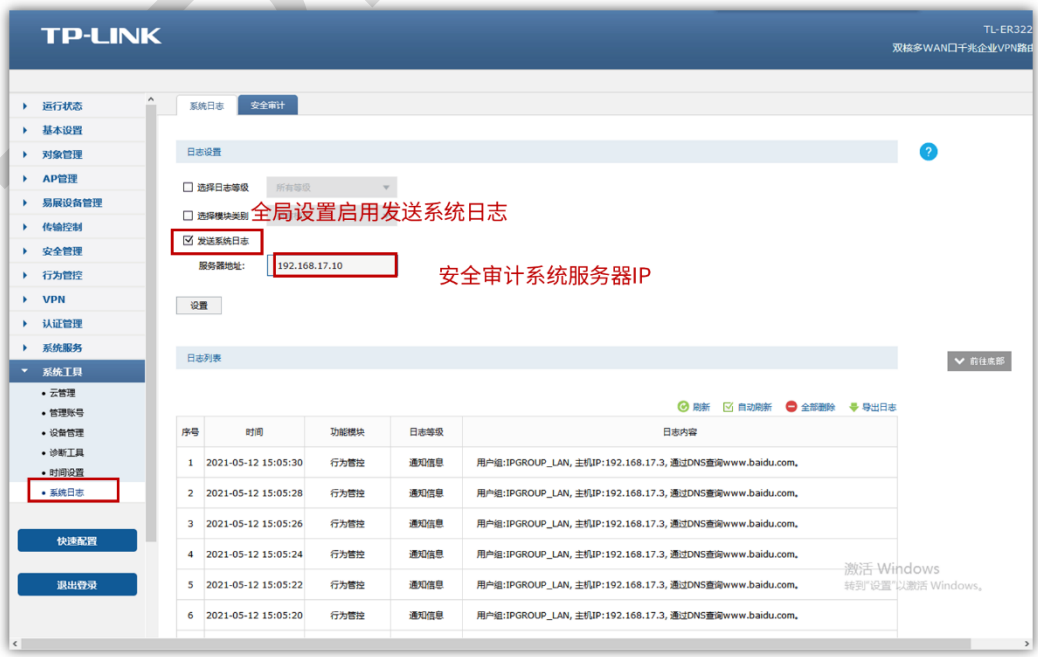

TP-LINK
全局设置启用URL过滤功能
点击记录到系统日志

3.1.2 行为日志发送到服务器



注意：服务器地址，若局域网部署，直接填写服务器 IP，若公网部署请填写设备 WAN 口 IP。

3.1.3 系统日志发送至服务器



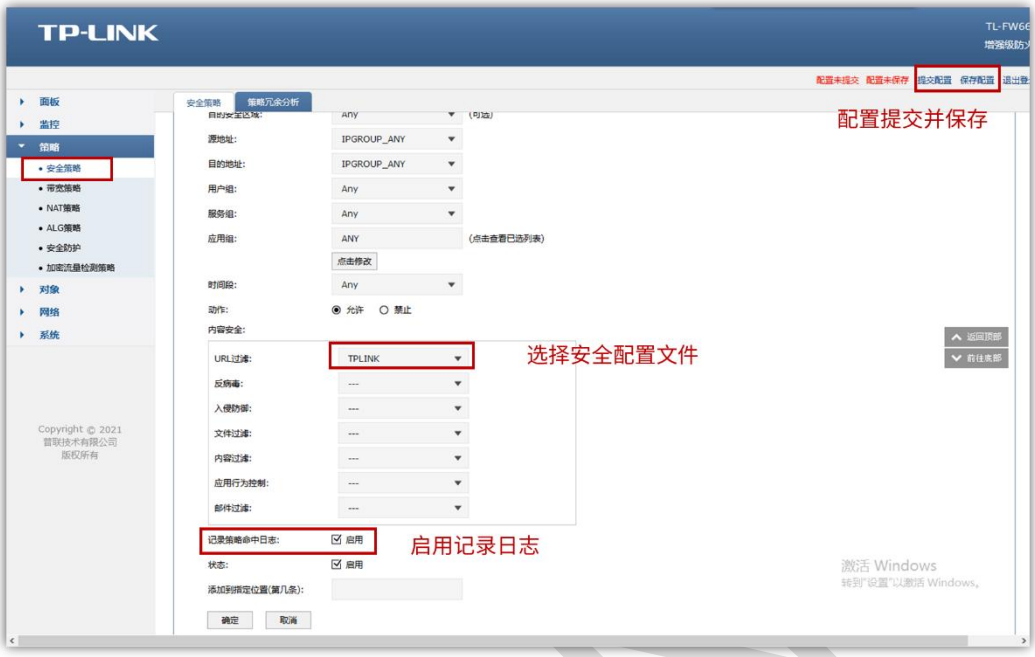
注意：服务器地址，若局域网部署，直接填写服务器 IP，若公网部署请填写设备 WAN 口 IP。

