

安全域流量监管系统 使用手册

北京创元启安科技有限公司

安全域流量监管系统 ¹ 使用手册



读者对象 2 读者对象 2 术语定义 3 产品架构 3 功能概述 3 用户登录 4 探针管理 6 设备管理 10 黑白名单管理 10 写连关系管理 20 互连关系管理 24 系统管理 24 那户管理 31 审计日志 36	概述	2
读者对象 2 术语定义 3 产品架构 3 功能概述 3 用户登录 4 探针管理 6 设备管理 10 黑白名单管理 10 黑白名单管理 18 互连关系管理 20 互连关系管理 24 系统管理 28 用户管理 31 审计日志 36	读者对象	2
术语定义 .3 产品架构 .3 功能概述 .3 用户登录 .4 探针管理 .6 设备管理 .10 黑白名单管理 10 国主关系管理 .20 互连关系管理 .20 互连关系管理 .20 写统管理 .24 系统管理 .28 用户管理 .3 雪计日志 .36	读者对象	2
产品架构 .3 功能概述 .3 用户登录 .4 探针管理 .6 设备管理 10 黑白名单管理 10 三连关系管理 20 互连关系管理 20 写连关系管理 24 系统管理 28 用户管理 31 审计日志 36	术语定义	3
功能概述 .3 用户登录 .4 探针管理 .6 设备管理 10 黑白名单管理 18 互连关系管理 20 互连关系管理 20 写连关系管理 24 系统管理 28 用户管理 31 审计日志 36	产品架构	3
用户登录 .4 探针管理 .6 设备管理 10 黑白名单管理 18 互连关系管理 20 互连关系管理 24 系统管理 28 用户管理 31 审计日志 36	功能概述	3
探针管理 .6 设备管理 10 黑白名单管理 18 互连关系管理 20 互连关系管理 20 互连关系管理 24 系统管理 28 用户管理 31 审计日志 36	用户登录	4
设备管理 10 黑白名单管理 18 互连关系管理 20 互连关系管理 24 系统管理 28 用户管理 31 审计日志 36	探针管理	6
黑白名单管理 18 互连关系管理 20 互连关系管理 24 系统管理 28 用户管理 31 审计日志 36	设备管理	
互连关系管理 20 互连关系管理 24 系统管理 28 用户管理 31 审计日志 36	黑白名单管理	
互连关系管理 24 系统管理 28 用户管理 31 审计日志 36	互连关系管理	20
系统管理 28 用户管理 31 审计日志 36	互连关系管理	
用户管理	系统管理	
审计日志	用户管理	
	审计日志	

前言

概述

本文档介绍了安全域流量监管系统的基本概念和相关操作。分别从探针管理、设备管理、互连关系管理、白名单管理、查询报表、系统管理、用户管理和日志审计等多个方面介绍了安全域流量监管系统的操作流程和使用方法。

读者对象

本文档主要适用于以下读者:

- 网络安全监控工程师
- 系统运维工程师
- 安全管理主管

读者对象

本文档主要适用于以下读者:

- 网络安全监控工程师
- 系统运维工程师
- 安全管理主管

安全域流量监管系统³ 使用手册

安全域流量监管系统概述

术语定义

◆ 安全域流量监管系统

通过在网络边界区域部署流量采集探针,发现以上边界区域中的设备之间的互连关系,并对互 连流量进行专业化的协议分析,以智能化区分出合法的互连流量的流量监控管理产品。

◆ 安全域

安全域(网络安全域)是一个逻辑范围或区域,指有相同的安全保护需求,相互信任,并具有 相同的安全访问控制和边界控制策略的子网或网络。

◆ 安全子域

一个安全域内可根据其管理需求的不同(如:维护管理部门的不同)、地域的不同(如:一个 网络或系统的不同物理节点)、数据分类不同(如:安全域中的交互网络域、计算域、服务域、 维护域),可进一步被划分为若干安全子域。

◆ 互连关系

设备间为实现通信和资源共享产生的访问关系

◆ 白名单

符合因业务运营及管理需要、正常业务流程需要、日常维护需要而生成的设备互访关系称为白 名单。

产品架构

创元启安安全域流量监管系统采用并行计算的高性能流量分析引擎,充分利用多核 CPU 的架构优势,大幅提升流量分析的性能指标。采用从 2-7 层的深度网络协议分析技术,完全还原网络协议内容,为各种合法流量、非法流量的分析定位提供强力支撑。

考虑到当前企业中网络流量巨大的特性,安全域流量管控系统应支持分布式部署、集中管控。 即流量采集、协议分析及包头数据的采集由覆盖各个内外部边界,而包头数据的统计分析、特征提 取、白名单确认和维护由集中控制端完成。

功能概述

安全域流量监控系统利用网络流量抓取的方式抓取安全域内部各子域、安全域不同接口流量, 形成可视化的设备互连关系视图,从而全面地掌握各通信网、业务网和各支撑系统安全域内部、安 全域之间设备互连关系,并根据业务生产逻辑需要和业务生产维护需要对检测到的已知合法的互连 关系进行合法的白名单定义。对于不能明确的互连关系,通过系统自动分析、提取协议内容、连接 特征等信息,并提供给业务系统或安全管理人员进行判断,以降低人工确认的复杂度。

探针管理

查看已部署、未激活的流量采集探针及探针的运行状态信息。实现对监测安全域边界、子域 之间、子域的流量进行原始流量采集,支持灵活配置采集范围,驱动数据采集和协议分析策略同步, 实现提取互连关系基础数据或全流量数据,对流量进行深度协议分析。

设备管理

通过流量发现 IP 设备,并提供 IP 地址与设备名称、设备类型、所属组织机构等属性信息的对应,并实现设备信息的批量导出和导入,提高互连关系的可读性。

• 互连关系管理

互连关系监控主要展现了网络中设备间因一定需求而事实存在的连接情况的总体视图。可以 制定、查看、修改各种统计分析策略,设定策略适用方法;依据策略对来自各个边界的白名单之外 的其它流量的协议分析结果进行多维度的统计分析,发现基于五元组的统计特征,如周期性、频次 等;可以配置优化策略,对不同边界提供的信息采取不同的统计方法、顺序。

• 白名单管理

根据已生成的互连关系,并结合其连接周期、频次、管理指令、登陆帐号等特征生成白名单, 用于区分网络环境中的合法流量和不明确流量。

报表中心

报表主要是用户可以查询已经确认的互连关系白名单、待确认互连关系名单、指定流量的包内容等信息,提供报表的生成、查看、导出功能,导出格式为 PDF、HTML 等常见格式。

系统管理

包括对系统的日志转发配置、系统组件管理、存储配置、软件升级及许可证信息。

用户管理

增加、修改、删除用户、用户组、角色及组织信息,可以在此模块中直接对用户进行授权: 授权的内容包括功能模块的读、写及访问权限、组织机构权限、设备权限。

日志审计

提供系统的查询及操作产生的日志,支持日志的导出。

用户登录

登录

系统页面的登录界面如下:



输入用户名和密码、验证码后,点击"登录"即进入系统。

首页

用户登录成功后,系统将显示出首页,如下图所示:



系统首页包括"最新系统信息"和"统计类信息"两部分。

最新系统信息的内容包括:系统监测时间、当前检测业务系统数量、当前未知设备数据、当前互连关系数量、当前合规互连关系数量、当前违规互连关系数据、不明确互连关系数量;本帐号 上次登录时间、当前登录用户名、连接时长信息。

统计类信息包括:会话趋势图、设备分布图、待确认互连关系 TOP5、未知设备互连关系 TOP5。

修改密码

用户需修改密码时,点击页面右上侧的"修改密码"按钮,系统将弹出修改密码窗口,如下 图所示:



北京创元启安科技有限公司

用户输入原密码、新密码、确认密码后点击确定即可修改密码。

退出系统

用户需退出系统时,点击页面右上侧的"退出"按钮,系统将自动退出。

探针管理

• 探针状态管理

探针状态管理用于显示当前系统部署的未激活和已激活的探针信息及状态,在页面左侧提供 探针查询功能,用户可以通过输入探针名称、探针 IP、位置等查询条件,查询探针信息。

点击"探针管理"-"探针状态管理"后,显示的是未激活的探针列表,如下图所示:

			●四 第11日間 ▼	126451	Ev 30/08#688	218	关系 単数中心 マ	系统管理 ♥		-
時相理 > 除针状态管理	R 1171	_								
探针查询	厂全石	# Q	编计名称	C.R	版本	29	护地址	推送	遺作	
七帝: 例:example_1	Π.	1	probe_888	PPP	2.3.0.56683	a	192.168.10.88	probe	*	
EEP: 例:10.1.1.1					共1条数据页次1/1页					Ι.
8 : ·								**	**	
意識 潮空										ln –
										() ()

未激活的探针,包括探针名称、位置、版本、型号、IP 地址信息和描述信息,点击探针信息 最后一列的【操作】栏的 按钮,可以激活探针,也可以勾选全选或多选,批量激活。 在页面的右侧点击"已部署",显示的是已激活的探针列表,如下图所示:

安全域流量监管系统 7 使用手册

📿 安全域流量	监管系统 v2	ł					👤 登取用户 : admin	\$\$\$1\$19] : 2013-06-06 16:5	365 (Jillim
			118 - 21811	N + 084	帕爾 石油火菇	• 15Z	190 - 26888 -		
麻叶竹蕈 > 麻叶板合竹蕈	*##	已部要求针列	18						
权计查询			81						
R1188 :			用针窗标	02	展本	200	IPISIE	Mile	最作
1298P :		1	probe_17	probe	2.2.0.3984	rul	10.110.184.17	SDFM-probe	িয়
12E :					< 第1条数据 至次1/12	≅.1-≅ 1			
## #X									
	1								

