语音设备安全防范措施

说明

（1） 下文中的“设备”、“语音设备”均指 国威 IPPBX 系列语音交换设备（含国威 HB100、HB1910、HB1930、HB1960、HB1981 等型号)。

（2） 下文中的截图，均为国威 IPPBX 设备的截图为例。

（3） 若您有任何疑问，请拨打技术支持热线 400-800-5056、0755-86662590。

语音设备作为公司的电话交换设备，给公司的日常通信和沟通带来便利，但是如果配置不当，很容易被黑客或者恶意分子利用，进行电话盗打行为，给公司带来损失。

电话盗打分如下几种情况：

- 设备暴露在公网上（WAN 口配置了公网地址，或者是 LAN 接入客户内网)，没有采取防火墙等措施，容易被黑客攻击，黑客一旦获取了 SIP 账号，就可以远程 SIP 注册过来盗打电话。
- 设备是采用 web 页面进行管理的，默认登陆密码过于简单，如果没有修改，别人就可以登陆到设备获取 SIP 账号，或者其他方式泄露 SIP 账号出去。通过 SIP 账号，就可以远程 SIP 注册过来盗打电话。

为了防止电话被盗打，需要做好各项安全配置。如下，

1. 不要将语音设备接入数据网络（包括公网、企业内网)，恶意分子进行电话盗打都是通过 IP 网络进行的 VOIP 电话拨打，只要物理上进行了链路隔绝，便可防止此类恶意盗打。
2. 修改设备的出厂 web 登陆密码，出厂分机注册密码，出厂 SIP 信令端口。

1. 登陆密码管理

设备开局后（不管设备能否上网）必须更改设备的 web 页面登陆密码，密码需要含有：数字、大小写字母、特殊字符（~！@#￥%%&）等未修改出厂密码时，每次登录 web，都会提示更改密码。如下图（国威 HB1930 为例）：

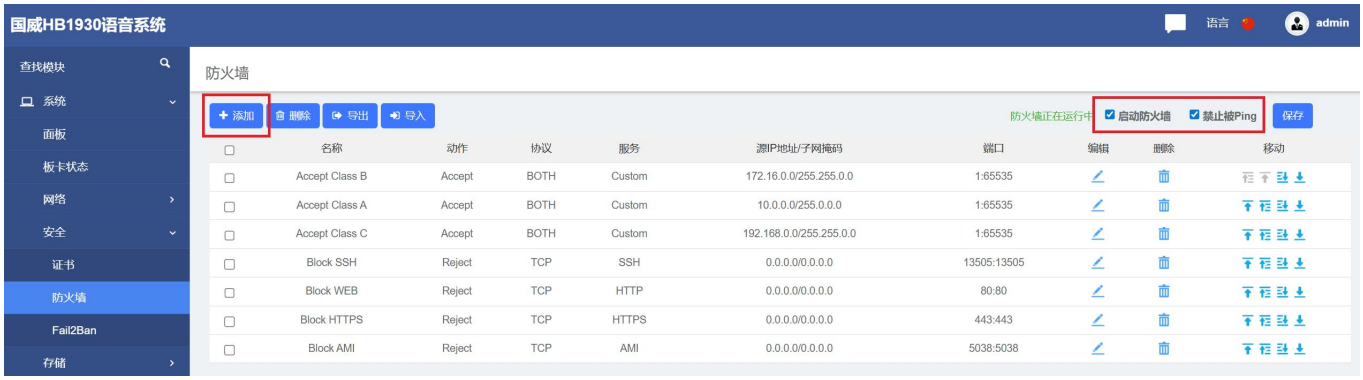
网页右上角，点击 admin ，出现如下图菜单，可以修改密码

2. 防火墙配置

为了增强 IPPBX 的网络安全，设备调试完成后必须开启防火墙功能，且开启设备禁 ping 功能和关闭允许远程注册功能，无特别需要关闭远程 web 页面登陆。

登陆设备，进入 系统 >> 安全 >> 防火墙 界面，对防火墙功能进行设置。

启用防火墙，禁止被 Ping，添加访问策略，如下图，



3. 用户权限控制

为了防止用户被黑客攻击后盗打电话情况的发生，客户在使用配置用户分机权限的时候尽量根据实际情况配置。如用户电话只有市话业务，可以给该分机设置市话权限；如用户电话只有国内长途业务，可以给该分机设置国内长途权限。