3.2 防火墙对接步骤（TL-FW6600 为例）

3.2.1 设置安全配置文件

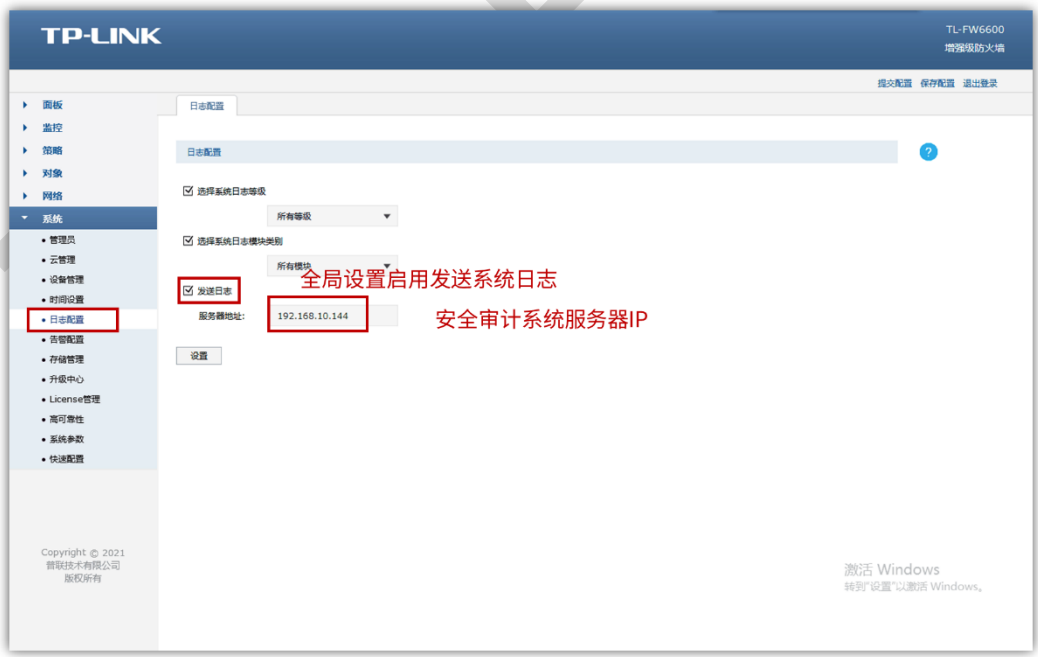
在“对象>安全配置文件”中创建安全配置文件，以 URL 过滤为例：

3.2.2 设置安全策略记录日志



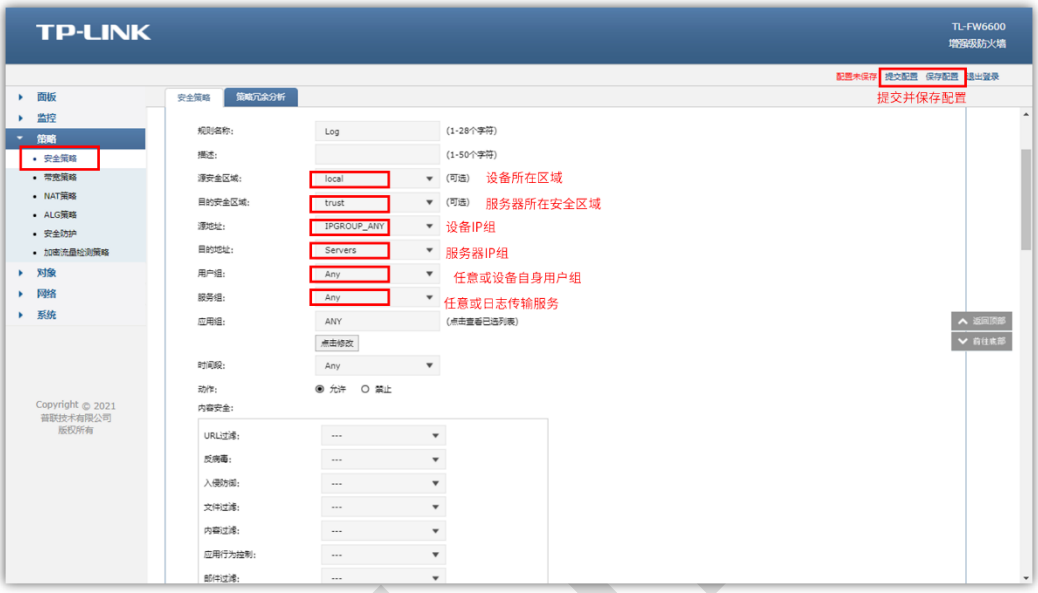
3.2.3 系统日志发送至服务器

先在日志配置中勾选发送日志并填写服务器 IP 地址：



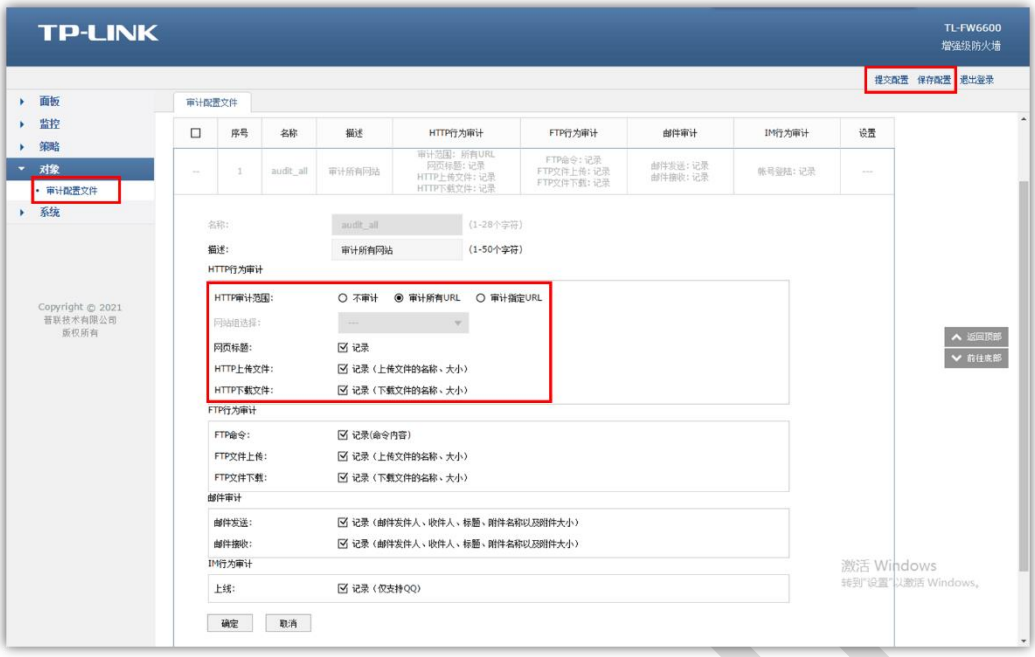
注意：服务器地址，若局域网部署，直接填写服务器 IP，若公网部署请填写设备 WAN 口 IP。

