H3C SecCenter 安全业务管理平台

开局指导手册

目 录

1 特性简述

1.1 产品介绍

SMP（Security Management Platform，安全业务管理平台）能够对网络中的 FW/IPS 安全设备进行统一管理，为部署于各关键位置的 FW/IPS 安全设备提供集中的安全策略管理与控制，并能直观的为实时事件监控和综合分析攻击等各种安全事件提供丰富的统计报告，方便用户随时了解网络安全状况。

1.2 系统介绍

SMP 平台提供了软件安装包和一键式部署工具，通过一键式部署工具可以实现远程安装，简化安装过程。

- SecCenterSMP_{版本号}.tar.gz：大小为约 1GB 的 SMP 平台安装（含升级）包，其中包含 SMP 软件包、Tomcat 安装包、JDK 安装包、ClickHouse 安装包、MySQL 安装包、数据库脚本。
- CSAP_SMP_install.zip：大小为约 20MB 的一键部署工具包，通过该工具可实现远程一键式安装。一键部署工具包仅支持在 Windows 7 64 位操作系统的主机上进行安装和运行。
- SecCenterSMP_{版本号}.iso：大小为约 2GB 的 SMP 虚拟化部署包，其中包含 H3Linux 操作系统及 SMP 平台相关软件包。

说明：SecCenterSMP_{版本号}.tar.gz 支持使用 CSAP_SMP_install.zip 工具在 Win7/10 主机进行部署或者升级，部署前需要先安装 SUSE 操作系统，一般金融场景客户要求使用 SUSE 系统时使用此软件包；SecCenterSMP_{版本号}.iso 仅支持虚拟化安装部署，同时包含 H3Linux 操作系统一起安装，不支持升级，后续的升级使用 SecCenterSMP_{版本号}.tar.gz 和工具在 Windows 7/10 主机进行升级。

图1-1 SMP 平台登录页面

1.3 系统部署

1.3.1 服务器配置要求

SMP 平台对服务器安装要求的配置如下所示，请按照不低于最低配置要求进行安装。

1. 单个 SMP 平台管理 1-10 台安全设备

- CPU：2*4 核（2.1GHz/8 核/20MB）
- 内存：32GB 及以上
- 硬盘：推荐 1TB
- 操作系统：SUSE12SP2、H3Linux
- 浏览器：chrome57 及以上版本
- 日志接收速率：<=10000 条/秒

2. 单个 SMP 平台管理 10-50 台安全设备

- CPU：2*4 核（2.1GHz/8 核/20MB）
- 内存：64GB 及以上
- 硬盘：推荐 2TB
- 操作系统：SUSE12SP2、H3Linux
- 浏览器：chrome57 及以上版本
- 日志接收速率：<=10000 条/秒

3. 单个 SMP 平台管理 50-100 台安全设备

- CPU：2*4 核（2.1GHz/8 核/20MB）
- 内存：128GB 及以上
- 硬盘：推荐 4TB
- 操作系统：SUSE12SP2、H3Linux
- 浏览器：chrome57 及以上版本
- 日志接收速率：<=10000 条/秒

1.3.2 远程安装主机配置需求

通过一键部署工具包进行远程安装时，对远程主机配置要求如下表所示。

表1-1 远程主机配置要求

配置项	配置要求
操作系统	Windows 7/10 64位操作系统
浏览器版本	Chrome74及以上

1.3.3 产品安装部署

产品部署请参考《H3C SecCenter 安全业务管理平台 安装指导-5W101》

2 License 说明

2.1 License说明

SMP 在售 License 类型说明如下：

(1) 基础平台软件通用授权函：控制系统登录，只有导入基础平台 license 才能使用登录使用，登录后包含平台基本功能授权，以及 1 节点的通用资产授权；导入后永久生效；

(2) IPS 功能管理授权函：控制特征库管理、入侵防御和防病毒功能项；导入后永久生效；

(3) 分级管理组件授权函：控制分级管理、特征库推送任务管理菜单；导入后永久生效；

(4) 基础平台软件高端授权函（IPS 绑定销售使用）：基础平台软件通用授权函+IPS 功能授权函，以及自带 1 节点的高端资产扩容；导入后永久生效；

(5) 中低端基础平台软件授权函（IPS 绑定销售使用）：基础平台软件通用授权函+IPS 功能授权函，以及自带 1 节点的中低端资产扩容；导入后永久生效；

(6) 平台管理节点通用授权函：控制资产的数目，节点授权函的节点数可以叠加(目前有 5、20、50、200 节点的授权函)；导入后永久生效；

(7) 终端管理授权函：包含基础平台软件通用授权函，自带 1 节点的通用资产扩容。控制终端日志、视频监控功能项。导入后永久生效；

(8) 应用交付管理平台授权函：包含基础平台软件通用授权函，自带 1 节点的通用资产扩容。控应用负载监控、应用负载配置功能项。导入后永久生效。

2.2 安装License激活文件

服务器上架并上电后需进行 License 激活才能登录 SMP 安全业务管理平台。有关 License 激活文件申请的详细介绍请参见《H3C SecCenter [CSAP][SMP]系列产品 License 使用指南》。

获取软件授权后，其安装步骤如下：

(1) 在安装主机 Chrome 浏览器地址栏中输入 https://{服务 IP}，按回车键进入安全业务管理平台登录页面，然后点击<产品注册>进入产品注册页面。

(2) 在“选择基本操作”页签选择“使用 License 文件对产品进行注册”后单击<下一步>。

(3) 导入已申请的激活文件即可。

3 系统配置指导

3.1 系统登录

导入 License 后，登录 SMP 平台，使用 Chrome 浏览器，输入服务器的 IP 地址进入安全业务管理平台系统登录界面。

首次使用系统管理员账户登录，用户名：admin，密码：admin@admin。登录完成后为了确保设备的安全性，建议立即修改默认登录密码或创建新的管理员帐号。

缺省 Web 登录账号信息如下表所示。

表3-1 缺省 Web 登录账号信息

角色	用户名/密码	权限
系统管理员	sysAdmin/sysAdmin	查看和修改系统配置
超级管理员	admin/admin@admin	全部权限。信息安全管理员日常管理维护使用超级管理员账户即可
业务管理员	buzAdmin/buzAdmin	查看各类安全业务报表
审计管理员	auditAdmin/auditAdmin	查看其它用户操作记录的权限，审计用户操作

图3-1 SMP 平台登录界面

3.2 系统用户管理

SMP 平台的用户管理界面位于【系统配置 > 系统管理 > 角色及权限管理】，进入角色及权限管理界面，可以对系统用户进行管理。

3.2.1 添加用户

进入【系统配置 > 系统管理 > 角色及权限管理 > 用户管理】界面，点击 <新增> 按钮，进行用户添加。

图3-2 新建管理员界面

4 运维管理

4.1 配置顺序

运维管理配置顺序如下，可以按照文档当前编写顺序进行配置。

(1) 设备协议及日志配置

(2) 平台区域配置

(3) 平台资产配置

(4) 安全业务管理

(5) 特征库管理

(6) 配置管理

(7) 抓包取证

4.2 设备协议及日志配置

入侵防御、防火墙和应用交付设备获取 cpu、内存信息需要配置 snmp 协议；进行特征库升级、回滚、策略下发以及从设备上读取策略相关信息，均需要配置 netconf over soap 协议。

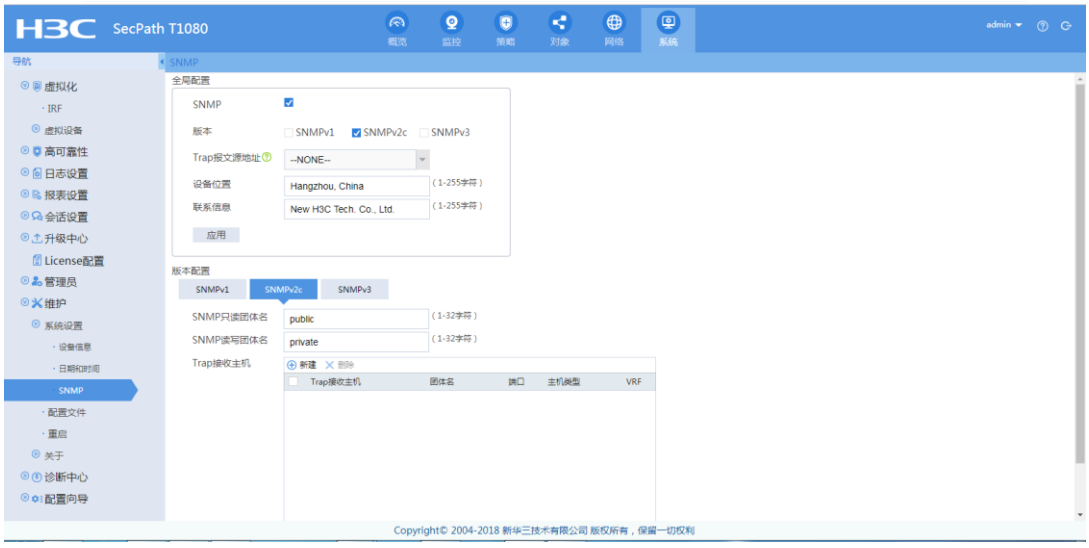
查看设备是否配置 snmp 和 netconf over soap，如无配置需要手动配置，已配置可忽略。

4.2.1 IPS/FW/LB 设备协议配置

(1) 在 IPS/FW/LB 设备 WEB 的【系统管理 >维护>系统设置 > SNMP 设置】页面配置 SNMP 协议，如无 web 页面请往下查看（2）、（3）命令行操作步骤。

说明：1）配置好后，需要点击应用按钮。 2）设备上配置协议参数需要与下 4.4.1 章节 SMP 平台配置保持一致。

图4-1 IPS/FW/LB 设备配置 SNMP



(2) 后台命令行配置 SNMP 协议

登录设备后台，使用命令查看是否已配置 snmp 协议，如图表示已配置

图4-2 IPS/FW/LB 查看 snmp 配置

```
[H3C]display current-configuration | inc snmp
 snmp virtual-access visible
 snmp-agent
 snmp-agent local-engineid 800063A280741F4A80AC0500000001
 snmp-agent community write private
 snmp-agent community read public
 snmp-agent sys-info version v1 v2c
```

