vSBC-5000用户手册

版本 1.3

版本变更历史

	日期	变更
VER 1.0	2021年11月23日	创建本文档
VER 1.1	2022年08月25日	安全功能，集中网关功能更新
VER 1.2	2022年09月29日	更正sip栈配置个数，增加中继组路由配置限制说明
VER 1.3	2022年10月14日	修正安装过程说明。

欲获取最新的产品信息，请访问我们的网站：http://www.ehangcom.com

声明：

本材料受中国和世界其他各国的知识产权和商业机密相关法律保护。除非得到广州市毅航互联通讯股份有限公司（下面有时简称毅航互联）的书面协议、合同或授权，任何复制、传播、或修改的行为（无论在本公司内部和外部）都是非法的。

本产品可能存在设计缺陷或错误，可能导致和该文档中的参数及描述有所偏差。我们一直努力使我们的产品手册在出版的时候更完整和更准确，但由于实际情况的不断变化，本文档只提供毅航互联产品的通用信息。

毅航互联对本文档不提供任何关于开发、销售任何特定功能的产品的承诺。也不提供任何对提到过或暗示过的产品应用的承诺。本文档的内容随时更新并且不做通知。因此，本文档的信息不应被看作是承诺和保证。

毅航互联不对本文档中任何技术或排版的错误、遗漏承担责任，也不对由此造成的任何损失承担责任。

毅航互联的产品并非针对且未被经认证授权可用于医疗、援救或生命维持等应用，以及任何可能会因为毅航互联的产品发生故障而导致人员伤亡的场合。

商标与知识产权

所有产品及服务的名称都是各各特定厂商的商标或者注册商标。本文档中提到的这些特定设备和软件的知识产权受中国和其他国家的相关法律条文的保护。

例如

Ehangcom, iSX, iSX4000, iSX UAP,Ehcomm 等都是毅航互联的注册商标。

Microsoft Windows, Microsoft Windows 98, Microsoft Windows 95, Microsoft NT等都是微软公司的注册商标。

SUN Solaris 是 SUN MicroSystem 公司的注册商标。

目 录

1 关于本手册

欢迎阅读本文档，该文档简要介绍毅航互联的 vSBC-5000。下面给出了有关本文档的使用目的、阅读对象、文档描述和相关信息。

目的

本手册提供简要介绍毅航互联 vSBC-5000 的安装和配置，便于市场人员、客户和使用人员了解和使用该平台。

阅读对象

1. 发布人员
2. 系统集成商
3. 工具包开发人员
4. 独立软件开发商
5. 系统买卖中间商
6. OEM 开发商

2 概述

毅航互联 vSBC-5000（简称 vSBC）提供类似 IMS 网络 A-SBC 和 I-SBC 的功能，用于网络拓扑隐藏、NAT 穿透、内外网隔离、VoIP 安全和广域网组网等场景，也可以用于协议转换、SIP 信令整形、视频会议、WebRTC 接入等 SBC 场景。

毅航互联 vSBC 支持双机主备冗余功能（HA），主备切换不影响通话，现有通话不会中断，满足运营级要求。

毅航互联 vSBC 支持话单，可用于计费等运营场景。

毅航互联 vSBC 是纯软件实现，可部署在专用服务器、通用服务器、虚拟机(VMware、KVM、VirtualBox)和云平台(阿里云、腾讯云、百度云、华为云等)。

毅航互联 vSBC 具有高性能和大容量的特点。呼叫：500 呼叫/秒，5000 并发。注册：500 事务/秒，5000 并发。

毅航互联 vSBC 支持媒体的编解码转换，并且采用内核包转发，具有极高的性能。

3 系统特性

3.1 容量

• 代理注册用户数量：10000

• 本地注册用户数量：10000

• 注册速度：500注册/秒

• 并发呼叫数量：5000

• 呼叫速度：500呼叫/秒

3.2 安全

• 拓扑隐藏

• 内置防火墙

• 基于VLAN的网络物理隔离

• 防DOS攻击

• 注册流控

• 呼叫流控

• 黑白名单

• ACL

•加密和鉴权：TLS, DTLS, SRTP, HTTPS, SSH, client/server SIP Digest

3.3 互操作

• SIP B2BUA

• 3xx redirect, REFER, PRACK, session timer, early media, delayed offer

• SIP over UDP/TCP/TLS/WebSocket/SCTP, IPv4/IPv6

• SIP头操作：增加/删除/替换

• RTP/SRTP/DTLS媒体的相互转换

• WebRTC网关功能：WebRTC和SIP网络的相互转换。Supports WebSocket, Opus, VP8 video coder, lite ICE, DTLS, RTP multiplexing, secure RTCP with feedback

3.4 可靠性

• HA：1+1主备

• 动态网络路由

• SIP中继冗余和负荷分担

3.5 路由

- 内置路由引擎
- 支持多种路由策略
- SIP中继路由支持主备、负载均衡
- 基于路由的号码变换

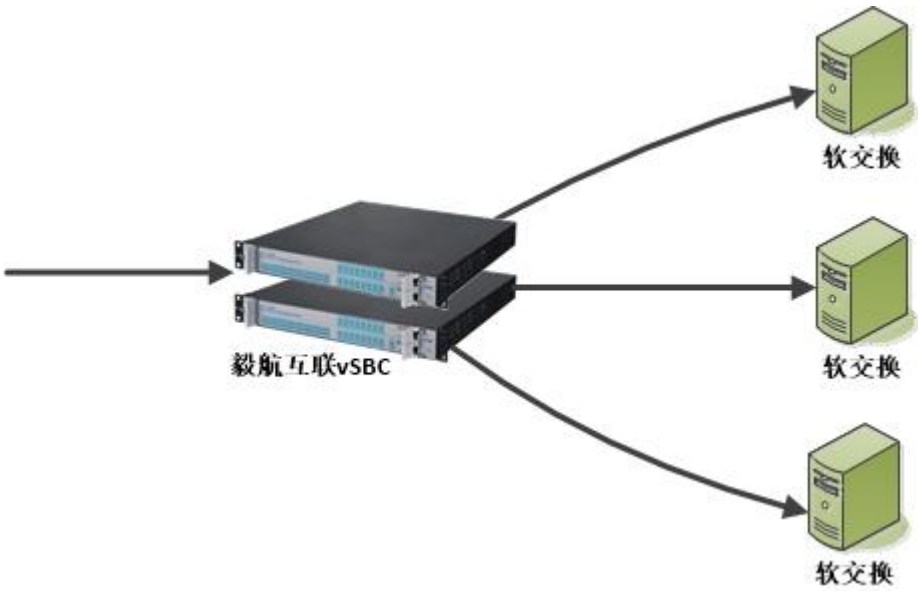
3.6 维护

- 远程升级
- WEB管理
- 配置导入导出
- 告警
- 日志
- 统计
- SNMP

4 使用场景

4.1 网络拓扑隐藏/负载均衡

当客户有多个基于 SIP 的软交换服务平台时，可以使用毅航互联 vSBC 在前端做负载均衡。如下图：



在 vSBC 上可以配置各个软交换服务器的容量和转发规则（均衡、优先级、主被叫号码等）。

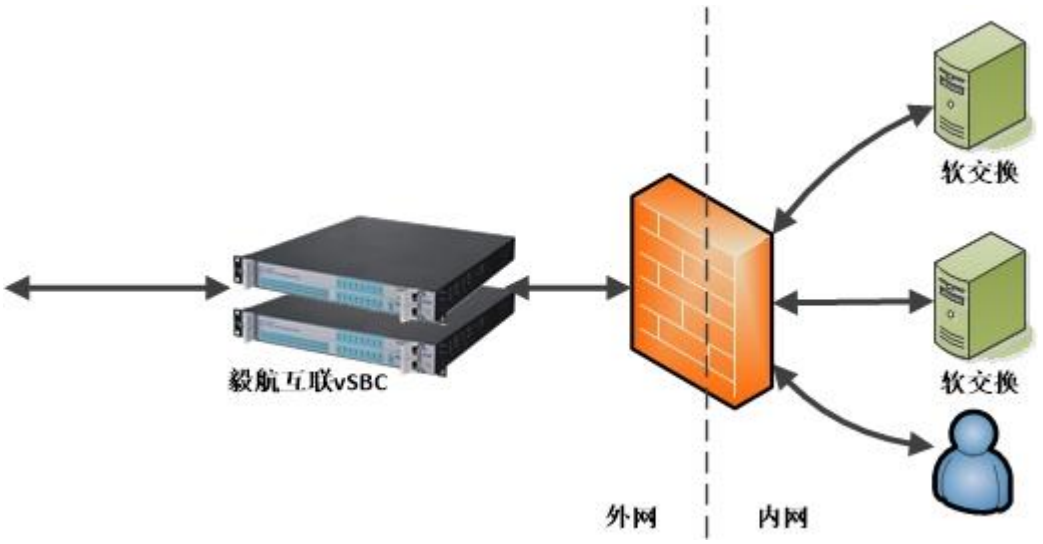
vSBC 和软交换间可以配置 OPTIONS 作为心跳检测，在心跳丢失时，可以自动将此软交换从均衡表中删除。

在 vSBC 上可以手动管理软交换，便于后端软交换的扩容、停机维护等操作。

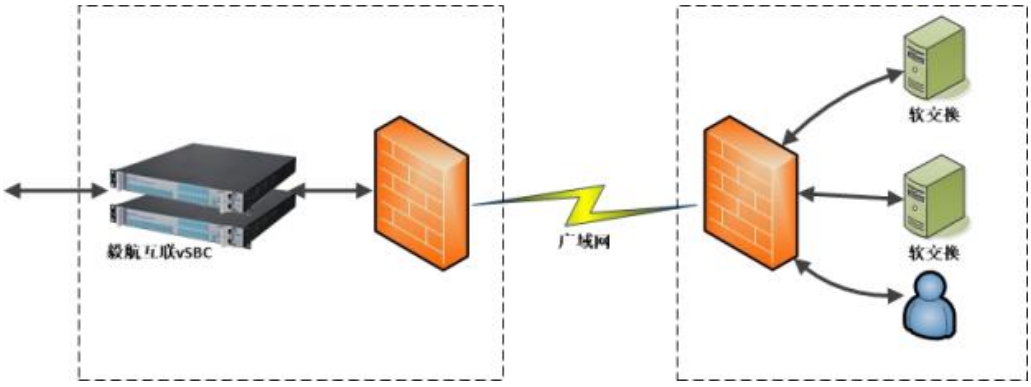
由于信令和媒体都由 vSBC 转发，在外部只看到 vSBC 的 IP 地址，从而隐藏了内部的网络结构。