然后在安全策略中，添加一条放行设备向服务器传输日志的安全策略：

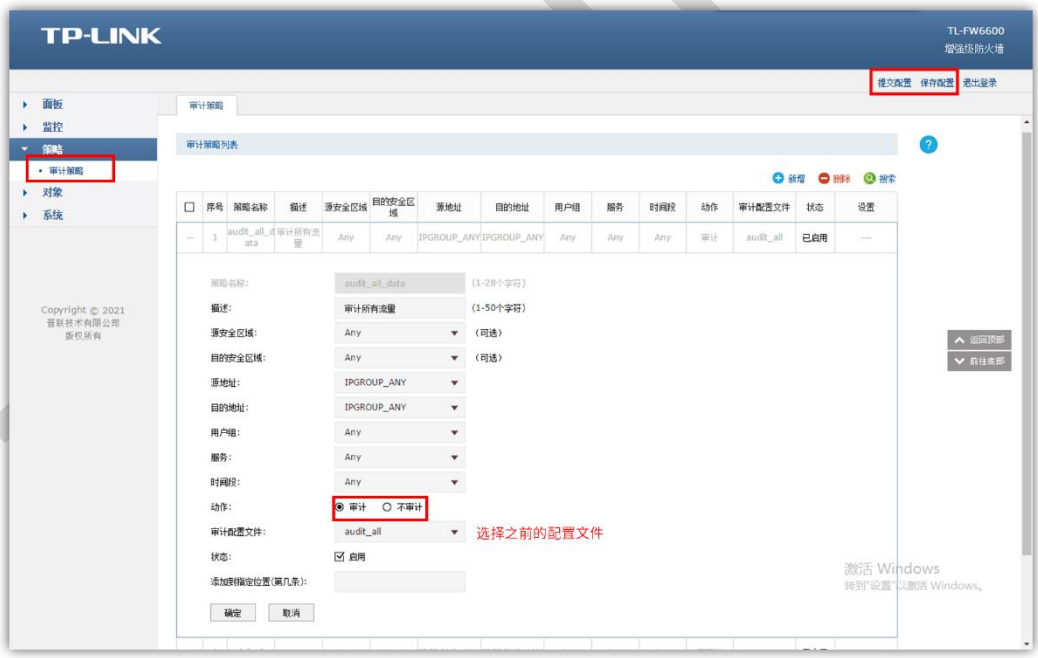


3.2.4 设置审计配置文件

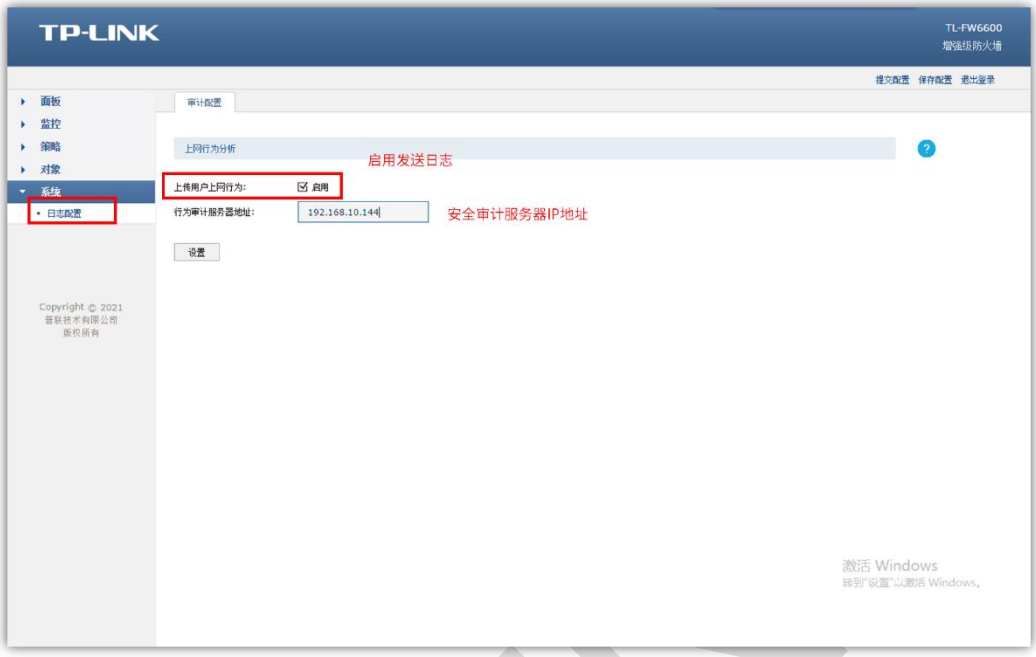
创建审计管理员，并以审计管理员身份登录防火墙，打开“对象”——“审计配置文件”，点击“新增”，根据需求设置审计行为：


TP-LINK
TL-FW6600
增强级防火墙
提交配置 保存配置 退出登录
面板
监控
策略
对象
审计配置文件
系统
审计配置文件
序号 名称 描述 HTTP行为审计 FTP行为审计 邮件审计 IM行为审计 设置
名称: audit_all (1-28个字符)
描述: 审计所有网站 (1-50个字符)
HTTP行为审计
HTTP审计范围: 不审计 审计所有URL 审计指定URL
网站组选择:
网页标题: 记录
HTTP上传文件: 记录（上传文件的名称、大小）
HTTP下载文件: 记录（下载文件的名称、大小）
FTP行为审计
FTP命令: 记录(命令内容)
FTP文件上传: 记录（上传文件的名称、大小）
FTP文件下载: 记录（下载文件的名称、大小）
邮件审计
邮件发送: 记录（邮件发件人、收件人、标题、附件名称以及附件大小）
邮件接收: 记录（邮件发件人、收件人、标题、附件名称以及附件大小）
IM行为审计
上线: 记录（仅支持QQ）
确定 取消
返回顶部
前往底部
Copyright © 2021
普联技术有限公司
版权所有
激活 Windows

3.2.5 设置审计策略


TP-LINK
TL-FW6600
增强级防火墙
提交配置 保存配置 退出登录
面板
监控
策略
审计策略
对象
系统
审计策略列表
新增 删除 搜索
序号 策略名称 描述 源安全区域 目的安全区域 源地址 目的地址 用户组 服务 时间段 动作 审计配置文件 状态 设置
策略名称: audit_all_data (1-28个字符)
描述: 审计所有流量 (1-50个字符)
源安全区域: Any （可选）
目的安全区域: Any （可选）
源地址: IPGROUP_ANY
目的地址: IPGROUP_ANY
用户组: Any
服务: Any
时间段: Any
动作: 审计 不审计
审计配置文件: audit_all
选择之前的配置文件
状态: 启用
添加到指定位置(第几条):
确定 取消
返回顶部
前往底部
Copyright © 2021
普联技术有限公司
版权所有
激活 Windows

