创元启安
CHUANGYUAN

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

目录

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：

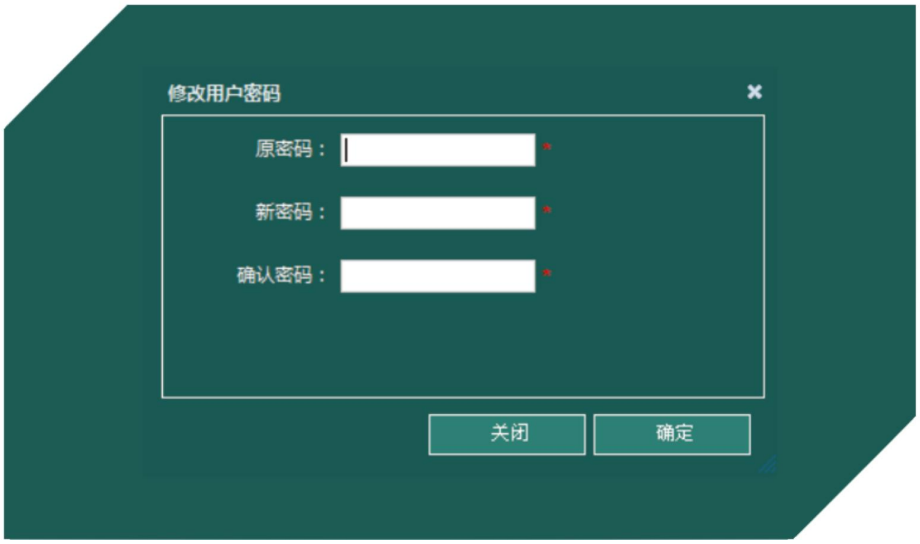
系统首页包括“最新系统信息”和“统计类信息”两部分。

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：



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：

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：

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：

- 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：

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：

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：

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：

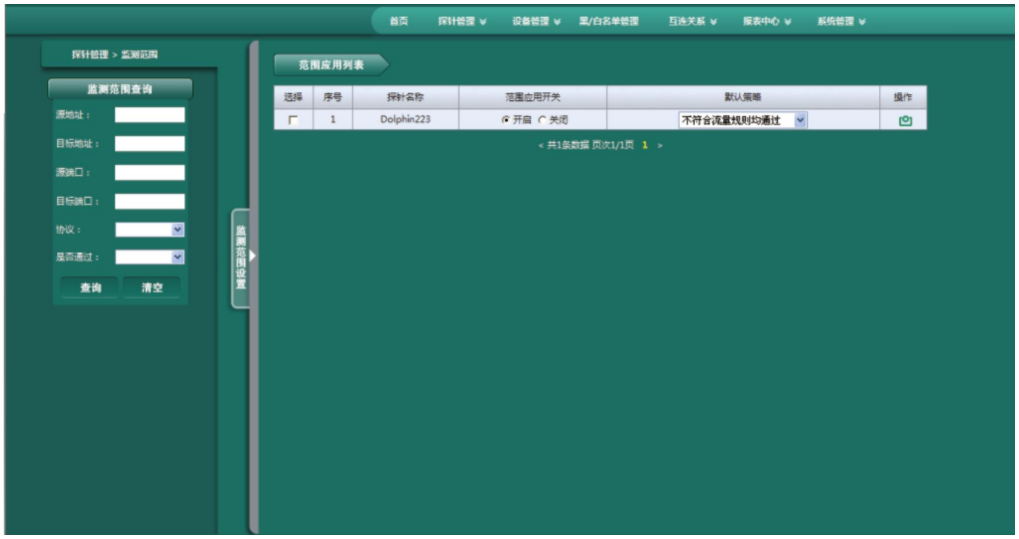
3. 应用策略

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：

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：



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：

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：

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：

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：

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：

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：

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：

- 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：

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：

用户可以进行“全选”操作后，点击 批量转为正常设备 按钮，将当前页面下的所有未知设备批量转为正常设备，如下图所示：

