

# SANGFOR 安全感知平台

## 快速安装手册



深信服智安全  
SANGFOR SECURITY

# 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
声明.....	3
前言.....	4
第一章 SIS、STA 系列硬件设备的安装.....	5
1.1 环境要求.....	5
1.2.电源.....	5
1.3.产品接口说明.....	6
1.4.配置与管理.....	7
第二章：SIS、STA 系列硬件设备的部署.....	11
2.1 SIS 和 STA 常规环境部署案例.....	11
2.1.1 SIS 配置步骤：.....	12
2.1.2 STA1 配置步骤：.....	22
2.1.3 STA2 配置步骤：.....	32
2.1.3 STA3 配置步骤：.....	36
2.2 SIS 和 STA 在多分支环境部署案例.....	41
2.2.1 SIS 配置步骤：.....	42
2.2.2 STA 配置步骤：.....	47
2.3 SIS 和 STA 在 DNS 环境部署案例.....	54
2.3.1 SIS 配置步骤：.....	55
2.3.2 STA 配置.....	55
第三章：密码安全风险提示.....	56
3.1 修改后台密码.....	56
附件一：主流交换机厂商镜像口流量配置.....	58
华为：.....	58
华三：.....	58
锐捷：.....	59
思科：.....	59
附件二：NGAF 7.3 版本对接安全感知平台配置.....	60
附件三：产品接口列表.....	60

## 声明

Copyright © 2016 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 SIS 2000 STA 200 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

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

SIS 与 STA 可在如下的环境下使用：

SIS	SIS1000(1U)	SIS2000(2U)
最大功率：	400W	550W
温度：	0~35℃	0~35℃
湿度：	20~80%	20~80%
尺寸（长*宽*高）	660mm*425mm*43mm	735mm*447mm*88mm

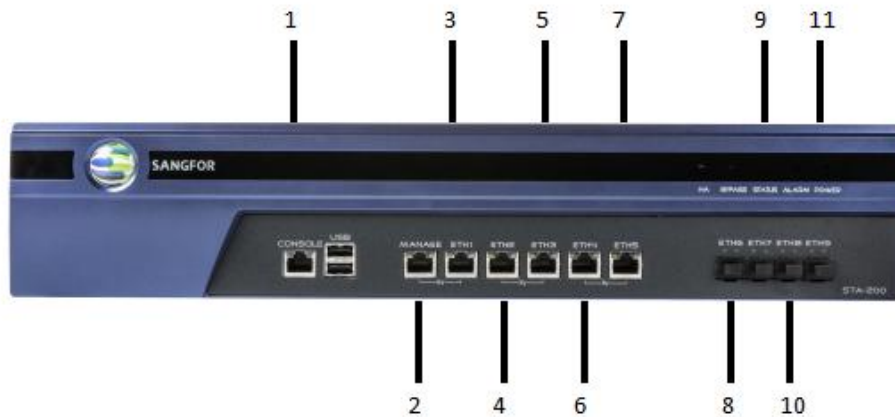
STA	STA100(1U)	STA200 (2U)	STA300 (2U)	STA400 (2U)
最大功率：	250W	300W	300W	760W
温度：	0~45℃	0~40℃	0~40℃	0~45℃
湿度：	5~90%	5~95%	5~95%	5~90%
尺寸（长*宽*高）	390mm*430mm *45.5mm	500mm*440mm *89mm	600mm*440mm *90mm	600mm*440mm *90mm

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 200 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	千兆电口
7	ETH5	千兆电口
8	ETH6	千兆光口
9	EHT7	千兆光口
10	EHT8	千兆光口
11	EHT9	千兆光口



SANGFOR SIS 前面板图（以 SIS 1000 为例）

设备名称	网口编号	网口类型
SIS2000	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。

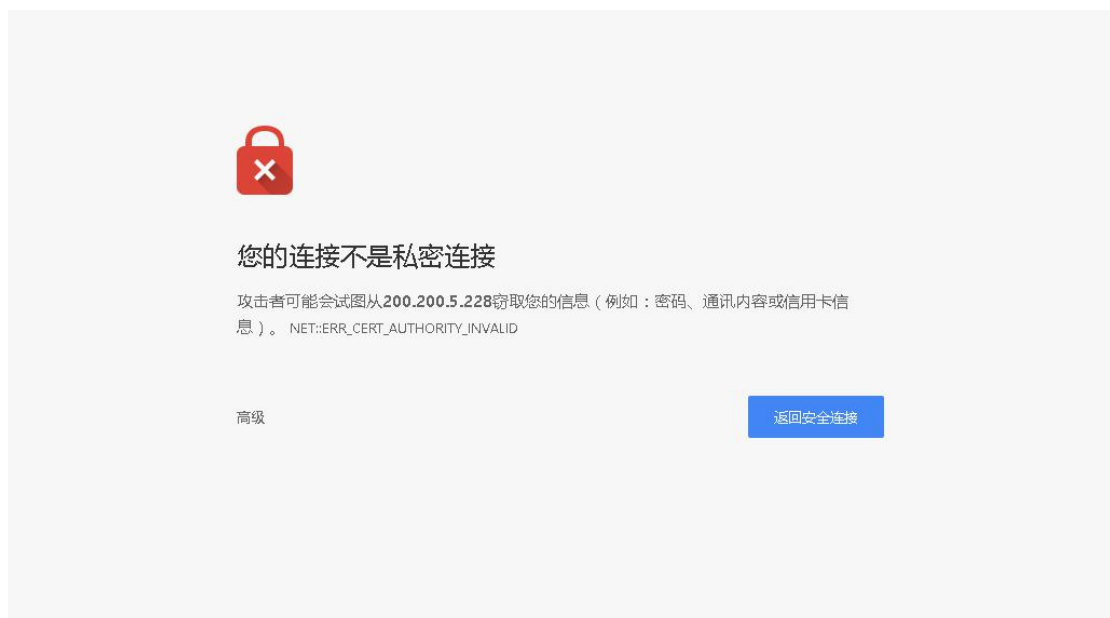


\*注：建议使用 chrome 浏览器登录 SIS 平台。

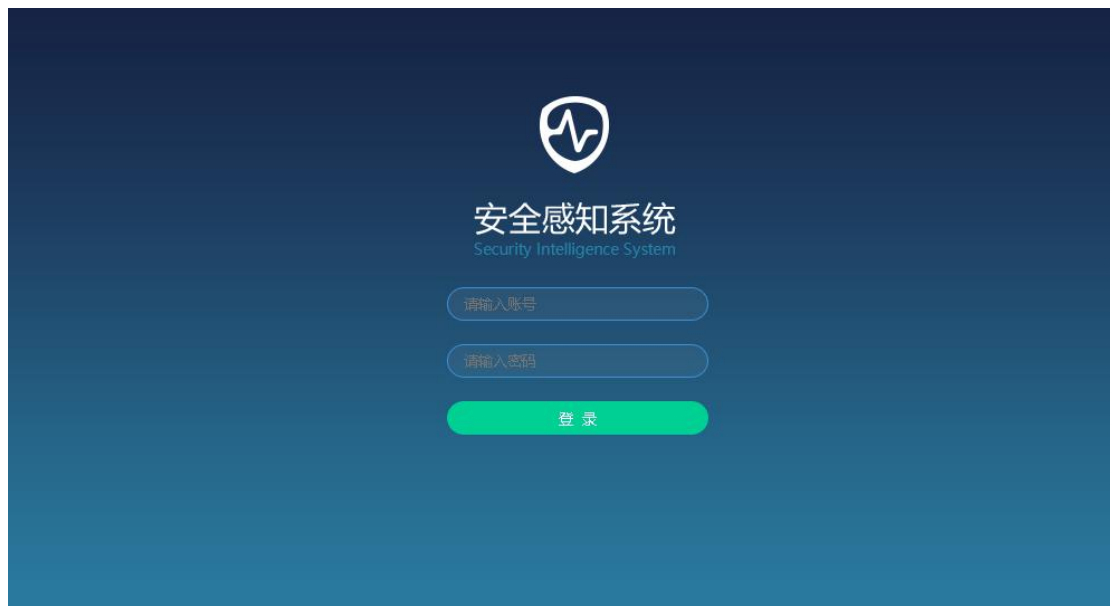
### 如何登录 SIS 设备控制台页面？

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：



### 您的连接不是私密连接

攻击者可能会试图从**200.200.5.221**窃取您的信息（例如：密码、通讯内容或信用卡信息）。NET::ERR\_CERT\_AUTHORITY\_INVALID

高级

返回安全连接

点击高级->继续前往 10.251.251.252（不安全）



### 您的连接不是私密连接

攻击者可能会试图从**200.200.5.228**窃取您的信息（例如：密码、通讯内容或信用卡信息）。NET::ERR\_CERT\_AUTHORITY\_INVALID

隐藏详情

返回安全连接

此服务器无法证明它是**200.200.5.228**；您计算机的操作系统不信任其安全证书。出现此问题的原因可能是配置有误或您的连接被拦截了。

继续前往200.200.5.228（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：

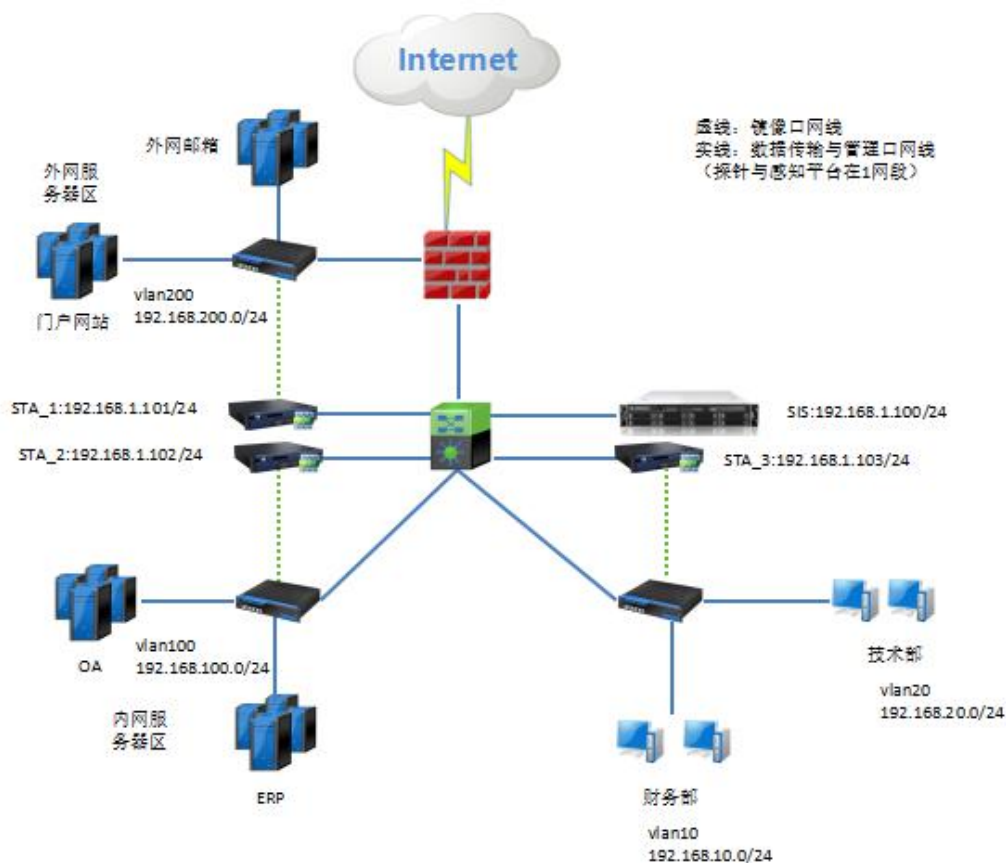
- \* 感知平台 ip 需要与探针管理口 ip 通信，接收探针发来的数据。SIS eth0 口配置 ip 为 192.168.1.100；STA\_1 eth0 口配置 ip192.168.1.101；STA\_2 eth0 口配置 ip192.168.1.102；STA\_3 eth0 口配置 ip192.168.1.103；

