

TP-LINK安全审计 系统入门指南

声明

Copyright © 2021 普联技术有限公司

版权所有,保留所有权利

未经普联技术有限公司明确书面许可,任何单位或个人不得擅自仿制、复制、誊抄或转译本手册部分或全部内容,且不得以营利为目的进行任何方式(电子、影印、录制等)的传播。

TP-LINK[®]为普联技术有限公司注册商标。本手册提及的所有商标,由各自所有人拥有。本手册所提到的产品规格和资讯仅供参考,如有内容更新,恕不另行通知。除非有特殊约定,本手册仅作为使用指导,所作陈述均不构成任何形式的担保。

目录

目录		I	I
第1章	系统	简介 1	1
第2章	系统	安装	3
第3章	设备	对接	7
3.1	路由智	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	防火均	啬对接步骤(TL-FW6600 为例))
	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12	1
	3.2.3	系统日志发送至服务器	1
	3.2.4	设置审计配置文件12	2
	3.2.5	设置审计策略13	3
	3.2.6	审计日志发送至服务器 14	1
3.3	服务	器所接入的 TP-LINK 设备端14	1
第4章	系统	功能介绍1	5

4.1	首页.		
4.2	日志.		
4.3	统计	服表	
	4.3.1	日志统计	
	4.3.2	流量统计	
	4.3.3	策略命中统计	20
第5章	系统.		
5.1	数据	车管理与备份.	
5.2	日志	屏蔽规则	
5.3	设备	鉴权	
5.4	安全ì	证书	
第6章	FAQ.		

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:

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;

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;

 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;

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;

1

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。

- TP-LINK 安全审计系统

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;

TP-LINK安全 选择安装 选择安装	全审计系统 - InstallShield Wizard 位置 这件夹			×
	安装 TP-LINK安全审计系统 到: F:\TP-linK			选择路径
	软件安装至少需要4GB磁盘空间			
InstallShield -				
		〈上一步	下一步>	取消

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。

TP-LINK安全审计系统 edmin ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	
	Mis Windows In call - day Windows

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:

TP-LINI	ĸ								TL-E 双核多WAN口千兆企业V
运行状态	 应用控制 	QQ黑白名单							
基本设置	功能设置								0
对象管理		_							
AP管理	☑ 启用应用控制	功能	全局设置	置启用应用	用控制功 能				
易展设备管理									
传输控制	设置								
安全管理									
行为管控	应用控制规则列:	ξ.							
 应用控制 								🕒 新道 😑	把 到5分
 网址过滤 网页安全 		序号	用户纲	41	故时间	留注	状态	设置	
 行为审计 	_								~ 城田田
• 策略库升级	~	1	IPGROUP_L	AN)			已启用		- 1012.00
VPN	Edia.		IDGROUD						
认证管理	70/ 38-				点击记	录列表词	可以选择应用证	进行记录	
系统服务			0 100-03-020	 KOR918 		0			
系统工具	☑ 社交	软件							
	図 講当	QQ	☑ 网页QQ	☑ 飞信	☑ 阿里旺旺				
快速配置	図調用	TM	☑ 多玩YY	区 企业QQ	☑ 微信				
		ī -	☑ 新浪微博	区知乎					
退出登录	☑ 老翁	软件						激活	Windows
	[1] 「「「「」」	视频	PPStream		☑ 快播			转到"话	建"以謝舌 Windows。
			N BB	EX III Coo	N minut				

网址过滤:

TP-LINK									30	TL-ER322 核多WAN口千兆企业VPN路自
 ▶ 运行状态 ▲ 基本设置 ▶ 对象管理 ▶ AP管理 ▶ 易展设音管理 	网络分组	國就过達功	は法述法律 URL社 部	金局设置	置启用网站	占过滤功	能			
 ▶ 传输控制 ▶ 安全管理 	规则列表	ŧ							🔓 新増 🕒 劃除	
▼ 行为管控		序号	用户组	規则类型	网站过滤列表	生效时间	状态	香注	设置	
 ·		1	IPGROUP_LAN	允许访问	所有网站	Any	已启用			
 ・ 双页安全 ・ 行为市计 ・ 須販売升収 > VPN > 以正管理 > 系统編系 > 系统編系 > 系统工具 使決乱管 保出管理 	用 规 选 访 生 聲 漆 状	戶組: 則與型: 译阿站: 问上述网站 就可间: 注: 加到指定(志: 确定	2章(第几条): 取满	IPGROUP_LAN ● 先许访问 ● 所有网站 ○ 记录到系统日本 Any ○ 点用	 <	记录到系	统日志		激活 Win ^{转到了说雷力}	▲ 認識證 ▼ 作住意题 dows 認知 Windows,
								共1条,每页: 10 🗸	条 当前:1/1页,1~1条 < 1 >	
¢										>