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：

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。

删除设备，点击“删除”按钮后，可删除当前的设备，如下图所示：

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。

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

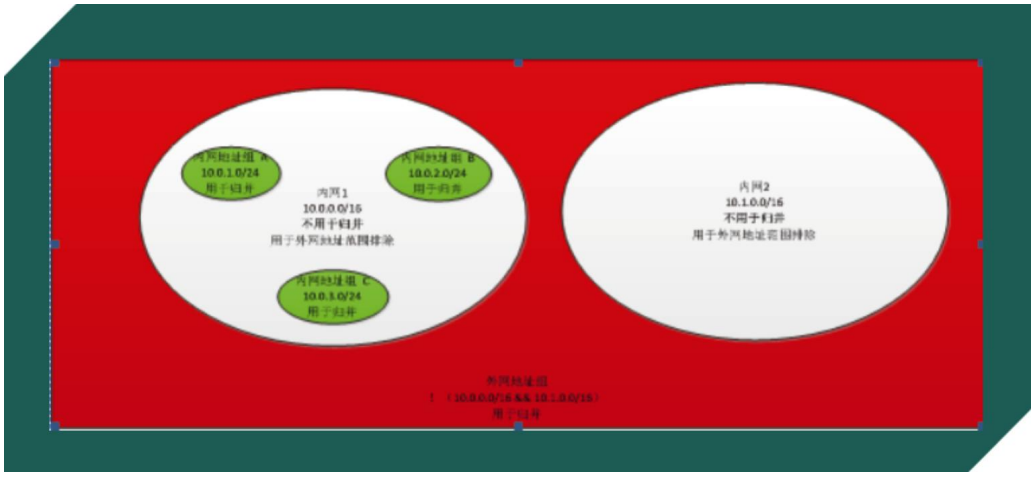
地址组管理，是允许用户通过添加地址组的方式，对一组设备进行定义。用户点击“设备管理”-“地址组管理”后，如下图所示：

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：

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

用户可通过点击地址组列表操作中的“修改”按钮  ，弹出修改窗口，如下：

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：

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。

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：

新增白名单

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：

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

后，如下图所示：

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：

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 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 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。

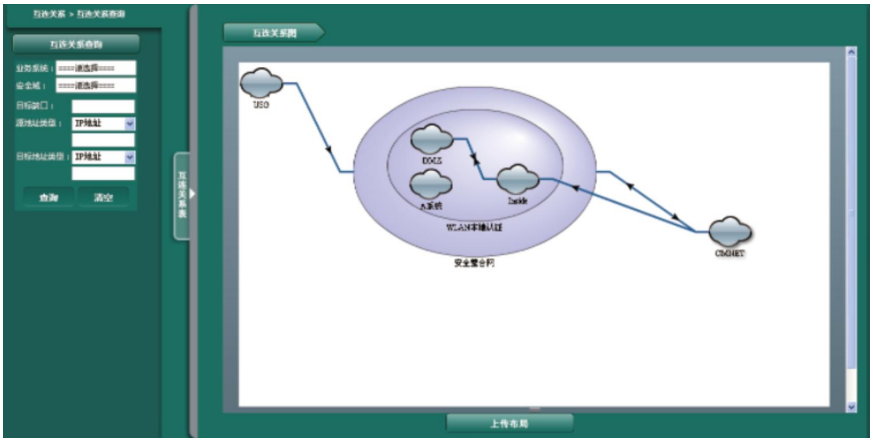
在二级条目中，点击按钮，将会更改已经选择的二级条目的处理状态。

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：

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 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。

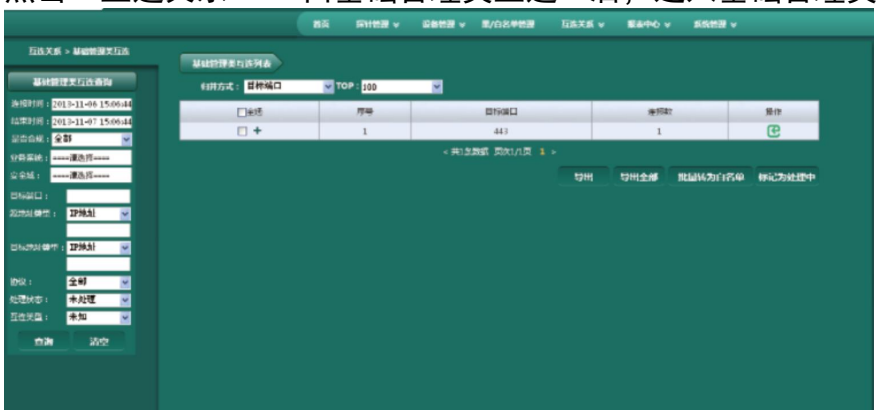
在二级条目中，点击 按钮，将会在弹出框中显示当前时间之前 24 小时内该条目的原始会话。

