SBC3000 Pro 会话边界控制器

用户手册 V1.0

深圳鼎信通达股份有限公司

地址：深圳南山区西丽街道新科一街创新谷一期 1 栋 A 座 18 楼

邮编：518052

电话：+86 755 2645 6664

传真：+86 755 2645 6659

邮箱：sales@dinstar.com, support@dinstar.com

网址：www.dinstar.cn

前言

欢迎选购

欢迎您选购鼎信通达 SBC3000 Pro 会话边界控制器！深圳鼎信通达股份有限公司为您提供全方位的技术支持，需要更多在线技术支持，请拨打技术支持热线电话：0755-26456110/112。

内容介绍

为了更好的帮助您了解和使用 SBC3000 Pro 会话边界控制器,我们编写了该产品的用户手册，主要介绍了该产品的应用场景、功能特性、安装方法、网络连接和 Web 配置&操作等。在使用 SBC3000 Pro 会话边界控制器的过程中，请仔细阅读本手册。

适用对象

本手册适合下列人员阅读：

- 用户
- 安装、配置和维护 SBC3000 Pro 会话边界控制器的工程师

修订记录

文档名称	文档版本	软件版本
SBC3000 Pro 会话边界控制器用户手册	V1.0	2.93.2.0

文档约定

本文档中所提及的系统或设备均指 SBC3000 Pro 会话边界控制器；文档中有注意或说明的内容，表示为需要用户特别注意的内容。

安全规则设置提示

为保障系统业务安全，请根据具体业务需求设置安全规则。如：IP 防攻击策略、SIP 防攻击策略、系统安全、访问控制、黑白名单、IP 地址白名单等。

配置和参数如有不明之处，可联系技术支持咨询。

目录

1 产品概述

1.1 产品简介

SBC3000 Pro 会话边界控制器，可以为电信运营商，虚拟运营商和企业的 SIP 网络提供安全保障、接入控制、网络互连、路由/策略管理、信令流控、QoS 和媒体处理等业务。它采用多核处理器，无阻塞千兆交换网，嵌入式 Linux 操作系统，能够在实现高性能的同时保持极低的功耗。SBC3000 Pro 支持双电源热备、双机热备(HA)和 WebRTC，具备电信级高可靠性。

SBC3000 Pro 支持 20000 个 SIP 分机注册和 1500 路语音媒体转码处理，并且支持拓扑隐藏、NAT 穿越，安全防护，SRTP 和 TLS 加密等安全通信方式，同时支持 G.729，G.723，G.711a/u，G.726，AMR，OPUS，iLBC 等多种媒体编解码。

1.2 应用场景

SBC3000 Pro 会话边界控制器的应用场景如下图所示：

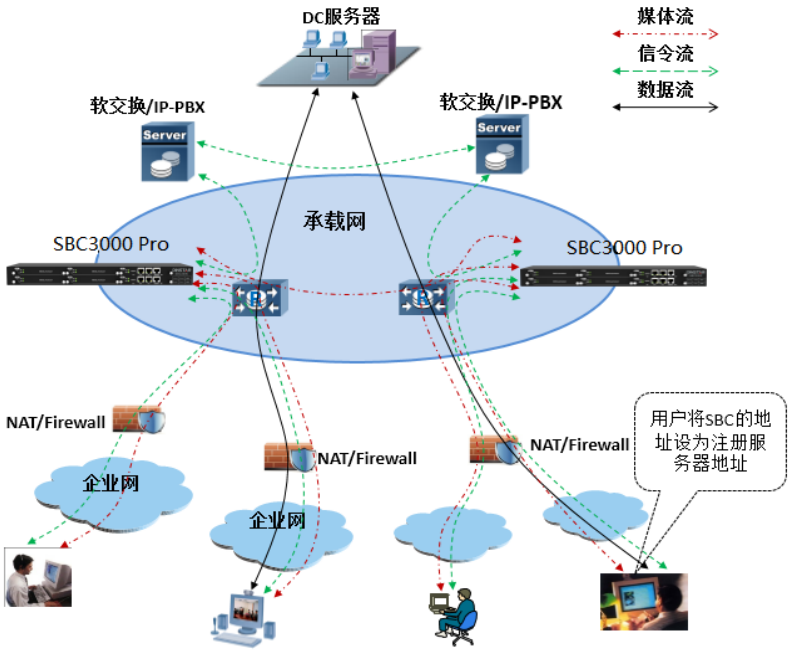


图 1-1 SBC3000 Pro 应用场景

1.3 产品外观

前面板：

后面板：

1.4 指示灯说明

指示灯	定义	状态	描述
PWR	电源指示灯	灭	无电源输入或电源输入不正常
		长亮	电源输入正常
RUN	运行状态指示灯	慢闪（亮 2s，灭 2s）	设备正常运行
		快闪两次（200ms），灭 1s	升级镜像成功
		快闪（200ms）	升级镜像失败
		其它	设备系统异常
网口(GE0~GE7)	网口绿灯(Link)	快闪	有报文交互
		常亮	网线连接正常
		灭	网络未连接或网络连接不正常
	网口黄灯(Speed)	长亮	网络速率为 1000Mbps
		灭	网络速率为 10/100Mbps

1.5 功能和特性

- **系统功能**

- SBC3000 Pro 支持 5000 并发会话和 1500 路语音媒体转码处理
- 支持双机热备
- 支持 WebRTC，语音/视频通话
- 标准 SIP 协议和灵活的路由规则，完美兼容 IMS 系统，SIP 账户组注册 5000 个账户
- 代理注册 20000 个账户
- 支持拓扑隐藏和安全防攻击策略，保护核心网
- 支持智能带宽限制和动态黑名单
- 支持跨网，NAT 穿越，适应多种组网环境
- 支持 SIP over TLS，SRTP 加密会话

- **语音特性**

- 语音编码：PCMA, PCMU, G.723.1, G.729AB，iLBC_13K，iLBC_15K, OPUS, AMR, OPUS-16k, G722
- 传真：T.38 和 Pass-through
- DTMF 模式：RFC2833/Signal/Inband
- 智能媒体处理
- RTP/RTCP
- 语音中断保护
- 媒体录音规范 (SIPREC)

- **业务路由**

- 支持多种灵活选路策略
- SIP 中继组支持主备、负载均衡模式
- 支持号码变换

➢ **协议**

- SIP v2.0, UDP, TCP, TLS, RFC3261
- B2BUA 用户代理
- SIP 呼叫流控
- SIP 注册流控
- SIP 注册报文攻击动态扫描检测
- SIP 异常呼叫攻击动态扫描检测
- SIP 头域变换
- SIP 头域透传
- SIP 报文冗余机制
- QoS 服务
- NAT 穿越

➢ **安全**

- DOS/DDOS 攻击防御
- 访问控制策略
- 基于策略的 IP 和 SIP 防攻击
- 畸形报文检测与处理
- UDP-Flood 攻击防御
- TCP-Flood 攻击防御
- SRTP 加密会话
- TLS 安全防护
- 主被叫号码黑白名单
- ACL 控制
- IP 语音防火墙

➢ **管理维护**

- WEB 管理
- SSH 命令行
- 配置备份与恢复
- 多语言支持（中英文）
- SNMP
- DMCloud (Dinstar NMS)
- 网络抓包

➢ **物理规格**

- 整框提供 1 个主控板（MCU）槽位和 4 个业务板（MFU）槽位
- 以太网接口:8*10/100/1000M Base-T 以太网接口
- 串口：1* USB 串口
- 双电源热备：100-240VAC, 50/60 Hz
- 功耗：70W
- 尺寸(W/D/H)：437*320*44mm(1U)
- 重量：6kg

➢ **工作环境**

- 电源：输入 AC100-240VAC，50-60 Hz
- 最大功耗：70W
- 网络接口：10/100/1000M 自适应 GE 口
- 工作温度：0 ℃ ~ 45 ℃
- 存储温度：-20 ℃ ~80 ℃
- 湿度：10%-90% （无冷凝）

2 安装指导

2.1 安装前准备

2.1.1 安全注意事项

在安装和使用 SBC3000 Pro 过程中，用户请遵照下列安全注意事项进行操作，以确保安全。

- 保证 SBC3000 Pro 安装场所远离潮湿及热源；
- 检查并确认供电电源在设备允许的使用范围；
- 请有经验或者受过培训的人员负责安装、维护 SBC3000 Pro；
- 佩戴防静电手腕；
- 确认 SBC3000 Pro 正确接地；
- 正确连接 SBC3000 Pro 接口电缆；
- 请不要带电插拔电缆；
- 建议用户使用 UPS 不间断电源；

2.1.2 检查机房环境是否维持良好的温/湿度条件

为保证设备正常工作和使用寿命，机房内需维持一定的温度和湿度。

- 机房环境湿度要控制在 10-90%（非冷凝），若湿度过大，则易造成绝缘材料绝缘效果不良甚至漏电，还会产生金属部件锈蚀等现象；若湿度过低，则易产生静电及绝缘垫片干缩而引起的紧固螺丝松动现象；
- 机房环境温度要控制在 0-45℃，若温度过高，则会加速元器件及绝缘材料的老化过程； 若温度过低，则可能造成系统运行不稳定。

2.1.3 检查洁净度/通风

灰尘对设备的运行安全是一大危害。放置设备的环境要保持一定的洁净度，要确保设备入风口及出风口处至少留有 5 厘米的空间，保持良好的通风以利于机箱的散热。安装 SBC3000 Pro 的机柜本身也要求具有良好的通风散热系统。

2.1.4 检查接地条件

在不具备独立接地系统的安装环境中，交流供电系统应该保证：

- 交流供电插座为带接地的三线供电；
- 交流供电系统的良好接地；
- 避免与产生电源干扰的设备共用电源插座排；

在具备独立接地的机房安装环境中， 应该将 SBC3000 Pro 提供的专用接地端子与机房的独立接地系统可靠地连接起来。这样既可以保证设备操作的安全，又可以避免语音质量受环境干扰。

2.1.5 检查电磁环境条件

设备在运行中可能会遇到各种干扰源，对设备的正常运行产生不良影响。为了增强设备的抗干扰及防雷击能力，有以下建议：

- 远离高功率无线电、雷达发射台及高频率大电流设备；
- 设备提供模拟线二级防雷击保护，应用环境需有一级防雷措施；
- 供电系统尽量独用并采取有效的防电网干扰措施；
- 保证设备的电源接地效果良好，或者加入避雷装置；

2.1.6 检查配套设备

机柜：安装 SBC3000 Pro 的机柜除了要保持良好的通风散热系统外，还要求其足够牢固，能够支撑设备的重量，此外，还要保证安装机柜有良好的接地条件。

中继线路：确定已向电信运营商申请了中继线，并已开通。

IP 网络：设备通过 10/100/1000M 标准以太网口连接到 IP 网上，与网络上各设备连接。检查 IP 承载网是否就绪，包括路由器、以太网交换机、网线布放情况，以保证网关可以正确地接入到 IP 网上。

电源插座：当使用插座排为设备提供就近的交流供电时，确保使用有接地保护接头的插座排。

2.1.7 安装工具

- 螺丝刀
- 防静电手腕
- 以太网、配置口电缆
- 电源线
- 电话线
- 集线器（HUB）、电话机、传真机或者小交换机（PBX）
- 配置终端（可以是普通的带有超级终端仿真软件的个人电脑）
- 万用表

2.1.8 开箱

在安装场所准备妥当之后，请打开包装箱进行验货，并确认设备及随机部件是否齐全。

一台基本配置的 SBC3000 Pro，通常包含以下配置：

- SBC3000 Pro 主机设备 1 台
- 电源线，1 米，AC250V/4A
- 网线 2 根
- 接地线 1 根

2.2 机架安装

2.2.1 安装准备

SBC3000 Pro 安装到机柜上有两种方式：托板安装和挂耳安装。

如果使用托板安装，那么需要明确机房是否提供托板，如不提供，则需要准备符合机柜尺寸的托板及螺钉。使用挂耳安装，需要确认机柜尺寸是否匹配，以下为对机架的要求：

- 机架的尺寸要求宽度为标准的 19 英寸，深度大于等于 550mm；
- 机柜良好接地；
- 建议安装位置大于 3U 高度，保证上下 1U 内无其他设备；
- 所需配件： 挂耳 1 副，机架螺钉 8 颗，以及接地线 1 根。

2.2.2 设备安装

安装步骤如下：

1. 在 L 型挂耳用螺钉固定在 SBC3000 Pro 的两侧；
2. 将 SBC3000 Pro 插入机架中，将 L 型挂耳的螺钉孔对着机架上的孔，并保持机身水平；
3. 用螺钉将 L 型挂耳固定到机架上。

2.2.3 地线的连接

在 SBC3000 Pro 设备后面板的接地点上差上接地线，并把接地线的另一端接在机柜的接地条上。

2.3 布设网线

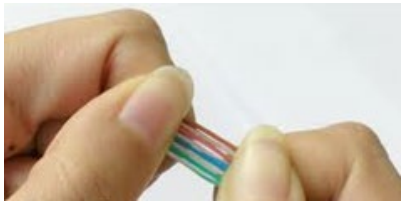
2.3.1 注意事项

布线时需按照机房规划，不破坏机房的布线格局，不能干扰或破坏机房其它设备的正常运转。 如需要布置多条线路，需在每条线路上用标签纸上做好标记，标注 IP 地址、目的端口等，便于后续连接调试及以后的管理维护。

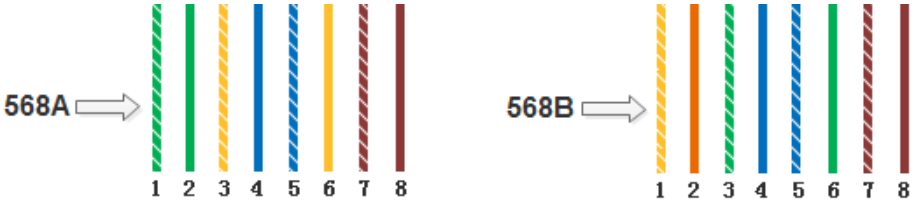
2.3.2 网线制作

步骤 1：利用斜口钳剪下所需双绞线长度，至少 0.6 米，最长不超过 100 米。然后用双绞线剥线器将双绞线的外皮除去 2 至 3 厘米。

步骤 2：剥线完成后的双绞线电缆如图所示。



步骤 3：小心的剥开每一对线，按照 EIA / TIA 568B 的标准来排列线对顺序，如图所示。

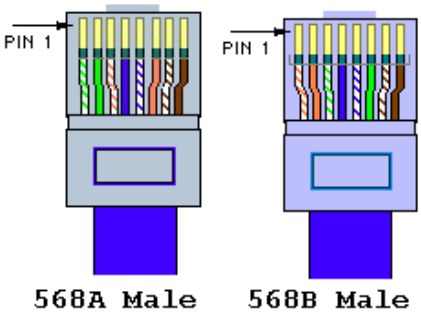


PIN1 线序左起为：白绿、绿、白橙、蓝、白蓝、橙、白棕；PIN2 线序左起为：白橙、橙、白绿、蓝、白蓝、绿、白棕、棕。

步骤 4：将裸露出的双绞线用剪刀或斜口钳剪下只剩约 14mm 的长度，再将双绞线的每一根线依照步骤三的线序放入 RJ-45 接头的引脚内，第一只引脚内应该放白绿色的线。

步骤 5：确定双绞线的每根线已经正确放置后，用压线钳压接 RJ-45 接头，如下图。

步骤 6：按照以上的步骤，制作另一端的 RJ-45 接头（另一端的线序为白橙、橙、白绿、蓝、白蓝、绿、白棕、棕）。



步骤 7：用网线测试工具检测网线的连通性。

2.3.3 连接到以太网

SBC3000 Pro 具有一个主控板（MCU），提供 8 个 GE 网口，分别是 GE0 到 GE7，默认使用 GE0 与千兆以太网相连接，然后登录 SBC3000 Pro 设备。

默认通过 GE0 连接网络，对 SBC3000 Pro 设备进行管理。

2.3.4 故障排查

当设备连接到千兆以太网后，设备前面板相应的 SPEED 和 LINK 指示灯均不亮时，可确定为网络连接故障。网络连接故障的排查一般遵从以下步骤：

步骤 1：将网线从业务网口换到管理网口，观察管理网口指示灯是否正常；或者将网线从管理网口换到业务网口，观察业务网口指示灯是否正常；

步骤 2：如果指示灯正常，那么可以确定为业务网口或管理网口发生故障；如果指示灯依然不亮，将网线连接到便携机（笔记本电脑或固定计算机），并访问网络；

步骤 3：如果便携机（计算机）可以正常访问网络，则可判定 SBC3000 Pro 网络端口出现故障；

步骤 4：如果通讯正常，可以判定设备接入以太网的网线存在问题，须重新制作；如果通讯失败，那么请通知机房网络管理员，由网络管理员解决。

3 参数配置

3.1 登录

3.1.1 登录准备

SBC3000 Pro 的主控板有 8 个千兆以太网接口（GE0 到 GE7），其中 GE0 是管理网口，其他 GE 网口为业务网口，带宽默认自动适应。GE0 默认 IP 192.168.11.1，GE1 默认 IP 192.168.12.1，GE2 默认 IP 192.168.13.1，GE3 默认 IP 192.168.14.1，GE4 默认 IP 192.168.15.1，GE5 默认 IP 192.168.16.1，GE6 默认 IP 192.168.17.1，GE7 默认 IP 192.168.18.1。

将设备接到千兆交换机，绿色数据灯闪烁，橙色速率灯常亮；接百兆交换机，绿色数据灯闪烁，橙色速率灯不亮。初次使用设备时，直接找一条网线，将 PC 与 SBC3000 Pro 的 GE0 网口直接连接，点开 PC 的 Internet 协议（TCP/IP）属性界面中的“高级”，添加个 192.168.11.XXX 地址，使 PC 和设备处在同一网段，以便登录到设备的 Web 界面。

出厂时，只有通过 GE0 网口连接设备，其它网口都不能访问（被禁用）。如果需要通过其它网口登录设备，请先通过 GE0 网口进入 web，然后在 ***安全-->访问控制*** *里打开其它网口的访问权限，如果需要 ping 其它网口，需在* ***安全-->系统安全*** *里将外网 ping 请求响应开启。*

3.1.2 登录

在浏览器中用 https 方式输入 GE0 网口的默认 IP 地址，即 https:// 192.168.11.1:1081，接着在登录页面输入用户名和密码，默认的用户名是 admin，密码是 admin@123#。

SBC3000 Pro 设备不支持 http 连接，必须采用 https 连接才能登录设备的 Web 页面。

如果用户修改默认 IP 地址后忘记了新的 IP 地址而导致不能进入配置页面，请用串口线将 PC 和 SBC3000 Pro 设备的串口连接起来，进入 en 模式，输入 show interface 即可查看设备的 IP 地址。

图 3-1-1 登录界面

输入默认用户名、密码和随机生成的验证码后进入下面的配置页面。默认的用户名是 admin，密码是 admin@123#。为了确保系统安全，当你登录后，建议你及时更改密码。admin 账户修改密码的位置位于 Web 界面上“系统→用户管理→密码设置”，界面如下所示。

图 3-1-2 更改密码

设备 Web 界面正上方是主配置菜单栏，左侧是导航树，通过菜单栏和导航树，用户可以在右边的配置页面查看、更改和设置设备信息。

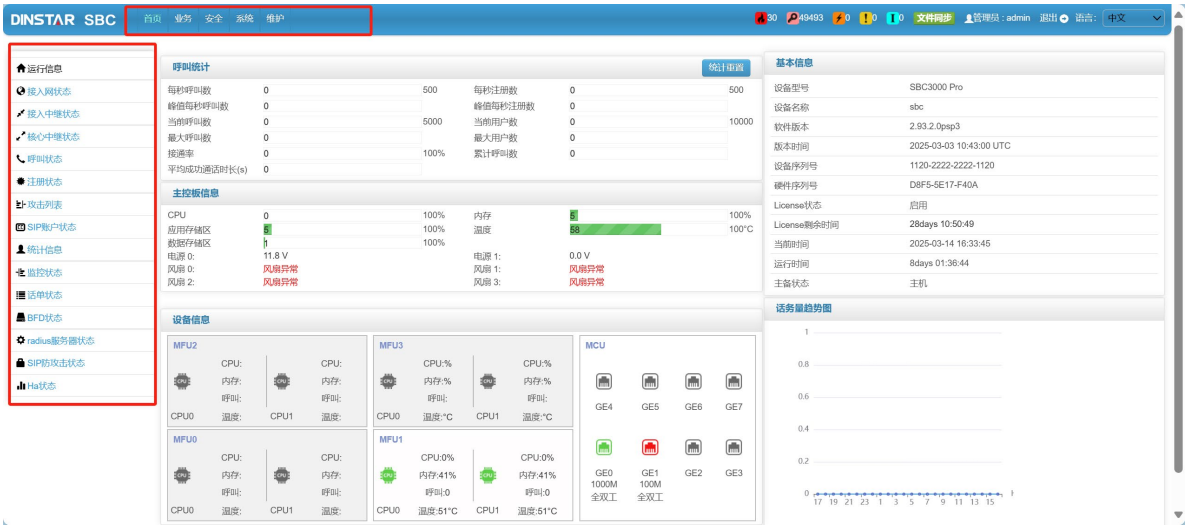


图 3-1-3 Web 首页

3.2 Web 界面结构和导航树

进入 Web 界面后首先显示的是运行信息。运行信息界面显示了设备的呼叫统计、主控板信息、设备信息、基本信息和话务量趋势图。

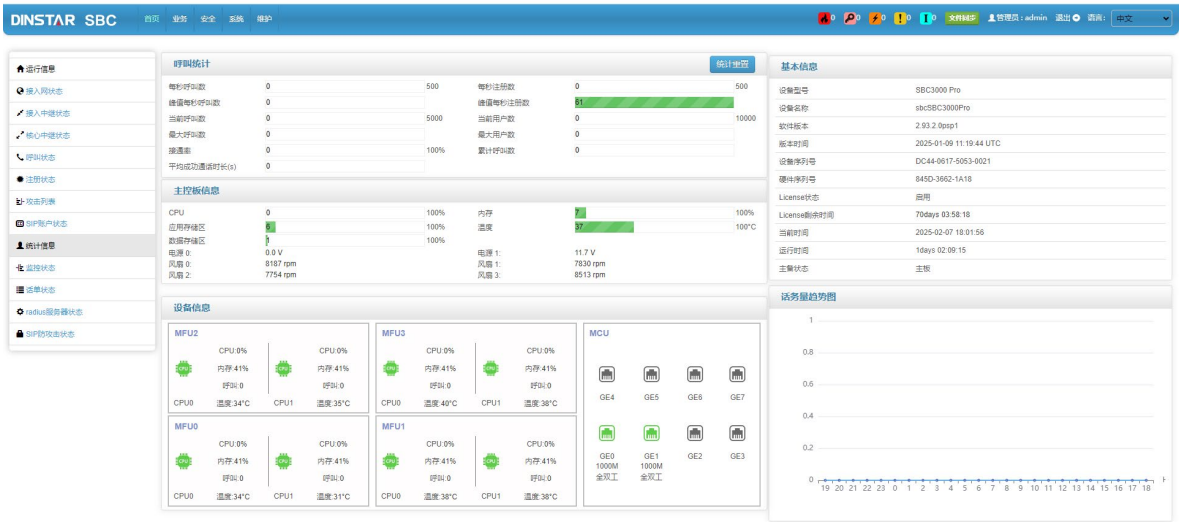


图 3-2-1 首页运行信息界面

界面的顶端左侧是公司 Logo，右侧是当前登录的账户和退出，登陆后的界面默认显示是中文界面。界面主体正上方是主菜单栏，左侧是导航树，右侧显示的是相应节点的具体内容。通过遍历菜单栏和导航树，可以在右侧配置界面完成对设备的查看、修改和配置。

Web 界面中，点击 + ADD 可以添加配置，点击 可以修改配置，点击 可以删除配置。

点击导航树可以查看导航树的分支，配置 SBC3000 Pro 正常的流程是如下图：

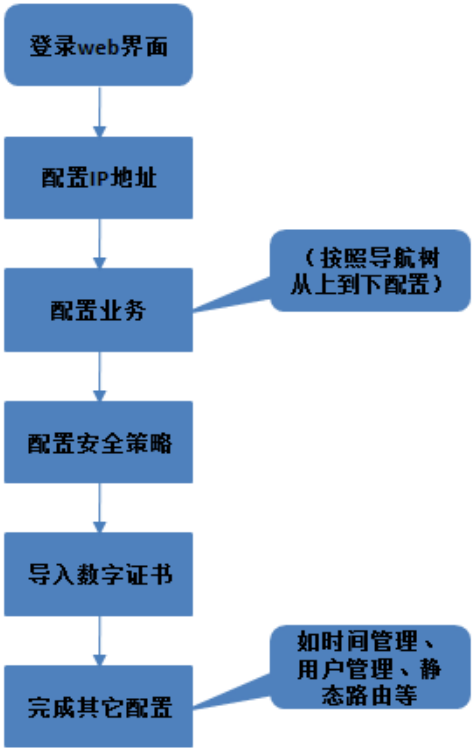


图 3-2-2 配置流程

3.3 首页

3.3.1 运行信息

打开菜单栏中首页，直接进入运行信息节点，可以查看设备的呼叫统计、主控板信息、设备信息、基本信息和话务量趋势图。

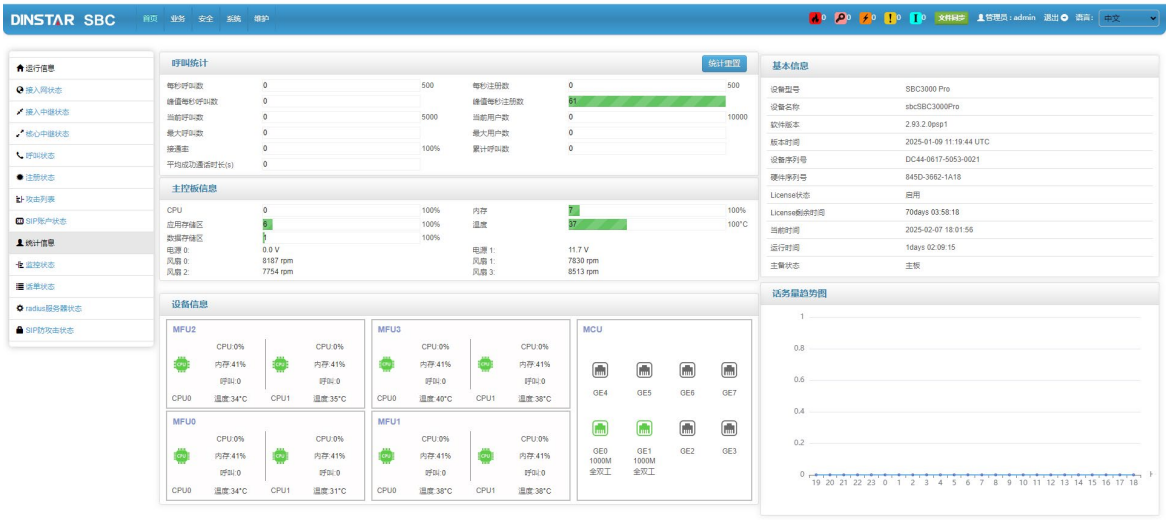


图 3-3-1 设备运行信息

表 3-3-1 呼叫统计的描述

参数	描述
每秒呼叫数	当前时间每秒新增的呼叫数
峰值每秒呼叫数	从系统启动运行到现在最大的每秒新增呼叫数
当前呼叫数	当前正在通话的呼叫数
最大呼叫数	从系统启动运行到现在最大呼叫数
接通率	从系统启动运行到现在呼叫成功次数除以全部合法呼叫请求数的百分比
平均成功通话时长	从系统启动运行到现在呼叫成功通话时长总和除以呼叫成功数
每秒注册数	当前时间点每秒新增的注册请求数
峰值每秒注册数	从系统启动运行到现在最大的每秒新增注册请求数
当前用户数	当前注册成功并在线的用户总数
最大用户数	从系统启动运行到现在最大用户数
累计呼叫数	从系统启动运行到现在全部合法的呼叫请求数

