

DBL 网关使用 AVS 加密手册

1. 软件要求:

网关软件版本 3.15-2 或以上版本。下载地址:

<http://202.96.136.145/update/A38HS-3.15-2.pkg>

2. 网关配置:

进入网关配置页面，在呼叫设置，击启用 VOS/AVS 加密，在弹出菜单点可选择 AVS 信令加密和 AVS 信令媒体全加密。保存改动，即可启用网关的 AVS 加密功能。

如图:

呼叫设置	
终端类型	H.323终端
终端模式	关守模式
配置模式	单服务器模式
电话号码	999
显示名	
H.323 Id	h323.test1
关守地址	192.168.1.1
	<input checked="" type="checkbox"/> 启用VOS/AVS加密
加密模式	AVS信令媒体加密
拨号规则	VOS信令加密 VOS信令媒体加密 AVS信令加密 AVS信令媒体加密

3. 配置 AVS 加密服务:

启用网关的 AVS 加密功能，需要 AVS 加密服务器的配合。对默认安装的 AVS 加密服务配置文件做出修改。

使用 SSH 远程登录到安装了 AVS 的服务器。使用命令“cd /root/avs/spu”进入 /root/avs/spu 文件夹。命令 vi rncsrv.ini 编辑 AVS 加密服务的配置文件。

配置文件如下:

```
[RNSC]^M
UsedSecret=0
LocalIp=192.168.1.1
LocalIp2=^M
LocalPort=69,123,161,182,4000^M
VirtualLocalIpStart=192.168.1.1
VirtualLocalIpEnd=192.168.1.1
RTPSecretIP=192.168.1.1
RTPSecretPortStart=4001^M
RTPSecretPortEnd=4001^M
ClientVIPStart=192.168.1.1
ClientVIPEnd=192.168.1.1
```

需要对以下两行作出修改。

```
VirtualLocalIpStart=192.168.1.1
```

表示 AVS 加密使用的的虚拟 IP 起始地址。

```
VirtualLocalIpEnd=192.168.1.1
```

表示 AVS 加密使用的的虚拟 IP 结束地址。

加密虚拟 IP 是虚拟不存在本机的 IP 地址，起始地址和结束地址是一个 IP 范围，需要和服务器的真实 IP 地址同一网段，但这个 IP 范围不能包括 AVS 服务器的真实 IP 。

现在以我的 AVS 服务器，IP 地址 192.168.1.1 为例作修改，用于公网的服务器，需要根据自己的实现情况修改。

```
VirtualLocalIpStart=192.168.1.100
```

 起始地址改为 192.168.1.100

```
VirtualLocalIpEnd=192.168.1.200
```

 结束地址改为 192.168.1.200

服务器 IP 192.168.1.1 不在 192.168.1.100-200 这个范围内。

保存退出 vi 。

4. 重启 AVS 加密进程 rnserv:

执行命令: `killall rnserv` 停止 rnserv 加密进程。

```
/root/avs/spu/rnserv
```

 启动 rnserv 加密进程

让 linux 启动时自动启动 rnserv 加密进程:

执行命令: `echo "/root/avs/spu/rnserv" >> /etc/rc.local`

AVS 加密配置完成。