2018

SIP SBC

Mizutech SIP SBC –User Guide

A friendly SIP SBC by Mizutech

Mizutech
6/9/2018

Contents

About

The Mizu SIP SBC is an easy to use software solution to control SIP signaling and media streams capable to enforce security and to perform various tasks such as validation of SIP sessions and NAT handling. The SIP SBC can be installed on Windows operating systems and runs as an NT service.

Features

The most important features are listed below:

- **GUI**: comfortable graphical user interface for configuration, management and monitoring (real-time, CDR's, statistics)
- **NAT**: the SBC has built-in NAT traversal, support capable to gracefully handle all types of NAT's, firewalls and routers
- **Security**: DoS and DDoS attack protection with intelligent firewall, topology-hiding, access control, call limits, rate limiter, stream and session protection, blacklist, fraud call detection and various other thresholds
- **Internetworking**: compatible with all SIP devices, will resolve any incompatibility issues between devices.
- **Routing**: intelligent routing of calls can be done by various rules such as priority, quality and load-balancing
- **Failover**: it can detect failed servers and reroute the calls to others or automatically temporarily disable servers
- **RTP relay**: bypass, route or off-route the media with various enhancements such as NAT handling, QoS and stream control. It can be set to automatic (will route the media only if necessary) or enforced by manual settings
- **Transcoding**: transcode between various codec's such as Opus, Speex, G.729, G.723, G.711 (PCMU/PCMA), GSM, iLBC (this is done automatically by default only when necessary and can be overridden manually)
- **Optional modules**: billing, user management, registrar, class 5 features, WebRTC-SIP, push notifications, tunneling, high-speed load balancer (up to 2 000 000 simultaneous calls!)

Contact us with any questions at info@mizu-voip.com.

Requirements

The mizu SIP SBC can be installed on any server or PC running Windows OS.

- OS: Windows Server 2003/2008/2012/2016 (Windows XP/Vista/7/8/10 for home usage or testing). Both 32 and 64 bit versions are supported. You can use the cheap Web edition license.
- CPU: a cheap dual core cpu for less than 500 parallel calls, a best-buy 4+ core CPU for less than 2000 parallel calls or a high-end CPU for more.
- RAM: 1 GB RAM for less than 500 simultaneous calls, 6 GB RAM for less than 2000 simultaneous calls or 8+ GB for more.
- Disk: 60 GB HDD (or more if your traffic is high and wish to store all CDR's or more logs or voice recording)

Example hardware for 30000 users with 2000 simultaneous calls:

  - a best buy 4 core Xeon such as Xeon E5-2665 which costs only $140
  - 6 GB RAM
  - 80 GB HDD

Install

The SIP SBC has a standard easy to use installer.

1. Download the SIP SBC installer from here
2. Double-click to start the install process and follow the instructions (requires Administrator rights)
3. Once the install completes, it should automatically start the Admin client with its Configuration Wizard. This is discussed in the next chapter.

Configuration Wizard

For the basic server configuration you should walk through the detailed **configuration wizard** which is started automatically at first usage or accessible from the “Tools” menu -> “Configure”.

Don’t change any setting that you don’t fully understand, just click on the “Next” button in this case. Most of the settings are self-explanatory with a short description near them and/or a hint if you hold the mouse over a control.

Pay **special attention to the “Network” and “SIP server”** pages:

- on the Network page enter the correct IP and NAT configuration ("offer services for")

- make sure that the ports used by the SBC (SIP port, Access port, Secure port) are not used by some other application such as a local web server (in this case either change the SBC ports or the third party app port or bind them to separate IP address)
- on the SIP server page enter your PBX/Softswitch details (later you can add more SIP servers if needed)

Click “Apply” on the last page to save the configuration. Check the displayed messages and instructions. If you select the “(Re)Start the server” checkbox, then the SBC service should start automatically. Otherwise start it from the “Control” menu or use the Windows Service manager and start the “mserver” service.

When you start the service for the first time, it is a good idea to open the “Analyze” form to check for any potential issues.
Once the service is started, you can connect with SIP clients or trunks and make calls.