4.2 NAT 穿透

为了安全，客户内外网间存在网络防火墙，这会导致 SIP 信令和媒体被防火墙更改，此时可以采用毅航互联 vSBC 执行 NAT 穿透处理。如下图：

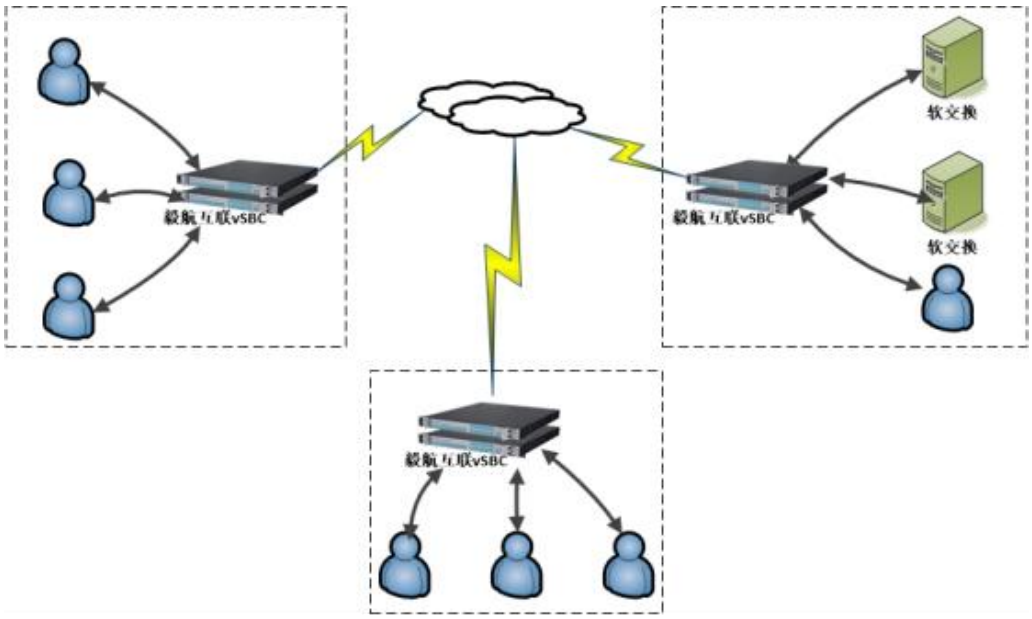


还存在连毅航互联 vSBC 都隐藏在防火墙（云平台部署的常见情景）后，需要做更加复杂的防火墙穿透的情况。如下图：



4.3 广域网组网

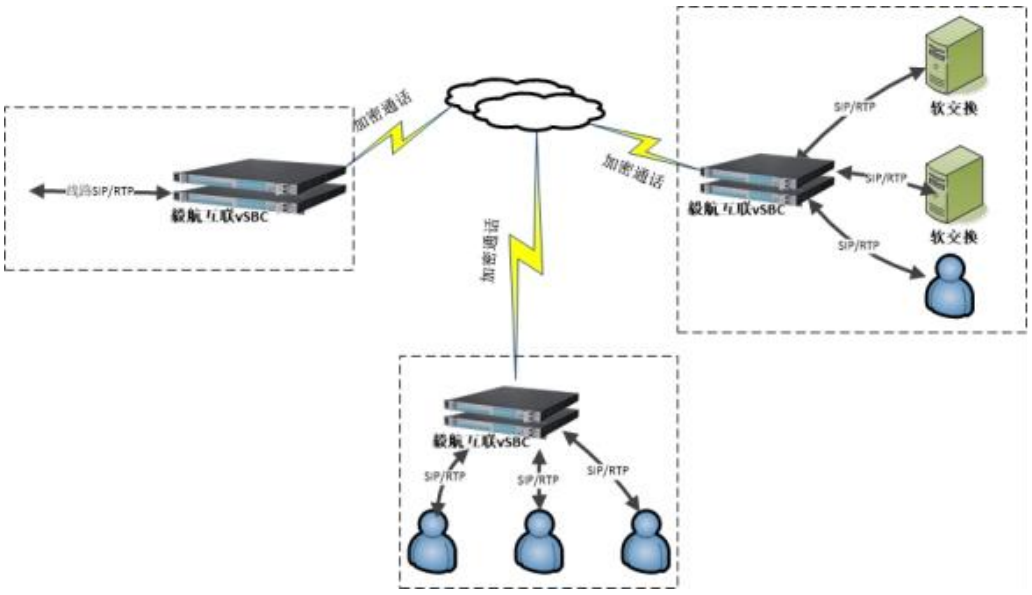
可以使用多套毅航互联 vSBC，将地域分散的各个分支机构组成单一的通信网。也可以利用 vSBC 将远程座席连接到呼叫中心平台。如下图：



4.4 加密通话

毅航互联 vSBC 同时支持 SIP/TLS/SRTP 和 SIP/UDP/RTP，因此，可以在现有平台间插入加密通话功能，避免通话在网络上很容易被窃取和监听。

在远程职场的情况下，业务呼叫必须经过广域网，存在网络泄密的可能性，如果做远程职场采用加密通话，就可以避免此类情况。如下图：



4.5 VoLTE 视频

毅航互联 vSBC 同时支持音频和视频的转发，因此，可以用于对接 VoLTE，提供注册、音/视频 NAT 转发等功能。

4.6 视频会议

毅航互联 vSBC 不光支持音频和视频的转发，还可以支持其他基于 UDP 的协议转发：比如 BFCP 协议、MSRP 协议。因此，它也可以用于视频会议的场景，解决视频会议中的 NAT 穿透、组网、负载均衡等问题。

4.7 WebRTC 一键呼叫

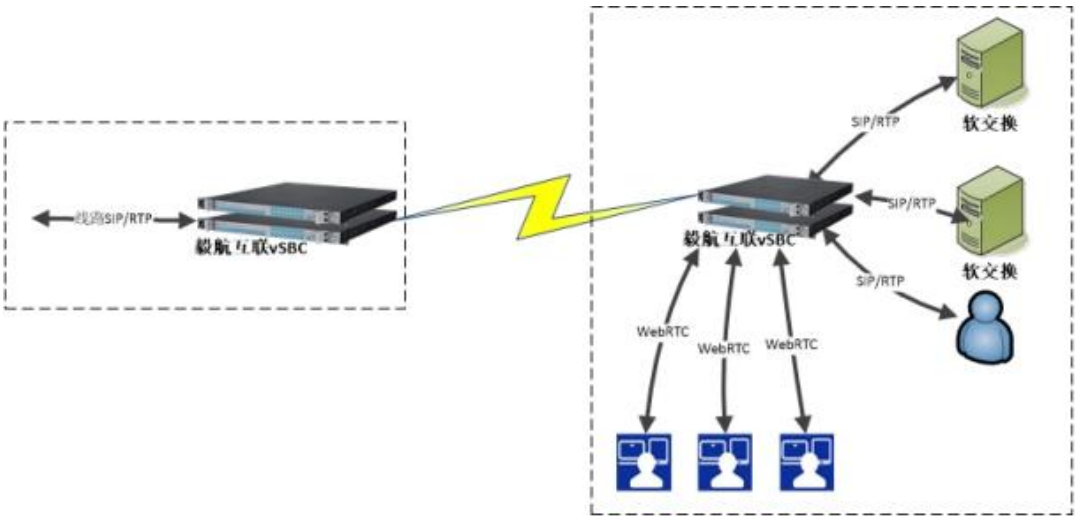
毅航互联 vSBC 支持 SIP over websocket、SRTP/DTLS 和 ICE，完全满足 WebRTC 的要求。同时，vSBC 也支持传统的 SIP/RTP，可以在 WebRTC 和传统 VoIP 网络间作相互换。

如下图，客户很容易在 web 中提供基于 webrtc 技术的界面，完成一键 click 呼叫，email 嵌入呼叫，短信嵌入呼叫等功能。

4.8 WebRTC 座席

传统座席电话不能够嵌入 web 或者采用插件嵌入，将座席界面分成两个不同的部分，不便于座席的单点登录等管理。采用 WebRTC 技术，将座席界面完全融合到 web 中，很容易实现单点登录，座席移机等功能，简化了座席的管理。

毅航互联 vSBC 支持基于 SIP over websocket 的座席代理功能，将 WebRTC 座席转换为标准 SIP 注册到原有系统中，并可以执行 WebRTC 和标准 SIP 间的信令和语音的相互转换，让原有呼叫中心系统不需要结构上的调整。如下图：



5 安装

5.1 硬件要求

CPU：INTEL 志强 E3 V2 系列或以上的 CPU；2.5G 或更高主频，至少 4 核 8 线程。

内存：不少于 8G。

网卡：推荐 INTEL I340（intel 82580）或更强的网卡。

硬盘：120G。

5.2 操作系统要求

CentOS_7.5 64 位系统，最小化安装，/home 目录至少需要 50g。

可前往 CentOS 官网 https://vault.centos.org 下载 iso 文件。

vSBC 运行需要很多系统库文件，安装包提供了 CentOS_7.5 64 位系统的相关 rpm 包。

目前支持 64 位操作系统：

CentOS_7.5 及以上版本，

SUSE Linux Enterprise Server 12 SP5 及以上版本，

银河麒麟 V10, Kylin Linux Advanced Server V10 (Tercel) 及以上版本。

5.3 安装

安装脚本必须用 root 执行，解压安装包后，进入 igateway_package_re_v3 目录。

执行./install.sh 安装。

```
# tar -zxvf vSBC-5000_XXX.tgz
# cd igateway_package_re_v3
# ./install.sh
```

安装完需要根据使用场景对媒体引擎做初始配置。

配置文件路径/home/ehang/MediaAgent/rtpengine.conf

注意配置以分号隔离，禁止带有空格等其他字符。

使用单 ip 的情况，媒体都从一个 ip 走，如 10.10.200.110。

```
### a single interface:
interface = 10.10.200.110/10.10.200.110;
```

使用多 ip 的情况，如 10.10.200.110 和 192.168.200.110。

```
### separate multiple interfaces with semicolons:
interface = 10.10.200.110/10.10.200.110;192.168.200.110/192.168.200.110
```

毅航互联 vSBC 在使用过程中需要获取 root 密码。为了安全考虑，我们提供了加密方法对密码进行加密。加密后的 root 密码保存在/home/ehang/oamproxy/configure.ini 中 的 PASSWORD 参数中。

