**安全管理(SecurityAccess)需求分析**

**目录**

[一、设备检测管理（主要功能：设备监测和拓扑管理） 2](#_Toc1290429264)

[二、流量管理（主要功能：监测流量） 2](#_Toc2123594160)

[三、资产管理（主要功能：查看目前的设备） 3](#_Toc839997970)

[四、策略管理（主要功能：自定义白名单规则以及出现异常时的告警方案） 4](#_Toc1433713549)

[五、警告管理（主要功能：设置警告方案） 4](#_Toc93627619)

[六、报表及展示管理(主要功能:对数据进行分析并使用图表的方式显示) 5](#_Toc1473690539)

[七、系统管理(主要功能:对于整个软件系统本身需要进行管理) 6](#_Toc1956888443)

## 一、设备检测管理（主要功能：设备监测和拓扑管理）

**1设备监控**

通过策略配置、设备监控、审计预警、安全响应等功能组成安全闭环，协助用户实时掌握信息系统的使用运行状态，实时监测各种安全事件，及时应对安全威胁，实现用户网络的整体安全，全面实现统一管理、统一预警和全局审计。

可分2个模块

**1.1设备状态**

**1.2安全事件**

**2拓扑管理**

拓扑发现功能分为两种，一种是手动设备添加，一种是自动发现设备。手动添加与自动发现是不能冲突的。自动发现设备是遵循SMAP协议，通过路由表发现在线的设备。但并非所有设备满足SMAP协议，因而需要手动添加一些设备，最终全面实现统一管理。

2.1 手动设备添加

2.2 自动发现设备

## 二、流量管理（主要功能：监测流量）

**1流量监测**

支持按时间范围监控指定IP的流量变化趋势；支持统计指定IP、指定时间范围内的协议流量组成，并对协议流量进行排行分析；支持按小时、按天、按月等对全网占用流量IP统计排行分析；支持流量动态基线管理，基线支持日基线、月基线等多种流量基线模型，分析网络是否存在异常流量。

## 三、资产管理（主要功能：查看目前的设备）

支持自发现在线网络设备及安全设备，自动生成在设备列表中，显示在线、离线和告警状态；支持对安全设备进行设备升级、自动发现和日志备份等配置操作功能；支持能够按照策略管理要求，对所管理安全设备划分安全域分别管理；支持查看安全设备的状态、型号、版本、端口状态、功能模式等信息；支持对工控设备管理，支持新增工控设备，并能够查看工控设备的厂商、序列号、型号等信息；支持网络内主机防护软件的配置管理及统一下发。

**1设备管理 （包括安全设备、工控设备和在线设备）**

通过第一个模块的设备监测功能,自动检测到了在线设备及安全设备并添加到设备列表中

1.1 显示在线、离线、告警三种状态

1.2 设备升级(如何升级?)

1.3 日志备份

1.4 划分安全域

1.5 查看设备详情

**2设备配置**

通过设备配置文档，使被选中的所有设备应用配置文档中的所有参数。

## 四、策略管理（主要功能：自定义白名单规则以及出现异常时的告警方案）

**1白名单方案管理**

白名单规则（学习时间可配置）

白名单学习协议例外功能

网络白名单学习的端口映射编辑功能

基于端口的私有协议定义和学习功能

对告警事件一键加入基线，后续将不再产生同类的告警

**2设备配置策略**

支持以单个设备和多个设备为单位进行策略管理（包括策略下发、设备操作等）

**3白名单管理**

（增删改查）

## 五、警告管理（主要功能：设置警告方案）

需要一个已经有的默认告警方案

**1告警方案**

事件实时告警，事件相关综合分析

管理平台支持告警监控总览界面，包括事件数量和安全设备连接状态；

支持事件实时告警；支持事件相关综合分析；

设备实时监控，支持对安全设备、工控设备和网络设备的实时监控功能；

未知设备监测，对系统内未知的设备接入进行实时告警，迅速发现系统中存在的非法接入；

比如支持对违法使用USB存储设备进行报警；支持声音告警、短信告警；

当产生相应级别的告警时，可以按照号码分组、警告级别发送给相应的接收人。

**2告警日志**

日志监控功能设置（监管工控安全网关日志记录功能、监管监测设计系统日志记录功能、监管工作站卫士系统的日志记录功能）

未知设备监测设置（有未知设备接入时进行告警，并迅速发现系统中存在的非法接入）

违法使用USB存储设备进行报警设置（支持声音告警、短信告警）

当产生相应级别的告警时，可以按照号码分组、警告级别发送给相应的接收人。

## 六、报表及展示管理(主要功能:对数据进行分析并使用图表的方式显示)

**1报表管理**

要求支持多种格式的显示

生成方法：1.手工报表2.自动报表（按照每小时、每天、每月、每年等周期的方式生成）

提供多种展现仪表盘：包括柱状图、折线图、饼状图、提供用户可定制TOP N展示图标，并支持报表下载。

## 七、系统管理(主要功能:对于整个软件系统本身需要进行管理)

**1系统监控**

系统自身状态监控（包括CPU,内存、硬盘使用率、网口IP地址等）

系统运行参数配置：（包括响应事件、策略管理、设备运行参数等相关信息）

系统各组件服务状态监控

**2日志管理**

需要对设备日志的存储管理

比如:日志存储空间溢出预警（日志可设定自动备份）

**3权限管理**

用户角色配置（基本包括系统管理员、系统安全员、系统审计员、普通管理员)系统管理员可以分配权限给不同的角色

3.1角色：系统管理员，系统安全员，系统审计员，普通管理员

3.2权限：可读性，编辑，管理员权限(增删改查)，审核权，发布安全方案。

管理平台与被管理设备之间采用加密传输（只是要求，不写入目录）

**4 IP拦截**

支持远程登录IP限制功能，仅允许特定的IP可以登录平台。

显示所有被拦截的IP

## **5 用户信息**

每个用户登陆系统,都能够查看到当前自己的用户信息,并且可以进行修改基本信息

5.1 用户基本信息查看

5.2 修改用户的基本信息