表 3-3-2 主控板信息的描述

参数	描述
CPU	当前 CPU 占用率百分比
应用存储区	当前应用存储区占用率百分比
数据存储区	当前数据存储区占用率百分比
内存	当前内存占用率百分比
温度	当前正在使用的主控板 CPU 的温度
电源	当前电源输出值
风扇	当前风扇转数

表 3-3-3 设备信息说明

参数		描述
业务板	CPU	当前业务板的 CPU 占用率百分比
	内存	当前业务板的内存占用率百分比
	呼叫	当前业务板的 CPU 正在呼叫的呼叫数
	温度	当前业务板的 CPU 的温度
主控板	网口	主控板具有的网口，其中处于使用状态的网口是绿色，未使用的网口是灰色

表 3-3-4 基本信息说明

参数	描述
设备型号	该产品的设备型号为 SBC3000 Pro
设备名称	用户可在 Web 界面中“系统 → 系统设置”页面里修改设备名称
软件版本	当前产品运行的软件版本号

License 状态	在 License 授权期内显示“启用”，过期显示“启用，剩余时间为 0”
License 剩余时间	显示 License 授权剩余时间
当前时间	SBC3000 Pro 设备当前的系统时间，用户可以在“系统 → 时间管理”页面里调整时区或者同步浏览器时间
运行时间	系统本次启动后运行的时长

说明

NTP 时间同步，需要优先级高的网口能正确解析域名。

3.3.2 接入网状态

接入网用于终端用户向 SBC3000 Pro 设备注册，SBC3000 Pro 再将注册转发到 SIP 服务器，接入网状态总是显示为“true”。

图 3-3-2 设备运行信息

表 3-3-5 中继状态描述

参数	描述
名称	接入网的名称，名称一般为关键字，添加配置成功后不可修改
状态	接入网的状态总显示为“true”
每秒呼叫数	当前时间每秒新增的呼叫次数
当前用户数	通过该接入网成功注册并在有效期内的总用户数
接通率	系统运行开始到现在，该接入网的总接通率：（呼叫成功数/总合法呼叫数）*100%
当前转码数	当前接入网正在转码呼叫通话数

呼叫数	当前接入网正在转发呼叫通话数
累计呼叫	系统运行开始到现在的总合法呼叫数

说明

1. 接通率中，呼叫成功数的判断标准为 invite 消息的成功响应。

2. 接通率、当前转码数、呼叫数、累计呼叫有来源和目的两个方向，来源表示该呼叫从其他终端用户到该 SBC 设备，目的则表示呼叫从该 SBC 设备到其它终端用户。

3.3.3 接入中继状态

接入网中继通过 SIP Trunk 方式使终端设备对接到 SBC 设备。如果接入网中继未开启心跳和注册，中继状态都显示为“true”；如果接入网中继已开启注册，则以注册结果判断中继状态；如果已开启心跳策略，则以 option 响应的结果判断中继状态。

图 3-3-3 接入中继状态

表 3-3-6 接入中继状态描述

参数	描述
名称	接入网中继的名称，一般为关键字，添加配置成功后不可修改
状态	true：表示该接入网中继连接正常，false：则表示该接入网中继连接中断
每秒呼叫数	当前时间每秒新增的呼叫数
当前用户数	通过该中继成功接入 SBC 设备并在有效期内的总用户数
接通率	系统运行开始至现在，该中继的总接通率：（呼叫成功数/总合法呼叫数）*100
当前转码数	当前中继正在转码呼叫通话数

呼叫数	当前中继正在呼叫通话数
累计呼叫	系统运行开始到现在的总合法呼叫数

说明

1. 如果该接入网中继未开启心跳和注册，中继状态则都显示为 true；如果中继开启注册，则以注册结果判断中继状态；如果开启心跳策略，会以 option 响应的结果判断中继状态。

2. 接通率中，呼叫成功数的判断标准为 invite 消息的成功响应。

3. 接通率、当前转码数、呼叫数、累计呼叫有来源和目的两个方向，来源表示该呼叫从接入网的其他设备到该 SBC 设备，目的则表示呼叫从该 SBC 设备到接入网的其它设备。

3.3.4 核心中继状态

核心网中继通过 SIP Trunk 方式使核心网的设备对接到 SBC 设备。如果核心网中继未开启心跳和注册，中继状态都显示为“true”；如果核心网中继已开启注册，则以注册结果判断中继状态；如果已开启心跳策略，则以 option 响应的结果判断中继状态。

图 3-3-4 核心中继状态

表 3-3-7 核心中继状态描述

参数	描述
名称	核心网中继的名称，一般为关键字，添加配置成功后不可修改
状态	true：表示该核心网中继连接正常，false：则表示该核心网中继连接中断
每秒呼叫数	当前时间每秒新增的呼叫数
当前用户数	通过该中继成功接入 SBC 设备并在有效期内的总用户数

接通率	系统运行开始至现在，该中继的总接通率：（呼叫成功数/总合法呼叫数）*100
当前转码数	当前中继正在转码呼叫通话数
呼叫数	当前中继正在呼叫通话数
累计呼叫	系统运行开始到现在的总合法呼叫数

说明s

1. 如果该核心网中继未开启心跳和注册，中继状态则都显示为 true；如果中继开启注册，则以注册结果判断中继状态；如果开启心跳策略，会以 option 响应的结果判断中继状态。

2. 接通率中，呼叫成功数的判断标准为 invite 消息的成功响应。

3. 接通率、当前转码数、呼叫数、累计呼叫有来源和目的两个方向，来源表示该呼叫从核心网的其他设备到该 SBC 设备，目的则表示呼叫从该 SBC 设备到核心网的其它设备。

3.3.5 呼叫状态

呼叫页面显示的是当前通话的呼叫的状态以及该呼叫的主叫、被叫和通话时长信息。

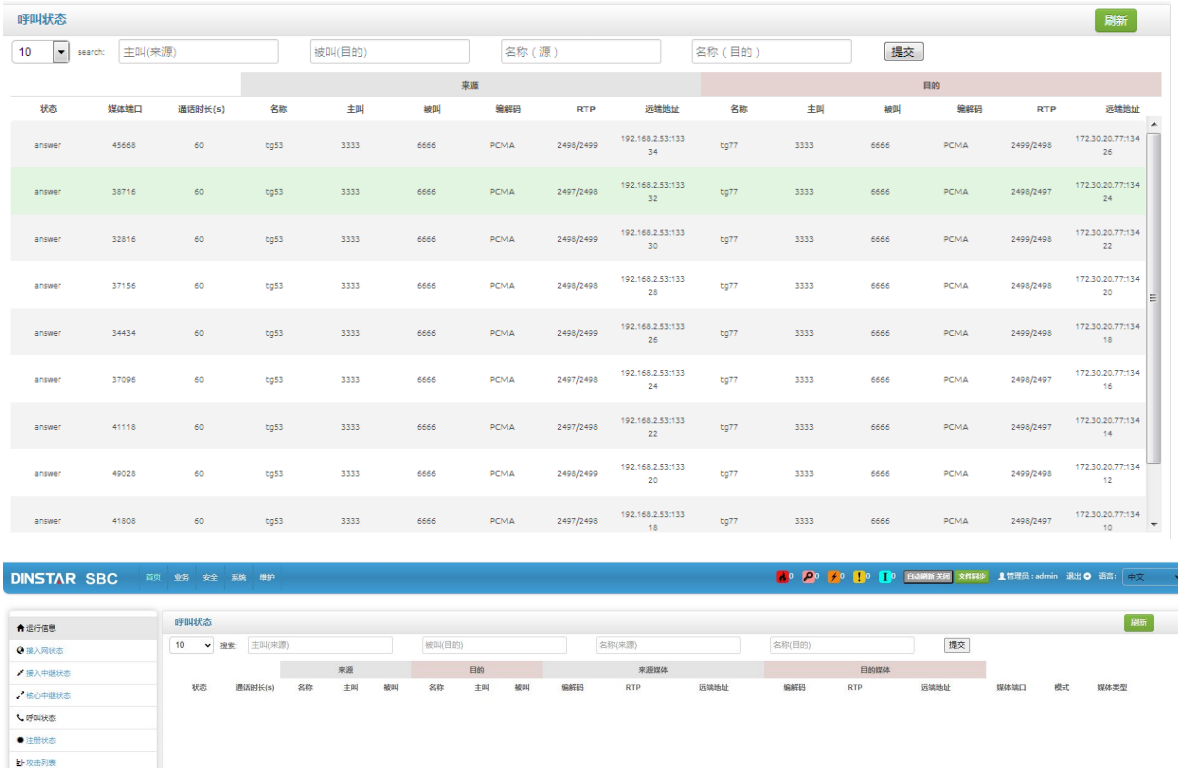


图 3-3-5 呼叫状态

表 3-3-8 呼叫状态描述：

参数	描述
状态	Init：收到 invite 请求，刚开始初始化该呼叫的控制块的状态； Outgoing：选路成功，发起呼出呼叫，等待响应； Early：接收到 18x 响应； Completed：接收到 2xx 响应，等待 ack； Answer：接收到 ack，呼叫建立成功
通话时长(S)	该呼叫建立成功到现在的时长，以秒为单位显示
名称	该呼叫通过接入中继、核心中继或接入网的名称
主叫	该呼叫的主叫号码
被叫	该呼叫的被叫号码
编解码	该通话采用的编解码，如果是转码，来源和目的地编解码会不一致
RTP	该通话接收/发送的 rtp 报文数，5 秒统计一次
远端地址	该通话 rtp 媒体的远端地址和端口
媒体端口	该通话的本地 rtp 端口，如果显示为 0，表示该 rtp 尚未建立成功
模式	转发或者转码
媒体类型	audio

3.3.6 注册状态

注册状态页面显示的是终端设备向 SBC 设备注册的状态。

图 3-3-6 注册状态

表 3-3-9 注册状态描述

参数	描述
状态	registering：接收到终端设备发出的注册请求，正在处理 registered：接收到注册成功响应，并在注册有效期内
用户名	终端设备注册时使用的用户名
名称	来源名称表示该注册是通过哪个接入网注册的；目的名称表示该注册是向哪个核心网中继注册的
注册周期	来源注册间隔表示终端设备注册到 SBC 的 Expire 时间，目的注册间隔表示 SBC 向核心中继注册的 Expire 时间
地址/NAT 地址	对端设备的地址和 NAT 地址
协议	注册所使用的协议类型（UDP/TCP/TLS/WSS）

3.3.7 攻击列表

攻击列表页面显示的攻击 SBC 设备的攻击来源、IP 地址和端口等。

图 3-3-7 攻击列表

表 3-3-10 攻击列表描述

参数	描述
攻击来源	攻击的来源，包含 DDoS/DoS
IP 地址（端口）	攻击来源的 IP 地址，或被攻击的目的端口
接口	被攻击的 SBC 设备的网口（如 GE1）
攻击流量	当攻击流量达到“安全 → 防攻击策略”页面设置的触发流量最大阈值，则设置的动作会被执行
动作	记录日志：该策略生效时，只记录该事件日志，不做其它处理 流量限制：该策略生效时，对该远端 IP 或设置的本地端口做流量限制，在限制时间内超

	过流量的报文全部丢弃 包速率限制：该策略生效时，对该远端 IP 或设置的本地端口做包速率限制，在限制时间内超过的报文全部丢弃 丢弃：该策略生效时，对该远端 IP 或设置的本地端口收到的报文，在限制时间内全部丢弃
限制时间	对发出攻击的 IP 执行所设置动作的时间

3.3.8 SIP 账户状态

SIP 账户状态页面显示 SBC 注册到 SIP 服务器的 SIP 账户的注册状态。可以设置条件进行筛选。

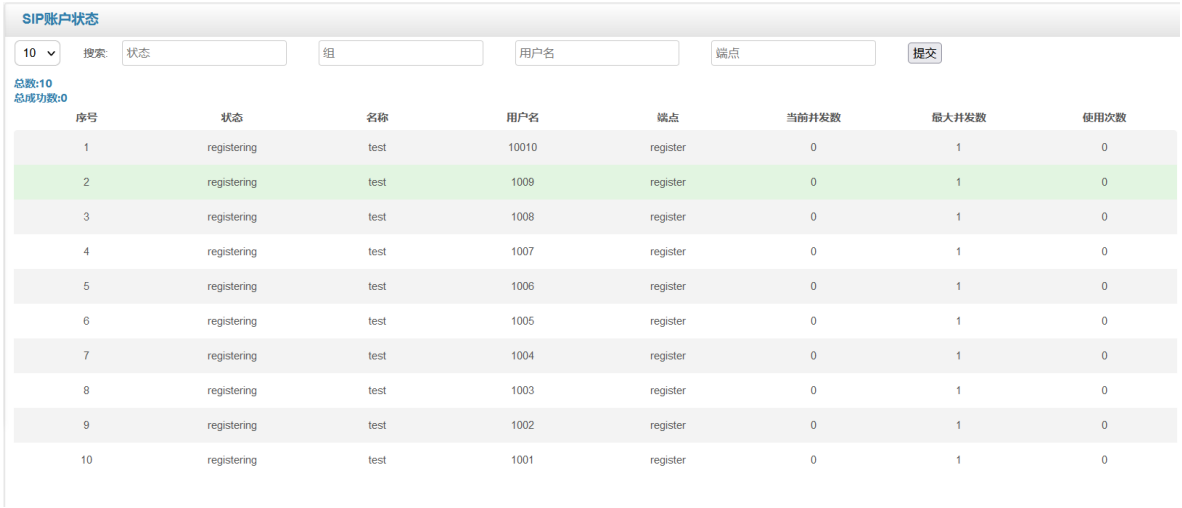


图 3-3-8 SIP 账户状态

表 3-3-11 SIP 账户状态描述

参数	描述
状态	Registering：设备发出的注册请求，正在处理 registered：接收到注册成功响应，并在注册有效期内
名称	SIP 账户用户组的名称
用户名	SIP 账户中用于向软交换注册的用户名
端点	SIP 账户绑定的中继名称
当前并发数	表示当前用户注册的并发数
最大并发数	表示当前用户注册的最大并发数
使用次数	表示当前用户被使用次数，如呼叫次数

3.3.9 统计信息

流量

展示当前以及历史网口、端点的接收/发送数据量。

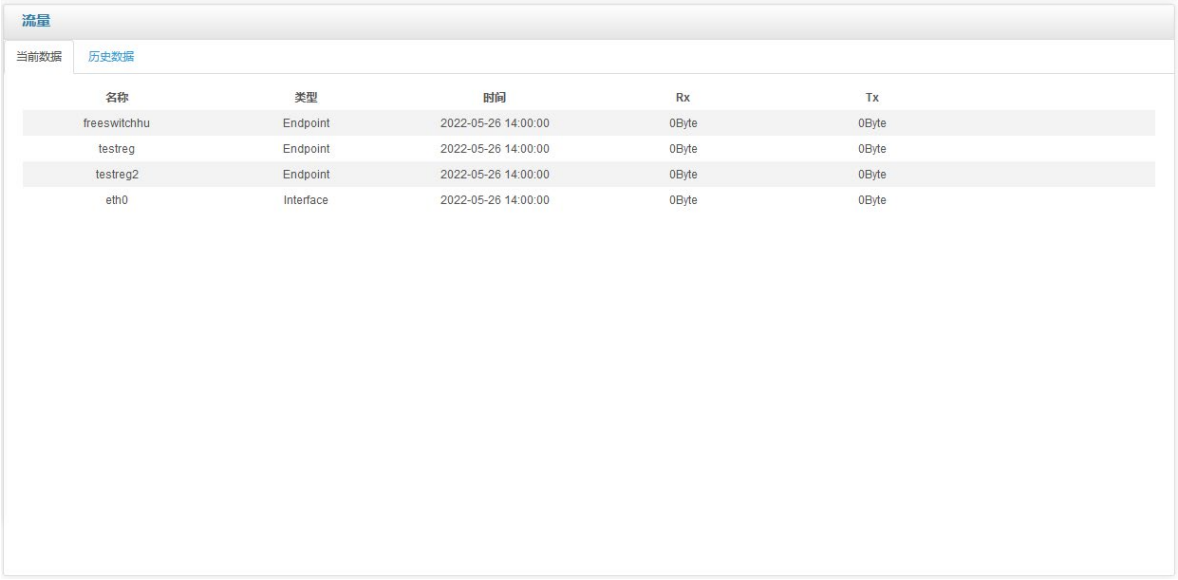


图 3-3-9 流量-当前数据

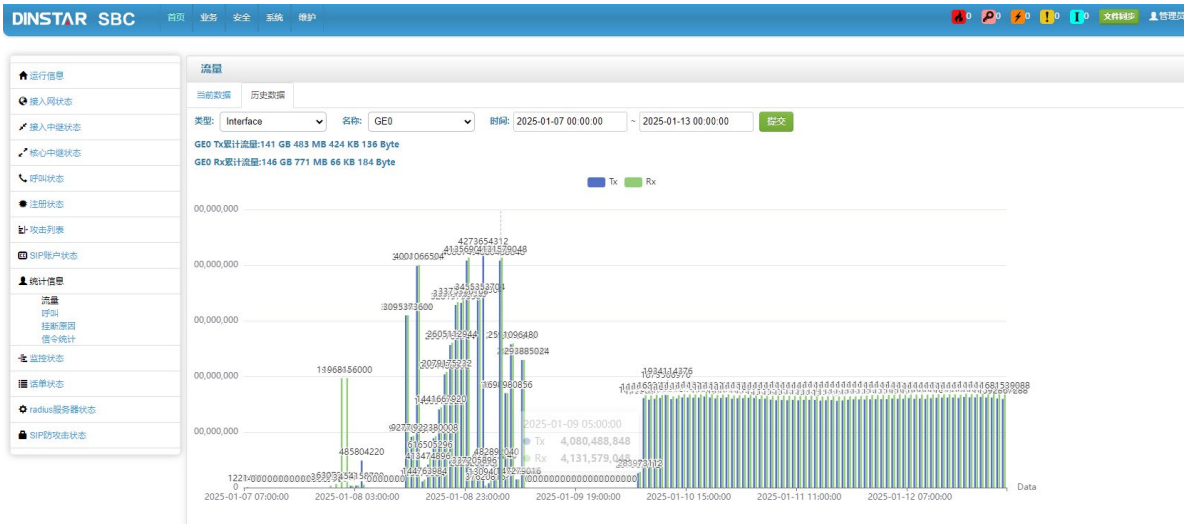


图 3-3-10 流量-历史数据

呼叫

展示一定时间段内系统成功的呼叫数量。

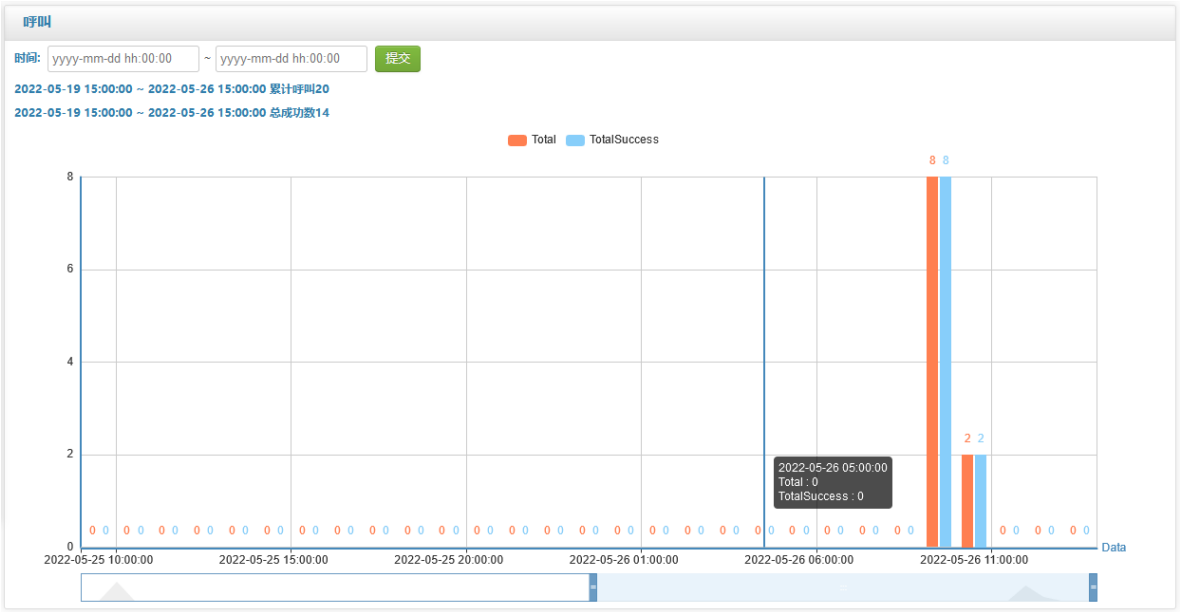


图 3-3-11 呼叫

挂断原因

展示系统启动后所有成功呼叫的挂断原因统计。

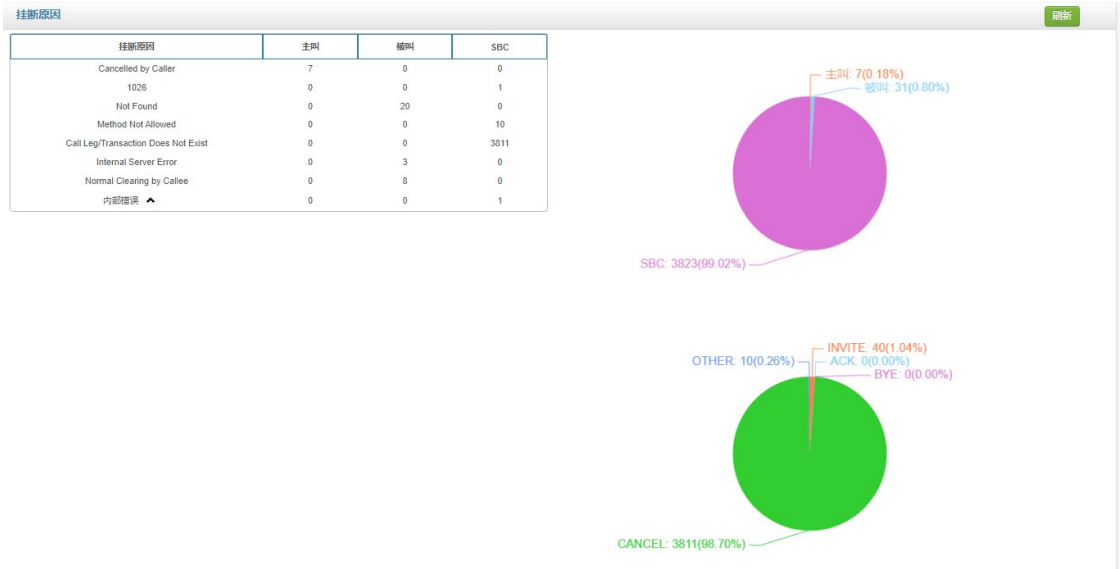


图 3-3-12 挂断原因

信令统计

展示系统运行后接收和发送的信令统计分析数据。

状态	接收请求	响应码	发送响应
ACK	19		
BYE	10	200	10
INVITE	19	100	19
		180	5
		183	5
		200	14
		407	6
NOTIFY	16	200	3
		503	1
REGISTER	65	200	60
		401	3
SUBSCRIBE	1	202	1

状态	发送请求	响应码	接收响应
ACK	20		
BYE	11	200	10
INVITE	19	100	18
		180	5
		183	5
		200	14
		407	6
NOTIFY	5	200	3
REGISTER	66	200	60
		401	3
SUBSCRIBE	1	202	1

图 3-3-13 信令统计

3.3.10 监控状态

监控状态页面显示通话的质量和网络质量参数，如抖动、丢包率、时延等信息。支持设置条件进行搜索。

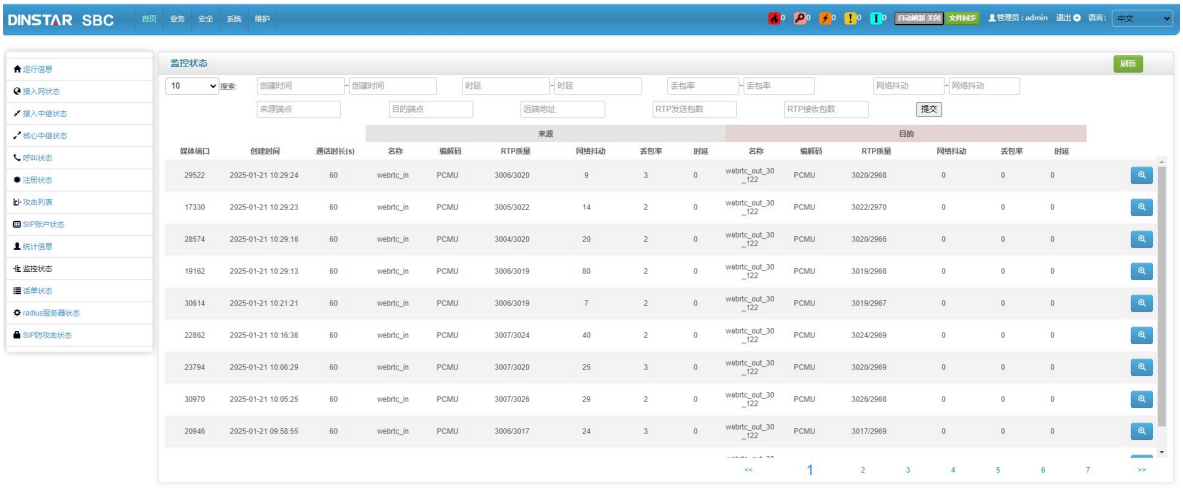


图 3-3-14 监控状态

表 3-3-11 监控状态描述

参数	描述
媒体端口	该端口为配置质量监控时的媒体地址所处的端口

创建时间	该监控状态记录创建的时间，一般为通话结束时间
通话时长	该呼叫的通话时长
名称	通话建立所走的中继名称
编解码	通话建立成功后协商的编解码
RTP 质量	接受/发送 RTP 包数量
网络抖动	网络状态以及延迟影响到通话质量的参数，也就是延迟变化的程度
丢包率	网络状态发生变化时的丢失数据包数量占所发送数据组的比率
时延	报文或分组从一个网络的一端传送到另一个端所需要的时间

3.3.11 话单状态

在话单管理中开启话单之后，可在话单状态页面查看系统所有通话的话单。可以设置条件对话单进行筛选。并且支持将所有话单导出到本地。

图 3-3-15 话单状态

表 3-3-12 话单状态描述

参数	描述
创建时间	话单创建的时间，一般为通话结束时间
通话时长	该呼叫的通话时长
名称	通话建立所走的中继名称
主叫	通话的主叫号码

被叫	通话的被叫号码
编解码	通话建立成功后协商成功的编解码
RTP	接受/发送 RTP 包数量

3.3.12 BFD 状态

双机热备配置 BFD 检测后，该页面展示 BFD 链路的状态。

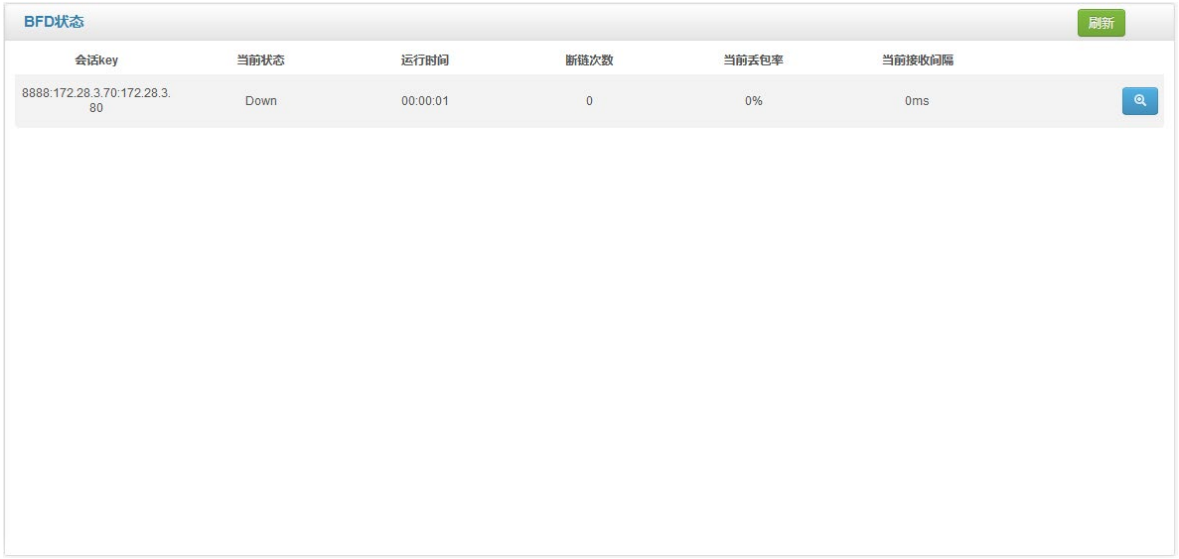


图 3-3-16 BFD 状态

表 3-3-13 BFD 状态描述

参数	描述
会话 Key	BFD 检测的会话 key
当前状态	BFD 当前状态
运行时间	BFD 配置生效后到当前累计运行时间
断链次数	BFD 正常后累计断链次数
当前丢包率	当前 BFD 链路的丢包率
当前接收间隔	当前接收数据的间隔

