New Rock Technologies, Inc.

SX3000 Enterprise Session Border Controller (SBC)

Quick Configuration Guide

Website: http://www.newrocktech.com
Email: gs@newrocktech.com

Document version: 201504

Contents

Contents of Figure

Contents of Table

1.1 Scope of This Guide

This note is applicable to the SX3000 SBC product.

1.2 Introduction

The SX3000, an enterprise SBC (Session Border Controller), is a member of VoIP product family developed by New Rock Technologies, Inc. It interconnects voice communication over different IP networks and provides security schemes to protect the network from attacks and the privacy of communications. It implements both interconnectivity and traffic convergence for remote IP sessions.

As an important component of the integrated VoIP solution for enterprises, the SX3000 is typically deployed on the border of VoIP service network (between SIP server and SIP UA), through which IP sessions from remote branches to the IP-PBX in headquarter over VPN or the Internet are easily and reliably connected. In addition, the device can also be deployed at the egress of the enterprise/VPN network for connection between converged communications server for Internet and the IP communication service network (such as the IMS) of the carrier.

The SX3000 implements the real-time communication requirements for IP voice interconnection, including access control, NAT and firewall traversal for SIP messages and RTP packets encryption and decryption), interception of illegal calls, and QoS management. It also offers user friendly Web-based GUIs to facilitate operations.

This guide describes the basic functions and the configurations.

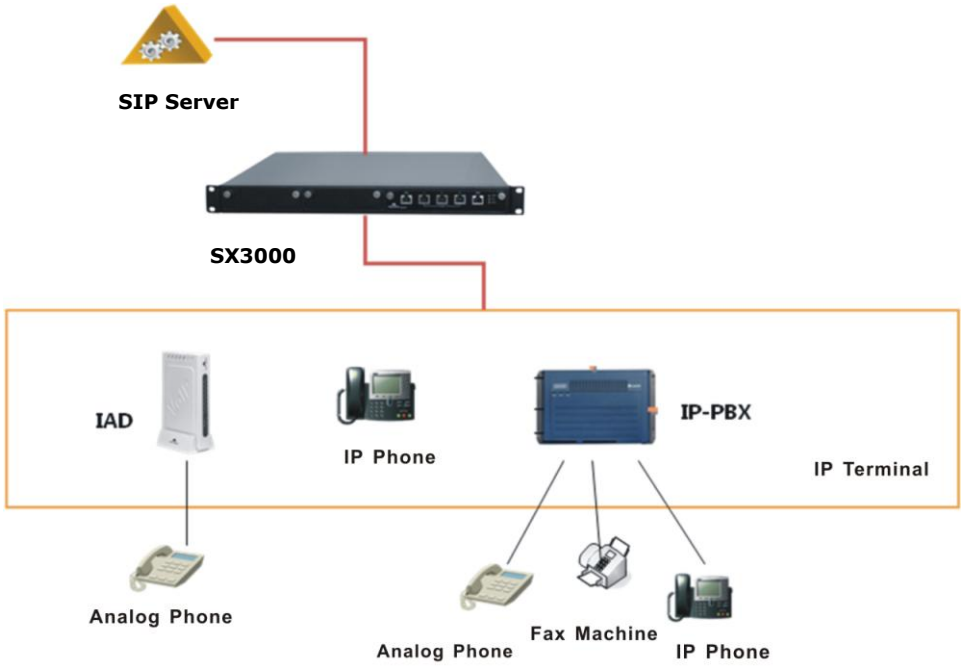
1.3 Main Features and Advantages

The main functions of the SX3000 are:

- Providing multiple network ports to interconnect voice systems in different IP domains.
- Encryption and decryption of signaling and voice media streams, including TLS/SRTP
- Filtering out and intercepting service-unrelated IP packets to enhance security of the IP voice network.
- Terminal device registeration and media service proxy.

The diagram below shows a typical deployment scenario of SX3000.