URL 过滤:

ТР	LINK	(TL-EI 双核多WAN口千兆企业VP
运行状态	^	网站	分组网站过滤	URL过滤									
基本设置													
対象管理		全局说	題									?	
AP管理		V ei	FILIDI SHIMTLAN	1.	全局设	罟 户 E	ELIDI 计语T	力能					
易展设备	管理	<u> </u>	HO KLIZINAVING		王问汉	旦/口/	TORLE	27.86					
传输控制		设置											
 安全管理 	_												
 ① 万官控 ○ 应用物制 	_	URLE	拉规则列表										
 网址过滤 													
 	_												
 行为审计 			序号	用户组	策略类型	过滹方式	过滤内容列表	生效时间	状态	暫注	设置		
 策略库升 	Ω												~
VPN													
认证管理			用户组:	IP	GROUP_LAN	*							
5.563655 			策略类型:	ۍ ک	许访问下列的UR	L O 🏦 🗄	方间下列的URL						
》 派班上具			过滤方式:	ۋ ھ	● 关键字 ○ 完整URL								
快速而	a			tp-	ink								
退出到	渌		过诸内容列表:			1	多个过滤内容以换行或者分号隔	π					
Copyrigh	© 2021		讷问 H述网站st-	হ হ	最到系统日志	1 5	点击记录到	系统日洋	志			訪	数活 Windows
#UEI技术 版权	月秋公可 所有		4100010D-			.							同 版直 以旅店 Windows
			10.+.		7 m	•							
			4081	1 s	用								

3.1.2 行为日志发送到服务器

	TP-LINK	(TL-ER322 双梭参WAN口千兆企业VPN路由
•	运行状态	行为审计			
•	基本设置				
•	对象管理	上网行为分析		全局设置启用上传用户上网行为	(2)
•	AP管理				
•	易展设备管理	上传用户上购行为:	⊠ 眉用		
+	传输控制	行为审计服务器地址:	192.168.17.10	安全宙计系统服务器IP	
•	安全管理	设置		文王中 开苏3660386	
•	行为管控				
	 应用控制 				
	 网址过滤 				
Ŀг	 • 两贝安主 • 行为审计 				
12	• 策略库升级				
•	VPN				
•	认证管理				
•	系统服务				
•	系统工具				
	快速配置 退出費录				激活 Windows 转野说意识激活 Windows,