如未配置，需手动输入命令：

```
snmp-agent sys-info version v2c                    //配置 snmp 版本为 v2c
snmp-agent community read public                   //配置只读团体字，默认为 public，根据需要配置
snmp-agent community write private                 //配置读写团体字，默认为 private，根据需要配置
```

(3) 后台命令行配置 netconf over soap 协议

登录设备后台，使用命令查看是否已配置 soap 协议，如图表示已配置

```
display current-configuration | inc soap
```

图4-3 IPS/FW/LB 设备查看 soap 配置

```
<IPS-T1080>dis cu
<IPS-T1080>dis current-configuration | inc soap
 netconf soap http enable
 netconf soap https enable
<IPS-T1080>
```

如未配置，需手动输入命令：

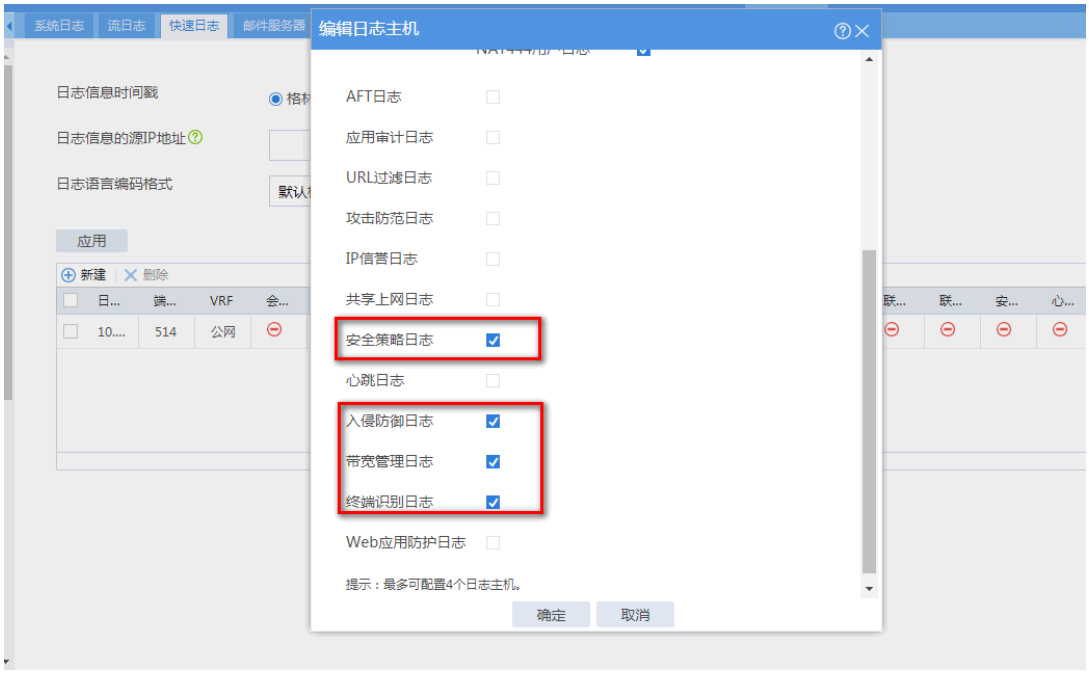
```
netconf soap http enable                //开启 netconf over soap over http
netconf soap https enable               //开启 netconf over soap over https
```

4.2.2 IPS/FW/LB 日志发送基本配置

管理平台支持采集设备发出的安全日志（漏洞攻击日志、病毒攻击日志、安全策略日志）、流量日志（NAT 会话日志，NAT444 会话日志，NAT444 端口块日志）、设备日志（故障日志、配置日志）、终端日志（终端识别日志、异常流量日志）、以及各类应用审计日志并展示。

如下为在设备侧配置。

(1) 在 IPS/FW/LB 设备 WEB 的【系统 > 日志设置 > 基本配置 > 快速日志】页面，设置日志主机为 SMP 平台地址，发送快速日志到 SMP，端口为 514，勾选应用审计日志（选配）、安全策略日志（选配）、入侵防御日志、防病毒日志、终端识别日志（选配）与带宽管理日志（选配）。



命令行方式：（命令行方式与设备页面配置方式二选一即可）

```
customlog host 127.0.0.2 export security-policy dpi audit ips traffic-policy terminal
```

(2) 在【系统 > 日志设置 > 基本配置 > 系统日志】页面配置系统日志，用于发送设备日志（故障日志、配置日志）到日志主机（SMP 平台）。

图4-4 IPS 设备新增系统日志主机页面

命令行方式：（命令行方式与设备页面配置方式二选一即可）

```
info-center enable
info-center loghost 172.31.0.61
```

(3) 在【系统 > 日志设置 > NAT 日志】页面，配置 NAT 日志。（选配）

命令行方式：（命令行方式与设备页面配置方式二选一即可）

```
nat log enable
nat log flow-active 120
nat log flow-begin
nat log flow-end
nat log no-pat ip-usage
nat log port-block-assign
nat log port-block-withdraw
```

(4) 在【系统 > 日志设置 > 基本配置 > 流日志】页面，配置流日志主机用于发送 NAT 日志，选择日志版本为 3.0，勾选日志负载分担。新建日志主机为 SMP 平台地址，端口为 9002，点击应用。（选配）

命令行方式：（命令行方式与设备页面配置方式二选一即可）

```
userlog flow export version 3
userlog flow export load-balancing
userlog flow export host 10.123.53.240 port 9002
```

参数说明：

- 日志主机：接收设备日志的管理平台的 IP（必填项）。
- 端口：514 或者 30514，与配置文件中设置的端口一致（必填项），NAT 流日志端口为 9002。
- VRF：默认为公网（必填项）。

4.3 平台区域配置

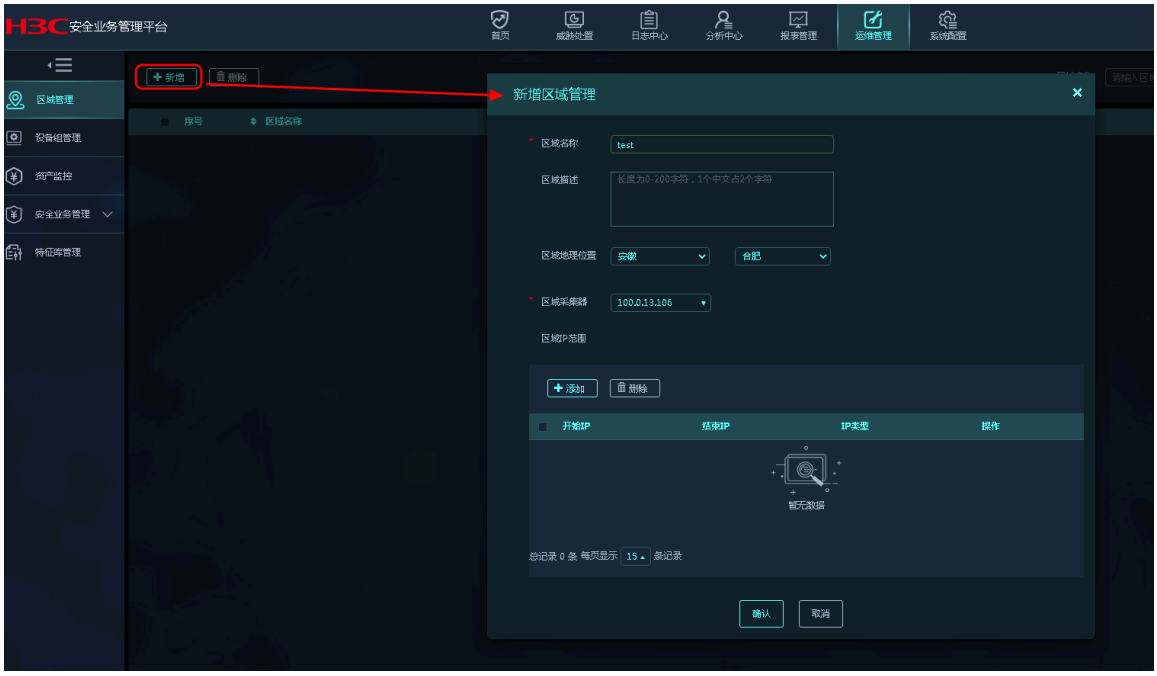
针对现场网络进行区域管理配置，根据用户的网络区域配置相应的区域。

在【运维管理 > 区域管理】界面点击<新增>按钮，进入新增区域管理界面。区域地理位置选择当前区域所在地理位置。选择当前区域所部署的采集器。在 IP 范围中添加用户网络网段范围。

说明

区域仅为 SMP 平台上针对客户网络进行的逻辑划分。区域主要是绑定区域采集器，与设备交互。设备信息的上报与下发均通过区域采集器实现。

图4-5 新增区域页面



4.4 平台资产配置

在【运维管理 >设备管理】界面进行用户资产配置。添加资产之前，需要先配置模板参数管理。系统支持配置 IPS、防火墙的设备资产进行维护。

4.4.1 模板参数管理

SMP 平台对资产进行监控管理，建议使用模板参数配置管理设备的参数，模板参数与设备的实际配置保持一致。

在【运维管理 >设备管理】界面，点击右上角<模板参数管理>按钮，进入模板参数管理界面。根据需要配置 SNMP 模板、SOAP 模板。点击<新增> 按钮，新增模板。