探针部署：

- \* 收集用户与用户之间的流量，需要在用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：

**常规**

如果网络支持此功能，则可以获取自动指派的 IP 设置。否则，您需要从网络系统管理员处获得适当的 IP 设置。

☐ 自动获得 IP 地址 (O)

☒ 使用下面的 IP 地址 (S):

IP 地址 (I):

子网掩码 (U):

默认网关 (D):

☐ 自动获得 DNS 服务器地址 (B)


☒ 使用下面的 DNS 服务器地址 (E):

首选 DNS 服务器 (P):

备用 DNS 服务器 (A):

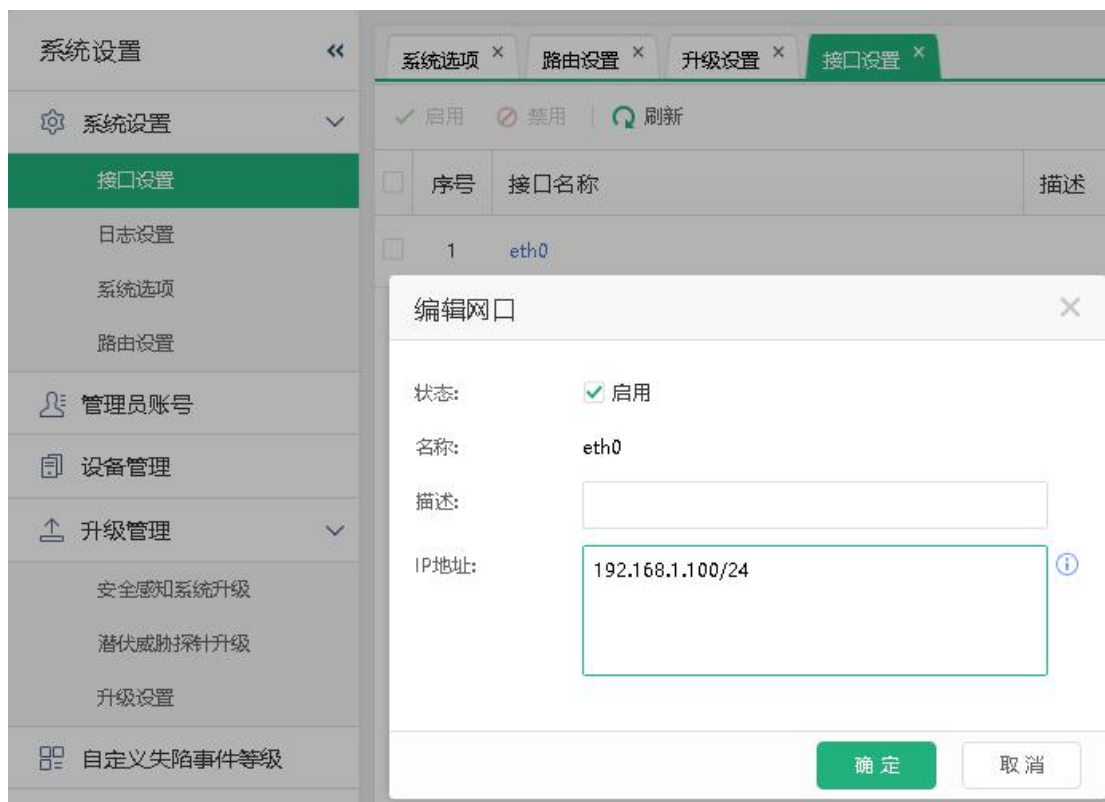
☐ 退出时验证设置 (L)

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：



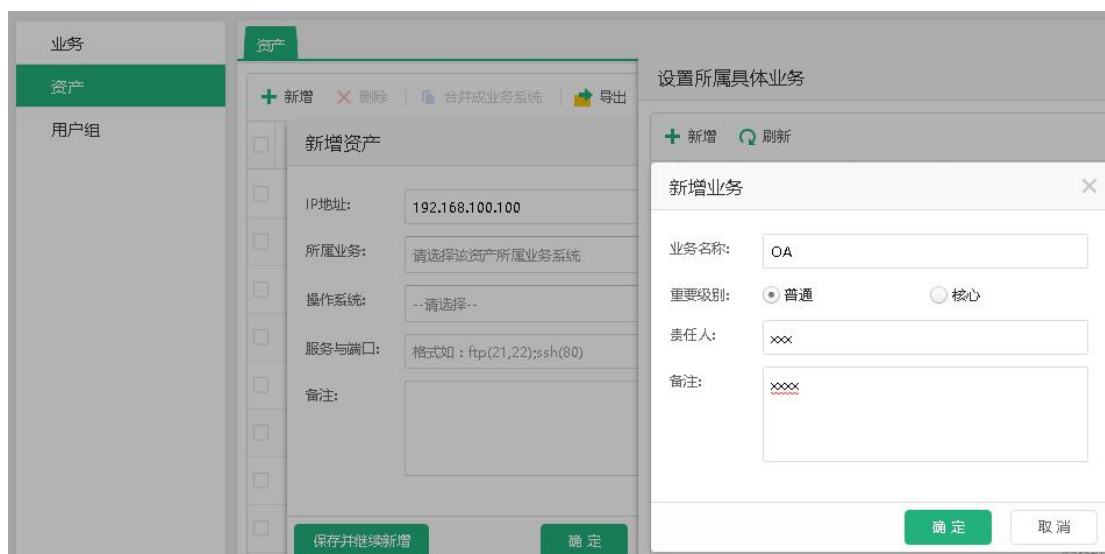
**安全感知系统**  
Security Intelligence System

第三步：配置网口 ip 用于管理及接收探针数据。（非 eth0 口需要先接上网线启用网口再配置 ip 地址）



【是否为管理口】：选择“是”才能通过该网口 ip 登录设备运行管理。

第四步：配置资产，资产管理->资产->新增



【ip 地址】：对应服务器的 ip 地址。

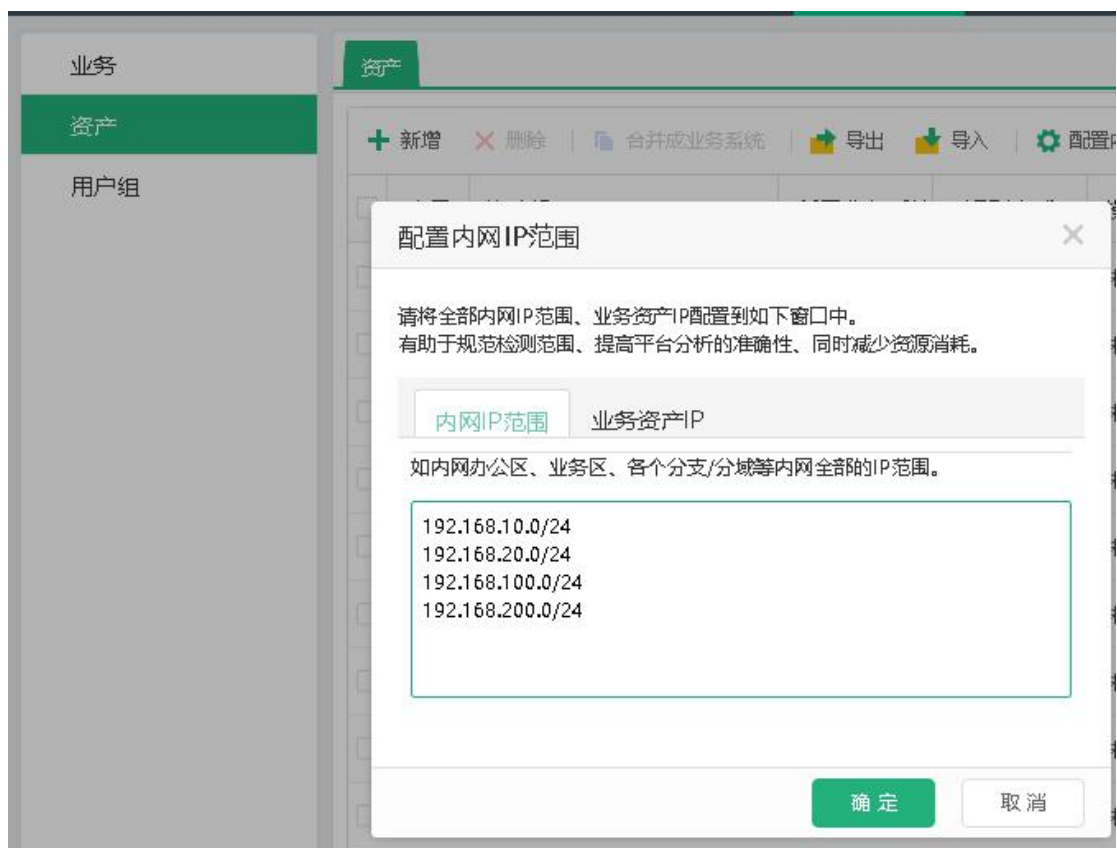
【所性业务】：对应服务器提供的业务，如 OA，EMAIL 等。业务可定义为普通与核心