Once the SIP SBC is installed and configured correctly, there is nothing much to manage as it has full auto-management capability (such as auto deleting log files, auto fine-tune to your hardware, automatic user management and others).

Troubleshooting

If you can’t connect/register or make calls, check the followings:
- Make sure that the service is actually started (check the “mserver” service status in Windows Service manager)
- Have a look at the “Dashboard” form
- Open the “Analyze” form and click on the “Analyze” button to detect potential issues
- Check any important errors or warnings on the “Logs” form
- Make sure that you have basic connectivity to the important ports such as SIP signaling 5060 and RTP ports
- Install a SIP softphone (such as X-Lite or MizuPhone) on the same server where you are running your SBC and make sure that you can make call to your SIP server from there.
- If you are making call to a user/extension, make sure that the called user is registered when you call it
- If you don’t hear any voice you might change the RTP routing for the user(s) to “always route RTP” from MizuManage -> Users and devices -> Edit tab
- In case of call failure you can check the disconnect reason from the “CDR” form
- Verify the log files. You can find the logs in the server app folder (near the mserver.exe) -> “logs” subfolder. You can also open the folder from MManage -> View Menu -> Dir -> Server logs.

- Open the last log file ("log_xxx.dat") with a fast text viewer (For example F3 from Total Commander). To find application errors, open the last log file in the server app directory and search for "ERROR" and "WARNING". To find a call, search for "INVITE sip:callednumber".
- You can modify the trace details with the "loglevel" configuration option: from 1 to 5.
- Contact Mizutech support if the problem persists and you have or wish to buy a license

MizuManage

All administration and monitoring tasks can be done from the **MizuManage** (MManage / MizuManagement) admin client, which is included in the SIP SBC install package.
Using the SBC, you will still need to use your Softswitch/PBX to manage your Users (authentication, authorization, and accounting), Routing and any other aspects of your network.
Regardless of this, the SBC also provides you complete monitoring and GUI based configuration managements, so you can easily change settings or find connectivity issues.

Always check the status bar (the bottom text display). MManage rarely displays popups and the success/error statuses of various operations are displayed on the status bar instead.

Filters:

Nearly all forms in MManage can be filtered with the followings:

- Quick filter: found in the top-left side in MizuManage. For example type "44*" in the quick filter box then open the "CDR" form and click "Load". You should be able to see all calls to 44….. numbers. Or enter "test" and open the "Users and devices" form. Click on the load button to see accounts containing the "test" word (in name, username, address, etc)
- Direction filtering: accessible by double clicking on the space above the quick filter or from the View menu -> Filter -> Set direction filter. When you are doing operation which needs more precision (eg. billing), always use the Set Directions form and not the quick filter.
- Date-Time filter: found in the top-left side in the MizuManage. Useful to restrict statistics, reports and CDR listing intervals.

Menu:

- The most important item is the Configuration wizard (from Tools menu -> Configure). Use this to (re)configure your SBC's most important settings.
- From the "Control" menu you can Stop/Start/Restart your server (you can do so also from windows Services management console)

- To export data from the application, use File menu -> “Save As”.
- From the “Fields” menu you can manipulate the selected dataset (grids, etc).
- The Tools menu -> “MManage Settings” form is used for local admin client configuration only.

The most important settings can be configured from Tools menu -> Configure -> Configuration Wizard as already discussed in the previous chapter.

User Management

All user records can be managed from the “Users and devices” form (below the “Access” node in the tree-view).
Users can represent real people, endpoints, extensions, devices or servers.

The most important user types are the followings:
- SIP server for outbound routing. Your SIP server(s) should be added here.
- Traffic senders for inbound routing. Your SIP server(s) should be added also here.
- Endusers: these are managed by the SBC automatically.
- Admin users: you should add yourself (and/or the administrator) here as it is used for various purposes such as sending alerts and reports.

The users are stored in the database tb_users table and they have a lot’s of properties which can be managed from the “Users and devices” form or (for advanced users only) changing database record fields (select a user the go to Fields menu -> Show fields).