1. 新增 SNMP 模板

新增 snmp 模板，如图所示：

图4-6 新增 snmp 模板

2. 新增 SOAP 模板

新增 soap 模板，如图所示：

图4-7 新增 soap 模板

4.4.2 添加资产

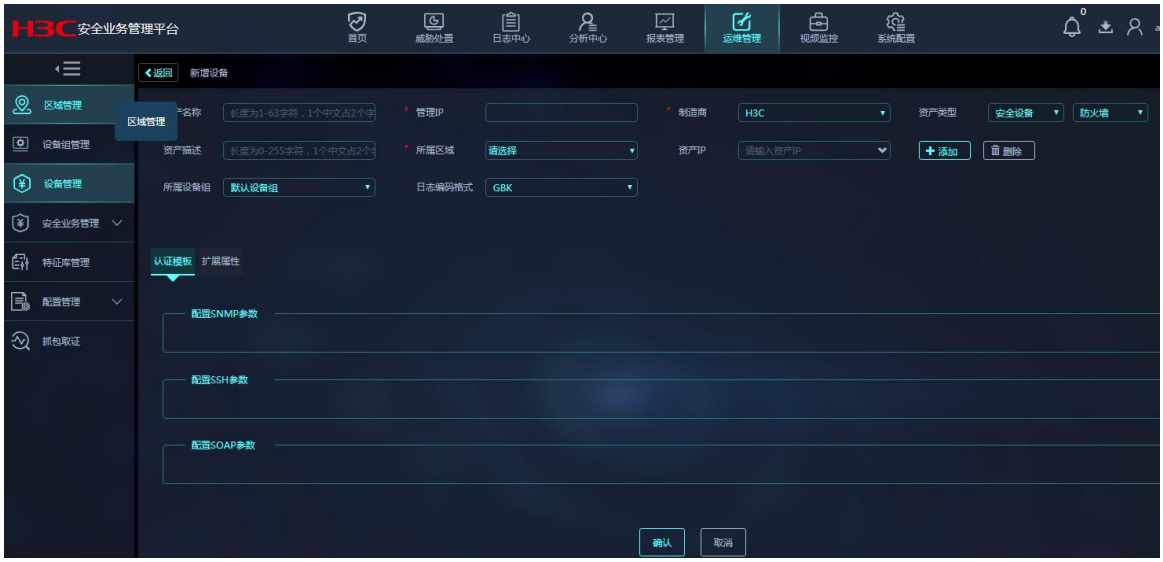
在【运维管理 > 设备管理】界面，点击<新增>按钮，进入新增资产信息界面，根据所需添加设备实际情况进行配置。

说明：添加资产，入侵防御、防火墙和应用交付获取 cpu、内存信息需要配置 snmp 参数；进行特征库升级、回滚、策略下发以及从设备上读取策略相关信息，均需要配置 soap 参数。

（认证模板建议从已有的参数模板中选择，减少配置量）

新增防火墙设备为资产，如图所示：

图4-8 新增防火墙设备



点击认证模板-配置 snmp 参数-设置，选择手工编辑或者从已有模板选取。

图4-9 新增资产配置 snmp 参数

点击认证模板-配置 soap 参数-设置，选择手工编辑或者从已有模板选取。

图4-10 新增资产配置 soap 参数

4.4.3 资产系统信息

(1) 在【运维管理 > 设备管理】界面，查看 cpu 利用率和内存利用率

图4-11 查看资产 cpu 、内存利用率页面

(2) 点击详情按钮，查看系统流量趋势图、cpu/内存趋势图、系统新建和并发趋势图（V5 系列设备没有会话连接数）。

图4-12 查看资产系统信息页面

4.5 安全业务管理

安全业务管理包括安全策略的配置以及下发。

4.5.1 安全策略下发

1. 安全策略下发前提条件

(1) 设备配置 snmp 和 netconf over soap，可获取到设备上已配置的安全域、IP 地址组、IPS 策略、AV 策略等；

(2) 添加区域；

(3) 添加设备为资产绑定区域，配置 snmp 参数和 soap 参数；

具体操作步骤详见 4.2 设备协议及日志配置、4.3 平台区域和**错误!未找到引用源。错误!未找到引用源。**（如已配置可忽略）；

(4) 在【运维管理 > 安全业务管理>全局资源】页面，配置 IP 地址组、服务、时间段、安全域、入侵防御策略、防病毒策略（全局资源可根据需要配置）。

图4-13 全局资源页面

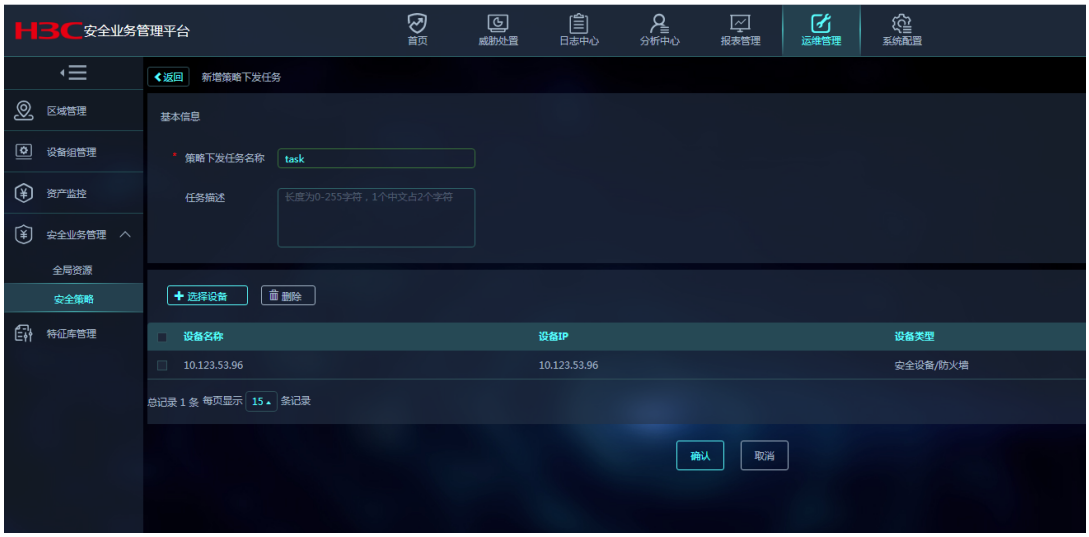
2. 配置步骤

(1) 在【运维管理 > 安全业务管理>安全策略】页面，点击<新增>按钮，新建安全策略。

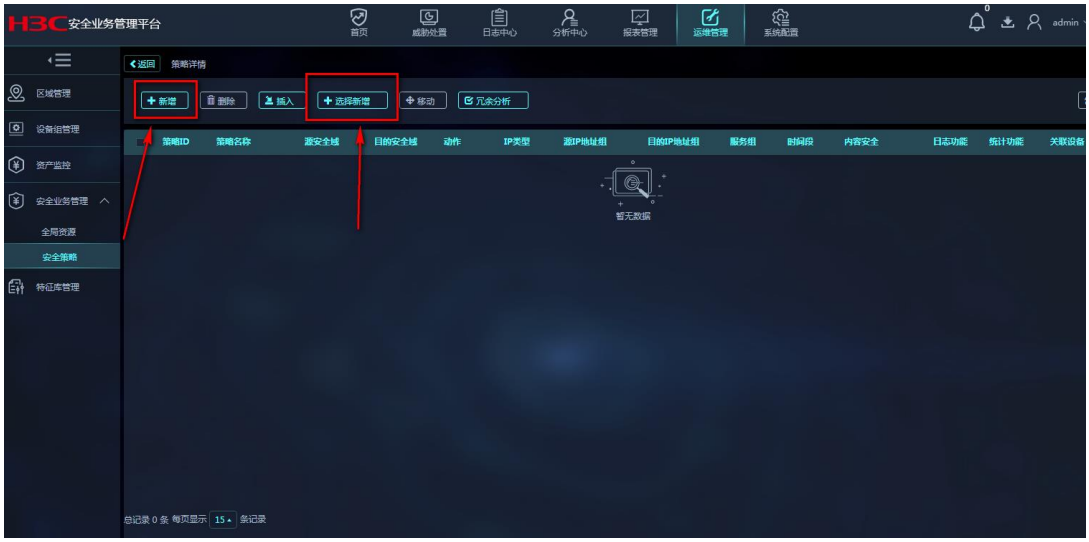
图4-14 新增设备策略页面

(2) 在【运维管理 > 安全业务管理>安全策略>策略下发任务】页面，点击<新增>按钮，新增策略下发任务。

图4-15 新增策略下发任务



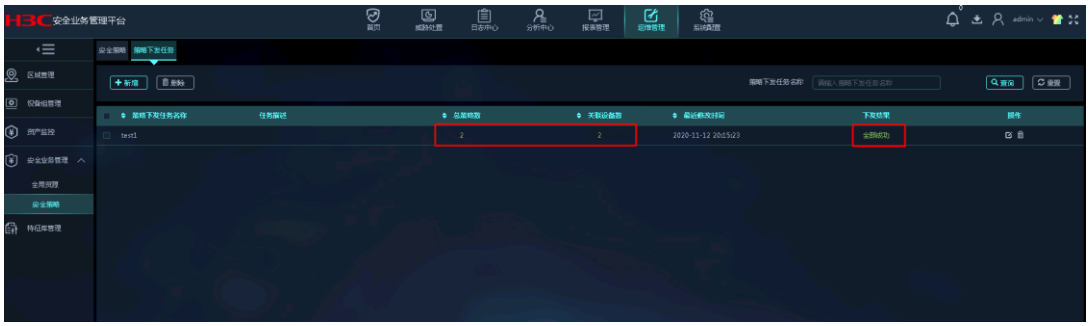
(3) 新增下发任务后自动跳转到策略详情页面，此页面可以<选择新增>已创建过的安全策略或直接<新增>策略下发，如图：



(4) 在已有策略列表的情况下，可根据业务需求对安全策略进行修改、移动、删除、插入、冗余分析等操作，无需操作点击<返回>即可回到策略下发任务列表页面：

(5) 在【运维管理 > 安全业务管理>策略下发任务】页面，查看已下发的策略，点击<总策略数>可查看策略详情，点击<关联设备数>可查看下发的设备，点击<下发结果>可查看每个策略下发的详情。

