

**SANGFOR 安全感知平台**

**快速安装手册**



# 

# 技术支持说明

为了让您在安装，调试、配置、维护和学习SANGFOR 设备时，能及时、快速、有效的获得技术支持服务，我们建议您：

1. 参考快速安装手册图文指导，帮助你快速的完成部署、安装SANGFOR设备。如果快速安装手册不能满足您的需要，您可以到深信服社区或官网获取电子版的完整版用户手册或者其他技术资料，以便您获得更详尽的信息。
2. 致电您的产品销售商（合同签约商），寻求技术支持。为了更快速地响应您的服务要求和保证服务质量，您所在地的SANGFOR的产品销售商配备有经过厂家认证的技术工程师，会向您提供快捷的电话咨询、远程调试及必要的上门技术服务。
3. 在不紧急的情况下，您可以访问深信服社区，寻求技术问题的解决方案和办法。
4. 致电深信服科技技术服务中心，确认最适合您的服务方式和服务提供方，技术服务中心会在您的技术问题得到解决后，帮助您获得有效的服务信息和服务途径，以便您在后续的产品使用和维护中最有效的享受技术支持服务，及时、有效的解决产品使用中的问题。

用户支持邮箱：support@sangfor.com.cn

技术支持热线电话：400-630-6430（手机、固话均可拨打）

深信服社区：bbs.sangfor.com.cn

深信服科技服务商及服务有效期查询：http://bbs.sangfor.com.cn/plugin.php?id=service:query

公司网址：[www.sangfor.com.cn](http://www.sangfor.com.cn)

返修查询，在线咨询，欢迎您关注深信服科技官方技术服务微信：



**目 录**

[技术支持说明 1](#_Toc20413)

[声明 3](#_Toc6373)

[前言 4](#_Toc21204)

[第一章 SIS、STA 系列硬件设备的安装 5](#_Toc13249)

[1.1环境要求 5](#_Toc14330)

[1.2.电源 5](#_Toc31938)

[1.3.产品接口说明 6](#_Toc9919)

[1.4.配置与管理 7](#_Toc14775)

[第二章：SIS、STA系列硬件设备的部署 10](#_Toc8243)

[2.1 SIS和STA常规环境部署案例 11](#_Toc22533)

[2.1.1 SIS配置步骤： 12](#_Toc21104)

[2.1.2 STA1配置步骤 23](#_Toc4732)

[2.1.3 STA2配置步骤 33](#_Toc17821)

[2.1.3 STA3配置步骤 35](#_Toc3806)

[2.2 SIS和STA 在多分支环境部署案例 39](#_Toc5602)

[2.2.1 SIS配置步骤 40](#_Toc30833)

[2.2.2 STA配置步骤 46](#_Toc18980)

[2.3 SIS和STA 在DNS环境部署案例 51](#_Toc2135)

[2.3.1 SIS配置步骤 52](#_Toc5512)

[2.3.2 STA配置 53](#_Toc12680)

[第三章 ：密码安全风险提示 54](#_Toc514)

[3.1修改后台密码 54](#_Toc5525)

[附件一：主流交换机厂商镜像口流量配置 56](#_Toc13446)

[华为： 56](#_Toc20648)

[华三： 56](#_Toc16273)

[锐捷： 57](#_Toc24154)

[思科： 57](#_Toc24353)

[附件二：NGAF 7.5版本对接安全感知平台配置 58](#_Toc9811)

[附件三：产品接口列表 58](#_Toc4445)

# 声明

Copyright © 2000-2018深信服科技股份有限公司及其许可者版权所有，保留一切权利。

未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

深信服科技股份有限公司（以下简称为深信服科技、SANGFOR）。

SANGFOR为深信服科技股份有限公司的商标。对于本手册出现的其他公司的商标、产品标识和商品名称，由各自权利人拥有。

除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。

本手册内容如发生更改，恕不另行通知。

如需要获取最新手册，请联系深信服科技股份有限公司客户服务部。

# 前言

本手册仅介绍SIS、STA设备安装部署的配置指导和最基本使用方法，如需要更详细配置介绍，请登录深信服社区下载详细电子版用户手册。深信服社区访问地址: <http://bbs.sangfor.com.cn>。

SIS与STA说明：

SIS为安全感知平台，用于分析探针上传过来的流量数据，基于大数据、机器学习对数据进行汇总分析处理。通过安全总览，大屏等方式，使得全网安全可视。

STA为探针，是数据收集设备，用于收集交换机镜像的流量，收集的流量主要包括用户区域-->互联网区域、业务区域 -->互联网区域、用户区域 -->业务区域、用户区域-->用户区域、业务区域-->业务区域，之间的访问流量。

**本手册以深信服**SIP-1000-D602 **STA 100为例进行说明。各型号产品硬件规格存在一定差异， 但是设备配置以及基本使用方法一致，本手册适用于所有型号的SIS、STA设备。**

[第一章 SIS、STA 系列硬件设备的安装](#page7)

本部分主要介绍了 SANGFOR SIS和SANGFOR STA系统产品的硬件安装。硬件安装正确之后，您方可进行配置与调试。

## 1.1环境要求

为保证系统能长期稳定地运行，应保证电源有良好的接地措施、防尘措施、保持使用环境的空气通畅和室温稳定。本产品符合关于环境保护方面的设计要求，产品的安放、使用和报废应遵照国家相关法律、法规要求进行。

## 1.2.电源

SANGFOR SIS和SANGFOR STA系列硬件设备使用交流110V到230V电源。在您接通电源之前，请保证您的电源有良好的接地措施。

## 1.3.产品接口说明



**SANGFOR STA**前面板图（以STA 100为例）

|  |  |  |
| --- | --- | --- |
| **序号** | **网口编号** | **网口类型** |
| 1 | CONSOLE(控制) |  |
| 2 | MANAGE口(ETH0) | 千兆电口 |
| 3 | ETH1 | 千兆电口 |
| 4 | ETH2 | 千兆电口 |
| 5 | ETH3 | 千兆电口 |
| 6 | ETH4 | 千兆光口 |
| 7 | ETH5 | 千兆光口 |



**SANGFOR SIS**前面板图（以SIP-1000-D602为例）

|  |  |  |
| --- | --- | --- |
| 设备名称 | 网口编号 | 网口类型 |
| SIP-1000-D602 | ETH1 | 千兆电口 |
| ETH2 | 千兆电口 |
| ETH3 | 千兆电口 |
| ETH4 | 千兆电口 |
| ETH5 | 千兆电口 |
| ETH6 | 千兆电口 |
| ETH7 | 万兆光口 |
| ETH8 | 万兆光口 |

1.图片仅供参考，不同型号的产品外观请以实物为准。

2. CONSOLE口仅供开发和测试调试使用。最终用户需通过网口接入设备。

1.4.配置与管理

设备出厂的默认IP见下表：

SIS：

|  |  |
| --- | --- |
| 接口 | IP地址 |
| ETH0 | 10.251.251.252/24 |

STA：

|  |  |
| --- | --- |
| 接口 | IP地址 |
| MANAGE口(ETH0) | 10.251.251.251/24 |

SIS、STA设备只支持安全的HTTPS登录，使用的是HTTPS协议的标准端口（443端口）登录。

\*注：建议使用chrome、firefox浏览器登录SIS平台。

**如何登录SIS设备控制台页面？**

将电脑网卡与SIS设备ETH0口接在同一个二层交换机或者直接将ETH0口和电脑网卡用网线连接，通过WEB界面来配置SANGFOR SIS设备。方法如下：

首先为本机器配置一个10.251.251.X网段的IP（如配置10.251.251.100掩码255.255.255.0），然后在chrome浏览器中输入SIS的默认登陆IP及端口https://10.251.251.252。在出现一个如下图的安全提示：



点击高级->继续前往10.251.251.252（不安全）

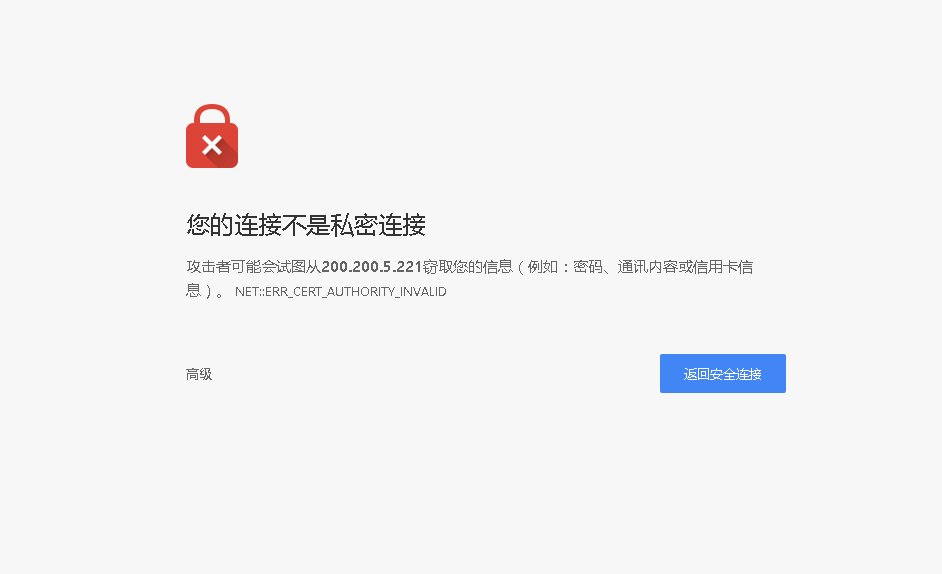


在登录框输入『用户名』和『密码』，点击登录按钮即可登录SIS设备进行配置，默认情况下的用户名和密码为admin/admin。

**如何登录STA设备控制台页面？**

将电脑网卡与STA设备MANAGE口（ETH0）接在同一个二层交换机或者直接将MANAGE口（ETH0）口和电脑网卡用网线连接，通过WEB界面来配置SANGFOR STA设备。方法如下：

首先为本机器配置一个10.251.251.X网段的IP（如配置10.251.251.100掩码255.255.255.0），然后在chrome浏览器中输入STA的默认登陆IP及端口https://10.251.251.251。在出现一个如下图的安全提示：



点击高级->继续前往10.251.251.252（不安全）



在登录框输入『用户名』和『密码』，点击登录按钮即可登录SIS设备进行配置，默认情况下的用户名和密码为admin/admin。

# 第二章：SIS、STA系列硬件设备的部署

本部分主要介绍了SANGFOR SIS和SANGFOR STA系列产品的部署方式和配置方法

## 2.1 SIS和STA常规环境部署案例

**客户环境与需求：**某用户网络是三层环境，需要检测内网用户之间；服务器之间；用户与服务器之间；用户与互联网之间的风险情况。感知平台与探针都使用旁路模式部署。

感知平台部署：

\* 感知平台ip需要与探针管理口ip通信，接收探针发来的数据。SIS eth0口配置ip为192.168.1.100；STA\_1 eth0口配置ip192.168.1.101；STA\_2 eth0口配置ip192.168.1.102；STA\_3 eth0口配置ip192.168.1.103；