3.2.6 审计日志发送至服务器



注意：

1、服务器地址，若局域网部署，直接填写服务器 IP，若公网部署请填写设备 WAN 口 IP。

2、在安全策略中，添加一条放行设备向服务器传输日志的安全策略（与 3.2.3 相同）

3.3 服务器所接入的 TP-LINK 设备端

局域网部署：无需其他设置

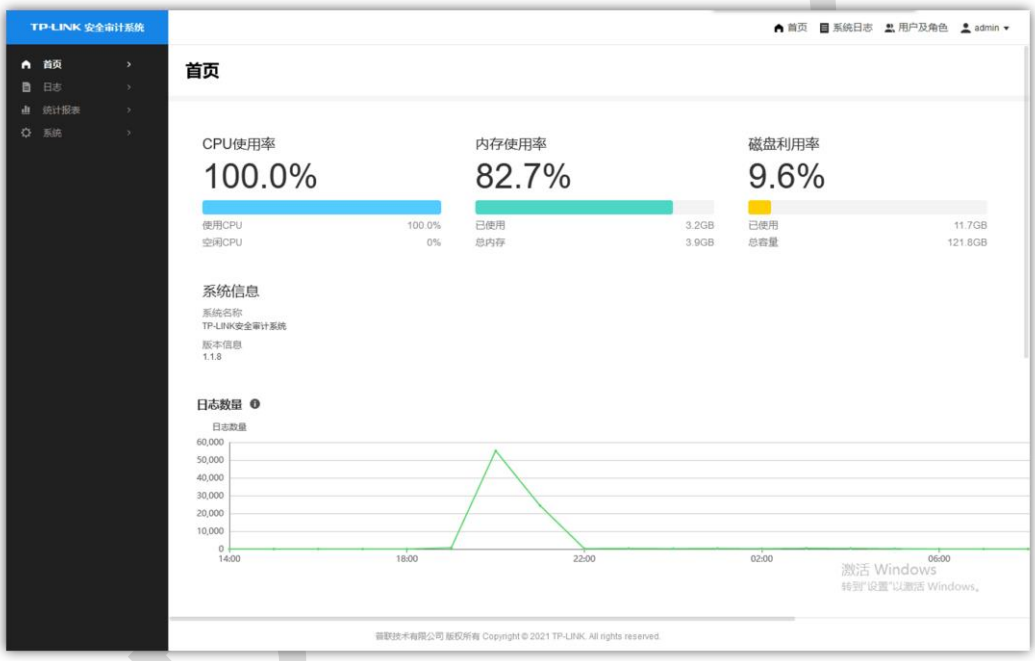
公网部署：在服务器所接的设备上设置端口映射，映射安全审计系统审计日志端口 514 和 WEB 的端口 8081、注意虚拟服务器映射时内外网端口要设置一致。

序号	规则名称	生效接口	外部端口	内部端口	内部服务器IP	服务协议	状态	设置
1	shenji	WAN1	514	514	192.168.17.10	ALL	已启用	
2	web	WAN1	8081	8081	192.168.17.10	ALL	已启用	