【操作系统】：选择对应业务所运行的操作系统，如 linux,windows 等

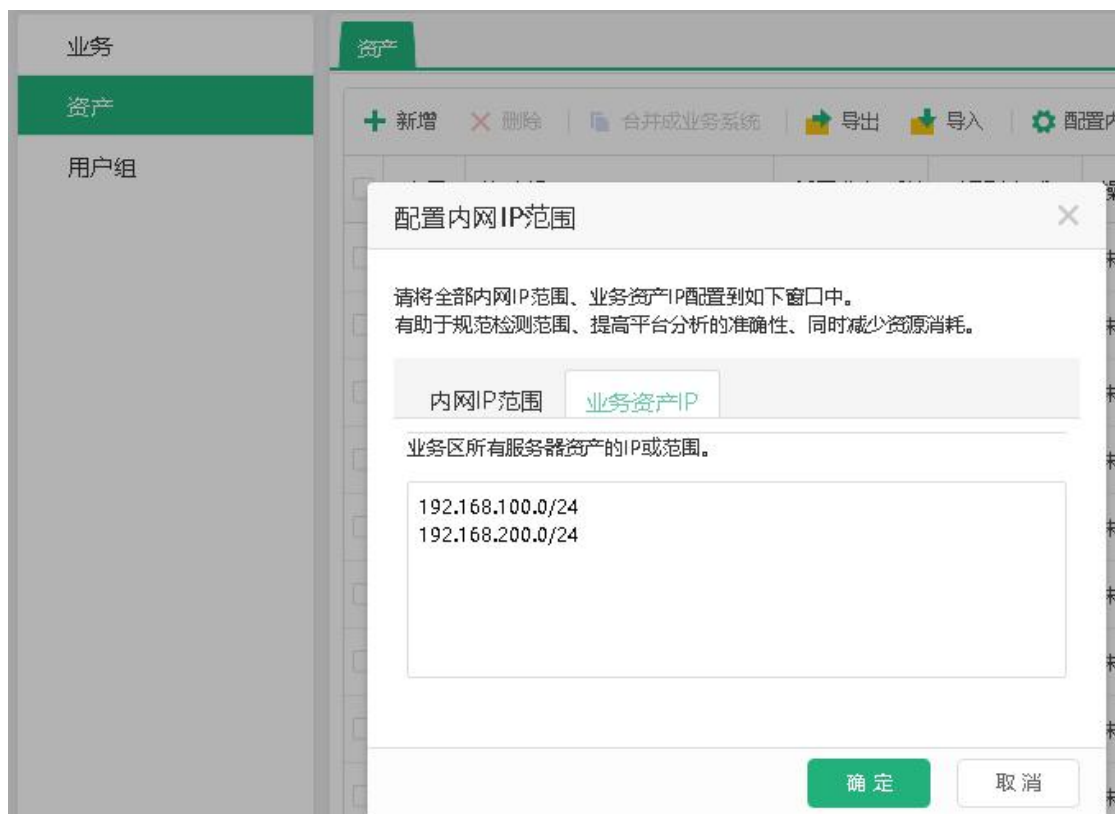
【服务与端口】：业务所使用的端口，如 web 业务使用 80 端口，数据库业务使用 3306 端口。

【备注】对该资产进行备注说明。

#### 第五步：配置内网 IP 范围



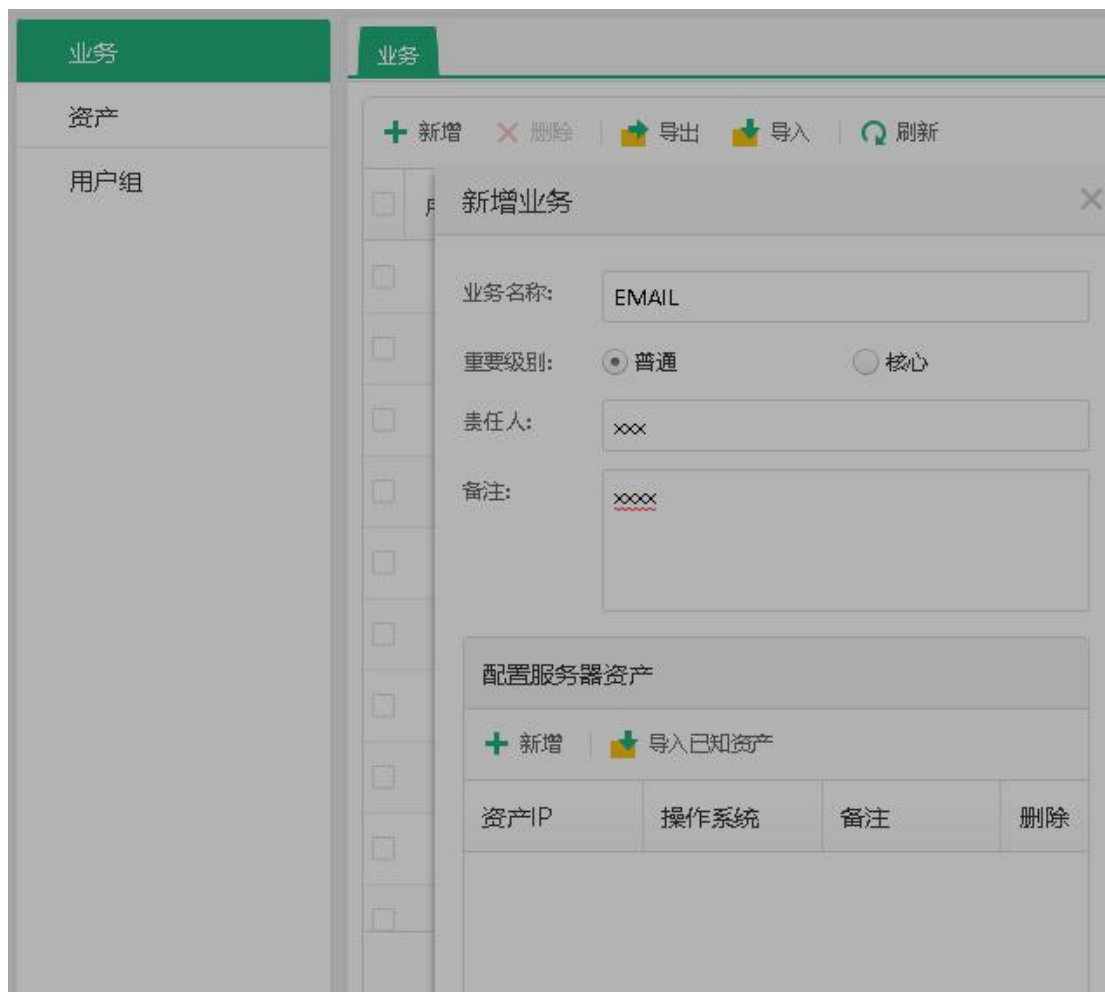




【内网 IP 范围】：内网所有网段，包括用户网段和业务网段

【业务资产 IP】：业务网段。

第六步：业务配置



【新增】：新增业务。

【配置服务器资产】：可以新增或选择第四步中新增的资产。

【导出】：可以将业务导出为.csv 文件。

【导入】：可以将业务导入系统中。

第七步：配置用户组

【名称】：用户组部门名称。

【IP 范围】：用户所在的网段。

#### 第八步：特征库升级设置

系统设置

系统设置

接口设置

日志设置

系统选项

路由设置

管理员账号

设备管理

升级管理

安全感知系统升级

潜伏威胁探针升级

升级设置

自定义失陷事件等级

白名单

全局IP白名单

系统选项 × 路由设置 × 升级设置 ×

升级服务器设置

选择服务器:

自动选择

测试服务器

0.0.0.0

代理设置

☒ 启用代理服务器

IP地址:

端口:

☐ 验证用户

确定

【路由设置】：需要配置默认路由，确保设备可以上网。

【代理设置】：当客户网络需要通过代理服务器上网时配置。

第九步：邮件告警功能

告警

告警策略

告警设置

告警日志

告警策略

告警设置

告警日志

邮件发送设置

启用邮件告警

\* SMTP服务器名称或IP地址:

smtp.qq.com

\* SMTP服务器端口:

25

\* SMTP用户名:

xxx@qq.com

\* SMTP密码:

.....

统一收件人:

xxx@163.com;xxx@sina.com

发送测试邮件

告警控制

告警控制设置

在 60 分钟内最多 50 份通知，超出的下个时间间隔发送。

确定

【邮件发送设置】：配置 SMTP 服务器地址，添加用于发送邮件的用户名/密码，最后配置收件人的邮箱地址，最多 10 个。

#### 第十步：配置告警策略

告警

告警策略

告警设置

告警日志

告警策略

告警设置

告警日志

① 邮件告警未启用，无法发送告警信息，点击进入告警设置

启用 禁用 查看告警日志

序号	告警名称	类型	邮件收件人
1	遭受攻击成功事件	安全	未设置，点击设置
2	发现风险用户	事件	未设置，点击设置
3	发现风险业务资产	事件	未设置，点击设置



【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。

【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。

#### 第八步：云端上报





安全分析服务

上报云端分析

导出分析数据

深信服的云端包含威胁情报库和处置经验库，借助云端分析可以快速、准确地定位威胁。上报的内容包含报表、部分安全日志等。（深信服不会收集用户的隐私数据）

\* 客户名称:

邮件上报报表: ☒ 是 ☐ 否 （系统将自动每天上报综合安全报告至深信服云端，如果您的安全感知系统无法连接互联网，建议开启该功能）

云端上报报表: ☒ 是 ☐ 否

确定

【客户名称】：注明客户名称。

【云端上报报表】：选择“是”

点击 **确定**



- 1、使用云端上报报表 SIS 需要能连接到公网。
- 2、感知平台内置 DNS，无需配置。
- 3、安全感知平台的威胁情报库、特征库更新需要联网，建议开放设备的上网权限。
- 4、探针的特征库是通过感知平台下载更新的，只需要保证感知平台能连接外网即可。
- 5、建议开启云端上报，将基础数据上传到深信服云端联动分析，加快应急响应速度，更好的为您解决安全问题。

## 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：

**常规**

如果网络支持此功能，则可以获取自动指派的 IP 设置。否则，您需要从网络系统管理员处获得适当的 IP 设置。

☐ 自动获得 IP 地址 (O)

☒ 使用下面的 IP 地址 (S):

IP 地址 (I):

子网掩码 (U):

默认网关 (D):

☐ 自动获得 DNS 服务器地址 (B)

☒ 使用下面的 DNS 服务器地址 (E):

首选 DNS 服务器 (P):

备用 DNS 服务器 (A):

☐ 退出时验证设置 (L)

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：

**SANGFOR**

技术服务热线  
400-630-6430

搜索“深信服技术服务社区”  
获取更多支持

**SUPPORT**

感谢使用深信服产品

感谢您的使用

**潜伏威胁探针**

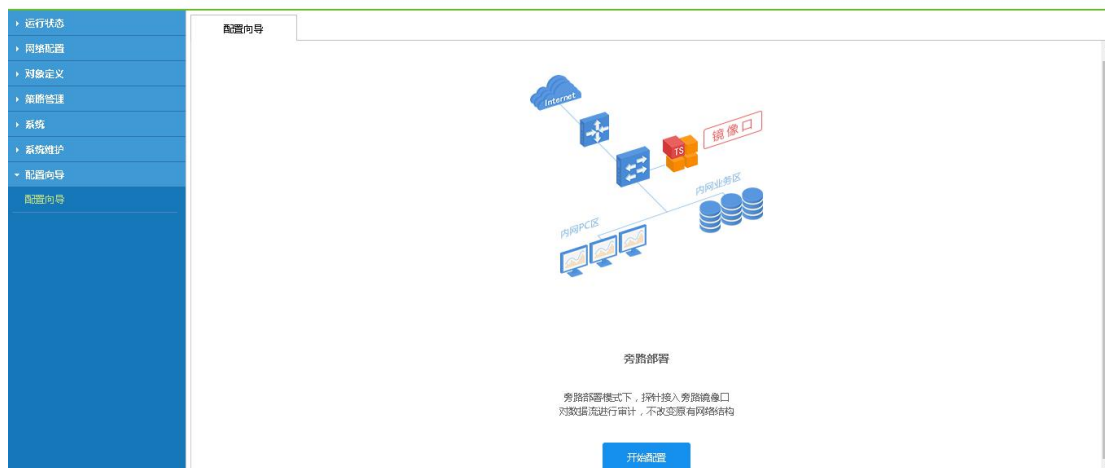
用户名

密码

© 2011-2017 深信服科技股份有限公司 版权所有

第三步：配置向导->开始配置





#### 第四步：配置管理口 ip

#### 旁路部署向导



区域 → 定义内网 → 连接感知系统 → 汇总

定义区域

管理区

当前管理口：eth0

静态IP地址：10.251.251.251/24  
192.168.1.101/24

下一跳网关：192.168.1.1

镜像区

旁路镜像接口：eth1,eth2,eth3,eth4,eth5,eth6,eth7,eth8,eth9

#### 温馨提示：

在当前进度中，您需要完成以下步骤：

- 1.配置管理口的静态IP地址，管理口将作为潜伏威胁探针设备以及感知系统数据进行同步的接口。
- 2.选择要作为旁路镜像口的接口。感知探针只针对该镜像接口的流量进行安全感知。