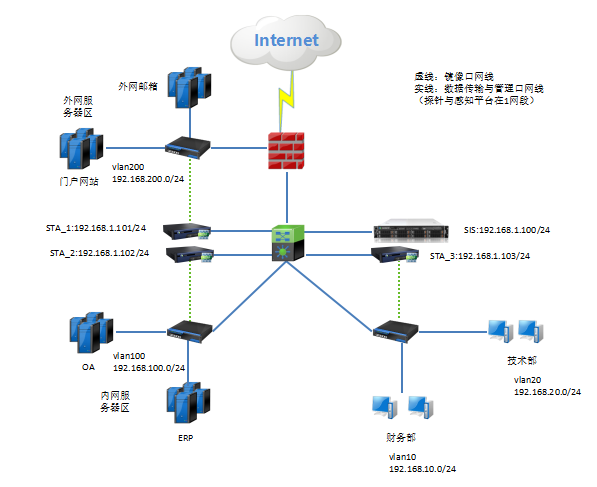
探针部署：

\* 收集用户与用户之间的流量，需要在客户的接入交换机上做一个镜像口给探针。

\* 收集内网服务器之间的流量，需要在内网服务器的接入交换机上做一个镜像口给探针。

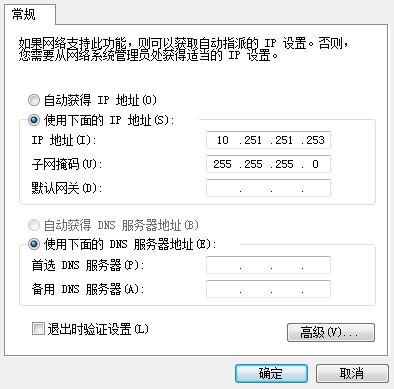
\* 收集外网服务器之间的流量，需要在外网服务器的接入交换机上做一个镜像口给探针。

\* 需要收集的流量包括，用户区域-->互联网区域、业务区域-->互联网区域、用户区域-->业务区域、用户区域-->用户区域、业务区域-->业务区域。



### 2.1.1 SIS配置步骤：

第一步：首先将设备开机，用网线接设备的EHT0，将电脑网卡的IP配置成10.251.251.253，界面如下：



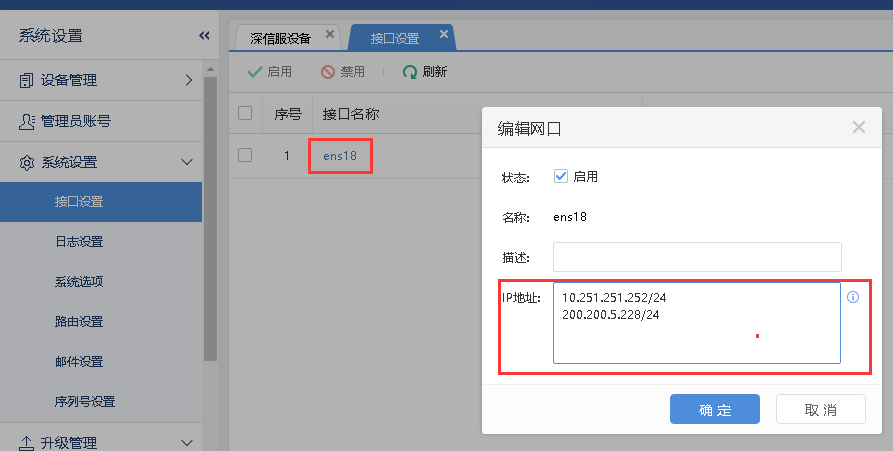
第二步：打开chrome浏览器，输入https://10.251.251.252，即可到登录界面，输入设备出厂默认的账号密码admin/admin，界面如下：



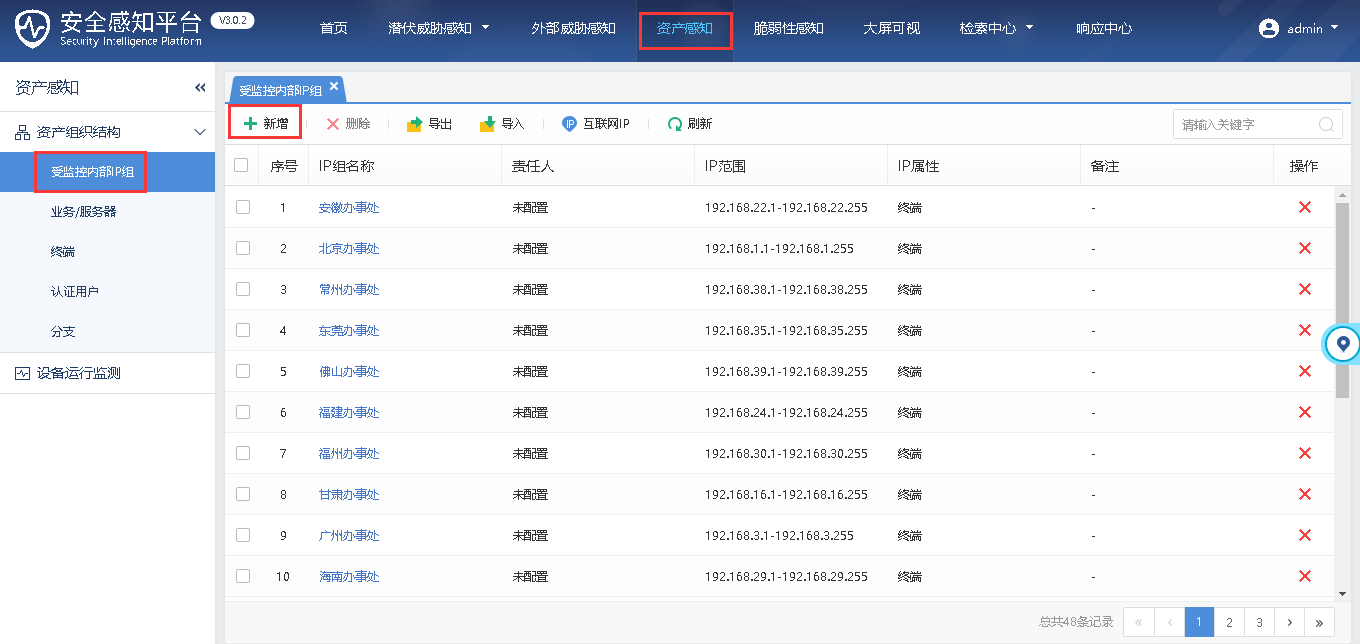
第三步：配置网口ip用于管理及接收探针数据。（非eth0口需要先接上网线并网口灯亮起后再启用网口，配置ip地址）



点击对应接口的“接口名称”可以添加IP地址。



第四步：配置资产，资产感知->资产组织结构->受监控内部IP组->新增



点击“新增”



【IP组名称】：定义IP组的名称，如行政部门（用户）、内网服务器（服务器）。

【IP属性】：所需要定义的IP范围为终端、服务器，若IP范围是终端、服务器都存在的，可以配置不“未配置”让系统自动识别。

【责任人】：所定义的IP范围的负责人，方便后续出现安全问题查找到相应的负责人。

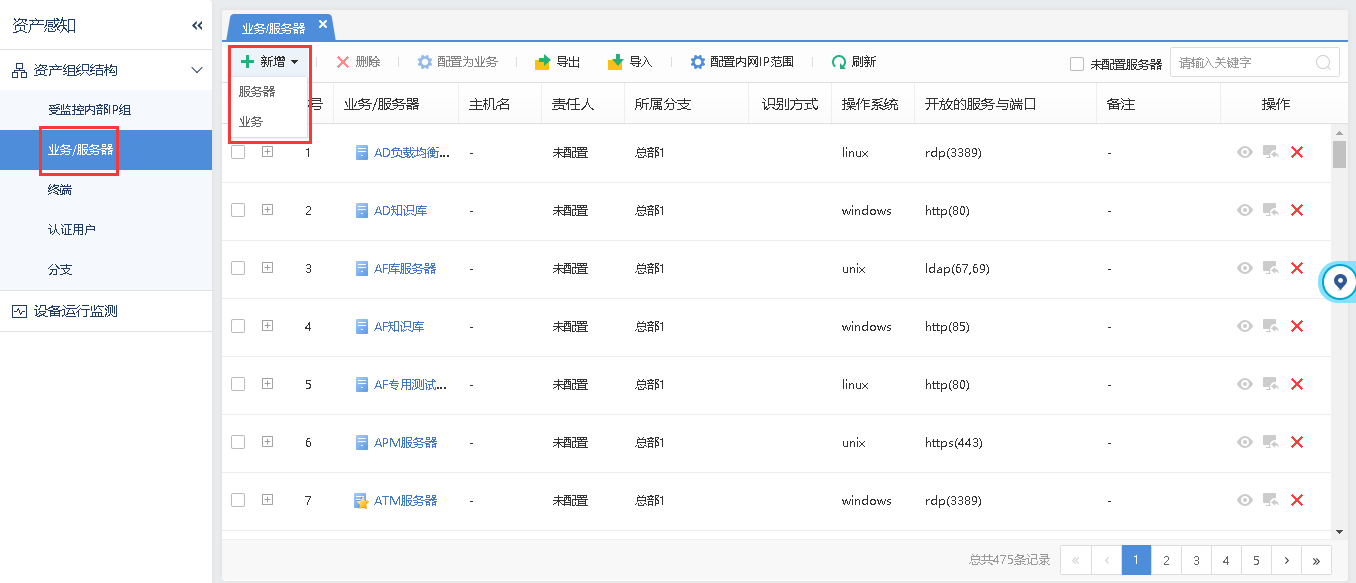
【责任人邮箱】：所定义的IP范围的负责人邮箱，方便后续出现安全问题联系到相应的负责人。

