DINSTAR 股票代码:870319 鼎信通达

SBC300 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
联系电话：0755-61919966
地址：深圳市南山区常兴路国兴大厦9楼

前言

欢迎选购

欢迎您选购鼎信通达 SBC300 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 SBC300 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 SBC300 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 SBC300 会话边界控制器的工程师

修订记录

文档名字	文档版本	软件版本
SBC300 会话边界控制器用户手册	V1.0 (2018/09/06)	1.91.1.1

文档约定

本文档中所提及的系统或设备均指 SBC300 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。

目录

1 产品概述

1.1 产品简介

随着通信网络融合与 ALL IP 发展趋势，越来越多的企业开始采用 IP-PBX、软交换、MCU 等产品技术构建内部 IP 通信系统，以降低通信成本、实现灵活部署、提供新业务功能，提升企业内外部沟通效率与核心竞争力。

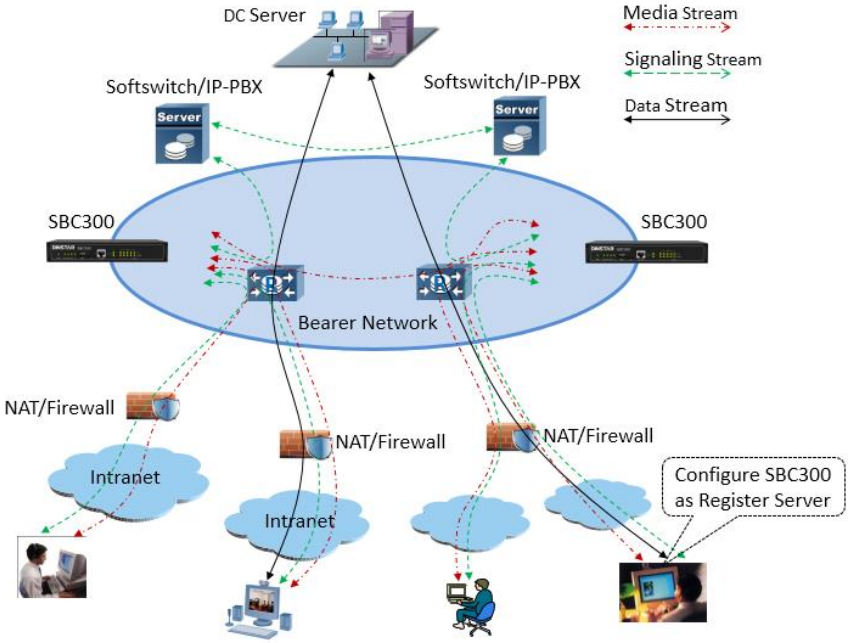
IP 通信系统为用户带来诸多便利的同时，也造成了一些其他麻烦。其中在复杂网络情况下的 IP 多媒体业务 NAT 穿越、终端用户的安全接入是许多企业建设管理 IP 通信系统时非常困扰的问题。

SBC300（Session Border Controller，会话边界控制器）相关解决方案能够低成本解决针对企业 IP 通信系统建设实施的两大问题：终端接入安全和 IP 多媒体业务 NAT 穿越。SBC300 采用了分布式的多核处理器、无阻塞千兆交换网架构和嵌入式 Linux 操作系统，在实现高性能的同时具有极低的功耗。其支持高达 500 并发会话和 200 路语音媒体转码处理，并支持 SIP over TLS、SRTP 加密会话。除了传统电信编解码，媒体处理还支持 AMR、OPUS 和 iLBC 等无线和互联网编解码转换。

1.2 应用场景

SBC300 会话边界控制器的应用场景如下图所示：

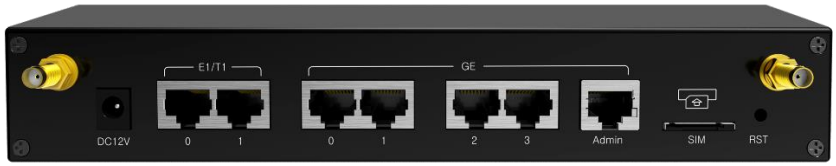
图 1-1 SBC300 应用场景



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（1s）	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(GE/Admin)	网口绿灯(Link)	快闪	网络连接正常
		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
E1/T1	E1/T1状态指示灯	预留（to do）	预留(to do)

1.5 功能和特性

1.5.1 系统功能

- 支持 3000 个 SIP 用户注册，最大 20/S 用户注册
- 支持 300 路媒体转发，最大 20/S 媒体转发，支持媒体加密
- 支持 120 路媒体和传真转码
- 支持多软交换和软交换防封杀，拓扑隐藏
- 灵活的路由规则配置，支持正则表达式，支持黑白名单
- 防 DOS/DDOS 攻击，支持防 IP 地址欺骗、非法 SIP/RTP 等报文攻击
- 支持带宽限制，支持动态黑名单
- 支持 VLAN、QoS、静态路由、NAT 穿透
- 支持登录用户分级管理，支持远程升级、配置导入导出
- 详细的系统用户安全日志和通话记录
- 友好的 Web 用户管理界面，提供多种管理方式
- 支持双机热备
- 支持批量账户创建和注册
- 支持 SIP 标准协议、传输协议 UDP/TCP/TLS
- WebRTC 网关（TBD）
- 视频业务（TBD）

1.5.2 语音特性

- 语音编码：PCMA，PCMU，G.723.1， G.729A/B，iLBC_13K，iLBC_15K，OPUS,G.726
- 传真：T.38 和 Pass-through
- DTMF 模式：RFC2833/Signal/Inband
- 智能媒体处理
- RTP 断流检测
- RTP 单通检测
- RTCP 报告

1.5.3 业务路由

- 内嵌业务路由引擎

- 支持多种灵活选路策略
- SIP 中继路由支持主备、负载均衡
- 支持号码变换

1.5.4 协议

- SIP V2.0 RFC3261
- SDP RFC2327
- RTP/RTCP
- HTTPS
- DNS
- DHCP
- NTP

1.5.5 安全

- 注册流控
- 呼叫流控
- 内嵌 VOIP 防火墙
- 拓扑隐藏
- 防 DOS 攻击
- 畸形报文检测与处理
- TLS 信令加密
- 媒体加密 SRTP
- 黑白名单
- ACL

1.5.6 管理维护

- 远程升级
- WEB 管理
- SSH/TELNET 命令行
- 配置导入导出
- 告警
- 日志

- 统计
- 多语言支持（中英文）
- SNMP
- TR069
- DMCloud （Dinstar NMS）
- DRP 远程 web/CLI
- 网络工具：Ping 和 Tracert
- 网络抓包

1.5.7 物理规格

- 提供 4 个 10/100/1000 Base-T 网口
- 提供 1 个 Console 口、1 个 Admin 口、1 个 USB 口
- 支持 2 个 E1
- 支持 LTE
- 支持电源状态监控
- 支持双电源接入
- 尺寸：437*300*44.4mm(1U)
- 净重：4.5kg