进入 oamproxy 目录

cd /home/ehang/oamproxy

执行 EncryptionTools 程序并输入-e 参数和 root 密码

./EncryptionTools -e root 密码

#后续使用过程中如有 root 密码变更，也需要执行上述操作

以上步骤完成后重启机器。

reboot

6 配置

6.1 WEB 登录

使用 firefox/chrome/edge 等浏览器登录 vSBC，必须 https 登录，端口为 8090。

如 https://10.10.200.110:8090，首次登录会有安全提示，点继续前往。

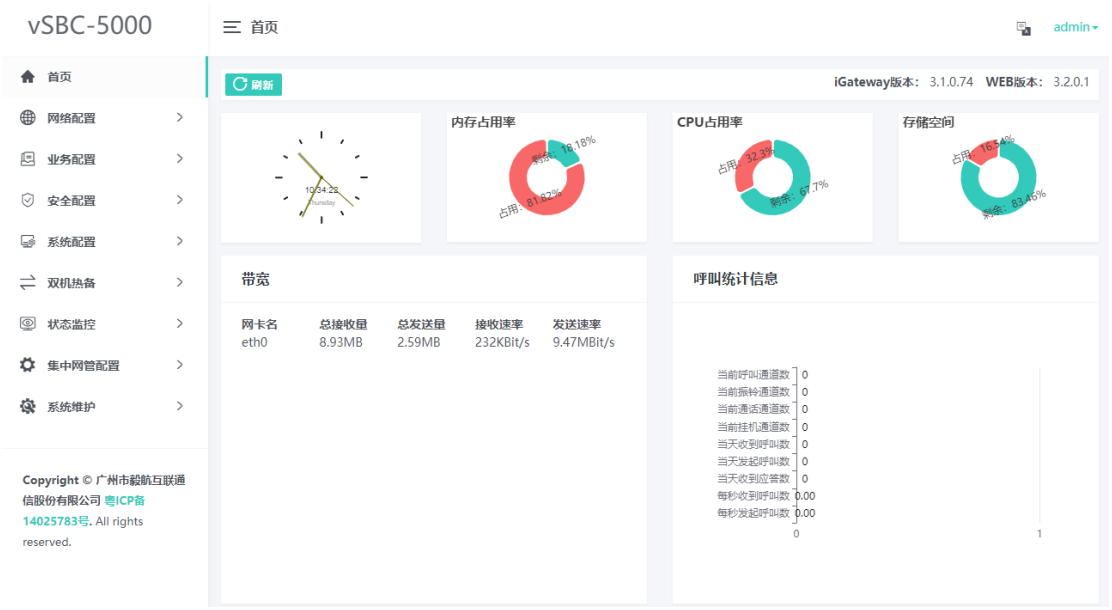
默认用户名 admin，密码为 Ehangcom@123，首次登录需强制修改密码。

为了较好的浏览体验，建议使用 1440x900 分辨率以上的显示器。

密码有检查复杂度机制，必须由数字、字母、特殊符号组成，最小长度为 8 位，区分大小写。

6.2 首页

首页显示软件版本、时间、内存占用、cpu 占用、存储空间、带宽及呼叫统计信息。



6.3 用户管理

点击页面右上角，可以修改密码，创建新用户并分配权限,管理员配置，隐私配置。

6.4 网络配置

6.4.1 网络接口配置

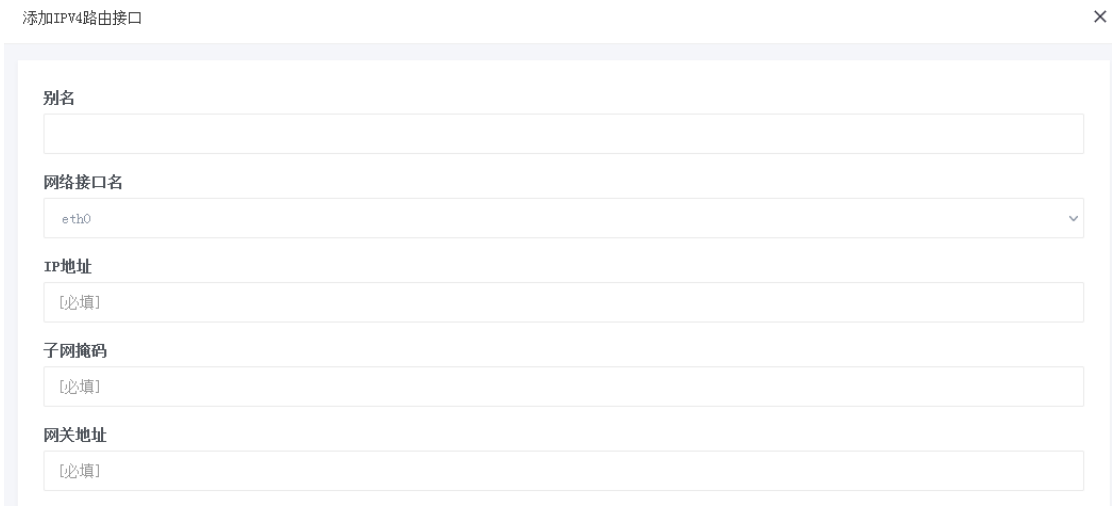
为系统配置 IP 等。

配置内容	描述
别名	作为标识。
网络接口名	从系统已有的网络接口中选择。
虚拟局域网 ID	可选项，如需要 vlan，在此填入 vlan id，范围 1-4094。
IP 地址	IP 地址。
子网掩码	子网掩码。
默认网关	可选项，默认网关。
DNS	可选项，DNS。

6.4.2 IP 静态路由配置

为系统配置 IP 静态路由。

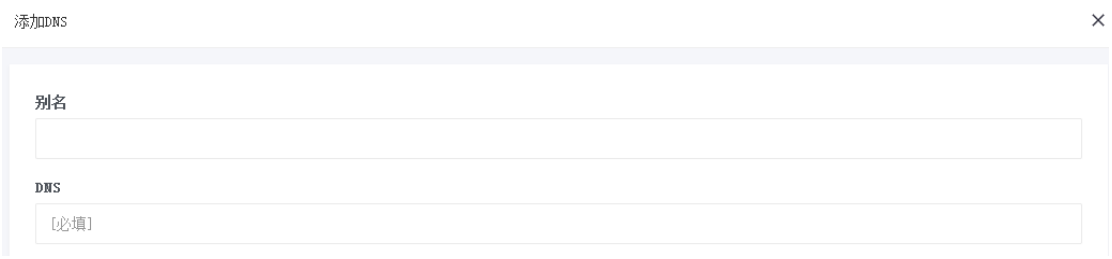
配置内容	描述
别名	作为标识。
网络接口名	从系统已有的网络接口中选择。
IP 地址	IP 地址。
子网掩码	子网掩码。
网关地址	网关地址。



6.4.3 DNS 配置

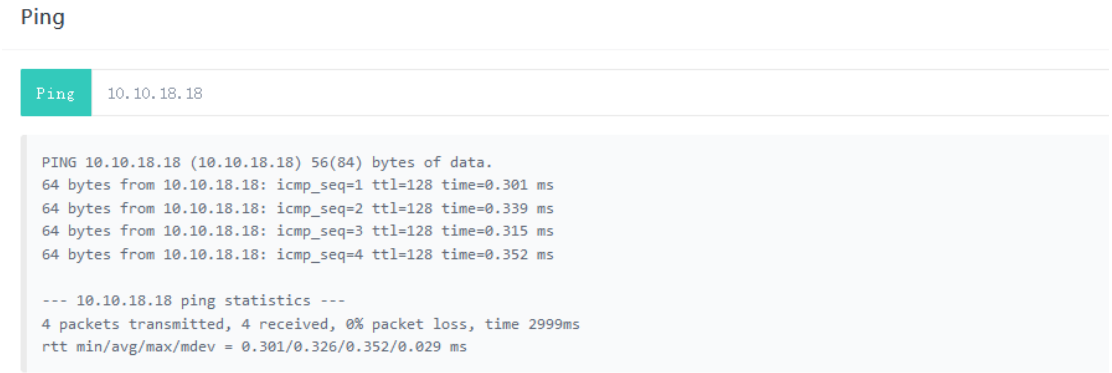
为系统配置 DNS。

配置内容	描述
别名	作为标识。
DNS	DNS。



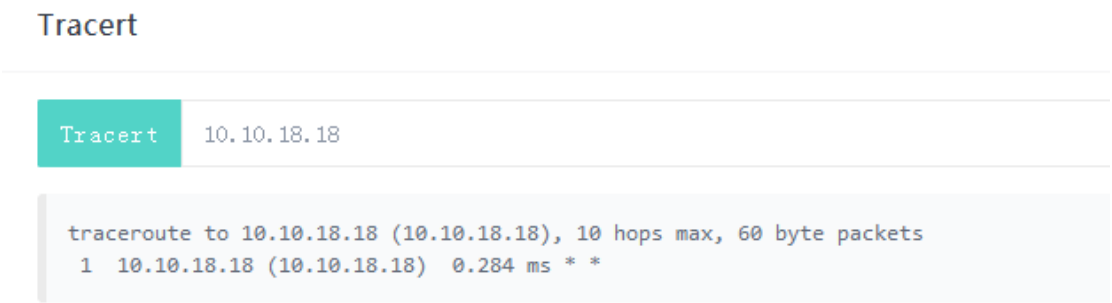
6.4.4 PING 测试

输入目的 ip，点击“Ping”，等待结果显示。



6.4.5 TRACERT 测试

输入目的 ip，点击“Tracert”，等待结果显示。



6.4.6 IP 地址查询

IP地址查询

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 52:54:00:27:28:98 brd ff:ff:ff:ff:ff:ff
    inet 10.10.0.8/16 brd 10.10.255.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
    inet 10.10.220.30/16 brd 10.10.255.255 scope global secondary noprefixroute eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::5054:ff:fe27:2898/64 scope link
       valid_lft forever preferred_lft forever
    inet6 fe80::4af7:b349:5b59:b198/64 scope link
       valid_lft forever preferred_lft forever
    inet6 fe80::e5d9:e684:7d22:fdc3/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 52:54:00:52:2a:cb brd ff:ff:ff:ff:ff:ff
    inet 10.10.0.4/16 brd 10.10.255.255 scope global noprefixroute dynamic eth1
       valid_lft 83166sec preferred_lft 83166sec
    inet 192.168.220.30/24 brd 192.168.220.255 scope global eth1
       valid_lft forever preferred_lft forever
    inet6 fe80::ab5b:d630:8ad8:5d82/64 scope link
       valid_lft forever preferred_lft forever
    inet6 fe80::40e5:e6b4:be52:6b38/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