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

	P-LINK						T 双核多WANロ千兆企
运行状态	æ ^	系统日志	安全审计				
基本设置	2 2						
对象管理	E.	日志设置					(2)
→ AP管理	E Constantino	□ 洗择日	末端级 所有端级				
易展设备	备管理		 	。 罢户田4	发送玄弦		
▶ 传输控制	84		映刻土内以	(且一一一)	又还示刘		
 安全管理 	理	☑ 发送系	统日志		-		
 行为管持 	控	服务器	助地: 192.168	8.17.10	」安	全审计系统服务器IP	
VPN		设置					
 认证管理 	理						
 认证管理 系统服务 	理 务	0+20					_
 认证管理 系统服务 系统工具 	理 务 具	日志列表					✔ 前往
 认证管理 系统服务 系统工具 - 云管理 	理 S S S S S S S S S S S S S S S S S S S	日志列表					✔ 前往
 认证管理 系统服务 系统工具 云管理 管理联系 	理 务 具 	日志列表		Tanan	2.00	ⓒ 殿新 区 自动物新 ● 全部数钟 ● 登出日志	♥ 前往
 认证管理 系统服务 系统工具 云管理 管理味 设留管理 动能工具 		日志列表	町1回	功能模块	日志等级	④ 刷新 ☑ 自动网新 ● 全部開始 ● 母出日き 日志内容	∨ 前往
 认证管理 系统服务 系统工具 云管理 管理账号 设备管理 设备管理 动断工具 动断工具 时间设置 	理	日志列表 序号 1 202	时间 21-05-12 15:05:30	功能模块 行为管控	日志等级 通知信息	④ 刷新 区 自动向新 ● 全部開始 ● 母出日き 日息内容 用户组:IPGROUP_LAN, 主机IP:192.168.17.3, 通过ONS面向www.baidu.com,	▼ 前住:
 入证管理 系统服务 系统工具 云管理 管理系統 设备管理 诊断工具 时间没 系統日本 	理 务 見 理 理 見 遺 造 志	日志列表 序号 1 202 2 202	时间 21-05-12 15:05:30 21-05-12 15:05:28	功能模块 行为管控 行为管控	日志等级 通知信息 通知信息	④ 除新 区 自动除新 ● 全部部数 ● 登出日き 日志内容 用产指:IPGROUP_LAN, 主机IP:192.168.17.3, 激过DNS查询www.baidu.com, 用产指:IPGROUP_LAN, 主机IP:192.168.17.3, 激过DNS查询www.baidu.com,	∨ #itt
 认证管理 系统工具 系统工具 云管理 管理系统 设备管理 诊断丁J 时间设置 系统日報 	理 务 具 理 理 理 理 通 志	日志列表 序号 1 202 3 202	时间 11-05-12 15:05:30 11-05-12 15:05:28 11-05-12 15:05:26	功能概块 行为管控 行为管控 行为管控	日志等级 通知信息 通知信息 通知信息	② 除新 区 自动物新 ● 全部数数 ● 导出日志 日志内容 用户语:IPGROUP_LAN,主机IP:192.168.17.3,激过DNS面询www.baidu.com, 用户语:IPGROUP_LAN,主机IP:192.168.17.3,激过DNS面询www.baidu.com, 用户语:IPGROUP_LAN,主机IP:192.168.17.3,激过DNS面询www.baidu.com,	▼ 前住
 认证管理 系统服务 系统工具 三管理 管理等 设备管理 设备管理 可用设置 系统目目 联络目目 (快速) 		日志列表 序号 1 202 2 202 3 202 4 202	时间 11-05-12 15:05:30 11-05-12 15:05:26 11-05-12 15:05:26	功能模块 行为管控 行为管控 行为管控 行为管控 行为管控	日志等级 通知信息 通知信息 通知信息 通知信息	② 解除 ○ 自認無能 ● 全部部除 ● 発出日報日本時間 日本時間 日本時間 用本語:IPGROUP_LAN, 主称IP:192.168.17.3, 激过ONS意識www.baidu.com, 日本語:IPGROUP_LAN, 主称IP:192.168.17.3, 激过ONS意識www.baidu.com, 日本語:IPGROUP_LAN, 主称IP:192.168.17.3, 激过ONS意識www.baidu.com, 日本語:IPGROUP_LAN, 主称IP:192.168.17.3, 激过ONS意赅www.baidu.com,	▼ Intel 5
 认证管理 系统取扱 系统工具 系统工具 若理味 设备管理 砂砾工具 可同段型 系统日本 (決重) (決重) (決重) 		日志列表 序号 1 202 2 202 3 202 4 202 5 202	时间 11-05-12 15:05:30 11-05-12 15:05:28 11-05-12 15:05:26 11-05-12 15:05:24	功能微块 行为管控 行为管控 行为管控 行为管控 行为管控 行为管控	日志等级 適加信息 適加信息 適加信息 通知信息	② 解除 図 向認識家 ● 全部課録 ● 登出日報 日志内容 用户磁:IPGROUP_LAN, 主机IP:192.168.17.3, 通过DNS查询www.baidu.com, 用户磁:IPGROUP_LAN, 主机IP:192.168.17.3, 通过DNS查询www.baidu.com, 用户磁:IPGROUP_LAN, 主机IP:192.168.17.3, 通过DNS查询www.baidu.com, 用户磁:IPGROUP_LAN, 主机IP:192.168.17.3, 通过DNS查询www.baidu.com, 用户磁:IPGROUP_LAN, 主机IP:192.168.17.3, 通过DNS查询www.baidu.com, 用户磁:IPGROUP_LAN, 主机IP:192.168.17.3, 通过DNS查询www.baidu.com, 通户磁:IPGROUP_LAN, 主机IP:192.168.17.3, 通过DNS查询www.baidu.com, 日本社IPGROUP_LAN, 主机IPF:192.168.17.3, 通过DNS查询www.baidu.com, 日本社IPGROUP_LAN, 主机IPF:192.168.17.3, 通过DNS查询www.baidu.com, 日本社IPGROUP_LAN, 主机IPF:192.168.17.3, 通过DNS查询www.baidu.com, 日本社IPGROUP_LAN, 主机IPF:192.168.17.3, 通过DNS查询www.baidu.com, 日本社IPGROUP_LAN, 主机IPF:192.168.17.3, 通过DNS查询www.baidu.com, 日本社IPGROUP_LAN, 主机IPF:192.168.17.3, 通过DNS查询www.baidu.com, 日本社IPGROUP_LAN, 主机IPGROUP_LAN, 主机IPGROUP_LAN, 主社IPGROUP_LAN, 主社IPGROUP_LAN, 主社IPGROUP_LAN, 主社IPGROUP_LAN, 主社IPGROUP_LAN, 生社IPGROUP_LAN, 生社IPGROUP_LAN, 士社IPGROUP_LAN, 士社IPGROUP_LAN, 士社IPGROUP_LAN, 士社IPGROUP_LAN, 士社IPGROUP_	s indows VJBMS Windows,