下一步>

【静态 IP 地址】：配置管理口 IP 及相应网关。

【旁路镜像口】：默认情况除 eth0 口外都是镜像网口。

## 第五步：内网定义

### 旁路部署向导



区域 → 定义内网 → 连接感知系统 → 汇总

#### 定义内网

##### 内网业务区

请输入业务区的所有网段：

192.168.100.0/24  
192.168.200.0/24



##### 内网PC区

请输入PC区的所有网段：

192.168.10.0/24  
192.168.20.0/24



#### 温馨提示：

配置内网业务区和内网PC区的网段，探针可以准确地识别整个内网区域内的所有访问关系。

配置内网业务区后，探针将会着重检测分析业务区的安全情况。

如不清楚某IP段为内网PC区还是内网服务器区，可无需配置该IP到以上区域内，自动识别算法会为你自动识别

< 上一步

下一步 >

【内网业务区】：定义内网服务器区的 ip 地址段。

【内网 PC 区】：定义内网用户上网区的 ip 地址段。

## 第六步：连接感知系统

## 旁路部署向导



区域 → 定义内网 → 连接感知系统 → 汇总

### 连接感知系统

感知系统地址：

日志传输模式：  
☒ 标准模式（推荐）  
☐ 精简模式（带宽较小时）  
☐ 高级模式

☐ 同步访问关系日志和netflow日志，其中访问关系日志主要用于感知平台展示访问关系，主要用于netflow引擎进行安全分析

☐ 同步DNS审计日志，主要用于平台dns flow分析引擎进行安全分析

☐ 同步HTTP审计日志，主要用于平台http flow分析引擎进行安全分析

### 温馨提示：

潜伏威胁探针的数据需要同步到感知系统上进行展示，请确保能正常连接到感知系统。

如果探针到感知系统的带宽较小，例如专网部署场景，建议将“日志传输模式”调整为“精简模式”。

< 上一步

下一步 >

【感知系统地址】：配置感知平台的 ip 地址。

【日志传输模式】：根据具体情况选择日志的传输模式。

第七步：汇总

## 旁路部署向导



区域 → 定义内网 → 连接感知系统 → 汇总

### 部署模式：旁路部署

#### 管理区

接口：eth0

管理地址：10.251.251.251/24  
192.168.1.101/24

#### 镜像区

接口：eth1,eth2,eth3,eth4,eth5,eth6,eth7,eth8,eth9

#### 定义内网

业务区：

192.168.100.0/24  
192.168.200.0/24

PC区：

192.168.10.0/24  
192.168.20.0/24

#### 感知系统

地址：192.168.1.100  
已启用标准模式！

### 探针将启用的检测内容：

- ✓ 漏洞利用攻击检测
- ✓ 僵尸网络检测
- ✓ 网站攻击检测
- ✓ 业务弱点发现

< 上一步

提交

确认以上信息配置无误则点击提交按钮

### 第八步：违规访问

定义合法的访问（白名单）和非法的访问（黑名单）



潜伏威胁探针

运行状态

网络配置

对象定义

策略管理

违规访问

安全策略

系统

系统维护

配置向导

违规访问

新增

删除

启用

禁用

上移

下移

移动

导入

导出

刷新

优先级	名称	防护对象	白名单	备注
1				
2				

新增白名单

启用

名称: 用户-OA

防护对象

目标IP组: 请选择

开放的服务: 预定义服务/any

白名单

允许访问的IP组: 请选择

允许访问的时间: 全天

备注: 可以直接在此处输入、编辑、删除

保存并继续新增

确定

取消

【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：

地址:深圳市南山区学苑大道1001号南山智园A1栋

28

咨询热线：400-806-6868

服务热线：400-630-6430

邮箱: market@sangfor.com.cn

网址: www.sangfor.com.cn

**白名单策略：**

针对目标IP（组）已开放的服务，只允许白名单里的IP（组）在指定的时间内访问，其他时间或其他IP的访问均被视为**违规**。安全感知系统将会以**橙色**关系线展示此违规访问，并记录请求内容。

**使用场景：**

类似ACL规则，可以查看内网中存在的合规性问题。例如：

**1.检测对核心服务器的违规访问**

为服务器设置白名单，任何不在白名单范围的IP视图对其访问均可被认为异常，需关注是否为权限控制配置遗漏导致。例如IT人员工作交接不明，新IT员工容易遇到此问题。

**2.找出可疑的跳板机**

长期不会访问该服务器的合法用户，突然使用RDP、FTP、SSH等风险应用频繁访问服务器，甚至时间段在凌晨，而此IP在白名单策略中只允许白天访问服务器的80端口。

运行状态

网络配置

对象定义

策略管理

违规访问

安全策略

系统

系统维护

配置向导

违规访问

新增

删除

启用

禁用

上移

下移

移动

优先级	名称	类型	目标IP组	开放的服务	允许
1					
2					

新增黑名单

启用

名称:

防护对象

目标IP组:

请选择

开放的服务:

预定义服务/any

黑名单

禁止访问的IP组:

请选择

禁止访问的时间:

全天

备注:

可以直接在此处输入、编辑、删除

保存并继续新增

确定

取消

【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

地址:深圳市南山区学苑大道1001号南山智园A1栋

30

咨询热线: 400-806-6868

服务热线: 400-630-6430

邮箱: market@sangfor.com.cn

网址: www.sangfor.com.cn



### 黑名单策略：

针对目标IP（组）已开放的服务，禁止黑名单的IP（组）在指定的时间内访问，否则将被视为**违规**。安全感知系统将会以**橙色**关系线展示此违规访问，并记录请求内容。

### 使用场景：

黑名单策略仅适用于对内网权限管理较为清晰的情况下使用。例如：

#### 1.检测越权访问的违规情况

针对某服务器，可将明确不具备权限访问该服务器的IP添加到黑名单中，来检测越权访问的情况。

#### 2.检视可疑IP对业务的影响

当已知某IP存在异常行为或已构成威胁，可将其配置到黑名单策略中，防护对象的目标IP组配置为业务区的IP组（IP范围），即可检视该可疑IP对业务的所有违规访问情况，进而排查是否构成影响。

## 第九步：安全策略的配置

必需要启用否则不记录安全日志。



### 潜伏威胁探针

<ul style="list-style-type: none"> <li>运行状态</li> <li>网络配置</li> <li>对象定义</li> <li>策略管理 <ul style="list-style-type: none"> <li>违规访问</li> <li>安全策略</li> </ul> </li> </ul>	<div>安全策略</div> <div><input checked="" type="checkbox"/> 启用</div> <div>请选择旁路安全监听策略</div> <div> <input checked="" type="checkbox"/> 网站攻击检测 <a href="#">设置</a> </div> <div> <input checked="" type="checkbox"/> 漏洞利用攻击检测 <a href="#">设置</a> </div> <div> <input checked="" type="checkbox"/> 僵尸网络检测 <a href="#">设置</a> </div> <div> <input checked="" type="checkbox"/> 业务弱点发现 </div> <div>保存</div>
--	---

默认设置即可。

## 第十步：安全感知平台

探针与感知平台对接



运行状态
网络配置
对象定义
策略管理
系统
系统配置
管理员帐号
安全感知平台

### 安全感知系统

☒ 启用

感知系统地址：

日志传输模式：

☒ 标准模式
☐ 精简模式
☐ 高级模式

☒ 同步访问关系日志和netflow日志，其中访问关系日志主要用于感知平台
☒ 同步DNS审计日志，主要用于平台dns flow分析引擎进行安全分析
☐ 同步HTTP审计日志，主要用于平台http flow分析引擎进行安全分析

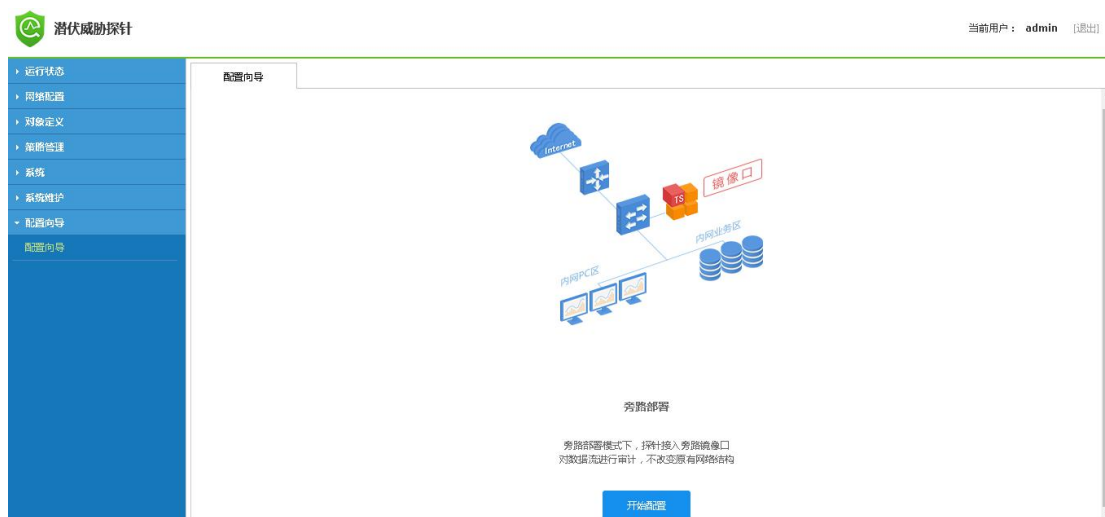
【标准模式】：适用于关注网络安全场景、占用网络资源适中

【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。

## 2.1.3 STA2 配置步骤：

第一步：配置向导->开始配置



第二步：配置管理口 ip

## 旁路部署向导



区域 → 定义内网 → 连接感知系统 → 汇总

### 定义区域

#### 管理区

当前管理口：eth0

静态IP地址：10.251.251.251/24  
192.168.1.102/24

下一跳网关：192.168.1.100



#### 镜像区

旁路镜像接口：eth1,eth2,eth3,eth4,eth5,eth6,eth7

### 温馨提示：

在当前进度中，您需要完成以下步骤：

- 1.配置管理口的静态IP地址，管理口将作为潜伏威胁探针设备以及感知系统数据进行同步的接口。
- 2.选择要作为旁路镜像口的接口。感知探针只针对该镜像接口的流量进行安全感知。