3.3.13 Radius 服务器状态

Radius 服务器状态页面显示设备和 radius 服务器之间的通信状态和话单统计等信息。

图 3-3-17 Radius 服务器状态

表 3-3-14 Radius 服务器状态描述

参数	描述
服务器 IP	Radius 服务器的 IP 地址
远端计费端口	Radius 服务器计费端口
状态	Radius 服务器状态，正常还是故障
成功发送话单数量	往 radius 服务器成功发送话单的数量

3.3.14 SIP 防攻击状态

显示按照 SIP 防攻击策略被限制的对象及到期时间。

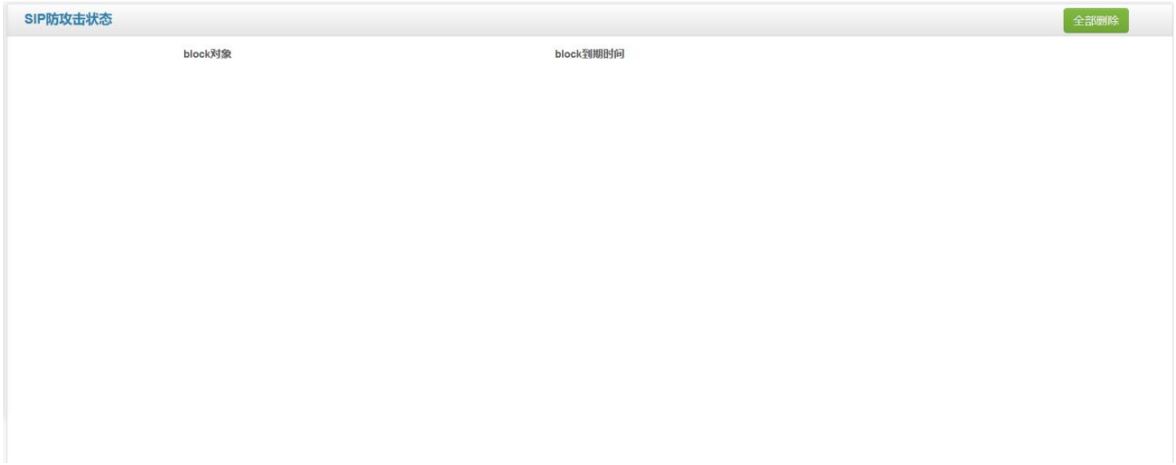


图 3-3-18 SIP 防攻击状态

表 3-3-15 SIP 防攻击状态描述

参数	描述
Block 对象	按照 SIP 防攻击策略被限制的 IP、SIP 账户、中继等
Block 到期时间	按照 SIP 防攻击策略 block 对象的解封时间

3.3.15 Ha 状态

该页面展示 SBC 的 Ha 状态。

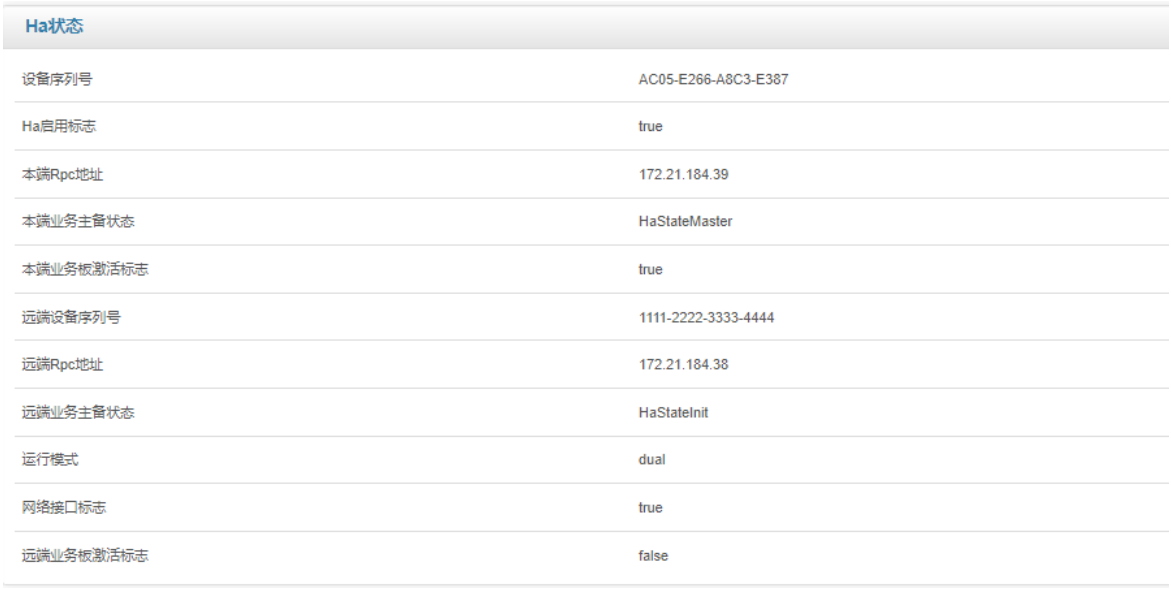


图 3-3-19 Ha 状态

表 3-3-16 Ha 状态描述

参数	描述
设备序列号	双机热备模式下本机设备序列号
Ha 启用标志	启用双机热备时显示标识
本端 Rpc 地址	本端设备的管理口 ip 地址，根据双机热备的具体配置显示
本端业务主备状态	本端设备为主机还是备机状态（HaStateSlave：备机；HaStateMaster：主机）
本端业务板激活标志	本端设备业务板激活标志，dsp 激活了显示为 true，未激活显示 false

远端设备序列号	双机热备模式下远端设备的序列号
远端 Rpc 地址	远端设备的管理口 ip 地址，根据双机热备的具体配置显示
远端业务主备状态	远端设备为主机还是备机状态（HaStateSlave：备机；HaStateMaster：主机）
运行模式	是否处于双机热备模式，dual 标志表示主备双机模式，disable 表示单机模式
网络接口标志	主备通信的网络接口的状态
远端业务板激活标志	远端设备业务板激活标志，dsp 激活了显示为 true，未激活显示 false

3.4 业务

3.4.1 传输端点

传输端点用于配置 SBC 与其他设备 SIP 信令交互的各种参数。

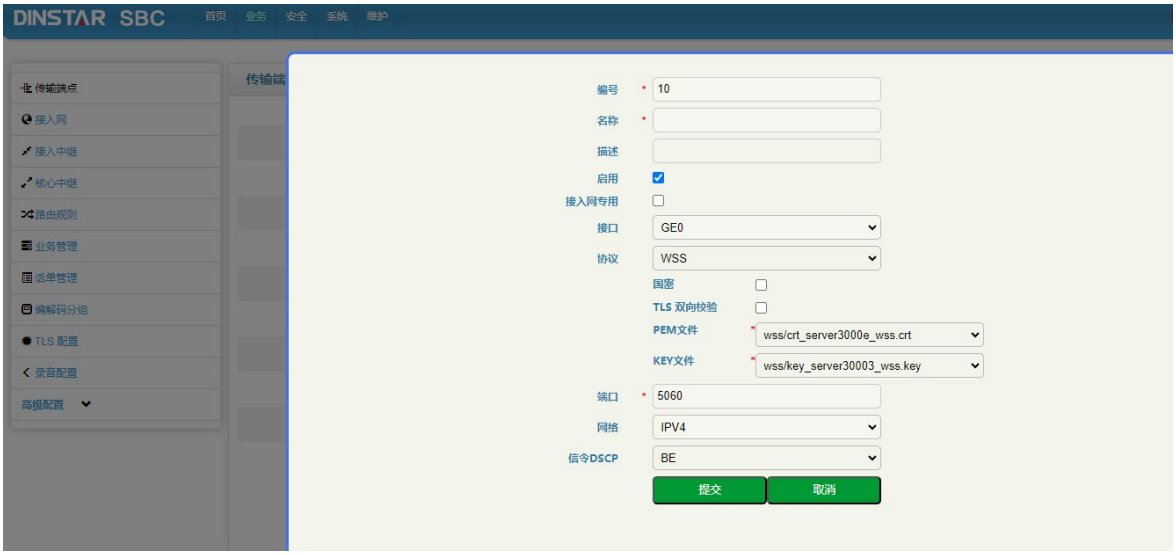


图 3-4-1 传输端点页面图

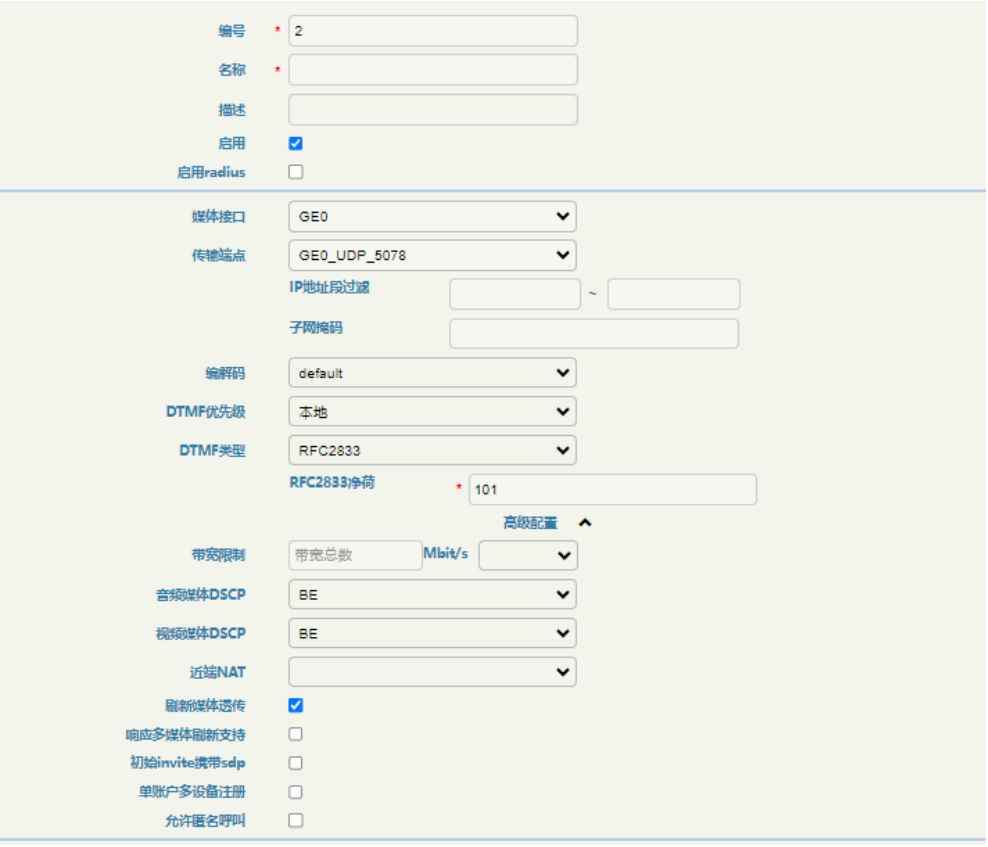
表 3-4-1 传输端点

参数	描述
编号	传输端点编号，可修改，但不可重复
名称	配置传输端点的名字，用户自定义，添加成功后不可修改

描述	该传输端点的描述，用户可以较为详细描述该传输端点的作用和规则
启用	选项默认勾选，去勾选时该条传输端点为禁用状态
接入网专用	默认不勾选，用于接入中继或者核心中继，勾选则表示该传输端点用于接入网
接口	SBC 接收/发送数据的网络接口或者 VLAN 接口
协议	采用的传输协议:UDP/TCP/TLS/WSS
端口	在配置的接口上的 SIP 监听端口，端口号在该接口上唯一
网络	配置采用的是 IPV4 还是 IPV6 网络，默认为 IPV4
信令 DSCP	设置 SIP 信令的 DSCP，DSCP 是为了保证通信的 QoS，在数据包 IP 头部的 8 个标识字节进行编码，来划分服务类别，区分服务的优先级。默认 DSCP 为 BE，总共有 14 种 DSCP

3.4.2 接入网

接入网用于配置外网终端（SIP 电话）通过 SBC 向软交换注册的接入域和各种参数。



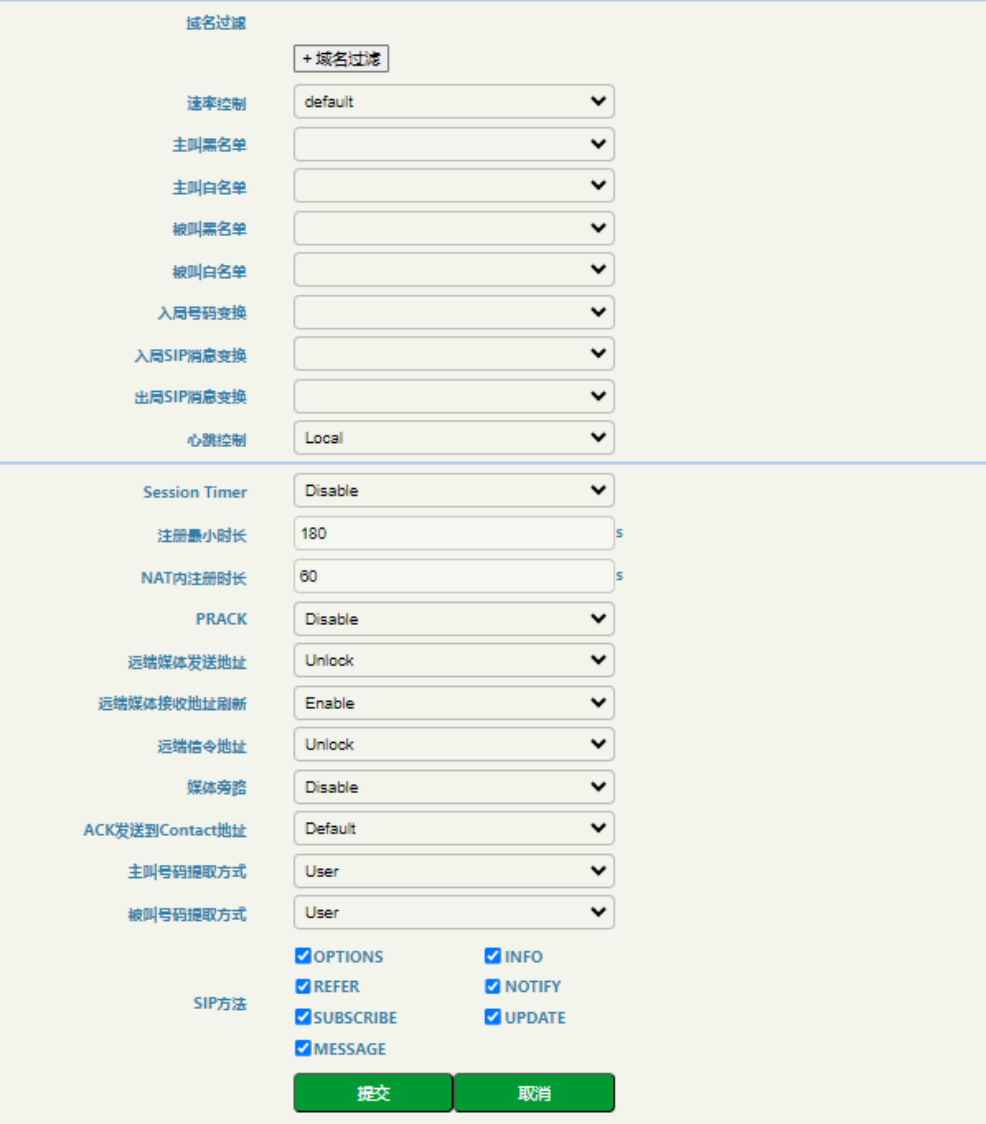


图 3-4-2 接入网页面

表 3-4-2 接入网

参数	描述
编号	配置接入网的编号，添加成功后可修改，但不可重复
名称	配置接入网的名字，用户自定义，添加成功后不可修改
描述	该接入网的描述，用户可以较为详细描述该接入网的作用和规则
启用	选项默认勾选，去勾选时该条接入网为禁用状态
启用 radius	默认关闭，勾选则表示启用 radius 服务器发送话单

媒体接口	接入网接收/发送媒体的网络接口或者 VLAN 接口
传输端点	选择接入网 SIP 信令交互的网络接口，已在传输端点界面配置好了
IP 地址过滤	配置接收 SIP 请求的合法来源 IP 地址范围
子网掩码	IP 地址范围的子网掩码
编解码	配置从该接入网呼入或呼出支持的编解码格式，参考 3.4.8 编解码分组
DTMF 优先级	DTMF 优先本地还是远端
DTMF 类型	DTMF 有 RFC2833/SIP INFO/Inband 三种发送模式，系统可根据配置选择对应的发送模式，一通电话如果 SBC 两侧的 dtmf 方式不一致，会通过 DSP 转换
带宽限制	在该条接入网最大带宽，单位为 Mbit/s
音频媒体 DSCP	设置音频媒体的 DSCP。默认 DSCP 为 BE，总共有 14 种 DSCP
视频媒体 DSCP	设置视频媒体的 DSCP。默认 DSCP 为 BE，总共有 14 种 DSCP
近端 NAT	近端 nat：设备在 nat 内部，在信令中需要带上 nat 的地址和对应的端口，默认不启用，在这里，启用时默认只需要配置对应防火墙出口 IP 地址即可，如果防火墙做了对应的端口变换，则需根据端口变换规则配置对应的 SIP 端口或 RTP 起始端口
刷新媒体透传	透传带 SDP 的会话刷新 reinvite 和 update 消息
响应多媒体刷新支持	当收到的 200 ok 的 SDP 中编解码大于一种时，将 SBC 协商的最终编解码以 reinvite 的形式发送给对端
初始 invite 携带 sdp	SBC 发送的初始 invite 携带 sdp
单账户多设备注册	默认不勾选，一个账户只允许一台终端注册；勾选，单账户支持多个终端同时注册
允许匿名呼叫	默认不勾选，不允许匿名呼叫；勾选，允许终端匿名呼叫
ssrc 变更同步	默认不勾选，勾选后当对端 RTP 的 ssrc 发生变更时，SBC 转发 RTP 的 ssrc 同步发生变更
域名过滤	只接收配置的域名的注册请求，支持正则配置
速率控制	配置该接入网每秒最大注册、呼叫量和总呼叫量，参考 速率控制。
主/被叫黑名单	配置不允许从该接入网呼入时主/被叫号码黑名单，如果接入网配置了黑名单，在黑名单内的主/被叫号码都不能通过该接入网呼入，参考 黑白名单。

主/被叫白名单	配置允许从该接入网呼入时主/被叫号码白名单，如果接入网配置了白名单，只有白名单内的主/被叫号码才能通过该接入网呼入，参考 黑白名单。
入局号码变换	配置从该接入网呼入时的号码变换规则（仅呼入，从该中继呼出该规则不生效），参考 号码变换。
入局 sip 消息变换	即从该接入网呼入时的 SIP 头域修改，参考 SIP 头域修改。
出局 sip 消息变换	即从该接入网呼出时的 SIP 头域修改，参考 SIP 头域修改。
心跳控制	默认配置为 local，表示 SBC 直接响应收到的 option 消息；配置为 Passthrough 时，SBC 将收到的 option 消息转发到远端地址，待收到远端地址的响应的 200ok 后转发 200ok。
Session Timer	会话定时器，是种会话保存激活的机制，如果启用，SBC 会在会话周期内发送 reinvite 报文保持会话激活，如果在会话周期内未检测到该消息，则认为会话已经终止，系统会主动拆除该会话。如果采用的是 require 模式，通过该接入网呼出时，必须要求被叫也支持 timer。
注册最小时长	终端注册的允许的最小时长，如果终端注册 REGISTER 报文中 expires 值小于这个值，SBC 可能会拒绝该注册请求。
NAT 内注册时长	SBC 如果发现终端在 NAT 下，则 SBC 响应的注册时长会自动变为该值，NAT 内注册时长值一般比较小，以免 NAT 地址发生变化时 SBC 不能及时发现。
PARCK	临时性响应的确认消息，用于确认收到了可靠的临时性响应。默认为关闭状态。
远端媒体发送地址	启用远端媒体地址锁定：当远端设备在公网时，那么锁定的就是 sdp 中的媒体地址；在私网时，就是动态锁定，要连续收到 30 个报文后就锁定该报文的原地址。
远端媒体接收地址刷新	和远端媒体发送地址配合使用，当远端媒体发送地址为 unlock 时，启用远端媒体接收地址刷新，当对端的媒体地址更新后，SBC 会向更新后的媒体地址发送媒体
远端信令地址	启用信令锁定：账户注册成功后，只接收该账户的主叫注册时同样地址来的呼叫报文。
媒体旁路	开启后同一 NAT 下的终端的 RTP 不经过 SBC 转发。
ACK 发送到 Contact 地址	默认配置 default，回复 ACK 到发送 200OK 的来源地址；配置为 Top Priority，回复 ACK 到 Contact 中的地址。
主叫号码提取方式	user：提取 invite 报文 from 域中 user 字段作为主叫 display name：提取 invite 报文 from 域中 display 字段作为主叫

被叫号码提取方式	user:提取 invite 报文 to 域中 user 字段作为被叫 display name：提取 invite 报文 to 域中 display 字段作为被叫 request-uri：提取 invite 报文 request-uri 的号码作为被叫
SIP 方法	配置该接入网允许接收的 SIP 请求方法，如果未启用对应的 SIP 请求方法，系统收到对应的 SIP 请求时，会直接拒绝。INVITE/REGISTER 和拆除会话请求默认都允许。

说明：

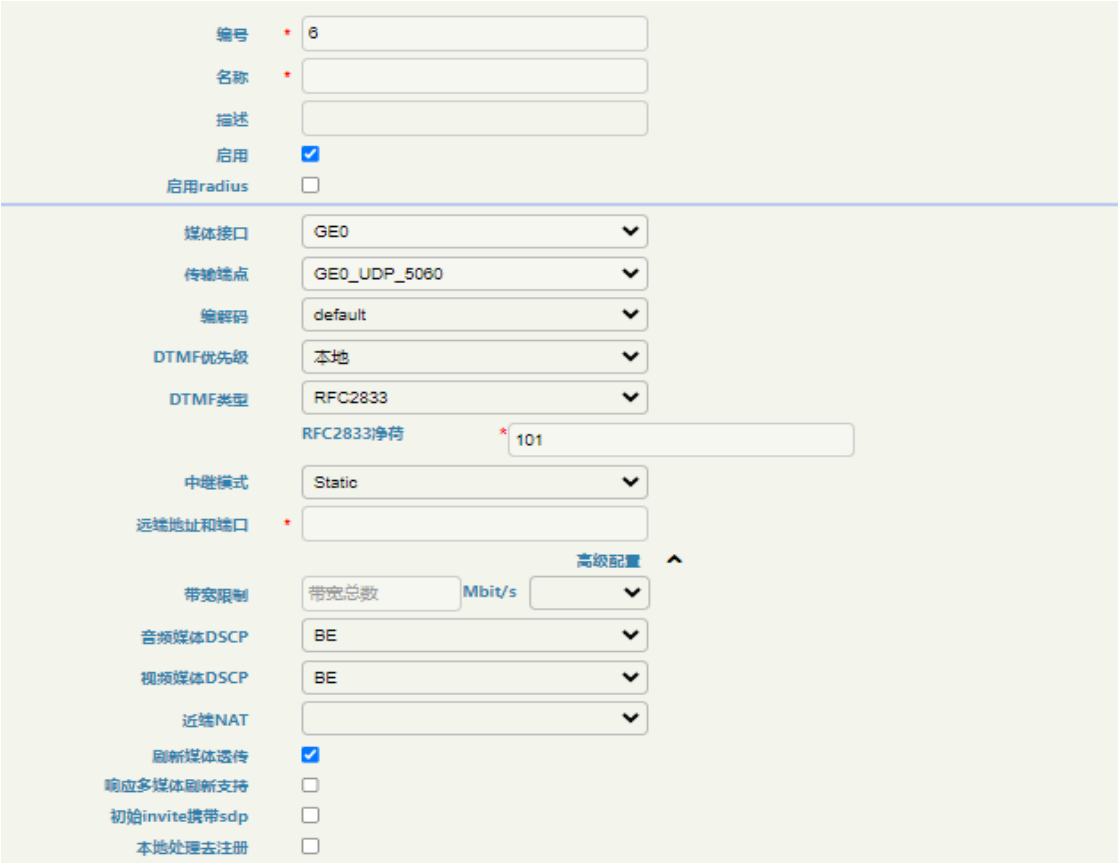
配置静态 NAT 时，默认 SIP 和 RTP 起始端口为空即可，如果防火墙做了对应的端口映射，则需要根据映射规则进行配置（举个例子）：

1. SIP 端口：一条中继本地端口为 5061，但防火墙将公网的 5061 端口映射成 8888，则在静态 NAT 的 SIP 端口配置为 8888；

2. RTP 起始端口：SBC 默认的 RTP 起始端口为 16384，如果防火墙将 16384-50000 端口映射为 12768-30000，在静态 NAT 的 RTP 起始端口配置为 12768，也就是以 16384 为基准，根据防火墙端口映射规则进行基准偏移。