已经部署的探针,包括探针名称、位置、版本、型号、IP 地址信息和描述信息,点击探针信息 最后一列的"操作"按钮,则显示的是选定当前探针的详细信息。

探针的详细信息除包括探针型号、名称、设备标识符、系统运行时间、所属管理接口、管理 IP 及当前状态外,还显示接口信息列表,包括接口名称、接口类型、RX、TX、链路模式、接口状态和 MAC 地址,还显示探针健康程度,包括探针 cpu、内存、磁盘的资源使用情况,还显示了近期探针 抓取到的流量情况。如下图所示:

					89 I	HIRE Y	RORD	*	#/R8W	**	124.8	× 1	ilite v		982 1	•		
HANNIN HAAMMA ()	["	112 ANEL A 215 1211	SDFM-2003		81 11	© proke_111 EP : 192.168.1			nawin Rifter	d ^{ang} antasi I		. **	2094 -	27,61.04	K1094			
		日前息列																
	124	建口条件		湯に発	2		RK			TX		結果式	100	2050E		M	ACHESE	
	1	eth8		manite	or	D		0	0	0			1	UP .		80.51.8	E-03-55-0	18
	2	*#8	mirro	orfrom eth	8 to ethe	0	1	0	0	0			1	UP		80.51.8	E-03:55:0	19
	8			manag	24	11745	7 1083	9954	23325	3917116	100	OM/Full	UPRU	NNING		80.51.8	E-03-35.0)F
	4	eth1		manag	34	0		0	0	0				μp		80.51.8	E-03-35-6	80
	5	eth2		decen	or	15045	3 5930	5167	18	1260	100	OM/Full	UP RU	NNING		80.51.8	03.35.0	1
							10 0.0 1	10 01/ 29	(> 1 2	7-2 8								
	-	波当趣—		***	*****	2013-08-2	ŋ		1	WOLL		•	***	# #(20	013-00	9-20)		
	1001								60,0	DOK	_	_		_	_	_	_	
	80	100							48,0	00K								
	50	2							36,0									
	30	1							24,0	JUOK I								
	1D 04						_		12,0	JUOK								
		4041	4341	10.4	154	9:41	100	4041		Ŧ	41	7		ŧ.	41	11	41	41
	Ŭ,	54041	115.90	39:41	34:41	24:41	19:41	14:41		DE	1941	1141	19-0	16.6	9:41	19-14	9:41	

探针密钥

探针密钥用于提供探针与中心端的通讯加密配置,用户可根据自身情况,选择密钥进行导入, 如下图所示:



监测范围

用户可以通过灵活的配置流量监测范围,实现对不同边界采集不同流量的策略方法。监测范 围包括新增、修改、删除监测策略,并通过勾选策略应用到探针。

用户点击"探针管理"-"监测范围"后,可进入探针监测范围的配置页面,如下图所示:

益詞范围查询 述:	200	14681	Pitt V Eism	D.	1912 :	×	Bifikud KR	1221: P地址 123: 高		≅: <u>優辻</u> ▼ 激加
D)	AMEN	设置列表								
o	「全市	序号	WOL	目标地址	79MC		1012	优先级	是实透过	操作
X	г +	1	192.168.10.1			21	TCP	*	通过	30×

1.新增监测策略

用户可通过页面中的"监测范围设置",自行添加监测策略。在填写策略信息时,需要输入源 地址类型(可以是 IP 地址或地址组)、目标地址类型(可以是 IP 地址或地址组)、源端口、目标端 口、使用协议、采集优先级和是否通过(当选择通过时,表示的是该条策略命中后,对流量进行保

存,反之则不保存)。

2.修改、删除策略

用户可通过页面中的"监测范围设置列表",查看当前已经生成的监测策略情况。如下图所示:

安全域流量监管系统⁹ 使用手册

■ 全选	序号	源地址	目标地址	源端口	目标踌口	协议	优先级	是否通过	操作
	1						高	通过	3 0 ×
	2	飞信-101			3		高	通过	30 ×
	3	飞信-101			2		高	通过	3 Ø ×
	4	飞信-101			1		高	通过	3 Ø ×

当需要对选定策略进行修改时,用户可通过点击"操作"中的"修改"按钮,对策略进行修改,如下图所示:

◎ 流望整形	策略							
源地址类型:	IP地址	•			目标地址类型:]	P地址	•	
源端口:		目标端口:	协议:	•	优先级: <mark>高</mark>	•	是否通过: <mark>通</mark> 波	<u>t</u> 💌
						[关闭	确定
						·		

当需要对选定策略进行删除时,用户可通过点击"操作"中的"删除"按钮,对策略进行删除, 如下提示:



3. 应用策略

当需要对选定策略应用到某探针时,用户可通过点击"操作"中的"应用到探针"按钮进行 配置,如下图所示:

- 北京创元启安科技有限公司 ----

! ! 地址类型: IP地址	B	标地址类型:IP地址	源靖口:	
1标端口:	协	议:	优先级:	<u> </u>
否通过: 通过				
□ 全选	序号	探针名称		探针软件版本
	1	probe_111		2.3.0.5683

用户在页面中勾选需要应用的探针后,点击"确定",即可完成策略应用到探针的操作。

4.范围应用列表

范围应用列表用于显示、修改当前探针的默认策略,如下图所示:

		远择	序号	探针名称	范围应用开关	默认策略	操作
源地址:		Г	1	Dolphin223	◎ 开启 ○ 关闭	不符合流量规则均通过 🖌	Ø
目标地址:					< 共1条数据 页次1/13	页 1 >	
渡端口:							
目标满口:							
协议:							
最否通过:	想を						
童狗 清空	12						
	Ч						

当"范围应用开关"设置为"开启"时,表示监测策略生效,"关闭"则表示不应用策略, 进行全部流量采集;

用户还可以通过修改默认策略灵活地设定,当不满足监测策略的流量是采集还是不采集。

设备管理

安全域定义 •

用户可以根据清晰、明了的安全域结构树,对安全域进行添加、修改、删除的管理操作。用 户点击"设备管理"-"安全域定义"后,可进入操作页面,如下图所示:

安全域流量监管系统 11 使用手册

🕐 安全域流量监管系	系统 v2.2.0.5678					▲ 登录用户:A	dmin 💮 系統財	间:2013-08-21 11:05:55	参数 本 研	しいの
		首页	\$\$ 11管理 ¥	设备管理 ¥	黑/白名单管理	互连关系 ∀	报表中心 ¥	系统管理 ∀		
記書補加 > 安全補正文	9 ■									

1. 添加下级安全域

用户鼠标选择相应安全域时,会在对应安全域后面显示出"添加"、"修改"、"删除"按钮, 通过点击添加按钮,右侧会显示添加安全域的菜单,如下图所示:

🕑 安全域流量监管	下系统 v2.2.0.4922	👤 豐東用戶: Admin 📀 奚姊时间: 2013-07-29 16:24:53 🔞 棒政能明 🕛 選出
	首页 探针管理 > 设备管	絵題 → 黒/白名牟絵語 「互连关系 → 报表中心 → 系统管理 →
G氟碱器。安全加亚文		澤加下敬史全城 是四是歐宗先統: ● 2 ○ 四 全立成本称: 上 山谷称: 「建立成本称: 正 「「「「」」」」 「「」」」 「「「」」」」 「」」」 「「」」」」 「」」」 「「」」」」 「」」」 「「」」」」 「」」」 「「」」」」 「」」」 「「」」」」 「」」」 「「」」」」 「」」」 「「」」」」 「」」」 「「」」」」」 「」」」」 「「」」」」」」 「」」」 「」」」」 「」」」 「「」」」」 「」」」 「「」」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」 「」」 「」」 「」」」 「」」 「」」 「」」 「」」」 「」」」 「」」」 「」」」 「」」」 「」」 「」」 「」」 「」」」 「」」 「」」 「」」 「」」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」」 <tr< td=""></tr<>

通过在菜单中编辑[是否是业务系统]、[安全域名称]、[上级名称]、[描述]来建立符合自己的安 全域,如下图所示:

是否是业务系统: 🛡 是 🔍 否		
安全域名称:	上级名称: 整合网	
描述:		
	添加清空	

2. 修改安全域

用户可点击选中安全域后右侧菜单"当前安全域"的修改按钮进行修改操作,如下图所示:

			- 当前安全城				
			安全域名称:WLAN本地认证系统	充	描述:	WLAN本地认证系统	
				删除	修改		
3.	删除	安全	域				

用户可点击选中安全域后右侧菜单"当前安全域"的删除按钮进行删除操作,如下图所示:



• 业务系统定义

业务系统定义,是用于对业务系统名称进行定义和维护。用户点击"设备管理"-"业务系统 定义"后,可以进入操作页面,如下图所示:

业务系统列表						
□±8	接着	系统装载	energia	INIE	1815	
	1	USG	2013-08-17 09:22:88	USG	Ø×	
	2	A55	2013-08-17 09:22:30	A受统	Øx	
			< 共2会教研 页次1/1页 1 >			

1. 添加业务系统

用户可通过手动添加业务系统名称,建立符合自身需要的业务系统名称,如下图所示:

务系统名称: 例	彩铃001	描述:	请添加描述	<u>^</u>		
				~	添加	
	1.1014 001			~	添加	

2. 修改业务系统

如果需要更改业务系统的名称,点击需要修改条目[操作]栏的 按钮,将弹出如下的修改窗口:



在此弹出框中修改业务系统的名称,修改后点击[确定]按钮,完成业务系统名称的修改。

3. 删除业务系统

页面中显示了已经生成的业务系统列表,用户可通过点击"删除"按钮,对不需要的项目进行 删除操作,如下图所示:

─ 潘加业务系统 ⇔一					
业务系统列表	>				
厂全选	序号	系统名称	创建时间	描述	操作
E C	1	USG	2013-08-17 09:22:38	USG	Ø×
Π.	2	A系统	2013-08-17 09:22:30	A系统	Øx
			* statesting block/ing is Findows Internet Explorer 区 (2) 输入要相除法业务系统信息公?		