6.4.7 IP 路由查询

IP路由查询

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.10.0.1       0.0.0.0         UG    100    0        0 eth0
0.0.0.0         10.10.0.1       0.0.0.0         UG    101    0        0 eth1
10.10.0.0       0.0.0.0         255.255.0.0     U     100    0        0 eth0
10.10.0.0       0.0.0.0         255.255.0.0     U     100    0        0 eth0
10.10.0.0       0.0.0.0         255.255.0.0     U     101    0        0 eth1
169.254.0.0     0.0.0.0         255.255.0.0     U     1003   0        0 eth1
192.168.220.0   0.0.0.0         255.255.255.0   U     0      0        0 eth1
192.168.220.0   0.0.0.0         255.255.255.0   U     101    0        0 eth1
192.169.0.0     0.0.0.0         255.255.0.0     U     0      0        0 eth2
```

6.4.8 ARP 查询

ARP查询

Address	HWtype	HWaddress	Flags Mask	Iface
10.10.18.27	ether	00:e0:70:28:85:b5	C	eth0
10.10.18.2	ether	e0:d5:5e:7c:84:3b	C	eth0
192.168.220.53	ether	00:0c:90:0b:66:22	C	eth1
192.168.220.60	ether	00:0c:90:0b:72:62	C	eth1
192.169.220.55	ether	00:0c:90:0b:69:82	C	eth2
192.169.220.57	ether	00:0c:90:0b:5e:22	C	eth2
10.10.19.200	ether	f0:de:f1:ee:54:0c	C	eth0
192.168.220.51	ether	00:0c:90:0b:63:02	C	eth1
192.168.220.58	ether	00:0c:90:0b:60:42	C	eth1
192.169.220.53	ether	00:0c:90:0a:cf:a2	C	eth2
192.169.220.60	ether	00:0c:90:0b:67:22	C	eth2
10.10.220.31	ether	52:54:00:55:bc:22	C	eth0
10.10.0.1	ether	e0:97:96:4e:2a:ad	C	eth1
192.168.220.54	ether	00:0c:90:0b:63:e2	C	eth1
192.168.220.56	ether	00:0c:90:0b:5c:e2	C	eth1
192.169.220.51	ether	00:0c:90:0b:6c:22	C	eth2
10.10.0.1	ether	e0:97:96:4e:2a:ad	C	eth0
192.169.220.58	ether	00:0c:90:0b:64:42	C	eth2
10.10.100.168	ether	44:a8:42:12:65:53	C	eth0
192.168.220.52	ether	00:0c:90:0b:77:c2	C	eth1
192.169.220.54	ether	00:0c:90:0b:5f:62	C	eth2

6.5 业务配置

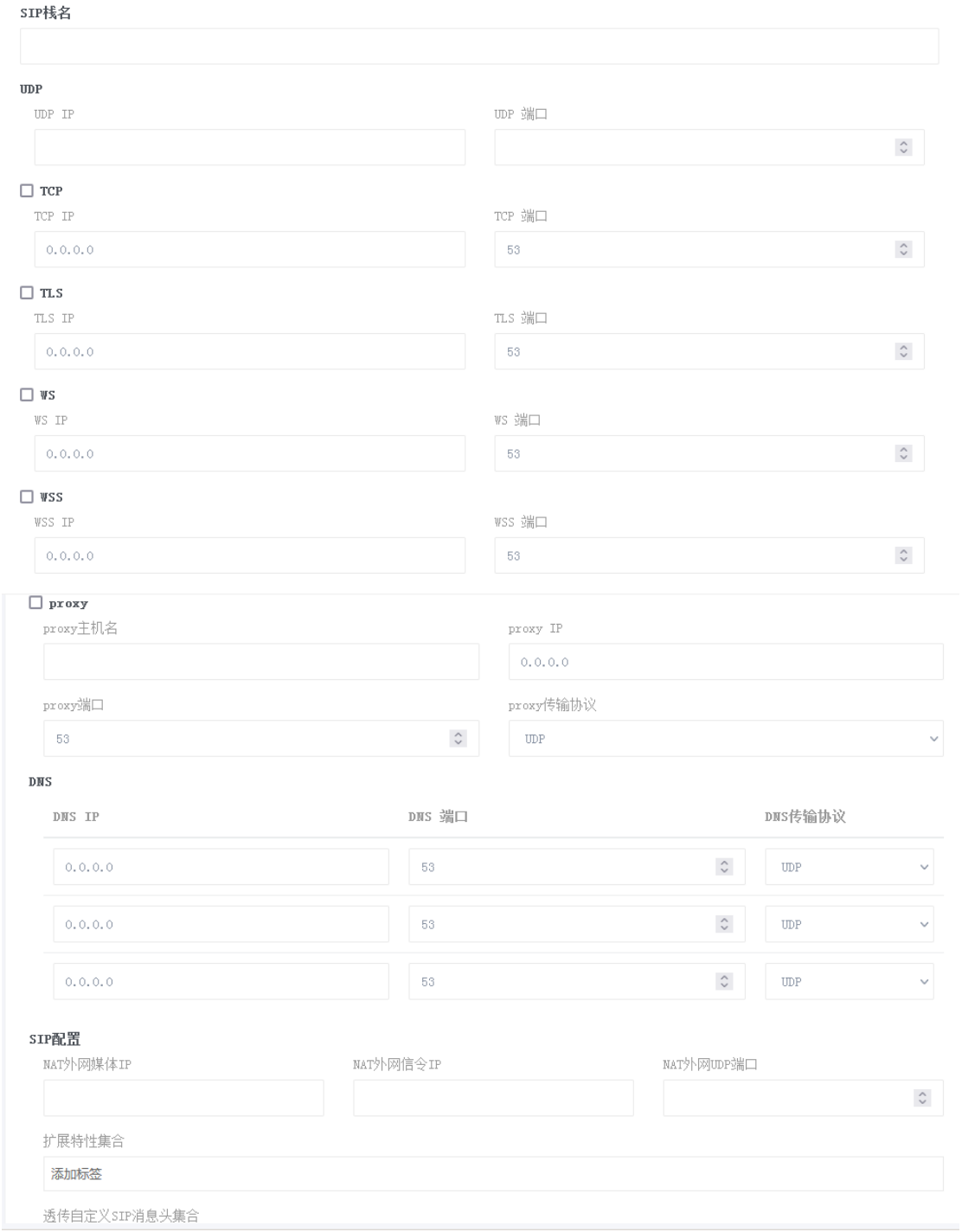
6.5.1 SIP 栈

SIP 栈主要配置本地的 SIP 信令地址，目前最多支持 8 个 SIP 栈。

注意 SIP 栈必须启用才生效，如果 SIP 栈被中继组引用，必须解除引用后才能删除。

配置内容	描述
SIP 栈名	作为标识，不可重名，为中继组所引用。
UDP	UDP 地址。
TCP	TCP 地址。
TLS	TLS 地址，必须同时配置 TCP 地址。
WS	WS 地址，必须同时配置 TCP 地址。
WSS	WSS 地址，必须同时配置 TCP 地址。
PROXY	外呼代理服务器。
DNS	外呼使用的 DNS。
NAT 外网媒体 IP	在 NAT 环境下，配置外网 SDP 媒体 IP。
NAT 外网信令 IP	在 NAT 环境下，配置外网 SIP 信令 IP。
NAT 外网 UDP 端口	在 NAT 环境下，配置外网 SIP 信令端口。
扩展特性集合	支持 100rel,timer,replaces,in-band-dtmf，如配置多项，用英文逗号隔开。 100rel：18x 的可靠传递功能。 timer：支持会话超时功能。 replaces：支持 SIP replace 功能。 in-band-dtmf：带内 dtmf。
透传自定义 SIP 消息头集合	将呼入消息的某些自定义 SIP 消息头透传，如配置多项，用英文逗号隔开，默认为:From,to 以支持 URL 过滤功能，

	如：From,to,X-Genesys-businessid,X-Genesys-vid,X-FS-Support
DoS/DDoS 攻击防护	防 ddos 攻击 ，开关。
畸形报文/无效请求攻击防护	防 sip 无效请求攻击， 开关。
注册攻击防护	防 sip 注册攻击， 开关。
呼叫攻击防护	防 sip 呼叫攻击， 开关。
每秒注册限制	防 sip 注册攻击每秒限制注册数量。
每秒呼叫限制	防 sip 呼叫攻击每秒限制呼叫数量。
最小的接收消息长度	最小的接收消息长度配置，畸形报文/无效请求攻击防护开关开启时生效。
最大的接收消息长度	最大的接收消息长度配置，畸形报文/无效请求攻击防护开关开启时生效。
注册信息记录的最大值	注册信息记录的最大值配置，注册攻击防护开关开启时生效。
注册等待鉴权的超时时间	注册等待鉴权的超时时间配置，注册攻击防护开关开启时生效。
频繁注册刷新计数器	频繁注册刷新计数器，注册攻击防护开关开启时生效。