3.4.3 接入中继

配置 SBC 系统环境支持外网 SIP/IMS 中继通过 SBC 对接到接入网终端的服务器和相关参数。



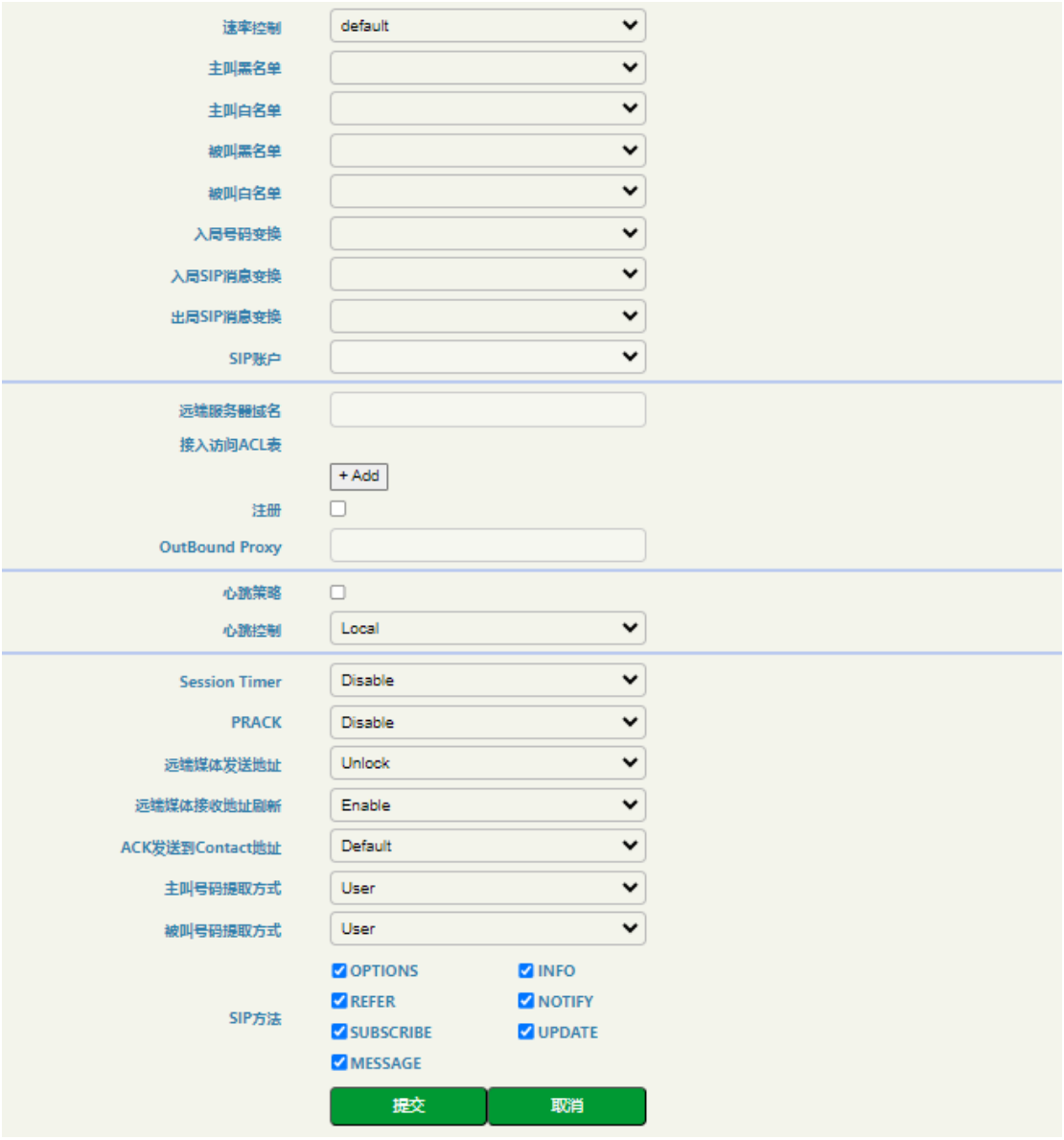


图 3-4-3 接入中继页面

表 3-4-3 接入中继

参数	描述
编号	配置接入网的编号，添加成功后可修改，但不可重复
名称	配置接入中继的名字，用户自定义，添加成功后不可修改。
描述	该接入中继的描述，用户可以较为详细描述该接入中继的作用和规则。
启用	选项默认勾选，去勾选时该条接入中继为禁用状态。
启用 radius	默认关闭，勾选则表示启用 radius 服务器发送话单。

媒体接口	该接入中继接收/发送媒体的网络接口或者 VLAN 接口。
传输端点	选择中继 SIP 信令交互的网络接口，已在传输端点界面配置好了
编解码	配置从该接入中继呼入或呼出支持的编解码格式，请参考 3.4.8 编解码分组。
DTMF 优先级	DTMF 优先本地还是远端。
DTMF 类型	DTMF 有 RFC2833/SIP INFO/Inband 三种发送模式，系统可根据配置选择对应的发送模式，一通电话如果 SBC 两侧的 dtmf 方式不一致，会通过 DSP 转换。
中继模式	默认为 static，模式为 static 时需要配置远端的地址和 ip；模式为 Dynamic 时，需要配置注册账户相关信息。
带宽限制	在该条中继的最大带宽，单位为 Mbit/s。
音频媒体 DSCP	设置音频媒体的 DSCP。默认 DSCP 为 BE，总共有 14 种 DSCP。
视频媒体 DSCP	设置视频媒体的 DSCP。默认 DSCP 为 BE，总共有 14 种 DSCP。
近端 NAT	近端 NAT：设备在 nat 内部，在信令中需要带上 NAT 的地址和对应的端口，默认不启用，在这里，启用时默认只需要配置对应防火墙出口 IP 地址即可，如果防火墙做了对应的端口变换，则需根据端口变换规则配置对应的 SIP 端口或 RTP 起始端口。
媒体刷新透传	透传带 SDP 的会话刷新 reinvite 和 update 消息。
响应多媒体刷新支持	当收到的 200 ok 的 SDP 中编解码大于一种时，将 SBC 协商的最终编解码以 reinvite 的形式发送给对端。
初始 invite 携带 sdp	SBC 发送的初始 invite 携带 sdp。
本地处理去注册	SBC 处理终端的去注册消息，不转发到服务器。
ssrc 变更同步	默认不勾选，勾选后当对端 RTP 的 ssrc 发生变更时，SBC 转发 RTP 的 ssrc 同步发生变更
速率控制	配置该接入网每秒最大注册、呼叫量和总呼叫量，参考 速率控制。
主/被叫黑名单	配置不允许从该接入网呼入时主/被叫号码黑名单，如果接入网配置了黑名单，在黑名单内的主/被叫号码都不能通过该接入网呼入，参考 黑白名单。
主/被叫白名单	配置允许从该接入网呼入时主/被叫号码白名单，如果接入网配置了白名单，只有白名单内的主/被叫号码才能通过该接入网呼入，参考 黑白名单。

入局号码变换	配置从该接入网呼入时的号码变换规则（仅呼入，从该中继呼出该规则不生效），参考 3.4.14 号码变换。
入局 sip 消息变换	即从该中继呼入时的 SIP 头域修改，参考 SIP 头域修改。
出局 sip 消息变换	即从该中继呼出时的 SIP 头域修改，参考 SIP 头域修改。
SIP 账户	配置 SBC 向服务器注册的 SIP 账户信息，参考 SIP 账户
远端服务器域名	配置远端服务器的域名。
接入访问 ACL 表	允许接入访问的 IP 地址和端口表，支持正则表达式。
注册	配置 SBC 作为客户端向 SIP 服务器注册的账户信息，包括用户名、认证 ID、密码、注册间隔、超时系数等信息。
OutBound Proxy	配置接入中继的代理服务器地址。
心跳策略	配置 SBC 向接入中继远端发送心跳的策略信息，包括心跳超时次数、心跳间隔以及是否仅检测 200 OK。
心跳控制	默认配置为 local，表示 SBC 直接响应收到的 option 消息；配置为 Passthrough 时，SBC 将收到的 option 消息转发到远端地址，待收到远端地址的响应的 200ok 后转发 200ok。
Session Timer	会话定时器，是种会话保存激活的机制，如果启用，SBC 会在会话周期内发送 reinvite 报文保持会话激活，如果在会话周期内未检测到该消息，则认为会话已经终止，系统会主动拆除该会话。如果采用的是 require 模式，通过该接入网呼出时，必须要求被叫也支持 Session Timer。需要配置会话超时时长、会话超时最小时长。
PARCK	临时性响应的确认消息，用于确认收到了可靠的临时性响应。默认为关闭。
远端媒体发送地址	默认为 unlock。配置为 lock 启用远端媒体地址锁定：当远端设备在公网时，那么锁定的就是 sdp 中的媒体地址；在私网时，就是动态锁定，要连续收到 30 个报文后就锁定该报文的原地址。配置为 staticlock 远端媒体地址为 SDP 中的媒体地址。
远端媒体接收地址刷新	和远端媒体发送地址配合使用，当远端媒体发送地址为 unlock 时，启用远端媒体接收地址刷新，当对端的媒体地址更新后，SBC 会向更新后的媒体地址发送媒体。
ACK 发送到 Contact 地址	默认配置 default,回复 ACK 到发送 200OK 的来源地址；配置为 Top Priority,回复 ACK 到 Contact 中的地址。

主叫号码提取方式	user:提取 invite 报文 from 域中 user 字段作为主叫 display name：提取 invite 报文 from 域中 display 字段作为主叫
被叫号码提取方式	user:提取 invite 报文 to 域中 user 字段作为被叫 display name：提取 invite 报文 to 域中 display 字段作为被叫 request-uri：提取 invite 报文 request-uri 的号码作为被叫
SIP 方法	配置该中继允许接收的 SIP 请求方法，如果未启用对应的 SIP 请求方法，系统收到对应的 SIP 请求时，会直接拒绝。INVITE/REGISTER 和拆除会话请求默认都允许。

3.4.4 核心中继

配置 SBC 系统环境通过此中继对接到核心网（内网）的 SIP/IPPBX 服务器和相关参数。

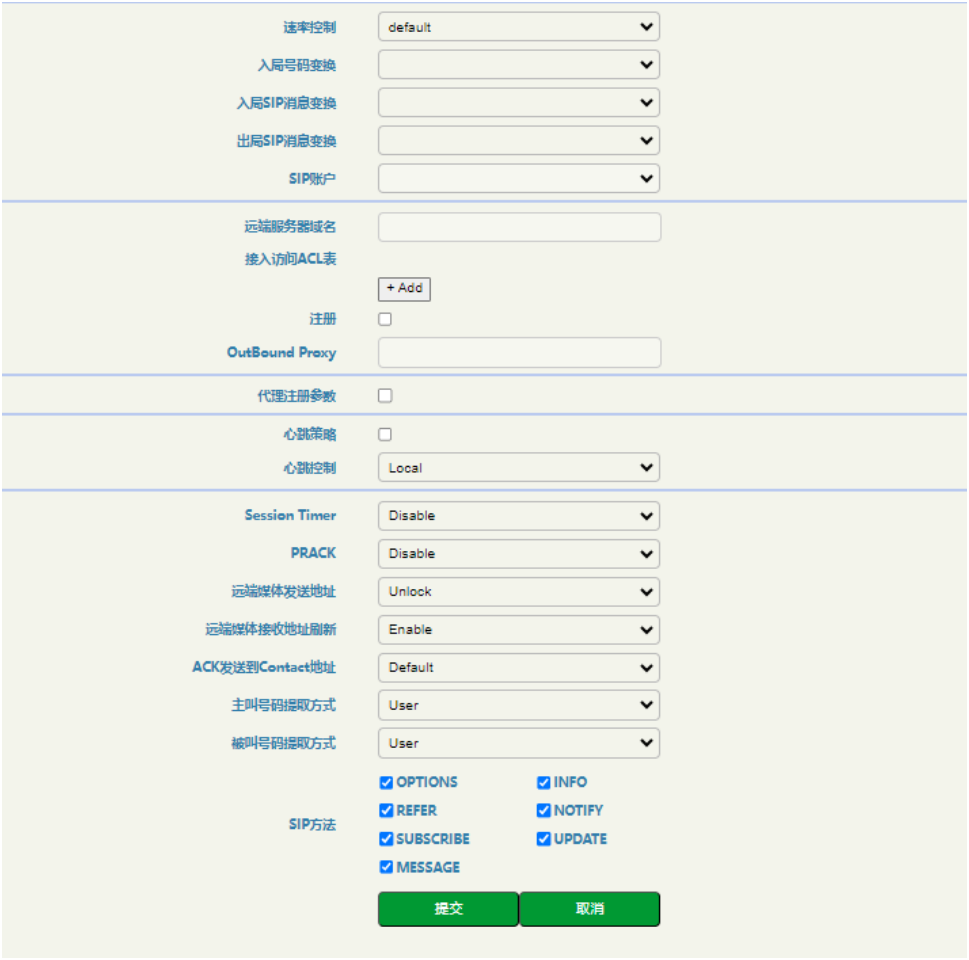


图 3-4-4 核心中继页面

表 3-4-4 核心中继

参数	描述
编号	配置接入网的编号，添加成功后可修改，但不可重复
名称	配置接入中继的名字，用户自定义，添加成功后不可修改。
描述	该接入中继的描述，用户可以较为详细描述该接入中继的作用和规则。
启用	选项默认勾选，去勾选时该条接入中继为禁用状态。
启用 radius	默认关闭，勾选则表示启用 radius 服务器发送话单。
媒体接口	该核心中继接收/发送媒体的网络接口或者 VLAN 接口。
传输端点	选择中继 SIP 信令交互的网络接口，已在传输端点界面配置好了

编解码	配置从该接入中继呼入或呼出支持的编解码格式，请参考 3.4.8 编解码分组。
DTMF 优先级	DTMF 优先本地还是远端。
DTMF 类型	DTMF 有 RFC2833/SIP INFO/Inband 三种发送模式，系统可根据配置选择对应的发送模式，一通电话如果 SBC 两侧的 dtmf 方式不一致，会通过 DSP 转换。
中继模式	默认为 static，模式为 static 时需要配置远端的地址和 ip；模式为 Dynamic 时，需要配置注册账户相关信息。
带宽限制	在该条中继的最大带宽，单位为 Mbit/s。
音频媒体 DSCP	设置音频媒体的 DSCP。默认 DSCP 为 BE，总共有 14 种 DSCP。
视频媒体 DSCP	设置视频媒体的 DSCP。默认 DSCP 为 BE，总共有 14 种 DSCP。
近端 NAT	近端 NAT：设备在 nat 内部，在信令中需要带上 NAT 的地址和对应的端口，默认不启用，在这里，启用时默认只需要配置对应防火墙出口 IP 地址即可，如果防火墙做了对应的端口变换，则需根据端口变换规则配置对应的 SIP 端口或 RTP 起始端口。
媒体刷新透传	透传带 SDP 的会话刷新 reinvite 和 update 消息。
响应多媒体刷新支持	当收到的 200 ok 的 SDP 中编解码大于一种时，将 SBC 协商的最终编解码以 reinvite 的形式发送给对端。
初始 invite 携带 sdp	SBC 发送的初始 invite 携带 sdp。
本地处理去注册	SBC 处理终端的去注册消息，不转发到服务器。
ssrc 变更同步	默认不勾选，勾选后当对端 RTP 的 ssrc 发生变更时，SBC 转发 RTP 的 ssrc 同步发生变更
速率控制	配置该接入网每秒最大注册、呼叫量和总呼叫量，参考 速率控制。
主/被叫黑名单	配置不允许从该接入网呼入时主/被叫号码黑名单，如果接入网配置了黑名单，在黑名单内的主/被叫号码都不能通过该接入网呼入，参考 黑白名单。
主/被叫白名单	配置允许从该接入网呼入时主/被叫号码白名单，如果接入网配置了白名单，只有白名单内的主/被叫号码才能通过该接入网呼入，参考 黑白名单。
入局号码变换	配置从该接入网呼入时的号码变换规则（仅呼入，从该中继呼出该规则不生效），参考 号码变换。
入局 sip 消息变换	即从该中继呼入时的 SIP 头域修改，参考 SIP 头域修改。
出局 sip 消息变换	即从该中继呼出时的 SIP 头域修改，参考 SIP 头域修改。

SIP 账户	配置 SBC 向服务器注册的 SIP 账户信息，参考 SIP 账户
远端服务器域名	配置远端服务器的域名。
接入访问 ACL 表	允许接入访问的 IP 地址和端口表，支持正则表达式。
注册	配置 SBC 作为客户端向 SIP 服务器注册的账户信息，包括用户名、认证 ID、密码、注册间隔、超时系数等信息。
OutBound Proxy	配置接入中继的代理服务器地址。
代理注册参数	SBC 作为代理服务器时，终端通过 SBC 代理注册到 SIP 服务器时的代理注册参数，包括注册间隔和超时系数。
心跳策略	配置 SBC 向接入中继远端发送心跳的策略信息，包括心跳超时次数、心跳间隔以及是否仅检测 200 OK。
心跳控制	默认配置为 local，表示 SBC 直接响应收到的 option 消息；配置为 Passthrough 时，SBC 将收到的 option 消息转发到远端地址，待收到远端地址的响应的 200ok 后转发 200ok。
Session Timer	会话定时器，是种会话保存激活的机制，如果启用，SBC 会在会话周期内发送 reinvite 报文保持会话激活，如果在会话周期内未检测到该消息，则认为会话已经终止，系统会主动拆除该会话。如果采用的是 require 模式，通过该接入网呼出时，必须要求被叫也支持 Session Timer。需要配置会话超时时长、会话超时最小时长。
PARCK	临时性响应的确认消息，用于确认收到了可靠的临时性响应。默认为关闭。
远端媒体发送地址	默认为 Unlock。配置为 Lock 启用远端媒体地址锁定：当远端设备在公网时，那么锁定的就是 sdp 中的媒体地址；在私网时，就是动态锁定，要连续收到 30 个报文后就锁定该报文的原地址。配置为 StaticLock 远端媒体地址为 SDP 中的媒体地址。
远端媒体接收地址刷新	和远端媒体发送地址配合使用，当远端媒体发送地址为 unlock 时，启用远端媒体接收地址刷新，当对端的媒体地址更新后，SBC 会向更新后的媒体地址发送媒体。
ACK 发送到 Contact 地址	默认配置 default,回复 ACK 到发送 200OK 的来源地址；配置为 Top Priority,回复 ACK 到 Contact 中的地址。
主叫号码提取方式	user:提取 invite 报文 from 域中 user 字段作为主叫 display name：提取 invite 报文 from 域中 display 字段作为主叫
被叫号码提取方式	user:提取 invite 报文 to 域中 user 字段作为被叫 display name：提取 invite 报文 to 域中 display 字段作为被叫 request-uri：提取 invite 报文 request-uri 的号码作为被叫

SIP 方法	配置该中继允许接收的 SIP 请求方法，如果未启用对应的 SIP 请求方法，系统收到对应的 SIP 请求时，会直接拒绝。INVITE/REGISTER 和拆除会话请求默认都允许。

3.4.5 路由规则

中继组

中继组将接入中继或核心中继进行分组，让该中继组呼出时能够做主备或负载均衡。

图 3-4-5 中继组页面

表 3-4-5 中继组

参数	描述
名称	配置中继组的名字，用户自定义，添加成功后不可修改。
描述	该中继组的描述，用户可以较为详细描述该核心网的作用和规则
路由组类型	分为接入中继组和核心中继组。
组内选择方式	主备：中继组主备模式下，当第一个中继状态为 true 时，呼出只走主中继，其它情况才走下一个备用中继，直到可用中继或无可用中继为止；如果超过第一个中继并发数，继续呼出到第二个中继，依此类推。 负载均衡：呼出时根据负载均衡策略，按比重把呼叫送到对应中继上。
中继名称	接入中继或核心中继的名称
容量分配	对应中继的容量分配或者权重值

路由


优先级
1018
描述
启用
dtmf 协商
透传不带sdp的183
透传sdp
媒体payload值适配
Normal(2833&rtp)
条件
号码规则
主叫用户名
被叫用户名
时间规则
主叫SIP URL
被叫SIP URL
来源
接入网
注册代理的目的路由必须是核心中继或核心中继组
1<webrtc_in>
Del
SIP方法
Request URI
目的
接入网
1<webrtc_in>
号码变换
SIP头域透传
request-uri 用户名
to inManipulation user
request-uri 地址
remote address
to 用户名
to inManipulation user
to 地址
remote address
to 显示用户名
to display
from 用户名
from inManipulation user
from 地址
local address
from 显示用户名
from display
提交
取消

图 3-4-6 路由页面

表 3-4-6 路由

参数	描述
优先级	相同条件下，优先级数字越小，优先级越高；呼叫选择路由会从高优先级的路由开始匹配，一旦条件都匹配成功，呼叫就根据该路由进行呼叫，路由选择不支持二次选路。
描述	该优先级的描述，用户可以较为详细描述该优先级的作用和规则
启用	选项默认勾选，去勾选时该条路由为禁用状态
DTMF 协商	启用后对 DTMF 协商，否则不协商 DTMF
透传不带 sdp 的 183	默认勾选，启用后透传不带 sdp 的 183
透传 SDP	默认不勾选，勾选后 SBC 将收到的 SDP 只替换媒体地址和端口为 SBC 相应的 IP 和端口转发到另一端。
媒体 payload 值适配	配置 payload 值是否适配到 2833、rtp
号码规则	配置该路由匹配的主被叫号码前缀（参考号码规则），如果为空，则表示主叫/被叫号码任意
主叫用户名	主叫号码的匹配规则，如果为空，则表示主叫号码任意，支持正则表达式匹配
被叫用户名	被叫号码的匹配规则，如果为空，则表示被叫号码任意，支持正则表达式匹配
时间规则	本条路由规则生效的时间段（参考时间规则），如果时间配置为空，则表示该路由任意时间段都可以使用
主叫 SIP URL	配置请求报文中 from 域的 SIP URL 字段匹配规则，如果为空，则表示主叫 SIP URL 不限制
被叫 SIP URL	配置请求报文中 to 域的 SIP URL 字段匹配规则，如果为空，则表示被叫 SIP URL 不限制
来源	设置该路由的呼叫来源，选择来源类型以及具体的端点。
SIP 方法	该路由支持的 SIP 请求方法，如果为空，表示不限制
Request URI	设置该路由的请求 URI
回铃音来源	设置回铃音的来源，可以选择远端、本地或者自适应
目的	设置该路由的呼叫目的，选择目的类型以及具体的端点。

号码变换	通过该路由时是否启用号码变换规则（参考 号码变换），默认不启用，号码变换会在在路由选择后完成
SIP 头域透传	通过该路由时是否启用 SIP 头域透传规则（参考 SIP 头域透传），默认不启用，SIP 头域透传会在在路由选择后完成
request-uri 用户名	配置 request-uri 用户名的来源，即从配置的项中提取值填充到 request-uri 用户名
request-uri 地址	配置 request-uri 地址的来源，即从配置的项中提取值填充到 request-uri 地址
to 用户名	配置 to 用户名的来源，即从配置的项中提取值填充到 to 用户名
to 地址	配置 to 地址的来源，即从配置的项中提取值填充到 to 地址
to 显示用户名	配置 to 显示用户名的来源，即从配置的项中提取值填充到 to 显示用户名
from 用户名	配置 from 用户名的来源，即从配置的项中提取值填充到 from 用户名
from 地址	配置 from 地址的来源，即从配置的项中提取值填充到 from 地址
from 显示用户名	配置 from 显示用户名的来源，即从配置的项中提取值填充到 from 显示用户名

注意：

接入网、接入中继和核心中继配置中也支持号码变换，这些号码变换只针对该接入网或中继呼入时生效，并且在路由选择前生效。

3.4.6 业务管理

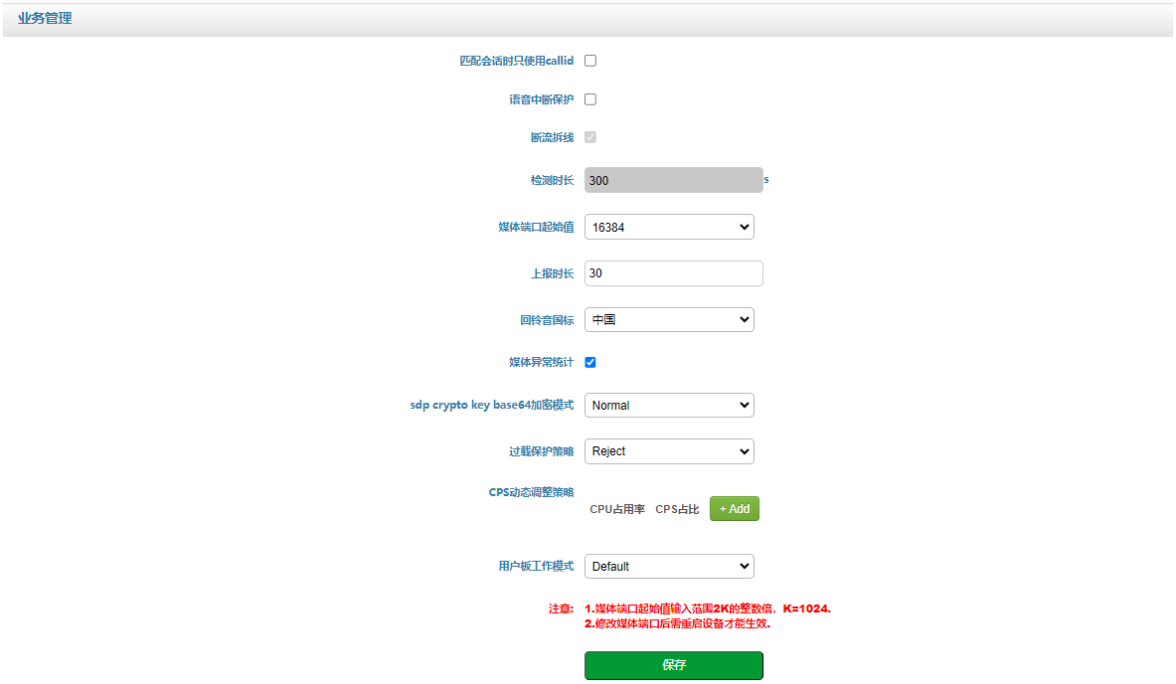


图 3-4-7 业务管理

表 3-4-7 业务管理

参数	描述
匹配会话时只使用 callid	启用后会话判断标准只匹配 call-id,from 和 to 的 tag 标签，不匹配主被叫号码
语音中断保护	语音单通或者双不通时拆除通话，需要配置断流拆线和检测时长
媒体端口起始值	SBC 的 RTP 媒体的起始端口，所有呼叫的媒体端口都大于该值，默认为 16384；媒体端口起始值可选择 8192、12288、16384、32768、49152。
上报时长	RTP 包统计的上报时长
回铃音国标	此选项允许用户设置回铃音的类型和标准。选择"中国"表示该系统将使用符合中国国家标准的回铃音配置
媒体异常统计	媒体异常时上报告警
sdp crypto key base64 加解密模式	配置的 sdp crypto key base64 加解密模式，normal 或者 padding

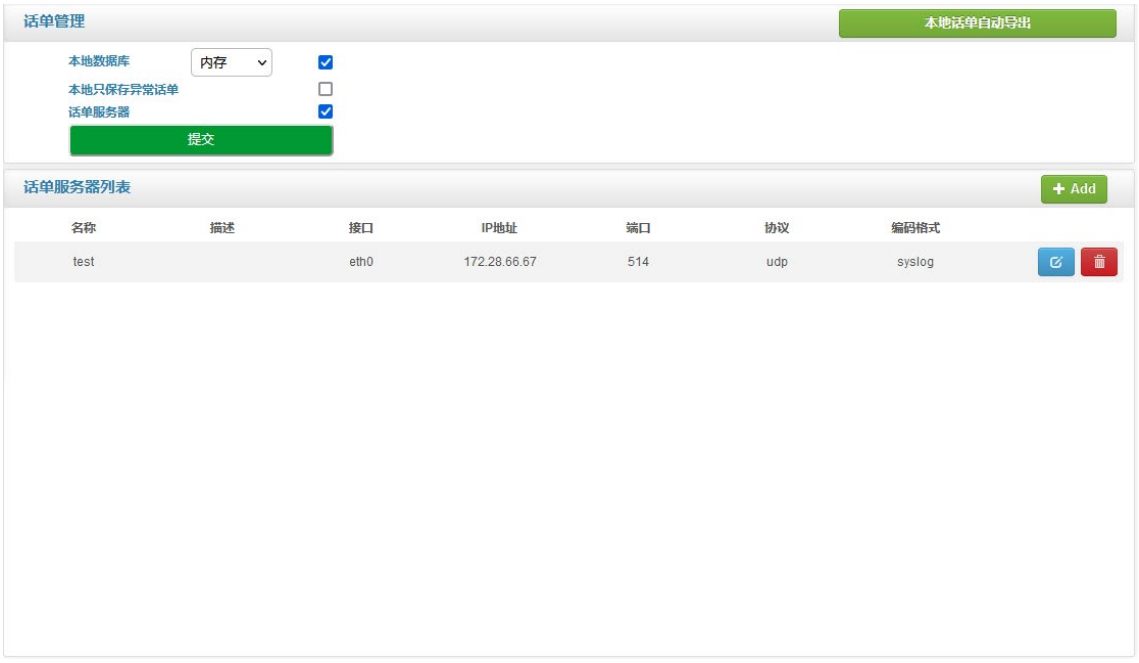
过载保护策略	系统的通话超过系统的承受能力时，再收到请求时的处理策略
CPS 动态调整策略	根据系统 CPU 调整系统的 CPS
用户板工作模式	默认配置 default，转码多，转发少，用户板使用前两个核转发；如果转码少，转发多，可配置 forwardding priority，表示使用前 4 个核转发。

3.4.7 话单管理

话单管理中本地数据库默认不勾选，不保存话单在本地数据库；勾选保存到内存，首页话单状态可以查看，重启设备后话单不清除；勾选保存到 flash，首页话单状态可以查看，重启设备后话单清除。