You don’t need to manage endusers/extensions on the SBC! In MManage you might see your endusers (extensions) listed on the “Users and devices” form, however that is only for monitoring purpose and for the SBC internals, auto created and managed by the SBC. Except your extension usernames, no authentication credentials (password) or any sensitive information (such as billing) are stored on the SIP SBC. Use your Softswitch/PBX for user management.

Listing users

Open the “**Users and Devices**” form (below the “Access” section) and (double) click on a user type to have a listing.
You can apply various filtering using the user “Type” checkbox-list, the dropdown-list on the top of the form or the already discussed direction filter or quick filter.
Your SIP servers can be found as “SIP Server” and “Traffic sender” accounts.

You can easily search for users using the “quick filter” box. For example to list all outbound routes whose username or name contains the “carrier” word, select the “SIP Server” and type “carrier” in the quick filter. The quick filter will also search in other fields such as IP, name, email and others.
Other listing options are available also from right click on the “Users and devices” node in the main tree-view or right click on user type node from within the “Users and devices” form.

Creating users

The best way to create new users is to clone an existing working account with the same user type.
For this, launch the “**Users and Devices**” form, select a user type, and click on the “Load” button. Then select any user entry and click on the “New User” button. Alternatively right click on the “New” button for other options to add user records.
Endusers are created automatically by the server at first time when an extension will try to register or call. These enduser records are only for internal management and statistics reasons. This are the same users as the extensions on your PBX, but the SBC might have information only about their username and display number (the SBC does not have to know the password since the authentications are forwarded to your SIP server). You don’t need to manage these endusers on the SBC (Keep using your PBX to manage your users).
The username can be also used as a real phone number; will be used also as the caller-id if not specified otherwise. Endusers can make voice or video calls, presence and chat directly between them without the need to be forwarded to your SIP server. (Alternatively you can disable direct routing between endusers by setting the alloweuserusercalls global config value to 0).
Traffic sender users are used for receiving traffic from your SIP servers (PBX, Softswitch, SIP proxy or other SIP device). The authorization type is usually set to “Auth ip must match” and you have to enter a correct “Auth Ip” (IP address based authentication).
SIP servers: For outbound traffic you need one (or more) SIP Server user. The most important parameter here is the “IP” where the VoIP calls will be sent. Then you will have to configure these also on the Routing form.
To be able to send and receive traffic to/from another SIP server or carrier you will have to add it as both a “traffic sender” and “sip server” user.

SIP Servers

A default/first SIP server record is automatically created for you once you complete the Configuration Wizard. Use the “Add Upper SIP server” form (available from “Tools” menu -> “Add or import users”) in case if you have more SIP servers where the traffic from the clients’ needs to be sent or accepted from. Also don’t forget to manage the routing in this case. The most important configuration for a SIP server is its network address (IP and/or domain name). Also you must specify the port number if your server is not using the default SIP port (UDP 5060). This can be done by just appending it after the IP after a colon (such as 11.22.33.44:5678) or as the “port” field in the user table.

Add SIP Server:
Your upper SIP server(s) can be added multiple ways:
1. from the Configuration wizard you can add your default/first SIP server on the "SIP server" page
2. from the "Add Upper SIP Server" form (from Tools menu -> Add Import users)
3. from the "Users and devices" form (This is discussed here)

A default/first SIP server can be added during the configuration wizard. (You can also modify it from right click on "Configurations" node in the tree-view and select the "Upper server" from the popup menu).
To add a SIP server open the "Add Upper SIP server" from Tools menu -> Add Import users.
(Alternatively right click on the "Users and devices" node in the tree-view and select "Add Upper SIP Server").
Pay attention to the following fields: IP, domain, port (you can also set the proxy field if needed).
Once you added your server, make sure to modify the routing after your needs (if you have more than one server, then the routing needs to be able to decide somehow which traffic to send to which server. You can create various rules for this on the "Routing" form)

When you add a SIP server, this is what happens:
1. a Traffic sender account is created which will handle inbound traffic coming from your SIP server
2. a SIP server account is created which will handle outbound traffic to your SIP server
3. a default routing entry is created for the above SIP server

Actually, you can "add a SIP server" also by just adding the above accounts manually from "Users and devices".