图4-16 查看已下发的策略



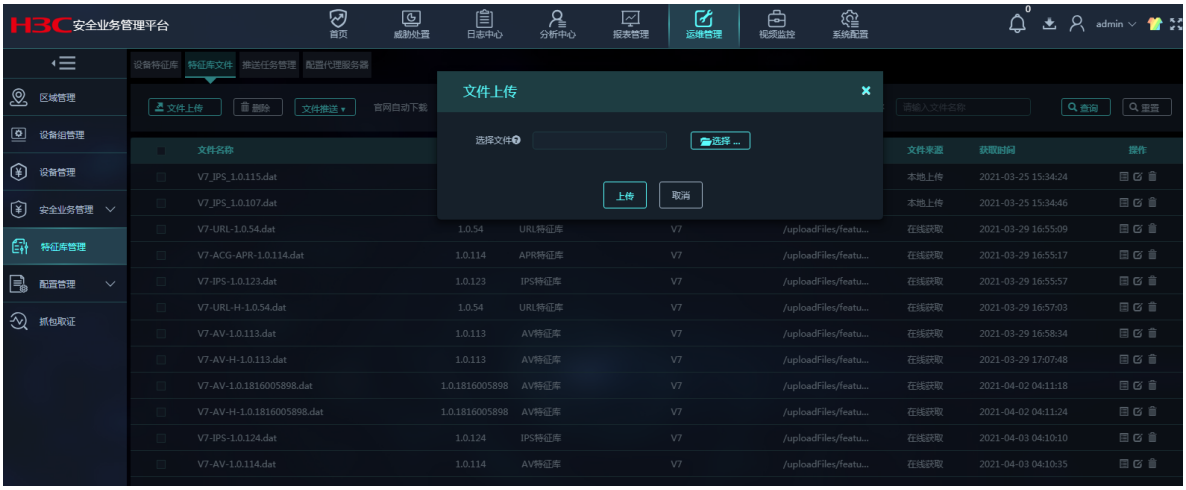
4.6 特征库管理

特征库管理包含特征库文件、特征库推送、特征库升级、特征库回滚等功能。

4.6.1 上传特征库文件

在【运维管理 > 特征库管理>特征库文件】页面，点击<文件上传>按钮，选择需要导入的特征库文件，点击<上传>即可。

图4-17 特征库文件上传页面



4.6.2 特征库升级

1. 特征库升级前提条件

(1) 设备配置 netconf over soap

(2) 添加区域

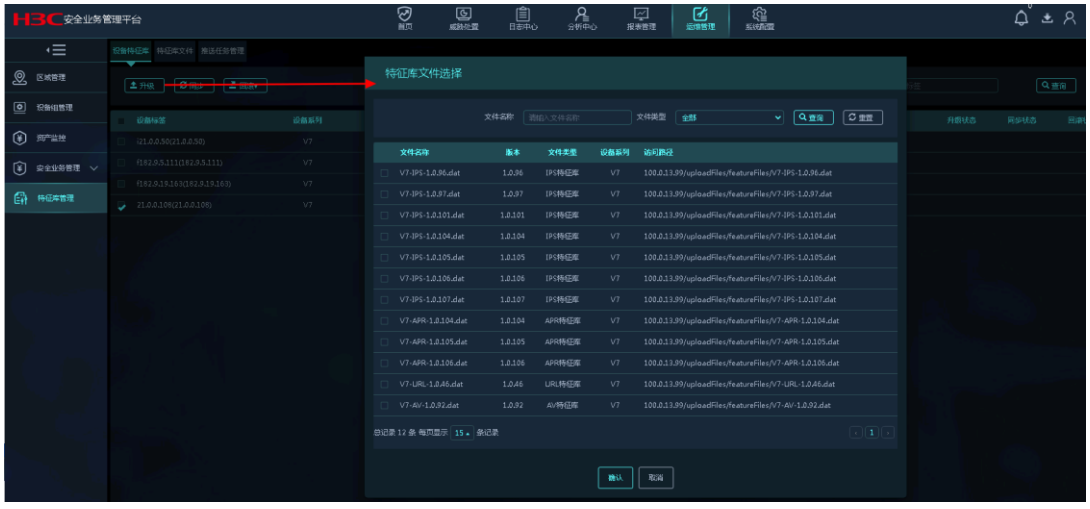
(3) 添加资产绑定区域，配置 soap 参数

具体操作步骤详见 4.2 设备协议及日志配置、4.3 平台区域和错误!未找到引用源。错误!未找到引用源。（如已配置可忽略）。

2. 配置步骤

(1) 在【运维管理 > 特征库管理>设备特征库】页面，选择设备，点击<升级>按钮，勾选特征库文件，进行升级

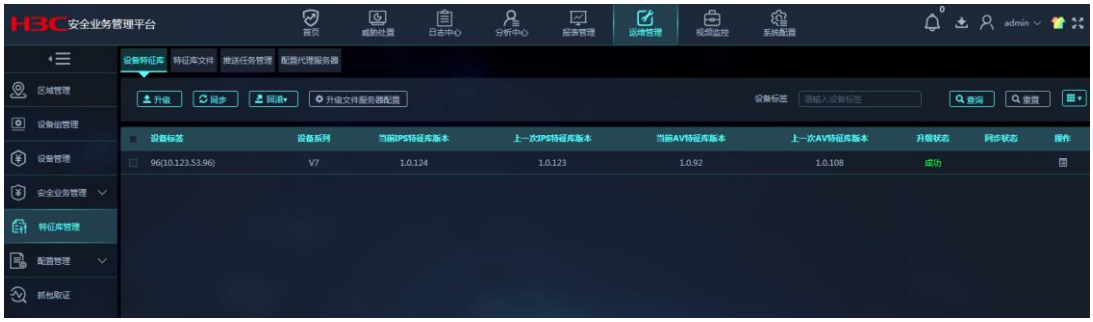
图4-18 特征库升级页面



说明：打开官网自动下载开关，将自动连接官网获取最新特征库同步到安全业务管理平台，打开自动升级开关，则会自动同步最新特征库到设备，自动升级开关默认关闭。

(2) 升级成功后，选择设备，点击同步，看到当前特征库版本信息更新。

图4-19 特征库升级结果界面



4.6.3 特征库回滚

特征库回滚操作可以将设备的特征库版本回退到上一版本或者出厂版本。

(1) 在【运维管理 > 特征库管理>设备特征库】页面，选择设备，点击<回滚>按钮，选择回滚至上一版本或出厂版本 （回滚不支持 V5 系列设备）

图4-20 特征库回滚页面

(2) 回滚成功后，选择设备，点击同步，看到当前特征库版本信息已经更新。

图4-21 特征库回滚结果页面

4.7 配置管理（选配）

4.7.1 配置下发

配置下发页面可以配置不同的命令脚本生成不同的部署模板，并支持对设备进行配置模板下发和回滚操作。

1. 配置部署模板

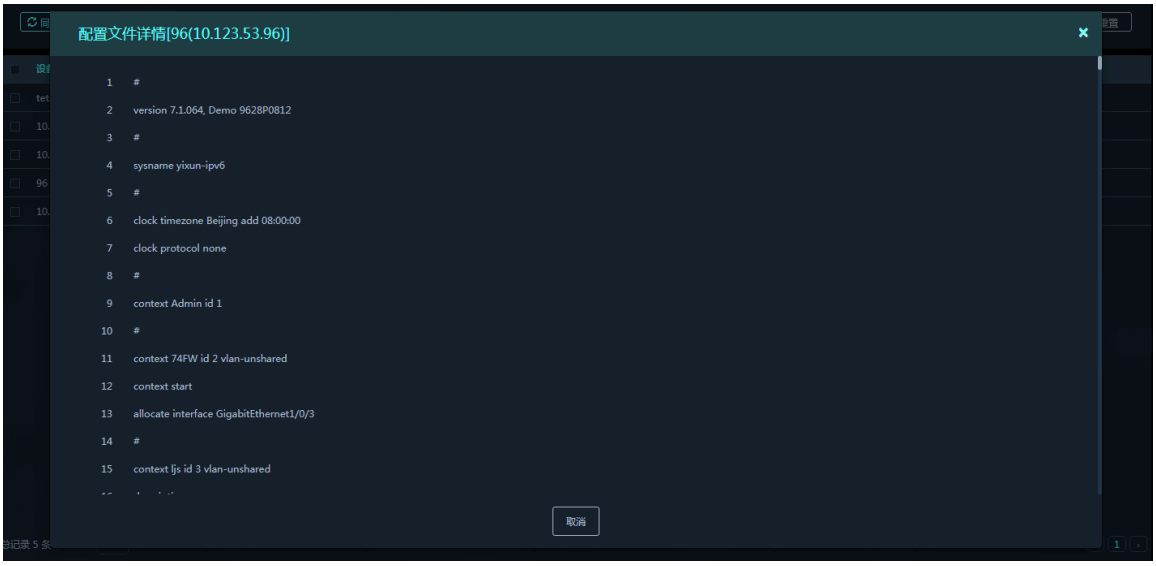
在【运维管理 > 配置管理>配置下发】页面，点击部署模板 tab 页，点击<新增>按钮，配置部署模板。

2. 下发部署任务

在【运维管理 > 配置管理>配置下发】页面，点击部署任务 tab 页，点击<新增>按钮，配置部署任务（选择部署模板、选择需要下发的设备以及任务基本信息）。

4.7.2 配置文件

在【运维管理 > 配置管理>配置文件】页面，查看设备配置文件列表，可通过同步按钮将设备的配置文件同步至平台，通过点击详情按钮，查看设备的配置文件详情。



4.8 抓包取证（选配）

4.8.1 使用限制和配置指导

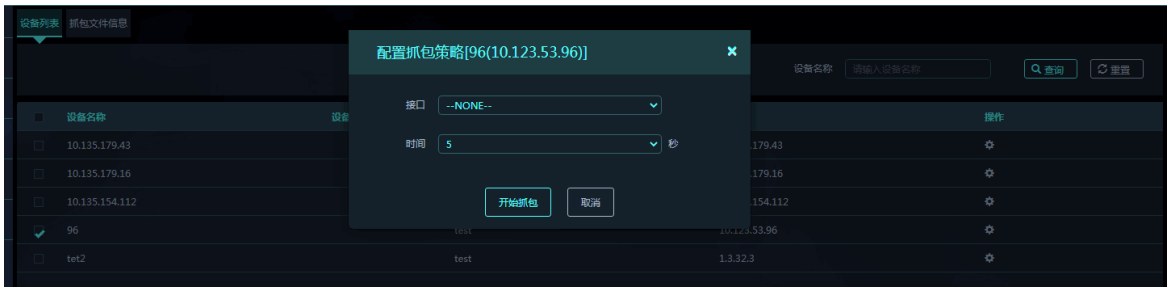
(1) 使用抓包取证功能前必须确保设备已配置 NETCONF over SOAP 功能，且设备已被平台添加为资产并指定所属区域和引用 SOAP 参数。