【IP范围】：配置所定义IP组的IP范围。如IP组名为行政部门，网段为192.168.11.0/24则IP范围配置为192.168.11.0/24网段。

【备注】对该定义的IP组进行备注说明。

第六步：业务/服务器配置

在配置完成第五步时可以先将探针进行对接，自动上传网络中发现的服务器。则些处只需要配置业务即可。



新增选择新增【业务】。



【业务名称】：定义服务器所提供的业务，如服务器192.168.0.51提供服务器OA，则业务名称可配置为OA系统

【重要级别】：可配置业务系统的重要级别，在后续发生安全事件可突出显示。

【责任人】：所定义的IP范围的负责人，方便后续出现安全问题查找到相应的负责人。

【责任人邮箱】：所定义的IP范围的负责人邮箱，方便后续出现安全问题联系到相应的负责人。

【备注】对该业务进行备注说明。

【配置服务器资产】可从已知服务器添加，即添加自动发现的服务器或手动添加的服务器。

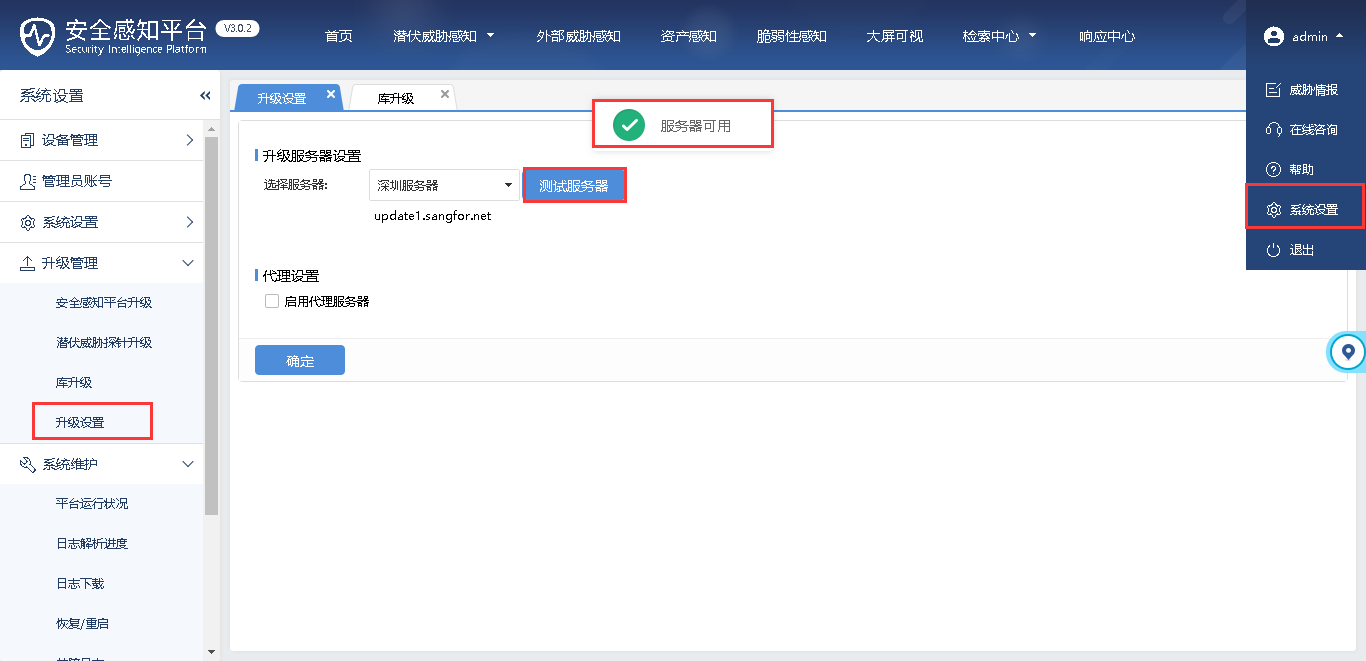
第七步：开启分析行为日志

需要探针开启高级后有效

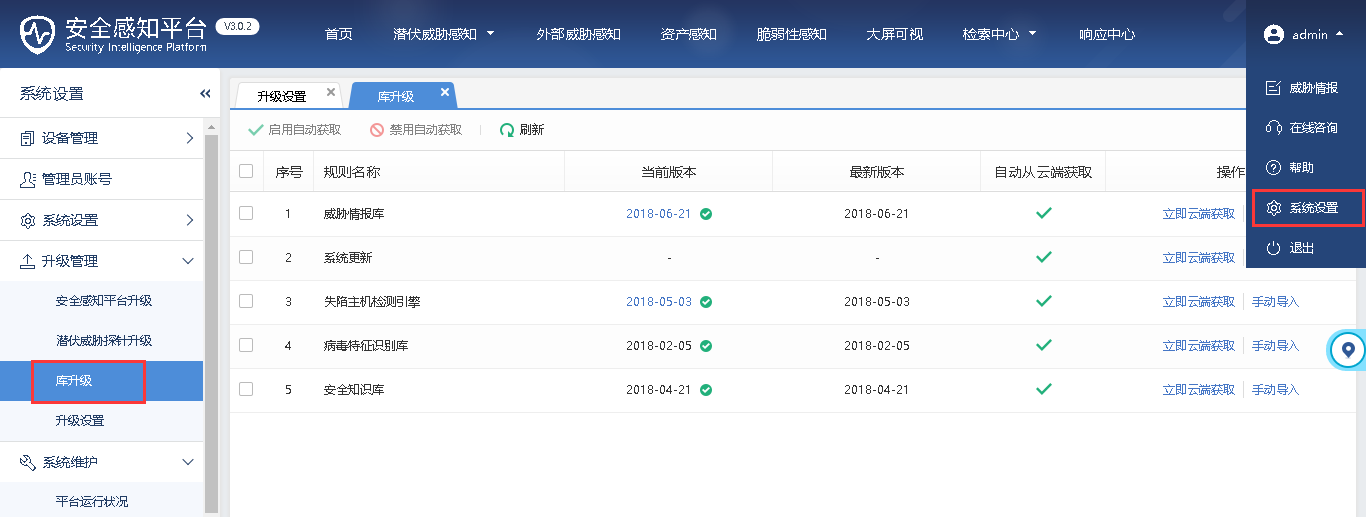


第八步：特征库检查

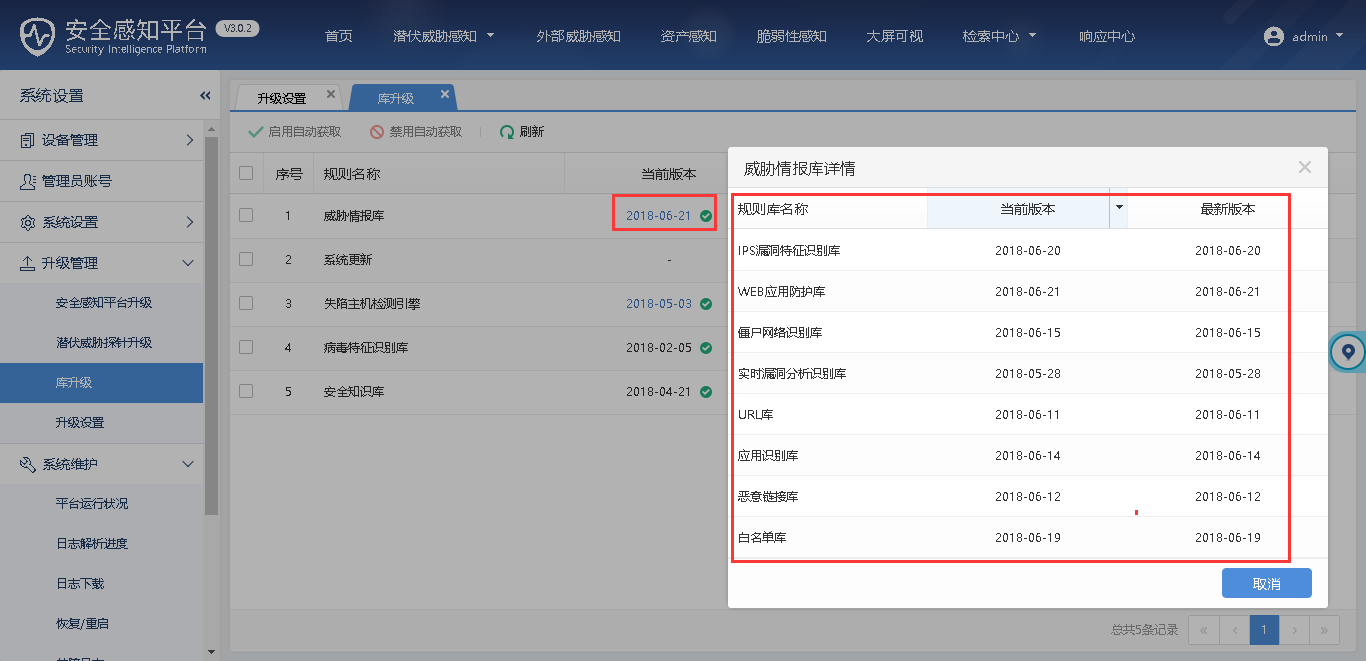
检测升级服务器连接情况。需要设备能连接互联网，点击“测试服务器”可确认设备是否连接升级服务器成功。



查看当前特征库是否与当前时间在一个月内。

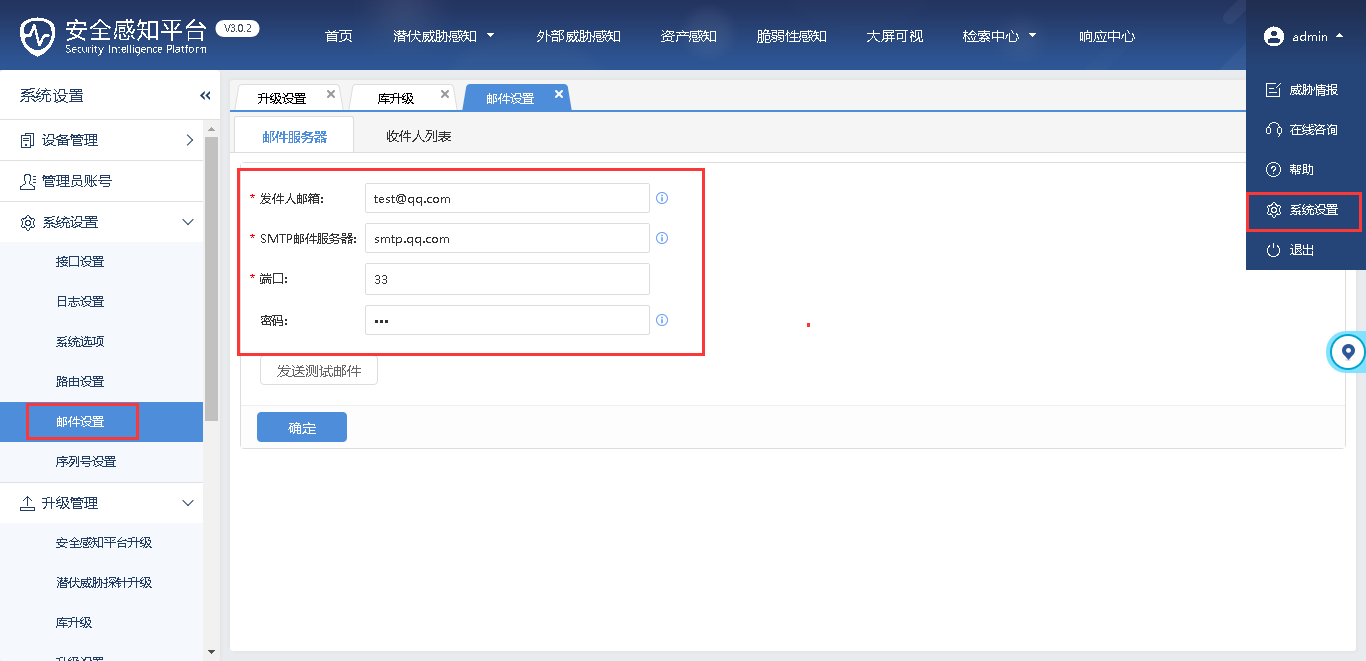


点击“当前版本”时间可以查看具体特征库的版本，例如点击“威胁情报库”