本地只保存异常话单默认不勾选，前提勾选了保存话单到本地数据库，所有话单都保存；勾选，只保存异常话单到本地数据库。

话单管理中的话单服务器默认不启用，需要启用后才能配置话单服务器。




名称 *
描述
接口 * GE0
编码格式 SYSLOG
IP地址 *
端口 * 514
协议 UDP
UDP是不安全的传输协议，请谨慎使用
属性名 描述 自定义 属性名 启用
SessionId 会话 Id
HangupStatus 错误码
HangupReason 挂断原因
HangupRole 挂断方
TalkTime 通话时间
CreateTime 创建会话时间
RingTime 振铃时间
AnswerTime 应答时间
HangupTime 挂断时间
呼入
InCaller 变换前主叫号码
InCallee 变换前被叫号码
OutCaller 变换后主叫号码
OutCallee 变换后被叫号码
IngressRealm 中继名称
IngressLocalAddr 信令本地IP
IngressMediaRemoteAddr 媒体远端IP

图 3-4-8 话单管理

表 3-4-8 话单服务器

参数	描述
名称	话单服务器名字，用户自定义，添加成功后不可修改
描述	话单服务器的描述，用户可以较为详细描述该服务器位置、作用、类型等
接口	和话单服务器交互的物理接口

编码格式	话单的编码格式，目前只支持 json 和 SYSLOG
IP 地址	话单服务器的 IP 地址
端口	话单服务器接收话单采用的端口
协议	传输话单采用的传输协，目前只支持 UDP
属性	话单的具体属性，勾选启用

图 3-4-9 本地话单自动导出

表 3-4-9 本地话单自动导出

参数	描述
定时导出	默认禁用，开启后，在设置时间点会自动导出话单
自动导出	默认禁用，开启后，会自动导出到备份服务器 URL
接口	话单导出的网络接口
协议	传输话单采用的协议，https
网络	采用的网络协议为 IPV4 还是 IPV6
用户名	备份服务器的用户名
密码	备份服务器的密码

备份服务器 URL	备份服务器的地址
话单格式	导出话单格式，默认为 txt 格式，有 csv 和 txt 两种格式

注意：

定时导出执行时间是以 SBC 的系统当前时间为参照。

备份服务器必须开启允许上传权限 。

3.4.8 编解码分组

SBC3000 Pro 系统支持 G.729、G.723、PCMU、PCMA、ILBC_13K、ILBC_15K、OPUS、OPUS_16K 和 AMR 以上几种编解码，用户可以根据需求将这几种编解码任意分组和调整优先级。

图 3-4-10 编解码分组

表 3-4-10 编解码分组

参数	描述
名称	编解码分组的名称，可自定义，添加成功后不可修改
描述	该编解码分组的描述，用户可以较为详细描述该编解码分组的作用和原因
最大打包时长	该编解码分组所有编解码支持的最大打包时长
编码名称	SBC3000 Pro 设备支持的编解码一共有以下几种： G.729、G.723、PCMU、PCMA、ILBC_13K、ILBC_15K、OPUS、OPUS_16K 和 AMR。

净荷值	每种编解码对应的 codec 值，不可修改
打包时长	每种编解码支持的默认打包时长，不可修改
禁用视频媒体	默认不勾选，勾选后不透传视频媒体
透传 MIME	默认不勾选，勾选后透传 MIME 结构的 sdp

注意：

名称为 default 的编解码分组为默认值，默认支持全部编解码，该条数据只可修改，不可删除。

3.4.9 TLS 配置

配置 TLS 协议的版本以及加密套件，只可修改默认配置，不能新增。

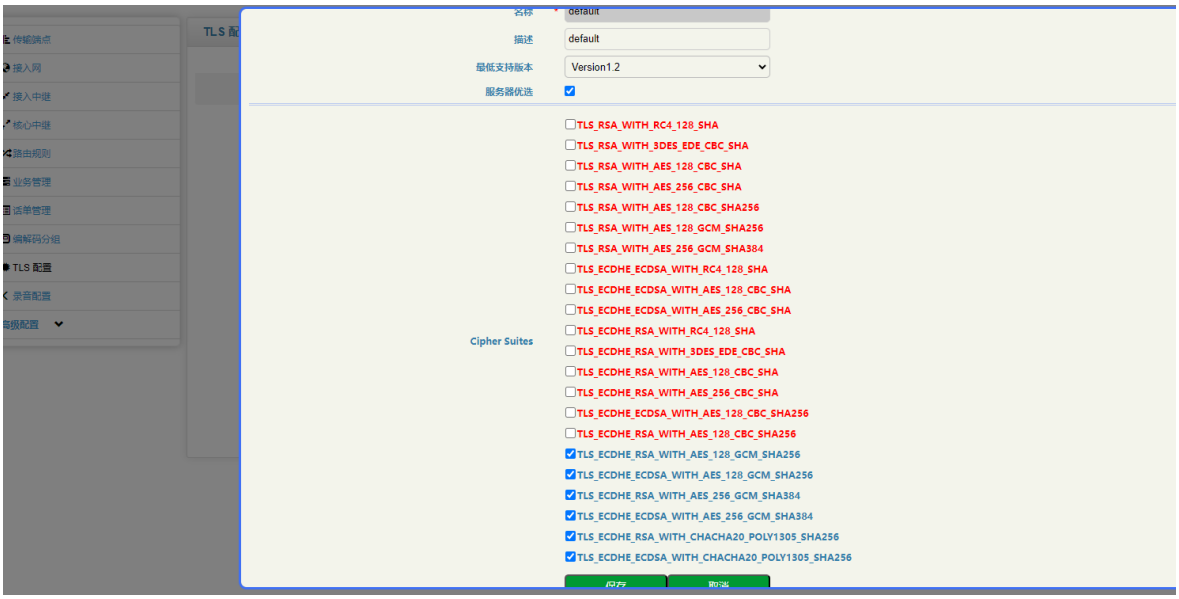


图 3-4-11 TLS 配置

表 3-4-11 TLS 配置

参数	描述
名称	TLS 配置的名称，默认 default，不可修改
描述	TLS 配置的描述，用户可以较为详细描述该 TLS 的作用
最低支持版本	设备支持的 TLS 协议的最低版本
服务器优选	勾选后优选服务器的 TLS 协议版本和加密套件

加密套件	勾选启用设备使用的加密套件

注意：

标红加密套件存在安全隐患，请谨慎使用。

3.4.10 主备

配置双机热备的相关参数、BFD 检测和主备切换条件等。

主备配置

配置主备机相关参数。

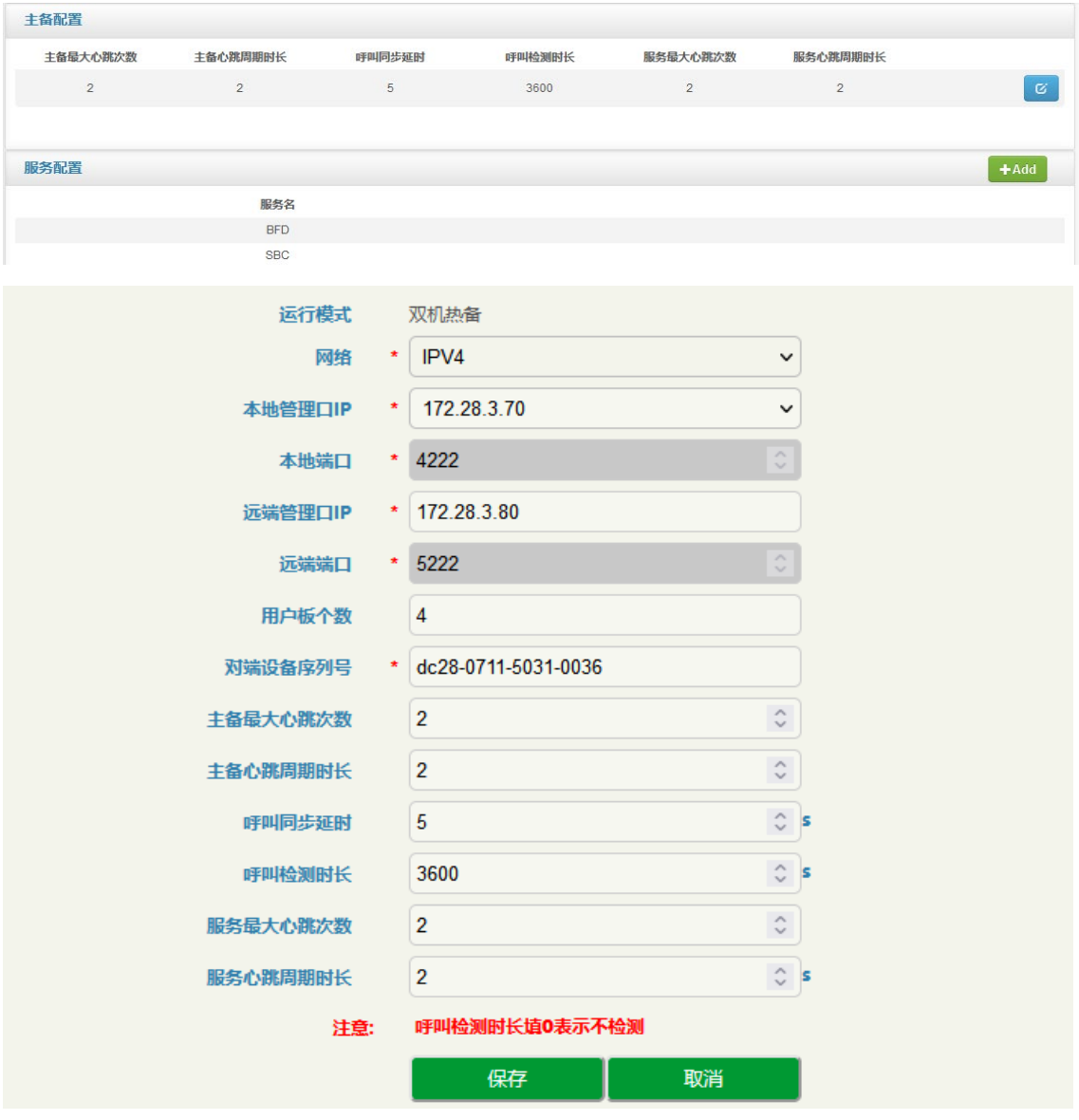


图 3-4-12 主备配置

表 3-4-12 主备配置

参数	描述
网络	采用的网络协议为 IPV4 还是 IPV6
本地管理口 IP	本机的管理口 IP 地址
本地端口	本机主备心跳检测和发送端口
远端管理口 IP	远端 SBC 的管理口 IP
远端端口	远端 SBC 主备心跳检测和发送端口
用户板个数	选择监测的用户板个数
对端设备序列号	远端 SBC 的设备序列号
主备最大心跳次数	主备检测的最大心跳次数
主备心跳周期时长	主备心跳发送的时间间隔
呼叫同步延时	主备呼叫同步的延时长度
呼叫检测时长	呼叫检测的时长，呼叫检测时长填 0 表示不检测
服务最大心跳次数	主备服务的最大心跳次数
服务心跳周期时长	主备服务的心跳发送时间间隔

BFD 检测

配置 BFD 检测的相关参数。

图 3-4-13 BFD 检测

表 3-4-13 BFD 检测

参数	描述
服务类型	业务服务类型或者主备服务类型，保存后不能修改
本地 IP 类型	选择 IP 地址类型，ipv4 或者 ipv6
本地 IP	选择 BFD 检测的本地 IP 地址
本地端口	配置 BFD 检测的本地端口
远端 IP 类型	选择远端 SBC 的 IP 地址类型，ipv4 或者 ipv6
远端地址	配置远端 SBC 的 IP 地址
远端端口	配置远端 SBC BFD 检测的端口
检查最大次数	BFD 检测的最大次数，超出后标识状态故障
最小发送周期	BFD 检测的最小发送时间间隔

期望最小接收周期	期望对端的 BFD 检测的最小发送时间间隔
ECHO 最小接收周期	ECHO 的最小接收时间间隔

注意：

BFD 主备配置会引起切换，必须保证主备机网络传输质量。

网络传输质量不高不许提高重传次数和重传间隔。

网口检测

选择网口检测的网口，选择后联动显示对应的 IP 地址等信息。

图 3-4-14 网口检测

切换规则

配置主备切换的规则，满足条件时主备机切换。

图 3-4-15 切换规则

表 3-4-14 切换规则

参数	描述
名称	选择已配置的网口检测
权重	配置该切换规则的权重，数值越大，权重越高

3.4.11 录音配置

siprec 配置

SBC3000 Pro 支持 siprec 服务器进行通话录音。

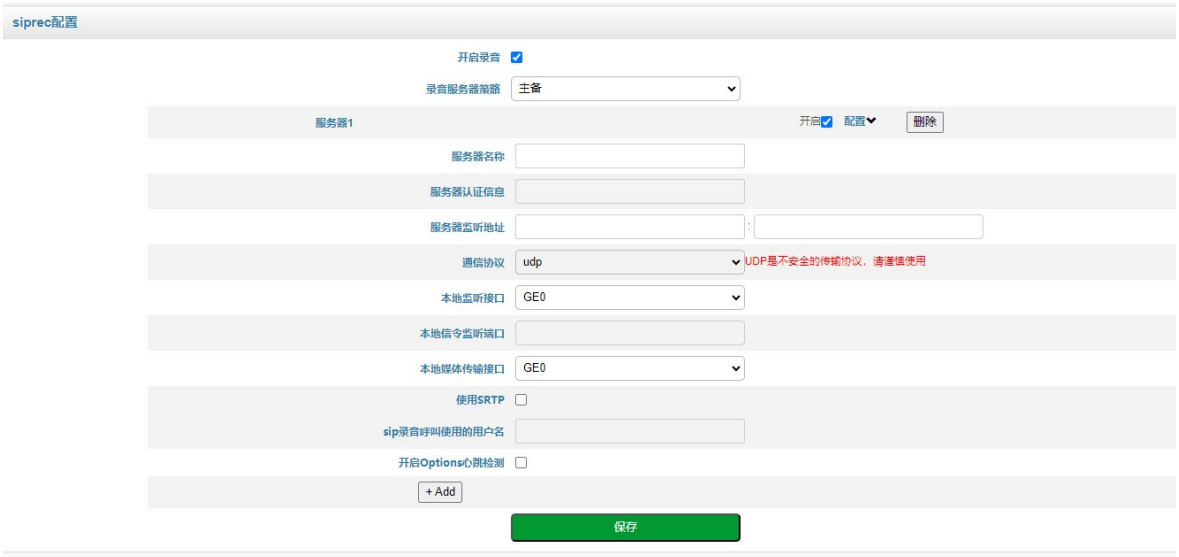


图 3-4-16 siprec 配置

表 3-4-15 siprec 配置

参数	描述
录音服务器策略	配置多个录音服务器时，服务器时使用策略，主备/负载均衡
服务器名称	配置服务器的名称，以便区分
服务器认证信息	服务器认证的秘钥
服务器监听地址	服务器的录音 IP
通信协议	和服务器交互的通信协议，暂时只支持 UDP

本地监听接口	SBC 设备信令监听的通信接口
本地信令监听端口	SBC 设备信令监听的端口
本地媒体传输接口	SBC 的录音媒体监听通信接口
使用 SRTP	默认不勾选，发送到录音服务器的媒体流不加密；勾选录音媒体流加密
权重值	只有负载均衡模式才有的参数，多个服务器时每个服务器的权重值
sip 录音呼叫使用的用户名	sip 录音呼叫使用的用户名
开启 option 心跳检测	开启后 SBC 定时向服务器发送心跳消息确认服务器是否在线或者和服务器的通信是否正常。需要配置心跳超时次数、心跳检测周期、只匹配 200 作为有效响应

3.4.12 号码规则

号码规则用于呼叫选择路由时主/被叫号码的前缀匹配。此处配置的号码规则不支持正则表达式。支持导入和导出配置。

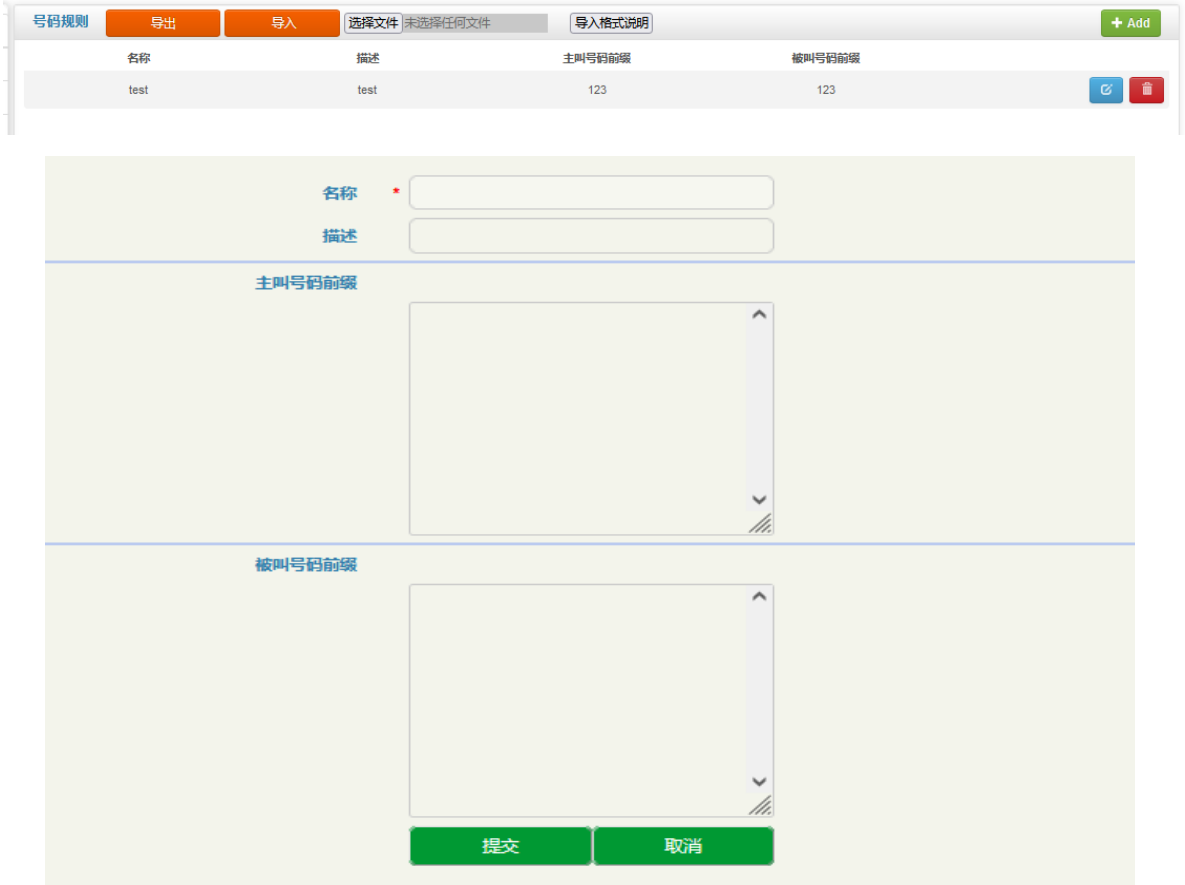


图 3-4-17 号码规则

表 3-4-16 号码规则

参数	描述
名称	号码规则的名称，用户自定义，添加成功后不可修改
描述	号码规则的描述，用户可以较为详细描述该号码规则的作用
主叫号码前缀	用于呼叫选择路由时匹配主叫号码前缀的号码规则，不支持正则表达式
被叫号码前缀	用于呼叫选择路由时匹配被叫号码前缀的号码规则，不支持正则表达式

3.4.13 黑白名单

在“业务黑白名单”页面，用户通过把号码列入白名单或黑名单来决定 SBC 系统是否接受该号码的呼叫和注册。它支持黑白名单导入和导出两种方式。

图 3-4-18 黑名单

图 3-4-19 白名单

表 3-4-17 黑白名单

参数	描述
黑名单组	黑名单组的名称，可自定义，添加成功后不可修改
白名单组	白名单组的名称，可自定义，添加成功后不可修改
描述	描述黑/白名单组，用户可以较为详细描述该黑/白名单组的作用
号码	黑/白名单的号码，支持正则表达式
描述	该条黑/白名单号码的具体描述

3.4.14 号码变换

号码变换用于呼叫选择路由时根据匹配规则将主/被叫号码变换成指定的主/被叫号码。

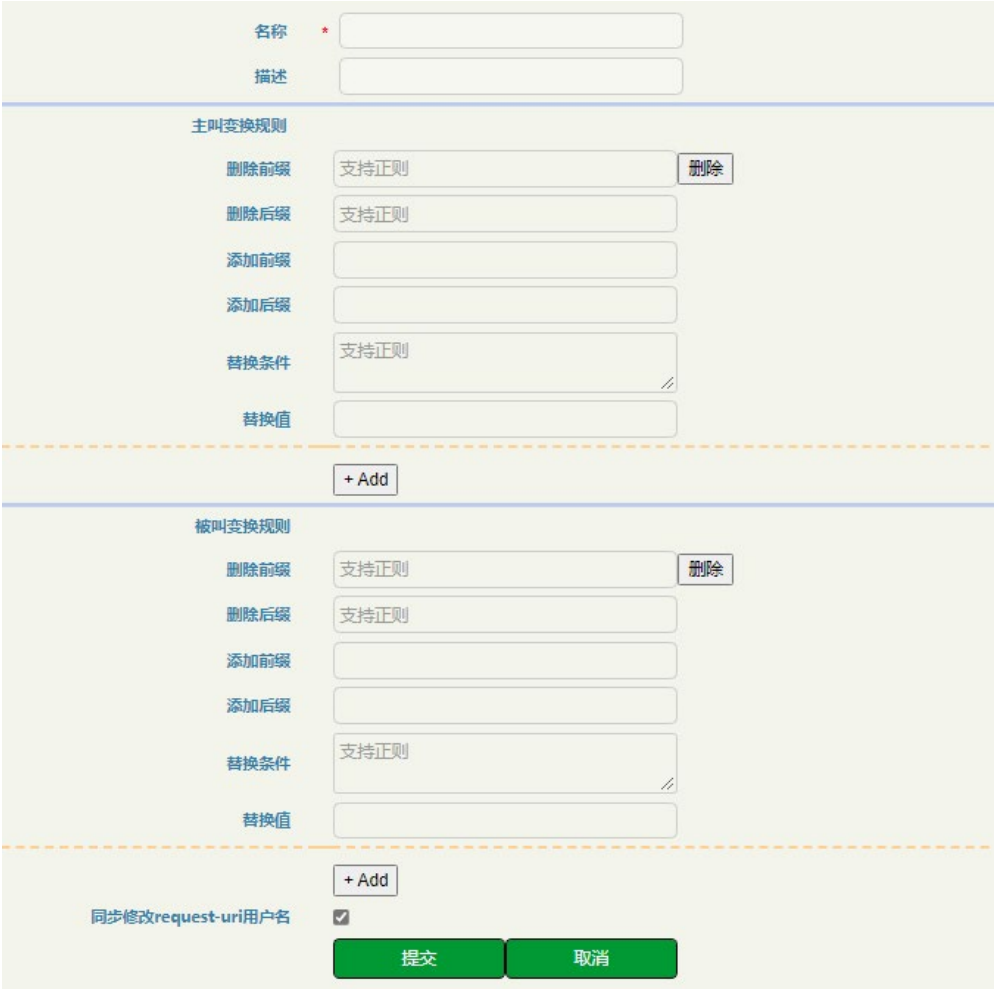


图 3-4-20 号码变换

表 3-4-18 号码变换

参数	描述
名称	配置号码变换的名字，用户自定义，添加成功后不可修改
描述	该号码变换的描述，用户可以较为详细描述该号码变换的作用和原因
删除前缀	删除掉匹配到的前缀内容，例如：号码为 67890000，删除前缀内容为 678，则匹配该号码变换规则后，号码变为 9000，如果号码为 16789000，则不删除该号码前缀，支持正则表达式配置，一条号码变换规则同时可以配置多条删除前缀规则
删除后缀	删除掉匹配到的后缀内容，例如：号码为 90000678，删除后缀内容为 678，则匹配该号码变换规则后，号码变为 9000，如果号码为 90006789，则不删除该号码后缀，支持正则表达式配置，一条号码变换规则同时可以配置多条删除前缀规则
添加前缀	在号码最前面添加上前缀，如原号码为 9000，添加前缀为 678，匹配该号码变换规则后，号码变换为 6789000，不支持正则表达式配置
添加后缀	在号码最后面添加上后缀，如原号码为 9000，添加后缀为 678，匹配该号码变换规则后，号码变换为 9000678，不支持正则表达式配置
替换条件	用正则表达式配置号码变换规则，如果号码能够匹配替换条件中的一条规则，则将号码变换为下面选项中的替换值
替换值	原号码如果能够匹配上面的替换条件中的一条规则，这替换为该替换值，替换值配置不支持正则表达式
同步修改 request-uri 用户名	勾选后会同步修改 request-uri 用户名

注意：

一条号码变换规则，会将号码从删除前缀、删除后缀、添加前缀、添加后缀依次处理，然后根据以上处理结果，再用来匹配替换条件。

入局号码变换，指的是对应中继（或接入网）呼入时选路前的号码变换。

出局号码变换，指的是选路后的号码变换，所以入局号码变换配置在中继（或接入网）配置中；出局号码变换配置放在路由配置中。

3.4.15 号码池

呼叫选择路由后，如设置号码池规则，那么从该路由出局的主叫或被叫号码会被号码池的号码随机替换。

图 3-4-21 号码池

表 3-4-19 号码池

参数	描述
名称	该号码池的名称，可自定义，添加成功后不可修改
描述	该号码池的描述，可较为详细描述该号码池的作用和原因
前缀	用于匹配主叫/被叫号码的前缀
起始数值	号码池的起始数值
结束数值	号码池的结束数值
同步修改 request-uri 用户名	勾选后会同步修改 request-uri 用户名

3.4.16 SIP 账户

配置 SBC 向服务器注册的账户信息。支持导入和导出。

图 3-4-22 SIP 账户

表 3-4-20 SIP 账户

参数	描述
名称	配置 sip 账户的名字，用户自定义，添加成功后不可修改
描述	该 sip 账户的描述，用户可以较为详细描述该 sip 账户的作用和原因

流控个数	单位时间内注册个数
流控单位时间	流控个数的最少注册时间
用户名	注册账户的用户名
认证 ID	注册账户的认证 ID，必须和 sip 服务器保持一致，否则注册不上
密码	注册账户的认证密码
注册周期	在此时间内发起注册，若未注册成功，此时间周期后再次发起注册
最大并发呼叫数	此账户最大呼叫的并发数
起始数值	用户名,认证 ID,密码选项支持规则适配，可变字符$1 的起始数值
步进	可变字符$1 的步进长度
账户数量	可变字符$1 的账户总数

注意：

*(账户总数 / 流控个数) * 流控单位时间 < 注册周期的 50%~90%。否则部分用户注册不上，流控只适用于 register 报文 。*

3.4.17 时间规则

时间规则配置路由生效时间段，可以按照日期、工作日、时间点进行配置。路由配置添加时间规则后，在配置时间内能该路由生效，配置时间外该路由不生效（呼叫匹配不到该路由）。

图 3-4-23 时间规则

表 3-4-21 时间规则

参数	描述
名称	路由时间的名称，用户可以自定义，添加成功后不可修改
描述	该路由时间的描述，用户可以较为详细描述该路由时间的作用
日期	路由生效的开始日期到结束日期，可以配置多个日期段
工作日	路由生效的工作日（周一到周日），可以复选
时间	路由生效的开始时间点到结束时间点，可以配置多个时间段

3.4.18 速率控制

速率控制页面主要是配置接入网、接入网中继和核心网中继的每秒最大注册数、每秒最大呼叫数和最大的呼叫并发数。

图 3-4-24 速率控制

表 3-4-22 速率控制

参数	描述
名称	配置该调速率控制的名称，可自定义，添加成功后不可修改
描述	该速率控制的描述，用户可以较为详细描述该速率限制的作用和原因
注册速率	每秒最大注册数
呼叫速率	每秒最大呼叫数
最大并发呼叫数	最大总呼叫并发数