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：



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。

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话。

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话。

在二级条目中，点击 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：

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：

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：

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：

- 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：

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：

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：

- 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：

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：

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：

- 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：

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：

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：

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：

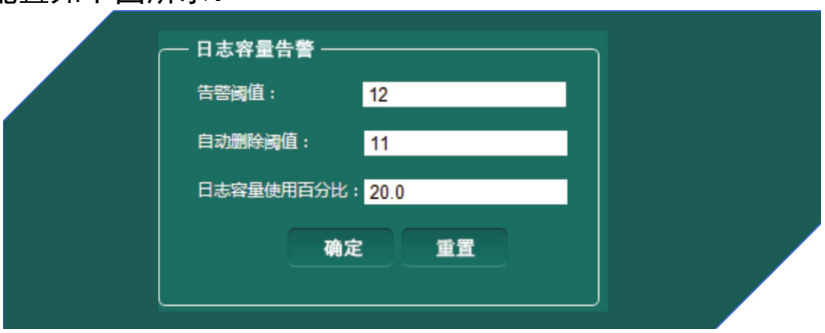
这里显示的是系统的日志情况，点击 “导出” 按钮，可以将日志的导出。

- 日志管理

日志管理页面如下图所示：

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：



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：

升级中心端：

用户通过先点击中心端升级中的浏览按钮，通过选择文件页面选中要上传的升级包文件。

选中文件后点击上传按钮，等待上传完成，系统弹出上传成功的提示窗口，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 “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 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。

- 数据维护

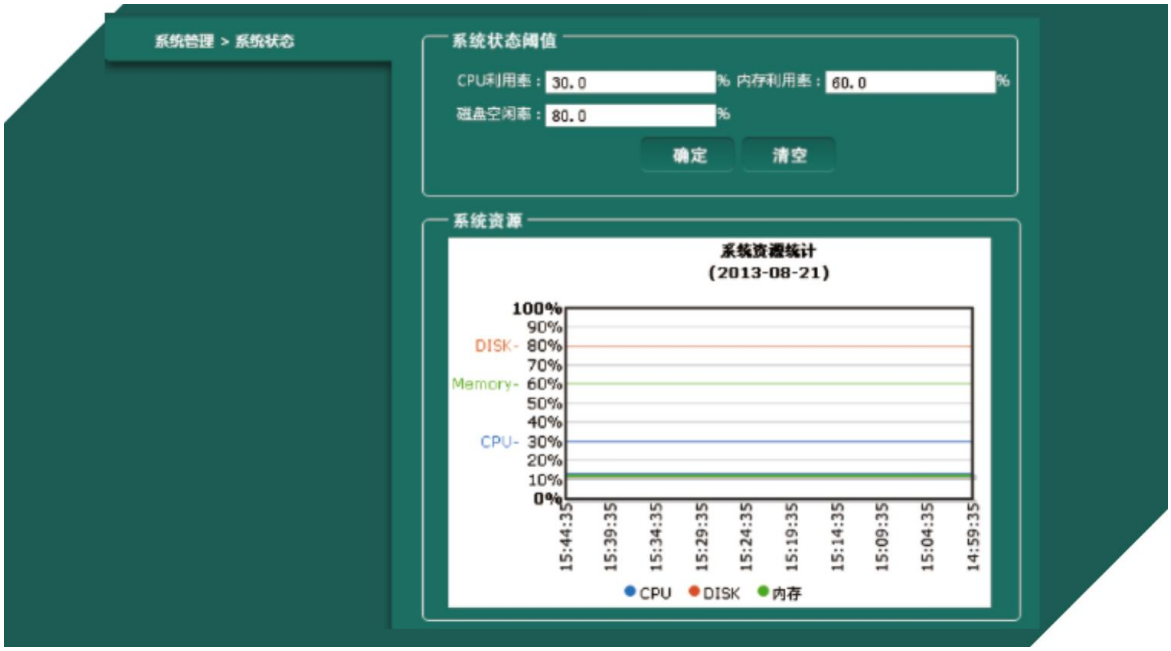
用户点击“系统管理”-“数据维护”即可进入，页面如下图所示：

用户可以在系统升级等需要备份的情况下，点击备份按钮，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，点击恢复中的浏览按钮，选择之前备份的文件路径，点击上传按钮进行恢复

- 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：



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

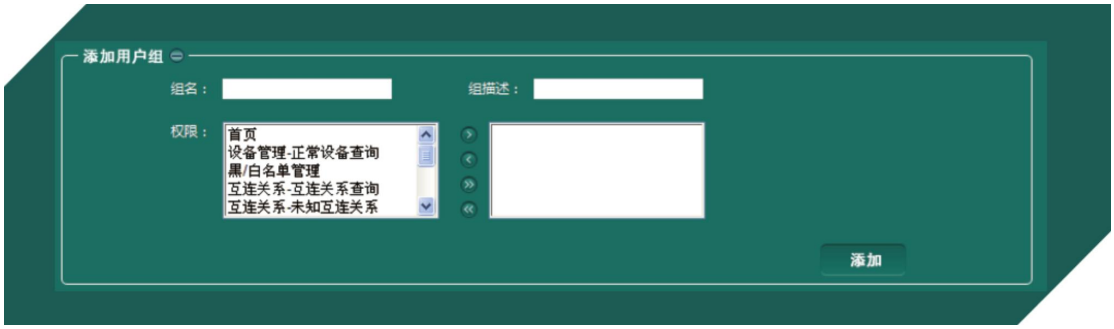
其它设置主要用于提供网络管理、SNMP 管理、时间设置和 DNS 设置，如下图所示：