If the SIP clients have to register to different SIP servers, set the "routingforregister" global config option to 1 (from the "Configurations" form). Otherwise set to 0. If the "routingforregister" is set to 0, then it will forward all registrations to your default SIP server which you have created during the configuration wizard.

Multiple SIP servers:
You can use one SBC SIP for multiple SIP servers (if you have more servers) for both outbound and inbound traffic.

Registrar routing:
By default all registrations will be routed to the default upper SIP server (what you have set during the configuration wizard or from global configuration search for "fwdregistrations").
If you have multiple upper SIP servers and the SIP clients need to register to different servers, make sure to set the routingforregister global config option to 1 (from the "Configuration" form).

Then the registrations will be routed after the routing rules which can be defined on the “Routing” form. The only exception is the called number since there is no called party in a registration (this is applicable only for calls).
However, if your SIP servers are for completely different domains/businesses, then you might consider to set-up a separate SIP SBC for each of them.

Note: The “routingforregister“ is only for registrations. Call and chat routing are always performed after your “Routing” settings

Call routing:

- Outbound calls are always routed based on routing rules which you define on the “Routing” form. Routing rules can be set for SIP servers (so you must create “SIP server” user(s) before to be able to work with routing.
- To be able to accept inbound calls (from your SIP server to SIP clients) you will need to create “Traffic Sender” user (usually with IP authentication with the Auth IP set to your SIP server address).
- Calls between users are handled automatically.

SIP Clients and Trunks

Check “how to connect?” from the “Help” menu for the exact details about SIP clients configuration.
For a quick test, register with two softphone and call from the first account to the second account.
Softphone configuration:

- domain: your SBC IP or domain name (and the SIP port if your changed it from the standard 5060 UDP port)
- proxy: you can leave it empty
- username / password: loaded from your SIP server (or from the SBC if you created a special user with username/password authentication)

Add SIP Client:
There is **no need** to add endusers, extensions or SIP clients manually.
Just continue to manage your users as before: on your SIP server.
You will be able to see the users on the “Users and devices” form -> Endusers, however these are managed automatically by the SIP SBC and there is no need to change any settings here except if you have some extra requirement such as setting call forwarding, call recording or some other per user setting. The first time a SIP client will register or make call, a user entry is automatically created by the SBC. This is mostly for internal usage only, but it also allows you to make per user changes if necessary. No password of these users are stored on the SIP SBC (The users are created with “Username” based authentication only, however the SIP SBC will also check other parameters such as same session / same address for further account restriction. If you wish, you can create additional users of your own for various other purposes.

For special purposes you might add users also manually. There are multiple ways to do this:

- click on the “New” button from “Users and Devices”
- or right click on the “New” button
- or right click on the “Users and devices” tree-view node.
- or from “Tools” menu -> “Add or import users”

Outbound Routing

Outbound routing rules are required for the SIP SBC to properly route the calls to your SIP server(s).

Calls between users are handled automatically as this will bypass the routing table and it is routed directly unless if you disable it. However for outbound routing you need to add a “SIP server” user first and then add it to your routing rules.

Once you add your upper server as a “SIP server”, open the “**Routing**” **form**.
In the left side you have to define your pattern which will restrict the condition when the actual route entries can be used. If all fields are empty and the time definition is set to “All times” then all patterns will match. You can make restrictions if you make specifications here (caller, called prefix, time restriction, etc). Make sure that you increase the priority for the pattern (to be higher than the “general” pattern where you have not made any restrictions).
On the right side you will have to add one or more sip proxy users. If you set more than one route with equal priority, then you have load balancing, LCR or BRS (depending on the “brs_lcr” global config option); otherwise the traffic will be routed after the prioritizations (will flow to the lower priority servers only if you have reached the maximum port limitations or because automatic failover).

If you have only one server then just create one pattern (left side) enabled for all times and no any filter set, then assign your SIP server user entry to this pattern (right side).

For more details please read the routing guide.