(2) 需要在设备侧配置报文捕获参数。配置报文捕获保存在外部服务器。路径：tftp://{IP}/capFiles/

4.8.2 抓包任务下发

抓包任务下发，将抓包相关配置下发至设备，设备将按照配置参数进行报文捕获，并上报至 SMP 平台。

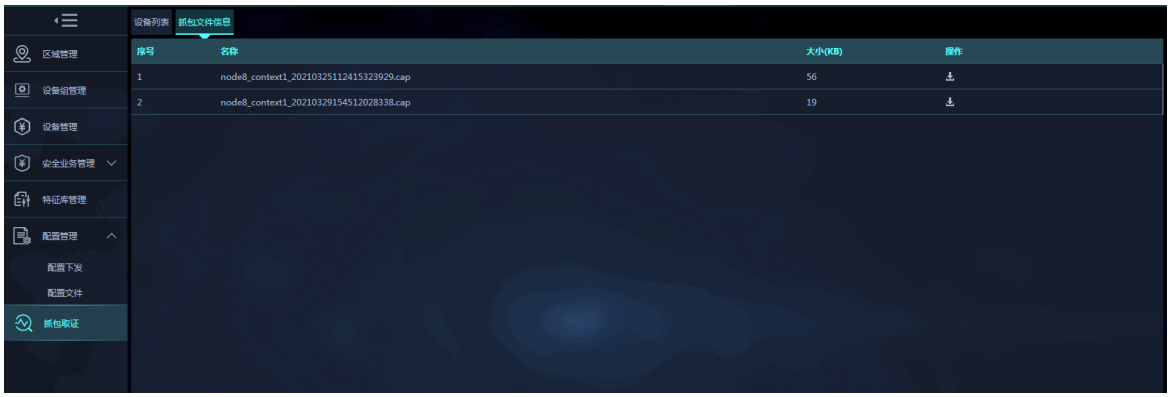
选择一个设备，单击设备列表中的<>按钮，配置报文捕获的接口以及抓包时长。点击<开始抓包>按钮，平台会将任务下发至设备。



4.8.3 抓包文件查看

支持列表的形式展示当前获取的抓包文件信息。包括名称、大小，支持抓包文件的下载

单击指定抓包文件右侧的<>按钮，下载抓包文件到本地进行查看。



5 首页展示配置

首页展示资产的 cpu 利用率、内存利用率、会话趋势图、IPS 攻击目的 IP Top50、IPS 攻击源 IP 和目的 IP Top50、IPS 阻断事件 Top50、攻击事件趋势图、设备日志接收趋势图。

5.1 前提条件

(1) 设备配置 snmp，日志主机

(2) 添加区域

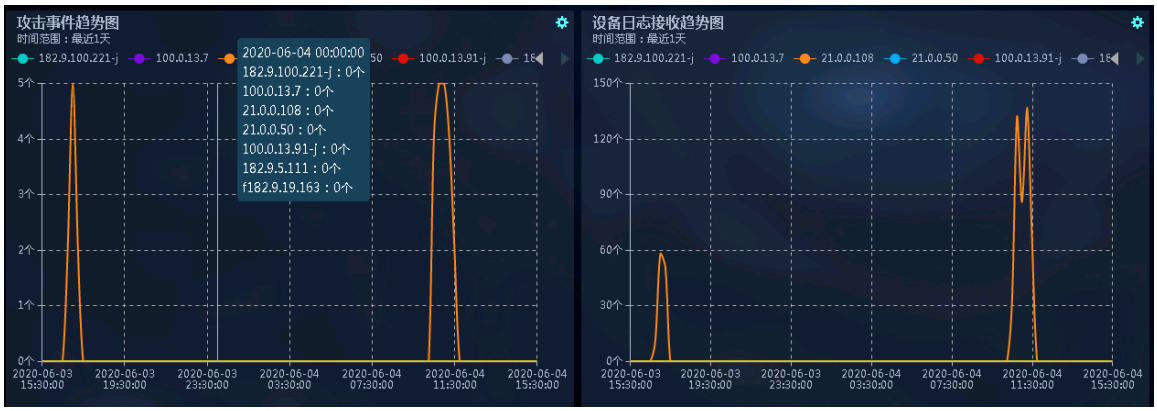
(3) 添加资产绑定区域，配置 snmp 参数

具体操作步骤详见 4.2 设备协议及日志配置、4.3 平台区域和错误!未找到引用源。错误!未找到引用源。（如已配置可忽略）。

5.2 参数设置

设置系统参数，勾选需要展示信息的资产、时间范围以及刷新时间

图5-1 首页系统参数设置



6 日志中心

6.1 安全日志

6.1.1 配置顺序

配置顺序如下，可以按照文档当前编写顺序进行配置。

(1) 设备配置日志主机

(2) 区域配置

(3) 资产配置

(4) 【报表管理】>【报表任务】

配置完成后，可以查看日志信息以及报表文件

6.1.2 配置步骤

以列表的形式展示采集的攻击日志和病毒日志以及安全策略日志。

1. 前提条件：

(1) 设备配置日志主机（详见 4.2 设备协议及日志配置）

(2) 添加区域（详见 4.3 平台区域）

(3) 添加资产绑定区域，配置 soap 参数（**错误!未找到引用源。错误!未找到引用源。**）

2. 漏洞攻击日志

在【日志中心> 安全日志 > 漏洞攻击日志】页面，查看漏洞攻击日志。

图6-1 漏洞攻击日志页面

3. 病毒攻击日志

在【日志中心> 安全日志> 病毒攻击日志】页面，查看病毒攻击日志

图6-2 病毒攻击日志页面

4. 安全策略日志

在【日志中心> 安全日志> 安全策略日志】页面，查看安全策略日志。

图6-3 安全策略日志页面

6.2 流量日志（选配）

6.2.1 NAT 会话日志

在【日志中心> 流量日志 > NAT 会话】页面，查看 NAT 流日志。

图6-4 NAT 流日志

6.2.2 NAT444 端口块日志

在【日志中心> 流量日志 > NAT444 端口块日志】页面，查看 NAT444 端口块日志。

图6-5 NAT 444 端口块日志

6.2.3 NAT444 会话日志

在【日志中心> 流量日志 > NAT444 会话日志】页面，查看 NAT444 会话日志。

图6-6 NAT 444 会话日志

6.3 应用审计日志（选配）

在【日志中心> 应用审计日志】页面，查看各应用审计日志。

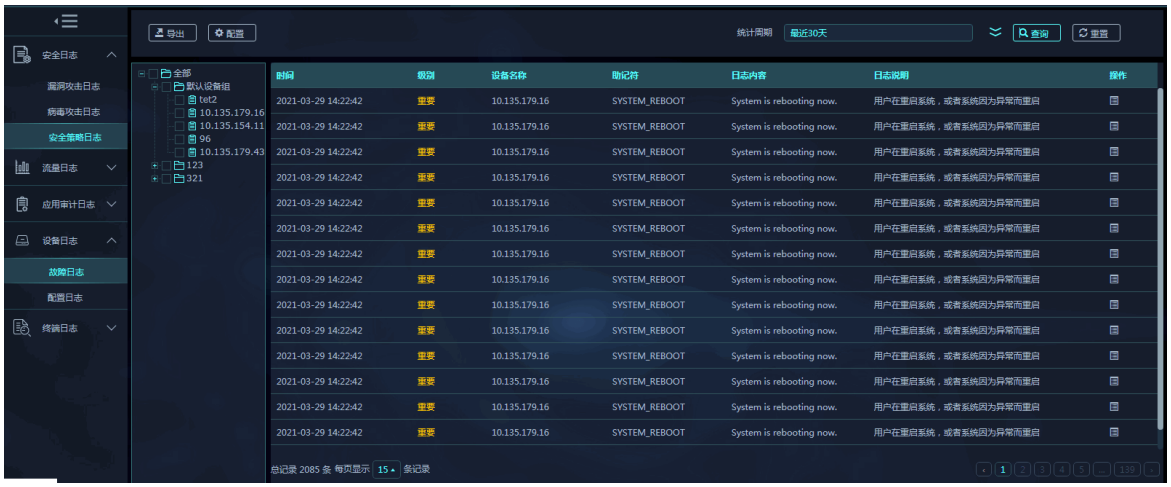
图6-7 应用审计日志

6.4 设备日志

6.4.1 故障日志

在【日志中心> 设备日志 > 故障日志】页面，查看故障日志。

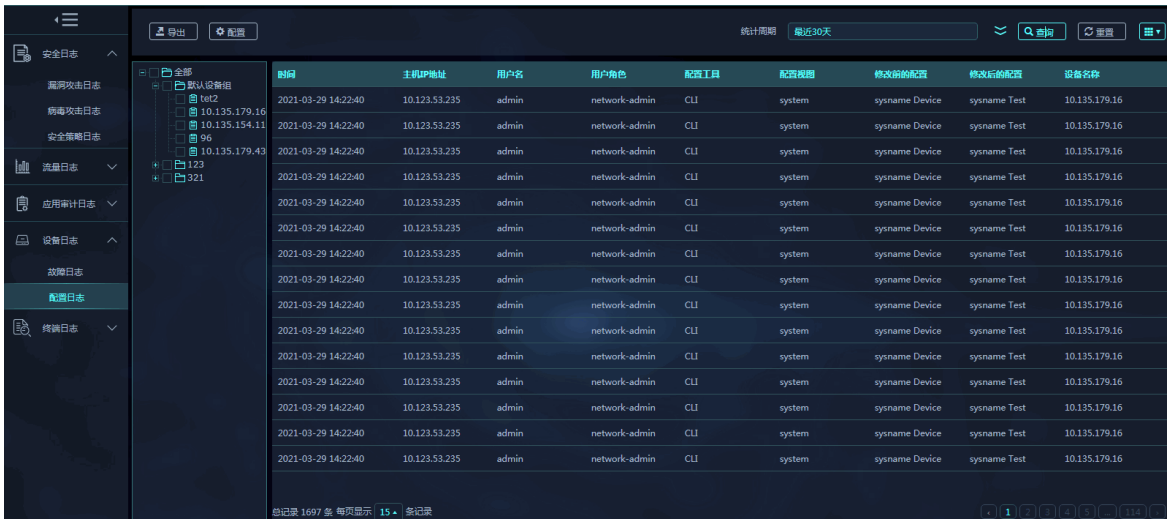
图6-8 故障日志



6.4.2 配置日志

在【日志中心> 设备日志 > 配置日志】页面，查看配置日志。

图6-9 配置日志



6.5 终端日志（选配）

6.5.1 终端识别日志

在【日志中心>终端日志 > 终端识别日志】页面，查看终端识别日志。

图6-10 终端识别日志

6.5.2 异常流量日志

在【日志中心> 终端日志 > 异常流量日志】页面，查看异常流量日志。

图6-11 异常流量日志

6.6 日志导出

6.6.1 前提条件

(1) SMP 平台已接入设备作为资产管理（详见 4.3 平台区域和错误!未找到引用源。错误!未找到引用源。）

(2) 接入设备的 NAT 日志、应用审计日志、安全策略日志、入侵防御日志与防病毒日志已配置日志主机（详见 4.2 设备协议及日志配置）

6.6.2 导出 EXCEL

在任意日志列表，点击高级查询，根据设备、源 IP、目的 IP 等条件查询日志，点击导出

以漏洞攻击日志导出举例，如下图：

6.7 黑白灰名单

SMP 支持对设备日志根据不同的参数条件（IP、端口、HOST、动作、特征 ID）筛选进行匹配，匹配的日志打上黑白名单标签，用于标识漏洞日志的黑白类型，未匹配黑白名单策略的日志为灰名单类型，日志查询检索支持根据黑白名单标签进行筛选；