注意：

1. 速率控制有一条默认数据，该数据在配置 License 时自动生成，配置速率控制的最大值，不能超过这条默认值。

2. 实际呼叫时所有总注册速率、总呼叫速率、总最大并发数，不会超过 license 限制值。

3.4.19 SIP 头域修改

当需要修改接入网、接入网中继或核心网中继时，可对指定 SIP 报文进行相应的头域修改，以满足某些对 SIP 头域有特殊要求（原始报文未提供）的需求。

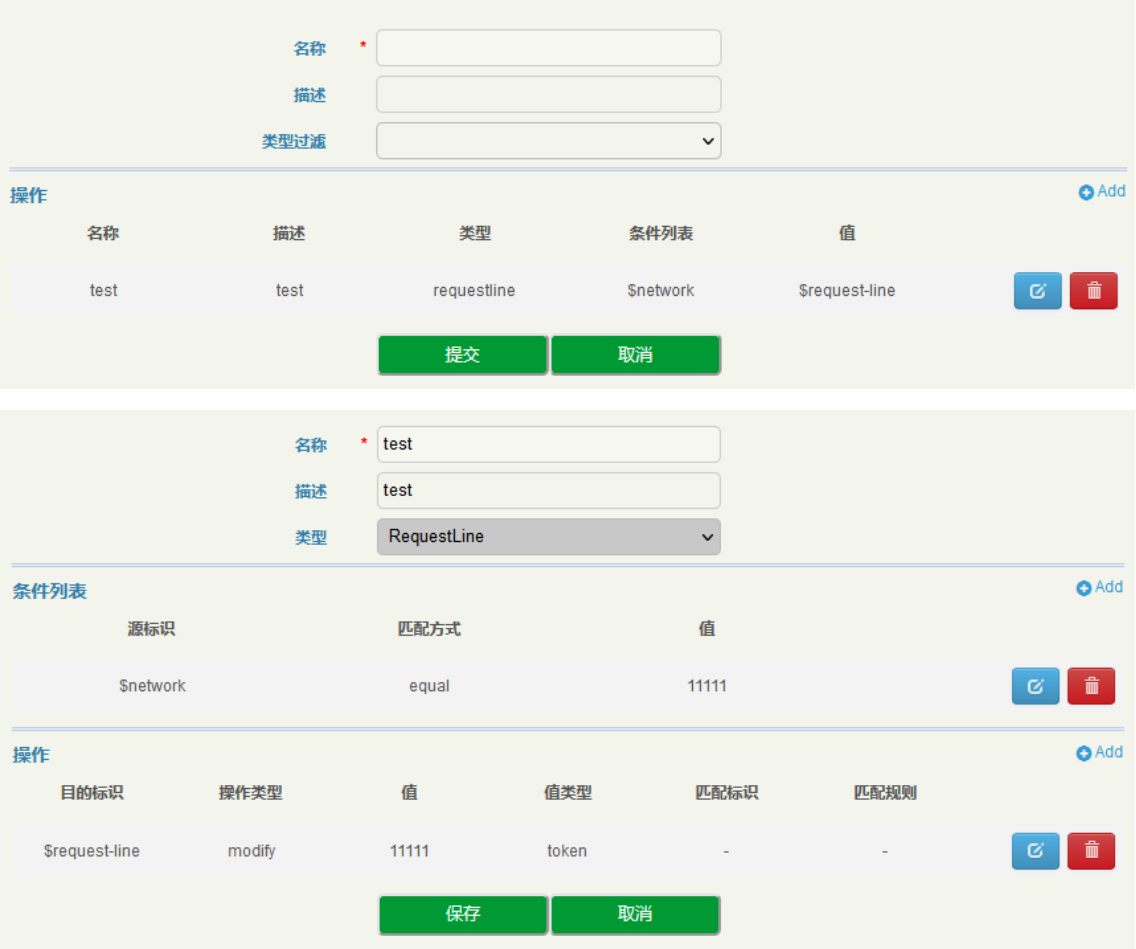


图 3-4-25 SIP 头域修改

表 3-4-23 SIP 头域修改

参数	描述
名称	配置头域变换的名字，用户自定义，添加成功后不可修改
描述	该 SIP 头域变换的描述，用户可以较为详细描述该号码变换的作用和原因
类型过滤	Requset：该规则只处理 SIP 的请求报文，响应报文不处理 Response：该规则只处理 SIP 的响应报文，请求报文不处理 List：该规则只处理选中的请求和响应报文，未选中的报文不处理。
操作规则	根据源标识的匹配条件列表（与关系），对目的标识进行头域变换（add、modify、remove）

类型	一条 SIP 头域修改规则可以有多条子规则，每条子规则只能处理一种类型，如果要同时处理多种类型，必须配置多条子规则： Request-line：SIP 报文请求行中的内容 Status-line：SIP 报文状态行中的内容 Header：SIP 报文中 header 的内容
源标识	指的是 SIP 原始来源报文，可以指定到原始 SIP 报文中某一个参数的内容
匹配方式	Equal：值为完全匹配，只有指定源标识的值完全等于配置的值，该规则才会生效 Regex：值为正则表达式匹配，当指定源标识的值符合配置的正则表达式，该规则就会生效
值	匹配条件指定的目标标识值
目的标识	指的是需要修改 SIP 报文指定的头域
操作类型	Add：在指定目标标识内容后面添加上对应的值 Modify：修改指定目标标识的值为对应的值 Remove：删除指定目标标识的值，如果目标标识为一个域，则删除该域
值类型	Token：值中带$标志的内容代表引用原始源报文指定域的内容，不带$标识的内容为配置是什么就是什么 Equal：值内容为配置是什么就是什么 Regex：regex 比较特殊，多了一个三级子规则，源报文内容必须和对应的匹配规则内容相同，该子规则才会生效
值	Token 和 Regex 值类型中，带$的标识引用原始报文指定域的值，Equal 中如果有$，无特殊意义

注意：

用$引用原始报文的值时，必须参考目标标识的配置方式，如，要引用原始报文中 to 域中的 user 值，输入的方式为$to.$.uri$.user。

所有用$引用的值，都是原始报文（未变换前的 SIP 报文）的值，不是经过处理的值（如号码变换、前面 SIP 头域修改等）。

每个 SIP 头域参数有对应的规格，用户修改建议严格按照参数规则来修改或匹配，用户可以参考附件中的《SMM 规则和变量（SIP 头域修改）.xlsx》确定每种域的参数规则和修改权限。

3.4.20 SIP 头域透传

“SIP 头域透传”可用来在指定路由中透传 SIP 消息中指定的扩展域。

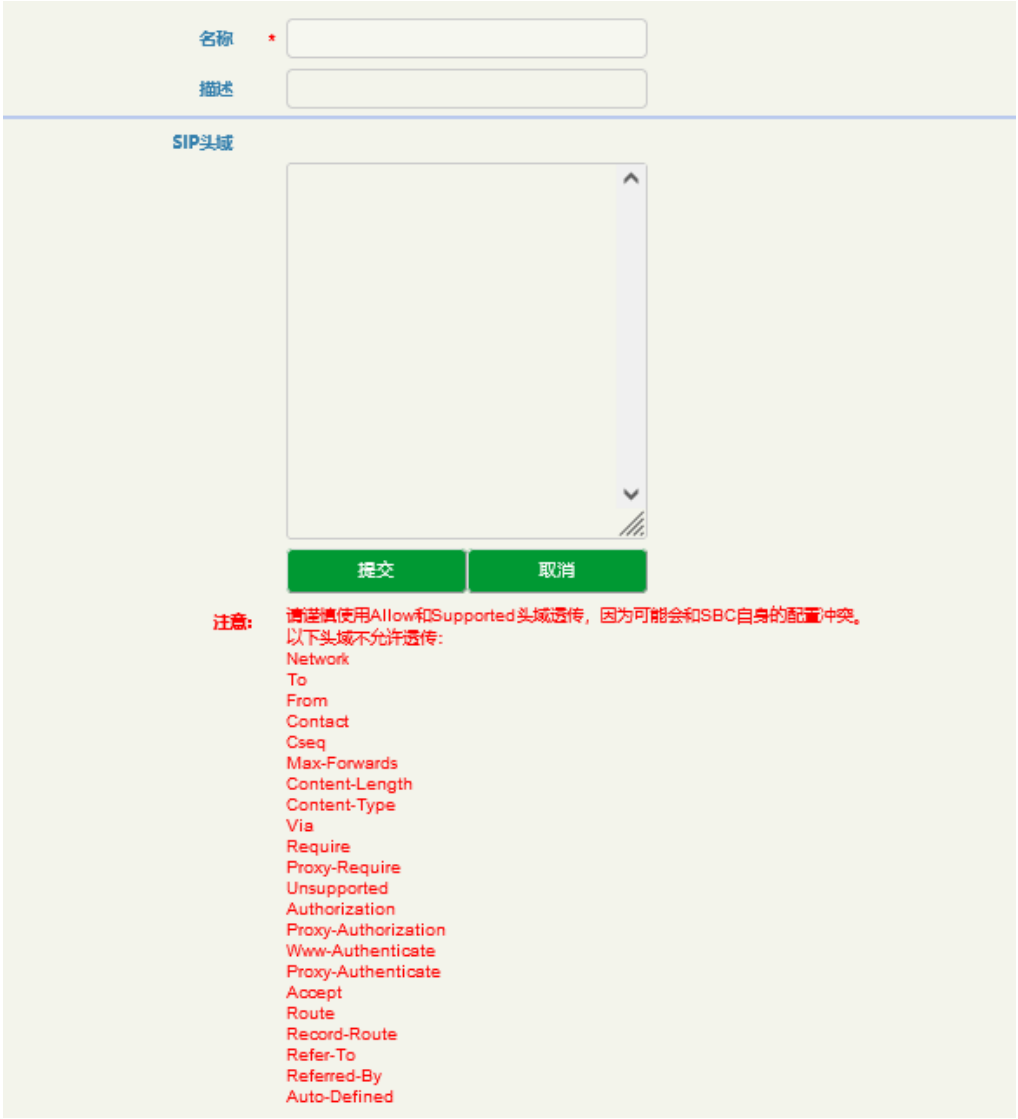


图 3-4-26 SIP 头域透传

表 3-4-24 SIP 头域透传

参数	描述
名称	配置 SIP 头域透传的名字，用户自定义，添加成功后不可修改
描述	该 SIP 头域透传的的描述，用户可以较为详细描述该接入网的作用和规则

SIP 头域	允许透传的头域，一行一个头域，头域区分大小写，完全匹配，不要有额外的标点符号

注意：

请谨慎使用 Allow 和 Supported 头域透传，因为可能会和 SBC 自身的配置冲突。以下头域不允许透传：

Network, To, From, Contact, Cseq, Max-Forwards, Content-Length, Content-Type, Via, Require, Proxy-Require, Unsupported, Authorization, Proxy-Authorization, Www-Authenticate, Proxy-Authenticate, Accept, Route, Record-Route, Refer-To, Referred-By 和 Auto-Defined。

3.4.21 质量监控

质量监控用于与监控与远端地址的网络质量，达到配置的标准后对于后续的通信进行处理。

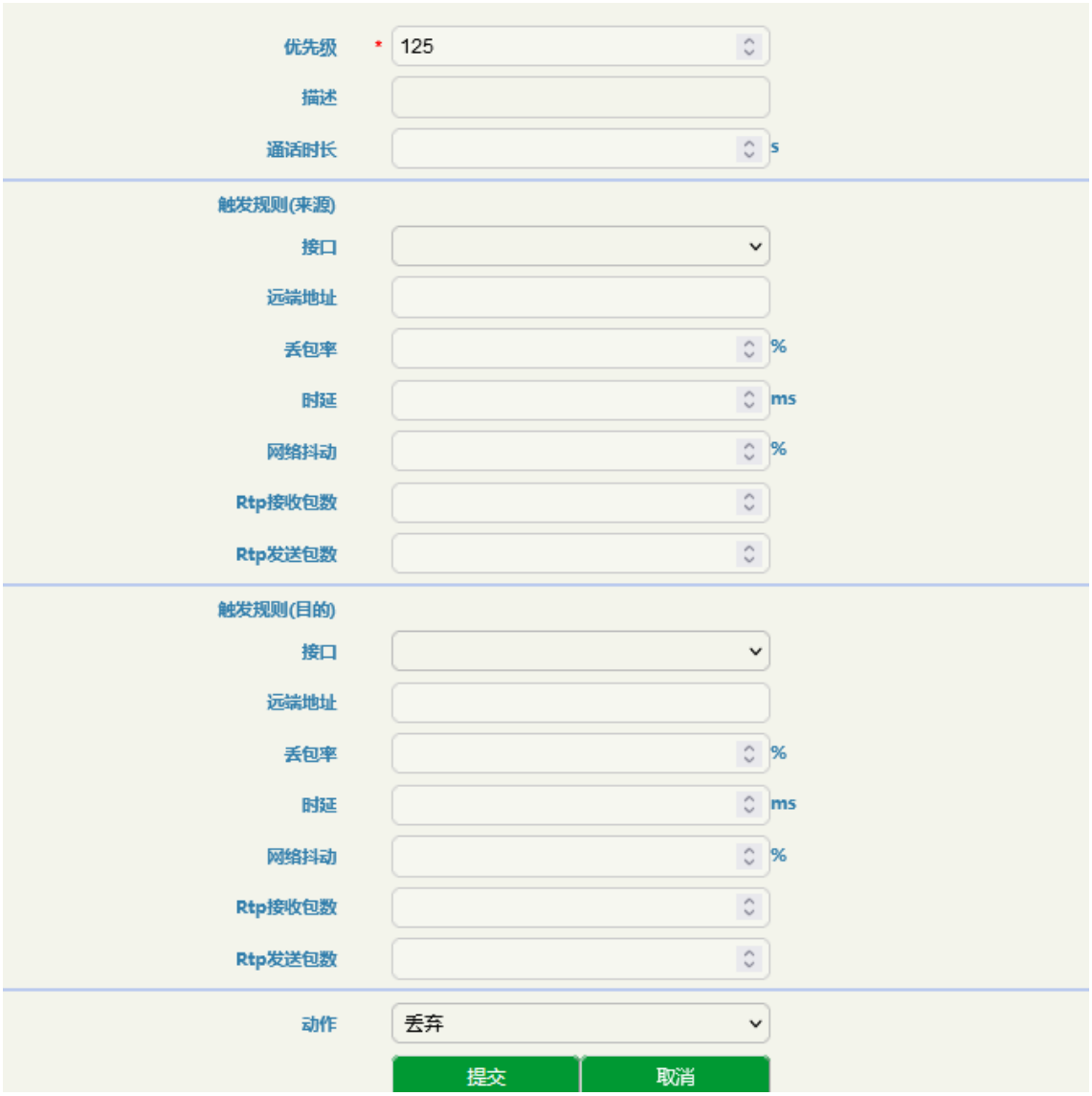


图 3-4-27 质量监控

表 3-4-25 质量监控

参数	描述
优先级	建立通话后通过该质量监控的优先级，数字越大优先级越高
描述	描述该质量监控的作用和目的，由用户自行设置
通话时长	通过该中继的通话时长
接口	被监控通话的接口
远端地址	通过该监控接口对应的远端 IP 地址
丢包率	网络状态发生变化时的丢失数据包数量占所发送数据组的比率
时延	报文或分组从一个网络的一端传送到另一个端所需要的时间
网络抖动	网络状态以及延迟影响到通话质量的参数，也就是延迟变化的程度
RTP 接收/发送包数	RTP 接收/发送包数
动作	达到触发条件后 SBC 的动作，丢弃/日志/告警

3.4.22 带宽限制

按照编解码限制每通语音/视频通话的带宽。

图 3-4-28 带宽限制

表 3-4-26 带宽限制

参数	描述
名称	该带宽限制的名称，用户保存后无法修改
描述	描述该带宽限制的作用和目的，由用户自行设置
音频/视频	在接入/核心中继配置中应用该规则后才会生效，应用后通过该接入/核心中继的音视频会被限制带宽，配置前注意底下红色标识字段

注意：

带宽限制预分配每路语音通话 20kbps、视频通话 2mbps，接通后，根据配置带宽数值多退少补。

3.5 安全

安全配置用于配置 SBC 系统通信接口的系统安全策略、防攻击策略和访问控制策略。

3.5.1 系统安全

系统安全主要功能是防止 SBC3000 Pro 设备受到各种 DOS/DDOS 大流量攻击，保障系统的稳定运行。

图 3-5-1 系统安全页面

表 3-5-1 系统安全

参数	描述
攻击日志	启用后，当系统受到攻击，并触发安全策略，系统会记录该攻击，攻击日志可以在 维护-->日志-->安全日志 里查看。
ICMP-Flood 攻击防御	ICMP-Flood 是一种 DDOS 攻击，它通过发送大量的 ICMP 报文对系统进行冲击，启用该攻击防御策略后，系统在 1 秒中内收到超过设置的 ICMP 报文，就会把超过的 ICMP 报文直接丢弃，配置范围 1-1000
TCP-NULL 攻击防御	TCP-NULL 是一种端口扫描方式，即发送一个没有任何标志位的 TCP 包，根据 RFC793，目标主机的相应端口如果是关闭的，应该发送回一个 RST 数据包，通过这种方式，可以辨别某台主机运行的操作系统是什么操作系统。启用该防攻击策略，系统会将直接丢弃这种报文
TCP XMAS TREE 攻击防御	通过发送带有特殊标志位的 tcp 数据包发送给目标主机，可以用来探测目标主机哪些端口开放。启用该防攻击策略，系统会将直接丢弃这种报文
TCP-Flood 攻击防御	TCP-Flood 是一种 DDOS 攻击，通过发送大量的 TCP 连接请求，抢占目标主机的系统资源，造成目标系统崩溃。启用该策略，系统在 1 秒中内收到超过设置的 TCP 连接请报文，就会把超过的请求报文直接丢弃，配置范围 1-1000

3.5.2 访问控制

设置设备的 WEB（https）和 SSH 访问控制端口，以及其他网口 GE1 到 GE7 网口和 VLAN 接口的访问控制策略，网口默认不能通过 web 和 SSH 访问。

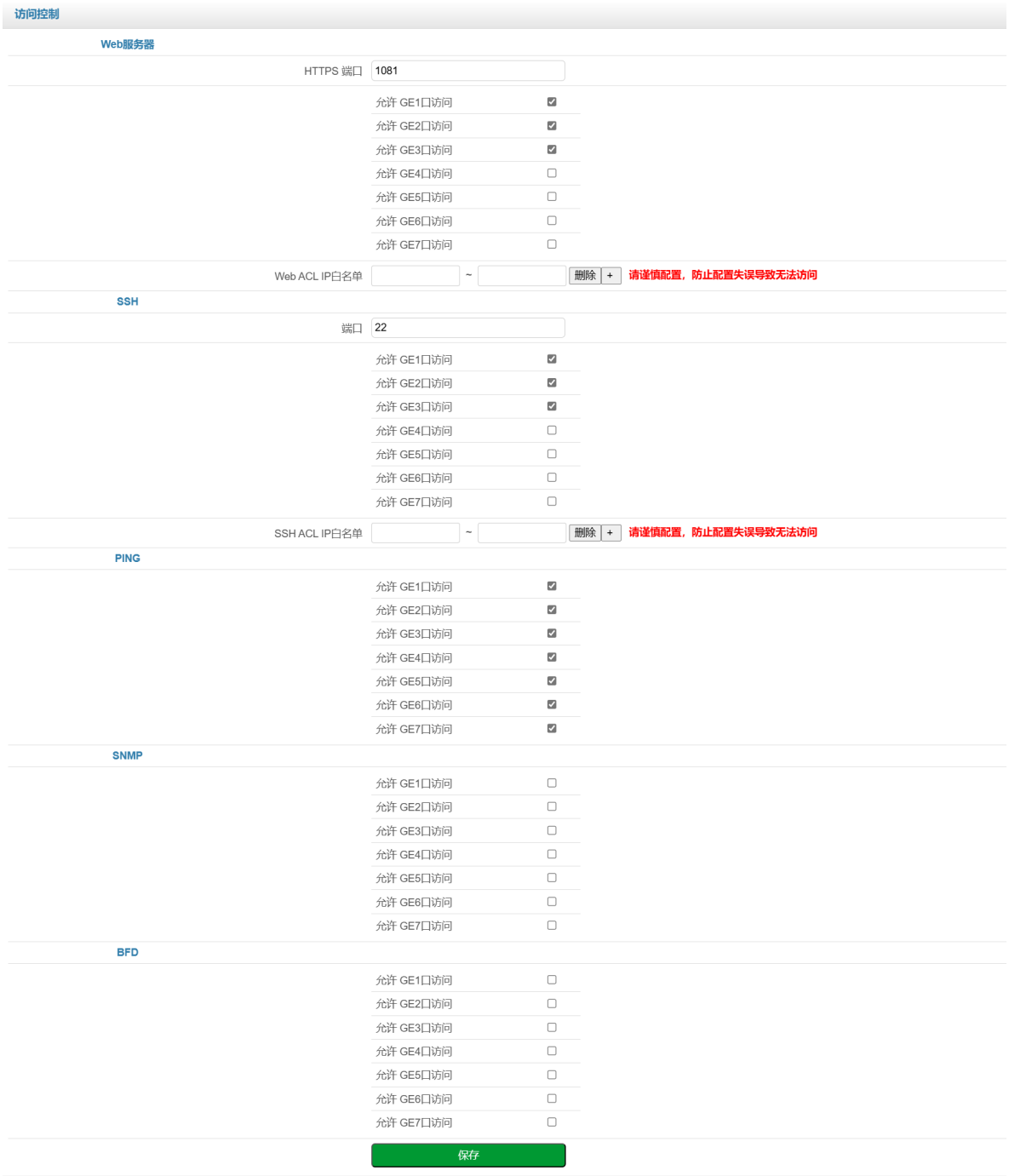


图 3-5-2 访问控制设置

表 3-5-2 访问控制

参数	描述
Web 服务器	HTTPS 端口：通过 web 的 https 协议访问时的端口，默认为 1081，用户可以修改成其它端口； 设置是否允许其他设备通过 GE1 到 GE7 网口以 Web 方式访问 SBC 设备，默认不允许
Web ACL IP 白名单	白名单内的 ip 允许访问设备 web
SSH	SSH 端口：通过 SSH 登录设备时的端口，默认为 22，用户可以修改成其它端口； 设置是否允许其他设备通过 GE1 到 GE7 网口以 SSH 方式登录 SBC 设备，默认不允许
SSH ACL IP 白名单	白名单内的 ip 允许 ssh 访问设备
PING	勾选端口表示您可以对该端口的 IP 地址进行 Ping 请求。如果取消勾选，则您将无法对该端口的 IP 地址进行 Ping 操作
SNMP	默认不勾选，勾选后允许通过该网口 snmp 管理设备
BFD	默认不勾选，勾选后允许通过该网口使用 BFD

3.5.3 防攻击策略

IP 防攻击

图 3-5-3 IP 防攻击

表 3-5-3 IP 防攻击

参数	描述
保护时间	将发起攻击的 ip 或者用户加入黑名单的时间
优先级	优先级的数字越低，优先级等级越高
描述	描述该 SIP 防攻击策略的作用和目的，由用户自行设置

攻击对象	配置攻击对象，Remote IP/local port Remote IP：当某一个 IP 发过来的报文流量超过设定阈值时，系统会根据动作类型对该 IP 发过来的报文做相应的处理。 local port：当 SBC 某一个端口收到的报文流量超过设定阈值时，系统会根据动作类型对发到该端口的报文做相应的处理。
CPU 使用率	配置设备的 CPU 达到触发的阈值
触发流量	配置达到流量阈值触发 IP 防攻击
动作类型	记录日志：该策略生效时，只记录该事件日志，不做其它处理 流量限速：该策略生效时，处理的流量被限速值， 丢弃：该策略生效时，对该 IP 或者端口收到的报文，在限制时间内全部丢弃 包速率限速：该策略生效时，对该 IP 或者端口收到的报文在限制时间内限制速率。

SIP 防攻击

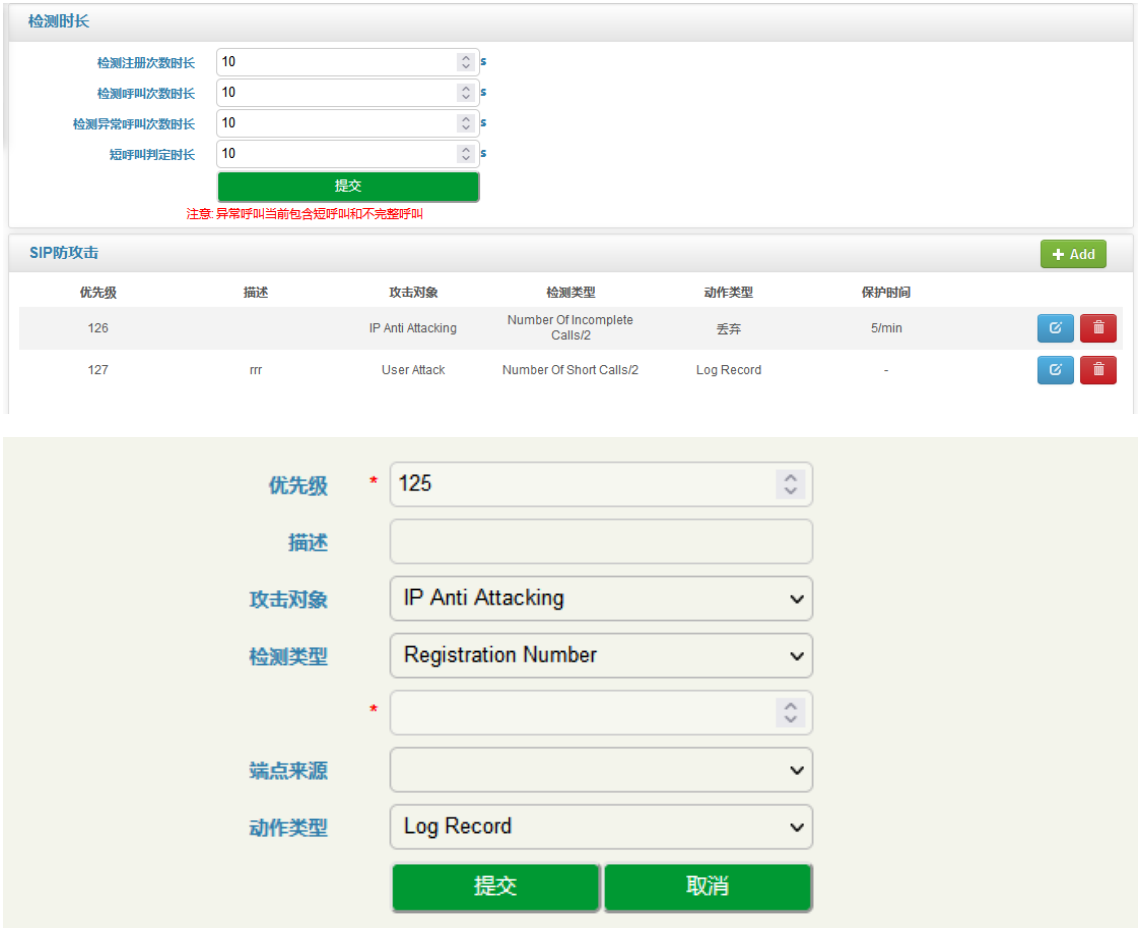


图 3-5-4 SIP 防攻击

表 3-5-4 SIP 防攻击

参数	描述
检测注册次数时长	配置时间内检测到配置次数的注册，则判定为 SIP 攻击
检测呼叫次数时长	配置时间内检测到配置次数的呼叫，则判定为 SIP 攻击
检测异常呼叫次数时长	配置时间内检测到配置次数的异常呼叫，则判定为 SIP 攻击，异常呼叫当前包含短呼叫和不完整呼叫
短呼叫判定时长	低于配置值的呼叫判断为短呼叫
优先级	优先级的数字越低，优先级等级越高
描述	描述该 SIP 防攻击策略的作用和目的，由用户自行设置
攻击对象	配置攻击对象的类型，IP Anti attacking/User attack IP 防攻击：当某一个 IP 在检测周期内发过来的 SIP 报文数超过设定阈值时，系统会根据动作类型对该 IP 发过来的 SIP 报文做相应的处理。 用户防攻击：在检测周期内发过来相同用户和接入网监听端口的注册/呼叫（主叫）报文数超过设定阈值时，系统会根据动作类型对该用户 SIP 报文做相应的处理。
检测类型	配置检测类型，number of registrations /number of calls /number of short calls /number of incomplete calls 注册次数：检测同一 IP 或用户发过来 SIP 报文中的 REGISTER 报文次数，在检测周期发现次数超过阈值，系统会根据动作类型对该 IP 或用户的 REGISTER 报文做相应处理 呼叫次数：检测同一 IP 或主叫用户发过来 SIP 报文中的 INVITE 报文次数，在检测周期发现次数超过阈值，系统会根据动作类型对该 IP 或用户的 INVITE 报文做相应处理 短呼叫次数：检测同一 IP 或主叫用户的短呼叫次数，在检测周期发现次数超过阈值，系统会根据动作类型对该 IP 或用户的 INVITE 报文做相应处理 不完整呼叫次数：测同一 IP 或主叫用户的不完整呼叫次数，在检测周期发现次数超过阈值，系统会根据动作类型对该 IP 或用户的 INVITE 报文做相应处理
端点来源	配置 SIP 攻击检测的端点
动作类型	记录日志：该策略生效时，只记录该事件日志，不做其它处理 丢弃：该策略生效时，对该端点收到的报文，在限制时间内全部丢弃 带宽限制：该策略生效时，对该端点收到的报文，在限制时间内限制带宽 包速率限制：该策略生效时，对该端点收到的报文，在限制时间内限制包速率
保护时间	SIP 防攻击策略生效的时间一个策略生效时，超过设置时间后需要重新判断策略是否生效