1.5.8 工作环境

- 电源：输入 AC100-240VAC，50-60 Hz
- 最大功耗：12W
- 网络接口：10/100/1000M 自适应 GE 口
- 操作温度：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 SBC300 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 SBC300 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 SBC300；
- 佩戴防静电手腕；
- 确认 SBC300 正确接地；
- 正确连接 SBC300 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 SBC300 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 SBC300 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 SBC300 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 SBC300，通常包含以下配置：

- SBC300 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

SBC300 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 SBC300 的两侧；
2. 将 SBC300 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 SBC300 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

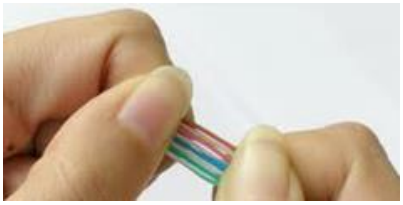
2.3.1 注意事项

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。

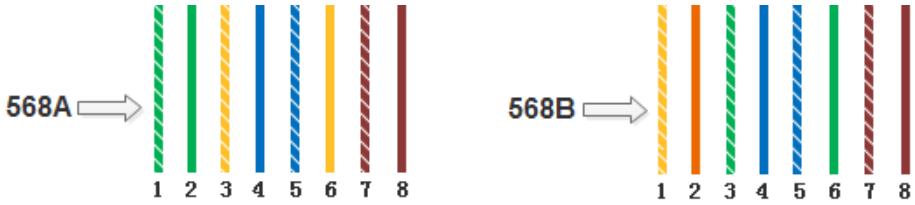
2.3.2 网线制作

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。

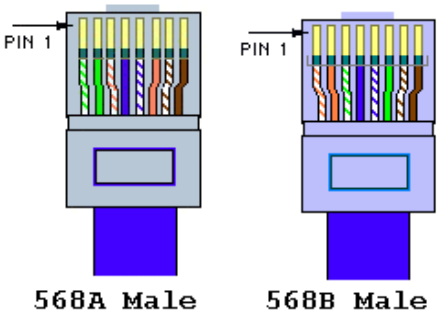


PIN1线序左起为：白绿、绿、白橙、蓝、白蓝、橙、白棕；PIN2线序左起为：白橙、橙、白绿、蓝、白蓝、绿、白棕、棕。

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

SBC300 提供 5 个 GE 网口，分别是 Admin、GE0、GE1、GE2 和 GE3，其中 Admin 是管理网口，其他 GE 网口为业务网口，建议使用业务网口与千兆以太网相连接，使 SBC300 设备工作在最优的网络环境中。

对 SBC300 设备的管理既可通过管理网口进行(需要通过 Web 打开相应权限)，也可以通过业务网口进行。当需要隔离设备的管理和设备的业务处理时，才使用管理网口。一般情况下，只使用业务网口连接以太网进行对设备的管理。

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 SBC300 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

SBC300 提供 5 个千兆以太网网口，分别是 Admin、GE0、GE1、GE2 和 GE3，其中 Admin 是管理网口，其他 GE 网口为业务网口，带宽默认自动适应。Admin 网口默认 IP 为 192.168.11.1，GE0、GE1、GE2 和 GE3 的默认 IP 分别是 192.168.12.1、192.168.13.1、192.168.14.1 以及 192.168.15.1。

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 SBC300 的 Admin 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，只能通过 Admin 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 Admin 网口进入 Web 页面，然后在“安全→访问控制”页面里打开其它网口的访问权限，如果需要 Ping 其它网口，则需在“安全→系统安全”页面里将外网 Ping 请求响应开启。

3.1.2 登录

在浏览器中用 https 方式输入 Admin 网口的默认 IP 地址，即 https:// 192.168.11.1，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#。

SBC300 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 SBC300 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、系统信息、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 

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 SBC300 正常的流程是如下图：

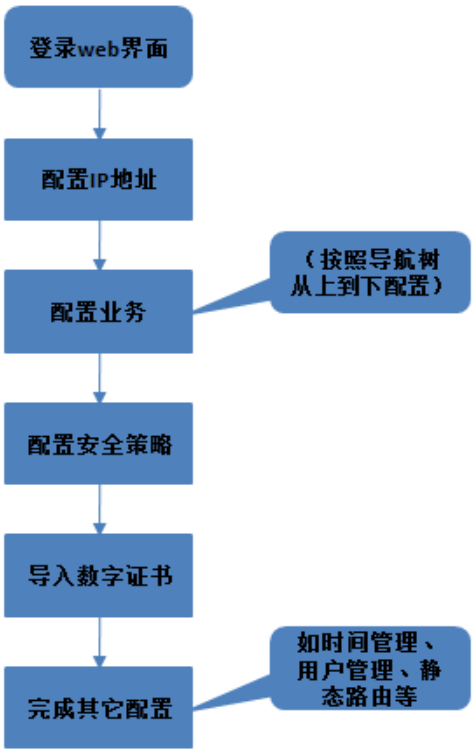


图 3-2-2 配置流程

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、系统信息、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

每秒呼叫次数	当前时间每秒新增的呼叫次数
峰值每秒呼叫次数	从系统启动运行到现在最大的每秒新增呼叫次数
当前呼叫数	当前正在通话的呼叫次数
平均呼叫接通率	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
每秒注册数	当前时间点每秒新增的注册请求次数
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次数
当前用户数	当前注册成功并在线的用户总数
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 系统信息的描述

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

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（Admin/GE0/GE1/GE2/GE3）	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

设备型号	该产品的设备型号为 SBC300
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	SBC300 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

如果已同步过系统时间，但每次系统启动后当前时间仍然不正确，则表示设备内置电池亏电，需要更换电池；另外，NTP 时间同步，只能通过 Admin 网口进行时间同步。

3.3.2 接入网状态

接入网用于终端用户向 SBC300 设备注册，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

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
转码连接数	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、转码连接数、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

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次数
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
转码连接数	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、转码连接数、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

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次数
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
转码连接数	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、转码连接数、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 3-3-6 呼叫状态

表 3-3-8 呼叫状态描述：

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
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
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	该呼叫通过接入网中继、核心网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，来源和目的的编解码会不一致
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