SMP 支持导入黑白名单，Excel 最多支持导入 5000 条记录，导入黑白名单支持源 IP、真实源 IP 的网段形式。

6.7.1 前提条件

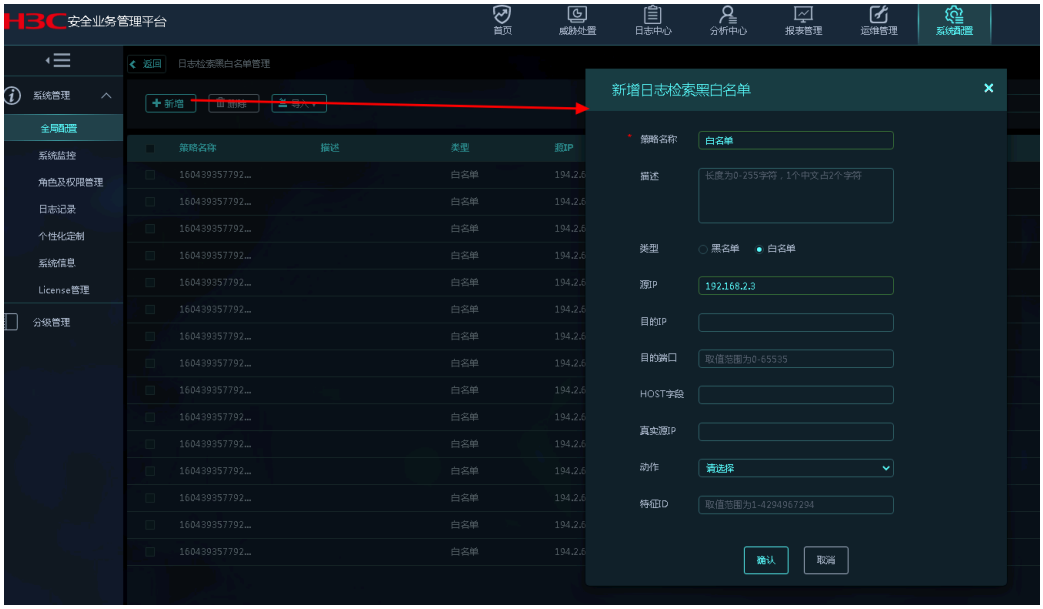
(1) SMP 平台已接入设备作为资产管理（详见 4.3 平台区域和错误!未找到引用源。错误!未找到引用源。）

(2) 接入设备的漏洞攻击日志（详见 4.2 设备协议及日志配置）

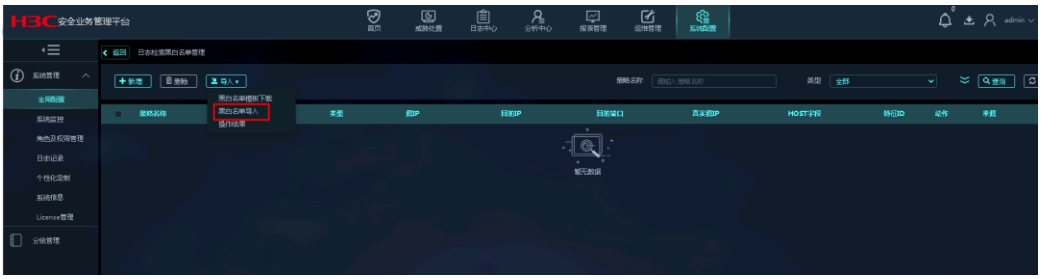
6.7.2 配置步骤

(1) 点击【系统配置】>【系统管理】>【全局配置】>【日志检索黑白名单】，创建黑、白名单：

a. 新增黑白名单方式：点击新增按钮，配置日志检索黑白名单参数。

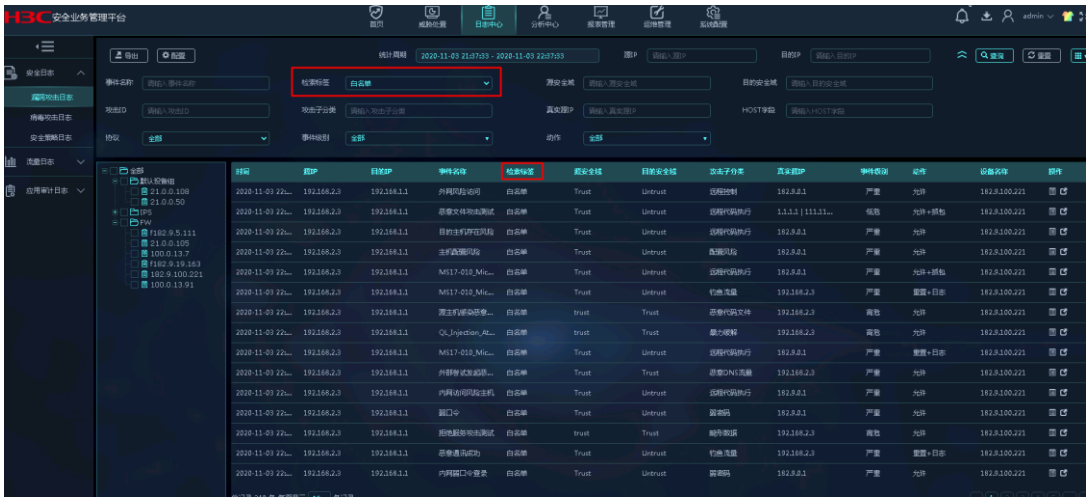


b. 导入黑白名单方式：点击导入－黑白名单导入，导入配置的黑白名单模板。

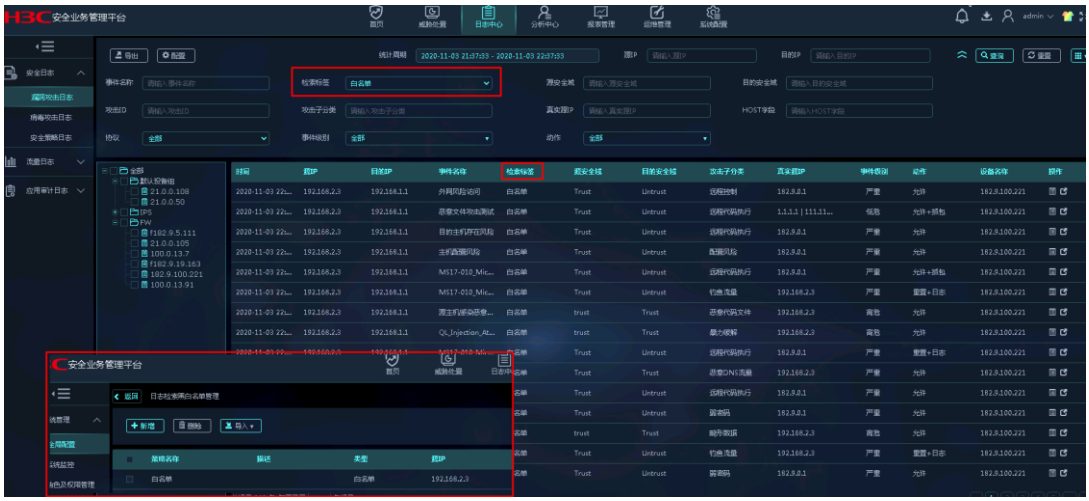


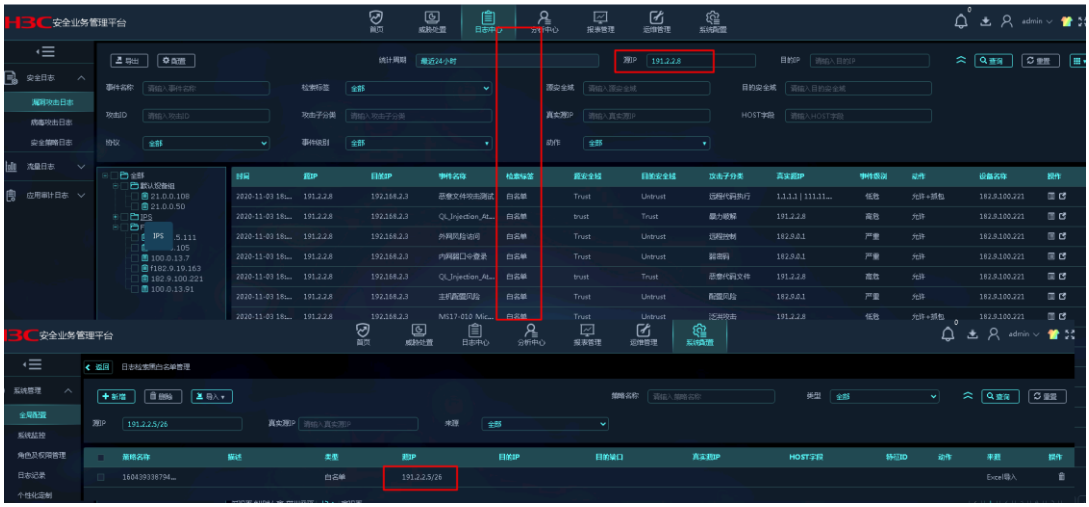
(2) 等待 30 秒，点击【日志中心】>【漏洞攻击日志】，点击定制列，勾选【检索标签】项：