3.5.4 Web 认证配置

3.5.3.1 认证策略

配置认证方式的优先级，可选本地认证, tacacs 认证和 radius 认证。认证方式默认为本地认证。当认证方式不包括本地认证时，如果认证失败，最后会进行本地认证。

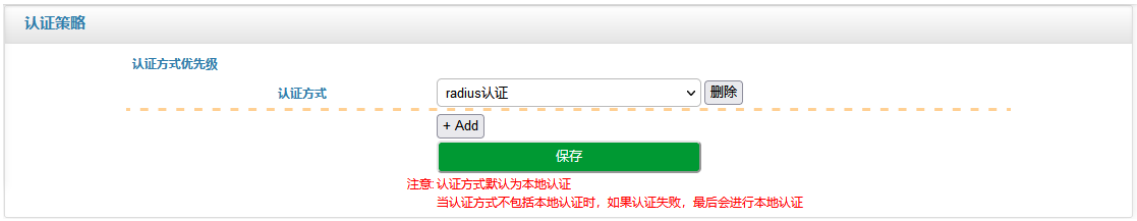


图 3-5-5 认证策略

Tacacs 认证配置

配置 tacacs 认证的服务器信息。

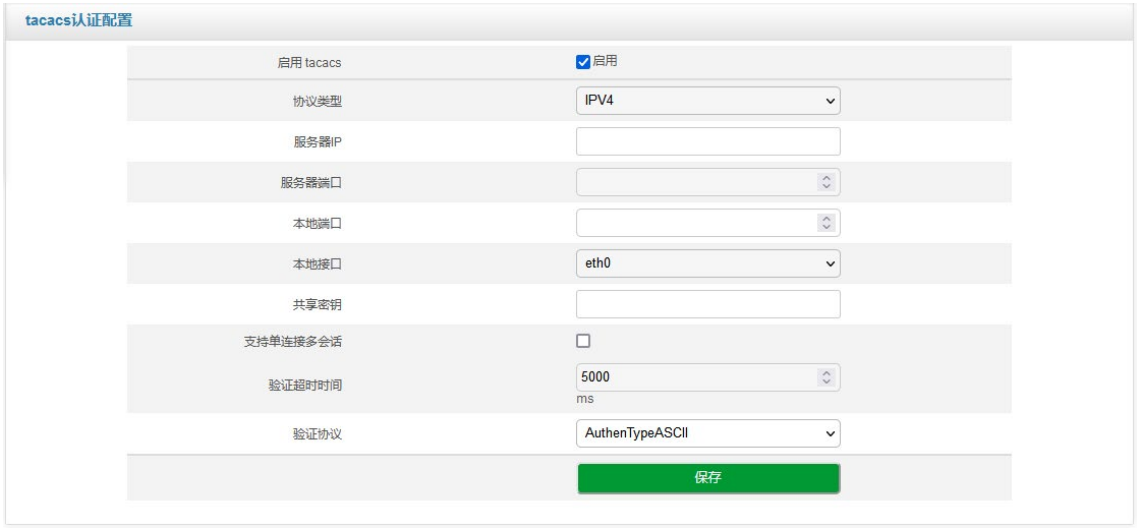


图 3-5-6 tacacs 认证配置

表 3-5-5 tacacs 认证配置

参数	描述
协议类型	和服务器交互的协议类型，ipv4/ipv6
服务器 IP	Tacacs 服务器的 IP 地址

服务器端口	Tacacs 服务器的认证端口
本地端口	SBC 的 tacacs 服务监听端口
本地接口	SBC 的物理网络接口
共享密钥	和 tacacs 服务器交互的共享密钥
支持单连接多会话	勾选后支持单连接多会话
验证超时时间	Tacacs 认证的超时时间，超过配置时间后认证失败
验证协议	Tacacs 认证的验证协议

Radius 配置

配置 radius 认证和计费的相关参数。

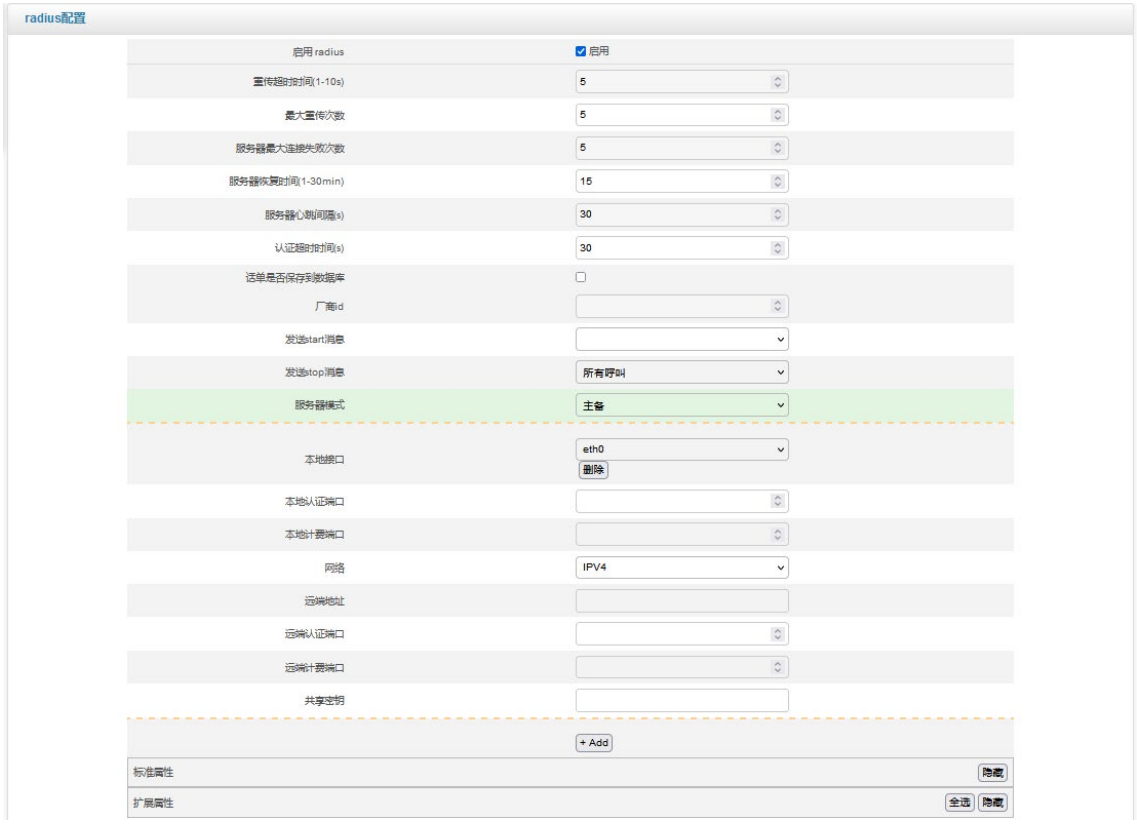


图 3-5-7 radius 配置

表 3-5-6 radius 配置

参数	描述
重传超时时间	Radius 消息重传的超时时间
最大重传次数	Radius 消息最大重传的次数
服务器最大连接失败次数	超出配置值后服务器更新为故障状态
服务器恢复时间	配置的时间后故障的服务器自动恢复为正常状态
服务器心跳间隔	和服务器交互的心跳消息的时间间隔
认证超时时间	配置的时间后未收到服务器的认证响应消息则认证失败
话单是否保存到数据库	勾选后话单先保存到 SBC 的数据库，服务器从数据库取话单一次性发送给服务器，需要配置从数据库取话单个数
厂家 ID	配置 radius 服务器厂家 ID
发送 start 消息	配置的状态时 SBC 发送计费 start 消息，invite 消息/振铃/接通
发送 stop 消息	配置的情况下 SBC 发送计费 stop 消息，所有呼叫/正常呼叫
服务器模式	多个 radius 服务器时消息发送策略，主备/负载均衡
本地接口	SBC 的 radius 消息发送的物理接口
本地认证端口	SBC 的 radius 认证监听端口
本地计费端口	SBC 的 radius 计费监听端口
网络	和服务器交互的协议类型，ipv4/ipv6
远端地址	Radius 服务器的 IP 地址
远端认证端口	Radius 服务器的认证端口
远端计费端口	Radius 服务器的计费端口
共享密钥	和 Radius 服务器连接的共享密钥
标准/扩展属性	Radius 计费消息的标准/扩展属性，勾选启用

3.6 系统

系统配置包括系统管理、web 配置管理、网络管理、静态路由、用户管理、备份与恢复、License 管理、数字证书管理、用户板管理。

3.6.1 系统管理

系统管理用来配置 SBC3000 Pro 设备名称。支持用户自定义修改。

图 3-6-1 系统管理

3.6.2 Web 配置管理

配置 web 访问的证书等。

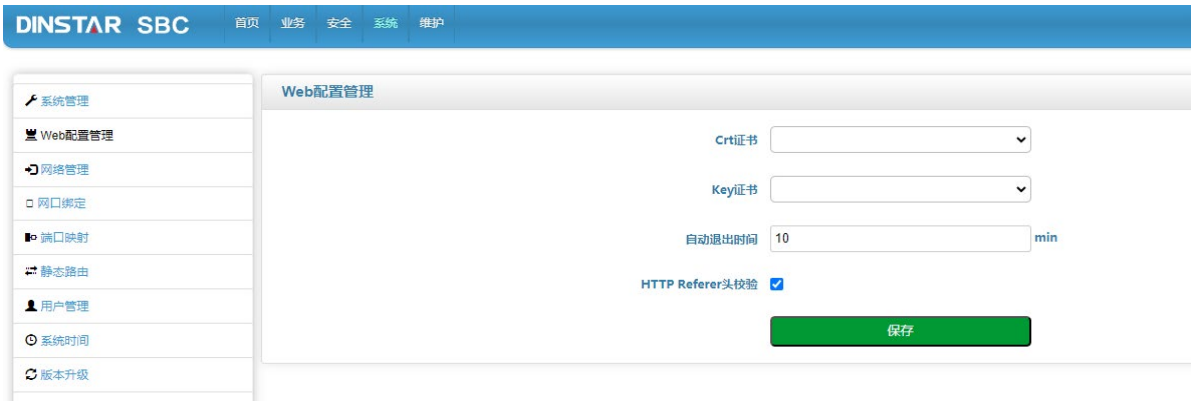


图 3-6-2 web 配置管理

表 3-6-1 web 配置管理

参数	描述
CRT 证书	选择 https 访问使用的 CRT 证书
KEY 证书	选择 https 访问使用的 KEY 证书

自动退出时间	Web 自动退出登录的时间
http referer 头校验	默认勾选，勾选后严格校验 http referer 头

3.6.3 网络管理

对设备网络信息的配置，包括 MTU 大小、ipv4、ipv6 地址、掩码、mac、网关、dns，支持设置网络接口是业务接口或者管理接口，可添加 vlan 接口和浮动 ip 地址。

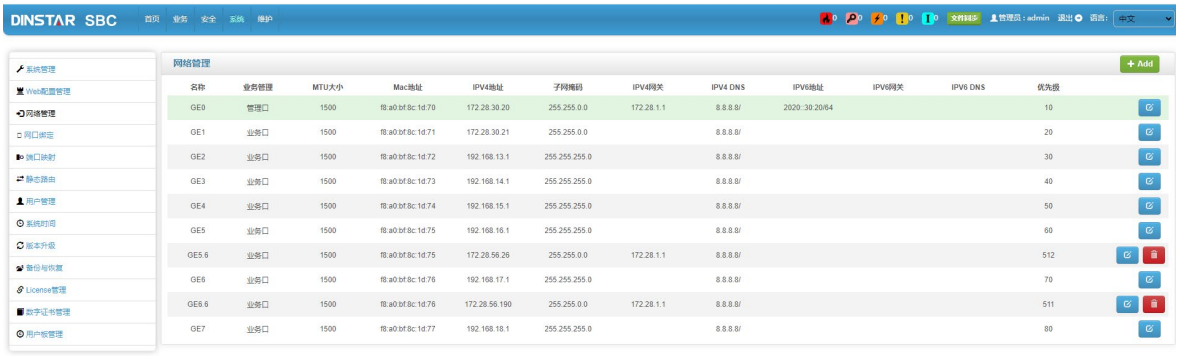


图 3-6-3 网络管理

点击页面右上方的  可以添加 VLAN，点击  可以修改 VLAN 或各个网口的接口配置，点击  则可以删除该 VLAN。

3.6.4 网口绑定

SBC3000 Pro 将多个网口绑定为一个组，实现网口冗余，负载均衡，达到高可用高可靠的目的。

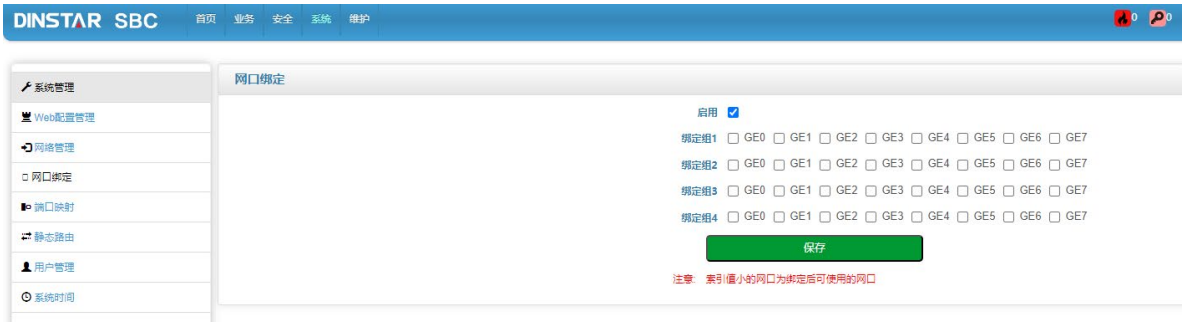


图 3-6-4 网口绑定

注意：*索引值小的网口为绑定后可使用的网口*

3.6.5 端口映射

端口映射可以将外网端口号和局域网内的主机 IP 地址、内网主机端口号建立映射关系，使得局域网内的主机的某个端口映射到外网，使外网的主机能够通过映射的端口访问内网的主机。

图 3-6-5 端口映射

表 3-6-2 端口映射相关参数描述

参数	描述
名称	该端口映射设置的名称，可自定义
状态	选择是否启用该端口映射的设置
网络	支持 IPV4 和 ipV6
协议	选择 TCP、UDP 或者 TCP/UDP
端口模式	支持单端口映射和多端口映射
本地接口	SBC 和外网连接使用的接口
本地端口	SBC 和外网连接使用的端口

目的接口	SBC 和内网连接使用的接口
目的 IP	需要映射到外网的内网主机的 IP 地址
目的端口	填写映射到外网的内网主机端口号（映射的内网主机端口不能与设备所使用的端口冲突）

3.6.6 静态路由

当设置静态路由后，去往指定目的地的报文将按照指定的路径进行转发。

图 3-6-6 静态路由

表 3-6-3 静态路由

参数	描述
优先级	静态路由的优先级，数字越小优先级越高
描述	对该静态路由的详细描述
网络	配置协议类型，ipv4/ipv6
目的 IP	静态路由需要到达的目的 IP 地址
子网掩码	静态路由需要到达的目的地址的子网掩码
接口	该静态路由发送报文时走的网络接口
下一跳	数据在到达目的地址前，需要经过的下一跳网关地址

3.6.7 用户管理

用户管理用来修改超级用户 admin 的密码和添加其它能够登录该设备的用户、密码和对应权限。

密码设置

修改当前用户的密码。出于系统安全方面的考虑，建议设置较为复杂的密码。

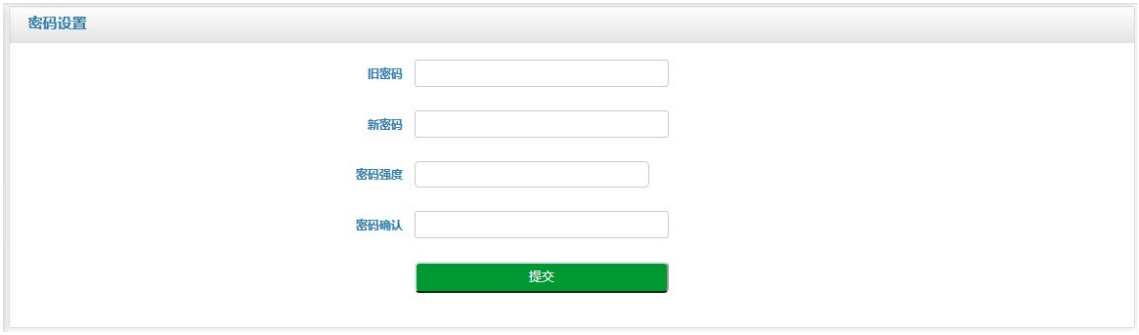


图 3-6-7 密码设置

用户列表

在用户列表页面，可添加除 admin 外的可以登录该 SBC 系统的其它用户。

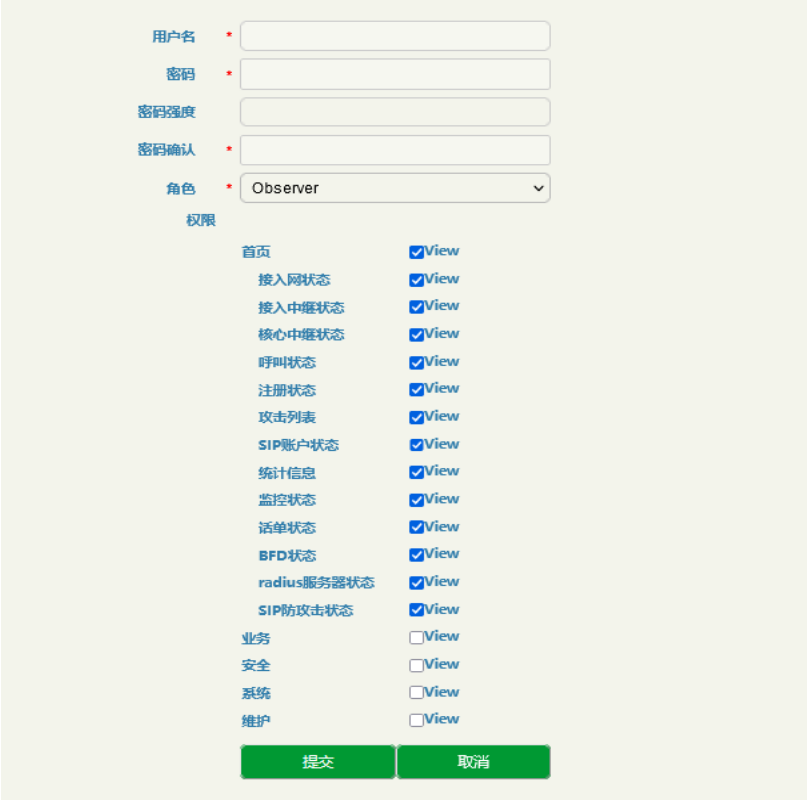


图 3-6-8 添加用户及设置权限

表 3-6-4 用户列表

参数	描述
用户名	用户登录 SBC 设备的账户名称
密码	用户登录 SBC 设备的密码
确认密码	确认用户登录 SBC 设备的密码，要求与密码要求一致
密码强度	设置的密码的强度
角色	管理员：可以添加操作员和维护员角色用户，可以重置其它用户密码，可以对 web 数据进行增加、修改和删除，管理员用户只有 admin 一个 操作员：可以访问大部分配置，修改配置数据等 维护员：只能查看 web 上的状态和部分配置，无修改删除权限
权限	配置用户的 web 页面权限，查看或者编辑，勾选启用

弱口令

配置系统的弱口令，弱口令列表的密码设置时有弱口令提示，不能设置。

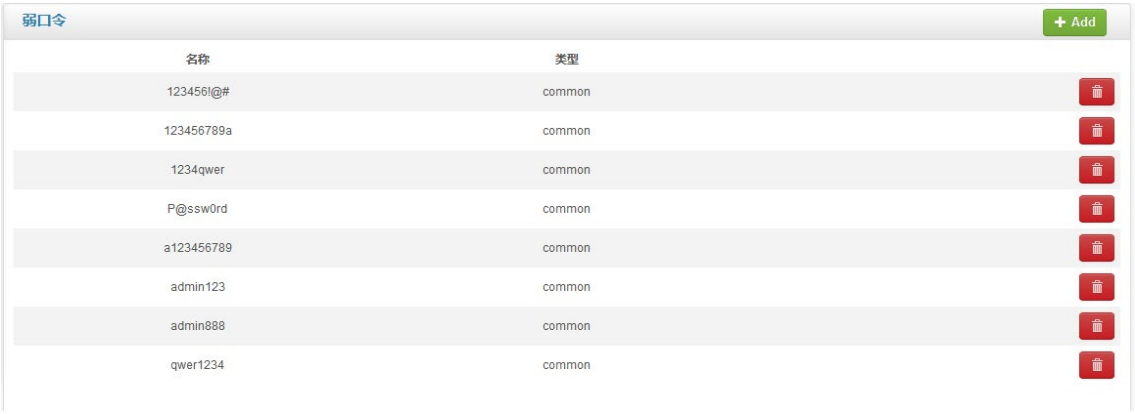


图 3-6-9 弱口令

表 3-6-5 弱口令

参数	描述
名称	设置的弱口令
类型	设置弱口令的类型，common/bussiness

3.6.8 系统时间

在系统时间页面，用户可配置系统时间，可以选择 NTP 服务器或者同步浏览器时间。

图 3-6-10 系统时间

表 3-6-6 时间管理

参数	描述
时区	配置设备所在的时区
同步浏览器时间	如果设备当前时间不准，并且无法同步 NTP 服务器，可以通过同步浏览器时间，将系统时间同步为用户登录该设备时的主机电脑时间
NTP 服务器	如启动，设备时间与 NTP 服务器将同步
同步浏览器时间	同步 NTP 服务器时间或者浏览器时间二选一方式设置设备的时间

3.6.9 版本升级

APP 升级

通过 Web 界面，可以将设备版本进行升级或回退。版本升级后需要重启设备才能生效。

图 3-6-11 APP 升级

一般情况下，版本升级文件为 1.93.x.x.ldf 文件，请不要选择其它产品的版本文件进行升级。

镜像升级

通过 Web 界面，可以将设备主控板和用户镜像进行升级。镜像升级后设备会重启。

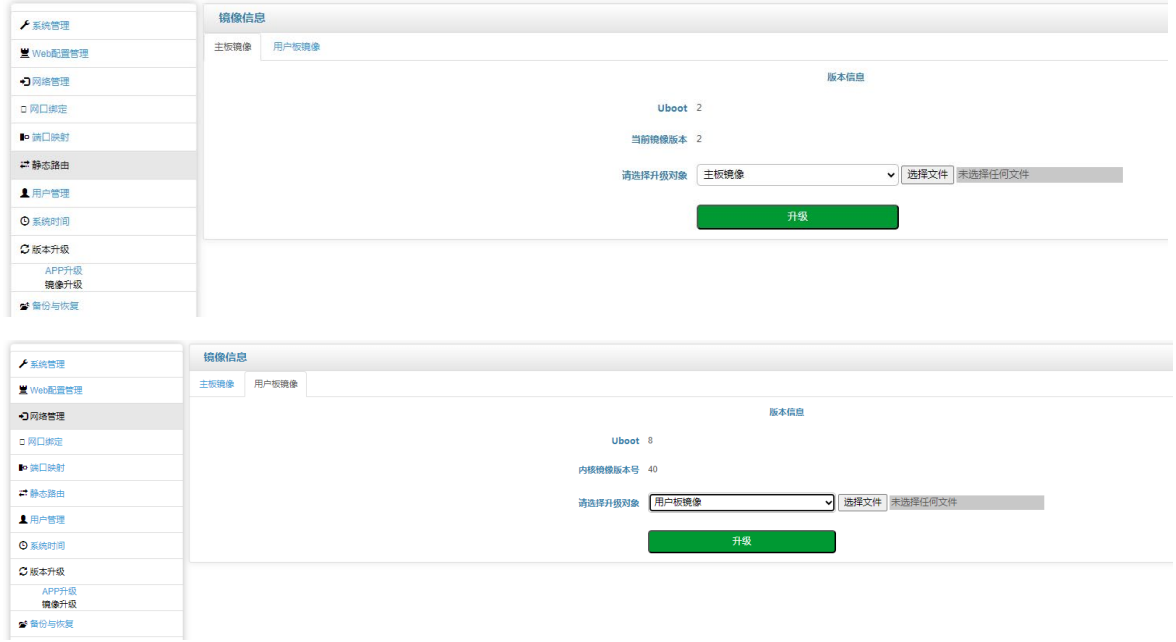


图 3-6-12 镜像升级

3.6.10 备份与恢复

在“备份与恢复”页面，用户可将 Web 上菜单栏业务的所有配置、网络配置和数字证书管理配置的数据进行备份或者恢复。恢复数据后设备会自动重启生效。可以对设备恢复出厂设置，将清除所有配置。

图 3-6-13 备份与恢复

表 3-6-7 备份与恢复

参数	描述
备份	下载需备份的 web 的配置数据，可以分别备份业务、证书文件、和网络配置，也可以任意组合备份，网络配置包括接口管理和静态路由的数据。
恢复	将备份的数据恢复到设备系统上，恢复成功设备会自动重启。
恢复出厂设置	将设备上的所有配置清除，恢复出厂默认配置

3.6.11 License 管理

License 管理限制设备的使用时长、注册最大用户数、最大并呼叫发数、最大每秒注册数、最大每秒呼叫数和最大转码呼叫数。License 过期后，其它设备将不能通过 SBC 进行注册和呼叫。