设备管理

设备管理包括当前监测范围下的未知设备和已知的、赋予设备属性的正常设备。

1.未知设备

用户通过点击"设备管理"-"设备管理",可进入"未知设备"的管理页面。未知设备如下 图所示:

			保针管理 ¥	设备管理 🛛 黒/白名单管理	┃ 互连关系 > 报表中心 > 系统	K∰ ≮
设备管理> 设备管理	未知设备列表	>				
设备资源	□ 全选	序号	地址组	IP地址	发现时间	操作
WLAN本地认证	Г	1	N/A	18.0.0.10	2013-07-29 17:00:45	e
ARIE	E	2	N/A	18.0.0.9	2013-07-29 17:00:45	e
test1	Г	3	N/A	18.0.0.8	2013-07-29 17:00:45	e
test2	E	4	N/A	18.0.0.7	2013-07-29 17:00:45	e
🗂 test3		5	N/A	18.0.0.6	2013-07-29 17:00:45	e
🗖 test4	Г	6	N/A	18.0.0.5	2013-07-29 17:00:45	e
地址类型: 旧地址 💟	F	7	N/A	18.0.0.4	2013-07-29 17:00:45	C
	Г	8	N/A	18.0.0.3	2013-07-29 17:00:45	e
所屬安全域:	Г	9	N/A	18.0.0.2	2013-07-29 17:00:45	e
设备关型:	E	10	N/A	18.0.0.1	2013-07-29 17:00:44	e
公留型号:				< 共10条数据 页次1/1页	11>	
**						
						t量转为正常设备

未知设备列表包括: IP 地址信息和设备发现时间。

2.未知设备转为正常设备

用户可通过点击"操作"按钮,将未知设备转为正常设备,如下图所示:

安全域流量监管系统 14 使用手册

设备名称: Dev	-79640389191	IP地址:	18.0.0.10	设备型号:		
所属业务系统:	~	所属安全域:	流量监管系统 🕑	设备类型: 一般)	铲 💟	

用户可以进行"全选"操作后,点击 知设备批量转为正常设备,如下图所示:

批量转为正常设备

按钮,将当前页面下的所有未

所属业务系统:	所属安全域: 流量监管系	统 🔽 设备类型: 一般资产 🔽 设备型号:
IP地址	地址组	设备名称
18.0.0.10	N/A	Dev-32324845263
18.0.0.9	N/A	Dev-11331436139
18.0.0.8	N/A	Dev-49444202229
18.0.0.7	N/A	Dev-66386842902
18.0.0.6	N/A	Dev-25569043764
18.0.0.5	N/A	Dev-30374883600
18.0.0.4	N/A	Dev-83325377557
18.0.0.3	N/A	Dev-19369264824
18.0.0.2	N/A	Dev-98925137363
18.0.0.1	N/A	Dev-48938587858

3.正常设备

点击页面中右侧的"正常设备"按钮,可显示当前系统中的正常设备,用户可以对这些设备进 行操作,也可以手工新增一台或一组设备。正常设备列表如下图所示:

设备管理> 设备管理	┌─添加	安全城	[设备 ♀						
设备资源 浮业驾系统 ◆ ◆		常设备	列表						
III WLAN本地认证	(三全法	序号	设备名称	设备类型	沒 쓸ᆋ통	IP地址	所属业务系统	所属安全域	操作
A系统		1	Dev-77176874022	一般资产	test123	10.19.71.3	WLANTSKIE	整合网	Ø×
testl		2	Dev-44153645232	一般资产	test123	10.19.71.4	WLAN本地认证	整合网	@×
test2		3	Dev-67492921684	网管采集机	cisco3500	10.19.71.5	test3	CMNET	@×
test3		4	集团客户超级管理员	一般资产	APV 3520	172.168.0.150	WLAN本地认证	WLAN本地认证系统	@×
test4	10	5	BJBJ-PS-WLAN-AW01	一般资产	APV 3520	172.168.3.4	WLAN本地以证	WLAN本地认证系统	@×
		6	BJBJ-PS-WLAN-SW02	一般资产	s5500	172.168.2.5	WLAN本地以证	WLAN本地认证系统	@×
·····································	10	7	BJBJ-PS-WLAN-SW01		\$5500	172,168,2,4	WLANASSUE	WLAN本地认证系统	@×
i腥安全域:		8	BIBI-PS-WLAN-FW02		fw1000	172,168,3,3	WIANTHUF	WIAN本地认证系统	RX
海美型:		9	BIBI-PS-WI AN-FW01		6×1000	172 168 3 2	WIANTHELLE	WIANTHUGE	RX
· 倫型号 :		10	BIBLOS WI AN Self02		IBMH22	172.168.0.202	WIANTERIG	DM7	RX
查询 清空				< 共65条数据	页次1/7页 1	2345下-	-页 尾页 >	批量修改	批量删除

正常设备列表包括:设备名称、设备类型、设备型号、IP 地址、所属业务系统和所示安全域。 用户可通过点击"操作"中的修改和删除按钮,对设备信息进行修改或删除该设备。

修改设备信息如下图所示,用户可修改设备名称、所属业务系统、所属安全域、设备类型和 设备型号字段。备信息进行修改或删除该设备。

设备名称: Dev-77176874022 所属业务系统: WLAN本地认证 ▼ 所属安全域: 整合网 ▼ 设备类型: 一般资产 ▼ 设备型号: test123	修改设备		>	•
 所属业务系统: WLAN本地认证 所属安全域: 整合网 设备类型: 一般资产 设备型号: test123 	设备名称:	Dev-77176874022		
所属安全域: 整合网 ▼ 设备类型: 一般资产 ▼ 设备型号: test123	所属业务系统:	WLAN本地认证	-	
设备类型: <u>一般资产</u> ▼ 设备型号: test123	所属安全域:	整合网	-	
设备型号: test123	设备类型:	一般资产	-	
	设备型号:	test123		
		关闭	确定	

删除设备,点击"删除"按钮后,可删除当前的设备,如下图所示:

Vindows Internet Explorer	
确认要删出设备名为: Dev-77176874022该条信息么?	
确定 取消	

用户也可以通过全选、多选操作,批量对设备进行修改或删除。

4.设备的导入

如果遇到大量的设备信息需要导入,需要使用"导入"操作完成,以节省设备信息填写的时间。

批量导入设备到安全域			ډ
设备文件:	浏览	导入	导入设备模版下载
			关闭

用户点击"批量导入设备"按钮后,如下图所示:

如果是第一次操作,那么需要通过点击"导入设备模板下载"按钮下载设备模板,用户在填写 模板后,点击"浏览…"选择要导入的文件,然后点击"导入",即可完成设备的批量导入操作。 5.设备的导出

用户在点击"正常设备导出"按钮后,即可将当前所有正常设备信息下载到本地,文件格式为 xls。

地址组管理

地址组管理,是允许用户通过添加地址组的方式,对一组设备进行定义。用户点击"设备管理"-"地址组管理"后,如下图所示:

		首页 探针管理 🗸	设备管理 👻 黒/I	白名单管理 互连关系	★ 报表中心:	≠ 系统管理 ¥	
设备管理 > 此证相管理	355 fm kit 14.00						
	地址组名称:		开启分组显示: 🔽 外部	地址排除该范围: 🔲 对该	范围内设备进行梳理	: V	
地址组查询	地址类型: IP网段	×	所屬安全域:	▼ 所属业务系统	ē:	v	
业组名称:	192.168.10.56 / 2	255.255.255.0	地址组模述:			減加	
始IP地址:							
床IP地站:	地址组列表						
查询 清空	下全 废号 地址组名称地址	类型 IP地址	子网绳码	所属安全域 所属业务系统	描述 分组显示	外部地址排除 设备梳理	操作
	T 1 test IPM	現段 172.165.9.0	255.255.255.0	test180 test200	开启	不排除 梳理	2 × 1
			< 共2条数据 页次				

1. 添加地址组

用户可通过手动添加和选择地址组名称、开启分组显示、外部地址排除该范围、对该范围内 设备进行梳理、地址类型、所属安全域、所属业务系统、地址组描述字段进行添加地址组操作,如 下图所示:

地址组名称:		开启分组显示: 🔽	外部地址排除该范围: 📃 对该范围	内设备进行梳理: 🔽
地址类型: IP网段	~	所属安全域:	▼ 所属业务系统:	~
192.168.10.56	/ 255.255.255.0	地址组描述:		
				nt ac

安全域流量监管系统 ¹⁷ 使用手册

分组显示: 当选中"分组显示"时, 在互连关系的呈现中选择地址组归并时会按地址组进行 归并显示。

外部地址排除该范围:外部地址使用反向逻辑进行定义,范围为:除所有选中"外部地址组 排除该范围"选项的地址组之外的地址(如下图),外网地址范围的地址不会进入"未知设备"。



如系统中没有定义任何"地址组",则全部地址都认为是"内部地址",且全部需要梳理,所有地址都会进入"未知设备"列表

对该范围内设备进行梳理: 当选中"对该范围内设备进行梳理",如相关 IP 没有在"正常设备"在安全域中定义,则该地址会进入"未知设备"列表,否则不会进入"未知设备"。