第九步：邮件告警功能

配置完成点击“发送测试邮件”可能会被识别为垃圾邮件，也请检查邮箱的垃圾邮件。



【发件人邮箱】：配置发送告警邮件或报报邮件的发送邮箱。

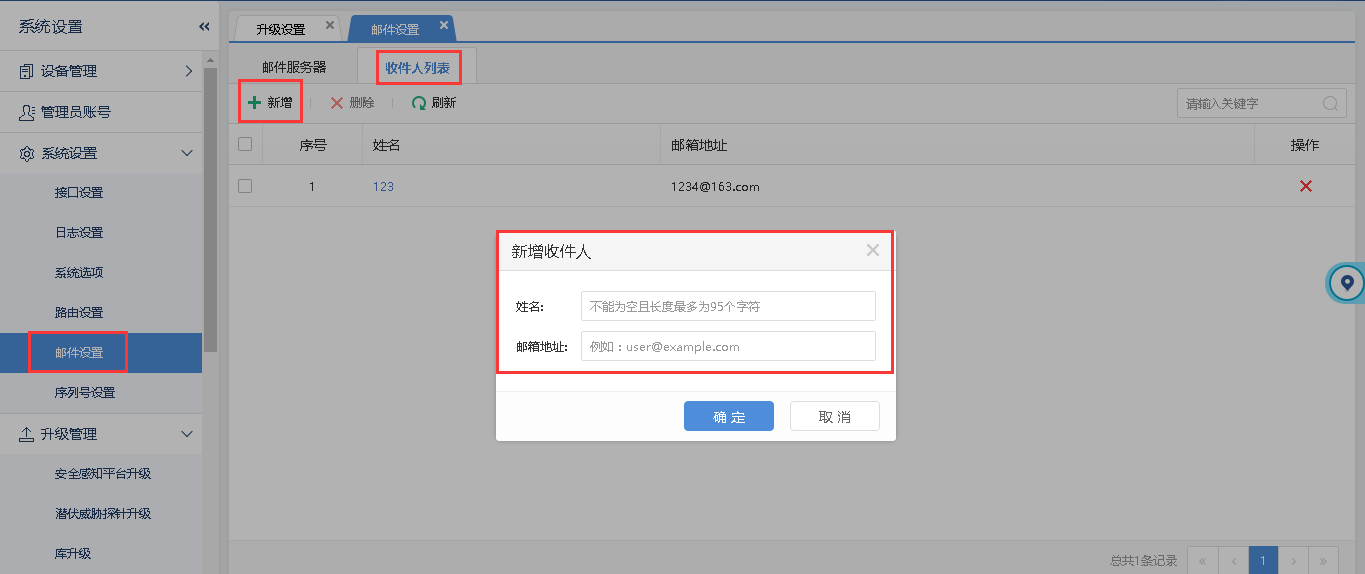
【SMTP邮件服务器】：所用邮箱的SMTP地址

【端口】：SMTP服务器的端口，默认为25端口。

【密码】：邮箱的登录密码，邮箱不能有二次认证。

第十步：配置收件人列表

收件人列表用于后续告警邮件或报告邮件配置时的调用。



【姓名】：用于备注邮件地址的收件人。

【邮箱地址】：后续用于接收邮件的地址。

第十一步：配置安全告警策略

可通过邮件发送“发现风险终端”、“发现风险业务资产”、“遭受攻击成功事件”的告警邮件



例如点击“发现风险终端”



【监控的IP地址】：配置需要监控的IP地址范围。

【发送间隔】：设置邮件发送的间隔。

【安全等级】：可选择需要告警的安全等级

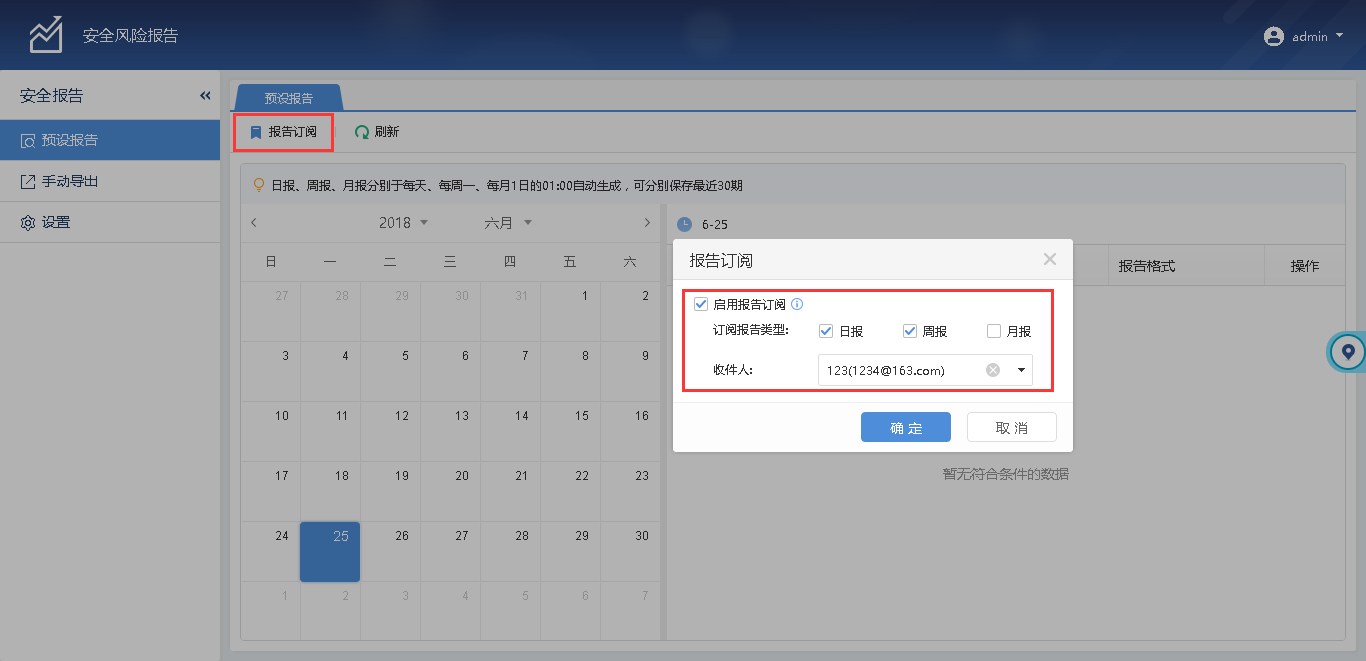
【收件人】：选择需要接收该告警邮件的邮箱地址，若些处为空，则默认只发给邮件告警设置中的统一收件人。