频繁注册刷新周期	频繁注册刷新周期配置，注册攻击防护开关开启时生效。
超短通话时长阈值	超短通话阀值， 呼叫攻击防护开关开启时生效。


SIP栈名
UDP
UDP IP
UDP 端口
TCP
TCP IP
TCP 端口
0.0.0.0
53
TLS
TLS IP
TLS 端口
0.0.0.0
53
WS
WS IP
WS 端口
0.0.0.0
53
WSS
WSS IP
WSS 端口
0.0.0.0
53
proxy
proxy主机名
proxy IP
0.0.0.0
proxy端口
53
proxy传输协议
UDP
DNS
DNS IP
DNS 端口
DNS传输协议
0.0.0.0
53
UDP
0.0.0.0
53
UDP
0.0.0.0
53
UDP
SIP配置
NAT外网媒体IP
NAT外网信令IP
NAT外网UDP端口
扩展特性集合
添加标签
透传自定义SIP消息头集合

6.5.2 中继组

中继组是一个网络接入点。SBC 收到呼叫时，根据传输协议、远端地址、本地地址等信息，匹配到具体的组，如有多个可能匹配的组，只会匹配第一个，如无法匹配，则拒绝该呼叫。

目前中继组最高支持 256 个。

中继组数量比较多时，可在中继组首页输入“中继组名”、“远端 IP”查找。

如果中继组被“呼叫路由”或“注册路由”引用，必须解除引用后才能删除。

中继组共有 3 种类型。

类型 1：SIP 中继组，即 SIP TRUNK 模式。

配置内容	描述
中继组类型	选中“SIP 中继组”。
中继组名	作为标识，不可重名，为“呼叫路由”或“注册路由”所引用。
传输协议	可选 UDP/TCP/TLS/WS/WSS，所引用的 SIP 栈必须先配置好对应的协议的地址。
180/183 消息转换	将 180/183 消息进行转换处理，一般情况下不需要转换，可根据实际情况灵活选择。
媒体支持	支持的媒体编码，ALAW，ULAW，G723，G729，iLBC 20m，iLBC 30m，GSM，AMR，AMR_WB，OPUS，722，speex 8k，speex 16k，speex 32k
并发限制	对该组呼叫并发做限制，统计包括呼入和呼出，设为 0 时不做限制。

SIP 栈名	使用的 SIP 栈，从已经配置好的 SIP 栈名中选择。
媒体 IP 集合	可选项，用于多个媒体 IP 的情况。
心跳包	发送 options 消息到远端地址，根据响应判断远端地址是否可达。
心跳包间隔（秒）	发送 options 心跳消息的间隔。
分发模式	当有多个远端地址时，外呼选择的策略。 主备：分发值设 1 的地址为主，设 0 的地址为备，配合心跳使用，当主地址不可达时，选择其他可用的备地址，当主地址恢复可达时，选择主地址。 均衡：分发值代表每个远端地址的最大并发数。 比例：分发值代表分发呼叫的比例，和并发无关。
自定义 SIP 消息头内容集合	外呼时添加固定的 SIP 消息头内容。
远端地址集合	对接的远端地址，有多个地址时，分发值的意义参考分发模式描述。 对于呼入的中继组，远端端口为 0 则忽略端口的判断，例如 tcp 接入时，远端发起呼叫是随机端口；对于呼出的中继组，远端端口为 0 则外呼时不使用该地址。 状态为 1 表示可达，0 表示不可达。不启用心跳包时，状态为 1；启用心跳包时，连续两个 options 消息没收到响应则状态为 0，后续重新收到响应时变为 1。
远端媒体地址锁定	开关，对接远端媒体地址，只接受 SDP 中的远端地址
RTP 会话防注入	开关，对接远端媒体地址过程中，会持续检查远端的 IP/PORT，如果和纪录的地址不匹配，包将被丢弃。
中继组带宽控制	开关，中继组配置带宽限制。
中继组最高带宽（kbs）	中继组带宽阀值配置，中继组配置带宽限制开关开启时生效
终端带宽限制	终端媒体带宽限制
断流检测	开关，断流检测
断流检测超时值（ms）	断流检测超时值阀值，断流检测开启时生效
QoS	Qos 值配置

类型 2：SIP 注册代理，接入点需要注册，配合注册路由转发到注册服务器。

配置内容	描述
中继组类型	选中“SIP 注册代理”。
中继组名	作为标识，不可重名，为“呼叫路由”或“注册路由”所引用。
传输协议	可选 UDP/TCP/TLS/WS/WSS，所引用的 SIP 栈必须先配置好对应的协议的地址。
180/183 消息转换	将 180/183 消息进行转换处理，一般情况下不需要转换，可根据实际情况灵活选择。
媒体支持	支持的媒体编码，ALAW，ULAW，G723，G729，iLBC 20m，iLBC 30m，GSM，AMR，AMR_WB，OPUS，722，speex 8k，speex 16k，speex 32k
并发限制	对该组呼叫并发做限制，统计包括呼入和呼出，设为 0 时不做限制。
SIP 栈名	使用的 SIP 栈，从已经配置好的 SIP 栈名中选择。
媒体 IP 集合	可选项，用于多个媒体 IP 的情况。
用户名过滤规则	对用户名使用正则表达式匹配，进行过滤，为空则不进行过滤。
域名	对注册消息的域名（to 内容的地址）匹配，进行过滤，为空则不进行过滤。
远端媒体地址锁定	开关，对接远端媒体地址，只接受 SDP 中的远端地址
RTP 会话防注入	开关，对接远端媒体地址过程中，会持续检查远端的 IP/PORT，如果和纪录的地址不匹配，包将被丢弃。
中继组带宽控制	开关，中继组配置带宽限制。
中继组最高带宽（kbs）	中继组带宽阀值配置，中继组配置带宽限制开关开启时生效
终端带宽限制	终端媒体带宽限制
断流检测	开关，断流检测
断流检测超时值（ms）	断流检测超时值阀值，断流检测开启时生效
QoS	Qos 值配置

类型 3：SIP 坐席，接入点需要注册，SBC 本身作为注册服务器。

配置内容	描述
中继组类型	选中“SIP 坐席”。
中继组名	作为标识，不可重名，为“呼叫路由”所引用。
传输协议	可选 UDP/TCP/TLS/WS/WSS，所引用的 SIP 栈必须先配置好对应的协议的地址。
180/183 消息转换	将 180/183 消息进行转换处理，一般情况下不需要转换，可根据实际情况灵活选择。
媒体支持	支持的媒体编码，ALAW，ULAW，G723，G729，iLBC 20m，iLBC 30m，GSM，AMR，AMR_WB，OPUS，722，speex 8k，speex 16k，speex 32k
并发限制	对该组呼叫并发做限制，统计包括呼入和呼出，设为 0 时不做限制。
SIP 栈名	使用的 SIP 栈，从已经配置好的 SIP 栈名中选择。

媒体 IP 集合	可选项，用于多个媒体 IP 的情况。
本地用户注册信息	配置 SIP 注册的本地用户名和密码，如果数量多，可通过导入文件的方式进行配置。状态为 1 代表注册成功，为 0 代表未注册成功。如果注册成功，可查看来源的 IP、端口。