Figure 1-1 Typical Application of the SX3000



Note

The terminal devices, such as VoIP gateway, SIP phone, IP-PBX and soft-phone, are registered to the SIP registration server through SX3000. In this type of application, the terminal devices are not required to configure URL of the SIP registration server; instead, only the address of SX3000 and its designated service port are to be configured. Through the service port, the SX3000 receives the packets from the terminal devices.

The signaling and media stream between the terminal devices and the SX3000 can be encrypted to enhance communication security. The SX3000 decrypts the received encrypted packets and implements conversion of the terminal addresses and ports of SIP messages, then transfers the signaling to the SIP server or IMS platform corresponding to the service port. The SX3000 also encrypts the packets received from the SIP server and then transfers them to the terminal devices to complete the call.

1.4 Quick Configuration

Step1 Logon

Note: The device configuration interface can be accessed using browsers such as IE 9 – IE 11, Firefox, and Google. The IE browser is used as an example below.

Enter the factory default IP address for the SX3000 in the address bar of the browser: https://192.168.2.240. Enter the username, password and authentication code.

Note

If you access the device using HTTPs and have not installed a security certificate, the IE browser will display this error message: *There is a problem with this website's security certificate*. In this case, click **Continue to this website**. If you use the default certificate and public/private key pair, the system will be at risk. You should replace them with the certificate and public/private key pair of your company. For details, see 2.6.2 SSL Security Management in the *Administrator Guide*.

Figure 1-2 Login Interface

Login users are classified into **administrator** and **operator**. For the default password, see Table 1-1.

Note

To eliminate a security risk, please change the default password on the **System Tools** interface after first login.

Table 1-1 Default Login Password

User	Default Password	Description
admin	SX3000@123	An administrator can configure all parameters.
operator	operator@123	An operator can only view some parameters.

Note

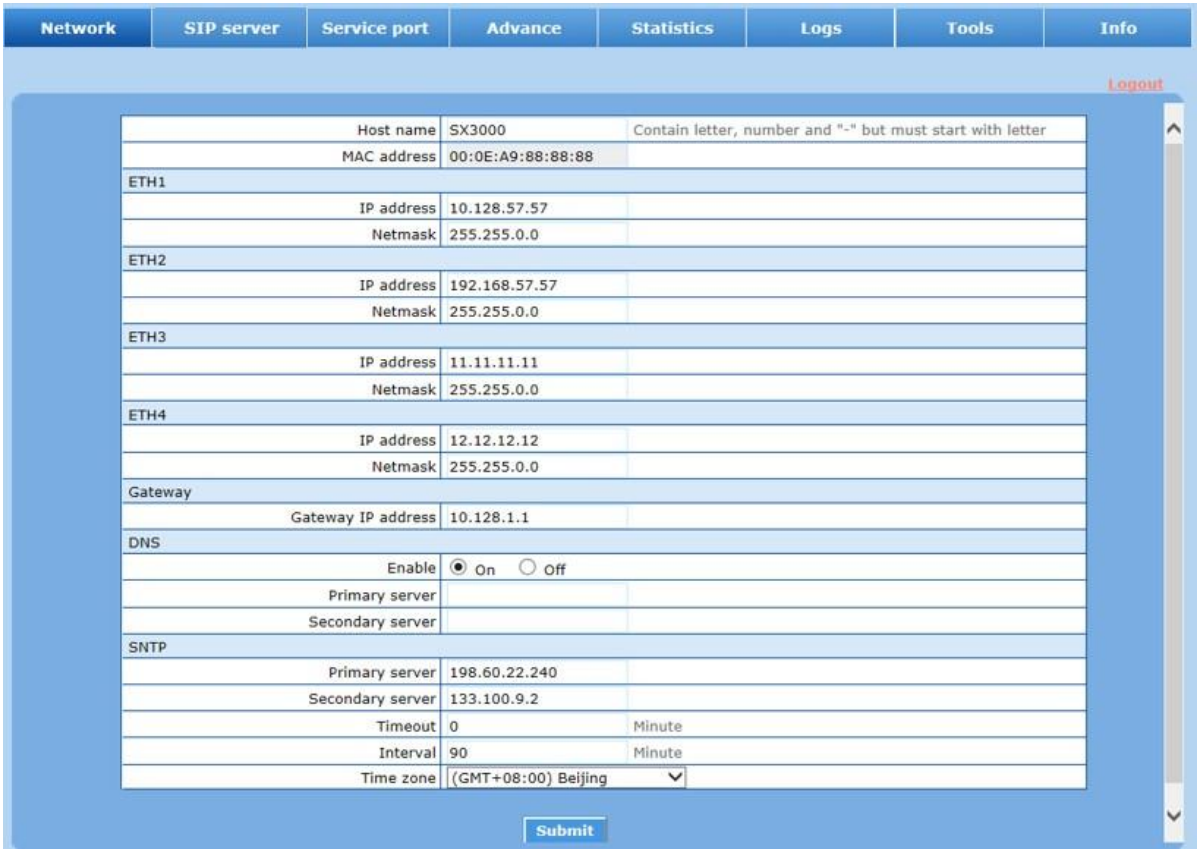
- The SX3000 supports concurrent access from multiple users. When multiple users are accessing the SX3000, the administrator accessing the device first is allowed to modify configuration, and subsequent administrators are only allowed to view the configuration.
- The verification code for login is valid for 90 seconds. Upon expiration of the verification code, please click **Refresh** to generate a new verification code, and then enter it.
- When logging in using the **admin** account, if the password is entered incorrectly three times, the account will be inaccessible for 10 minutes, but the **operator** account is allowed. When logging in using the **operator** account, if the password is entered incorrectly three times, the IP address will be forbidden for 10 minutes.
- If the username is entered incorrectly six times, the IP address will be forbidden for 10 minutes.
- The system will confirm timeout if users do not conduct any operation within 10 minutes after login. They are required to login again for continuing operations.
- Upon completion of the configuration, click **Logout** to return to the login page, so as not to affect the login permission of other users.