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：

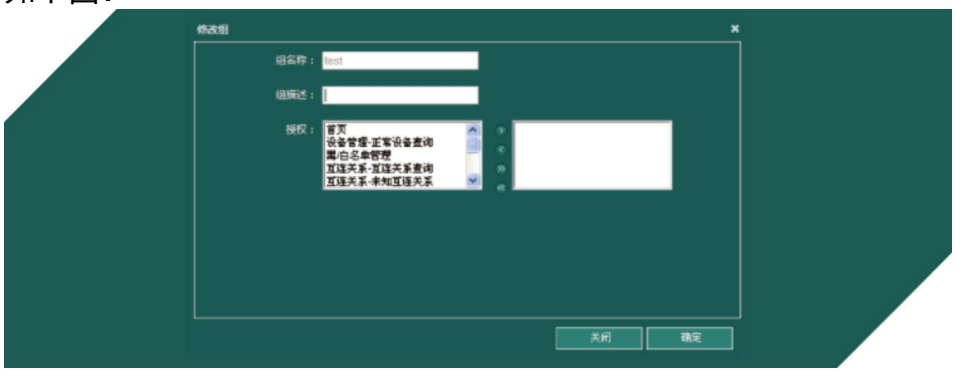
添加用户组



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  ，将弹出用户组修改窗口，如下图：



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。

用户帐号管理页面如下图所示：

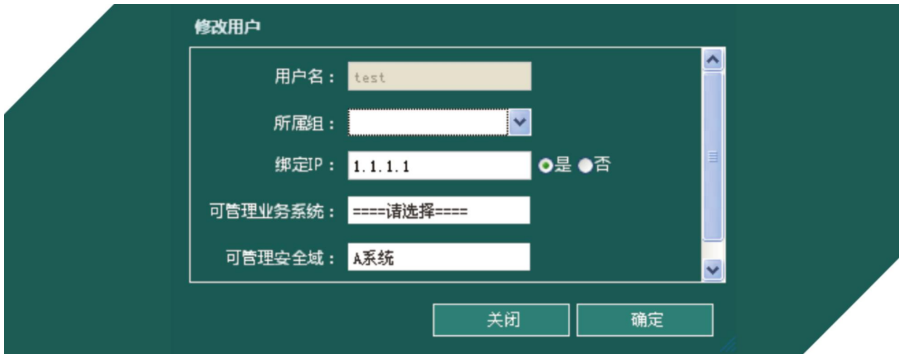
添加用户

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：



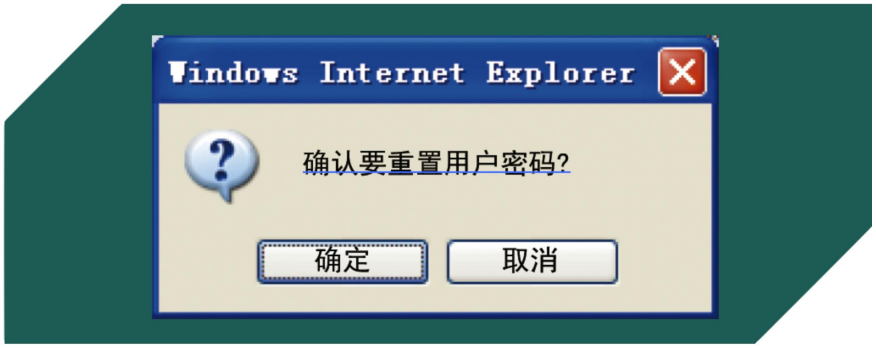
删除用户

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。

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

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 ，出现如下提示：



点击[确定]按钮后，出现如下提示：

为用户解除锁定

只有用户被锁定后才会出现解锁按钮 ，如下图中 test 用户操作中出现的 ：

点击 按钮后，出现如下提示信息：

点[确定]后，提示如下：

- 用户安全策略

用户安全策略用于配置用户口令策略，如下图所示：

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：

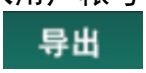
用户可输入用户名、所属组、登录 IP、时间等查询条件对在线用户进行查询。

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:

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 

按钮后，可实现日志信息的导出。