【邮件发送设置】：告警策略都会发送给“统一收件人”。

第十二步：预设报告

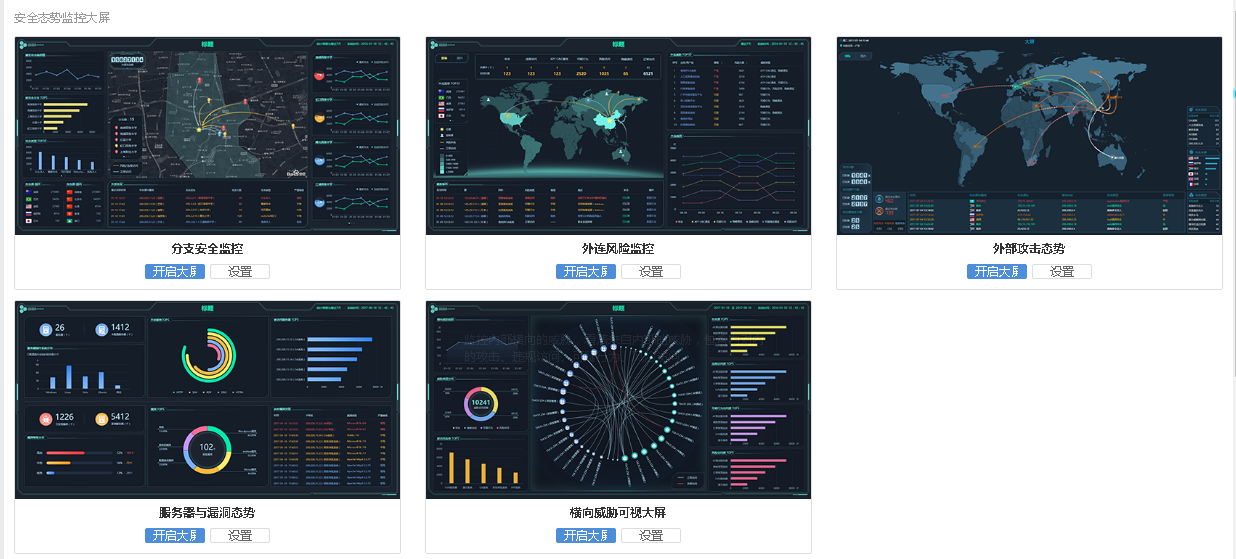




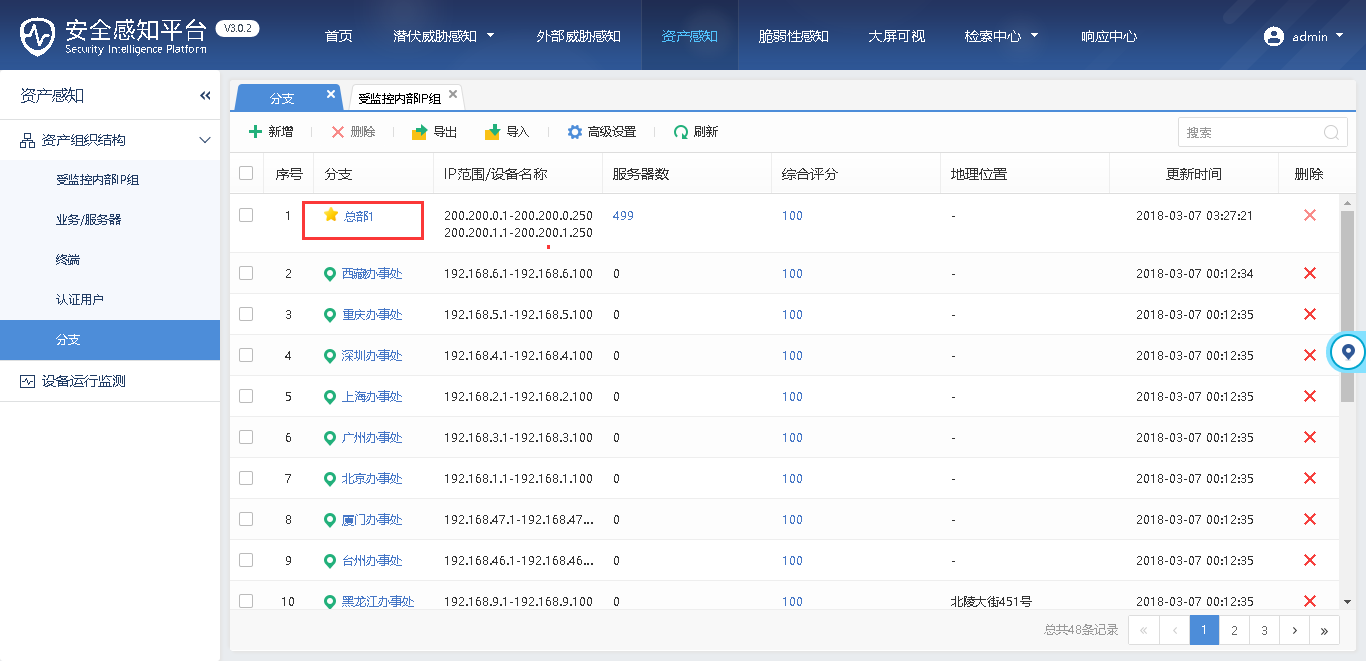
【报告订阅】：可选择“日报”、“周报”、“月报”。

【收件人】：指定需要接收人的邮件地址。

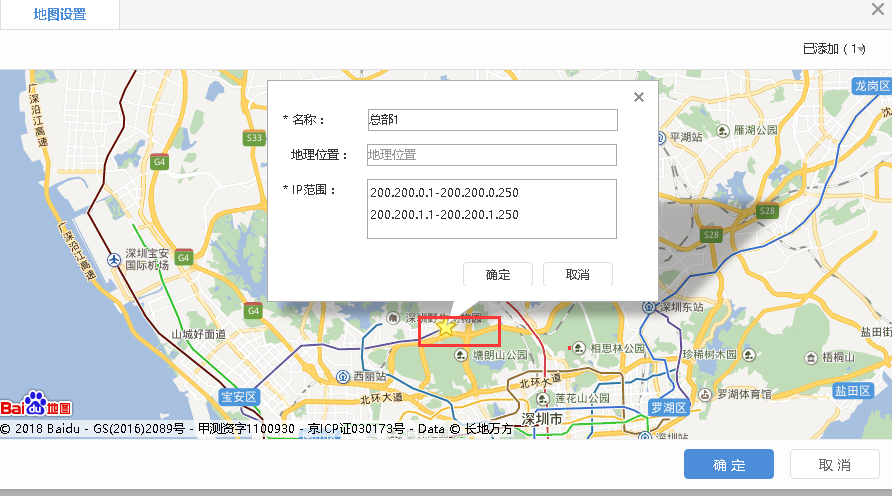
第十三步：大屏位置修改



【分支安全监控】位置为地方为【资产感知】->【分支】

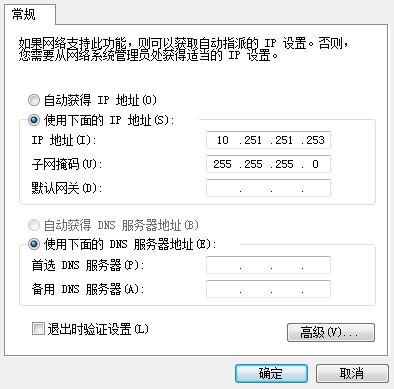


拖动“星”的位置，可修改大屏总部的位置。



### 2.1.2 STA1配置步骤

第一步：首先将设备开机，用网线接设备的EHT0，将电脑网卡的IP配置成10.251.251.253，界面如下：



第二步：打开chrome浏览器，输入https://10.251.251.251，即可到登录界面，输入设备出厂默认的账号密码admin/admin，界面如下：



第三步：网络配置->物理接口

点击eth0可配置网口IP地址，10.251.251.251不能删除只再添加需要的IP地址。

类型为路由口。所配置的IP地址需要能与SIP进行通信。



【类型】：管理口的类型必须为路由。

【连接类型】：配置IPv4的静态IP地址。

配置完成后点击提交完成网口配置。

第四步：网络配置->路由

默认情况只需要配置默认路由，让STA能与SIP正常通信。



第五步：内网服务器自动发现

建议只需要勾选“自动识别”即可。若定义了“自定义内网服务器IP组”、“自定义内网客户端IP组”则会限制自动发现的范围，当网络中新增加了网段时当不会被发现。



第六步：安全策略

建议将所有的安全策略都勾选启用。



并对“网络攻击检测”进行设置检查。

默认情况下检测的端口都为默认端口，若网络中使用的是非默认端口，如使用了http 8080提供服务，则需要将8080端口加入到HTTP中，其它协议类似。



网络中存在负载均衡并且使用XFF字段传输源IP地址，则探针上也需要开启XFF字段记录源IP地址。



第七步：违规访问

需要确认默认策略的日志记录是否勾选，勾选即可。



定义合法的访问（白名单）和非法的访问（黑名单），需要了解业务不能被哪些网段访问，并配置黑名单做监控



【名称】：定义黑名单名称。

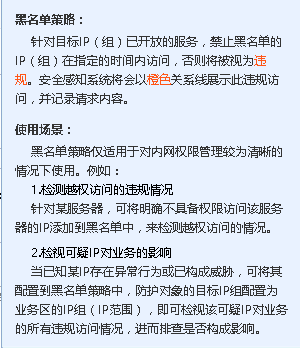
【目标IP组】：被防护的业务或用户对应的ip组。

【开放的服务】：被防护业务对应的端口号。

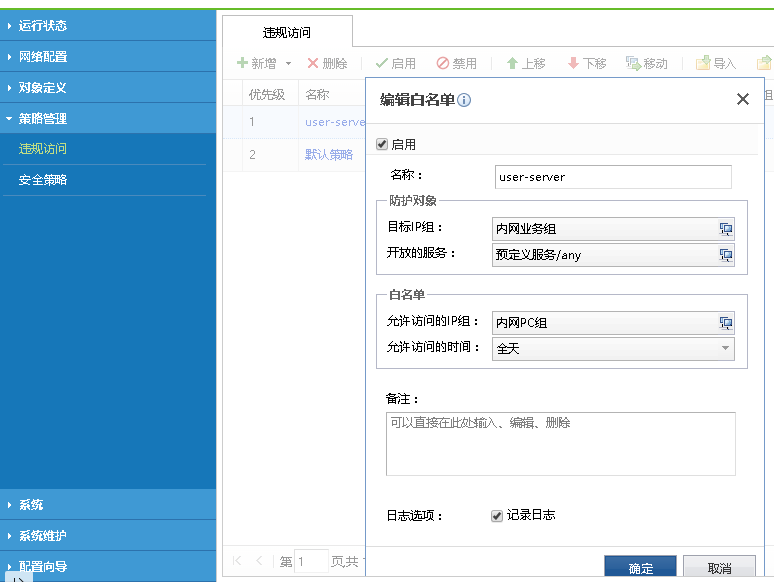
【允许访问的IP组】：主动发起访问的业务或用户对应的IP组。

【允许访问的时间】：设备禁止访问的时间断。

\* 说明



白名单监控



【名称】：定义白名单名称。

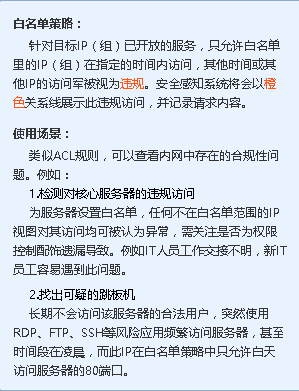
【目标IP组】：被访问的业务或用户对应的ip组。

【开放的服务】：业务对应的端口号。

【允许访问的IP组】：主动发起访问的业务或用户对应的IP组。

【允许访问的时间】：设备允许访问的时间断。

\* 说明：



确认以上信息配置无误则点击确定按钮

第八步：安全感知平台

探针与感知平台对接

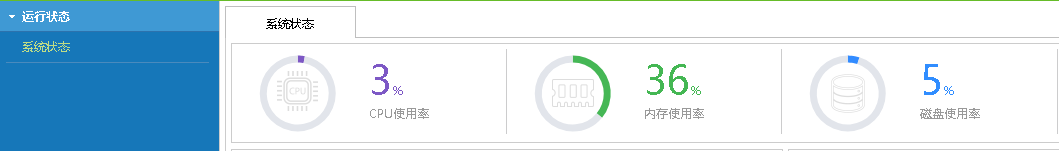


【标准模式】：适用于关注网络安全场景、占用网络资源适中

【精简模式】：适用于专网场景，探针与感知系统之间可利用的带宽较少时。

【高级模式】：适用于对内网安全较严格的场景、但占用网络资源较高。

建议在CPU不持续超过65%时使用高级模式并勾选启用所有的flow分析引擎



第九步：库升级

探针的规则库通过安全感知平台进行升级，检测是否与平台最新版本相同。若不相同可点击“立即更新”同步。



\*注：使用TCP4488连接安全感知平台进行下载，若网络在有防火墙则需要放通

### 2.1.3 STA2配置步骤

STA2给出了一些常规的配置，更多的配置详情见[STA1配置步骤](#_2.1.2 STA1配置步骤：)

第一步：网络配置->物理接口

点击eth0可配置网口IP地址，10.251.251.251不能删除只再添加需要的IP地址。

类型为路由口。所配置的IP地址需要能与SIP进行通信。



【类型】：管理口的类型必须为路由。

【连接类型】：配置IPv4的静态IP地址。

配置完成后点击提交完成网口配置。

第二步：网络配置->路由

默认情况只需要配置默认路由，让STA能与SIP正常通信。



第三步：内网服务器自动发现

建议只需要勾选“自动识别”即可。若定义了“自定义内网服务器IP组”、“自定义内网客户端IP组”则会限制自动发现的范围，当网络中新增加了网段时当不会被发现。



第四步：安全感知平台

探针与感知平台对接

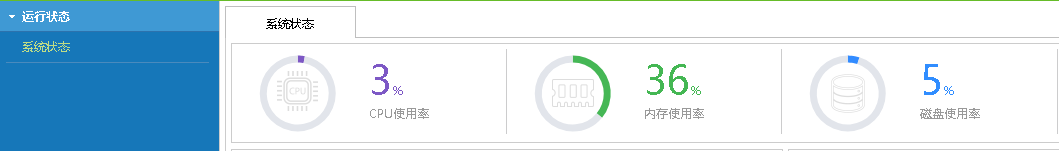


【标准模式】：适用于关注网络安全场景、占用网络资源适中

【精简模式】：适用于专网场景，探针与感知系统之间可利用的带宽较少时。

【高级模式】：适用于对内网安全较严格的场景、但占用网络资源较高。

建议在CPU不持续超过65%时使用高级模式并勾选启用所有的flow分析引擎



第五步：库升级

探针的规则库通过安全感知平台进行升级，检测是否与平台最新版本相同。若不相同可点击“立即更新”同步。



\*注：使用TCP4488连接安全感知平台进行下载，若网络在有防火墙则需要放通

### 2.1.3 STA3配置步骤

STA3给出了一些常规的配置，更多的配置详情见[STA1配置步骤](#_2.1.2 STA1配置步骤：)

第一步：网络配置->物理接口

点击eth0可配置网口IP地址，10.251.251.251不能删除只再添加需要的IP地址。

类型为路由口。所配置的IP地址需要能与SIP进行通信。



【类型】：管理口的类型必须为路由。

【连接类型】：配置IPv4的静态IP地址。

配置完成后点击提交完成网口配置。

第二步：网络配置->路由

默认情况只需要配置默认路由，让STA能与SIP正常通信。



第三步：内网服务器自动发现

建议只需要勾选“自动识别”即可。若定义了“自定义内网服务器IP组”、“自定义内网客户端IP组”则会限制自动发现的范围，当网络中新增加了网段时当不会被发现。



第四步：安全感知平台

探针与感知平台对接

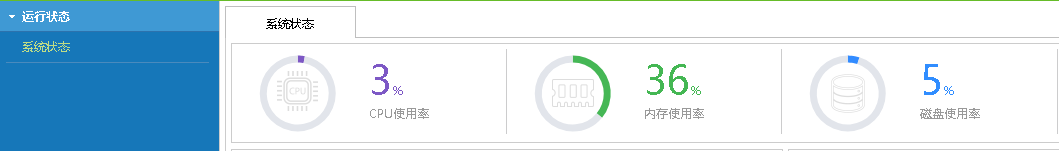


【标准模式】：适用于关注网络安全场景、占用网络资源适中

【精简模式】：适用于专网场景，探针与感知系统之间可利用的带宽较少时。

【高级模式】：适用于对内网安全较严格的场景、但占用网络资源较高。

建议在CPU不持续超过65%时使用高级模式并勾选启用所有的flow分析引擎



第五步：库升级

探针的规则库通过安全感知平台进行升级，检测是否与平台最新版本相同。若不相同可点击“立即更新”同步。



\*注：使用TCP4488连接安全感知平台进行下载，若网络在有防火墙则需要放通

## 2.2 SIS和STA 在多分支环境部署案例

**客户环境与需求：**某用户网络是三层环境，需求检测总部与多个分支的风险情况。

感知平台部署：

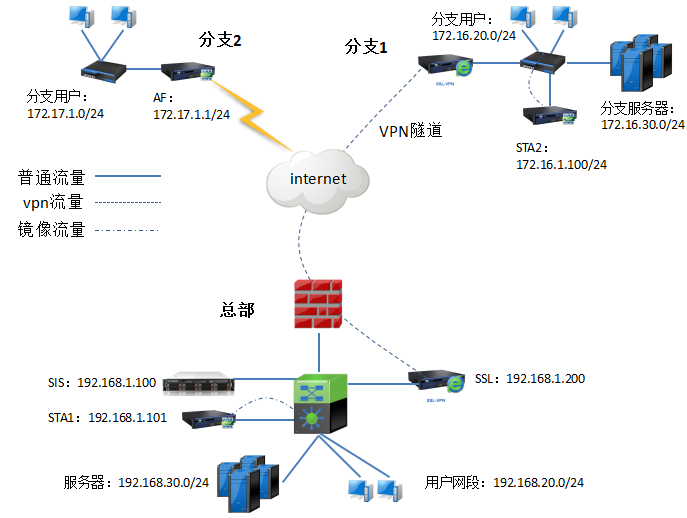
\* 感知平台ip需要与探针管理口ip通信，接收探针发来的数据。SIS eth0口配置ip为192.168.1.100；STA\_1 eth0口配置ip192.168.1.101；STA\_2 eth0口配置ip172.16.1.100；