下一步>

**【静态 IP 地址】：**配置管理口 IP 及相应网关。

**【旁路镜像口】：**默认情况除 eth0 口外都是镜像网口。

第三步：内网定义

## 旁路部署向导



区域 → 定义内网 → 连接感知系统 → 汇总

### 定义内网

#### 内网业务区

请输入业务区的所有网段:

192.168.100.0/24  
192.168.200.0/24

#### 内网PC区

请输入PC区的所有网段:

192.168.10.0/24  
192.168.20.0/24

### 温馨提示：

配置内网业务区和内网PC区的网段，探针可以准确地识别整个内网区域内的所有访问关系。

配置内网业务区后，探针将会着重检测分析业务区的安全情况。

如不清楚某IP段为内网PC区还是内网服务器区，可无需配置该IP到以上区域内，自动识别算法会为你自动识别

< 上一步

下一步 >

【内网业务区】：定义内网服务器区的 ip 地址段。

【内网 PC 区】：定义内网用户上网区的 ip 地址段。

第四步：连接感知系统

## 旁路部署向导





区域 → 定义内网 → 连接感知系统 → 汇总

## 连接感知系统

感知系统地址：

日志传输模式：

☒ 标准模式（推荐）☐ 精简模式（带宽较小时）☐ 高级模式☐ 同步访问关系日志和netflow日志，其中访问关系日志主要用于感知平台展示访问关系，主要用于netflow引擎进行安全分析☐ 同步DNS审计日志，主要用于平台dns flow分析引擎进行安全分析☐ 同步HTTP审计日志，主要用于平台http flow分析引擎进行安全分析

## 温馨提示：

潜伏威胁探针的数据需要同步到感知系统上进行展示，请确保能正常连接到感知系统。

如果探针到感知系统的带宽较小，例如专网部署场景，建议将“日志传输模式”调整为“精简模式”。

&lt; 上一步

下一步 &gt;

**【感知系统地址】：**配置感知平台的ip地址。**【日志传输模式】：**根据具体情况选择日志的传输模式。

第五步：汇总

## 旁路部署向导



区域 → 定义内网 → 连接感知系统 → 汇总

## 部署模式：旁路部署

## 管理区

接口：eth0

管理地址：10.251.251.251/24  
192.168.1.102/24

## 镜像区

接口：eth2,eth3,eth4,eth5

## 定义内网

业务区：

192.168.100.0/24  
192.168.200.0/24

PC区：

192.168.10.0/24  
192.168.20.0/24

## 感知系统

地址：192.168.1.100  
已启用标准模式！

## 探针将启用的检测内容：

- ✓ 漏洞利用攻击检测
- ✓ 僵尸网络检测
- ✓ 网站攻击检测
- ✓ 业务弱点发现

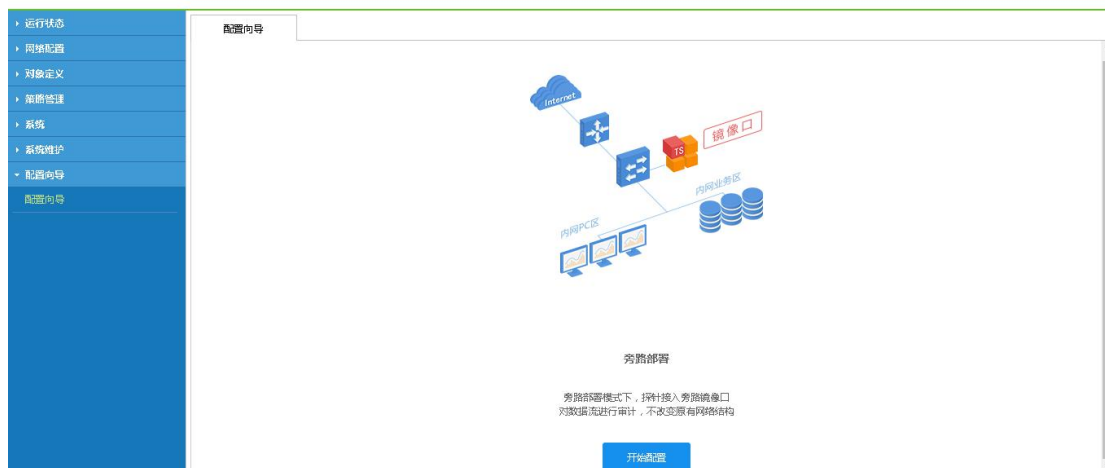
&lt; 上一步

提交

确认以上信息配置无误则点击提交按钮

## 2.1.3 STA3 配置步骤：

第一步：配置向导-&gt;开始配置



## 第二步：配置管理口 ip

### 旁路部署向导



区域 → 定义内网 → 连接感知系统 → 汇总

#### 定义区域

##### 管理区

当前管理口：eth0

静态IP地址：10.251.251.251/24  
192.168.1.103/24

下一跳网关：192.168.1.1

##### 镜像区

旁路镜像接口：eth2,eth3,eth4,eth5

#### 温馨提示：

在当前进度中，您需要完成以下步骤：

- 1.配置管理口的静态IP地址，管理口将作为潜伏威胁探针设备以及感知系统数据进行同步的接口。
- 2.选择要作为旁路镜像口的接口。感知探针只针对该镜像接口的流量进行安全感知。

下一步>

【静态 IP 地址】：配置管理口 IP 及相应网关。

【旁路镜像口】：默认情况除 eth0 口外都是镜像网口。

### 第三步：内网定义

#### 旁路部署向导



区域 → **定义内网** → 连接感知系统 → 汇总

#### 定义内网

##### 内网业务区

请输入业务区的所有网段:

192.168.100.0/24  
192.168.200.0/24

##### 内网PC区

请输入PC区的所有网段:

192.168.10.0/24  
192.168.20.0/24

#### 温馨提示：

配置内网业务区和内网PC区的网段，探针可以准确地识别整个内网区域内的所有访问关系。

配置内网业务区后，探针将会着重检测分析业务区的安全情况。

如不清楚某IP段为内网PC区还是内网服务器区，可无需配置该IP到以上区域内，自动识别算法会为你自动识别

< 上一步

下一步 >

【内网业务区】：定义内网服务器区的 ip 地址段。

【内网 PC 区】：定义内网用户上网区的 ip 地址段。

### 第四步：连接感知系统

## 旁路部署向导



区域 → 定义内网 → 连接感知系统 → 汇总

### 连接感知系统

感知系统地址：

日志传输模式：

☒ 标准模式（推荐）

☐ 精简模式（带宽较小时）

☐ 高级模式

☐ 同步访问关系日志和netflow日志，其中访问关系日志主要用于感知平台展示访问关系，主要用于netflow引擎进行安全分析

☐ 同步DNS审计日志，主要用于平台dns flow分析引擎进行安全分析

☐ 同步HTTP审计日志，主要用于平台http flow分析引擎进行安全分析

### 温馨提示：

潜伏威胁探针的数据需要同步到感知系统上进行展示，请确保能正常连接到感知系统。

如果探针到感知系统的带宽较小，例如专网部署场景，建议将“日志传输模式”调整为“精简模式”。

< 上一步

下一步 >

【感知系统地址】：配置感知平台的 ip 地址。

【日志传输模式】：根据具体情况选择日志的传输模式。

第五步：汇总



旁路部署向导



区域 → 定义内网 → 连接感知系统 → 汇总

部署模式：旁路部署

管理区

接口：eth0

管理地址：10.251.251.251/24  
192.168.1.103/24

镜像区

接口：eth2,eth3,eth4,eth5

定义内网

业务区：

192.168.100.0/24  
192.168.200.0/24

PC区：

192.168.10.0/24  
192.168.20.0/24

感知系统

地址：192.168.1.100  
已启用标准模式！

探针将启用的检测内容：

- ✓ 漏洞利用攻击检测
- ✓ 僵尸网络检测
- ✓ 网站攻击检测
- ✓ 业务弱点发现

< 上一步

提交

确认以上信息配置无误则点击提交按钮

## 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：

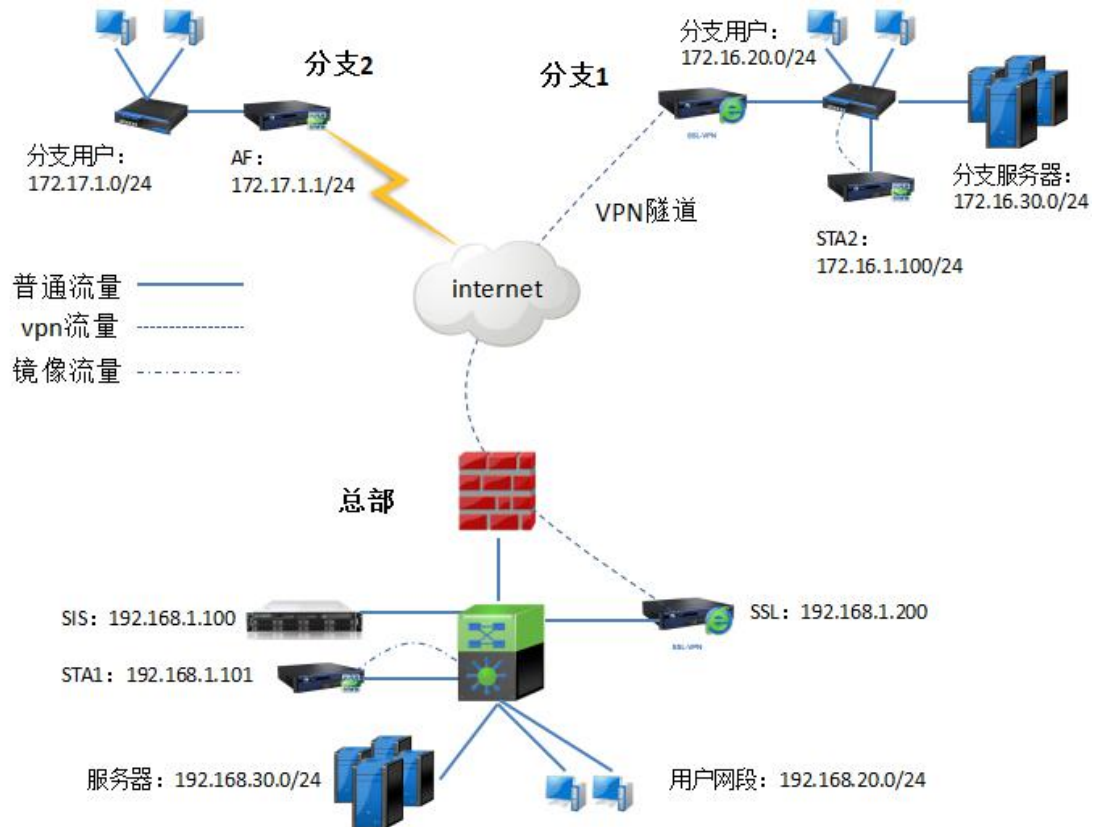
\* 感知平台 ip 需要与探针管理口 ip 通信，接收探针发来的数据。SIS eth0 口配置 ip 为 192.168.1.100；STA\_1 eth0 口配置 ip 192.168.1.101；STA\_2 eth0 口配置 ip 172.16.1.100；