Step2 Network Configuration

ETH1 is the factory default Ethernet port. If multiple network ports need to be used, you need to configure IP addresses in different network segments.

Click **Network** to enter the configuration interface.

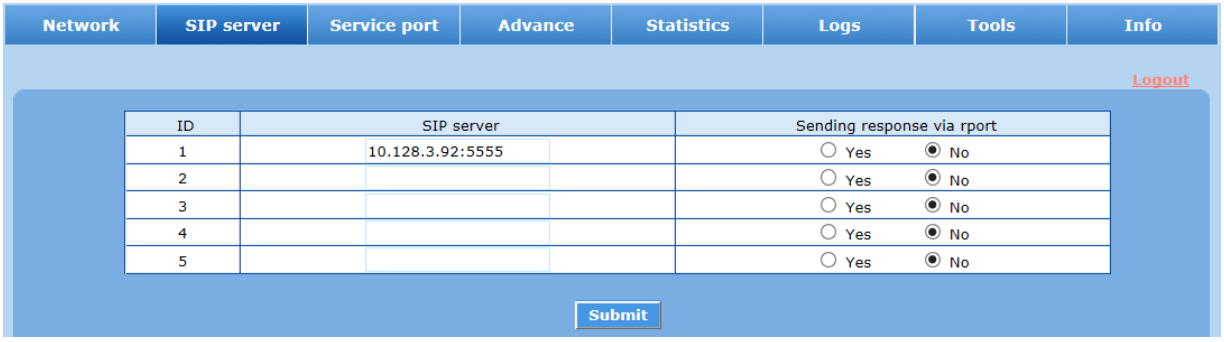
Figure 1-3 Network configuration interface



Step3 SIP server Configuration

Click **SIP server** and enter the configuration interface of SIP proxy. Up to five SIP proxies can be added. Each proxy starts with an ID and followed by the IP address of the proxy including the address and the UDP port, e.g. 220.248.118.50:5060. Select **Yes** for **Sending response to rport** if SX3000 needs to send response messages to the sending port of the proxy. Otherwise, select **No**.