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:

IP-LIN	K									TL-FW66 増强级防>
画板	URLitin	\$ 文件过滤	应用行为控制	都件过来 1	内容过滤 关键字	組 反病毒 全	電配置		提交階級	查 保存配置 退出登
留略 对象	URLitzis	规则列表					, 夫	京击新增		2
地址时间段		序号	名称	策略类型	过滹方式	过滤内容列表	网站过滤列表	備注	 ○ 新増 ○ 新除 设置 	
 IP地址池 用户 服祭 	-	-1	WPS	禁止	网站分组		视频,游戏,射经, 社交,购物,生活, 音乐,煤乐,论坛, 小说,体育,阅盘	限制WPS云		
 网站 <u>応用</u> 安全配置文件 入侵防部 加密检測配置文件 证书 	名 策 辺	称: 縣类型: 違方式: 站分坦:	TPLINK 〇 仅允许 ● 网站分 视频, 谢	、 访问下列的URL 组 〇 URL关键 成,财经,社交, 制	(1-28个字符) ● 禁止访问下列的UK 字 ○ 完整URL	填写相	应内容			
网络 系统		at. 确定 I	PRess/ol	JIPLINK	(4)20,1-301-9					
							共1条, 制	顾: 10 ∨ 条 計	当前: 1/1页, 1~1条 < 1 →	
Copyright © 2021 普联技术有限公司 版权所有									激活 Wind 转到"设置"以	dows 눌活 Windows。

3.2.2 设置安全策略记录日志

				配置未提交 配置未保存 提交配置 保存配置
自极	安全策略 策略冗余分析 目的安全区域:	Any	▼ (P)32)	配置提交并保存
ely tes	源地址:	IPGROUP_ANY	•	
安全策略	目的地址:	IPGROUP_ANY	•	
带宽策略	用户组:	Any	*	
NAT策略	服务组:	Any	*	
ALG策略	应用编:	ANY	(点击查看已选列表)	
安全的护加密流量检测策略	UNACTATION CA	点击修改		
刺象	时间段:	Any	•	
网络	动作:	● 允许 ○ 禁止		
系统	内容安全:			▲ 返回頂
	URL过滤:	TPLINK	 选择安全配置文件 	✔ 前往底
	反病毒:			
	入侵防御:		*	
opyright © 2021	文件过峰:		*	
al 味觉不何限公司 版权所有	内容过滤:		*	
	应用行为控制:		*	
	邮件过滤:		*	
	况景策略命由日 主 ·			
	经本:		胡记录日志	WEF Windows
				病则已Windows 转到"设置"以激活Windows。

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:

		TP-LINK		TL-FW6600 増强级防火墙
				提交配置 保存配置 退出登录
	+	面板	日志和査	
	•	监控		
	•	策略	日志配置	2
	+	对象		
	•	网络	☑ 选择系统日志等级	
	•	系统	所有等级	
4		 管理员 	☑ 选择系统日志模块类别	
ų		 云管理 		
		 设备管理 	全局设置启用发送系统日志	
		 时间设置 	B2588999 102 148 10 144 0 0 0 0 0 0 1 2 5 5 5 7 10 144	
	L	 日志配宣 牛燃配器 	女王甲订杀坑服穷奋IP	
		 古宮北直 存储管理 	22	
		 升级中心 		
		• License管理		
		 高可常性 		
		 系统参数 		
		 快速配置 		
		Copyright © 2021 普联技术有限公司 版权所有		激活 Windows 時町 役置つ場開着 Windows。

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:

TP-LINK				TL-FW660 增强级防火
77.64				配置未保存提交配置保存配置通出議員
回极	安全简略 策略九第分析			提父开保存配置
加速	规则名称:	Log	(1-28个字符)	
· 安全策略	描述:		(1-50个字符)	
 蒂宠策略 	源安全区域:	local	▼ (可造) 设备所在区域	
• NAT策略	目的安全区域:	trust	▼ (可應) 服务器所在安全区域	
 ALG策略 安全防护 	源地址:	IPGROUP_ANY	▼ 设备IP组	
 加密流量检测策略 	目的地址:	Servers	▼服务器IP组	
对象	用户组:	Any	▼ 任意或设备自身用户组	
网络	服务组:	Any	▼ 任意或日志传输服务	
系统	应用组:	ANY	(点击宣誓已运列表)	 太田市
		点击修改		✓ 前往病
	时间段:	Any	•	
	动作:	● 允许 O 禁止		
Copyright © 2021 普联技术有限公司	内容安全:			
版权所有	URL过滤:		v	
	反病毒:		v	
	入侵防御:		v	
	文件过滤:		v	
	内容过滤:		•	
	应用行为控制:		v	
	即件过滤:		v	

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:

6	in (1901	要文件							提交配责	保存配置 遗
12 12		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	
略 家 新計配書文件		1	audit_all	审计所有问题	审计范围:所有URL 网页标题:记录 HTTP上传文件:记录 HTTP下载文件:记录	FTP命令:记录 FTP文件上传:记录 FTP文件下载:记录	邮件发送:记录 邮件摘收:记录	帐号登陆:记录		
Ŕ	4	(#t):		audit_all	(1-28个字符	F)				
	5	i述:		审计所有网站	(1-50个字符	})				
	н	TTP行为审计	+							
Copyright ② 2021 普联技术有限公司	1	HTTPRIN	5FEI :	〇 不能计 (● 審社師者URL 〇 審社様	iccURL				
		Citate in the		0 144	-					
版权所有		POPERATE:								~
		阿贝林題:	- Dia .							~ 1
		HTTPE#X	()+; 70+;		2(HB)464(1、大小) 在(HB)484(1、大小)					
	F	TP行为审计		LEI RURC C FAR.	CITUPENIC X(17)					
		FTP&A:		☑ 记录(命令内	(客)					
		FTP文件上的	6 :	I 记录 (上传)	文件的名称、大小)					
		FTP文件下	£:	I 记录 (下载)	文件的名称、大小)					
	đ	附审计								
		邮件发送:		I 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;		I 记录 (邮件)	发件人、收件人、标题、附件名	称以及附件大小)				
	I	竹为审计							激活 Wind	ows
	- T								转到"设置"以激	的话 Window

3.2.5 设置审计策略

TP-LINK	<															TL-FW66 增强级防火
															提求	武 士 保存配置 退出登
面板	审	计策略														
監控																
	1 PP 1	计跟踪分	戦													
审计策略													0 8	印 〇	H\$1 🙆 ###	R .
对象		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	劫作	审计配置文件	状态	设置	
1-76		1	audit_all_d	审计所有流量	Any	Any	IPGRÖUP_A	NY IPGROUP_ANY	Any	Any	Any	审计	audit_all	已启用		
Copyright © 2021 普联技术有限公司 重权乐者		編起 編述 源表 目的 源地 目的 月 戸 服务	名称: (:)安全区域:)地:)地址:)地址: ;;		audt Fritfi Any Any IPGRC IPGRC Any Any	al_data 有读量 DUP_ANY DUP_ANY	* * * *	 (1-28个字符) (150个字符) (可透) (可透) 								<mark>▲</mark> 逝回 ▼ 杭住
		时间 动作 审计 状态	殿: :: 香透文件: :: 接销编定位置(第几条):	Any ● 审计 audit_ 区周	〇 不审ì all	+	选择之前的	同配置文件	ŧ					激活 W 转到"设置	indows 以蹤活 Windows,

3.2.6 审计日志发送至服务器

TP-LIN	ĸ		TL-FW660 增强级防火炸
面板	审计数据		提交戰畫 保存戰畫 過出登录
监控			
策略	上阿行为分析		0
对象			
系统	上传用户上网行为: [2 启用	
 日志配置 	行为审计服务器地址:	192.168.10.144 安全审计服务器IP地址	
	设要		
	Vi.ask		
Copyright © 2021 晋联技术有限公司			
版权所有			
			激活 Windows
			weth 说直 以取话 Windows。

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	已启用区	🥕 🛍
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。