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。

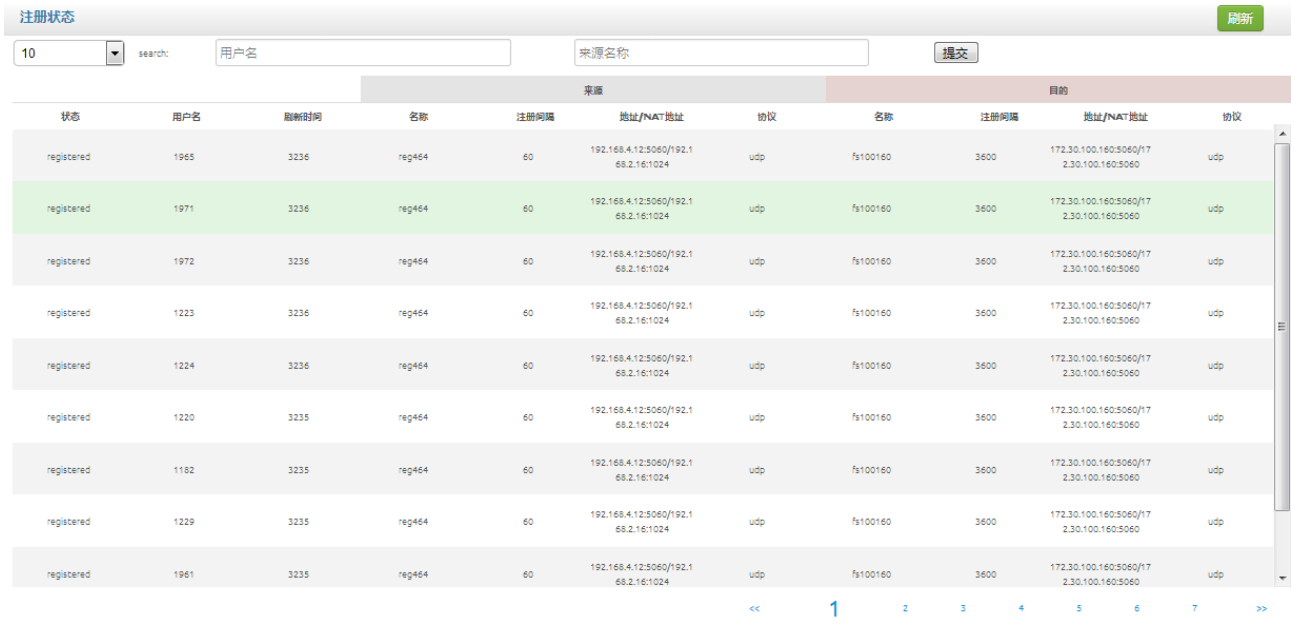


图 3-3-7 注册状态

表 3-3-9 注册状态描述

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
刷新时间	SBC 设备需要向服务器刷新注册的剩余时间
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那个核心网中继注册的
注册间隔	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

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 3-3-8 注册列表

表 3-3-10 攻击列表描述

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

3.4 业务配置

3.4.1 业务管理

图 3-4-1 业务管理

业务管理现只有启用/禁用媒体故障检测，如果启用，SBC300 设备会监控每通通话的 rtp 报文，如果在检测时间间隔内都未收到/发送 rtp 报文，SBC300 会将该通话拆除。

3.4.2 话单管理

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。

图 3-4-2 启用话单服务器

图 3-4-3 话单配置

表 3-4-1 话单管理

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
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，有 UDP 和 TCP 两种
编码格式	话单的编码格式，目前只支持 json

3.4.3 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。

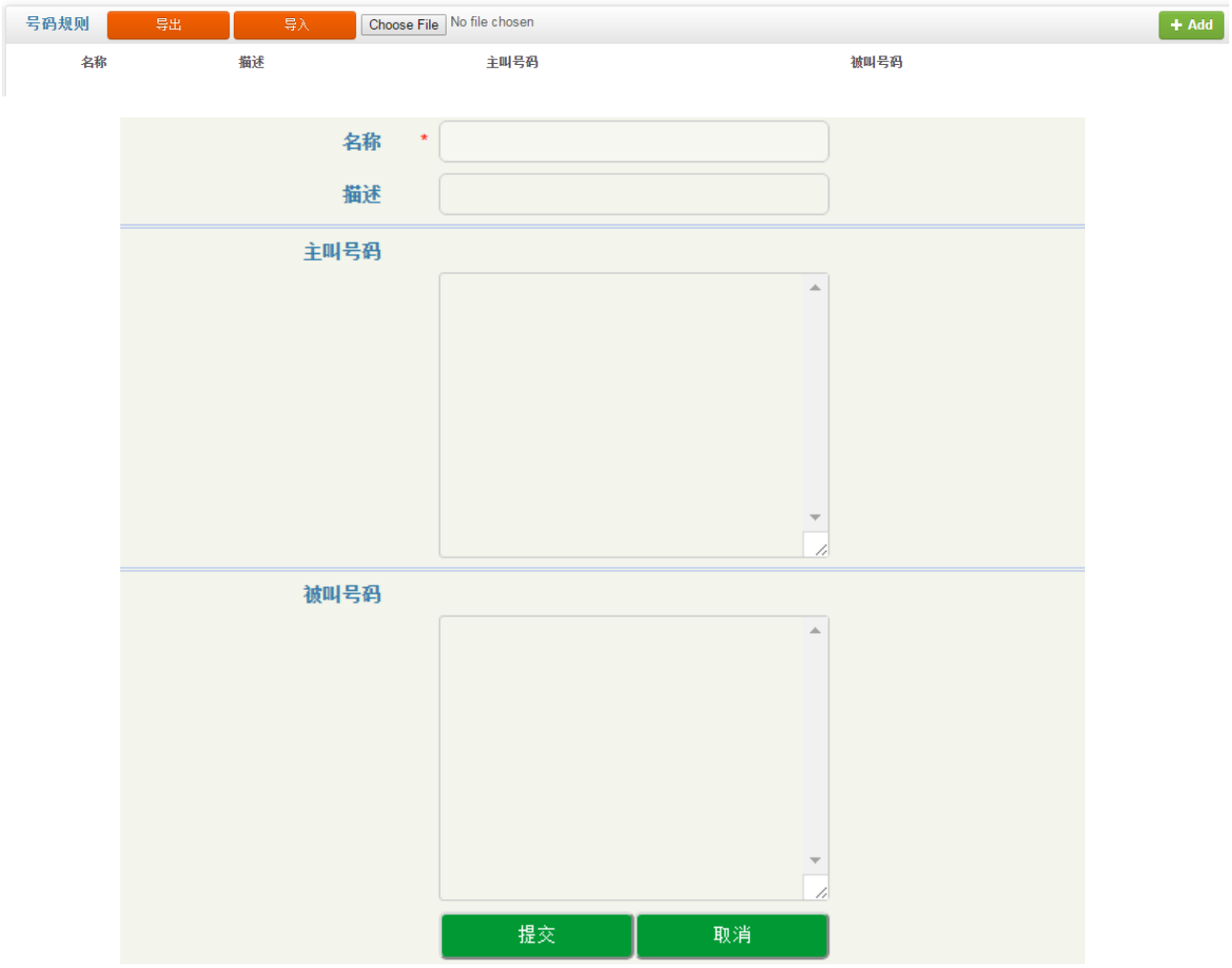


图 3-4-4 添加号码规则

表 3-4-2 号码规则相关参数描述

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	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	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