(3) 点开高级查询，按类型进行查询：



(4) 漏洞攻击日志能够根据设置的黑白名单策略显示为对应的黑白名单，未匹配的与之前的日志检索标签为灰名单



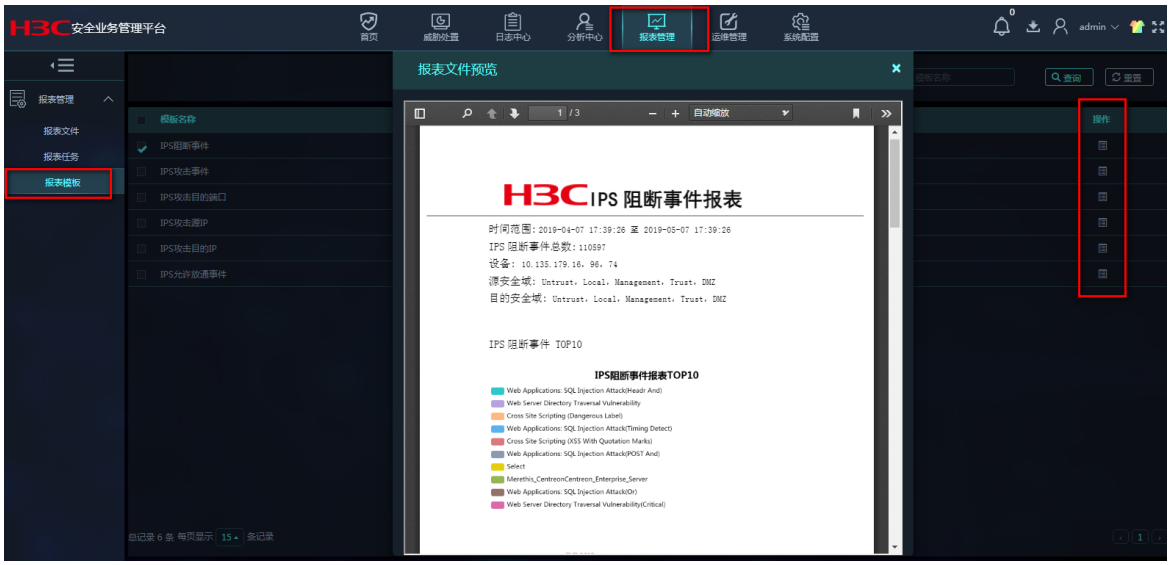


7 报表管理

7.1 报表模板

在【报表管理>报表管理>报表模板】页面，点击预览，查看报表模板

图7-1 报表模板预览



7.2 报表任务

新增报表任务，生成报表文件，根据不同的任务类型，可分为两大类型：周期性报表（日报、周报、月报，根据设置时间定时生成报告）、及时性报表（立即执行，可立即生成报告)。

(1) 在【报表管理>报表管理>报表任务】页面，点击新增按钮，新增报表任务

图7-2 新增报表任务页面

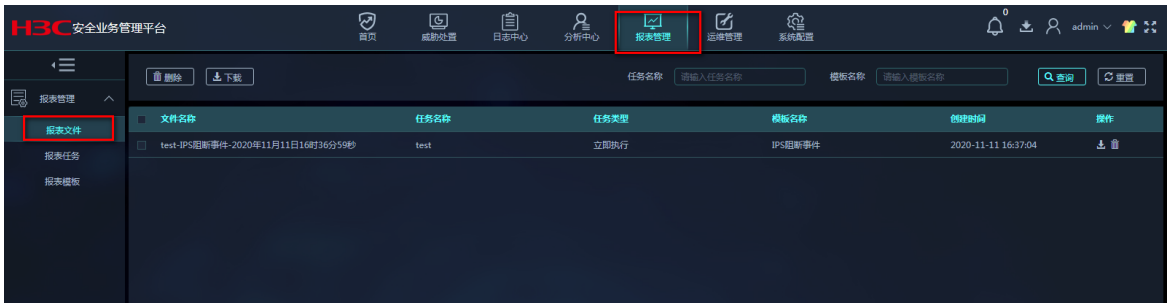
(2) 在【日志报表 > 报表管理>报表任务】页面，查看任务运行结果。

图7-3 报表任务运行结果

7.3 报表文件

展示报表文件列表，可查看文件名称、任务名称、任务类型等文件信息，用户可通过界面可以检索、下载、删除报表文件。

在【报表管理> 报表管理>报表文件】页面，选择生成的报表文件，点击下载。



8 分析中心

8.1 安全分析

安全事件分析通过对日志的分析，展示事件趋势图、事件对比图、攻击目的对比图、攻击源对比图、攻击协议对比图、攻击目的端口对比图。

说明：安全事件分析每天晚上 8 点开始进行统计分析，接入日志当天，报表无数据展示。

在【安全分析>安全事件分析】页面，选择周期，查看安全事件分析。

图8-1 安全事件分析页面

9 威胁处置

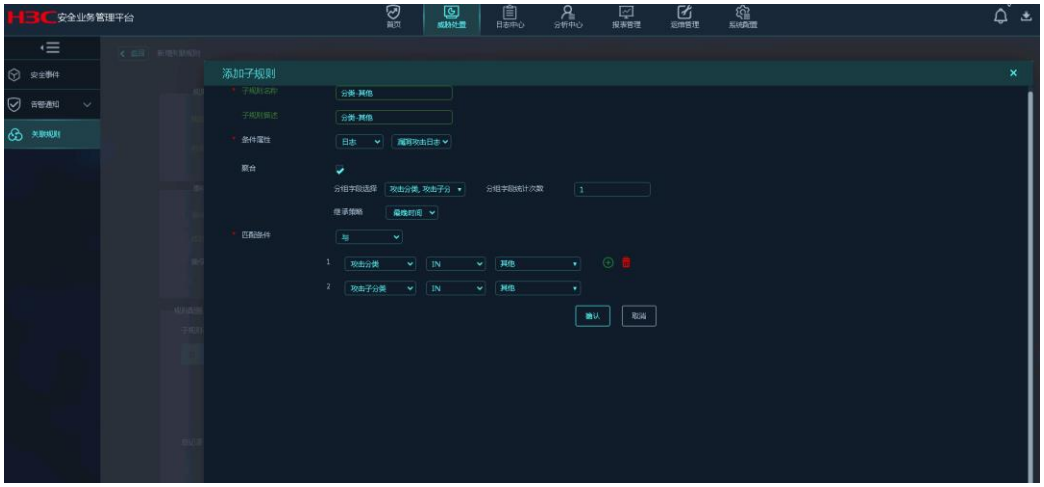
9.1 安全事件

SMP 平台支持设置关联规则生成安全事件并弹窗。

(1) 登录设备，点击系统-日志设置-威胁日志，选择输出快速日志，点击应用。点击系统-日志设置-基本配置-快速日志，设置日志主机为 SMP 平台地址；（勾选入侵防御日志）（详见文档 4.2.2 IPS/FW/LB 日志发送基本配置，如已配置请忽略）

(2) 在【威胁处置 > 关联规则】页面，使用预定义的关联规则生成事件或添加自定义的关联规则。

a. 新增自定义关联规则：填写必填项，点击添加规则，进入子规则配置页面，根据业务需求配置子规则后点击确认。



b. 启用关联规则：

c. 接入设备的威胁日志，点击安全事件，查看启用的预定义规则、自定义规则生成的安全事数；

d. 关联规则，查看规则命中次数

9.2 告警通知

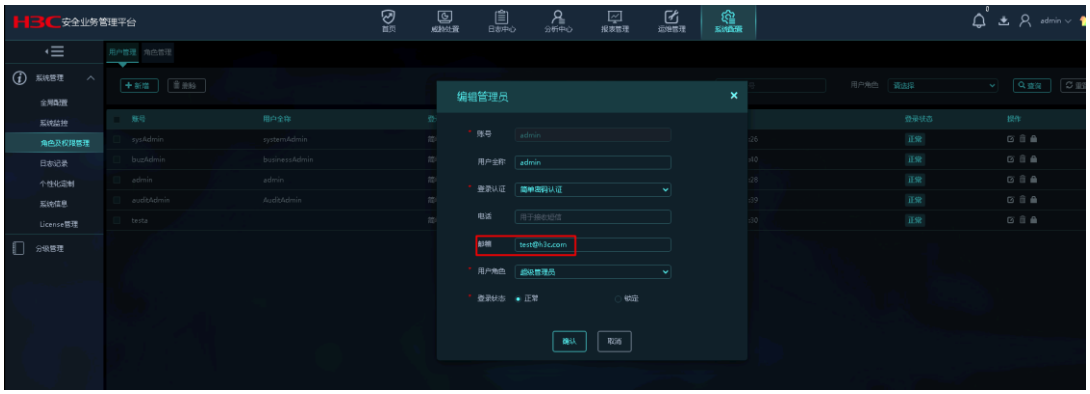
SMP 平台支持设置告警策略，推送告警邮件并形成告警记录。

(1) 登录设备，点击系统-日志设置-威胁日志，选择输出快速日志，点击应用。点击系统-日志设置-基本配置-快速日志，设置日志主机为 SMP 平台地址；（勾选入侵防御日志）（详见文档 4.2.2 IPS/FW/LB 日志发送基本配置，如已配置请忽略）

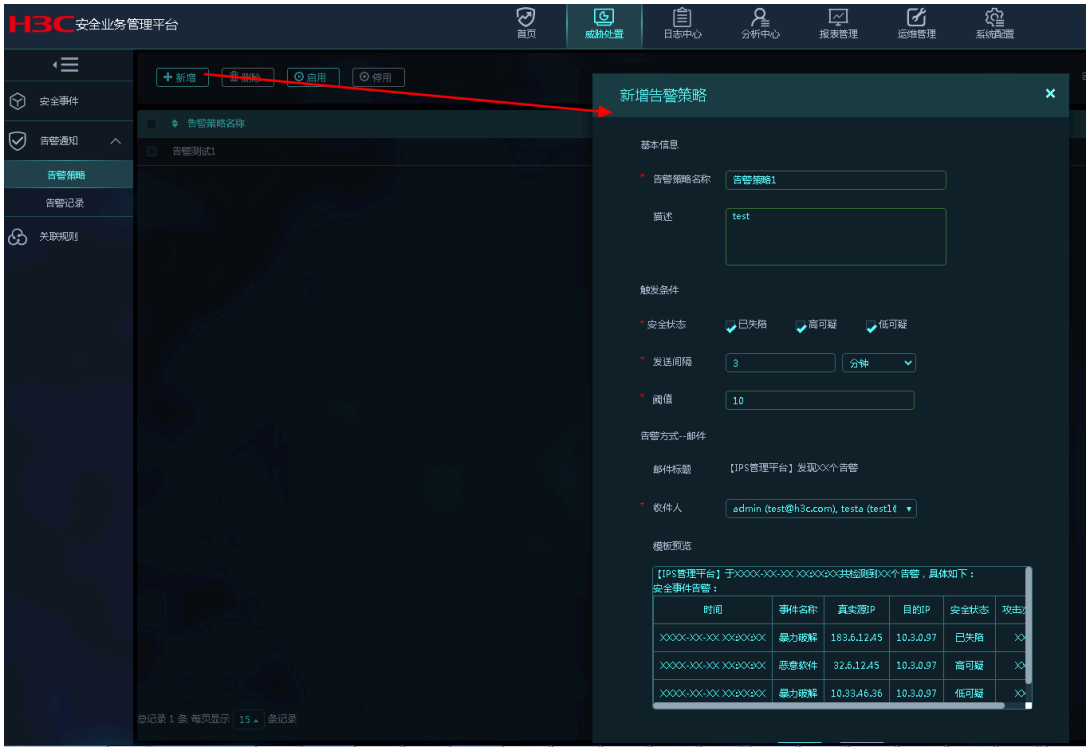
(2) 点击【运维管理】>【资产监控】，新增设备为资产（详见 4.3 平台区域和**错误!未找到引用源。错误!未找到引用源。**），如已配置，请忽略。