2. 修改地址组

用户可通过	^也 点击地址组列表操作中的	"修改"按钮	Ø,	弹出修改窗口,	如下:
	修改设备地址组			×	
	│ 开启分组显示: 🔲 外部地址排除该范围: 📕 🤉	对该范围内设备进行梳理:	V		
	地址组名称: 1.1.1.1 月	所属安全域:	¥		
	所属业务系统:	茵述:			
	地址类型: IP网段 🗸				
	192.168.10.0 /255.255.255.0				
	L				
		关闭	确定		

在地址组弹出窗口中,可以对地址组名称、开启分组显示、外部地址排除该范围、对该范围 内设备进行梳理、所属安全域、所属业务系统、地址组描述等字段进行修改。

3. 删除地址组

用户可通过点击地址组列表操作中的"删除"按钮 , 会有如下提示弹出框, 点击[确定]完成 地址组的删除。

黑白名单管理

用户可以根据清晰、明了的安全域结构树,对安全域进行添加、修改、删除的管理操作。

1. 域间互访策略

点击导航栏的黑/白名单管理按钮,可进入域间互访策略页面,如下图所示:



添加域间互访策略

用户通过手动添加源业务系统、源安全域、目标业务系统、目标安全域、优先级、合规性和 描述进行添加域间互访策略操作,如下图所示:



策略命中后,可看到当前命中策略的互连关系数量,点击数量后,可查看命中该策略的互连 关系,如下图所示:

域间互访梦	育略列表									
厂全选	序号	源域	源业务系统	目标域	目标业务系统	优先级	合规性	描述	命中次数	操作
	1			DMZ		÷	违规		P	19
Г	2	Inside		DMZ		裔	合规		Q	6)
				< 共2	微据页次1/1页 1 >					

用户可通过点击操作列的应用到探针按钮,将策应用到相应的探针上。

应用到探针

批量删除

用户在点击"导出全部"按钮后,即可将当前所有域间互访策略信息下载到本地,文件格式为 xls,如下图所示:



用户也可以通过全选、多选操作,批量对策略进行应用,如图:

用户也可以通过全选、多选操作,批量对策略进行批量删除,如图:

2. 自定义白名单

用户点击右侧"自定义白名单"后,可进入白名单管理页面,如下图所示:

黑/白名单管理	- 1		自定义	自名单 ○						_					
白名单查询			原业务	519 :		~	源地址关型:	IP地址 🞽		- 1	源))(日:				
经业务系统 ◆ ◆			目标业	务系统:		×	目标地址美型:	IP地址 🞽	_	- 11	目标端口	-			
A系统						*	合规性:	合規 🚩 描述:			添加原因				
tert200													nt äli		
test210				-											
l安全域: 💌		HÆX	(目名	早列表											
标安全域:		厂全选	序号	潭业务系统	源地址	源決口	目标业务系统	8 目标地址	目标通口	协议	合规性	操作人	操作原因	操作	
はは、日本地 🗹		-	1								合规	Admin	d	SOX	
	遊		2								合规	Admin	12	SOX	
xx: <u>⊻</u> R#□:	Ľ.	-	3	A系统	1.1.1.1	1111	A系统	2.2.2.2	2222	HTTP	合规	Admin	1	SOX	
标满口:							<共	3条数据 页次1/1页	1 >						
語合規: 💙															
麦询 清空											导出	全部	应用到探针	批量删除	





用户通过填写源业务系统、源地址类型、源地址信息、源端口、目标业务系统、目标地址类型、目标地址信息、目标端口、协议、合规性、描述信息和添加原因,完成白名单的创建。

修改白名单

如果需要对已添加的用户进行修改,则在用户条目操作中点击 ,将弹出用户修改窗口,如 下图:

原业务系统:	A系统	~	源地址类型:	IP地址	2 1.1.1.1	源第日:	1111		
目标业务系统	A系统	~	目标地址类型	IP地址	2222	目标跳口	: 2222		
幼议:	HTTP	~	合规性:	合規	×	振述:	22		

删除白名单

用户可通过白名单中操作中的删除按钮,完成白名单的删除。用户也可以通过全选、多选操作,批 量对白名单进行删除,如图:

应用到探针

用户通过点击"应用到探针"按钮,将选定的白名单应用到探针。选定一个白名单后,点击



源城:		月标城:	∭0⊺P:	172.168.1.201	
目标IP: 172.168.2.	.54	渡端口:	目标端口:	4600	
协议:		合规性: 合规	描述:	转换为白名单	
□ 全选	序号	探针名称		探针软件版本	
	1	Dolphin_222		2.2.0.4948	

用户在选择所要应用的探针时后,点击"确定"即可完成操作。

如果需要将多条白名单进行同步,用户可通过全选、多选操作,批量将白名单应用到探针,

如图: 应用到探针

导出全部白名单

用户在点击"导出全部"按钮后,即可将当前所有白名单信息下载到本地,文件格式为 xls。

互连关系管理

• 互连关系查询

用户点击"互连关系管理"-"互连关系查询"后,可进入互连关系查询页面。这里显示的是正常设备的互连关系,如下图所示:



页面左侧是查询条件输入界面,查询条件包括连接开始的时间、连接结束的时间、是否合规、 业务系统、源安全域、目标安全域、源端口、目标端口、源地址类型、源地址、目标地址类型、目 标地址、协议和处理状态。

右侧则显示的是互连关系的查询情况,查询结果可根据源 IP、源 IP+目标端口、目标 IP+目标 端口、目标端口、地址组、协议的方式进行归并显示。

点击 "导出" 按钮,将已经选择的二级条目导出,导出的条目的数量不能超过 TOP 限制的数量。

点击"导出全部"按钮,导出的条目以连接频次倒序排序,数量不能超过 TOP 限制的数量。 点击"批量转化白名单"按钮,将已经选择的二级条目,批量转换为白名单。

点击"标记为处理中"按钮,将"处理状态"为未处理的条目,标记为处理中。

在二级条目中,点击 ² 按钮,将会在弹出框中显示当前时间之前 24 小时内该条目的原始会 话。

在二级条目中,点击 C 按钮,将会在弹出框中显示当前时间之前 24 小时内该条目的原始会 话。

在二级条目中,点击已按钮,将会更改已经选择的二级条目的处理状态。

注: 该页面中默认显示的条目为一级条目, 当点击一级条目会展开显示其下的二级条目。

互连关系图

互连关系图将在安全域定义的各个安全域之间发生的互连关系情况,以可视化的图展现出来。 这样可以更加直观的让用户清晰的了解到网络中安全域之间的访问情况。

互连关系查询-互连关系图展示如下:



• 未知互连关系

用户点击"互连关系管理"-"未知设备互连关系"后,进入未知设备的互连关系查询页面, 如下图所示:

		首页 探	针管理 × 设备管目	!× 黑/白名单管理	互连关系 >	服表中心 ¥	系统管理 ×	
互连关系 > 未知互连关系								
	未知互连关系列表							
未知互连关系查问	归并方式: 目标端口	🗸 ТОР :	100 💌					
接时间:2013-11-06 15:06:17	□全场		序号		目标演口		连接数	
課时间: 2013-11-07 15:06:17			1		3306		1	
2务系统: ====			2		22		1	
2全城: ====请选择====			2		442		1	
1标准口:				and the second second	445		-	
即地址美型: IP地址 🔽				共3號数量 贝次1/1贝				
					登出	导出全部	批量转为正常设备	标记为处理中
目标地址类型: IP地址								
加以: 全部 🚩								
出理状态: 未处理 🔽								
三连単型: 未知 🖌								
查询 清空								

右侧则显示的是未知互连关系的查询情况,查询结果可根据源 IP、源 IP+目标端口、目标 IP+ 目标端口、目标端口、地址组、协议的方式进行归并显示。

点击"导出"按钮,将已经选择的二级条目导出,导出的条目的数量不能超过 TOP 限制的数量。

点击"导出全部"按钮,导出的条目以连接频次倒序排序,数量不能超过 TOP 限制的数量。 点击"批量转为正常设备"按钮,将已经选择的二级条目,批量转换为正常设备。 点击"标记为处理中"按钮,将"处理状态"为未处理的条目,标记为处理中。 在二级条目中,点击 ^②按钮,将会在弹出框中显示当前时间之前 24 小时内该条目的原始会

话。

在二级条目中,点击 C 按钮,将会在弹出框中显示当前时间之前 24 小时内该条目的原始会 话。

在二级条目中,点击已按钮,将会更改已经选择的二级条目的处理状态。

注: 该页面中默认显示的条目为一级条目, 当点击一级条目会展开显示其下的二级条目。

• 基础管理类互连

用户点击"互连关系"-"白基础管理类互连"后,进入基础管理类互连页面,如下图所示:

			政格管理 ∀ 第/白名单管理	互換关系 マ	8890 v	新统管理 🗸	
石达关系 > Main的关石法	March Barris MA						
基础管理支互连条件	\$1并方式: 算样端口	TOP : 100					
HER109 : 2013-11-06 15:06:44	Tet.	7 4	E1508C		米田町		新作
ARDIN : 2013-11-07 15:06:44	• +	1	443		1		œ
anna (1997) : ★ (1) \% (1) \%			< 共12333 页次1/1页 1 >				
(金城:灌西将				50 H	17H12# 1	化晶体为白名单	你记为处理中
9640							
malenti : IPMal 🖌							
ingalouti : IPikal							
112.: 소비 🔽							
記状态: 未处理 🕑							
始建就态: 未处理 👱 2位关系: 未知 👱							