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

### 配置内网IP范围



请将全部内网IP范围、业务资产IP配置到如下窗口中。  
有助于规范检测范围、提高平台分析的准确性、同时减少资源消耗。

内网IP范围

业务资产IP

如内网办公区、业务区、各个分支/分域等内网全部的IP范围。

192.168.1.0/24  
192.168.20.0/24  
192.168.30.0/24  
172.16.1.0/24  
172.16.20.0/24  
172.16.30.0/24  
172.17.1.0/24

确定

取消

### 配置内网IP范围



请将全部内网IP范围、业务资产IP配置到如下窗口中。  
有助于规范检测范围、提高平台分析的准确性、同时减少资源消耗。

内网IP范围

业务资产IP

业务区所有服务器资产的IP或范围。

192.168.20.0/24  
192.168.30.0/24  
172.16.20.0/24  
172.16.30.0/24

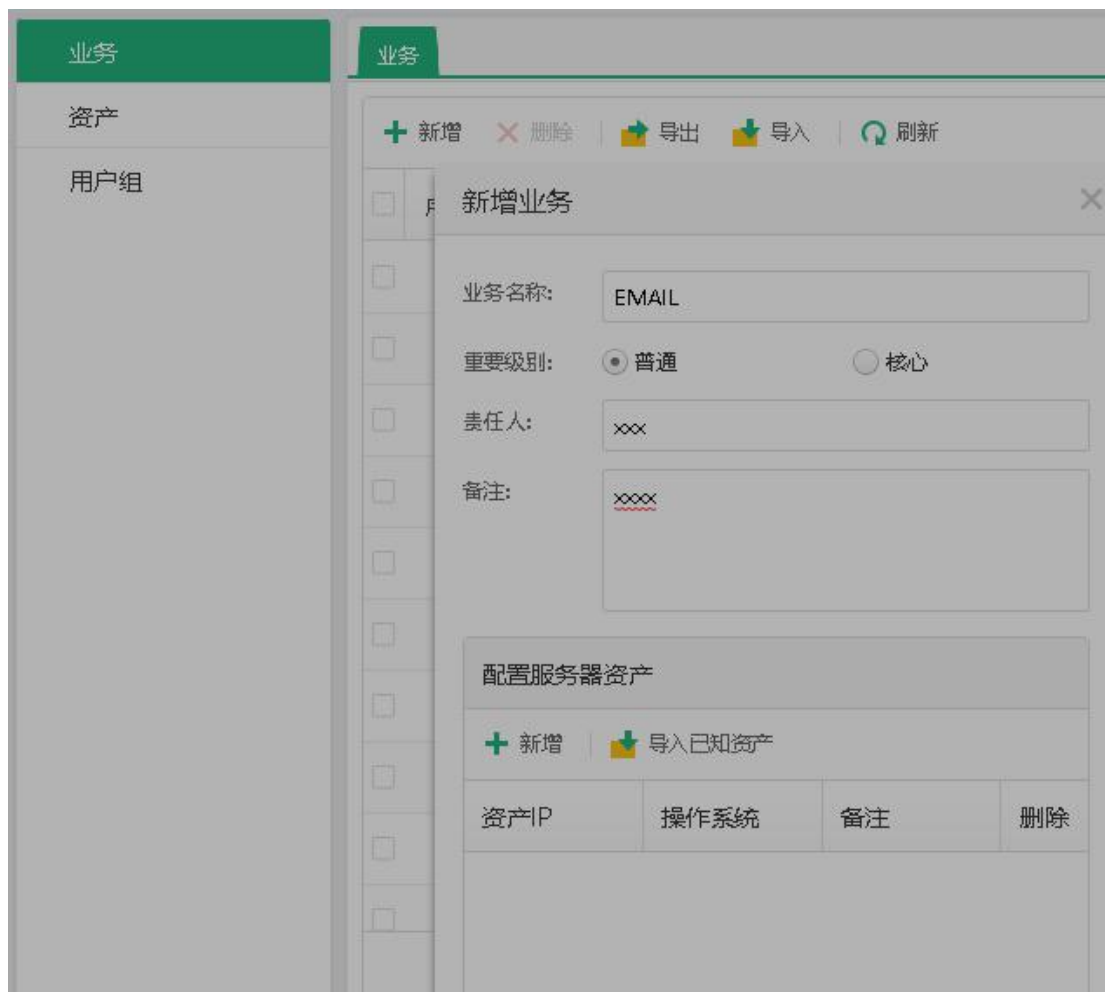
确定

取消

**【内网 IP 范围】**：内网所有网段，包括用户网段和业务网段

**【业务资产 IP】**：服务器网段。

## 第二步：业务配置



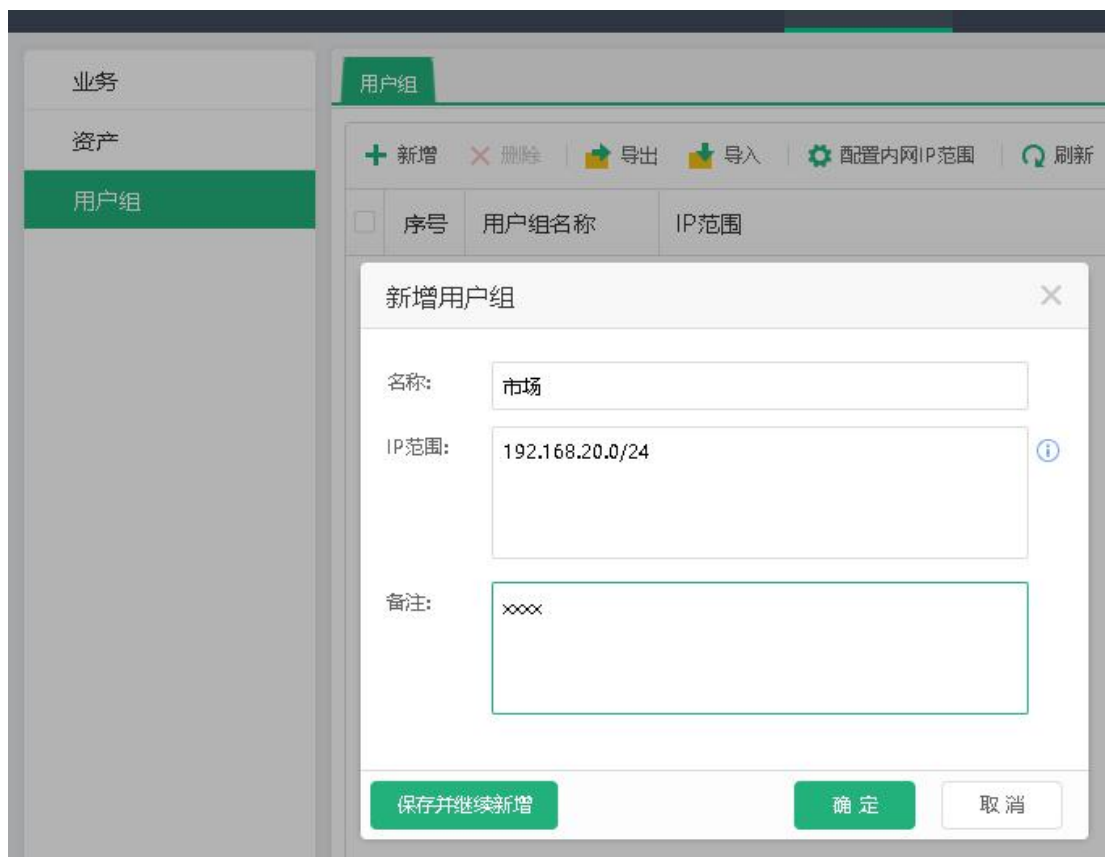
【新增】：新增业务。

【配置服务器资产】：可以新增或选择第四步中新增的资产。

【导出】：可以将业务导出为.csv 文件。

【导入】：可以将业务导入系统中。

第三步：配置用户组



【名称】：用户组部门名称。

【IP 范围】：用户所在的网段。

第四步：分支配置，选择单位标识。

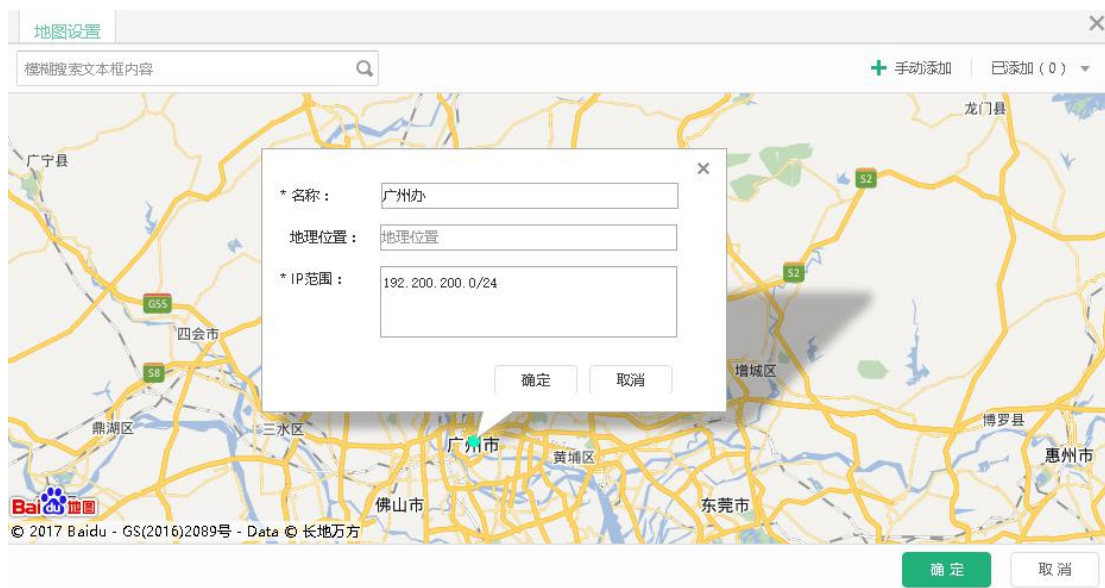




【ip 范围】：适用于所有分支单位的流量共用统一出口，各单位以 IP 范围为标识；

【设备】：适用于各分支单位流量非统一出口，以设备 ID 区分各单位；

#### 第五步：新增分支——选择 IP 范围

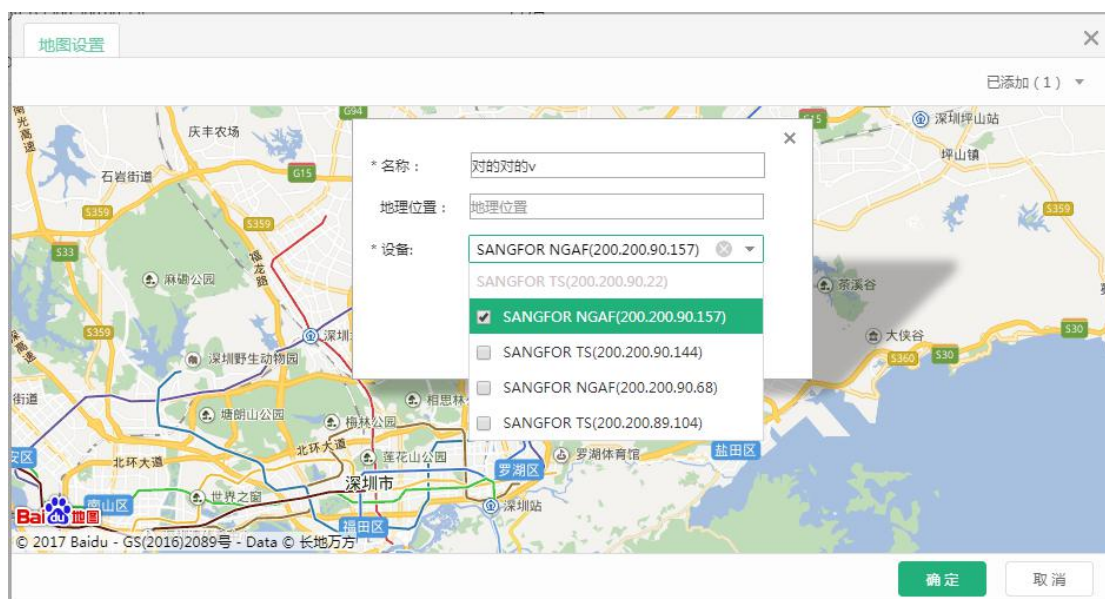


【手动添加】：将光标移动到分支的相应位置。

【名称】：分支名称。

【IP 范围】：分支的 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

旁路部署向导 ×

区域 → 定义内网 → 连接感知系统 → 汇总

定义内网

内网业务区

请输入业务区的所有网段:

192.168.30.0/24  
172.16.30.0/24

?

内网PC区

请输入PC区的所有网段:

192.168.20.0/24  
172.16.20.0/24

?

**温馨提示：**

配置内网业务区和内网PC区的网段，探针可以准确地识别整个内网区域内的所有访问关系。

配置内网业务区后，探针将会着重检测分析业务区的安全情况。

如不清楚某IP段为内网PC区还是内网服务器区，可无需配置该IP到以上区域内，自动识别算法会为你自动识别

< 上一步

下一步 >

【内网业务区】：定义内网服务器区的 ip 地址段。

【内网 PC 区】：定义内网用户上网区的 ip 地址段。



## 第二步：连接感知系统

旁路部署向导

区域

→

定义内网

→

连接感知系统

→

汇总

连接感知系统

感知系统地址：

192.168.1.100

日志传输模式：

● 标准模式（推荐）

● 精简模式（带宽较小时）

● 高级模式

同步访问关系日志和netflow日志，其中访问关系日志主要用于感知平台展示访问关系，主要用于netflow引擎进行安全分析

同步DNS审计日志，主要用于平台dns flow分析引擎进行安全分析

同步HTTP审计日志，主要用于平台http flow分析引擎进行安全分析

温馨提示：

潜伏威胁探针的数据需要同步到感知系统上进行展示，请确保能正常连接到感知系统。

如果探针到感知系统的带宽较小，例如专网部署场景，建议将“日志传输模式”调整为“精简模式”。

< 上一步

下一步 >

【感知系统地址】：配置感知平台的 ip 地址。

【日志传输模式】：根据具体情况选择日志的传输模式。

