上海迅时通信设备有限公司

SX3000 企业级会话边界控制器

配置指南

网址：www.newrocktech.com
论坛：bbs.newrocktech.com
电话：021-61202700
传真：021-61202704

文档版本：201504

目　录

插图目录

表格目录

1.1 概述

SX3000 会话边界控制器（Session Border Controller，以下简称 SX3000）是迅时通信 VoIP 产品系列中的一款，用于跨接不同 IP 域内的 IP 语音话务，实现异地 IP 会话的互通和流量汇聚，提供网络安全保障。

作为企业 VoIP 整体解决方案中的重要部件，SX3000 通常部署在 VoIP 服务供应商网络的边缘（软交换平台和语音接入网关之间），用于将企业异地分支机构的 IP 会话方便而安全地接入到企业内网 (Intranet) 中的融合通信服务器（如 IP-PBX），另外也可以部署在企业/VPN 网络的出口，使企业内网中的融合通信服务器连接到运营商的 IP 通信业务网（如 IMS 平台）。

SX3000 执行 IP 语音互连的实时通信要求，如访问控制、防火墙穿越、信令互通、保障信息安全（加密与解密）、拦截非法访问以及对服务质量（QoS）进行管理等。同时提供友好的图形化 Web 操作界面，使用方便。

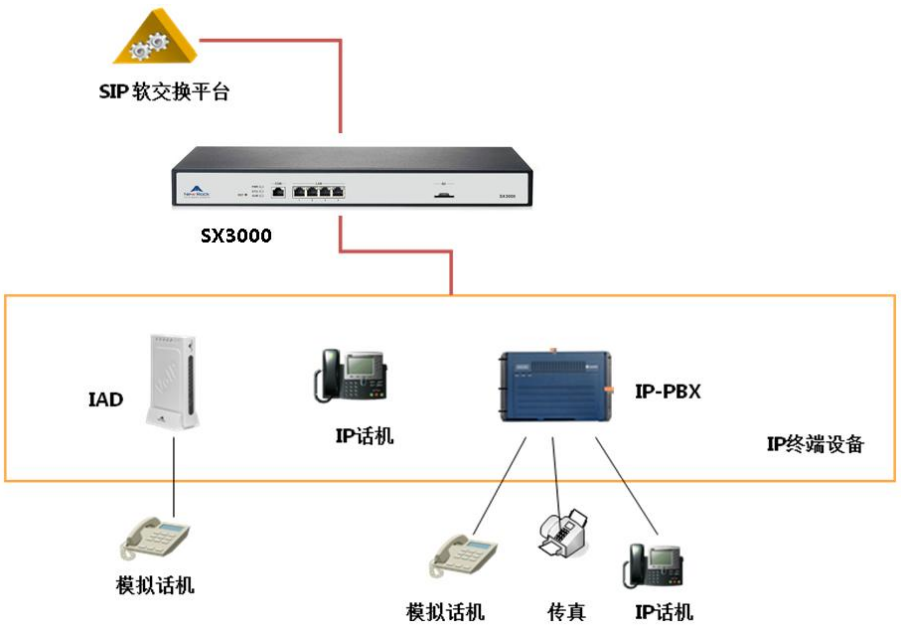
本文介绍 SX3000 的主要功能和配置步骤。

1.2 主要功能

SX3000 的主要功能包括：

- 提供多个网口，帮助实现不同 IP 域语音系统的跨接
- 提供信令和媒体加密（如 TLS/SRTP 等方式），提高信息安全性
- 过滤和拦截与业务无关的 IP 包，提高 IP 语音网安全性
- 终端设备注册和媒体代理

图1-1 SX3000 的典型应用



终端设备，如接入网关 IAD、IP 话机、IPPBX、软电话等，可以通过 SX3000 注册到 SIP 软交换

平台。终端设备无需知道软交换平台的地址信息，只要知道 SX3000 的地址和服务端口即可。SX3000 通过服务端口接收来自终端设备的信令消息。终端设备和 SX3000 之间可以使用加密的信令和媒体流，提高通信安全性。SX3000 对收到的加密消息进行解密，并对 SIP 消息中的终端地址及端口进行转换处理，将处理后的信令转发到该服务端口对应的软交换或 IMS 平台；从软交换回应的消息也会经过 SX3000 进行加密后，再转发给终端设备，进而完成整个呼叫。

1.3 配置步骤

步骤 1 登录用户界面

说明：登录设备配置界面的浏览器支持 IE9~IE11、火狐、谷歌。本文以 IE 浏览器为例进行说明。

在 IE 浏览器的地址栏中输入设备的 IP 地址：https://192.168.2.240（出厂缺省 IP 地址），在登录界面输入用户名、密码和验证码，即可进入配置界面。

注意

用 HTTPS 访问设备，如果未安装证书，IE 浏览器会提示“此网站的安全证书有问题”，单击“继续浏览此网站”进入。采用系统默认证书和公私钥对，存在安全风险，请用户及时替换为自己公司的证书和公私钥对。具体操作参见《管理员指南》的 2.6.2 SSL 证书管理。