Figure 1-4 SIP server Configuration Interface



Note

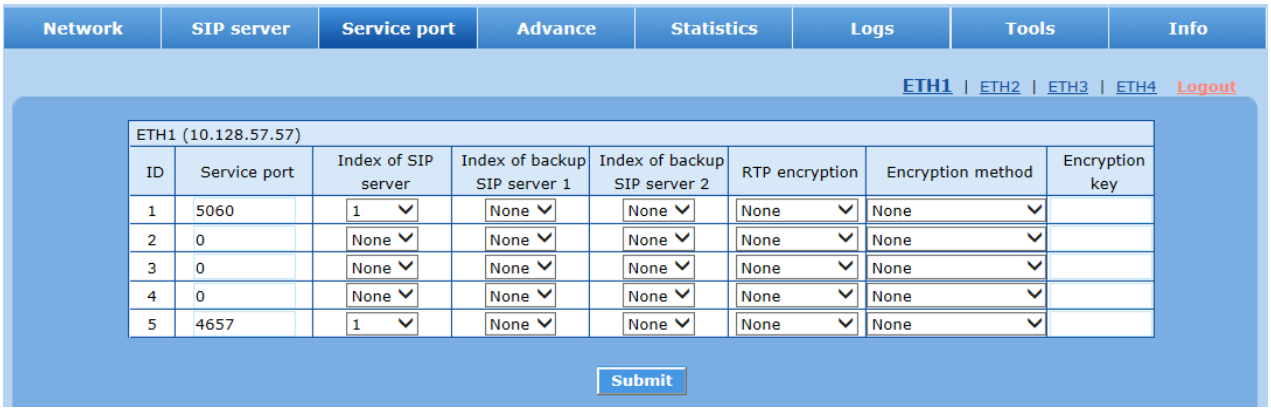
- The signaling port for the SIP server must be specified.
- When SX3000 is deployed with Huawei SoftCo, it is recommended to use “No” for this parameter.

- Before transferring packets to the SIP server, the SX3000 determines if any network port is in the same network segment with the SIP server IP address. If yes, the SX3000 transfers the packets using the detected port; if no, the SX3000 transfers the packets using a network port in the same network segment with the IP address of the default gateway.

Step4 Port Configuration

Click **Service port** to configure the Ethernet ports.

Figure 1-5 Service Port Configuration Interface



Note

- The service port is used to receive the SIP messages from terminals, which will be processed and redirect to the SIP server associated to the port.
- Up to five service ports can be configured on SX3000, each associated with a primary SIP server and its backup SIP servers.
- Up to two backup SIP servers can be associated with a service port, Backup 1 and Backup 2. When heartbeat function on SX3000 is enabled, the system will monitor the availability of the SIP server. The system will failover to the backup SIP server once the primary SIP server becomes not accessible, and will fail back when it recovers.
- The messages received from a service port can be encrypted if it is required. The encryption can be applied to media streams and/ or the SIP messages, and the factory default is no encryption. When the encryption is selected, SX3000 will perform decryption to the received messages from terminals before they are redirected to the SIP server; similarly, SX3000 will perform encryption to the messages from the SIP server before they are sent to the terminals.
- There are three encryption schemes which can be selected to apply to the media streams, including

  RTP: Perform encryption to the entire RTP packets;

  RTP Header: Perform encryption only to the headers of RTP packets;

  RTP Body: Perform encryption only to the bodies of RTP packets.