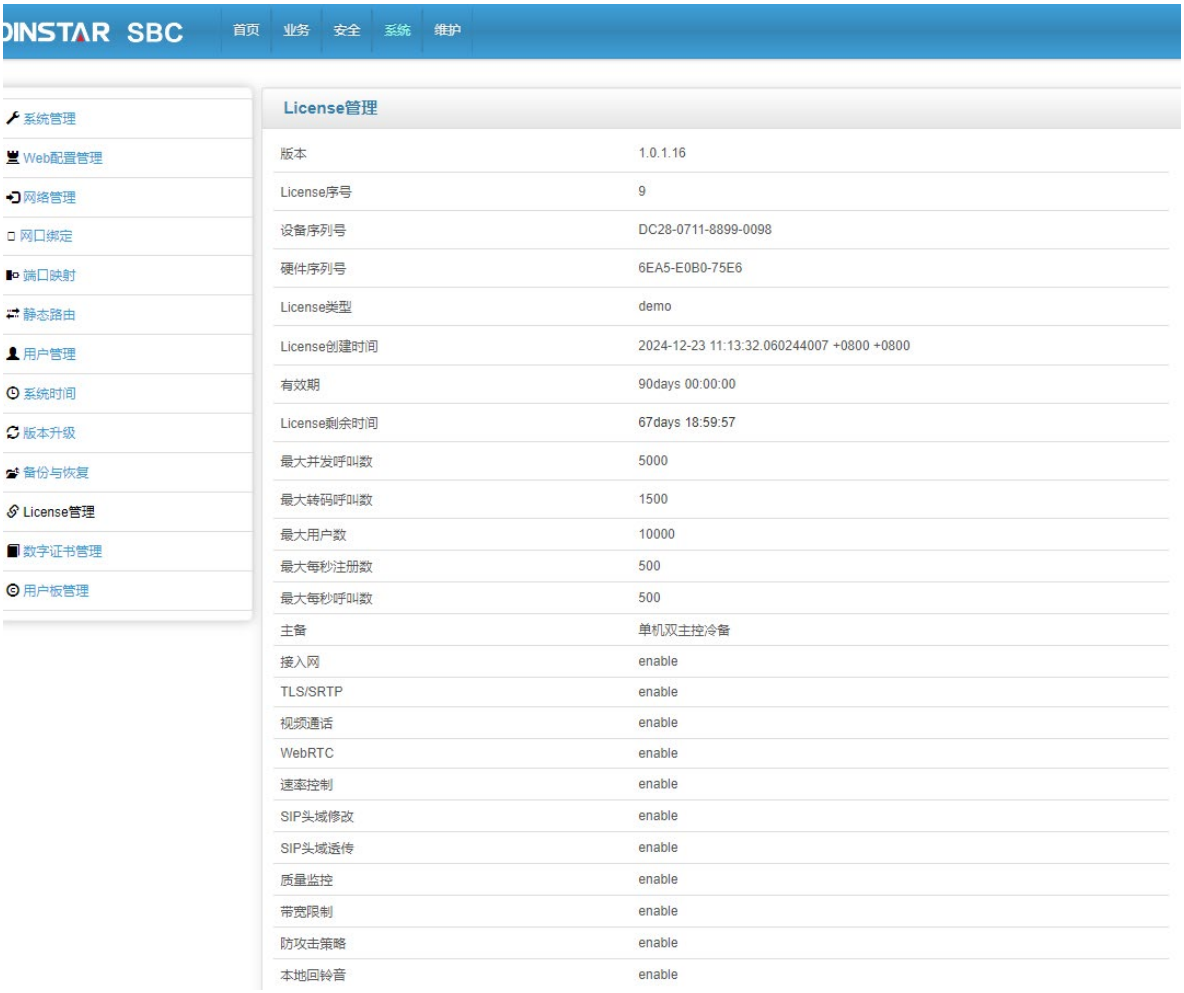


图 3-6-14 License 管理

3.6.12 数字证书管理

数字证书管理用于添加登录设备的 Web 界面的安全证书，只有证书认证通过，主机才能登录到设备的 Web 界面。非 admin 用户无数字证书管理权限。

图 3-6-15 数字证书管理

3.6.13 用户板管理

管理用户板和端口是否启用，默认都勾选启用。

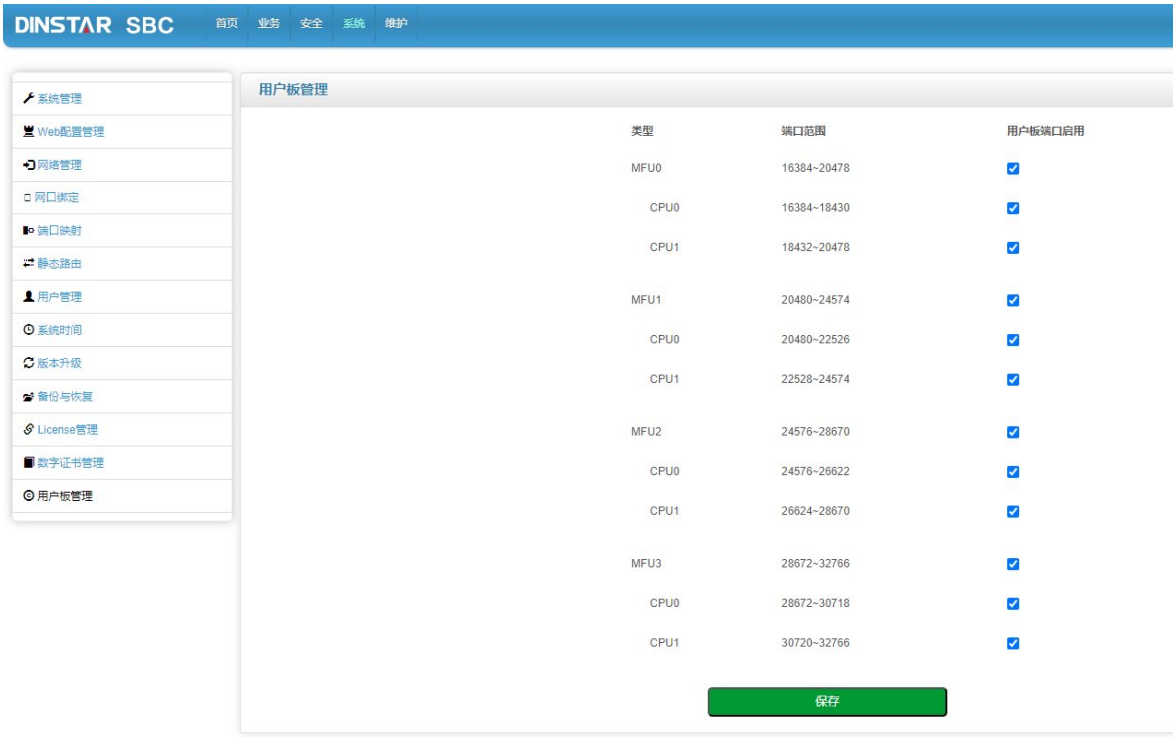


图 3-6-16 用户板管理

3.7 维护

3.7.1 日志

在日志页面，用户可以查看系统的登录日志、操作日志和安全日志，可以设置条件筛选日志，并且可以将这些日志导出到本地主机上。

图 3-7-1 登录日志

图 3-7-2 操作日志

图 3-7-3 安全日志

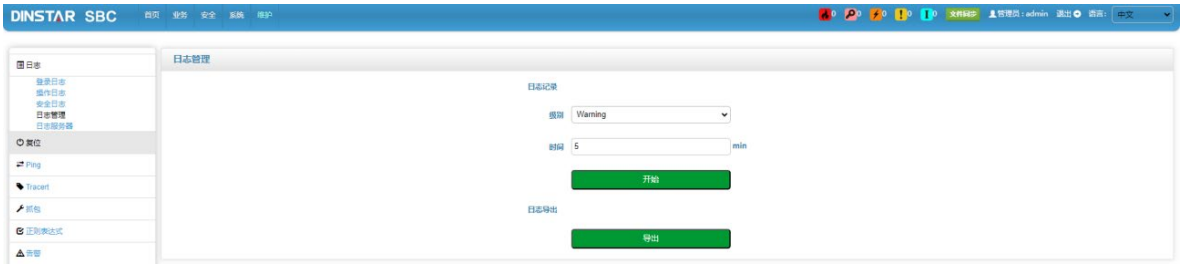


图 3-7-4 日志管理

图 3-7-5 日志服务器

表 3-7-1 日志服务器

参数	描述
级别	日志的级别，分别为 disable/emerg/alert/crit/err/warning/notice/info/debug
网络	配置协议类型，ipv4/ipv6
服务器地址	日志服务器的地址
端口	日志服务器监听端口，默认 514，不能修改
协议	网络协议，支持 UDP/TCP

3.7.2 复位

对设备的用户板、主控板和整机的复位。

图 3-7-6 复位

表 3-7-2 复位

参数	描述
用户板复位	可单独对某一个或者多个用户板进行复位
主控板硬复位	调用主控板系统的 reboot 命令，对主控板系统进行复位
主控板软复位	将主控板的相关进程 kill 掉进行复位
整机复位	主控板和用户板都复位。在调用主控板系统 reboot 命令前给用户板发送复位命令，然后再 reboot 主控板。

3.7.3 Ping

Ping 是对一个网址发送测试数据包，看对方网址是否有响应并统计响应时间，以此测试网络连接状态。Ping 发送一个 ICMP 回声请求消息给目的地并报告是否收到所希望的 ICMP 回声应答。

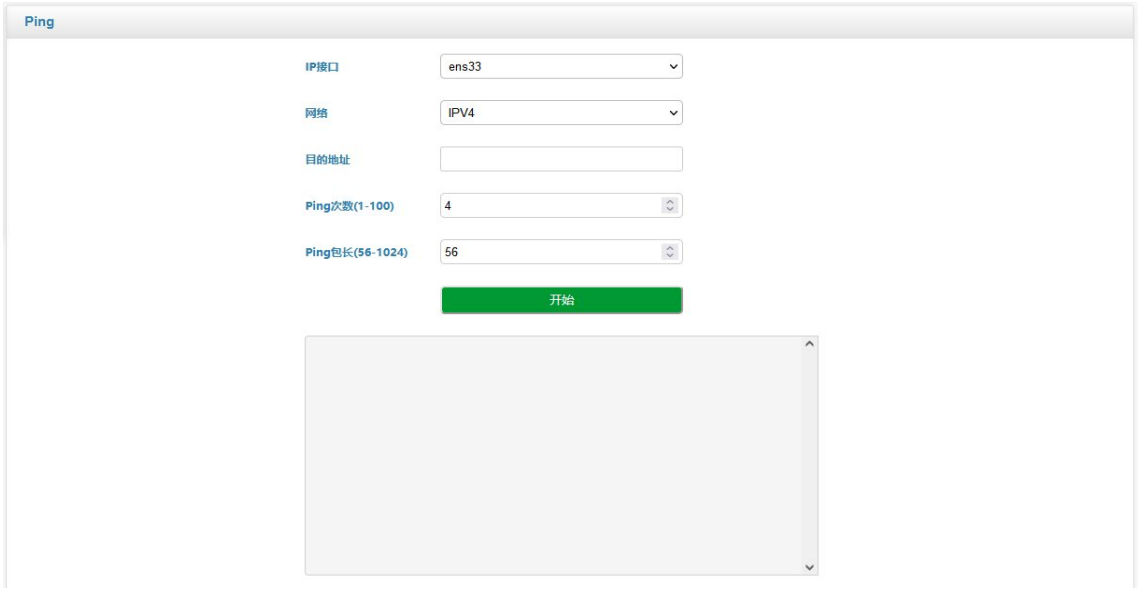


图 3-7-7 ping

表 3-7-3 ping

参数	描述
IP 接口	选择进行 ping 测试的网络接口
网络	选择网络类型，ipv4/ipv6
目的地址	Ping 测试的目的 IP 或者域名
Ping 次数	发送 ping 包的次数
Ping 包长	发送的 ping 包的长度

3.7.4 Tracert

Tracert 命令详解：Tracert（跟踪路由）是路由跟踪实用程序，用于确定 IP 数据报访问目标所通过的的路径。Tracert 命令用 IP 生存时间 (TTL) 字段和 ICMP 错误消息来确定从一个主机到网络上其他主机的路由。

通过向目标发送不同 IP 生存时间 (TTL) 值的“Internet 控制消息协议 (ICMP)”回应数据包，Tracert 诊断程序确定到目标所采取的路由，要求路径上的每个路由器在转发数据包之前至少将数据包上的 TTL 递减 1。数据包上的 TTL 减为 0 时，路由器应该将“ICMP 已超时”的消息发回源系统。

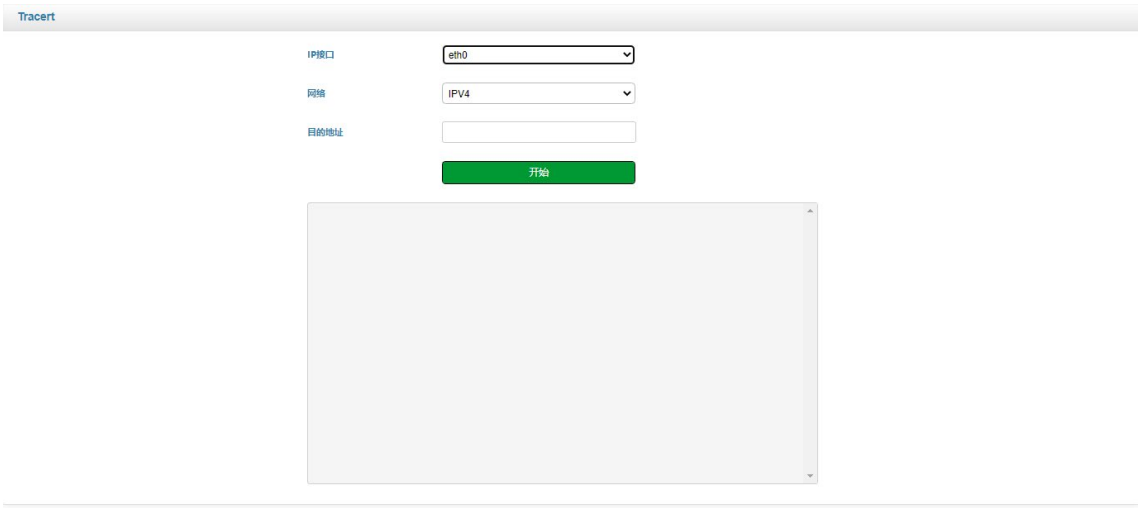


图 3-7-8 Tracert

表 3-7-4 Tracert

参数	描述
IP 接口	选择进行 Tracert 测试的网络接口
网络	选择网络类型，IPv4/IPv6
目的地址	Tracert 测试的目的 IP 或者域名

3.7.5 抓包

图 3-7-9 抓包

表 3-7-5 抓包

参数	描述
服务器类型	选支持本地服务器抓包和远程服务器抓包，远程服务器抓包需要相应的抓包工具配合

过滤组类型	选择本地服务器抓包，默认自定义输入值，另外可选择精准匹配/MFU0/MFU1/MFU2/MFU3,根据不同的过滤条件进行抓包。 自定义输入值：匹配端口范围、网络、源 ip、目的 ip 和协议的抓包 精准匹配：抓取匹配上主叫号码、被叫号码和入局端点的呼叫 选择 MFU0/MFU1/MFU2/MFU3:网络、源地址、目的地址和协议匹配的选择 MFU 上的呼叫抓包
端口范围	过滤组选择自定义抓包的端口范围
网络	可选择抓包的网络为 IPv4 或者 IPv6
源 IP	抓包的源 IP 地址
目的 IP	抓包的目的 IP 地址
协议	默认全勾选，支持 TCP、UDP、ICMP 和 ARP
时间	抓包的时长
文件最大值	抓包文件最大值，超过最大值删除前面时间的内容
远端服务器抓包	网络：SBC 和远端服务器网络，可选择 IPv4 和 IPv6； 服务器地址和端口， 接口：SBC 连接远端服务器的网口 本地端口：SBC 本地监听端口 服务器心跳端口：和 SBC 发送心跳消息的服务器端口 过滤组：根据不同的过滤组进行抓包

说明：

多个 IP 地址，可以用 | 号隔开；抓到的报文后可以保存到电脑上，然后用抓包工具打开分析。

该抓包工具不能抓 RTP 包，如果要抓 RTP 包，请用镜像交换机用 PC 机抓包！

注意：

因为 SBC3000 Pro 设备的呼叫量可能会非常大，为了避免因为抓包导致系统内存不够而崩溃，抓包时，一定要输入具体的源和目的 IP 地址和端口，并选择指定协议类型抓包，抓包时间不宜过长。

3.7.6 正则表达式

用于进行正则表达式测试，验证用户的正则表达式是否正确，是否能够正确匹配。

图 3-7-10 正则表达式

3.7.7 告警

显示系统的告警，可通过条件筛选。全部确认后告警消失。

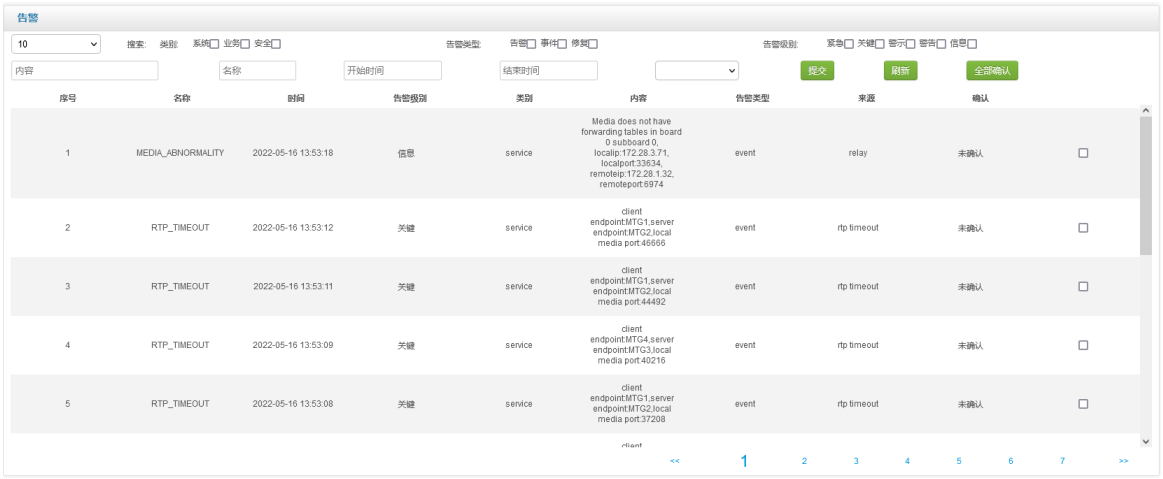


图 3-7-11 告警

3.7.8 SNMP 配置

用于连接 SNMP 服务器，进行远程设备管理。

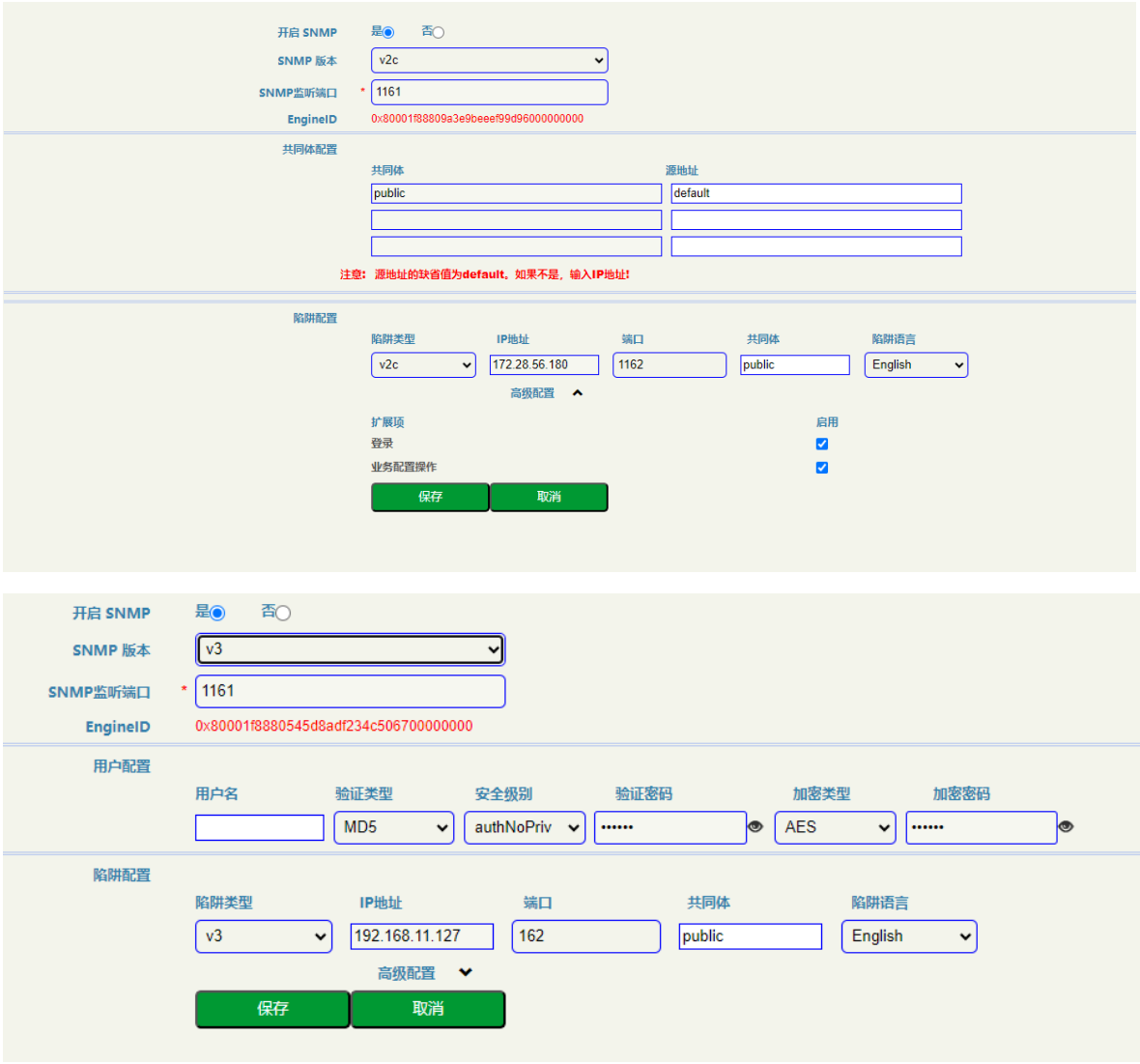


图 3-7-12 SNMP 配置

表 3-7-6 SNMP 配置

参数	描述
SNMP 版本	支持 V1,V2C 和 V3
SNMP 监听端口	使用 SNMP 连接 SBC 的监听端口
共同体配置	共同体：加入的共同体名称 源地址：默认为 default，所有 ip 均可通过 snmp 连接 SBC 设备；填写具体的 ip 地址仅填写 ip 地址可 snmp 连接 SBC。

陷阱配置	陷阱类型：跟随 SNMP 版本的配置，支持 V1,V2C 和 V3 IP 地址：接收 SBC 推送 SNMP trap 消息的地址 端口：接收 SBC 推送 SNMP trap 消息的端口 共同体：共同体名称 陷阱语言：默认为英文，可选择中文。
扩展项	登录：默认不启用，启用后登录和退出设备均会推送相应的 trap 消息 业务配置操作：默认不启用，启用业务配置时会推送相应的 trap 消息
用户配置	SNMP 配置 V3 才会有。 用户名：SBC 与 SNMP 服务器之间认证的名称，用户自定义； 验证类型：支持 MD5 和 SHA 安全级别：可选择 authPriv 和 authNoPriv 验证密码：验证密码 加密类型：支持 DES、AES 和 AES128

3.7.9 NMS 服务配置

用于连接 NMS 服务器，进行远程设备管理。

图 3-7-13 NMS 服务配置

表 3-7-7 NMS 服务配置

参数	描述
请求方式	SBC 和 NMS 服务器交互使用的协议，http/https。http 协议存在安全问题，请谨慎使用。

NMS 服务器地址	NMS 服务器的 IP 或者域名
NMS 服务器端口	NMS 服务器的监听端口
接口	和 NMS 服务器交互的网络接口
设备端口	SBC 的 nms 服务监听端口
日志最大占用空间	SBC 和 NMS 交互日志最大文件大小
日志文件最大数量	SBC 和 NMS 交互日志最大数量
协议版本号	https 的协议版本号

3.7.10 信令跟踪配置

用于连接信令跟踪服务器，将 SBC 的信令信息推送到信令跟踪服务器，便于问题定位。

图 3-7-14 信令跟踪配置

表 3-7-8 信令跟踪配置

参数	描述
启用	默认不启用，勾选后可配置其他参数
接口	SBC 和信令跟踪交互的接口
设备端口	SBC 和信令跟踪交互的监听端口
远端地址	信令跟踪工具的地址（这个地址可以是任意地址只用于下发规则）

3.7.11 Webrtc

SBC3000 Pro 的 web 集成了 webrtc 客户端界面，用于 webrtc 客户端使用。

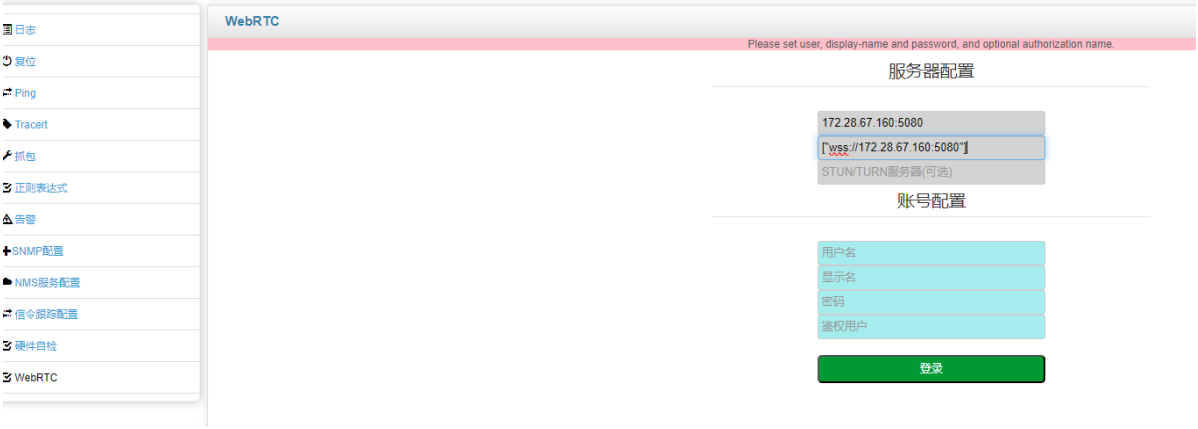


图 3-7-15 webrtc 配置

表 3-7-9 webrtc 配置

参数	描述
SIP 域名	该客户端向注册的 SIP 域名，例如 172.28.67.160:5080
SIP 服务器地址	该客户端向注册的 SIP 域名,例如["wss://172.28.67.160:5080"]
账号配置	向 SIP 服务器注册的用户名、显示名、密码和鉴权用户名

4 术语

SBC：会话边界控制器（Session Border Controller）

SIP：会话发起协议（Session Initiation Protocol）

DTMF：双音多频（Dual Tone Multi Frequency）

NAT：网络地址转换（Network Address Translation）

VLAN：虚拟局域网（Virtual Local Area Network）

附录 【跟踪命令】

一、en 模式下常用命令：

Welcome to Command Shell!

Username:admin

Password:*****

ROS>en

ROS#

1、查看系统当前时间，启动时间和运行时间 ROS#sh clock

2、查看各用户板状态 enable# show board state

3、查看 dsp 信息 enable#sh dsp info

4、查看当前呼叫 enable#Show call info

5、查看系统时间 enable#show date

6、查看产品型号和序列号 enable# show device

7、查看接入网/接入网中继/核心网中继状态 enable# show endpoint callstat

8、查看系统故障日志 enable# show error

9、查看系统内存使用情况 enable# show flash

10、查看网络 IP 信息 enable# show interface

11、查看网络端口信息 enable# show netstat

12、查看用户注册状态 enable# show register info

13、查看系统服务运行状态 enable# show service

14、查看系统运行时间 enable# show uptime

15、查看系统版本 enable# show version

二、常用跟踪命令

SSH 登录后

Username: admin

Password:

> enable

admin@SBC3000 Pro enable#

1、打开跟踪开关　enable # trace ？

all　打开全部跟踪

board　打开用户板跟踪（输入？可以查看后续参数）

call　打开呼叫跟踪（后面还有四个参数 主叫号码 被叫号码 呼入中继名称 呼出中继名称； *代表任意）

level　设置跟踪等级 (disable/emerg/alert/crit/err/warning/notice/info/debug/detail))

register　打开注册跟踪（后面还有三个参数 用户名 接入网名称 核心网名称； *代表任意）

transport　打开传输跟踪(后面还有六个参数 传输协议 源 IP:端口 目的 IP:端口 主叫号码 被叫号码 SIP 方法，输入？可以查看后续参数说明）

2、进入跟踪　enable#ada

3、退出跟踪　ada> exit

4、查看进程占用情况　enable#top

5、查看系统进程　enable #ps

6、重启设备　enable #reboot system

7、重启用户板　enable #reboot board [0-3]

8、关闭跟踪　enable #no trace all