白基础管理类互连是将所有非一般资产的互连关系展示在此列表中,通过源 IP、源 IP+目标端 口、目标 IP+目标端口、目标端口和地址组的方式进行归并显示,可以显示 top100-1000 条互连关系。 页面左侧是查询条件输入界面,查询条件包括连接时间、结束时间、业务系统、源安全域、

目标安全域、源端口、目标端口、源地址类型、源地址、目标地址类型、目标地址和协议。

点击"导出"按钮,将已经选择的二级条目导出,导出的条目的数量不能超过 TOP 限制的数

量。

话。

点击"导出全部"按钮,导出的条目以连接频次倒序排序,数量不能超过 TOP 限制的数量。 点击"批量转为正常设备"按钮,将已经选择的二级条目,批量转换为正常设备。 点击"标记为处理中"按钮,将"处理状态"为未处理的条目,标记为处理中。

在二级条目中,点击 🔎 按钮,将会在弹出框中显示当前时间之前 24 小时内该条目的原始会

在二级条目中,点击 C 按钮,将会在弹出框中显示当前时间之前 24 小时内该条目的原始会 话。

在二级条目中,点击 会按钮,将会更改已经选择的二级条目的处理状态。

注: 该页面中默认显示的条目为一级条目, 当点击一级条目会展开显示其下的二级条目。

• 原始会话

用户点击"互连关系"-"原始会话"后,进入原始会话页面,如下图所示:

互连关系 > 原始会话音询		始会话列表													
原始会话查询	厂全活	潜止的系统 漂水	8 (#1512	澤油口	目标业务系统	864	Blinut	BISMO	建立时间	inite to the	使用他议	会现性	上行沈重	下行沈晨	\$6
时间: 2013-08-21 00:00:00	C 1		192.168.20.9	51897			163.177.65.157	25	2013-08-21 16:54:09	10.0	SIMTP	未知	1273	5092	₽ ±
RTR 2013-08-21 17-05-01	E.		111.161.52.179	8000			192.168.20.9	4000	2013-08-21 16:54:09	30.0	UDP	未知	0	2689	₽ ±
-4-10 -	E.		8.8.8.8	53			192.168.20.9	62621	2013-08-21 16:54:09	30.0	DNS	未知	0	79	Ρ±
	Г		8.8.8.8	53			192.168.20.9	55416	2013-08-21 16:54:09	30.0	DNS	未知	0	107	₽ ¥
<u> </u>			8.8.8.8	53			192.168.20.9	61132	2013-08-21 16:54:09	90.0	DNS	未知	0	122	ρ±
	F		8.8.8.8	53			192.168.20.9	50910	2013-08-21 16:54:09	30.0	DNS	未知	0	80	₽ ±
	Π.		112.90.85.197	8000			192.168.20.9	62622	2013-08-21 16:54:09	30.0	UDP	未知	0	122	Ρ±
an 🗆 :	F		192.168.20.9	54629			8.8.8.8	53	2013-08-21 16:54:09	180.0	DNS	未知	148	70	₽ ±
1	1		192.168.20.9	50974			8.8.8.8	53	2013-08-21 16:54:09	180.0	DNS	未知	216	126	₽ <u>¥</u>
P1	E.		172.16.1.120	137			172.16.1.8	137	2013-08-21 16:53:08	30.0	UDP	未知	0	96	₽ ±
					共202年取録	页次1/	21页 1 2 3 4		78910下-页第	LUI >					

原始会话列表是将源地址和目标地址为 IP 地址的互连关系展示在原始会话列表中,列表的列 字段包括:有源业务系统、源域、源地址、源端口、目标业务系统、目标域、目标地址、目标端口、 建立时间、持续时间、使用协议、合规性、上行流量、下行流量和合规性。 页面左侧是查询条件输入界面,查询条件包括连接时间、结束时间、是否合规、源域、目标 域、源端口、目标端口、源 IP、目标 IP 和协议。

点击操作中的"显示协议信息"按钮,如图: 🔎 ,会弹出对话框显示该会话的协议解析内 容。

点击操作中的"下载 payload"按钮,如图: 👱 ,将探针抓包获取的 payload 文件从服务 器下载到本地。

点击"导出"按钮,将导出全部原始会话。

互连关系管理

- 白名单报表
- 1. 白名单列表

点击"报表中心"-"白名单报表"即可进入白名单报表页面,如下图所示:

		首页:	¥针管理 ¥ i	86倍强 *	黑/白名单智	理 互连关	tativ na	表中心 ¥	系统	1918 ¥			
服表中心 > 白名单报表	* 白名单列表	>											
报表查询	连接建立时间	源业务系统	源IP	源地址设备	目标业务系统	目标IP	目标地址设备	目标跳口	协议类型	确认操作账号	确认原因	连接持续时间	产生流
2013-08-01 14:48:40	2013-08-17 21:49:15	WLAN本地认证	192.168.10.100			58.63.236.225		80	TCP			10	9286
时间: 2013-08-20 14:48:40	2013-08-17 21:49:15	WLAN本地认证	192.168.10.100			58.63.236.225		80	TCP			10	9286
K-2:	2013-08-17 21:49:15	WLAN本地认证	192.168.10.100			58.63.236.225		80	TCP			10	9286
4.3.	2013-08-17 21:49:15	WLAN本地认证	192.168.10.100			58.63.236.225		80	TCP			10	9286
122请选择	2013-08-17 21:49:15	WLAN本地认证	192.168.10.100			58.63.236.225		80	TCP			10	9286
	2013-08-17 21:49:15	WLAN本地认证	192.168.10.100			58.63.236.225		80	TCP			10	9286
	2013-08-17 21:49:15	WLAN本地认证	192.168.10.100			58.63.236.225		80	TCP			10	9286
	2013-08-17 21:49:15	WLAN本地认证	192.168.10.100			58.63.236.225		80	TCP			10	9286
⊉: ⊻	2013-08-17 21:49:15	WLAN本地认证	192.168.10.100			58.63.236.225		80	TCP			10	9286
** **	2013-08-17 21:49:15	WLAN本地认证	192.168.10.100			58.63.236.225		80	TCP			10	9286
				< 共72章	鐵選页次1/8]		5 下—页 5	四 >					
	> 招表外理终于												EV.CE

白名单列表列出筛选后的白名单统计报表,包括:连接建立时间、源业务系统、源 IP、源地 址设备、目标业务系统、目标 IP、目标地址设备、目标端口、协议类型、确认操作帐号、确认原因、 连接持续时间和产生流量等。

报表查询可以对白名单列表进行筛选,可筛选项:包括建立时间、结束时间、操作账号、业务系统、源 IP、目标 IP 和协议类型。

2. 报表处理格式

点击下方报表处理格式按钮,可切至报表处理格式页面,如下图所示:

更用·	于	1	ij	
-----	---	---	----	--

			1911111 v	设备管理 👻	黑/白客	약한팬 E	這美縣 ♥	报表中		系统管理	l v			
报表中心 > 白名单报表														
报表查询	▶ 白名单列表													
Tethe 2013-08-01 15-03-52	*报表处理格式										нтм		PDF	EXCE
2013-00-01 13:03:32							155222			19.75				
期间: 2013-08-20 15:04:20	· 通报建立时间	1 課业务兼职	(# 1 P	源地址设备	#177.477 統	貫标IP	#17-12-21 K	- 02 AR	协议类型	941153CL	時认原因		- <u>2</u> m	
	14:59:97		192.168.10.100			192.168.10.20	10	21	TCP			2	1821	
186.91	2013-08-19 14:06:24		192.168.10.100			183.60.187.4	1	80	TCP			3128	20388	
	2013-08-19 14:06:24		192.168.10.100			202.108.33.6	0	80	TCP			3120	1392	
5.5t.5To	2013-08-19		192.168.10.100			0.0.0.0		53	UDP			180	418	
P:	2013-08-17	WLANTEN	192.168.10.100			203.90.242.12	12	80	TCP			10	2458	
	2013-08-17	WLAN本地认	192.168.10.100			124.192.205.1	50	80	TCP	-		10	14871	
RIP:	21:49:15 2013-08-17	12 MLAN本地认	102 148 10 100			104 100 004 0		80	700	<u> </u>		10	87184	
	21:49:15	证 MLAN本他认	192.100.10.100						107	-			07204	
(美型: 💙	21:49:15	1	192.168.10.100			58.63.236.33	·	80	TCP	<u> </u>		10	2464	
	21:49:15	EXERCISIV.	192.168.10.100			111.161.68.23	15	80	TCP			10	1936	
查询 清空	2019-08-17 21:49:15	WLAN本地认 這	192.168.10.100			58.62.226.22	5	80	TCP			10	92862	
	2012-08-17	WLAN X HOW	192.168.10.100			124.199.205.1	41	80	TCP			10	11809	
	2019-08-17	WLAN本地认	192.168.10.100			58.62.226.42		80	TCP	<u> </u>		10	5023	
	21:49:15 2012-08-17	u MLAN本地认	100 160 10 100			104 100 005 0	41	80	202	-		10	4804	
	21:49:15	11 X 2 4 1						**		<u> </u>				
	21:49:15	1	192.168.10.100			198.47.108.4	2	80	TCP			10	2815	
	2013-08-17	STURN TO A	192.168.10.100			202.108.43.16	50	80	TCP			10	551027	
	2019-08-17 21:49:13	WLAN本地认 证	192.168.10.100			58.63.236.47	,	80	TCP			10	30326	
	2013-08-17	WLAN × 地议	192.168.10.100			55.63.236.40		80	TCP			10	60028	

报表处理格式可以分为 HTML、PDF 和 EXCEL 的格式进行显示,按钮如图:

HTML PDF EXCEL

黑名单报表

1. 黑名单列表

点击"报表中心"-"黑名单列表"即可进入黑名单报表页面,如下图所示:

* 王久兰列表	皆页	保针管理	¥ i£\$11	1.1.1 1.1.1	单管理	互连关系 ¥	报表中	0¥	系统管理 ¥			
* 医火单列表												
王久兰刊表												
	>											
连接建立时间	源业务系统	源IP	源地址设备	目标业务系统	目标IP	目标地址设备	目标独口	协议类型	确认操作账号	确认原因	连接持续时间	产生活
2013-08-19 10:54:45	管理网	10.9.3.3		WLAN本地认证	10.16.2.2		21	TCP			120	92
					1条数据页》							
	3.009.02.0910	1289年8月2月1日 2013-08-19 10:5445 繁濃時	1889年18月1日 #1825年8月1日 109-33 2013-08-19 10:54:45 第日日日 10:9-33	12996日2019日 2013-08-19 10:5645 新聞所 10.0-3.3	12013-08-19 10:5445 新聞戸 10:93.3 中日2015年65 2013-08-19 10:5445 新聞同 10:93.3 中日2015年65 - 元	1326年6月22日前日 前日255,665 6月9 1月75日(2017) 2013-08-19 10:5445 管理時 10:93.3 WHAN 年時以上 4月16年8月1日 - 月16年8月1日 - 月16日 - 月175 - 月17	1999年11月29日。 #25125年855 2019 #1952年25455 日初の上記455 2013-08-19 10:5445 新聞同 10:933 WILAN+1世知以正 10:16:22 ・共日来政策 同次は12页 1 ・	12日本語(11月前日) 第三日本時代 部グ 第三日本時代 日本日日本 日本日日本 日本日本日本 日本日本日本 日本日本日本日本日本日本	13時間近か時 新たびを放ち 新か 新たびた新 11日2005 新日 11日2012 11日 11日2012 11日2012 11日 11日 11日 11日 11日 11日 11日 11日 11日 1	12013-08-19 105645 800 部プ 単位24100 目目125655 目目727 目目125655 目目727 目目125645 1050242 単体2415755 2013-08-19 105645 第1前前 109033 WHANESENUE 10.16.2.2 21 TCP ・月16年50日前の21/237 】 ・	王朝帝國之政時間 第七章の後的 第5 前年では、第十年前日の「新行政之政務局」前付か「新行政之政務員」前付前川」等以の定義 第七時前川 第50年代表 第七時前日 10.05-20 201 10-05-19 10-56-45 第三時間 10.9.3.3 WILAN 本市が以至 10.16-22 21 TCP ・ 「日本市政 国家 日本市政 日本市政 日本市政 日本市政 日本市政 日本市政 日本市政 日本市政	12日本品は2月1日 2月22日本部 2月19日 2月11日 日本11日2日本部 日本11日 日本11日日本 日本11日日 日本11月日 日本11日日 日本11月日 日本11月日 日本11月日 日本11月日 日本11月日 日本11月日日

黑名单列表主要用于显示筛选后的黑名单统计报表,包括连接建立时间、源业务系统、源 IP、 源地址设备、目标业务系统、目标 IP、目标地址设备、目标端口、协议类型、确认操作帐号、确认 原因、连接持续时间和产生流量。

报表查询可以对黑名单列表进行筛选,可筛选项包括建立时间、结束时间、操作账号、业务 系统、源 IP、目标 IP 和协议类型。

2. 报表处理格式

点击下方报表处理格式按钮,可切至报表处理格式页面,如下图所示:

26 安全域流量监管系统 使用手册

 用名单列表 报表处理格式 进资用工作用 													
 第二百年列表 第条处理格式 #39世교行向 #39世교行向 1000000000000000000000000000000000000													
* 报表处理格式 进资度正时间													
进投建正时间										нтм		PDF	EXCEL
进投建立时间											and the second		
2018-00-19	原业务系统	8229	源地软化备	1728A	■ 枳 エ₽	H TO TALK		防保典型	95 (1438) 	得认原因。	S ST AT	1 <u>- 3</u> at	
17:10:20 2010-20-19	1	2.160.10.110			172.16.1.15		1205	707			120	1209	
2013-00-19 00:08:21	2	2.165.10.110			172.16.1.15		1234	TCP			120	1229	
	POLY 12	P00+8-13 1	2015-92-33 2019-33 102-349-32-339	2017/213 2019/02 2019/	2633223 6938223 1942 1943 1943 1943 1943 1943 1943 1943 1943	2210023 142.145.22.33 172.145.2.35	2639923 393923 199323	2010023 100.00.00.00	192.246.3.35 192.358 192 991928	2692923 149.345.15.337 179.346.3.3	201923 146.10.333 172.345.1.35 1278 729	1999-193 1999-193 1999-193 199-194 190	2010/03 100.000.01 100.000.01 100.000.00

报表处理格式可以分为 HTML、PDF 和 EXCEL 的格式进行显示, 按钮如图:

HTML	PDF	EXCEL

灰名单报表

1. 灰名单列表

点击"报表中心"-"灰名单列表"即可进入灰名单报表页面,如下图所示:

			-							*	
		首页 探针管	理 ¥ 设备管理	[¥ 累/白;	5年管理 互连	送版 ¥ 报表	中C ¥ 系	统管理 ¥		_	
报表中心 > 灰名单报表											
报表查询	* 灰名单列表	7									
thetill 2012-09-01 15:25:10	连接建立时间	漂业务系统	源IP	源地址设备	目标业务系统	目标IP	目标地址设备	目标端口	协议类型	连接持续时间	产生》
2013-00-01 13:23:10	2013-08-17 19:00:27	WLAN本地认证	192.168.10.223		WLAN本地认证	192.168.20.15		4965	TCP	43199	24
東时间: 2013-08-20 15:25:10					电1条数据 页次1/1页						
B系统 ====诸选择====											
IP:											
φīP:											
2类型:											
春油 清空											

灰名单列表主要用于展现筛选后的灰名单统计报表,包括:连接建立时间、源业务系统、源 IP、源地址设备、目标业务系统、目标 IP、目标地址设备、目标端口、协议类型、确认操作帐号、 确认原因、连接持续时间和产生流量。

报表查询可以对灰名单列表进行筛选,可筛选项:包括建立时间、结束时间、操作账号、业 务系统、源 IP、目标 IP 和协议类型。

2. 报表处理格式

点击下方报表处理格式按钮,可切至报表处理格式页面,如下图所示:

安全域流量监管系统 ²⁷ 使用手册

🕑 安全域流量监	管系统 v2.2.0	.5678						a : Admin 💮	系统时间	: 2013-08	20 15:25:4	2 🔕 🕫 🛪 🛙	弱 (し) 温出
		首页	採针管理。	, ig s t	!理 ¥ 黒/自	名单管理	互连关系 ¥	报表中心 ¥	, B	统管理 ¥			
报表中心 > 灰名单报表	<u> </u>	_											
报表查询	× 41 + 71 4												
时间: <mark>2013-08-01 15:25:10</mark>	报表处理价	x									TML	PDF	EXCEL
时间: <mark>2013-08-20 15:25:10</mark>	道道	受建立时间	源业务展现	@IP	標地社役各	目标业务系统	首根IP	目标地址设备	目標期日	协议类型	递接持续时	同声生流	
系统 ====请选择====	20	19:00:27	WLAN本地认证 192	.160.10.223		NLAN本地认证	192.160.20.15		4965	TCP	43199	240	
P:													
470): 🔍													
별며 개오													

报表处理格式可以分为 HTML、PDF 和 EXCEL 的格式进行显示,按钮如图:

HTML PDF EXCEL	
----------------	--

- 互连关系查询报表
- 1. 互连关系列表

用户点击"报表中心"-"互连关系查询报表",可进入互连关系查询报表页面,如下图所示:

🕐 安全域流量监管	音系统 v2.2.0.5678					1 100月户: Ad	lmin 🕜 \$168			13 🔘 Baker	د ال الله ال
		879 9 79	158 v 285	BE ¥ 25/6	1名单管置	互渔关联 ♀	6840 v	¥朱岱王 ▼			
报表中心 > 互连关系应该报表											
形表立力	* 当地天景列表										
Prest 0000 0000 00 00 0000	這個建立时间	源业资料统	10 P	源地社设教	目标业务系统	用板IP	用标地进设种	REMO	他以美国	這時時候时间	产生法量
2012-00-01 15:20:05	2013-08-19 14:06:24		192.168.10.100			202.108.33.60		80	TCP	3128	1392
CHESTER 2013-08-20 15:26:05	2013-08-19 14:06:24		192.168.10.100			202.108.33.60		80	TCP	31.28	1392
ava 20.44	2013-08-19 14:06:24		192.168.10.100			202.108.33.60		80	TCP	3128	1392
	2013-08-19 14:06:24		192.168.10.100			202.108.33.60		80	TCP	31,28	1392
RDP:	2013-08-19 14:06:24		192.168.10.100			202.108.33.60		80	TCP	8128	1392
BKJP:	2013-08-19 14:06:24		192.168.10.100			202.108.33.60		80	TCP	31.28	1392
A 100 10 10 10	2013-08-19 14:06:24		192.168.10.100			202.108.33.60		80	TCP	3128	1392
NO1620	2013-08-19 14:06:24		192.168.10.100			202.108.33.60		BD	TEP	31.28	1392
東山 清空	2013-08-19 14:06:24		192.168.10.100			202.108.33.60		80	TCP	3128	1392
	2013-08-19 14:06:24		192.168.10.100			202.108.33.60		80	TCP	31.28	1392
				41509. 83 8 A							
	• 报表处理格式	0							HTML	PDF	EXCEL