第4章 系统功能介绍

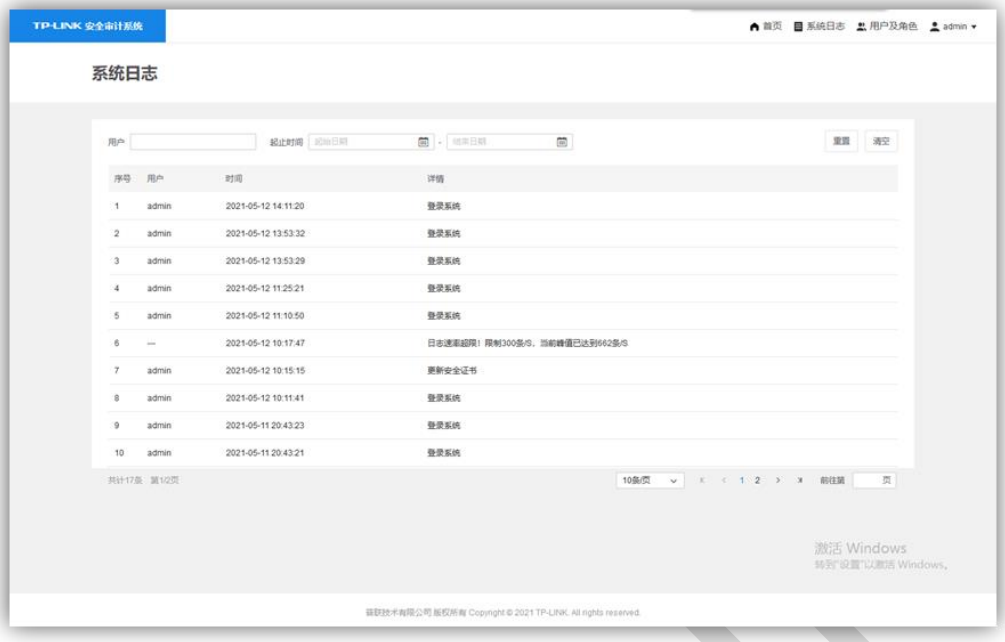
4.1 首页

登录成功后即可进入安全审计系统首页。此处可概览服务器的当前状态。包括 CPU 使用率、内存使用率、磁盘利用率、系统信息、日志数量和服务器总流量的变化情况。

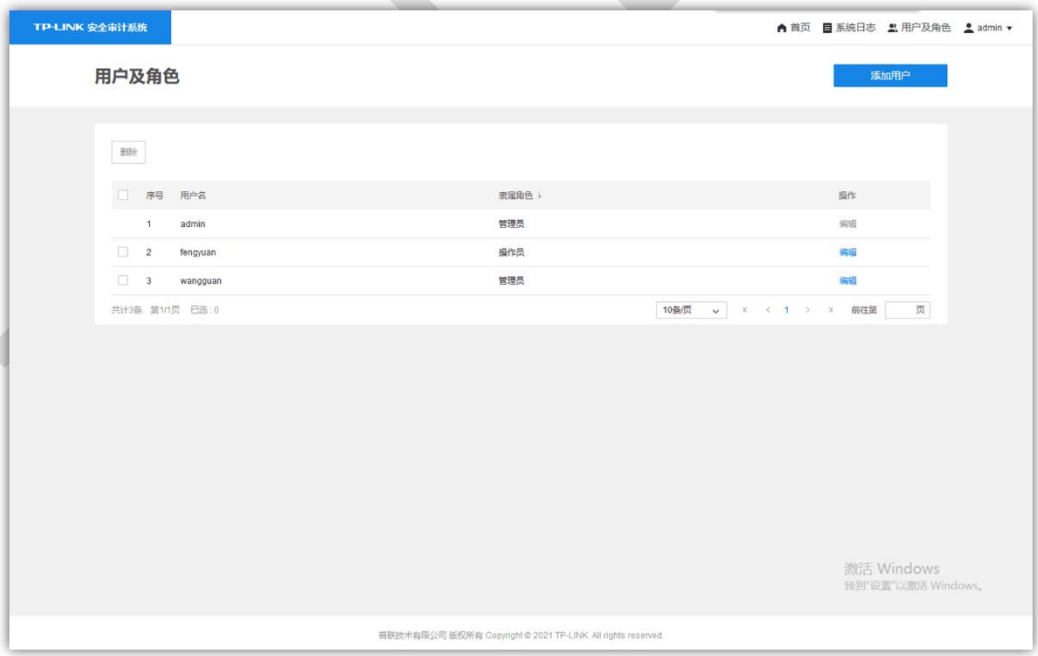


页面左侧列出了安全审计系统所有的管理类目。页面右上角有四个快捷按钮：

- 首页：在任何页面点击此处回到首页。