Dial plans

You can manipulate number format, SIP headers or the Caller-ID from the following settings:

- Users and devices form: caller-id, username, other numbers (DID match), tech prefix
- Routing form: you can only specify routing direction here without number changes
- Rules form: this is a powerful module which you can use to change almost anything (including caller-id, called number format and many others)
- Global configuration: a few global configuration options might also affect the dial plan. Right click on the “Configuration” node and select “Number rewrite” for the details.
- Prefix rules and the dial plan form: use the “Rules” form instead when possible.

You can find more details in the VoIP Admin Guide below the Routing section.

Inbound Routing

If you would like to accept traffic from your servers, you need to have one or more "**Traffic sender**" user account created. Usually you can use IP based authentication. For this, add the peer IP to the "**Auth IP**" field.
For each incoming call, the server will first check if the called party is a local user. If not, then the call is routed according to the rules which are set by the "Routing" form.

One "Traffic sender" user entry can handle incoming traffic with IP authentication from multiple IP addresses. Use the "…" button near the "Auth IP List" to add more IP addresses.

Usually there is no need to setup any routing rule for inbound calls (as these will be calls to local SIP users which are found automatically).

Traffic between endusers/extensions is handled automatically.

CDR

A CDR (call details report) is generated for each call on your SIP SBC.
You can access these records by using the **"CDR**" form under the "Monitoring" node in the tree-view. By default only the most important fields are listed (date-time, connect time, call duration, etc). You can see more details if you check the "All fields" checkbox.
To quickly list the CDRs that belong to a user, open the "Users and devices" form. Find the user record, then right-click on it and select "Set Direction". Than go back to the CDR record form and click on the "Load/Reload" button.
You can easily filter calls with a specific prefix by typing the prefix in the quick search box following with an asterisk and hit enter. For example searching for 44* will list all CDRs where the called number begins with 44.
You can also see various statistics based on these CDRs by using the "Advanced Statistics" or the "Disc. Reasons" forms.

Statistics and Monitoring

The Mizu SIP SBC provides endless possibilities for monitoring both real-time and statistics history. Some of the most important tools are the followings:
Dashboard: a summary of the most important parameters and a start point for management (Note: You can access various statistics by just clicking on the Dashboard items. For example click to "CCalls" will show the current calls)

By using the "**Analyze**" form you can have a quick overview about the system and warnings for malfunctions or configuration suggestions
List the active sessions: Monitoring -> "Current Calls" form
Disconnect reasons: Monitoring -> Disc. Reasons will show statistics about call disconnect codes.
Statistics by SIP server: Monitoring ->Advanced Statistics -> Group By: called servers (useful if you have multiple server, softswitch or PBX)
Statistics by users: Monitoring ->Advanced Statistics -> Group By: caller
Statistics by day: Monitoring ->Advanced Statistics -> Group By: day
Logs: the most important logs can be listed from the "Logs" form. Detailed logs can be found in log files accessible from View menu -> Dir -> Server Logs directory
Other more **advanced statistics** can be generated by using the Advanced Statistics form and using different fields/options/grouping/directions.
All statistics can be filtered by the "set direction" form or the "quick filer" edit-box and by a time interval selection.
Automatic reports: The SIP SBC can send daily reports for administrators or email/sms alerts on malfunctions. For this you have to setup an "Admin" user with a valid email address (From the "Config Wizard" or from "Users and Devices"). Then set the following user fields to 1 (after your needs): "sendemailalert", "senddailyemal", "sendmonthlyemail", "sendsmsreport", "sendsmsalert".

Start/Stop

You can start/stop the SBC service from:

- the "Control" menu in MManage
- or by the Windows Service manager locate the "mserver" entry, right click and select "Start" or "Stop"

Note: the first start might take a bit longer (around one minute), otherwise the start-up time should be below 10 seconds.

Backup/Restore

A backup for the SIP SBC can be done with simple file copy (xcopy) and just copy back the files for restore.
You can back-up all your data and settings by just copying the mserver.sdf file from the app folder
Alternatively, you might choose to copy the entire app directory, excluding logs (however these files can be easily recreated by a reinstall, so you really need only the mserver.sdf).
By default the SBC will automatically create nightly backups and auto-delete old backups (Search for "backup" in the global configuration to change this).