	全审计系统					▲ 首页 🚦 系統日志	🚉 用户及角色 💄 admin
首页	> \	首页					
】 日志 	> >						
	>	CPU使用率		内存使用率		磁盘利用率	
		100.0%		82.7%		9.6%	
		100.070		02.17		0.070	
		使用CPU 空闲CPU	100.0%	已使用 总内存	3.2GB 3.9GB	已使用 总容量	11.7GB 121.8GB
		系统信息					
		所统合称 TP-LINK安全审计系统					
		版中信思 1.1.8					
		日志数量 •					
		日志数量					
		50,000		\wedge			
		40,000					
		20,000					
		10,000					
		14:00	18:00	22:00		02:00 激活 V	/indows
						非使 <u>于1</u> 1.023	E Kalline Windows,
			着联技术有限公司 版权	所有 Copyright © 2021 TP-LINK. All rights res	served.		
	·		レズルシロナ				
页面	左侧列	出了安全审计	「糸玧m乍	的官埋奀日。	灾面石」	_角有四个快	捷按钮 :
页面	左侧列	出了安全审计	「糸玧所有	的官埋突日。	灾面石」	_角有四个快	捷按 钮:
页面	左侧列	出了安全审计	「系玧所有	的官埋奀日。	灾面石」	_角有四个快	捷按 钮:
页面	左侧列	出了安全审计	「杀玧所有	的官埋突日。	贞面石」	_角有四个快	建按钮:
页面	左侧列	出了安全审计	「杀玧所有	的官埋突日。.	灾面石」 	_角有四个快	捷按钮:
页面	左侧列	出了安全审计	「系玧所有	的官埋突日。	灾面石」 	_角有四个快	捷按钮:
页面	左侧列		「系筑所有	的官埋突日。.	東面石」	_角有四个快	捷按钮:
页面	左侧列		「系筑所有 系统日志	的官埋突日。	_{页面石」}	_角有四个快 L admi	捷按钮: n ▼
页面	左侧列		「系筑所有 系统日志	的官埋交日。	_{页面石」}	_角有四个快 Ladmi	捷按钮: n ▼

- 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。

LINK 安全审计	5.69			▲ 龍页	■ 系統日志	▲ 用户及角色	L admin
系统	日志						
用户		\$2120100 18200 B FR	. (11#12#1		22	現立	
190	9. 用户	时间	详情				
1	admin	2021-05-12 14:11:20	整梁系统				
2	admin	2021-05-12 13:53:32	整梁系统				
3	admin	2021-05-12 13:53:29	整要系统				
4	admin	2021-05-12 11:25:21	整梁系统				
5	admin	2021-05-12 11:10:50	整景系统				
6	-	2021-05-12 10:17:47	日志速車超限1限制300条5、当前韓值已达到662条5				
7	admin	2021-05-12 10:15:15	更新安全证书				
8	admin	2021-05-12 10:11:41	發換系统				
9	admin	2021-05-11 20:43:23	聖景系统				
10	admin	2021-05-11 20:43:21	登录系统				
共计	17版 第1/23	π	10965	页	× REEM	页	
					激(舌) 病到"说	Windows	lows,
			副研技术有限公司 医权所者 Copyright © 2021 TP-LINK, All rights reserved.				

- 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。

	TP-LINK 安全审计系统		▲ 莆页 🚦 系统日志 🙁 用户及角色 👱 admin 🗸
L	用户及角色		添加用户
	新 印合		
	序号 用户名	家屋角色 ↓	銀作
	1 admin	管理员	编辑
	2 fengyuan	操作员	病道
	3 wangguan	管理员	编辑
	共计3条 第1/1页 已选:0		10条页 V K K 1 > X 前往第 页
4			
1			
			激活 Windows 转到"设置"以激活 Windows。
Ľ		普联技术有限公司 版权所有 Copyright © 2021 TP-LINK All rights resen	ed.