## 第三步：汇总

## 旁路部署向导



区域 → 定义内网 → 连接感知系统 → 汇总

### 部署模式：旁路部署

#### 管理区

接口：eth0      管理地址：10.251.251.251/24  
192.168.1.101/24

#### 镜像区

接口：eth1,eth2,eth3,eth4,eth5,eth6,eth7,eth8,eth9

#### 定义内网

业务区： 192.168.30.0/24  
172.16.30.0/24

PC区： 192.168.20.0/24  
172.16.20.0/24

#### 感知系统

地址：192.168.1.100  
已启用标准模式！

### 探针将启用的检测内容：

- ✓ 漏洞利用攻击检测
- ✓ 僵尸网络检测
- ✓ 网站攻击检测
- ✓ 业务弱点发现

< 上一步

提交

确认以上信息配置无误则点击提交按钮

## 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

## 旁路部署向导



区域 → 定义内网 → 连接感知系统 → 汇总

### 定义内网

#### 内网业务区

请输入业务区的所有网段:

192.168.30.0/24  
172.16.30.0/24



#### 内网PC区

请输入PC区的所有网段:

192.168.20.0/24  
172.16.20.0/24



### 温馨提示:

配置内网业务区和内网PC区的网段，探针可以准确地识别整个内网区域内的所有访问关系。

配置内网业务区后，探针将会着重检测分析业务区的安全情况。

如不清楚某IP段为内网PC区还是内网服务器区，可无需配置该IP到以上区域内，自动识别算法会为你自动识别

< 上一步

下一步 >

【内网业务区】：定义内网服务器区的 ip 地址段。

【内网 PC 区】：定义内网用户上网区的 ip 地址段。

## 第二步：连接感知系统

## 旁路部署向导





区域 → 定义内网 → 连接感知系统 → 汇总

## 连接感知系统

感知系统地址：

日志传输模式：

☒ 标准模式（推荐）☐ 精简模式（带宽较小时）☐ 高级模式☐ 同步访问关系日志和netflow日志，其中访问关系日志主要用于感知平台展示访问关系，主要用于netflow引擎进行安全分析☐ 同步DNS审计日志，主要用于平台dns flow分析引擎进行安全分析☐ 同步HTTP审计日志，主要用于平台http flow分析引擎进行安全分析

## 温馨提示：

潜伏威胁探针的数据需要同步到感知系统上进行展示，请确保能正常连接到感知系统。

如果探针到感知系统的带宽较小，例如专网部署场景，建议将“日志传输模式”调整为“精简模式”。

&lt; 上一步

下一步 &gt;

**【感知系统地址】：**配置感知平台的ip地址。**【日志传输模式】：**根据具体情况选择日志的传输模式。

第三步：汇总

## 旁路部署向导



区域 → 定义内网 → 连接感知系统 → 汇总

### 部署模式：旁路部署

#### 管理区

接口：eth0

管理地址：10.251.251.251/24  
192.168.1.101/24

#### 镜像区

接口：eth1,eth2,eth3,eth4,eth5,eth6,eth7,eth8,eth9

#### 定义内网

业务区：

192.168.30.0/24  
172.16.30.0/24

PC区：

192.168.20.0/24  
172.16.20.0/24

#### 感知系统

地址：192.168.1.100

已启用标准模式！

### 探针将启用的检测内容：

- ✓ 漏洞利用攻击检测
- ✓ 僵尸网络检测
- ✓ 网站攻击检测
- ✓ 业务弱点发现

< 上一步

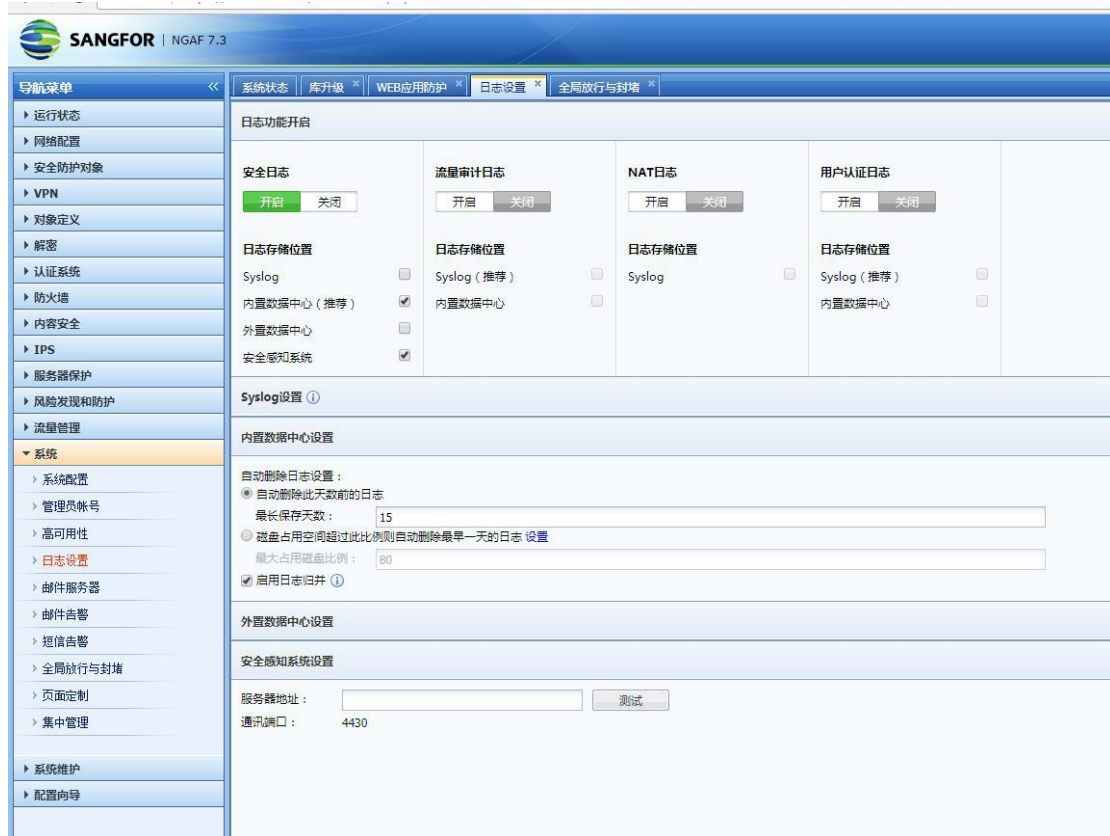
提交

确认以上信息配置无误则点击提交按钮

### 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：配置与感知平台



- 1、STA 与 SIS 的数据传输端口为 4430。
- 2、vpn 环境下建议在探针上开启精减模式。
- 3、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。