(3) 点击【系统配置】>【系统管理】>【全局配置】>【邮件服务器】，配置邮件服务器参数。

(4) 点击【系统配置】>【系统管理】>【角色及权限管理】，为用户绑定邮箱。

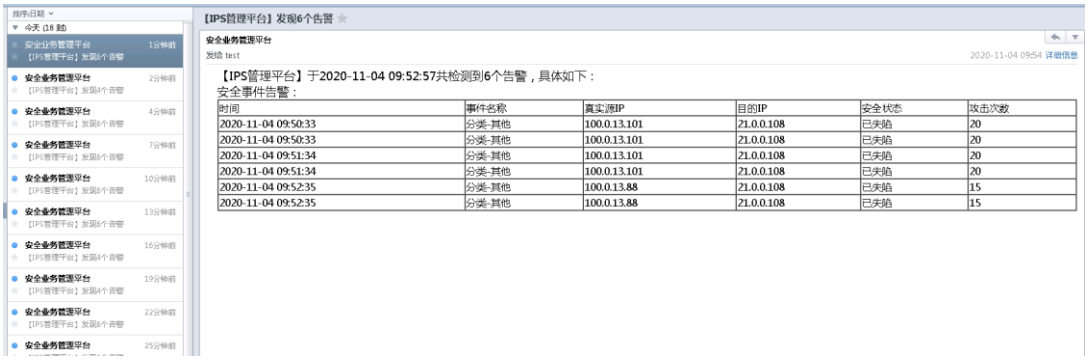


(5) 点击【威胁处置】>【告警通知】>【告警策略】，配置告警策略。



(6) 点击关联规则，确保有启用的关联规则。

(7) 等待 2 分钟，点击告警事件，待产生告警事件后，点开接收邮箱。



(8) 点击告警事件-安全告警-告警记录。

10 视频监控（选配）

10.1 终端资产管理

本功能是对终端资产的管理，包括所有终端、新发现终端和非法终端三个模块，可查看具体的终端信息并支持终端信息的新增、修改、删除、批量审批、导入、封堵、放通功能。

1. 所有终端

本功能包含了新发现终端和非法终端的所有终端信息，支持终端信息的新增、修改、删除、批量审批、导入、封堵、放通功能，支持多条件查询终端信息。

2. 新识别终端

新发现终端是为了展示主动采集和被动流量识别所发现的终端，包括视频终端和其他终端，支持多条件查询和批量审批、封堵、放通功能，其中批量审批、封堵、放通功能和所有终端页面中的功能是相同的操作。

3. 非法终端

用于集中展示合规状态为非法的终端，支持多条件查询和终端批量审批、封堵/放通功能。

10.2 业务分析

本功能包括异常流量、NAT 网中网、弱口令三个模块，是通过分析异常流量日志、终端识别日志和弱口令的漏洞攻击日志生成的。

1. 异常流量

异常流量是对异常流量日志的分析，支持异常流量事件的批量处理、一键处理、封堵/放通、原始事件数的下钻页查看。

一键处理/批量处理：选择一条或多条异常流量，可批量处理成已处理或未处理的状态。单击一键处理能把所有的未处理异常流量修改成已处理的状态。

2. NAT 网中网

NAT 网中网是对异常流量日志和终端识别日志的分析，支持 NAT 网中网的批量处理、一键处理、封堵/放通功能，原始事件数的下钻页查看。并支持 NAT 网中网匹配条件配置，包括流量阈值、时间周期、终端指纹阈值。

识别规则配置：

在【视频监控> 业务分析 > NAT 网中网】页面，查看生成的 NAT 网中网事件列表

3. 弱口令

弱口令是通过分析攻击子分类为弱口令的漏洞攻击日志而生成的，支持弱口令事件的批量处理、一键处理、封堵/放通功能，原始事件数的下钻页查看。

在【视频监控> 业务分析 >弱口令】页面，查看生成的弱口令事件列表

10.3 网关管理

1. 全局配置

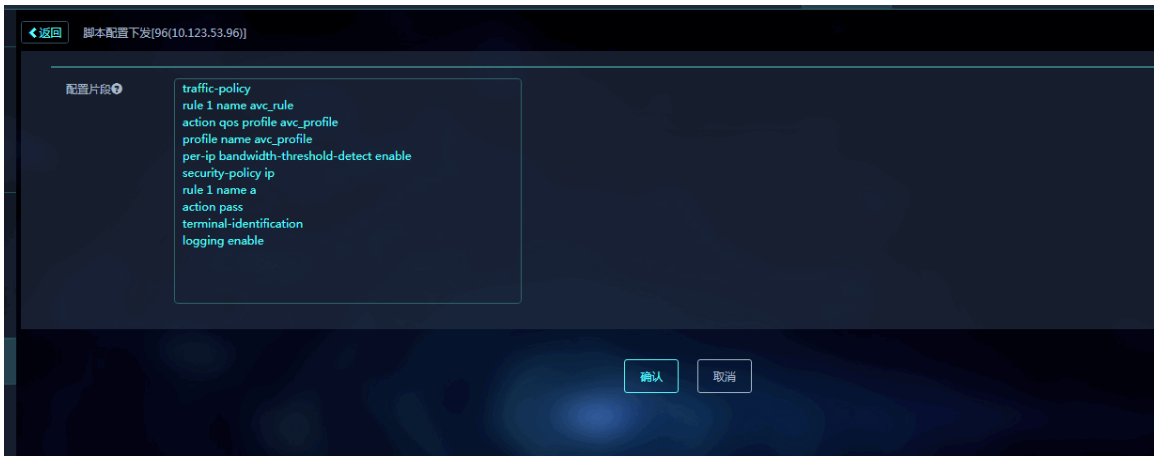
可配置白名单模式为 IP 或 MAC 模式，其中 MAC 模式下不可修改终端识别模式。 终端识别模式可选择告警模式或白名单模式。

2. 白名单配置

如果全局配置为 IP 模式，通过单击白名单配置后进入的是 IP 白名单配置页面，可新增，修改或删除成员。如果全局配置为 MAC 模式，单击白名单配置后进入的是 MAC 白名单配置页面， 也可新增，修改或删除成员。

3. 脚本配置下发

单击脚本配置下发后进入脚本配置下发页面，默认有一些预定义的配置片段，可通过修改配置后直接下发给设备。



4. 封堵详情

单击封堵详情后，可查看此设备的封堵详情。

11 应用交付管理（选配）

11.1 应用负载监控

本功能是应用交付设备的监控，包括虚服务器、服务池和业务主机，可查看具体的监控信息并支持趋势统计功能。

1. 虚服务器

本功能包含了监控负载均衡设备虚服务器设备名称、状态、槽号、连接数、带宽，支持趋势统计。趋势统计页面用来显示虚服务器统计信息随时间的变化情况，方便管理员更直观的获取虚服务器信息。

2. 服务池

本功能包含了监控负载均衡设备服务池设备名称、状态、成员总数、可用成员数、槽号、连接数，支持趋势统计。趋势统计页面用来显示服务池统计信息随时间的变化情况，方便管理员更直观的获取服务池信息。

3. 业务主机

本功能包含了监控负载均衡设备业务主机设备名称、状态槽号、连接数、带宽，支持趋势统计。趋势统计页面用来显示业务主机统计信息随时间的变化情况，方便管理员更直观的获取业务主机信息。

11.2 应用负载配置

1. 虚服务器

虚服务器是负载均衡设备上面向用户业务的虚拟载体，是为了判断是否需要对进入负载均衡设备的报文进行负载均衡。只有匹配上虚服务器的报文才会被进行负载均衡处理。

配置步骤：点击【运维管理】>【应用负载配置】>【虚服务器】进行虚服务器配置的增删改查。

2. 服务池

为了便于对业务主机进行统一管理，可将具有相同或相似功能的业务主机抽象成一个组，称为服务池。比如，可按存储内容的不同划分为歌曲服务池、视频服务池和图片服务池等。服务池可被虚服务器或动作引用。

配置步骤：点击【运维管理】>【应用负载配置】>【服务池】进行服务池配置的增删改查。

3. 业务主机

业务主机是负载均衡设备上处理用户业务的实体。一个业务主机可以属于多个服务池，一个服务池也可以包含多个业务主机。

配置步骤：点击【运维管理】>【应用负载配置】>【业务主机】进行服务池配置的增删改查。

4. 负载均衡策略（选配）

将流量特征和动作关联起来就构成了负载均衡策略。负载均衡策略是指导报文转发的一种方式，用户可以为匹配特定流量特征的报文指定执行的动作，以及为未匹配任何流量特征的报文指定默认动作。用户可以在一个负载均衡策略中指定多个流量特征，转发报文时会按照配置顺序来匹配流量特征，匹配成功则执行相应的动作，否则继续匹配下一条流量特征。如果所有流量特征均未匹配，则执行默认动作。负载均衡策略可被虚服务器引用。

配置步骤：点击【运维管理】>【应用负载配置】>【负载均衡策略】进行负载均衡策略配置的增删改查。