3.4.4 路由时间

路由时间页面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 3-4-5 路由时间配置

表 3-4-3 路由时间相关参数描述

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

3.4.5 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 3-4-6 速率控制页面

表 3-4-4 速率控制相关参数的描述

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。

3.4.6 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 设备是否接受该号码的呼叫和注册。

图 3-4-7 黑名单页面

图 3-4-8 白名单页面

表 3-4-5 黑白名单相关参数描述

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，不支持正则表达式
描述	该条黑/白名单号码的具体描述

3.4.7 编解码分组

SBC300 设备支持 G729、G723、PCMU、PCMA、ILBC_13K、ILBC_15K、OPUS、AMR 和 G726 这几种编解码，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 3-4-9 编解码分组页面

表 3-4-6 编解码分组

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	SBC300 设备支持的编解码一共有以下几种： PCMA，PCMU，G.729A/B, G.723, iLBC,_13K, iLBC_15K, AMR, OPUS, G.726
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

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。

3.4.8 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 3-4-10 号码变换页面

表 3-4-7 号码变换

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

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。

3.4.9 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 3-4-11 号码池设置

表 3-4-8 号码池相关参数描述

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
主叫/被叫变换规则	当此处设置的前缀匹配同一路由出局的主叫或被叫号码，主叫或被叫号码会被号码池的号码随机替换。 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

3.4.10 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 3-4-12 SIP 头域修改页面

表 3-4-9 SIP 头域修改

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
目标标识	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。

3.4.11 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。

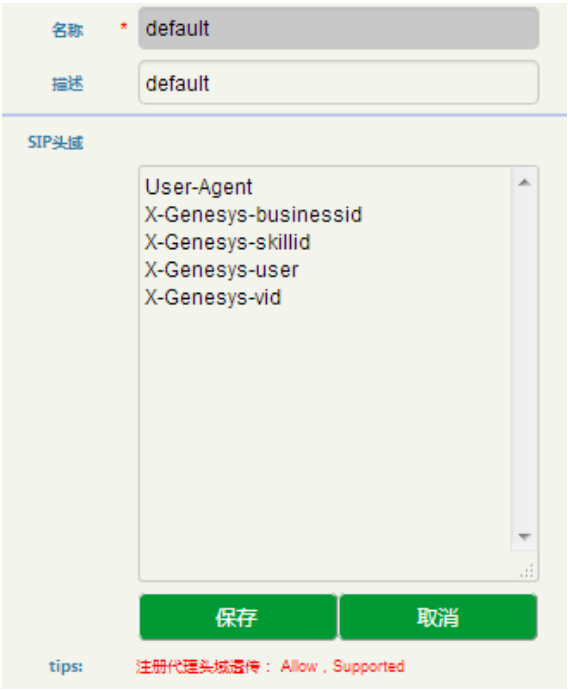


图 3-4-12 SIP 头域透传页面

表 3-4-10 SIP 头域透传

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, Auto-Defined。

3.4.12 接入网

接入网用于配置允许配置终端通过 SBC 向软交换注册的接入域和各种参数。

图 3-4-13 接入网页面

表 3-4-11 接入网

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
接口	接入网配置的接口为 eth0、eth1 或 VLAN 接口
端口	该接入网在本设备 eth0 口上的 SIP 监听端口，端口号在 eth0 口上唯一
网络	配置该接入网采用的是 IPV4 还是 IPV6 网络，默认为 IPV4
协议	该接入网采用的传输协议:UDP/TCP/TLS

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
信令 QoS	SIP 信令报文 QoS 标志配置
媒体 QoS	媒体报文 QoS 标志配置
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（说明）
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 3.4.5 速率控制
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 3.4.7 编解码分组
黑名单	配置不允许从该接入网呼入时主叫号码黑名单，如果接入网配置了黑名单，在黑名单内的主叫号码都不能通过该接入网呼入，参考 3.4.6 黑白名单
白名单	配置允许从该接入网呼入时主叫号码白名单，如果接入网配置了白名单，只有白名单内的主叫号码才能通过该接入网呼入，参考 3.4.6 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 3.4.8 号码变换
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
入局 SIP 消息变换	即从该接入网呼入时的 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
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。
PRACK	PRACK 是 SIP 消息中保证临时消息(101-199)可靠传输的机制，可参考 RFC3262 文档。配置为 disable 时，SBC 发送的请求或 1xx 响应默认都不带 100rel；配置为 support 时，SBC 的请求或 1xx 响应会在 supported 域里带上 100rel；配置为 require 时，SBC 的请求或 1xx 响应会在 require 域带上 100rel，

	如果对端不支持，则响应 420，如果支持，则会在收到 1xx 响应时，发送 PRACK 消息回来。
From 头域	Fom 头域采用的是对端的域名或者本地域名，默认为本地域名。
远端媒体地址	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
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：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：提取 invite 报文 to 域中 display 字段作为被叫 request-uri：提取 invite 报文 request-uri 的中的 user 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 32768，如果防火墙将 32768-50000 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 32768 为基准，根据防火墙端口映射规则进行基准偏移。

3.4.13 接入网中继

配置 SBC 设备通过中继对接到接入网终端的服务器和相关参数。


名称 * ag244
描述
接口 eth0
协议 UDP
端口 * 5100
网络 IPV4
信令DSCP BE
媒体DSCP BE
近端NAT
速率控制 default
编解码 default
黑名单
白名单
入局号码变换
DTMF类型 * RFC2833
RFC2833净荷 * 101
入局SIP消息变换

图 3-4-14 接入网中继页面

表 3-4-12 接入网中继

名称	配置接入网中继的名字，用户自定义，添加成功后不可修改
描述	该接入网中继的描述，用户可以较为详细描述该接入网中继的作用和规则
接口	接入网中继配置的接口为 eth0、eth1 或 VLAN 接口
端口	该接入网中继在本设备 eth0 口上的 SIP 监听端口，端口号在 eth0 口上唯一
网络	配置该接入网中继采用的是 IPV4 还是 IPV6 网络，默认为 IPV4
协议	该接入网中继采用的传输协议:UDP/TCP/TLS
信令 QoS	SIP 信令报文 QoS 标志配置
媒体 QoS	媒体报文 QoS 标志配置
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（参考接入网的 说明）