- 系统日志：点击此处查看安全审计系统日志，包括用户登录信息、更改参数历史等。



- 用户及角色：点击此处可添加或删除安全审计系统的用户，此操作仅能由管理员账户进行。管理员账户可添加管理员或操作员账户。



- 您的用户名：点击此处可修改您的登录密码或退出登录。

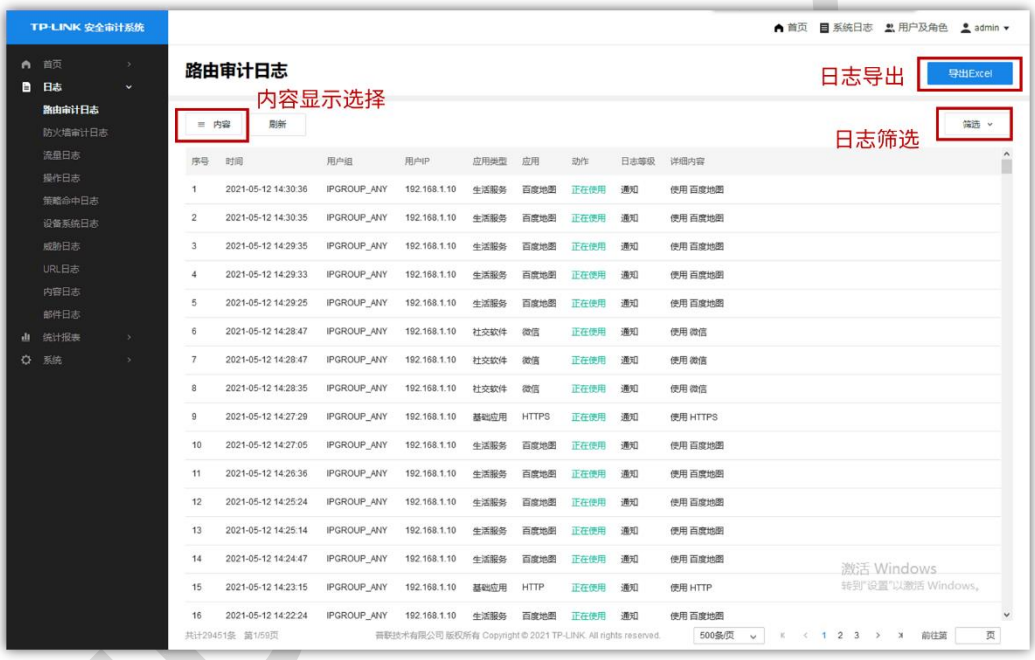
4.2 日志

TP-LINK 安全审计系统一共包含十种条目类别，分别为路由器审计日志、防火墙审计日志、流量日志、操作日志、策略命中日志、设备系统日志、威胁日志、URL 日志、内容日志、邮件日志。其中：