注册有效期（秒）	注册成功后的有效期，如果在有效期内没有重新注册，则状态变为 0。
远端媒体地址锁定	开关，对接远端媒体地址，只接受 SDP 中的远端地址
RTP 会话防注入	开关，对接远端媒体地址过程中，会持续检查远端的 IP/PORT，如果和纪录的地址不匹配，包将被丢弃。
中继组带宽控制	开关，中继组配置带宽限制。
中继组最高带宽（kbs）	中继组带宽阀值配置，中继组配置带宽限制开关开启时生效
终端带宽限制	终端媒体带宽限制
断流检测	开关，断流检测
断流检测超时值（ms）	断流检测超时值阀值，断流检测开启时生效
QoS	Qos 值配置

6.5.3 呼叫路由

呼叫路由的主要构成是“一入一出”两个中继组，将呼入中继组的呼叫送往对应的呼出中继组，同时可以做一些条件的限制和号码变换等。

目前呼叫路由最高支持 512 个配置。

呼叫路由根据优先级排列，依次选择。

呼叫路由数量比较多时，可在呼叫路由首页输入“中继组名”、“呼叫路由名”查找。

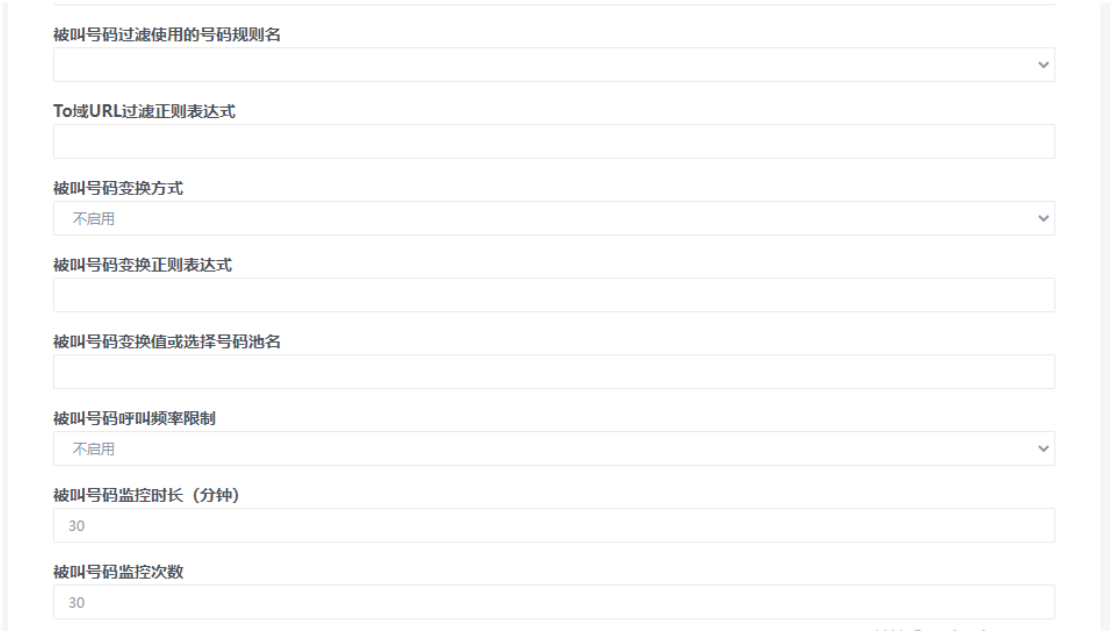
如果需要配置大部分内容相同的呼叫路由，使用呼叫路由的复制功能比较方便。

“测试路由”功能，输入“呼入中继组名”、“原始主叫”和“原始被叫”，返回路由是否成功、“呼出中继组名”、“主叫”和“被叫”等信息，可验证路由配置是否与预期的一致。

配置内容	描述
呼叫路由名	作为标识，不可重名。
呼入中继组名	呼入的中继组，从已经配置好的中继组名中选择。
呼出中继组名	呼出的中继组，从已经配置好的中继组名中选择。
呼叫路由方向	可选项，仅作为标识，如呼入的组对接运营商，呼出的组对接客户平台，可设为“呼入”。

启用标识	是否启用。
优先级	作为路由排列的顺序，数字越小优先级越高。
时间段限制	路由生效的时间段。
H 码表使用方式	需配合导入 H 码表使用，可限制某些地区的号码或根据地区做号码变换。使用限制功能时，只需在地区配置里选择对应的地区；使用号码变换功能时，需配合号码池使用，默认使用区号作为号码池名，也可修改使用其他号码池名。
号码变换 url	外部号码变换接口，通过 HTTP/JSON 交互，当客户的号码变换需求复杂，SBC 本身的号码变换无法满足时，做定制开发。
指定挂机值重呼其他路由	可根据指定的远端返回的挂机值，继续选择其他匹配的路由重新发起呼叫。
号码过滤正则表达式	对主叫或被叫号码使用正则表达式匹配，进行过滤，为空则不进行过滤。
号码规则	从已配置的号码规则中选择，对主叫或被叫号码使用号码规则匹配（参考 6.5.7 号码规则），进行过滤，为空则不进行过滤。
黑名单	从已配置的号码黑名单中选择，对主叫或被叫号码进行过滤（参考 6.5.5 号码黑名单），为空则不进行过滤。
号码变换方式	对主叫或被叫号码变换的方式，有添加、替换、删除和号码池等方式。
号码变换正则表达式	对主叫或被叫号码中需要变换的部分的内容使用正则表达式匹配。
号码变换值或号码池名	对主叫或被叫号码中需要变换的部分的内容进行变换，如果是号码池方式则是完全替换（参考 6.5.6 号码池）。
号码呼叫频率限制	对 SBC 呼出的主叫或被叫号码（如有号码变换，指变换后的号码）进行频率限制，监控时长内最多只能呼出一定的次数。


号码变换url
指定挂机值重呼其他路由
主叫
主叫黑名单使用的黑名单名
主叫白名单使用的白名单名
主叫号码过滤正则表达式
主叫号码过滤使用的号码规则名
From域URL过滤正则表达式
主叫号码变换方式
不启用
主叫号码变换正则表达式
主叫号码变换值或选择号码池名
主叫号码呼叫频率限制
不启用
主叫号码监控时长（分钟）
30
主叫号码监控次数
30
被叫
被叫黑名单使用的黑名单名
被叫白名单使用的白名单名



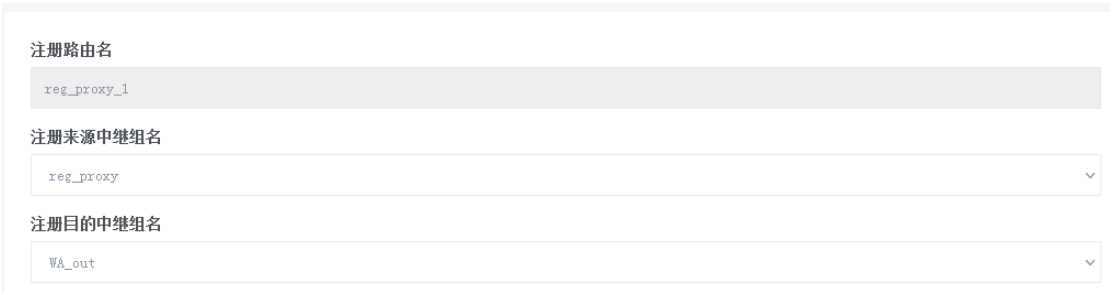
6.5.4 注册路由

注册路由的主要构成是“一入一出”两个中继组，将来源中继组的注册送往对应的目的中继组。

注册路由数量比较多时，可在注册路由首页输入“中继组名”、“注册路由名”查找。

配置内容	描述
注册路由名	作为标识，不可重名。

注册来源中继组名	注册来源中继组，从已经配置好的中继组名中选择。
注册目的中继组名	注册目的中继组，从已经配置好的中继组名中选择。



6.5.5 号码黑名单

号码黑名单用于在“呼叫路由”中对主叫或被叫号码进行限制。

如果已经被“呼叫路由”引用，必须解除引用后才能删除。

配置内容	描述
黑名单名	作为标识，不可重名，为“呼叫路由”所引用。
黑名单内容	号码，多个号码以英文逗号做分割，匹配规则为前缀匹配，如配置了“200”，则“200”、“2000”、“20011”等号码都属于黑名单。

6.5.6 号码白名单

号码白名单单用于在“呼叫路由”，仅对主叫或被叫号码进行放行。

如果已经被“呼叫路由”引用，必须解除引用后才能删除。

配置内容	描述
白单名	作为标识，不可重名，为“呼叫路由”所引用。
白单内容	号码，多个号码以英文逗号做分割，匹配规则为前缀匹配，如配置了“200”，则“200”、“2000”、“20011”等号码都属于白名单。

6.5.7 号码池

号码池用于在“呼叫路由”中对主叫或被叫号码进行变换。

如果已经被“呼叫路由”引用，必须解除引用后才能删除。

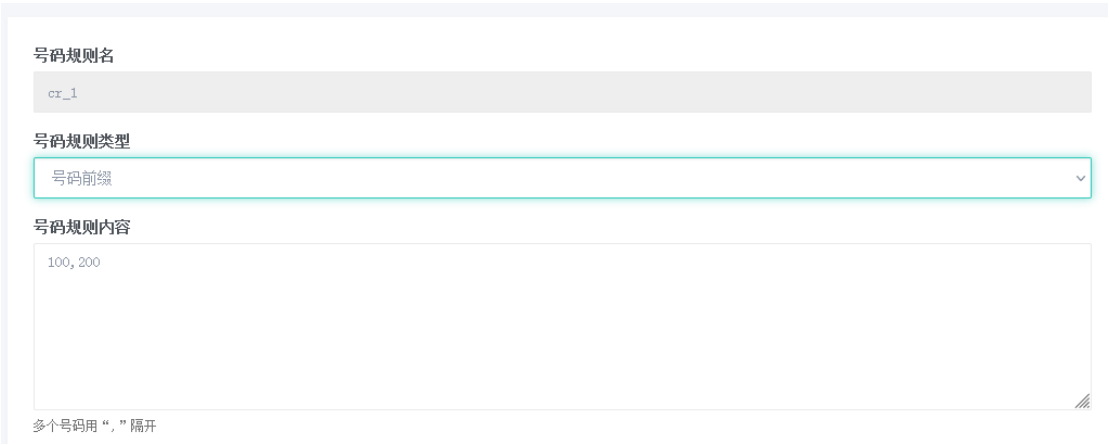
配置内容	描述
号码池名	作为标识，不可重名，为“呼叫路由”所引用。
号码池内容	号码，多个号码以英文逗号做分割。

6.5.8 号码规则

号码规则用于在“呼叫路由”中对主叫或被叫号码进行过滤。

如果已经被“呼叫路由”引用，必须解除引用后才能删除。

配置内容	描述
号码规则名	作为标识，不可重名，为“呼叫路由”所引用。
号码规则类型	分为“号码前缀”和“手机号码段”两种，如果要匹配的号码是中国大陆地区的手机号码段（例如前 7 位），使用“手机号码段”可以更加快速处理，相对“号码前缀”做了专门优化。
号码规则内容	号码，多个号码以英文逗号做分割，匹配规则为前缀匹配，如配置了“200”，则“200”、“2000”、“20011”等号码都匹配。



6.5.9 H 码表

H 码表是对中国大陆地区的手机号段进行地区区分的数据。

当“呼叫路由”需要 H 码表相关功能时，必须先导入 H 码表文件，才能正常使用。

H 码表文件为必须是如下图格式的文本文件，依次为：

前 7 位手机号码，省份，城市，运营商标识，区号，邮政编码。

运营商标识和邮政编码虽然未有使用，但格式上要求，可以填其他内容代替，不能为空。

注意要使用英文逗号隔开。