探针部署：

\* 收集总部用户区域-->互联网区域；总部业务区域 -->互联网区域；总部用户、业务-->总部用户、业务之间的数据；总部用户、业务区域-->分支用户、分支业务区域之间的数据。需要在总部核心交换机将流量镜像给STA1。

\* 收集分支1用户区域-->互联网区域；总部业务区域 -->互联网区域；总部用户、业务-->总部用户、业务之间的数据；总部用户、业务区域-->分支用户、分支业务区域之间的数据，需要在分支核心交换机将流量镜像给STA2。

\* 收集2用户区域-->互联网区域的安全情况。

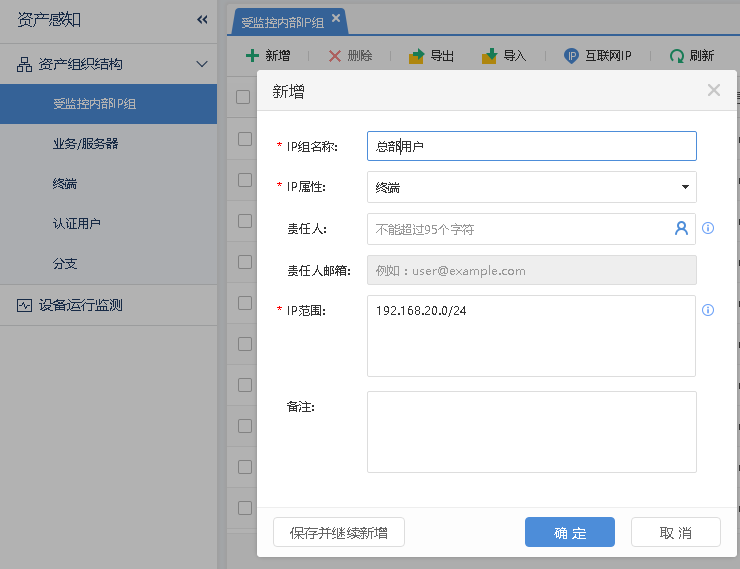


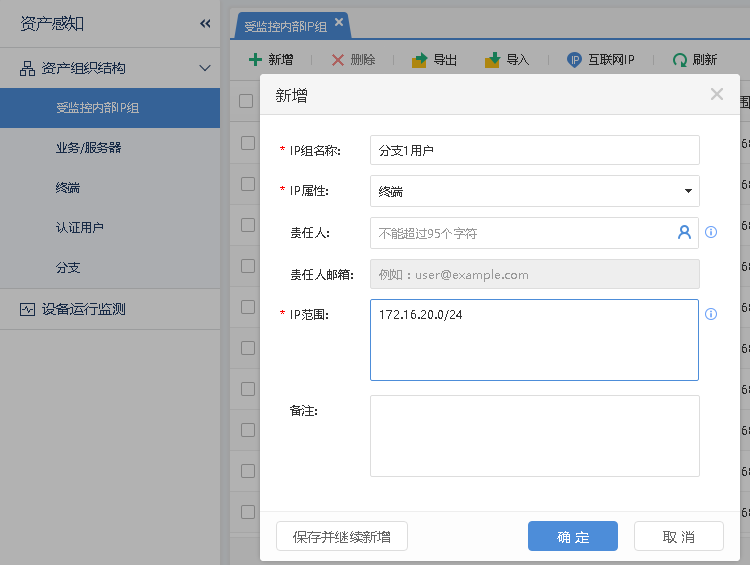
### 2.2.1 SIS配置步骤

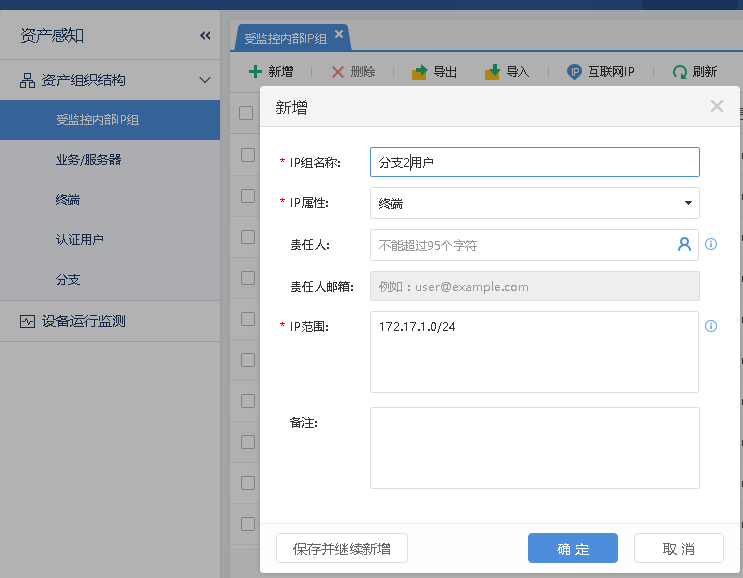
**常规配置参考2.1章节**

第一步：配置内网IP范围

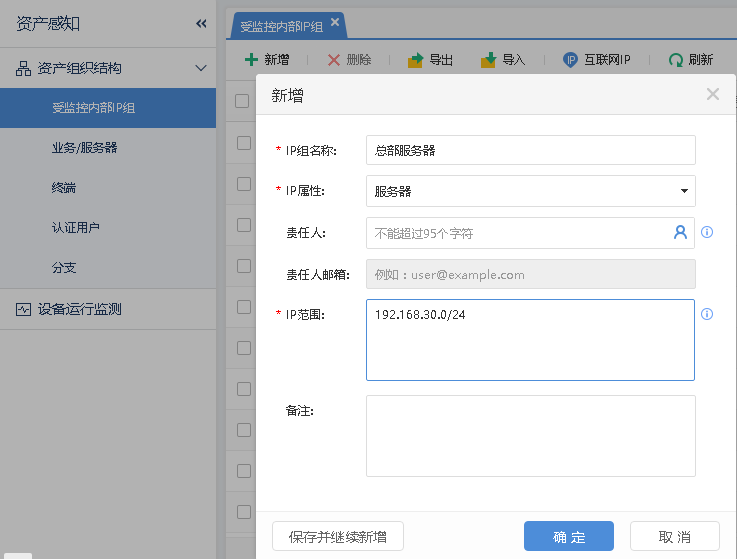
配置总部、分支1、分支2的终端用户

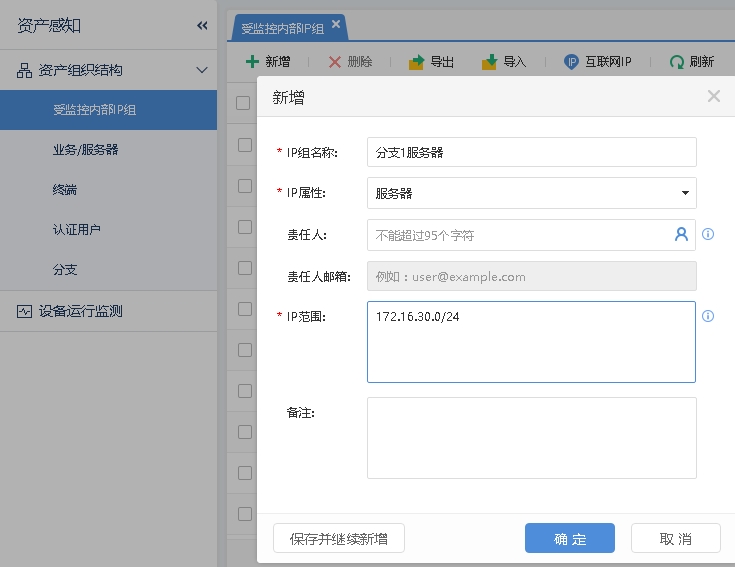




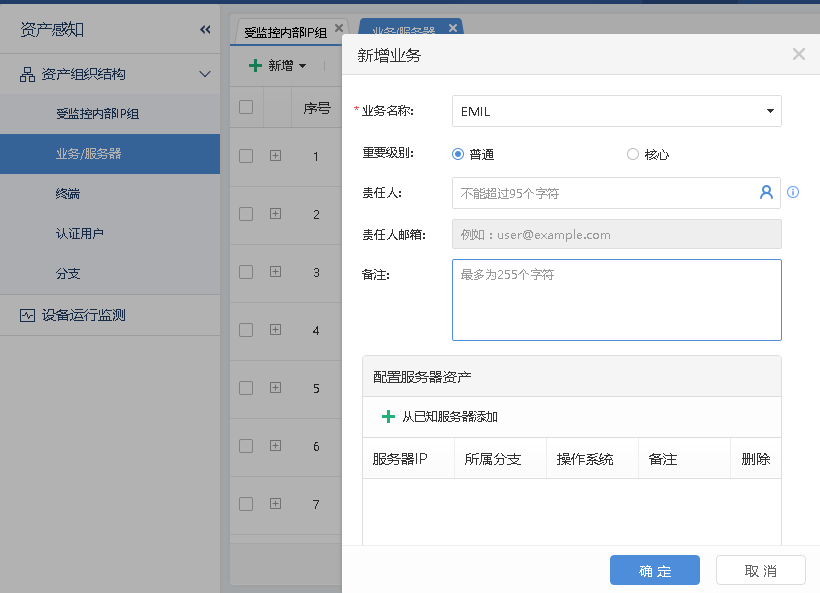


配置总部、分支1、分支2的业务服务器





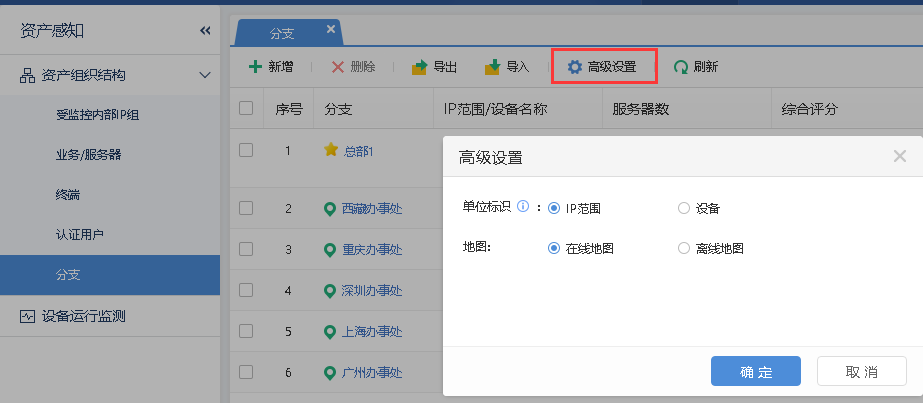
第二步：业务配置



【新增】：选择新增业务。

定义业务名称并选择从已知服务器添加

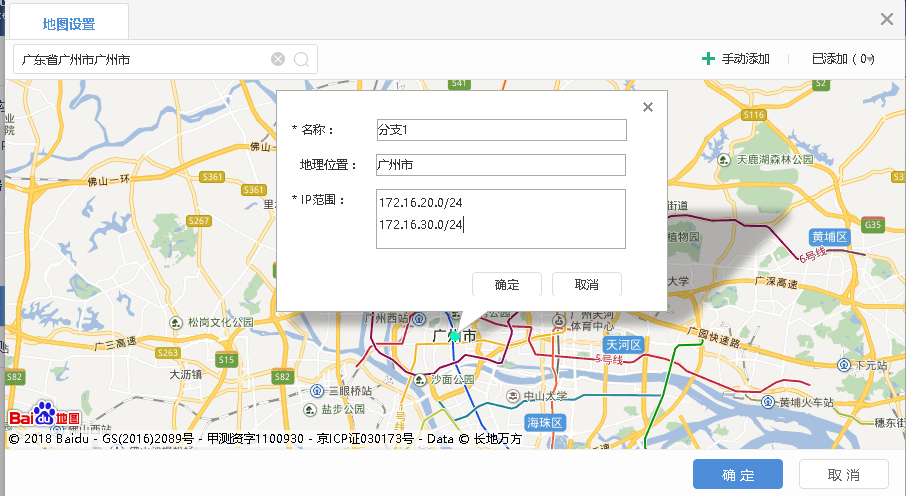
第三步：分支配置，选择单位标识。



【ip范围】：适用于所有分支单位的流量共用统一出口，各单位以IP范围为标识；

【设备】：适用于各分支单位流量非统一出口且分支之间有IP地址冲突的情况，以设备ID区分各单位；

第五步：新增分支——选择IP范围

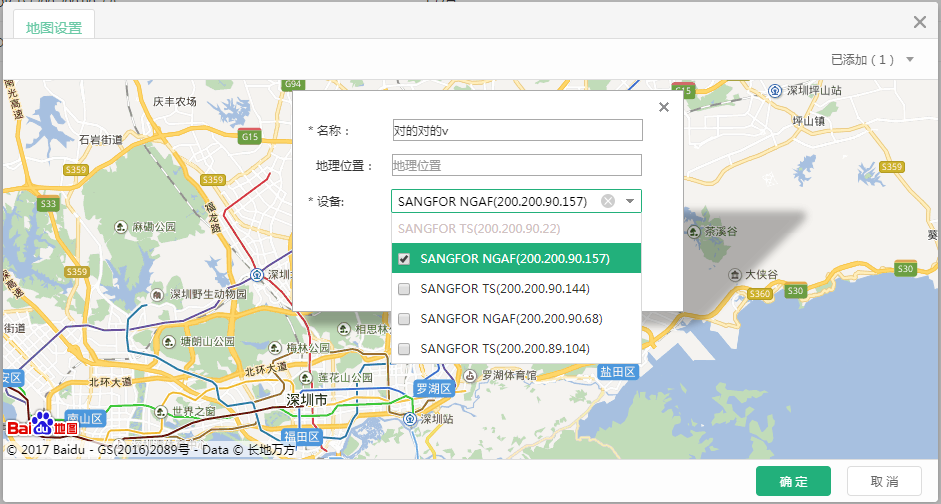


【手动添加】：将光标移动到分支的相应位置。

【名称】：分支名称。

【IP范围】：分支的内网ip地址范围。

第六步：新增分支--选择设备



【手动添加】：将光标移动到分支的相应位置。

【名称】：分支名称。

【设备】：选择接入到感知平台的设备。

### 2.2.2 STA配置步骤

2.2.2.1 总部STA1配置

**常规配置参考2.1章节**

第一步：内网定义

在分支的环境，建议分支的探针能配置明细的IP地址段。

如总部的终端网段为192.168.20.0/24，则勾选“自定义内网客户端IP组”并配置IP组为192.168.20.0/24。

服务器网段为192.168.30.0/24，则勾选“自定义内网服务器IP组”并配置IP组为192.168.30.0/24



【自定义内网服务器IP组】：定义内网服务器区的ip地址段。

【自定义内网客户端IP组】：定义内网用户上网区的ip地址段。

第二步：连接感知系统

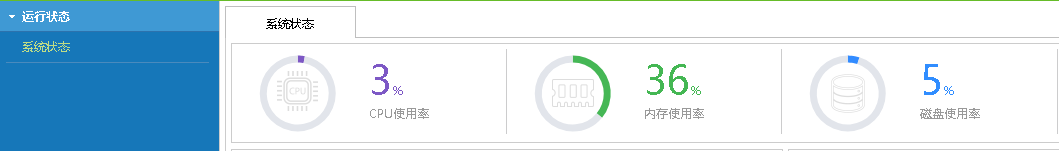