速率控制	配置该接入网中继每秒最大注册、呼叫量和总呼叫量，参考 3.4.5 速率控制
编解码	配置从该接入网中继呼入或呼出支持的编解码格式，参考 3.4.7 编解码分组
黑名单	配置不允许从该接入网中继呼入时主叫号码黑名单，如果接入网中继配置了黑名单，在黑名单内的主叫号码都不能通过该接入网中继呼入，参考 3.4.6 黑白名单
白名单	配置允许从该接入网中继呼入时主叫号码白名单,如果接入网中继配置了白名单，只有白名单内的主叫号码才能通过该接入网中继呼入，参考 3.4.6 黑白名单
入局号码变换	配置从该接入网中继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 3.4.8 号码变换
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
服务器地址类型	静态：需配置远端地址和端口，表示该中继对接到这个地址和端口上 动态：该接入网中继作为服务器，需配置验证的用户名和密码，远端设备要通过指定的账户密码向该接入网中继和监听端口发起注册，注册成功，中继状态为 true，注册失败或未注册，中继状态为 false（参考 3.3.2 中继状态）
远端地址和端口	接入网中继对接对端设备的 IP 地址和监听端口，只有在远端地址类型为静态时显示
注册	只有在服务器地址类型为静态时显示。启用注册，则表示该接入网中继要根据配置的账户密码注册到远端地址和端口上，注册成功，中继状态为 true，注册失败，中继状态为 false（参考 3.3.2 中继状态）
心跳策略	不启用：系统不主动探测该接入网中继对端设备网络是否连通 启用：系统根据配置定期向对端发送 option 探测报文，如果收到响应，则表示与对端连接正常，中继状态为 true，如果连续超过配置次数都未收到响应报文，则表示与对端设备连接中断，中继状态为 false（参考 3.3.2 中继状态）
入局 SIP 消息变换	即从该中继呼入时的 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
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，必须要求被叫设备也支持 timer
PRACK	PRACK 是 SIP 消息中保证临时消息(101-199)可靠传输的机制，可参考 RFC3262 文档。配置为 disable 时，SBC 发送的请求或 1xx 响应默认都不带 100rel；配置为

	support 时，SBC 的请求或 1xx 响应会在 supported 域里带上 100rel；配置为 require 时，SBC 的请求或 1xx 响应会在 require 域带上 100rel，如果对端不支持，则响应 420，如果支持，则会在收到 1xx 响应时，发送 PRACK 消息回来。
From 头域	Fom 头域采用的是对端的域名或者本地域名，默认为本地域名。
远端媒体地址	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
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：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：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。

3.4.14 核心网中继

配置 SBC 设备通过中继对接到核心网的服务器和相关参数。

图 3-4-15 核心网中继页面

表 3-4-13 核心网中继

名称	配置核心网中继的名字，用户自定义，添加成功后不可修改
描述	该核心网中继的描述，用户可以较为详细描述该核心网中继的作用和规则
接口	核心网中继配置的接口为 eth0、eth1 或 VLAN 接口
端口	该核心网中继在本设备 eth1 口上的 SIP 监听端口，端口号在 eth1 口上唯一
网络	配置该核心网中继采用的是 IPV4 还是 IPV6 网络，默认为 IPV4
协议	该核心网中继采用的传输协议：UDP/TCP/TLS
信令 QoS	SIP 信令报文 QoS 标志配置
媒体 QoS	媒体报文 QoS 标志配置
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（参考接入网的  ）
编解码	配置从该核心网中继呼入或呼出支持的编解码格式，参考 3.4.7 编解码分组
黑名单	配置不允许从该核心网中继呼入时主叫号码黑名单，如果核心网中继配置了黑名单，在黑名单内的主叫号码都不能通过该核心网中继呼入，参考 3.4.6 黑白名单
白名单	配置允许从该核心网中继呼入时主叫号码白名单，如果核心网中继配置了白名单，只有白名单内的主叫号码才能通过该核心网中继呼入，参考 3.4.6 黑白名单
入局号码变换	配置从该核心网中继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 3.4.8 号码变换
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
服务器地址类型	静态：需配置远端地址和端口，表示该中继对接到这个地址和端口上 动态：该核心网中继作为注册服务器，需配置验证的用户名和密码，远端服务器要通过指定的账户密码向该核心网中继和监听端口发起注册，注册成功，中继状态为 true，注册失败或未注册，中继状态为 false（参考 3.3.2 中继状态）
远端地址和端口	核心网中继对接服务器的 IP 地址和监听端口，只有在远端地址类型为静态时显示
注册	只有在服务器地址类型为静态时显示。启用注册，则表示该核心网中继要根据配置的账户密码注册到远端地址和端口上，注册成功，中继状态为 true，注册失败，中继状态为 false（参考 3.3.2 中继状态）
心跳策略	不启用：系统不主动探测该核心网中继对端设备网络是否连通

	启用：系统根据配置定期向对端发送 option 探测报文，如果收到响应，则表示与对端连接正常，中继状态为 true，如果连续超过配置次数都未收到响应报文，则表示与对端设备连接中断，中继状态为 false（参考 3.3.2 中继状态）
入局 SIP 消息变换	即从该中继呼入时的 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
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，通过该核心网呼出时，必须要求被叫设备也支持 timer
PRACK	PRACK 是 SIP 消息中保证临时消息(101-199)可靠传输的机制，可参考 RFC3262 文档。配置为 disable 时，SBC 发送的请求或 1xx 响应默认都不带 100rel；配置为 support 时，SBC 的请求或 1xx 响应会在 supported 域里带上 100rel；配置为 require 时，SBC 的请求或 1xx 响应会在 require 域带上 100rel，如果对端不支持，则响应 420，如果支持，则会在收到 1xx 响应时，发送 PRACK 消息回来。
From 头域	Fom 头域采用的是对端的域名或者本地域名，默认为本地域名。
远端媒体地址	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
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：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：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	配置该核心网中继允许接收的 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。

3.4.15 路由规则

1. 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 3-4-16 中继组页面

表 3-4-14 中继组

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	分为接入网中继组和核心网中继组，参考 3.4.10 和 3.4.11
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，直道可用中继或无可用中继为止 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	接入网中继或核心网中继的名称

2、路由

图 3-4-17 路由页面

表 3-4-15 路由

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
号码集	选择路由时匹配的主被叫号码集合（参考 3.4.3 号码集），如果号码集选择为空，用户在下面主叫用户名和被叫用户名中配置主被叫号码的匹配条件
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	本条路由规则生效的时间段（参考 3.4.4 时间），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
来源类型	设置该路由的呼叫是从接入网侧还是核心网侧呼入的，如果是接入网侧呼入，呼出只能是核心网侧；如果是核心网侧呼入，呼出只能是接入网侧；
SIP 方法	该路由支持的 SIP 请求方法，如果为空，表示不限制
目的类型	设置经过该路由是从接入网侧还是核心网侧呼出的，如果是接入网侧呼入，呼出只能是核心网侧；如果是核心网侧呼入，呼出只能是接入网侧；
号码替换	通过该路由时是否启用号码替换规则（参考 号码替换），默认不启用，号码替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

接入网、接入网中继和核心网中继配置中也有号码替换，这些号码替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。

3.5 安全配置

安全配置用于配置 SBC 设备 GE0、GE1、GE2 和 GE3 侧的系统安全策略、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 SBC300 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

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
外网 ping 请求响应	指的是 eth0（GE0）的 ping 请求响应，默认不响应。
UDP-Flood 攻击防御	UDP-Flood 是一种 DOS 攻击，经常是利用利用大量 UDP 小包冲击系统设备，启用该攻击防御策略后，系统在 1 秒中内收到超过设置的 udp 报文，就会把超过的 udp 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-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
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