互连关系列表用于显示筛选后的互连关系统计报表,包括:连接建立时间、源业务系统、源 IP、源地址设备、目标业务系统、目标 IP、目标地址设备、目标端口、协议类型、持续连接时间和 产生流量。

报表查询可以对互连关系列表进行筛选,可筛选项:包括建立时间、结束时间、操作账号、 业务系统、源 IP、目标 IP 和协议类型。

2. 报表处理格式

点击下方报表处理格式按钮.	可切至报表处理格式页面.	如下图所示:
---------------	--------------	--------

🕑 安全域流量监	管系统 v2.2.0.5678					1 2280	: Admin 🔘	616931Q		20 15:26:41	© 9388	<u>ه ل</u> ه
		n 97112		2822 ¥ 32/A	名单管理	当油关器 ∨	5840 v		802 v			
服養中心 > 互连关系直路服表												
	• 互连关系列表											
报表查询												
	* 报表处理终式								H	-	INF.	ENCE
2013-08-01 15:26:05	in the second se											ence
2013-08-20 15:28:05	运动趋立时间	潜业务事项	271P	招继任使各	目标业务集团	日日17	日标地社会系	1000	力以失望	江田村田村町	7 1 1	
	2013-08-19	-	189,169,90.9			149.160.10.10		192	17.0			
and an and the second second	15:02:10											
HUADO HUADO	14-85-88	1 1	172.16.1.120			172.16.1.8		137	100	30	58	
the second se	2015-08-10		182.162.10.180			182.160.10.10		447	208	191	40	
P:	14:19:42											
	14+85+37	1 1	192.148.10.100			192.168.10.200		23	TCP	:	1821	
UTP-	2013-08-10		192,160,20,15			182,160,10,10		447	209	192	356	
	2012-01-12											
	14+80+10		192.148.10.12			192.148.10.10		137	100	30	90	
	2015-08-14		192.160.10.12			192.160.10.52		197	129	49	100	
	2012-00-19											
自治 清 空	14-14-48		192,148,10.16			192.148.10.240		965	TCP	120	276	
	2013-08-16		192.160.10.100			1.1.1.1		58	129	100	418	
	2012-00-19											
	14+0#+24		194.148.19.100			***			TOP	*114	1094	
	2013-08-10	1 1	192.148.10.100			108.60.107.41		88	209	8128	20920	
	2019-00-19							****				
	14+08+10		192.100.20.9			100.117.00.107		110	157	8414		
	2013-08-19	管辖同	10.8.8.8		NLM车地认证	10.16.2.2		21	900	120	92	
	2013-05-15	-										
	10+84+48					1.1.10.1.1			107	- 20		
	2013-08-18		172.14.1.8			172.16.1.120		198	TDP	80	213	
	2019-08-18		2.1.1.1					23	100	21.0	1484	
	18+83+01	-								-10		
	2013-08-18		192.148.10.110			172.16.1.15		4681	202	120	12299	

报表处理格式可以分为 HTML、PDF 和 EXCEL 的格式进行显示,按钮如图:

HTML PDF EXCEL

系统管理

用户点击"系统管理"菜单后,可实现对系统日志、日志管理、许可证管理、系统状态、其 它配置的配置。

• 系统日志

系统日志页面如下图所示:

📿 安全域流量监	管系统、	/2.2.0.	5678			👤 登录用户:	Admin 🛞 系统时间:2013-08-2	0 15:27:12 💮 修改密码 🕛 退出
			首页	探针管理 🛛	设备管理 🛛 黒/白名单管型	星 互连关系 ≫	报表中心 ≥ 系统管理 ≥	
系统管理 > 系统日志	740	-t- TOL B						
日志查询	杀驼日	志列农						
日士來酒	「全选	序号	日志类型	日志来源	事件名称	事件来源	日志产生时间	操作
		1	进程信息	192.168.10.60	互联关系处理模块	互联关系处理模块	2013-08-20 11:40:15	প্র
日志类型:		2	进程信息	192.168.10.62	互联关系处理模块	互联关系处理模块	2013-08-20 11:00:59	<u>র</u>
开始时间: 2013-08-01 15:27:00		3	进程信息	192.168.10.60	互联关系处理模块	互联关系处理模块	2013-08-17 06:13:36	<u>রি</u>
		4	进程信息	192.168.10.60	互联关系处理模块	互联关系处理模块	2013-08-17 02:22:15	<u>রি</u>
结束时间: 2013-08-20 15:27:00		5	告警信息	192.168.10.60	cpu告答	事件处理模块	2013-08-16 09:25:27	হি
282.362 386.970		6	进程信息	192.168.10.60	互联关系处理模块	互联关系处理模块	2013-08-16 10:41:29	<u>ର</u>
		7	进程信息	192.168.10.60	互联关系处理模块	互联关系处理模块	2013-08-15 03:21:58	ি বি
		8	进程信息	192.168.10.60	互联关系处理模块	互联关系处理模块	2013-08-15 03:20:46	ি
		9	告警信息	192.168.10.60	内存告警	事件处理模块	2013-08-14 06:15:21	হ
		10	告警信息	192.168.10.60	内存告答	事件处理模块	2013-08-14 06:10:21	2
				< 共79条数	据页次1/8页 1 2 3 4 5 6	578下一页尾页>		
								导出
	系统的	日	志情	况,点	击"导出"	'按钮,	可以将日志	的导出。

日志管理

日志管理页面如	如下图所示:	
🕑 安全域流量监	管系统 _{V2.3.0.5683}	👤 登录用户:Admin 💮 系統时间:2013-08-20 15:25:59 🧔 修改密码 🕛 退出
	首页 探针管理 > 设备管理 > 黑/白名单管理	互连关系 ≥ 报表中心 ≥ 系统管理 ≥
<i>系统管理</i> > 日志管理	● 日志响应方式	日志容量告書 告密樂道: 自动删除调道: 日志容量使用百分比: 确定
	# 2	

这里主要提供日志的响应方式,用户可根据自己的需要选择日志的转发方式。日志转发支持 Syslog、SNMP trap 和 Email 三种方式。

日志容量的告警配置如下图所示:

── 日志容量告書 ─────	
告警阈值: 12	
自动删除阈值: 11	
日志容量使用百分比: 20.0	
确定重置	

当满足告警阈值、自动删除阈值、日志容量使用百分比时,系统就会自动进行告警。

• 系统升级

用户点击"系统管理"-"系统升级"即可进入,页面如下图所示:

		首页	保計管理 ¥	设备管理 ¥	黑/白名单管理	互连关系 ¥ 报表	時中心 ¥ 系统管	≣¥	
統任者 > 系统计载	中心境升级 — 中心境 当前版本: 2: 升级包版本: 最后升级时间:					 一 探针升级 ——— 探针 上传升级包: 升级包版本: 			
	上传升级包:		•			探针名称	探针版本	最后升级时间	攝作

升级中心端:

安全域流量监管系统³⁰ 使用手册

上传成功后点击"升级"按钮,即可完成对中心端的升级操作。此时中心端会自动更新并 重新启动系统,用户只需等待系统自动重启后,即可使用。

升级探针:

用户点击探针升级中的 🔤 浏览按钮, 在选择文件页面选中要上传的升级包文件。

选中文件后点击 全上传按钮,等待上传完成,上传成功后会显示当前版本和上传版本的版本号。____

上传成功后点击 **希** 按钮,即可完成对探针的升级操作。此时探针会自动更新并重新启 动系统,用户只需等待系统自动重启后,即可使用。

用户点击"系统管理"-"数据维护"即可进入,页面如下图所示:

	首页 序計管理 > 没管管理 > 第/白名单管理 互逐关系 > 集表中心 >	₩66位理 ¥
Q纸管理 > 数属地护		
	- 記蓋恢复	
	#552280: · · ·	
	NN : REACADES OR 1918. MGR. EGASH. FRED N. MIERSAN.	n - William,
	·后本互连日志静行: 🜍	
	(2日) 10日日本内容地区 FASS文目由文系、人工商业三法文系以外交行 単成型、 単成型、	自然重直,为保持政策一致,诸先因

用户可以在系统升级等需要备份的情况下,点击备份 **步**按钮,系统会将备份的文件导出,用 户可以直接下载此备份文件____

在系统升级后等需要恢复的情况下,点击恢复中的浏览²按钮,选择之前备份的文件路径,点击上传 2 按钮进行恢复

系统状态

用户可点击"系统管理"-"系统状态"进入,页面如下图所示:

数据维护

31 安全域流量监管系统 使用手册

CONTRACT -			_		100				
CPU利用率: 30.0)			6 M/F	利用率	60.	0	_	*
磁盘空闲毒: 80.0)			6					
		1	命定		清空				
·									
				系统资	波统计	ł			
			(:	2013-	08-2	1)			
100%									_
90% DISK- 80%									
70%									- 1
Memory- 60%									
40%									
20%									
10%									
0%°	35	35	35	35	35	35	35	35	35
44	39:	34:	29	:24	19	14	60:	04:	23
15	15	15	15	15	15	15	15	15	14

系统状态阈值:

设置 CPU 利用率、内存利用率和硬盘空闲率的阈值。在系统运行中 CPU 利用率、内存利用率 和硬盘空闲率超过设置的阈值,将会产生告警,告警日志在系统日志中查看。

系统资源:

在此页面显示当前系统运行中 CPU 利用率、内存利用率和硬盘空闲率的实时信息,也可以看 到系统状态阀值设置的情况。

其它设置 •

其它设置主要用于提供网络管理、SNMP 管理、时间设置和 DNS 设置,如下图所示:



用户管理

组管理

组管理是提供用户组织机构组的功能,如下图所示:

安全域流量监管系统 32 使用手册

🕐 安全域流量监管系	统 _{V2.3.0.5731}			👤 登录用户:S	uper 🕞 系統时间:2013-08-21 16:42:5	4 ② 修改密码 () 退出
		用户	管理 *			
用户管理 > 组管理	┌─ 潘加用户组 ○ ──					
用户组查询	組名:		組織迷:			
选择用户组 🔹 🕨	权限:	首页 设备管理。正学说	24.5 m			
▶ 全部组		黑/白名单管理				
▶ 用户管理员		互连关系-互连3 互连关系-未知3	○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○			
🗖 审计管理员						
🗖 系统管理员					nd affe	
🗖 test						
查询 清空	用户组列表	\geq				
	□ 全选	序号	組名称	組描述	操作	
		1	test		Ø×	
	—	2	系统管理员	系统默认组	系统默认组	
	•	3	审计管理员	系统默认组	系统默认组	
	E	4	用户管理员	系统默认组	系统默认组	
			< 共4条数据 页)	欠1/1页 1 ≻		
					批量删除	

添加用户组

一添加用尸丝	10-					
	组名:		组描述:			
	权限:	首页 设备管理-正常设备查询 黑/白名单管理 互连关系-互连关系查询 互连关系-未知互连关系	> > > > >			
					添加	

用户在输入组名和描述信息,并将权限分配给该用户组后,点击"确定",即可完成对用户 组的定义。

修改用户组

如果需要对已添加的用户组进行修改,则在用户组条目操作中点击 💋 ,将弹出用户组修

烧改组	×
組名称: Itest	
组织法:	
授以: 官克 《令客情》正言论各意询 第合总章智慧 五道关系: 王室光系 重词 五道关系: 本州五道关系	
关闭	. सिंह

删除用户组

点击需要删除用户组条目操作中的 🗙 ,出现如下提示,点击[确定]按钮,完成删除。



如果需要一次删除多个用户组,则选择多个用户组,然后点击 批量删除 按钮,完成多个用户组批量删除。

账号管理

系统内置三个预置账号分别为 Super、Audit 和 Admin,这三个账号无法被修改或删除。

Super 账号为用户管理员账号,默认密码为: Super123!。使用该账号登录后,可以对用户组、 用户账号进行添加、删除和修改,还可以查看在线用户和设置用户安全策略。

Audit 账号为审计员账号,默认密码为: Audit123!。使用该账号登录后,可以查看所有用户对系统的操作日志。

Admin 账号为系统管理员账号,默认密码为: Admin123!。使用该账号登录后,可以对系统进 行设置和管理。主要管理功能包括: 探针管理、设备管理、黑/白名单管理、互连关系、报表中心和 系统管理。

			Я	iPeze ¥				
用户管理 > 账号管理	─ 藩加新用	I¢ ⊕ —						
用白麦油	用户部			(1995) :			藏认用码:	
3450 000				▼ #2P	: ●是 • 否		f载入IP:	
☑ 全部组	可管理	业务系统	====请选择===	= 可管理	安全城:请选择	-		雨毒
■ 用户管理员								
■ 审计管理员	用户	列表	\geq					
■ 系統管理员	記念□	序号	用户名	组名作	Ib	統定	是否抑定IP	操作
客		1	abe			未敏定	未推定	Ø×¥
否缺定: 🛭 敏定 🌒 未数定		2	123			未锁定	未绑定	Ø×¥
 ● 全部 		3	test		1.1.1.1	未缺定	未爆定	Ø×¥
1P師定: ● 郡定 ● 未師定 ● 全部		4	longt		19216811	未被定	御臣	Ø×¥
		5	longq		172.16.1.15	未缺定	未御定	Ø×¥
अय मध		6	Admin	系统管理员		未被定	未绑定	算统默认用户
		-				-	-1-140.000	and a second second second
		7	Audit	审计管理员		干部定	干排定	系统默认用户
		8	Audit Super	軍计管理员 用户管理员		未被定	干师/定 未仰定	京纪默认用户 京纪默认用户
		8	Audit Super	用户管理员	< 共8条数据 页次1/1页	干领定 未被定 1 >	平市/道 未詳定	系统默认用户 系统默认用户
户		7	Audit Super	审计管理员 用户管理员	< 共8条数据 页次1/1页	平敬道 未敬足 1 >	平地道 未詳足	
户 ─ 添加新用户 ↔ ─ _{用户名:}		7 8	Audit Super		< 共振動調 開次1/1页	中和2 中和2 1 -	^{●●} +#2 、 、 、 、 、 、 、 、 、 、 、 、 、	》。《使化》相四 》。《使化》相四 张雪相相
 一添加新用户 ↔ — 用户名: 词:		7 8	Audit Super 空田 新聞	■+管理所 用户智道所	< 共振動調 向文1/1页 	中初定	●*** +#注 认密码:	》。《使化》相声 章 《使化》相声 章 《使化》相声
户 添加新用户 &> ^{用户名:} 组:		7 8	Audit Super 密码 绑定	¥<1-1635 用户部連点 [P:●	< 共5条数据 凤☆10 页 是 ● 否	中和王 中和王 1 > 章 指	^{●●●} 秋密码:	》。《使心相声 章 《使心相声 使者 新述

用户帐号管理页面如下图所示:

添加用户时,用户名、密码、确认密码、组、可管理安全域这五项为必填项。

如果要限制用户在特定设备上才能进行登录,则需要在添加用户时,为用户绑定 IP。这样被 绑定 IP 的用户,只能在绑定 IP 的设备上进行登录。

修改用户

如果需要对已添加的用户进行修改,则在用户条目操作中点击 ,将弹出用户修改窗口,如下图:______

修改用户	
用户名: test	
所属组:	
第定P: 1.1.1.1 ○ 是 ●否 [□]	
可管理业务系统: ====请选择====	
可管理安全域:▲系统	
关闭	
删除用户	
点击需要删除用户条目操作中的,出现如下提示,点击[确定]按钮,完成删除。	
Vindows Internet Explorer	
· · · · · · · · · · · · · · · · · · ·	
确定现消	
批量删除	
如果需要一次删除多个用户,则选择多个用户,然后点击	月
批量删除。	
重置用户密码	
如果需要对已添加的用户进行密码重置,则在用户条目操作中点击 凙 ,出现如下提示:	
Vindows Internet Explorer 🔀	

点击[确定]按钮后,出现如下提示:

取消

确定



清空

确定

安全域流量监管系统 36

使用手册

密码长度:此为最小密码长度。设置用户密码时,不能低于设置的值。

密码复杂度: 启用密码复杂度后, 密码必须为大小写字母、数字和特殊字符组成。停用密码 复杂度后, 则对密码设置不做复杂度要求。

生存周期:用户账号的有效期。从用户账号创建开始计算,有效期超过设置的值,则该账号 无法继续使用。

尝试次数:用户登录时,登录失败的次数不能超过设置的值。如果超过设置的值,则用户账 号将被锁定,需要用户管理员进行解锁。

空闲时间:用户登录后,超过空闲时间设置的值没有进行任何操作,则用户将登出。

在线用户

在线用户界面用于查看目前系统在线的用户列表,如下图所示:

		_		-1918 ¥					_
用户管理 > 在线用户	在线用	月户列表							
在线用户查询	□全透	序号	所願祖	用户名	組織法	臺景时间	登录IP	操作	
用户名:		1	用户管理员	Super		2013-08-21 03:53:54	192.168.20.112	系统默认	
新原語: 全部組 🔽					< 共	1条数据页次1/1页 1 >			
整录IP:								强制下线	
整录时间:									
吉東时间:									

用户可输入用户名、所属组、登录 IP、时间等查询条件对在线用户进行查询。 用户管理员可选择一个在线用户点击"强制下线" 操作,将已在线的用户进行强制下线。

审计日志

审计日志用于审计用户的操作日志,如下图所示:

				审计日志				
审计日志		日志列						
审计日志查询	「金地	序号	用户账号	操作增加	操作内容	操作事件	是否成功	日志中原
户烁号:		1	Audit	2013-08-21 15:58:22	用户:Audit运得过期,请你改运得	医高生存周期	失敗	192.168.20.112
術結果:● 成功 ● 失敗		2	Super	2013-08-21 15:58:10	用户:Super退出系统	退出系统	成功	192.168.20.112
O 全选		3	Super	2013-08-21 15:53:54	用户Super密码过剩,请你改密码	医弱生存期期	失敗	192.168.20.112
始时间: 2013-08-20 15:58:22		4	Admin	2013-08-21 15:53:39	用户:Admina题出写统	退出系统	成功	192.168.20.112
(TR)*(D) 0012-00-01 IF-FD-00		5	Admin	2013-08-21 15:48:31	修改整形成量	Admin	成功	192.168.10.190
2013-08-21 15:58:22		6	Admin	2013-08-21 15:32:54	修改整形成量	Admin	成功	192.168.10.190
查询 清空		7	Admin	2013-08-21 15:24:38	整形成量应用操作	Admin	成功	192.168.10.190
		8	Admin	2013-08-21 15:24:34	澤加菜量些測	Admin	成功	192.168.10.190
		9	Admin	2013-08-21 15:24:20	深加地址且	Admin	威功	192.168.10.190
		10	Admin	2013-08-21 15:24:09	深如地址旧	Admin	威功	192.168.10.190
				< 共170条数据 页次1/17页	1 7 3 4 5 6 7 8 9 1	0 5 -00 6	205 h	

用户可输入用户帐号、操作结果、操作时间等查询条件对日志进行查询。 用户点击 导出 按钮后,可实现日志信息的导出。