【标准模式】：适用于关注网络安全场景、占用网络资源适中

【精简模式】：适用于专网场景，探针与感知系统之间可利用的带宽较少时。

【高级模式】：适用于对内网安全较严格的场景、但占用网络资源较高。

建议在CPU不持续超过65%时使用高级模式并勾选启用所有的flow分析引擎



2.2.2.2 分支STA2配置

**常规配置参考2.1章节**

第一步：内网定义

在分支的环境，建议分支的探针能配置明细的IP地址段。

如总部的终端网段为172.16.20.0/24，则勾选“自定义内网客户端IP组”并配置IP组为172.16.20.0/24。

服务器网段为172.16.30.0/24，则勾选“自定义内网服务器IP组”并配置IP组为172.16.30.0/24



【自定义内网服务器IP组】：定义内网服务器区的ip地址段。

【自定义内网客户端IP组】：定义内网用户上网区的ip地址段。

第二步：连接感知系统

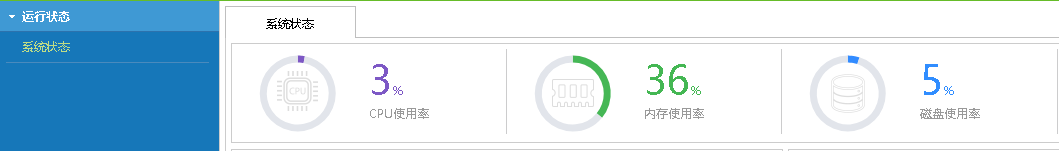


【标准模式】：适用于关注网络安全场景、占用网络资源适中

【精简模式】：适用于专网场景，探针与感知系统之间可利用的带宽较少时。

【高级模式】：适用于对内网安全较严格的场景、但占用网络资源较高。

建议在CPU不持续超过65%时使用高级模式并勾选启用所有的flow分析引擎

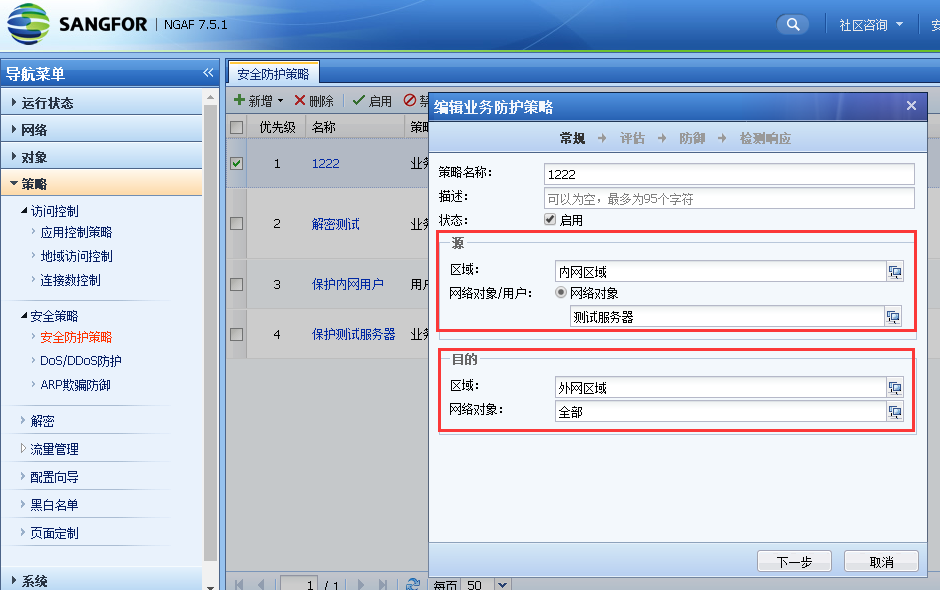


2.2.2.3 分支AF配置

第一步：防火墙路由模式上架（见防火墙快速上架手册）

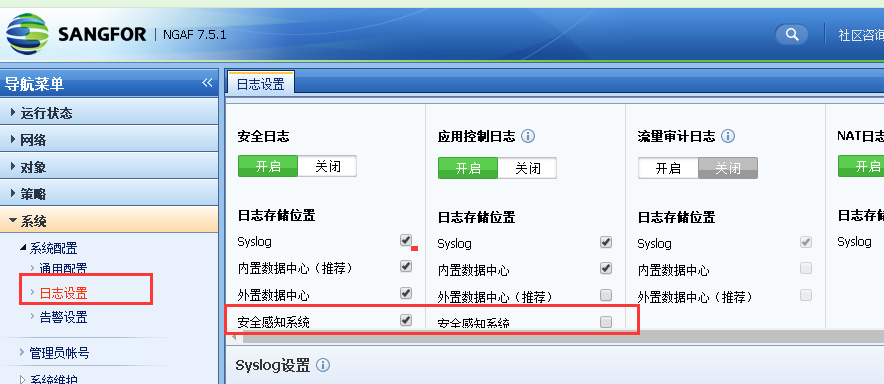
第二步：防火墙“反向”策略配置。

**因为失陷主机会向外发起攻击或C&C通信等行为，正常有防火墙配置主要是针对互联网对内网发起的攻击做检测或拦截，所以当与安全感知对接时需要配置“反向”的安全策略来检测失陷主机的恶意行为。**



第二步：配置与感知平台

\*NGAF7.4版本以上可以上传安全日志和应用控制日志。





1、STA、AF与SIS的数据传输端口为4430。

2、配置分支时切换“IP范围”、“设备”时，之前的分支配置会被清除。

## 2.3 SIS和STA 在DNS环境部署案例

**客户环境与需求：**某用户网络是三层环境，并且有内网DNS代理服务器，需求检测内网业务及用户的风险情况。DNS服务器接在核心交换机上。

感知平台部署：

\* 感知平台ip需要与探针管理口ip通信，接收探针发来的数据。SIS eth0口配置ip为192.168.1.100；STA\_1 eth0口配置ip 192.168.1.101；

探针部署：

\* 收集用户之间（用户都接在核心交换机上），服务器之间（服务器都接在核心交换机上），用户与服务器之间的镜像数据。

注意：探针收集下图中核心交换机g0/0/1、g0/0/2、g0/0/3的镜像数据。并将DNS服务器IP地址加入到SIS的全局白名单中。

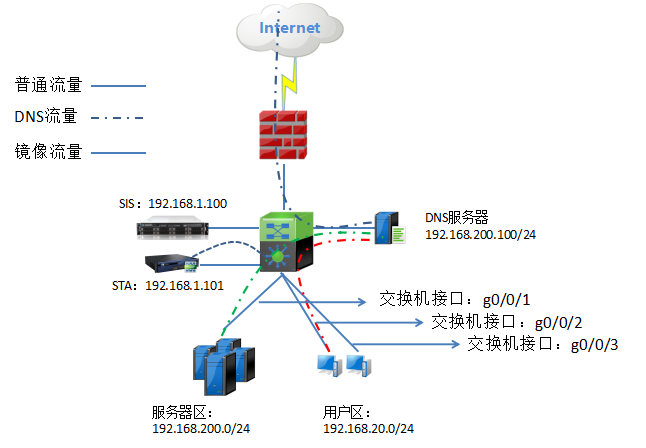
**思路：**镜像内网DNS代理之前的数据，及PC或业务到内网DNS这段的数据。抓内网DNS服务器地址和53端口的数据包，