3.5.2 访问控制

设置设备的 WEB（https）和 SSH 访问控制端口，以及 GE0、GE1、GE2 和 GE3 网口的访问控制策略，网口默认不能通过 web 和 SSH 访问。

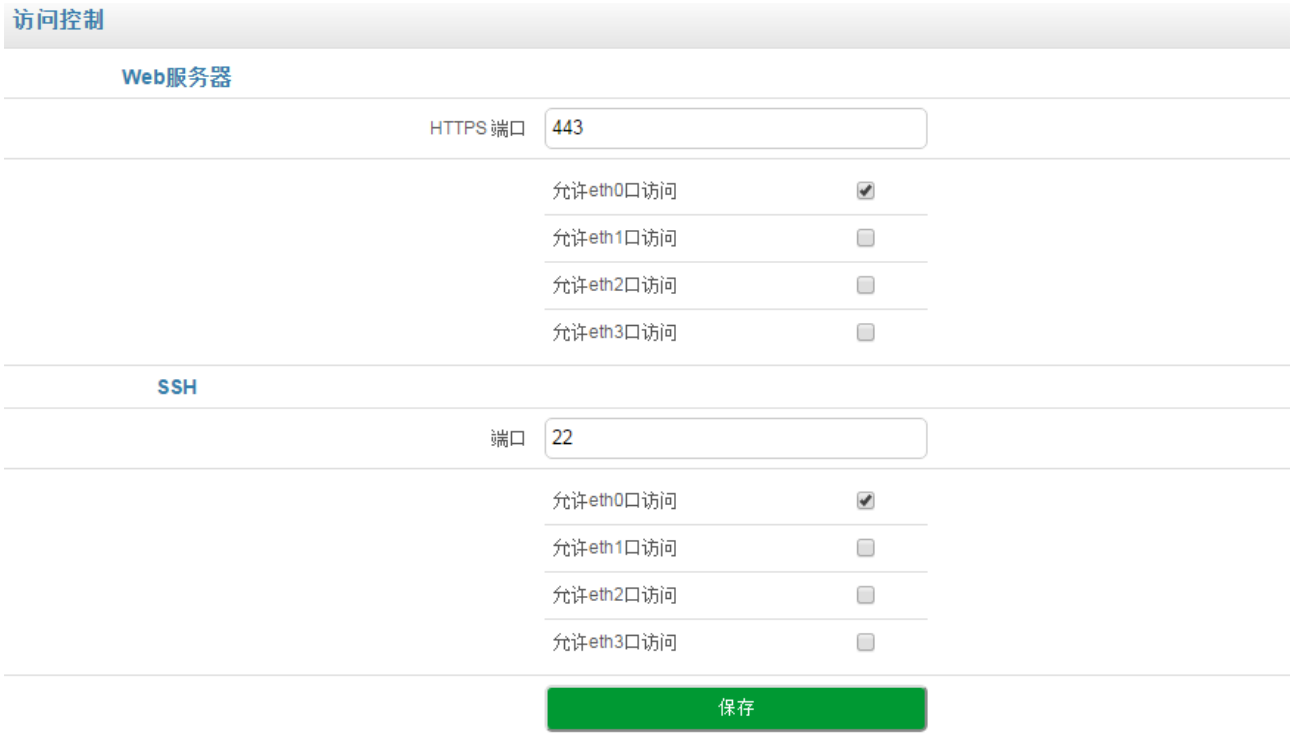


图 3-5-2 访问控制设置

表 3-5-2 访问控制

Web 服务器	HTTPS 端口：通过 web 的 https 协议访问时的端口，默认为 443，用户可以修改成其它端口； 设置是否允许其他设备通过 eth0、eth1、eth2 和 eth3 口以 Web 方式访问 SBC 设备，默认不允许
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 eth0、eth1、eth2 和 eth3 口以 SSH 方式登录 SBC 设备，默认不允许

3.6 防攻击策略

1. IP 防攻击策略

图 3-5-3 IP 防攻击策略

点击 

按钮添加 IP 防攻击策略，在这里也可以删除或修改 IP 防攻击策略。

图 3-5-4 添加 IP 防攻击策略

表 3-5-3 IP 防攻击策略

限制时间	IP 防攻击策略生效时的时间，一个策略生效时，超过限制时间后需要重新判断策略是否生效
优先级	优先级的数字越低，优先级等级越高
名称	IP 防攻击策略名称，添加后不可修改
类型	远端 IP：当某一个远端 IP 发过来的报文流量超过触发流量（KBPS）设定阈值或 CPU 使率超过设定阈值时，系统会根据动作对该该远端 IP 做相应的处理。 本地端口：当设置的本地端口收到的报文流量超过触发流量（KBPS）设定阈值或 CPU 使用率超过设定阈值时，系统会根据动作该端口做相应的处理
CPU 使用率	指的是系统的总 CPU 使用率，为空代表不判断 CPU 使用率

触发流量（KBPS）	允许接收远端 IP 或指定端口报文的最大流量阈值，超过该阈值，会根据动作做相应的处理
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

2. SIP 防攻击策略

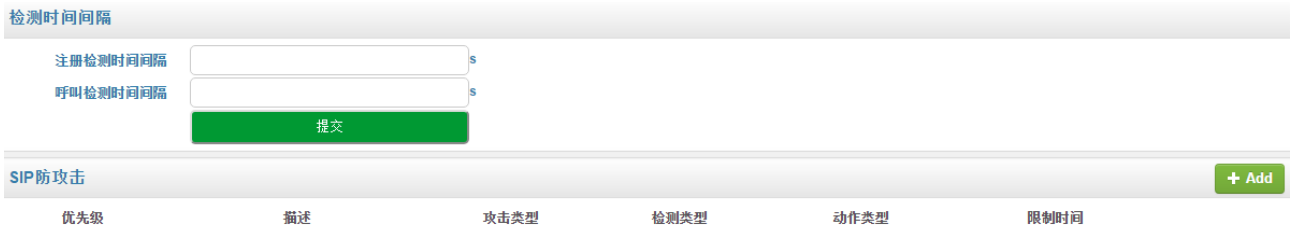


图 3-5-5 SIP 防攻击策略

点击 ADD 按钮添加 IP 防攻击策略，在这里也可以删除或修改 P 防攻击策略。

图 3-5-6 添加 SIP 防攻击策略

表 3-5-3SIP 防攻击策略

注册检测时间间隔	SIP 防攻击注册报文的检测周期
呼叫检测时间间隔	SIP 防攻击呼叫报文的检测周期
优先级	优先级的数字越低，优先级等级越高
名称	SIP 防攻击策略名称，添加后不可修改
攻击类型	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	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 REGISTER 报文做相应处理
接入端点	用户攻击检测的接入网，如果接入端点不配置，那么检测的是用户名，如果配置了接入网，那就是只对这个接入网进行规则匹配，参考 3.4.9 接入网
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 SIP 包流量限制，在限制时间内超过流量的 SIP 注册/呼叫报文全部丢弃 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 SIP 包速率限制，在限制时间内超过的 SIP 注册/呼叫报文全部丢弃 丢弃：该策略生效时，对该远端 IP 或设置的本地端口收到的 SIP 注册/呼叫报文，在限制时间内全部丢弃
时间	SIP 防攻击策略生效时的时间，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