● 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。

										_				
TP-LINK 安	全审计系统										▲ 首页	■ 系統日志	用户及角色	💄 admin 👻
● 首页 ■ 日志		路由	审计日志 内容显	示诜择								日志导	出	导出Excel
路由审计日表 防火培审计日		= P	内容 刷新									日志	筛选	備选 ~
流量日志		序号	时间	用卢组	用户IP	应用类型	应用	动作	日志等级	详细内容				î
1987Fロル5 策略合中日共		1	2021-05-12 14:30:36	IPGROUP_ANY	192.168.1.10	生活服务	百度地图	正在使用	通知	使用百度地图				
设备系统日志		2	2021-05-12 14:30:35	IPGROUP_ANY	192.168.1.10	生活服务	百度地图	正在使用	通知	使用百度地图				
威胁日志		3	2021-05-12 14:29:35	IPGROUP_ANY	192.168.1.10	生活服务	百度地图	正在使用	通知	使用百度地图				
URL日志		4	2021-05-12 14:29:33	IPGROUP_ANY	192.168.1.10	生活服务	百度地图	正在使用	通知	使用 百度地图				
内容日志		5	2021-05-12 14:29:25	IPGROUP_ANY	192.168.1.10	生活服务	百度地图	正在使用	通知	使用百度地图				
▲ 统计报表		6	2021-05-12 14:28:47	IPGROUP_ANY	192.168.1.10	社交软件	微信	正在使用	通知	使用 微信				
○ 系统		7	2021-05-12 14:28:47	IPGROUP_ANY	192.168.1.10	社交软件	微信	正在使用	通知	使用微信				
		8	2021-05-12 14:28:35	IPGROUP_ANY	192.168.1.10	社交软件	微信	正在使用	通知	使用 微信				
		9	2021-05-12 14:27:29	IPGROUP_ANY	192.168.1.10	基础应用	HTTPS	正在使用	通知	使用 HTTPS				
		10	2021-05-12 14:27:05	IPGROUP_ANY	192.168.1.10	生活服务	百度地图	正在使用	通知	使用 百度地图				
		11	2021-05-12 14:26:36	IPGROUP_ANY	192.168.1.10	生活服务	百度地图	正在使用	通知	使用 百度地图				
		12	2021-05-12 14:25:24	IPGROUP_ANY	192.168.1.10	生活服务	百度地图	正在使用	通知	使用 百度地图				
		13	2021-05-12 14:25:14	IPGROUP_ANY	192.168.1.10	生活服务	百度地图	正在使用	通知	使用 百度地图				
		14	2021-05-12 14:24:47	IPGROUP_ANY	192.168.1.10	生活服务	百度地图	正在使用	通知	使用百度地图		20427-1	Mindows	
		15	2021-05-12 14:23:15	IPGROUP_ANY	192.168.1.10	基础应用	HTTP	正在使用	通知	使用 HTTP		病()占 转到"说	置"以激活 Win	dows,
		16	2021-05-12 14:22:24	IPGROUP_ANY	192.168.1.10	生活服务	百度地图	正在使用	通知	使用百度地面				~
		共计294	51条 第1/59页	音联	支术有限公司 版权	所有 Copyrig	ht © 2021 TP	-LINK. All rig	hts reserved.	500条/页 🗸	к с	1 2 3	> > 前往第	页

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。

TP-LINK 安全i	計系统				▲ 首页 🚦 系统日志 🚨 用户及角色 💄 admin 👻
● 首页 目 日志		日志统计	选择统计的设备		
山 统计报表 日志统计 流量统计 策略命中统计		TL-ER3220G(192.168.17.1) ~]		选择统计的时间段
		■ 14950日 ● 日本部注意 2,000 1,500 0 0 1500 1900 日本設置 1 1 日本設置 1	23.00 01	300 0700 • Ita • Ita • Fi	① ② ◎ ① 11.00 15:00 ■ ● 臨天 ● 昭和 ● - 第四 ● 田田 ● 第回 1000 回 ①
		晋朝	支术有限公司 版权所有 Copyright © 2021 TP-LINK All	rights reserved.	转到"设置"以激活 Windows。

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。

	•	'P-UNK 安全审	计系统					▲ 首页	系统日志 👱 用户及角色 👱 admin 🗸
	A B			流量统计					导出PDF
	ф	统计报表		设备流量统计 源IP流量统计					导出pdf
		日心现计 流量统计						切换上下行	选择时间段
4		策略命中统计		Top5设备流量统计 🟮				E	
				流量	2021年5月11日			2021年5月12日	
				292.97KB					人 设备列表
				195.31KB					
				97.66KB					
				0B +	19:00	23:00	03:00	07:00	11:00 15:00
				设备		上行总流量		下行总流量	
				192.168.1.1		354.83KB		5.13MB	
L				共计1条 篇1/1页				10影页 🗸	к < 1 > X 前往第 页
I									激活 Windows 转到"设置"以激活 Windows。
L					普联技术有限公司版	設所有 Copyright @ 2021 TF	P-LINK. All rights reserved.		

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。

TP-LINK 安全审计系统			▲ 首页 🚦 系統日志 🙁 用户)	及角色 👱 admin 👻
▲ 首页 >	流量统计		导出P	DF
	设备流量统计 源IP流量统计			导出pdf
流量统计			切换上下行选	择时间段
策略命中统计	Top5源IP流量统计 0		上行流量下行流量(0 🕲 🖸
	流量 2021年5月11日			●- 192.168.17.2
	292.97KB		Δ	设备列表
	195.31KB		/ \	
	97.66KB			
	08 +	23:00 03:00	07:00 11:00	15:00
	颤P	上行总流量	下行总流量	
	192.168.1.10	349.63KB	5.12MB	
	192.168.17.2	5.20KB	2.89KB	
	共计2条 篇1/1页		10条页 🧹 К < 1 > 米	前往第 页
			激活 Window 转到"设置"以激励	W S § Windows。
	磺联技术有限	公司 版权所有 Copyright © 2021 TP-LINK. All rights reserved.		