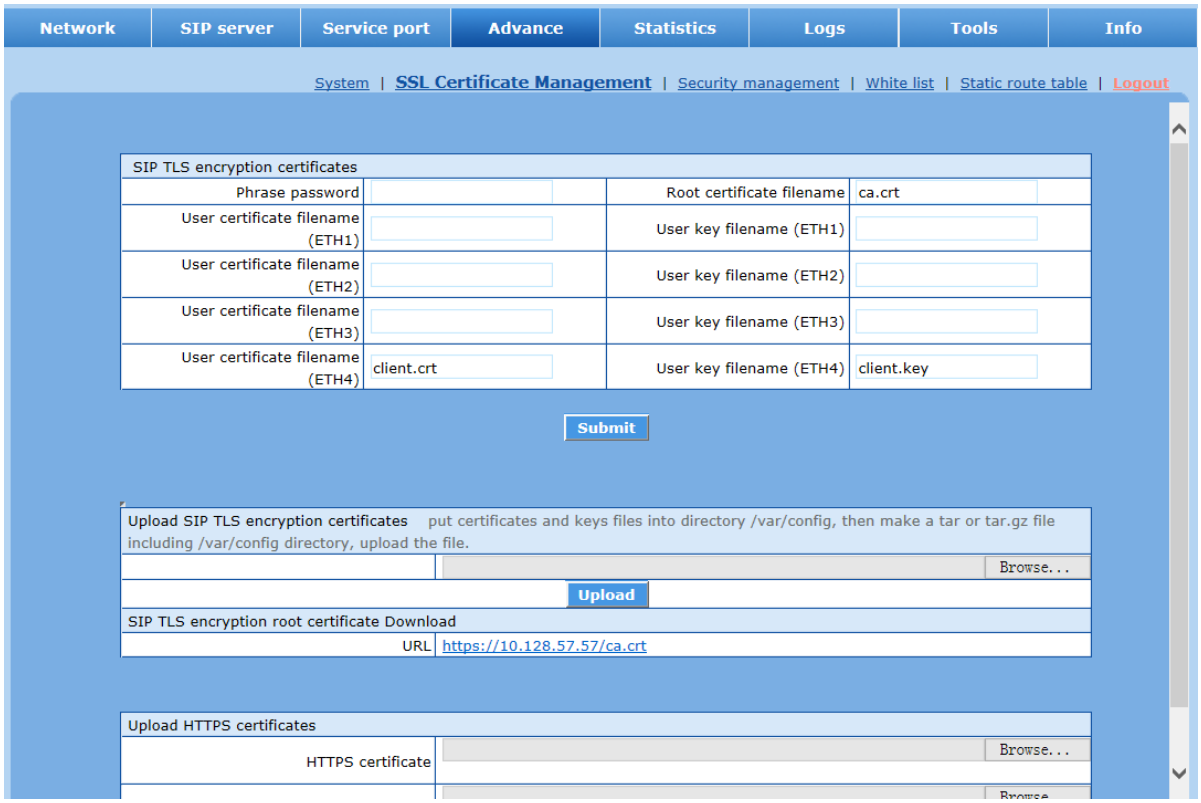
  It is recommended to use the default value **None**. Otherwise the normal operation of the device could be affected.
- Signaling encryption method: TLS, TCP Not Encrypted, TCP Encrypted, UDP Not Encrypted, UDP Encrypted, Using Keyword, Using Keyword2, or Encrypt 14.
- Encryption key may be needed for some encryption methods (except UDP Encrypted and TLS), and the key used should be identical on both SX3000 and the terminals.
- When TLS encryption method is selected, SRTP will be used to encrypt/decrypt RTP packets. SSL certificate related settings should be configured. For details, see Step5 SSL Certificate

Management.

Step5 SSL Certificate Management

Click **Advance > SSL Certificate Management** to configure SSL certificate.

Figure 1-6 SSL Security Management Interface



If TLS encryption is selected for service port, SSL certificate related parameters should be configured.

Table 1-2 Parameter Description

Name	Description
Phrase password	The password corresponding to the root certificate, which is optional. The password used to generate an SSL CA certificate.
Root certificate filename	The name of the file which contains the root CA certificate. Network ports 1–4 use the same root certificate.
User certificate filename (ETH n)	The name of the file which contains the custom CA certificate for ETH n.
User key filename (ETH n)	The name of the file which contains the custom private key for ETH n.

Note

For information about how to create an IP TLS encryption certificate, see the Appendix.

Uploading the certificate from SFTP server for the first time

1. Copy the created root certificate file ca.crt, the user certificate file client.crt, and the user key file

client.key to a directory in the SFTP server.