3.7 系统

系统配置包括系统管理、接口管理、静态路由、用户管理、时间管理、版本升级、备份与恢复、License 管理、数字证书管理。

3.7.1 系统管理

系统管理用来配置 SBC300 设备的名称。

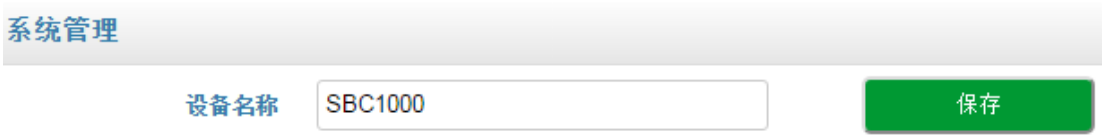


图 3-6-1 系统管理

3.7.2 接口管理

接口管理配置设备 admin、eth0、eth1、eth2 和 eth3 网口的 IP 地址、子网掩码、网关和 DNS 等，另外还可以添加 VLAN。

图 3-6-2 接口管理

图 3-6-3 GE0 的网口配置

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。

图 3-6-4 添加 VLAN 的网口配置

表 3-7-1 接口管理

VLAN ID	网络 VLAN 的 ID 号
接口	网络接口 eth0（GE0）或 eth1（GE1）
MTU 大小	网口发包时的 MTU 最大值，默认为 1500
优先级	当跨网段访问其他 IP 地址，如果对端地址没有在静态路由中，默认从优先级值最小的网口或 VLAN 出局访问
网络设置	该网络接口获取 IP 地址的模式，目前只支持静态 IP 地址模式
IP 地址	对应网络接口或 VLAN 的 IP 地址
子网掩码	对应网络接口或 VLAN 的子网掩码
网关	对应网络接口或 VLAN 的网关
DNS 服务器	对应网络接口或 VLAN 的 DNS 服务器地址

3.7.3 端口映射

为保证局域网的安全，USB1000 会阻断从因特网主动发起的连接请求。因此，如果用户想让因特网用户能够访问局域网内的主机，需要设置端口映射。

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 端口映射配置

表 3-7-2 相关参数描述

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
接入主机端口号	要访问内网的外网主机的端口号
协议	选择 TCP、UDP 或 TCP\UDP
目的主机 IP 地址	映射到外网的内网主机的 IP 地址
目的主机端口号	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）

3.7.4 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。点击 + Add 按钮，即进入静态路由设置页面。

图 3-6-6 静态路由配置

表 3-6-3 静态路由

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
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

3.7.5 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。

1. 密码设置

图 3-6-7 超级用户 admin 的密码设置

出于系统安全方面的考虑，建议设置较为复杂的密码。

2. 用户列表

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

图 3-6-8 添加用户及设置权限

表 3-6-4 用户列表

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

3.7.6 系统时间

在系统时间页面，用户可配置时区、当前时间和 NTP 服务器。

图 3-6-9 时间管理

表 3-6-5 时间管理

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

3.7.7 版本升级

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 3-6-10 版本升级

一般情况下，版本升级文件为 1.91.x.x.ldf 文件，请不要选择其它产品的版本文件进行升级。

3.7.8 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。

图 3-6-11 备份与恢复

表 3-6-6 备份与恢复

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	将配置数据恢复到设备的出厂默认值

3.7.9 双机热备

SBC300 支持双机热备。同样的业务在两台 SBC300 设备上互为主备状态（Active-Standby 方式）， 当其中一台 SBC300 设备发生故障，另一台 SBC300 会承担相应业务，从而保证呼叫等业务不断线。