- 路由审计日志由 TP-LINK 路由器设备产生，记录了当前路由器网络内用户的上网行为历史，可以查看某时某用户使用了何种应用连接网络及路由器对其采取的动作。
- 防火墙审计日志由 TP-LINK 防火墙设备产生，记录了经过防火墙的网络请求。
- 流量日志由 TP-LINK 防火墙设备产生，记录了所有通过防火墙的上行/下行流量信息。
- 操作日志由 TP-LINK 防火墙设备产生，记录了管理员登录防火墙进行操作的历史详情，如 修改策略、添加策略等。
- 策略命中日志由 TP-LINK 防火墙设备产生，记录了流量命中策略的历史记录。
- 设备系统日志由 TP-LINK 路由器设备和防火墙设备产生，记录了系统运行详情历史。
- 威胁日志由 TP-LINK 防火墙设备产生，记录了上网流量中被安全策略定义的威胁类型、威胁名称以及上网设备信息。

- URL 日志由 TP-LINK 路由器设备和防火墙设备产生，记录了上网流量中包含对应 URL 过滤内容的条目信息。
- 内容日志由 TP-LINK 防火墙设备产生记录了文件上传下载的信息。
- 邮件日志由 TP-LINK 防火墙，记录了设备收发邮件的历史信息。

对于表中条目，可以进行筛选、导出、选择显示内容等操作。

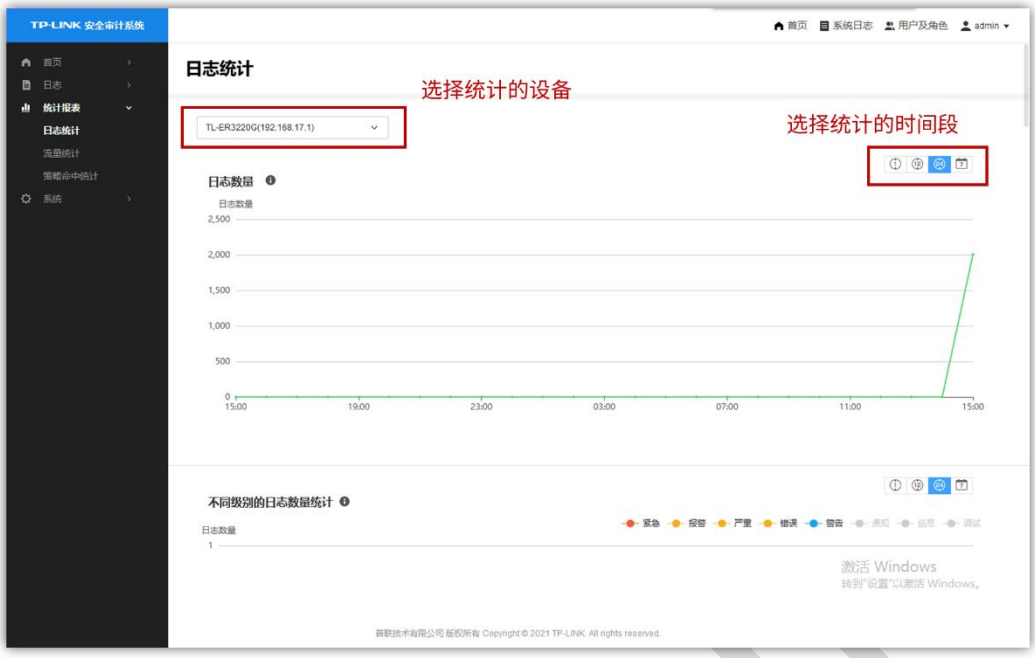


4.3 统计报表

注意：本部分涉及各种数据图表。在以下所有统计图标中，图中每一个点的取值为上一个时间点到该时间点之间的累加值；最后一个点为上一个时间点到当前时间之间的累加值。

4.3.1 日志统计

日志统计页面包含日志的统计信息。在左上角的下拉框，可选择需要查看日志统计的路由器。点击每个统计图右上角的图标，可在 1 小时、12 小时、24 小时和 7 天内切换查看时间段。