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。

	TP-LINK 安全审	计系统		▲ 首页 📑 系統日志 💐 用户及角色 💄 admin	•
Ê			策略命中统计		
	防火墙审计日志		TL-FW6300(192.168.1 > 选择显示设备	选择时间段	t
			館館命中数量Top5 ❶	T @ 7	
	策略命中日志 设备系统日志 威胁日志		推明命中效量 200 2021年5月11日 250	2021年5月12日 显示策略名称 ▲ asdque]
			200	\land	
	邮件日志		50		
	日志施计		0 1 22:00 02:00	06.00 10.00 14.00 18.00	
	流量统计 策略命中统计		所有策略结果		
٥			策略	命中政量	
			asdqwe	321	
			共计语 篇10页	10条次 v K く 1 > > 前住道 页	
				激活 Windows 转到"设置"以激活 Windows,	
			番联技术有限公司 版权所有 Copyright © 202	021 TP-LINK. All rights reserved.	

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。

TP-LINK 安全审计系统	▲ 首页 ■ 系統日志 👱 用戶及角色 🛓 admin 🗸
▲ 首页 → 数 目 日志 →	效据库管理与备份
 曲 統计报表 、 日志統计 	រានស
洗煎約计 第第曲中均计 3 新休 ~ 数款付留等与新分 日志爾爾原則 设备鉴察及 安全证书	EXEMPSION ① 开目 * 留台保存时间 天 型期間高清空散份文件 * 目記留台周期 1 备份时间 天 型 备份后清空数据体 * 目記留台周期 1 备份时间 天 型 备份后清空数据体 * 目記留台周期 Figeamitteacturplate 备份地址
JAS	
	守入致据库 激活 Windows _{转到该重以激活 Windows} 。
	葡萄誌水和現公司 版权所有 Copyright © 2021 TP-LINK, All rights reserved.

- 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。

TP-LINK 安全审计系统		系统	▲ 蕭页	■ 系统日志 🚉 用户及角色 👤 admin 👻
♠ B	首页 > 日志 >	F	日志屏蔽规则	
di		-	选择日告严重等级 等级选择 。 低于该等级的日告将会长去年	
0	策略命中统计 系统		2014第前的85米型 设备系统目志 2014年1日志 30大海市1日志 第第命中日志 操作日志 近曜日志 2014日本 2014日本 2014日本 2014日本 2014日本 2014日本 2014日本 2014日本	□ 威胁日志 □ URL日志
	数据库管理与备份 日志屏蔽规则 设备鉴权 安全证书			
				激活 Windows 转到"设置"以激活 Windows,
			需要结卡有限公司 版权所有 Copylight © 2021 TP-UNIX All rights reserved.	

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 → ■ 日志 → 	设备鉴权		
■ 统计报表 → 日志统计 流量统计 策整命中统计			
○ 系统 ~ 股据库管理与备份	添加 删除		Q 提紧
日志屏蔽规则	序号 设备名称	IP地址 ト	操作
设备鉴权	1 TI-ER3220G	192.168.17.1	编辑
	ANTINE MUTUAL ECON.U		10000gg ♥ K C Y J X mream
			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.	

5.4 安全证书

此处可以查看服务器的安全证书信息,包括到期日期以及日志管理性能。TP-LINK 安全审计 系统默认提供 200 条日志/秒的日志存储规格,一般可以供 200 人以下的网络实现审计日志 存储,若日志提示规格不足或者需要提升存储规格,需要付费申请更高规格的证书,具体可 以联系 400-8860-400 客服热线或者咨询当地办事处。

TP-UNK 安全审计系统	▲ 蕭页 📑 系統日志 💐 用户及角色 👱 admin 🗸
 ▲ 首页 → ● 首页 → ● 日志 → 	安全证书
 (1) 新統 (1) 新統	安全证书信息
	運動安全证书 激活 Windows 彩引 「空国」でJulitifi Windows, 研究技术和限公司 版役所存 Capyright © 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?

在不购买安全证书的情况下为 200 条/s。

3、如何升级规格?

可以联系当地办事处购买安全证书进行升级规格。

4、如何选择合适的规格数呢?

一般来说,可以按照大约1个终端1条/s的速度进行计算,购买相应的规格。日志速率超限后,安全审计系统的系统日志也会提示日志速度超限,并提示当前日志速率峰值,购买相应规格速度即可。