```
1300000,山东,济南,山东联通130卡,0531,250000
1300001,江苏,常州,江苏联通130卡,0519,213000
1300002,安徽,巢湖,安徽联通130卡,0565,231500
1300006,江苏,南京,江苏联通130卡,025,210000
1300008,湖北,武汉,湖北联通GSM卡,027,430000
1300010,北京,北京,北京联通130卡,010,100000
1300011,北京,北京,北京联通130卡,010,100000
```

6.5.10 录音配置

通过配置 siprec 服务器地址来配置录音。

录音需在路由配置上做开启操作

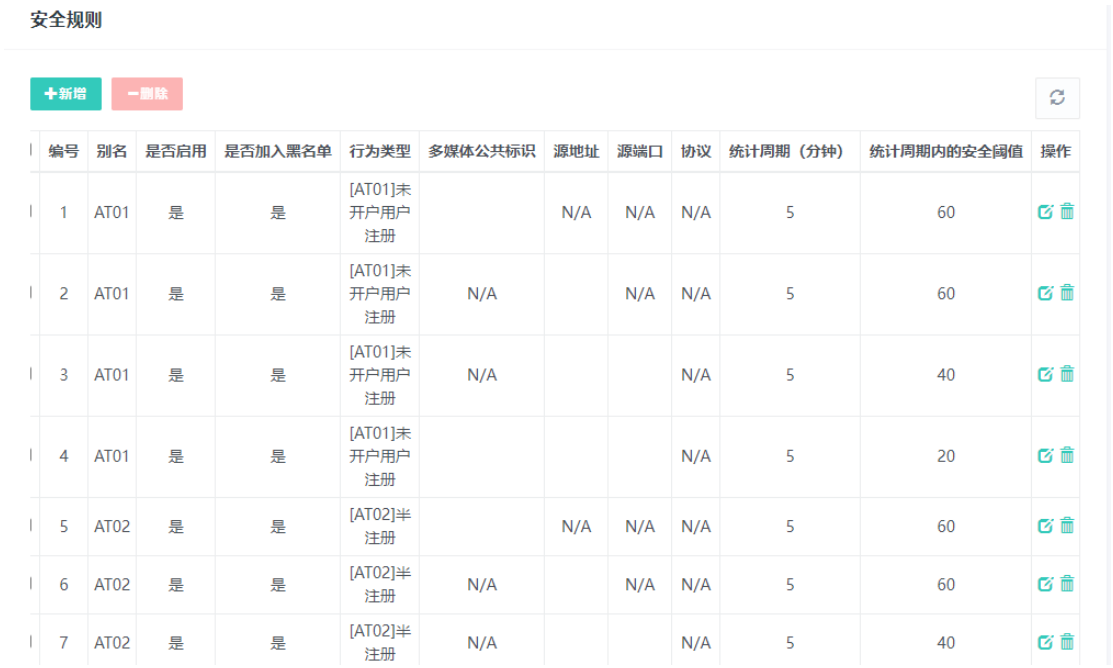
6.6 安全配置

6.6.1 系统基本安全防护

系统基本的 IP 层防护，TCP Flood 防御，UDP Flood 防御，端口扫描防御，TCP Flood 防御

6.6.2 安全规则

SBC 入侵防护规则，按照 IMPU、源 IP+源 Port 和源 IP 这三个维度对异常信息进行统计，统计周期默认为 5 分钟。如果统计值超过了规则配置的，则将 IMPU、源 IP+源 Port 或者源 IP 加入到黑名单中。



新增系统自带默认安全规则，可以进行自定义规则新增。

6.6.3 异常信息统计

异常信息收集统计表格。

6.6.4 攻击黑名单

异常攻击黑名单表格，如果统计值超过了安全规则配置的上限，则将 IMPU、源 IP+源 Port 或者源 IP 加入到黑名单中，并且对系统防火墙进行联动。

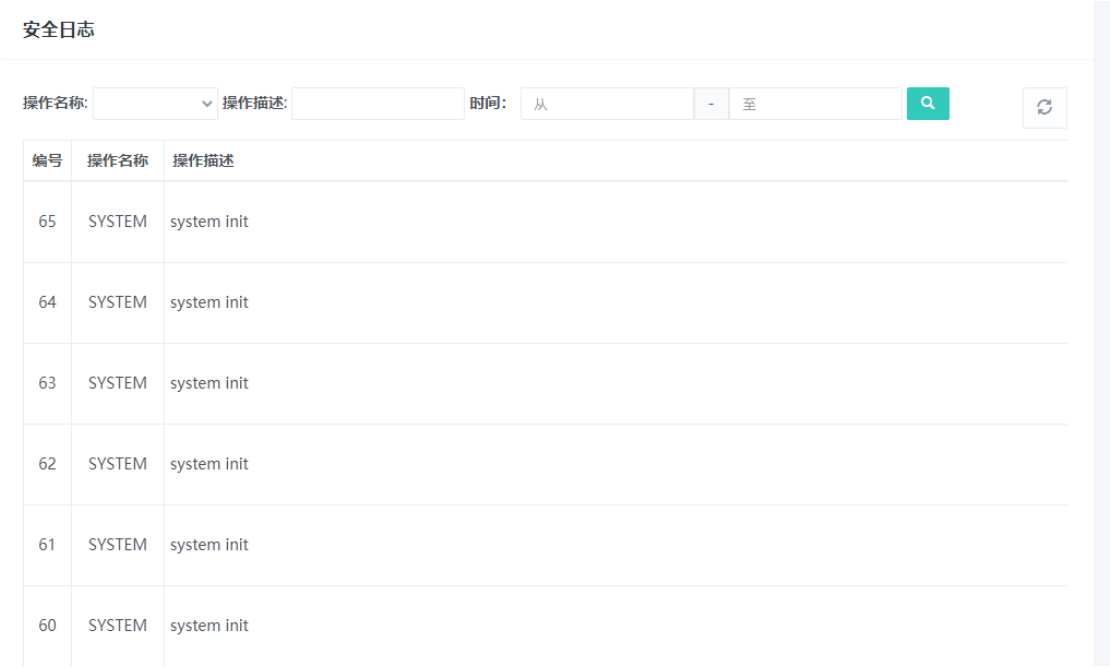
6.6.5 攻击灰名单

异常攻击灰名单表格。

黑名单达到老化时间后，会被删除。此时 IMPU 或源 IP+源 Port 会被升级为灰名单用户，进入观察期。观察期默认是 5 分钟，观察期结束后，IMPU 或源 IP+源 Port 变为正常用户。在观察期内只要出现一次异常信息，则 IMPU 或者源 IP+源 Port 会被再次加入黑名单。

6.6.6 安全日志

安全模块相关日志表格。

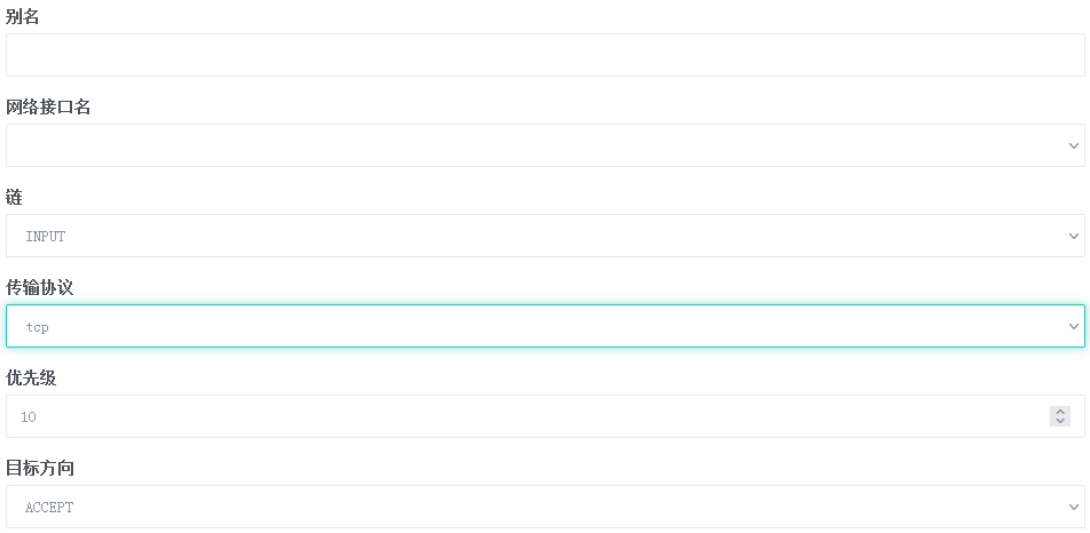


6.6.7 防火墙规则配置

防火墙规则基于 iptables，SBC 默认只开启管理和业务相关的端口，如 HTTP（默认 8090）、SSH（22），当新建或修改中继组时，会自动创建规则开启对应的业务端口，无需手动创建规则。

如有其他规则需求，可以手动创建或修改，但必须谨慎，防火墙规则配置错误可能导致系统无法访问。

配置内容	描述
别名	作为标识。
网络接口名	从系统已有的网络接口中选择，为空则代表所有网络接口。
链	INPUT 代表进来的数据包，OUTPUT 代表出去的数据包。
传输协议	支持 TCP、UDP 和 ICMP。
优先级	作为规则排列的顺序，数字越小优先级越高。
目标方向	ACCEPT 代表接收数据包，DROP 代表丢弃数据包。
源 IP	数据包的来源 IP，为空代表任意 IP。
源端口	数据包的来源端口，为空代表任意端口。
目标 IP	数据包的目的 IP，为空代表任意 IP。
目标端口	数据包的目的端口，为空代表任意端口。
iptables 拼接后缀	基于 iptables 命令的一些其他参数。



源IP

源端口

目标IP

目标端口

iptables拼接后缀

6.6.8 FILTER 规则查询

查询当前 FILTER 表的规则。

防火墙查询

查询filter表的详细信息：<hr>Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target   prot opt in   out   source   destination
 327K   25M RTPENGINE udp -- *   *   0.0.0.0/0   0.0.0.0/0   RTPENGINE id:0
 1876 132K ACCEPT   udp -- *   *   0.0.0.0/0   0.0.0.0/0   udp dpts:40000:60000
 3729 592K ACCEPT   tcp -- *   *   0.0.0.0/0   0.0.0.0/0   tcp dpt:8090
28299 2038K ACCEPT   tcp -- *   *   0.0.0.0/0   0.0.0.0/0   tcp dpt:22
    0   0 ACCEPT   icmp -- *   *   0.0.0.0/0   0.0.0.0/0
    0   0 ACCEPT   udp -- *   *   0.0.0.0/0   10.10.220.32   udp dpt:5060
    0   0 ACCEPT   tcp -- *   *   10.10.220.31   10.10.220.30   tcp dpt:9400
    0   0 ACCEPT   tcp -- *   *   10.10.220.31   10.10.220.30   tcp dpt:6379
    0   0 ACCEPT   tcp -- *   *   10.10.220.31   10.10.220.30   tcp dpt:9680
    0   0 ACCEPT   udp -- *   *   192.168.220.40   192.168.220.30   udp spt:5060 dpt:5060
    0   0 ACCEPT   udp -- *   *   192.169.220.40   192.169.220.30   udp spt:5060 dpt:5060
    0   0 ACCEPT   udp -- *   *   0.0.0.0/0   10.10.220.32   udp dpt:5060
8010K 1111M ACCEPT   all -- *   *   0.0.0.0/0   0.0.0.0/0   state RELATED,ESTABLISHED
  453 27133 ACCEPT   all -- lo   *   0.0.0.0/0   0.0.0.0/0
 278K   22M DROP   all -- *   *   0.0.0.0/0   0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target   prot opt in   out   source   destination

Chain OUTPUT (policy ACCEPT 8050K packets, 1127M bytes)
 pkts bytes target   prot opt in   out   source   destination

Chain FORWARD_IN_ZONES (0 references)
 pkts bytes target   prot opt in   out   source   destination

Chain FORWARD_IN_ZONES_SOURCE (0 references)
 pkts bytes target   prot opt in   out   source   destination

6.6.9 NAT 规则查询

查询当前 NAT 表的规则。

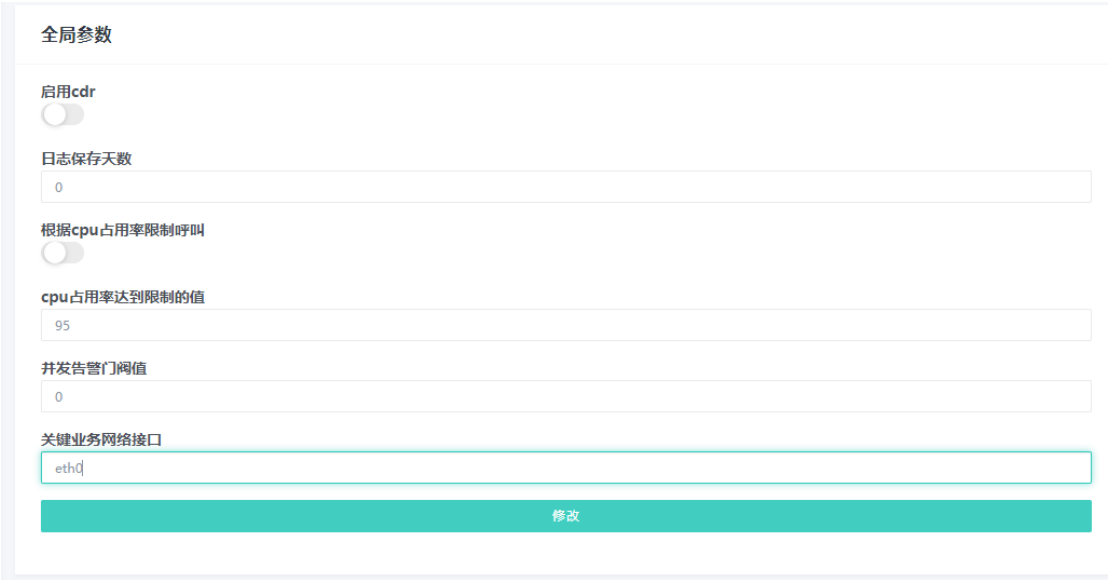
NAT查询