图1-2 登录界面

登录用户分管理员和操作员两级，默认密码如表 1-1 所示。

注意

采用系统默认密码存在安全风险，请在首次登录后进入“系统工具”页面及时修改密码。

表1-1 默认登录密码说明

用户	默认密码	说明
admin	SX3000@123（必须大写）	管理员 admin 可进行所有配置
operator	operator@123（必须小写）	操作员 operator 只可浏览部分配置

注意

- SX3000 允许多人登录。多人登录时，先登录的管理员有修改权限，后登录的管理员只能浏览。
- 登录时需要输入的验证码有效时间为 90 秒，超时后请点击“刷新”重新生成验证码后输入。
- 以 admin 账号登录，如连续输错 3 次密码，则 10 分钟内将禁止 admin 登录，但允许 operator 登录。若再连续输错 operator 登录密码 3 次，则该 IP 地址在 10 分钟内禁止登录。
- 连续输错登录用户名 6 次，则该 IP 地址在 10 分钟内禁止登录。
- 登录后 10 分钟内未进行操作，系统认定超时。继续操作需重新登录。
- 配置完成后，请点击“注销”按钮退出，以免影响其他管理员的操作。

步骤 2 设置网络参数

设备出厂默认只启用网口 1，若需要使用多个网口，需给各网口配置不同网段的 IP 地址。点击“网络”，进入该配置界面。

图1-3 网络配置界面

步骤 3 设置软交换

点击“软交换”，进入配置界面。在对应的序号后面输入软交换 IP 地址和信令端口，格式示例：220.248.118.50:5060。SX3000 最多可设置 5 个软交换。

可根据软交换要求在 SX3000 上设置信令回复端口：

- 选择“朝对方发送端口回复”为“是”：表示 SX3000 根据信令从软交换发过来时的源端口进行回复。
- 选择“朝对方发送端口回复”为“否”：表示 SX3000 根据此处配置的软交换的信令端口进行回复。

图1-4 软交换配置界面

注意

- 填写软交换时，必须填写软交换的信令端口。
- 与华为 U1900 连接时，建议使用默认值“否”，否则可能会影响系统正常使用。
- SX3000 转发到软交换前会先判断是否有网口与软交换地址在同一个网段，若有，则通过该网口转发；若无，则通过与默认网关地址相同网段的网口转发。

步骤 4 设置服务端口

点击“服务端口”，选择终端设备所连的网口进行设置。

图1-5 服务端口配置界面

注意

- 服务端口是 SX3000 接收终端信令消息的端口。在端口上收到的消息，经处理后，SX3000 会根据端口上设置的软交换序号，将消息转发到对应软交换。
- 每个网口可以设置 5 个服务端口，端口值必须唯一，每个服务端口对应一个主软交换。每个服务端口

可以设置两个备份软交换。SX3000 开启心跳监测功能，可监测主软交换是否宕机。主软交换宕机时，如果存在正常的备份软交换，SX3000 自动切换到备份软交换，在主软交换故障排除后，重新切换回主软交换。

- 每个服务端口上的消息处理都可以设置是否加密，默认不启用加密。如果端口上设置了加密，则 SX3000 将先对该端口上收到的消息进行解密，再转发到对应软交换；反之，从软交换回来的消息，会先进行加密，再转发给终端设备。
- 语音加密方式：RTP（RTP 包整体加密）、RTP Header（RTP 头文件加密）或 RTP Body（RTP 包内容）。建议使用默认值“无”，否则可能会影响设备正常使用。
- 信令加密方式：TLS、TCP Not Encrypted、TCP Encrypted、UDP Not Encrypted、UDP Encrypted、Using Keyword、Using Keyword2 和 Encrypt 14 等八种加密方式。
- 启用加密时可以设置密钥（UDP Encrypted 、TLS 不需要加密密钥）。SX3000 上设置的密钥与对接终端设备使用的密钥必须一致。
- 选择 TLS 加密方式时，SX3000 将对 RTP 使用 SRTP 方式加密。选择 TLS 加密方式，需要设置 SSL 证书相关参数，详见步骤 5 SSL 证书管理。

步骤 5 SSL 证书管理

如果服务端口启用 TLS 加密方式，则需要配置本步骤。

点击“高级 > SSL 证书管理”，进入该页面。

图1-6 SSL 证书管理界面

配置参数描述

说明：SIP TLS 加密证书制作过程见**附录**。

- 证书口令：填写根证书口令，非必填项。

- 根证书文件名：制作的 SSL 根证书文件名称。网口 1~网口 4 使用同一根证书文件。
- 用户证书文件名(网口 1/2/3/4)：为网口 1/2/3/4 制作的用户证书文件名称。
- 用户密钥文件名(网口 1/2/3/4)：为网口 1/2/3/4 制作的用户证书密钥文件名称。