3.7.10 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 SBC300 进行注册和呼叫。

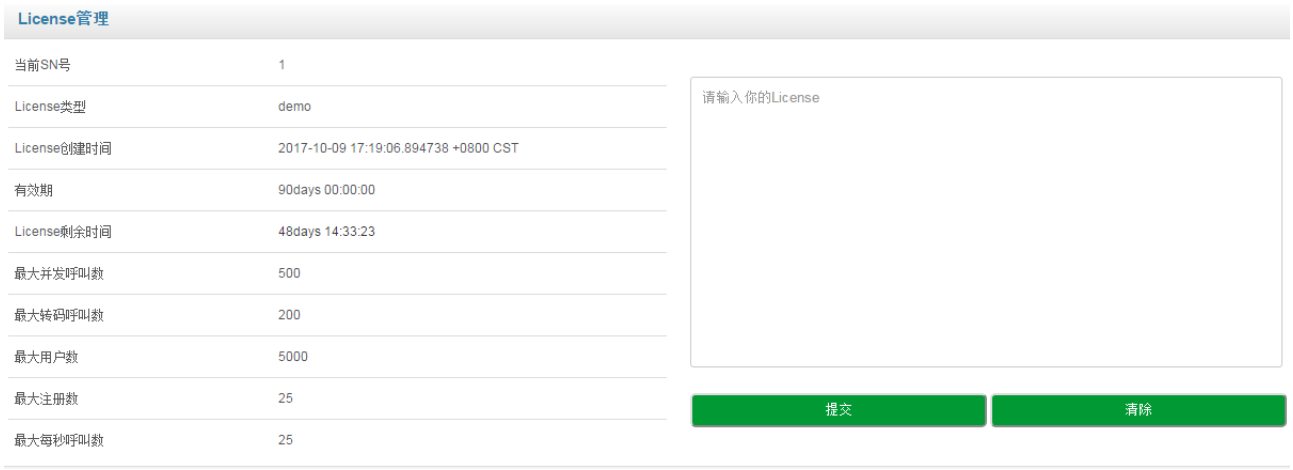


图 3-6-12 License 管理

3.7.11 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。

图 3-6-13 数字证书管理

3.8 维护

3.8.1 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，并且可以将这些日志导出到本机上。

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 日志导出

3.8.2 维护工具

维护工具可以复位设备系统和用户板、网络诊断 ping 和 tracert，并能根据条件进行抓包，方便定位问题。

1. 复位

图 3-7-5 复位

可以复位指定的业务板和系统，如果业务板出现故障，可以通过复位业务板尝试恢复，如果系统出现故障，可以通过系统复位尝试恢复。

2. ping

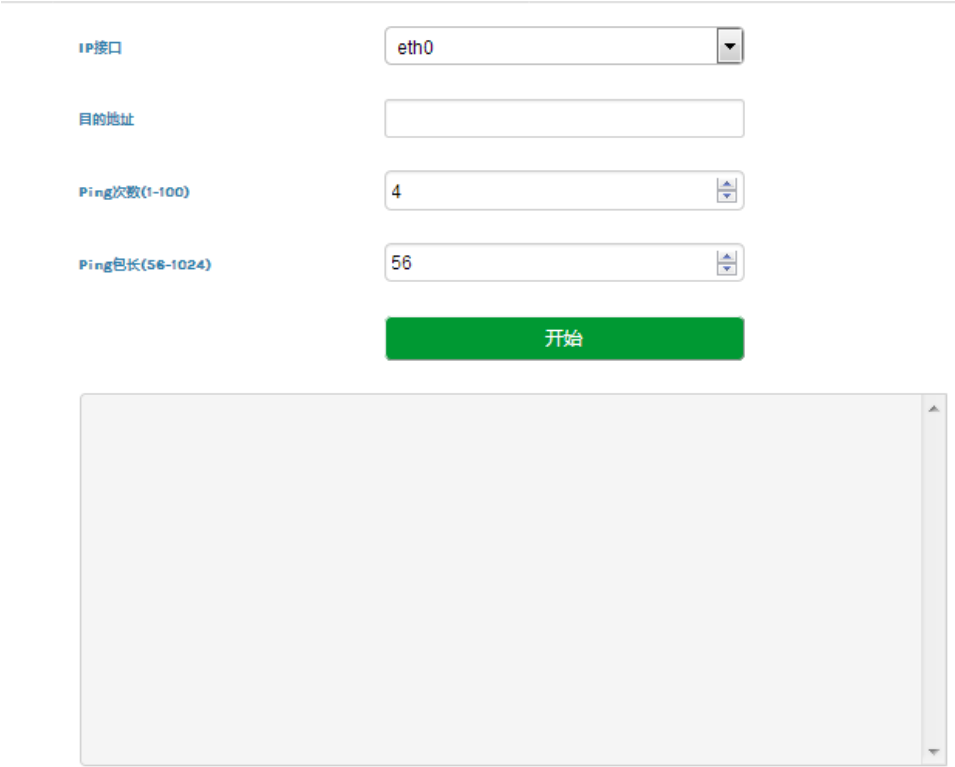


图 3-7-6 ping

Ping 命令详解：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。

应用格式：Ping IP 地址。它是用来检查网络是否通畅或者网络连接速度的命令。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。

Ping 命令使用说明：

1）选择要 ping 的网络接口 admin、eth0、eth1、eth2 或者 eth3；

2）在 ping 输入框内输入要 ping 的 IP 地址或者域名，并设置 ping 的次数和 ping 报文的长度，点击开始开始进行连通性检测；

3）收到全部响应报文表明网络连接正常，否则网络连接有故障。

3. tracert

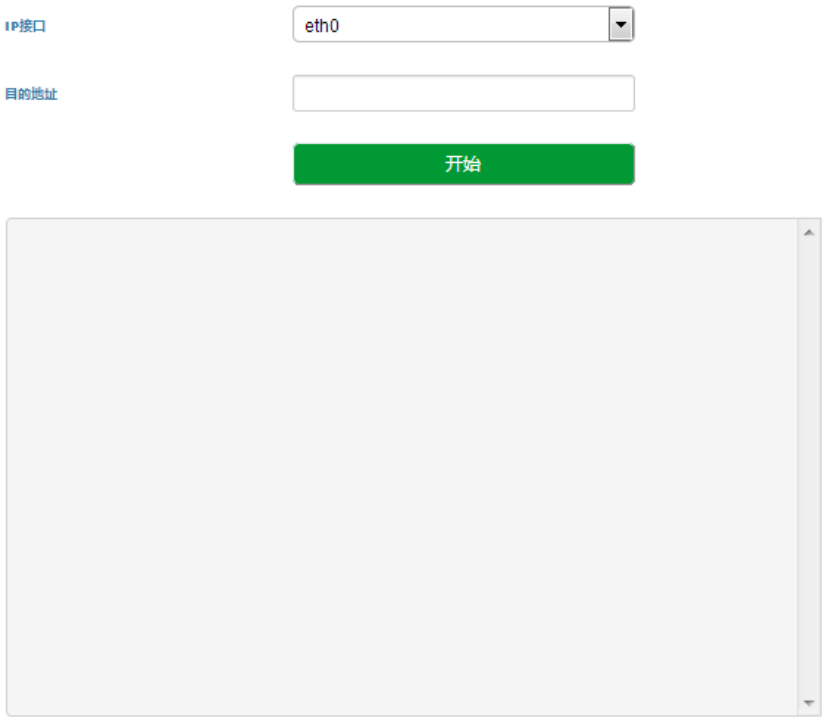


图 3-7-7 tracert

Tracert 命令详解：Tracert（跟踪路由）是路由跟踪实用程序，用于确定 IP 数据报访问目标所采取的路径。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。

Tracert 使用说明：

1）选择要 tracert 的网络接口 admin、eth0、eth1、eth2 或者 eth3；

2）在 tracert 输入框内输入 IP 地址或者域名，点击开始开始进行路由跟踪；

3）根据结果查看路由跟踪信息。

4、抓包

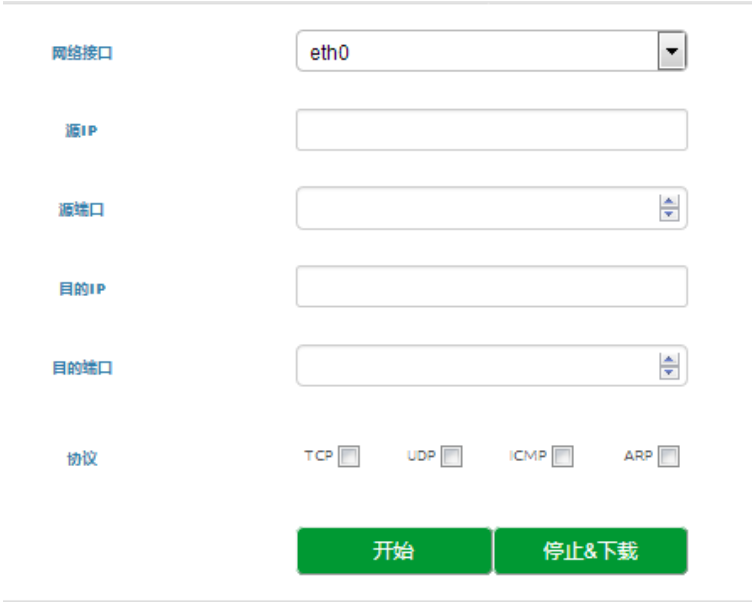


图 3-7-8 抓包

通过 WEB 页面抓取网口上的数据，可以根据配置得到具体某个 IP 地址和某个端口的报文。配置项包括：

1）选择要抓包的网络接口 admin、eth0、eth1、eth2 或者 eth3；

2）源 IP 地址；

3）源端口；

4）目的 IP 地址；

5）目的端口；

6）协议类型，协议类型有 TCP UDP ICMP ARP；

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 SBC300 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。

简单问题定位：

SBC 进程未启动：

如果 web 登入后主界面的呼叫统计没有数据，则代表 SBC 进程未启动

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@SBC300 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