```
Chain PREROUTING (policy ACCEPT)
num  target     prot opt source               destination
1    PREROUTING_direct  all  --  0.0.0.0/0            0.0.0.0/0
2    PREROUTING_ZONES_SOURCE  all  --  0.0.0.0/0            0.0.0.0/0
3    PREROUTING_ZONES  all  --  0.0.0.0/0            0.0.0.0/0

Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
1    OUTPUT_direct  all  --  0.0.0.0/0            0.0.0.0/0

Chain POSTROUTING (policy ACCEPT)
num  target     prot opt source               destination
1    POSTROUTING_direct  all  --  0.0.0.0/0            0.0.0.0/0
2    POSTROUTING_ZONES_SOURCE  all  --  0.0.0.0/0            0.0.0.0/0
3    POSTROUTING_ZONES  all  --  0.0.0.0/0            0.0.0.0/0

Chain OUTPUT_direct (1 references)
num  target     prot opt source               destination
```

6.7 系统配置

6.7.1 全局参数

配置内容	描述
启用 CDR	把话单记录到数据库。
日志保存天数	设置日志保存的天数，日志会占用一定的存储空间。
根据 cpu 占用率限制呼叫	Cpu 占用限制呼叫开关
cpu 占用率达到限制的值	设置限制呼叫的 cpu 占用率阀值
并发告警门阀值	呼叫并发告警阀值
关键业务网络接口	配置关键业务网络接口，接口异常将产生告警。



6.7.2 系统参数

配置内容	描述
系统时区	系统时区配置
系统时间	系统时间配置
NTP 服务器	NTP 服务器 开关功能
节点配置	客户端 或 服务端选择
NTP 服务器地址	NTP 服务器地址配置

6.8 双机热备

采用两台相同配置的 SBC，通过主备切换方式实现高可用性。

主备 SBC 使用的是相同的业务 IP 地址（浮动 IP 地址）对接业务，正常情况下主 SBC 自动设置业务 IP 地址对接业务，当主 SBC 故障时将自动切换改用备 SBC 接管业务（主 SBC 将清除业务 IP 地址，备 SBC 将转为主机设置业务 IP 地址继续提供服务）。

发生切换时已接通的呼叫能够继续保持，正在建立中的呼叫则被丢弃，整个切换过程可在 1~2s 内完成，切换完成后才可以建立新的呼叫，原主 SBC 故障恢复正常后将自动转为备 SBC。

6.8.1 HA 配置

注意修改 HA 配置后必须重启机器才生效，建议修改完同时重启机器，避免配置内容和实际生效的不一致。

配置内容	描述
是否启用	是否启用。
本机 IP	本机 IP，用于两台机器之间通信。
远端 IP	另一台机器 IP，用于两台机器之间通信。
VIP	浮动 IP，用于对接业务。目前支持 2 个 VIP，从系统已有的网络接口中选择接口，配置 IP 和掩码。
ARP Ping 远端 IP	可选项，设置一个目的 IP，启用 arp ping 功能。如果持续收不到该 IP 的 arp reply，则认为本机网络故障，变为离线状态，此时本机是“主机”状态的话则发生切换；后续重新收到 arp replay 后恢复在线状态。

6.8.2 HA 同步

在两台机器的 HA 配置（参考 6.8.1HA 配置）都完成的前提下，将本机的配置（除了网络和 SIP 栈配置）同步到另一台机器（即时生效）。

正常情况下在任意一台机器所做的配置都会自动同步到另一台机器，无需人工同步。

6.8.3 HA 状态

查看两台机器的状态，状态为“主机”表示当前获得 VIP，接管业务；状态为“备机”表示机器正常，处于热备状态；状态为“离线”表示机器故障（内部资源或网络问题）或者人工强制了离线，无法热备。

如有需要，可以强制将机器设为“在线”或“离线”。


HA状态
分类
ip
状态
强制 在线/离线
本地机器
10.10.220.31
主机
冗余机器
10.10.220.30
离线

7 状态监控

7.1 当前通话信息

查看当前的通话信息。

7.2 代理注册信息

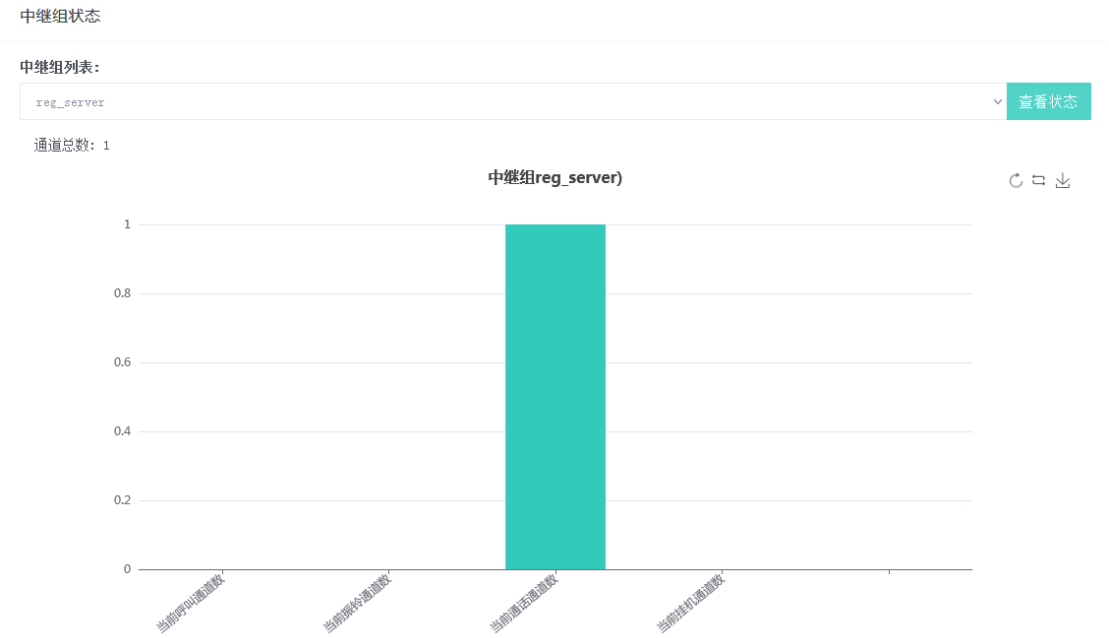
查看当前的代理注册信息。

7.3 CDR 话单

在启用 CDR 的前提下，可以查看已结束通话的话单。

7.4 中继组状态

查看某个中继组的当前呼叫状态数据。



7.5 中继组呼叫并发量统计

查看中继组（一个或多个组合）最近 7 天的呼叫并发量量统计，每 5 分钟统计最大值。

7.7 中继组呼叫总量统计

查看中继组（一个或多个组合）最近 7 天的呼叫总量统计。
时间颗粒度: 可选 5 分钟 1 小时、1 天为颗粒度统计
输出的曲线为，呼入总量，呼出总量，和总的呼叫量。

7.8 告警查询

查询系统告警信息日志。

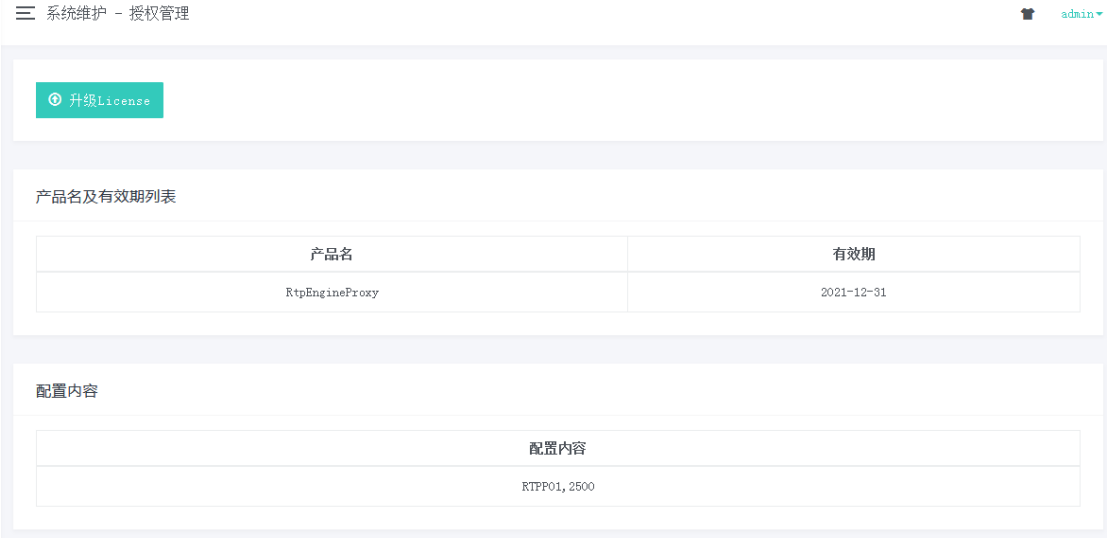
8 系统维护

8.1 抓包分析

为方便查找问题，可以在 SBC 上根据添加的条件（网口、协议、端口等）进行抓包，抓包完成后可以下载并使用 wireshark 工具进行分析。

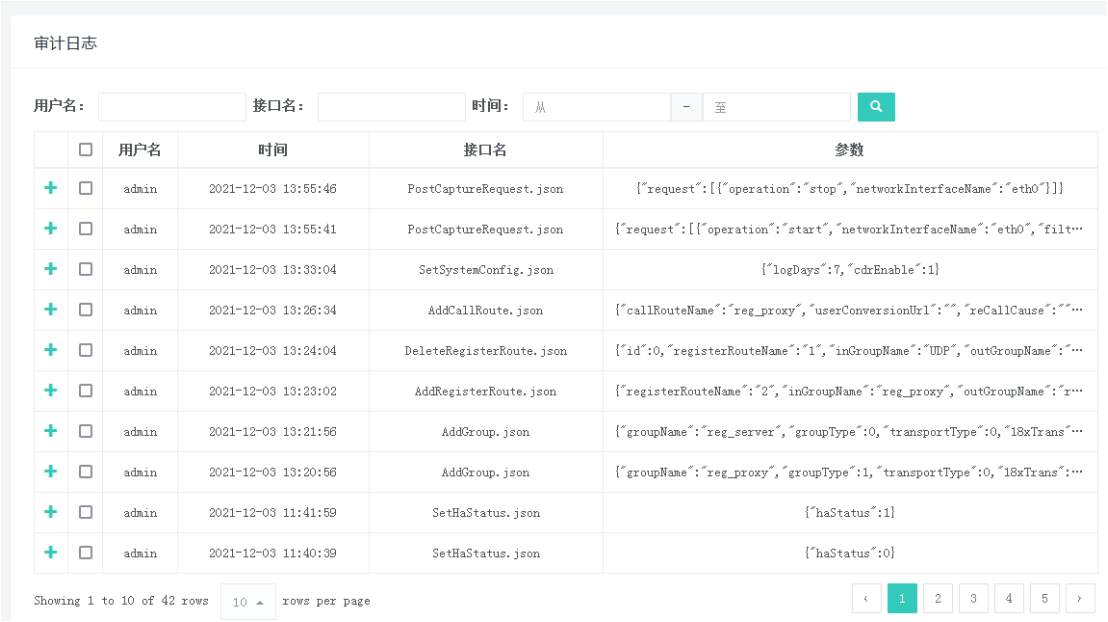
8.2 授权管理

可查看当前授权的产品信息，或者进行授权更新操作。



8.3 审计日志

提供 WEB 操作记录的查询，方便追溯因配置或操作错误引起的问题。



8.4 重启 WEB 服务

重启 WEB 服务，不影响业务。

8.5 重启网络服务

重启网络服务，会影响业务，需谨慎。

8.6 重启 iGateway

重启主程序 iGateway，会影响业务，需谨慎。

8.7 重启机器

重启机器，会影响业务，需谨慎。

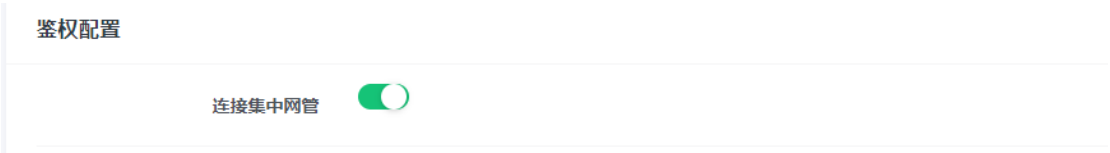
9 集中网关配置

9.1 鉴权配置

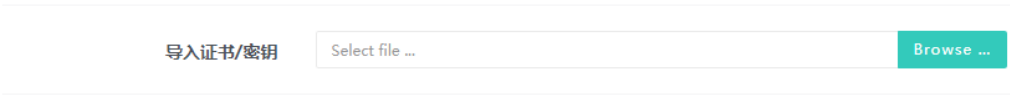
集中网管鉴权配置和使能。

导入证书秘钥，配置 kafka 主机名，kafka 服务器 ip 地址和端口号

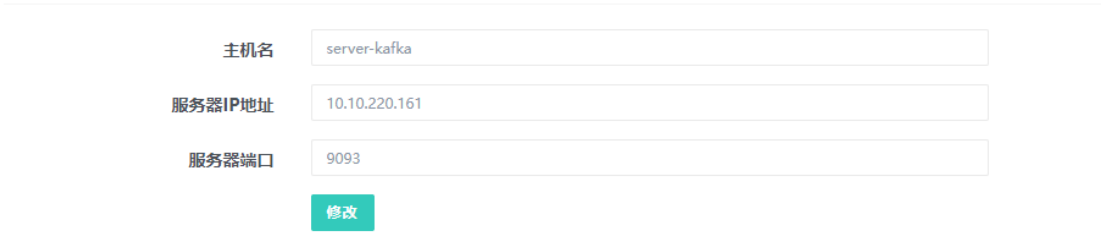
使能开关：



导入证书：



主机服务配置：



配置主机名，ip ,端口：

注意！上传证书和主机配置相关 ，需进行使能开关按钮，关闭操作，避免相关模块配置不同步问题。请先停用连接集中网管功能，再进行配置。

10 获得帮助

感谢您关注和使用本公司的产品，希望我们的产品能实实在在的带给您帮助，解决您的需求。

如果您有问题或疑问，请先仔细阅读本系统提供的相关文档，尤其是相关FAQ，里面有常见问题的恰当处理方法。

如果没有找到问题的答案，请访问我们的网站：http://www.ehangcom.com，查找有关最新消息或问题解答；或者在我们网站上的“联系我们”栏目找到我们的技术支持电话，我们将会热忱为您解答。