若内网DNS服务器IP即为源，又为目的，则将DNS服务器加入全局 白名单。

若内网DNS服务器IP只为源，则表明镜像的数据只有代理后的，需要重新镜像。

若内网DNS服务器IP只为目的，则表明镜像正确。

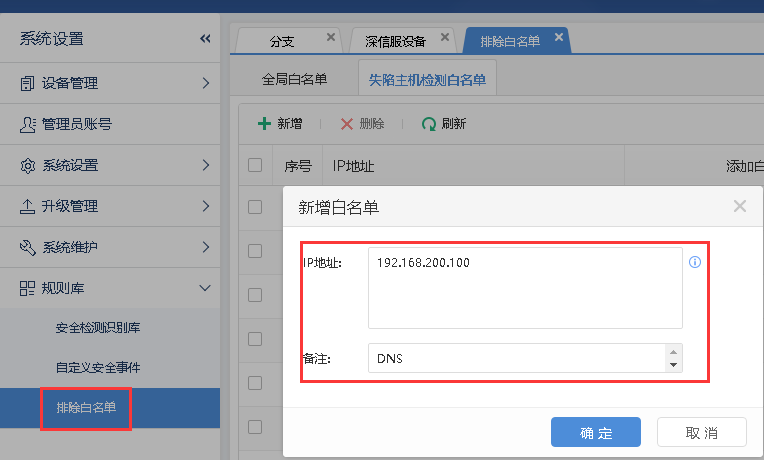
当DNS服务器加入到白名单中。（对于已自的扫描器等IP地址也加入此处）。



### 2.3.1 SIS配置步骤

**常规配置参考2.1章节**

第一步：将DNS服务器加入到系统白名单中。



【失陷主机检测白名单】：不对白名单中的IP进行风险分析。

### 2.3.2 STA配置

**常规配置参考2.1章节**

1、在DNS环境中探针需要收集PC、服务器请求DNS前的镜像数据，并将DNS的IP地址加入到SIS的全局白名单中。

# ：密码安全风险提示

为了防止其他无关人员或恶意攻击者通过默认账号密码登录和更改设备配置，请修改NGAF设备登录的默认密码。

## 3.1修改后台密码

**SIS修改控制台管理员密码：**

[系统设置]->[管理员账号] 修改对应帐号的密码。

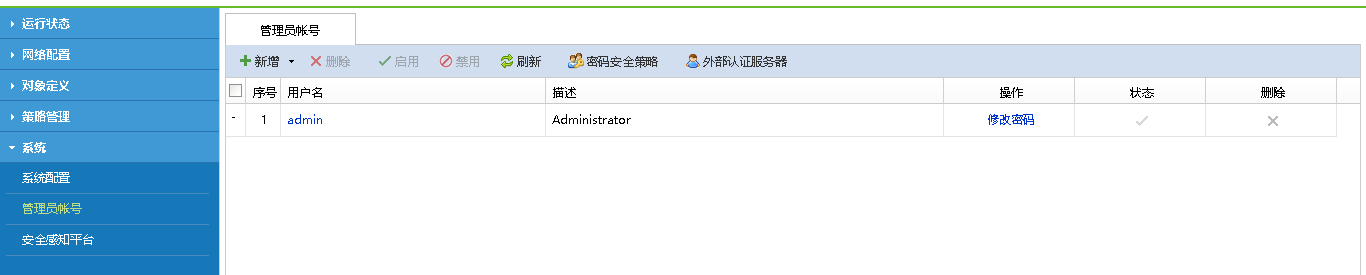


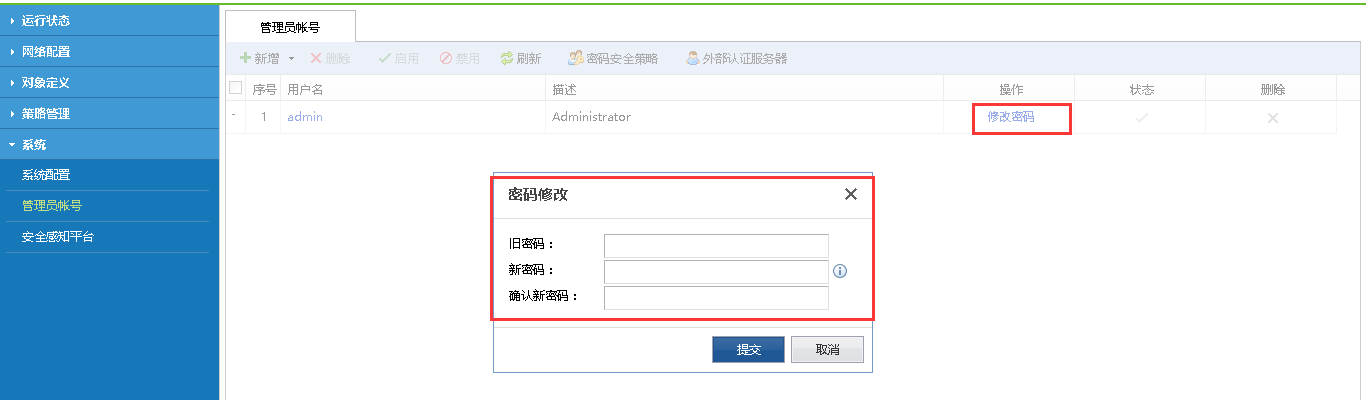


输入旧密码和新密码，点击确定，保存和生效配置。

**STA修改控制台管理员密码**

[系统]->[管理员帐号] 修改对应帐号的密码。





输入旧密码和新密码，点击提交，保存和生效配置。

**1. 如果有多个网络管理员需要登录设备，请给每位管理员设置登录账号，超级管理员admin的密码请勿广泛流传。**

**2.修改了控制台admin的密码后，SANGFOR设备升级系统的登录密码也会做相应的修改。**

# 附件一：主流交换机厂商镜像口流量配置

## 华为：

# 配置GigabitEthernet0/0/1为镜像接口，GigabitEthernet0/0/2为观察接口，观察接口索引号为1。镜像GigabitEthernet0/0/1上的双向业务流量到GigabitEthernet0/0/2上。  
<Quidway> system-view  
[Quidway] observe-port 1 interface gigabitethernet 0/0/2  
[Quidway] interface gigabitethernet 0/0/1  
[Quidway-GigabitEthernet0/0/1] port-mirroring to observe-port 1 both

步骤1 执行命令system-view，进入系统视图。  
步骤2 执行命令observe-port index interface interface-type interface-number ，配置观察接口。  
步骤3 执行命令interface interface-type interface-number，进入镜像接口的接口视图。  
步骤4 执行命令port-mirroring to observe-port index { both | inbound | outbound } ，配置接口  
镜像。

## 华三：

# 配置GigabitEthernet0/0/1为镜像接口，GigabitEthernet0/0/2为观察接口，观察接口索引号为1。镜像GigabitEthernet0/0/1上的双向业务流量到GigabitEthernet0/0/2上。

<sysname>system-view

[sysname] mirroring-group 1 local

[sysname] mirroring-group 1 mirroring-port G0/0/1 both

[sysname] mirroring-group 1 monitor-port G0/0/2

步骤1 执行命令system-view，进入系统视图。

步骤2 执行命令mirroring-group number local ，建立一个镜像组。

步骤3 执行命令mirroring-group 1 mirroring-port G0/0/1 { both | inbound | outbound }，将端口加入到镜像组中，镜像可以根据实际情况灵活选择入方向、出方向及全部流量；both，全部流量；inbound，入方向流量；outbound，出方向流量

步骤4 执行命令mirroring-group 1 monitor-port G0/0/2 ，设置镜像的目的端口

## 锐捷：

# 配置fa0/1为镜像接口，fa0/2为观察接口，观察接口索引号为1。镜像fa0/1上的双向业务流量到fa0/2上。  
Switch# configure terminal  
Switch(config)#[monitor](http://www.vants.org/?tag=monitor) session 1 source interface fa0/1 both

Switch(config)#[monitor](http://www.vants.org/?tag=monitor) session 1 destination interface fa 0/2

步骤1 执行命令configure terminal，进入全局配置模式。

步骤2 执行命令[monitor](http://www.vants.org/?tag=monitor) session 1 source interface fa0/1 { both | inbound | outbound } ，建立观察接口索引号为1，并将fa0/1加入该索引，镜像可以根据实际情况灵活选择入方向、出方向及全部流量；both，全部流量；inbound，入方向流量；outbound，出方向流量

步骤3 执行命令[monitor](http://www.vants.org/?tag=monitor) session 1 destination interface fa 0/2 设置fa0/2为监控口

## 思科：

# 配置fa0/1为镜像接口，fa0/2为观察接口，观察接口索引号为1。镜像fa0/1上的双向业务流量到fa0/2上。

Switch# configure terminal

Switch(config)# monitor session 1 source interface fastethernet 0/1 both

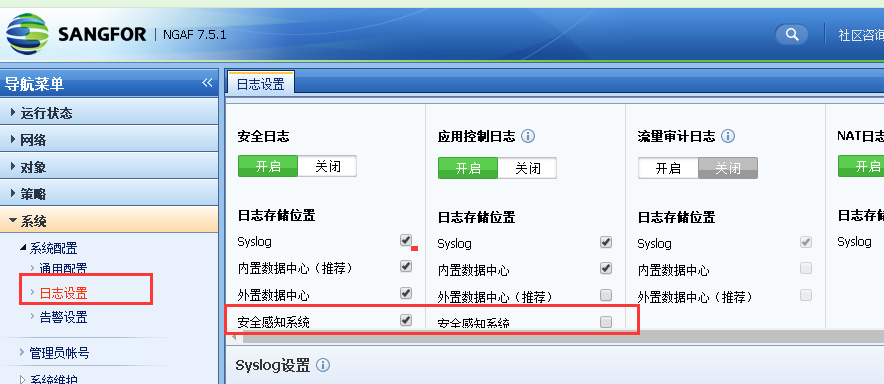
Switch(config)# monitor session 1 destination interface fastethernet 0/2

步骤1 执行命令configure terminal，进入全局配置模式。

步骤2 执行命令[monitor](http://www.vants.org/?tag=monitor) session 1 source interface fa0/1 { both | inbound | outbound } ，建立观察接口索引号为1，并将fa0/1加入该索引，镜像可以根据实际情况灵活选择入方向、出方向及全部流量；both，全部流量；inbound，入方向流量；outbound，出方向流量

步骤3 执行命令[monitor](http://www.vants.org/?tag=monitor) session 1 destination interface fa 0/2 设置fa0/2为监控口

# 附件二：NGAF 7.5版本对接安全感知平台配置





# 附件三：产品接口列表

**STA接口列表**

|  |  |
| --- | --- |
| 型号名称 | 网口情况 |
| STA-100-B420 | 4电2光 |
| STA-100-B440 | 4电4光 |
| STA-100-C640 | 6电4光 |
| STA-100-D642 | 6电4光2万兆 |
| STA-100-E642 | 6电4光2万兆 |
| STA-100-F842 | 8电4光2万兆 |
| STA-100-G884 | 4电8光4万兆 |

SIS接口列表

|  |  |
| --- | --- |
| 型号名称 | 网口情况 |
| SIP-1000-A600 | 6电 |
| SIP-1000-B400 | 4电 |
| SIP-1000-C402 | 4电2光 |
| SIP-1000-D602 | 6电2万兆 |