首次上传证书（通过 SFTP 服务器）

1. 把制作好（制作方法参见**附录**）的根证书文件 ca.crt、用户证书文件 client.crt 和用户密钥文件 client.key 拷贝到 **SFTP** 服务器的目录下。
2. 通过 Telnet 或 SSH 登录设备后，输入命令 cd /var/config（SX3000 基于 Linux 操作系统，所用命令同 Linux 系统），进入 config 目录。
3. 输入命令 sftp 用户名@xxx.xxx.xxx.xxx（**SFTP** 服务器的地址）以及密码登录 **SFTP** 服务器；
4. 输入命令 get ca.crt 将根证书文件下载到 SX3000 下。
5. 输入命令 get client.crt 将用户证书文件下载到 SX3000 下。
6. 输入命令 get client.key 将用户密钥文件下载到 SX3000 下。
7. 输入命令 exit 退出 sftp。
8. 输入命令 reboot 重启 SX3000。

证书导出（通过 SFTP 服务器）

1. 通过 Telnet/SSH 登录设备后，输入命令 cd /var/config（SX3000 基于 Linux 操作系统，所用命令同 Linux 系统），进入 config 目录。
2. 输入命令 tar cvzf ssl_cert.tar.gz /var/config/client.crt /var/config/client.key /var/config/ca.crt /var/config/bin_version 打包，生成文件 ssl_cert.tar.gz。
3. 将 ssl_cert.tar.gz 文件上传至 SFTP 服务器上。


注意

后续若要再导入证书，可登录 Web 管理页面，进入 SSL 证书管理，在 SIP TLS 加密证书上传 处选择 tar 包上传即可。

步骤 6 安全管理

点击“高级 > 安全管理”，设置安全管理。

可以选择开启或关闭 Telnet/SSH 服务。关闭后，终端将无法通过 Telnet/SSH 登录设备。

SX3000 可以灵活设置访问控制，具体请参考 linux 下 iptables 相关使用文档。


注意

- **设备默认关闭 Telnet/SSH 服务。**
- **添加访问控制命令时，需要在命令前加路径 /var/run/，示例如下：**

  /var/run/iptables -A INPUT -s 10.128.23.23 -p tcp --dport 80 -j ACCEPT
- **错误的访问控制配置可能导致无法通过网口访问设备。**

配合华为 U1900 使用时，以下配置参数建议使用出厂默认值。

表1-2 配置参数默认值

配置界面	参数名	出厂默认值
软交换	朝对方发送端口回复	否
服务端口	语音加密	无
高级	语音流转发	转发
	语音流中断检测时长	300
	NAT 穿越	是

附录：SIP TLS 加密证书制作


注意

SX3000 目前支持 sha、sha1、sha256 算法。

创建根证书 CA

在装有 OpenSSL 的 Linux 环境下，执行以下步骤：

步骤 1 创建根证书密钥文件（建议密钥长度≤1024)

openssl genrsa -des3 -out ca.key 1024

看到输入证书口令提示后，输入字符串作为密码，后面的输入密码均使用此密码。输入密码后将生成密钥文件 ca.key。

步骤 2 创建签名的根证书文件（需用到步骤 1 中创建的密钥文件 ca.key）。

openssl req -new -x509 -days 9000 -key ca.key -out ca.crt

看到输入密码提示后，请输入与步骤 1 相同的密码。

根据提示，输入其他相关信息，下面示例中的加粗部分仅供参考：

Country<97> ***CA***

State or Province<97>***British Columbia***

Locality (city or town)<97>***Burnaby***

Organization Name<97>***NewrockTech Inc***

Organizational Unit Name<97>***Voice***

Common Name<97>***NewrockCA***

E-mail address<97>***admin@newrocktech.com***

最终生成证书文件 ca.crt。

创建用户证书

步骤 1 创建用户证书密钥文件（建议密钥长度≤1024)

openssl genrsa -out client.key 1024

生成用户证书密钥文件 client.key。

步骤 2 创建用户证书请求文件

openssl req -new -key client.key -out client.csr

根据提示输入相应信息，下面示例中加粗部分仅供参考：

Country<97> ***CA***

State or Province<97>***British Columbia***

Locality (city or town)<97>***Burnaby***

Organization Name<97>***NewrockTech Inc***

Organizational Unit Name<97>***Voice***

Common Name<97>*此处要输入* ***SX3000*** *对应加密网口的* ***IP*** *地址*

E-mail address<97>***admin@newrocktech.com***

根据提示输入**密码**

An optional company name: ***NewRock***

最终生成文件 client.csr。

步骤 3 用根证书对用户证书请求签名并生成用户证书文件

openssl x509 -days 9000 -CA ca.crt -CAkey ca.key -req -CAcreateserial -CAserial ca.srl -in client.csr -out client.crt

根据提示输入**密码**

最终生成用户证书文件 client.crt

Common Name 后面需要输入 SX3000 对应加密网口的 IP 地址。例如：在网口 1 上使用 TLS 服务，为网口 1 制作用户证书，则需在此处输入网口 1 对应的 IP 地址。而生成的用户证书只适用于 SX3000 网口 1。在 SX3000 Web SSL 证书管理界面，填写格式参照图 1-6 SSL 证书管理界面，文件名与实际制作名称相同。