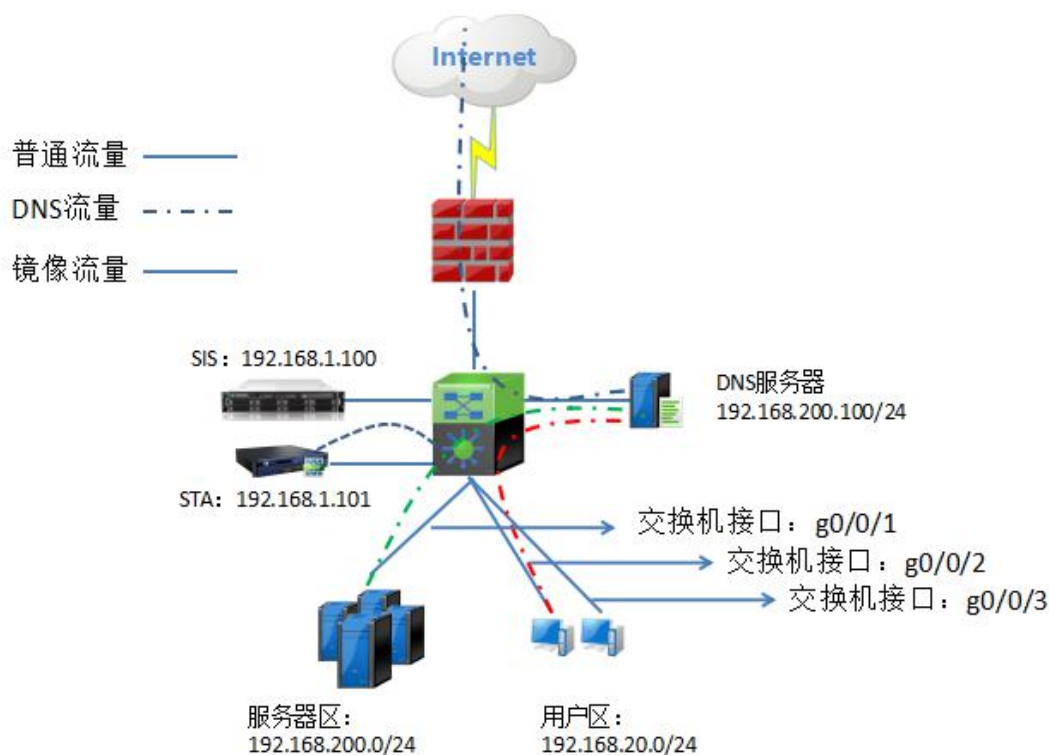
感知平台部署：

- \* 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。

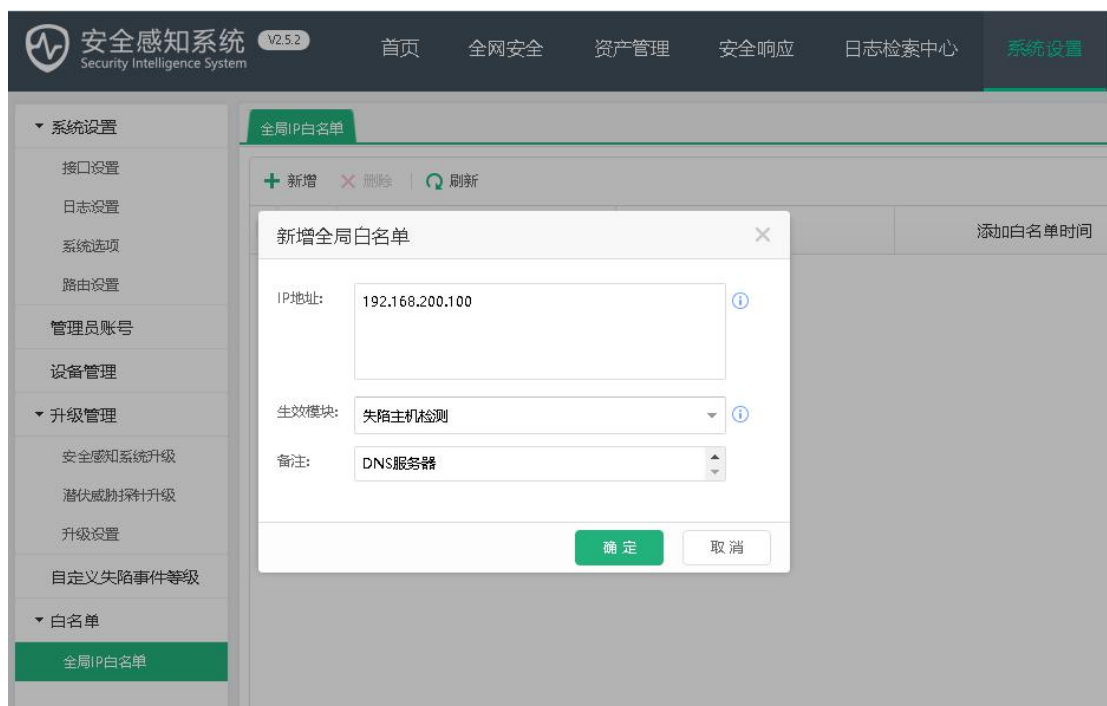
注意：探针收集下图中核心交换机 g0/0/1、g0/0/2、g0/0/3 的镜像数据。并将 DNS 服务器 IP 地址加入到 SIS 的全局白名单中。



## 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。



【全局 IP 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。



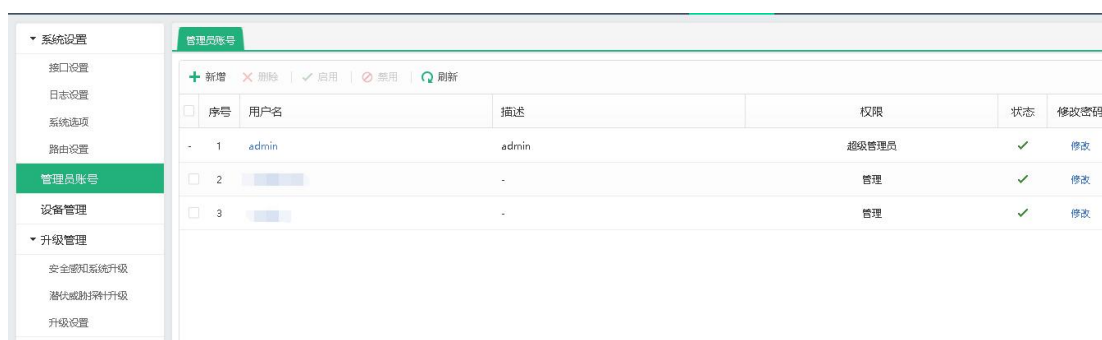
## 第三章：密码安全风险提示

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。



修改密码

旧密码:

新密码:  ⓘ

确认密码:  ⓘ

确定 取消

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。



密码修改

旧密码：

新密码：

确认新密码：

提交

取消

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 session 1 source interface fa0/1 both

Switch(config)#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 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 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

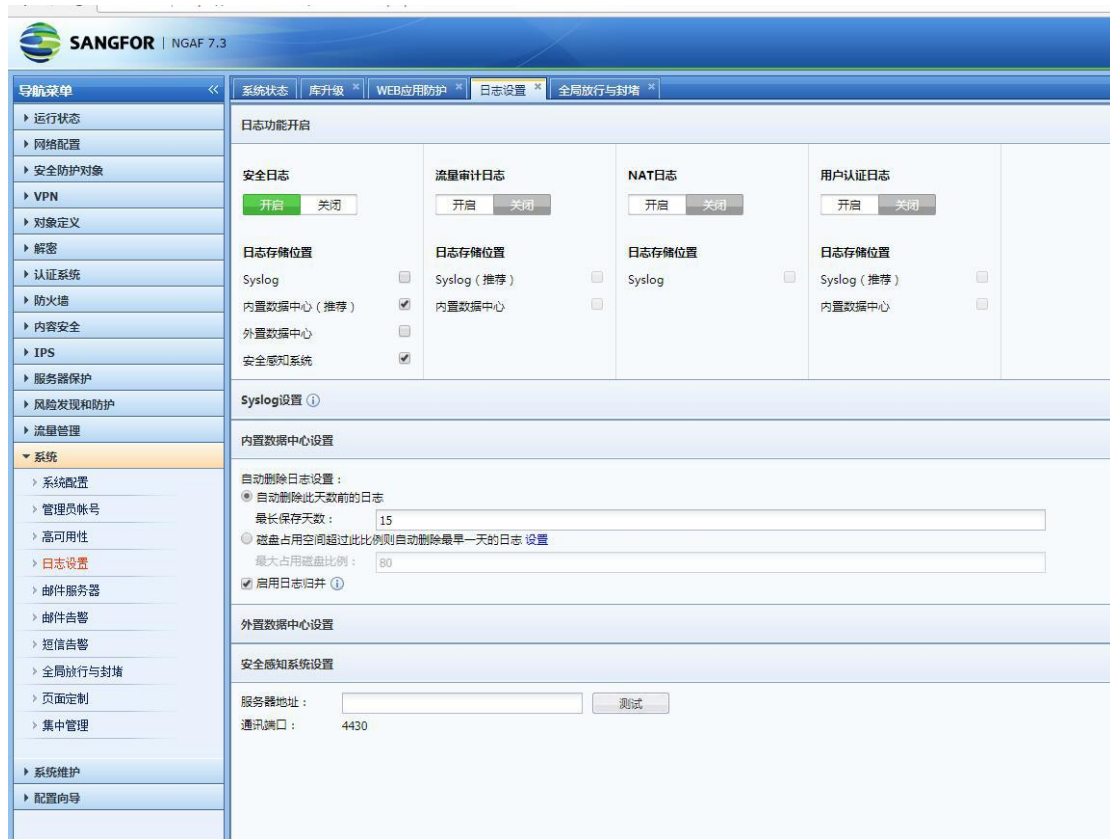
Switch(config)# monitor session 1 destination interface fastethernet 0/2

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 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 session 1 destination interface fa 0/2` 设置 fa0/2 为监控口

## 附件二：NGAF 7.3 版本对接安全感知平台配置



## 附件三：产品接口列表

### STA100——4 电 2 光

设备名称	网口编号	网口类型
STA100	MANAGE 口(ETH0)	千兆电口
	ETH1	千兆电口
	ETH2	千兆电口
	ETH3	千兆电口
	ETH4	千兆光口
	ETH5	千兆光口

### STA200——6 电 4 光

设备名称	网口编号	网口类型	网口编号	网口类型
STA200	MANAGE 口 (ETH0)	千兆电口	ETH5	千兆电口
	ETH1	千兆电口	ETH6	千兆光口
	ETH2	千兆电口	ETH7	千兆光口
	ETH3	千兆电口	ETH8	千兆光口
	ETH4	千兆电口	ETH9	千兆光口

### STA300——8 电 4 光 2 万兆

设备名称	网口编号	网口类型	网口编号	网口类型
STA300	MANAGE 口 (ETH0)	千兆电口	ETH9	千兆电口
	ETH1	千兆电口	ETH6	千兆光口
	ETH2	千兆电口	ETH7	千兆光口
	ETH3	千兆电口	ETH10	千兆光口
	ETH4	千兆电口	ETH11	千兆光口
	ETH5	千兆电口	ETH12	万兆光口
	ETH8	千兆电口	ETH13	万兆光口

### STA400——9 电 8 光 4 万兆

设备名称	网口编号	网口类型	网口编号	网口类型
STA-400	MANAGE 口 (ETH0)	千兆电口	ETH10	千兆光口
	ETH1	千兆电口	ETH11	千兆光口
	ETH2	千兆电口	ETH12	千兆光口
	ETH3	千兆电口	ETH13	千兆光口
	ETH4	千兆电口	ETH14	千兆光口
	ETH5	千兆电口	ETH15	千兆光口
	ETH6	千兆电口	ETH16	千兆光口
	ETH7	千兆电口	ETH17	万兆光口
	ETH8	千兆电口	ETH18	万兆光口
	ETH9	千兆光口	ETH19	万兆光口
			ETH20	万兆光口

### SIS-1000——6 电

设备名称	网口编号	网口类型
SIS1000	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

## SIS-2000——6 电 2 万兆

设备名称	网口编号	网口类型
SIS2000	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