2. Telnet/SSH into SX3000 and type **cd/var/config** to enter the **config** directory (The SX3000 is based on Linux, so Linux commands are used here).
3. Enter **SFTP xxx.xxx.xxx.xxx** (IP address of SFTP server). Then enter username and password of SFTP server to login to it.
4. Enter **get ca.crt** to download the root CA certificate to SX3000.
5. Enter **get client.crt** to download the custom CA certificate to SX3000.
6. Enter **get client.key** to download the custom CA certificate to SX3000.
7. Enter **exit** to logout of SFTP server.
8. Enter **reboot** to restart SX3000.

Exporting the certificate through the SFTP server

1. Log in to the SX3000 using a Telnet/SSH session, and then type **cd/var/config** to enter the **config** directory (The SX3000 is based on Linux, so Linux commands are used).
2. Type **tar cvzf ssl_cert.tar.gz /var/config/client.crt /var/config/client.key /var/config/ca.crt /var/config/bin_version** to generate ssl_cert.tar.gz.
3. Upload ssl_cert.tar.gz to the SFTP server.

Note

To import the certificate later, open the Web management interface, choose **Advance** > **SSL Certificate Management**, and then unload ssl_cert.tar.gz in the **Upload SIP TLS encryption certificates area**.

Step6 Security Management

Click **Advance > Security** to configure security related parameters.

Telnet/SSH service can be disabled or enabled on the **Advanced > Security** interface. When this service is disabled, Telnet/SSH are not allowed to log on to SX3000. Access control can be flexibly configured for the SX3000. For details, see the related documents in the Linux Iptables.

Note

- By default, Telnet/SSH is disabled.
- When adding an access control command, add **/var/run/** before the command. For example: */var/run/iptables -A INPUT -s 10.128.23.23 -p tcp --dport 80 -j ACCEPT*
- If the access control configuration is incorrect, you may not be able to access the device through a network port.

When the SX3000 works with Huawei U1900, it is recommended to use the default values of the following parameters.

Table 1-3 Default Parameter Values

Configuration Interface	Parameter	Default Value
SIP server	Sending response via rport	No
Service port	RTP encryption	None

Advance	RTP proxy	Yes
	RTP disconnect timeout	300
	NAT traversal	On

Appendix: Creating an SIP TLS Encryption Certificate


Note

The SX3000 supports algorithms such as SHA, SHA1, and SHA256.

Creating the root CA

Step1 Create RSA private key for the root CA (it is suggested to set the length of key as 1024 bits)

openssl genrsa -des3 -out ca.key 1024

You should enter a stream of characters, when you will be prompted to enter the password, and this password should be used throughout the procedure.

The private key will be generated in ca.key.

Step2 Create a self-signed CA certificate with the private key generated in the above steps, using the following command:

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

When prompted to enter a password, enter the password which is the same as in Step 1.

Enter other information as instructed. All bold fonts on the settings below are for reference only.

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***

The CA certificate file “ca.crt” is generated.

Creating the user CA certificate

Step1 Create a RSA private key for the user CA certificate (it is suggested to set the length of the key as 1024 bits) using the following command

openssl genrsa -out client.key 1024

Enter the password when you are prompted.

The private key file client.key is generated.

Step2 Create custom certificate signing request (CRS) using the following command. The settings in bold font below are for reference only.

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

Enter the related information when you are prompted as in the following example:

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>***the IP address of the encrypted port corresponding to the SX3000.***

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

Enter the **password** when you are prompted for the password.

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

The file client.csr is generated.

Step3 Create custom CA certificate signed by this CA certificate using the following command:

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

Enter the **password** when you are prompted for the password.

The custom CA certificate file client.crt is generated.


Note

In the Common Name command in the example above, the IP address of the Ethernet port on SX3000 should be entered. For example, when TLS is used for ETH1, the IP address of ETH1 should be filled in generating CA certificate. Further, on the SSL management interface of SX3000, the client.crt and the client.key should be filled in User certificate filename (ETH1) and User key filename (ETH1) fields, respectively.