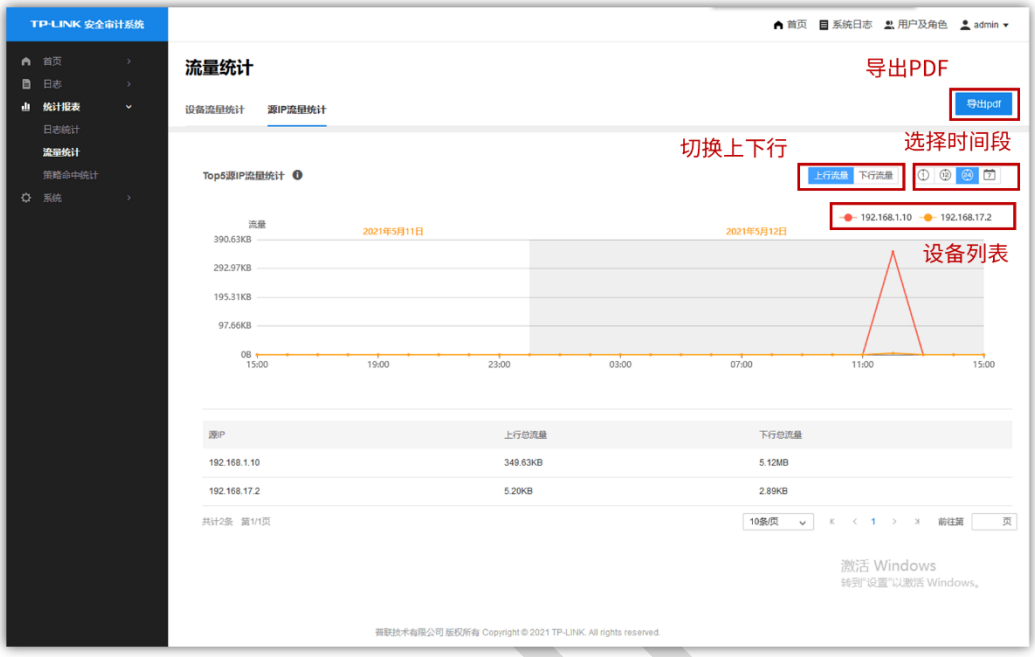
4.3.2 流量统计

设备流量统计

设备流量统计展示了产生流量前 5 名的各设备的流量统计数据，点击图表右上角的按钮，可切换查看上行流量和下行流量，以及不同的统计时间段。点击页面右上角的导出 pdf 按钮，可将当前统计图表导出为 pdf 文件。

源 IP 流量统计

设备流量统计展示了产生流量前 5 名的源 IP 的流量统计数据，点击图表右上角的按钮，可切换查看上行流量和下行流量，以及不同的统计时间段。点击页面右上角的导出 pdf 按钮，可将当前统计图表导出为 pdf 文件。



4.3.3 策略命中统计

策略命中统计展示了命中数量前 5 名的策略的命中数量统计。 点击左上角的下拉框，可选择需要查看日志统计的路由器。点击图表右上角的按钮，可切换查看不同的统计时间段。

第5章 系统

5.1 数据库管理与备份

本安全审计系统记录了大量日志和数据统计，可在此处设置数据库备份以保护您的数据。可以实现自动备份、手动备份、恢复备份等操作。

- 备份保存时间：可设置数据备份文件保存的时长，以及到期时是否清空备份文件。
- 自动备份周期：可设置每隔多长时间自动进行备份，以及每次完成备份后是否清空现有数据库。
- 自动备份地址：设置自动备份保存的路径。 设置完成后请点击保存。

注意： 当某种日志的数量超过 3000 万条以后，系统会自动备份最老的 100 万条数据。

5.2 日志屏蔽规则

此处可设置系统自动屏蔽并丢弃某种类型的日志记录。可从日志严重等级、日志类型和关键 词三个方面定义需要屏蔽的日志特征。

注意： 日志等级、日志类型、关键词屏蔽互不影响，满足任意一项条件将进行屏蔽。

5.3 设备鉴权

此处可将网络中的设备添加至白名单，只有此白名单内的设备产生的日志才会被记录。 点击添加按钮，即可设置需要添加入白名单的设备名称及其 IP 地址。 对于已在白名单中的设备，若需删除，请勾选设备前方的复选框，点击删除按钮即可。


TP-LINK 安全审计系统
首页
系统日志
用户及角色
admin
首页
日志
统计报表
日志统计
流量统计
策略命中统计
系统
数据库管理与备份
日志屏蔽规则
设备鉴权
安全证书
设备鉴权
设备鉴权
开启
开启功能
开启后只接受白名单设备上的日志
白名单设备列表
添加设备
添加
删除
序号
设备名称
IP地址
操作
1
TI-ER3220G
192.168.17.1
编辑
共计1条 第1/1页 已选：0
10条/页
前往第
激活 Windows
转到"设置"以激活 Windows。
普联技术有限公司 版权所有 Copyright © 2021 TP-LINK All rights reserved.

第6章 FAQ

1、安全审计系统是否收费?

目前安全审计系统可以免费安装使用，无需缴纳任何费用。

2、安全审计系统可以接受多少条日志呢?

最大可以达到 200 条/s。