用户分机权限设置如下：

4. SIP 协议端口设置

修改设备 SIP 信令端口（默认端口为 5060），尽可能降低设备被扫描定位的几率。

登陆设备，进入 PBX>>设置>>SIP 设置 界面，对 UDP 监听端口进行更改，如下图，

5. SIP 用户设置

1. 配置 SIP 用户，注册密码一定要设置复杂，设置大小写字母，特殊字符串和数字的组合

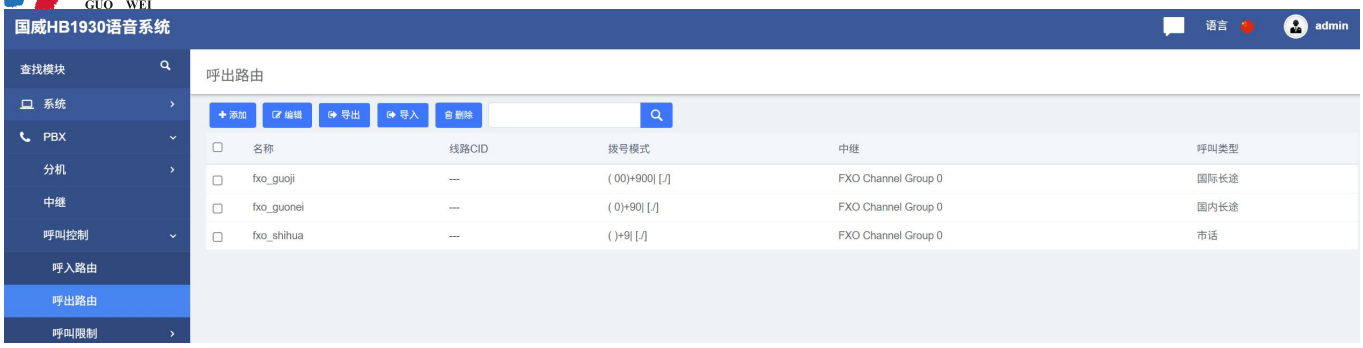
2．分机---高级，开启 IP 限制，填写允许注册此分机的 IP 地址和子网掩码

6. 防 SIP DOS 攻击设置

国威 IPPBX 为了防止黑客攻击，在设备里面增加了防 SIP DOS 攻击功能，增加了 IPPBX 的安全性。SIP 账户向 IPPBX 发起注册请求，同一 IP 地址在指定周期内如果注册失败次数达到最大值，该 SIP 账户主机 IP 地址将系统被拉入黑名单，IPPBX 将对该 IP 地址发起的注册请求不响应。

7. 合理配置用户权限、呼出路由权限

对于具有国际长途权限的呼出路由，应当配置成国际长途呼叫类型，当用户权限大于或者等于呼出路由呼叫类型，才能使用这条路由，所以只有具有国际长途权限的用户才能从此呼出路由呼出。如下图所示，



上图中配置有三条呼出路由，出局前缀为 9。呼叫权限从上到下依次是：国际长途、国内长途、市话。

1. 当客户拨打市话时，拨打的号码为“9+号码”，会走上图中第三条呼出路由（该路由权限为市话），如果用户权限大于或者等于市话权限，则可以呼出，否则不可以呼出。

2. 当客户拨打国内长途时，拨打的号码为“90+号码”，会走上图中第二条呼出路由（该路由权限为国内长途），如果用户权限大于或者等于国内长途权限，则可以呼出，否则不可以呼出。

3. 当客户拨打国际长途时，拨打的号码为“900+号码”，会走上图中第一条呼出路由（该路由权限为国际长途），如果用户权限大于或者等于国际长途权限，则可以呼出，否则不可以呼出。

8. 删除无用或者测试账号，防止被他人利用

9. 建议去电信运营商办理每月话费限额或者时长限额

例如企业如果平均每月消费 8000 元话费，可以去办理限额为 1 万元，这样即使电话被盗打，也不能超过 1 万元，减少损失。每月定期检查话费账单，观察是否有可疑话费产生。

10. 对 VOIP 通信的保护

建议客户选择专业的 VPN（虚拟专用通道）对 VOIP 通信进行保护，减少被黑客攻击的风险和 SIP 用户被盗打的概率，从而保护 VOIP 通信安全。