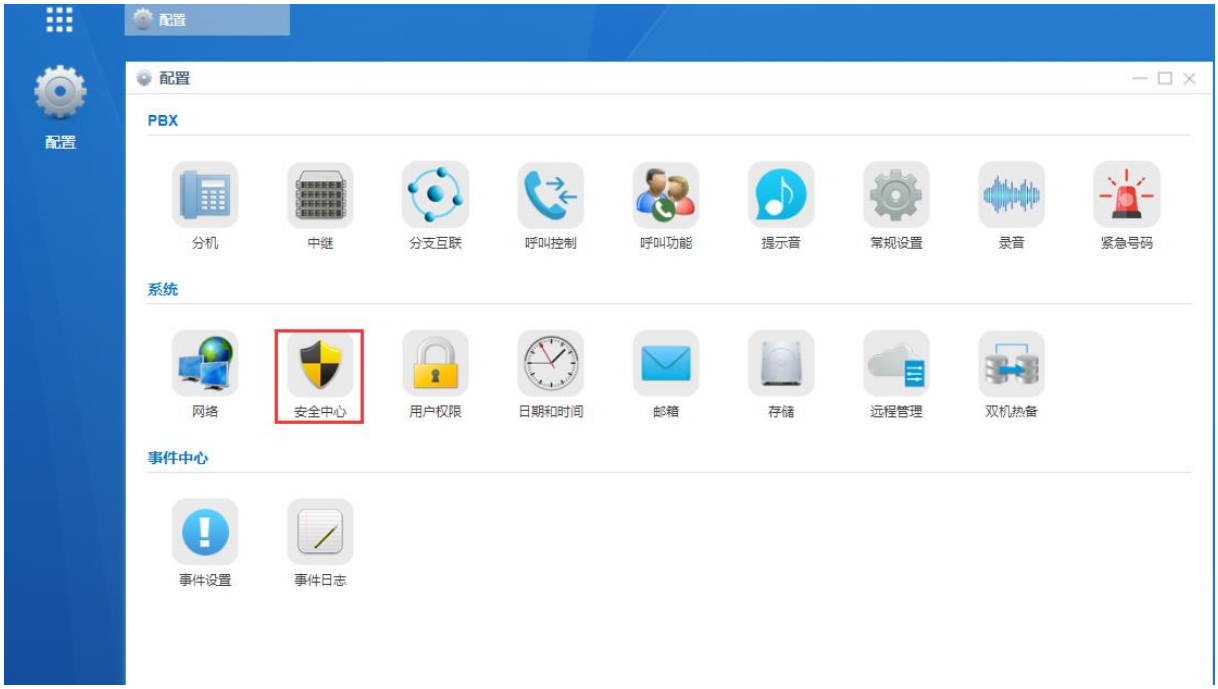
S 系列防火墙配置

首先登录到 S 系列。这里示例环境中内网网段位 192.168.9.0/255.255.255.0

其中 S100 的 IP 地址为 192.168.9.153

点击配置 - 安全中心 可进入防火墙配置菜单



一、同网段中的部分话机经常被 S 系列拉黑，需要手动清理 IP 黑名单

遇到这种情况是，就需要在 S 系列里面添加针对 IP 的白名单。首先在安全中心 - 防火墙规则中点击添加

1. 动作选择接收

2. 协议选择 BOTH

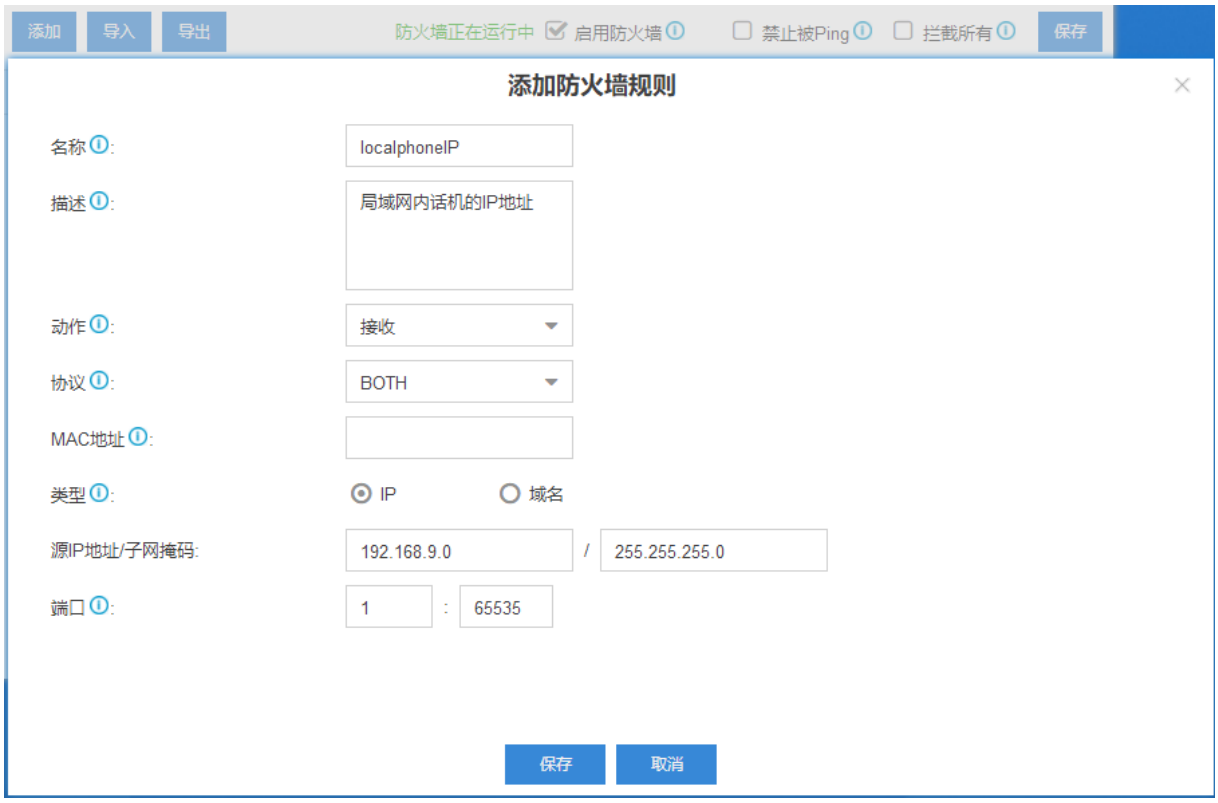
3. MAC 地址可不填。在类型中选择 IP。输入局域网的 IP 地址以及掩码

   192.168.9.0/255.255.255.0

4. 端口选择 1-65535

在这样的设置下，所有 192.168.9.0/24 段的都已经成为本台 S 系列上面的白名单 IP。

注：防火墙需要处于开启状态。 



二、设备映射到公网，内网放行，外网只限定几个 IP 可以访问。

遇到这种情况需要在一的基础上开启拦截所有。

在这样的设置下，所有白名单之外的 IP 都会被 S 系列拦截，如果还需要额外几个 IP 访问到 S 系列。就需要单独再添加白名单。

按照下图设置，8.8.8.8 这个 IP 可以通过外网访问到 S 系列的 5060，也就是 UDP 注册端口。具体可根据需求来放行，以下附上几个常用端口。

5060	UDP/TCP	SIP 端口
80/8088	TCP	页面访问端口
8022	TCP	SSH 端口

10000-12000	UDP	RTP 端口
8111	UDP/TCP	LINKUS 端口

三、未开启拦截所有的情况下，禁止某个 IP 访问指定端口

比如，管理员需要禁止 192.168.9.43 这个 IP 访问设备的页面，但是又可以进行 SIP 注册。需要在防火墙规则中点击添加，新建防火墙规则。具体如下图所示。


添加防火墙规则
名称:
example
描述:
动作:
拦截
协议:
TCP
MAC地址:
类型:
IP
域名
源IP地址/子网掩码:
192.168.9.43
/
255.255.255.255
端口:
8088
:
8088