Settings

The below discussed settings have to be changed only if you have some special requirements, otherwise the default settings are optimal out of the box.

Through this guide we often refer to various configuration keys also called as “global configuration” or “global config”. All these can be managed from the “Configuration” form (below the “Other” node in the tree-view).

The SIP SBC has a long list of configurable settings which you might adjust to turn on/off features or to adjust the SBC behavior after your needs.
The settings can be categorized in the following way:

- global configuration (editable from the “Configuration Wizard” and from the “Configuration” form)
- per user configuration (editable from “Users and devices”)
- other configurations (editable form various forms such as “Routing”, “Rules” and others)

Global Configuration

You can quickly change any global configuration from the “Configuration” form (below the “Other” node from the main tree-view). Just search for your keyword to find the related setting(s).
Most of the changes can be applied instantly (click on the “Apply Now” button), however some changes (such as local/bind ip/port reconfiguration) require a restart.
Some settings groups can be accessed by right clicking on the “Configuration” form.
SBC related options can be listed by right click on the “Configuration” node and select the “Gateway” from the popup. Some important gateway related settings are the following:
autocreatereguse: 0=no,1=when fwd authenticated ok register, 2=always (when we receive the register)
fwdregistration: 0=no,1=only from alternate port, 2=always
fwdregistrations_address/fwdregistrations_domain/fwdregistrations_ip/fwdregistrations_port: the address of your SIP server (the upper server)
forwardauthentifications: 0=no (default),1=yes,2=yes with username as callername, 3=yes with phonenumber as callername, 4=yes with username as authname too, 5=yes with phonenumber as authname too, 6=replace authorization with username but leave the A number intact, 7=replace authorization with sipphonenumber
forwardauthpassword: 0=fwd from ep, 1=means 2 if from rtc for recent users, 2=answer from local always,3=answer from local also for register, 4=answer from remapped upperusername/upperpassword

Clean Install

By default when you reinstall the SBC service, it will keep your old settings and data, thus you can easily upgrade to new versions.
If you wish to begin with a clean state, delete (backup!) the old mserver.sdf file before launching the installer, thus you will have a clean state with all your previous settings and data erased.

Change IP address

If you migrate the SBC to another box or your IP changed, then you will need to set the new IP.
There are 2 ways to easily change the SBC IP:

1. going through the Configuration Wizard and make changes on the "Network" page
2. or right click on the "Configuration" node in the main tree-view (below the "Other" node) and select "Network -Basic" and rewrite the IP

Restart your SIP SBC once you changed the IP because this can't be applied at runtime.

Ports

The SIP SBC will listen on several ports to offer its services: SIP signaling, RTP/RTCP ports range and others.
It is recommended to keep the default ports since the defaults are optimized for maximum connectivity and/or are conform to standards.

If these ports are already used by some software running on the same box, then we recommend to assign a secondary IP for your server and bind the SBC to this new IP (set the bindip), then reconfigure the other software's to use only the old IP (bind to the old IP). For example IIS can be bound to an IP with the following command:
netsh http add iplisten ipaddress=IPADDRESS (replace IPADDRESS with the IP to bind)
If you are hosting the SIP SBC on the same box where your softswitch is running, then assign a separate IP (bindip) to the SBC if possible. If this is not possible, then make sure to change the ports on the SBC to avoid conflicts (if your SIP server is listening on 5060, then set a different "localport" for the SBC).

Here is the **list of ports** used by the SBC and their global config options which you can change from the "Configuration" form if needed.
Mandatory ports:

- localport UDP and TCP (main SIP signaling port. Default is 5060)

- mainaport TCP (main server port for various purposes such as API and others. Default is 80.)
- MinRTP-MaxRTP range UDP (for RTP and RTCP)

Optional ports (good to allow also these):
- Remote desktop TCP 3386 (for easy server administration)
- TCP 1433 and/or 2223 (for remote management)
- adminport TCP (for remote CLI access from MManage server console. Default is 9885)
- monitorport TCP (to easy access logs from remote MManage. Default is 9889)
- localport+1 TCP (for secure SIP. Default is 5061 -if you enable TLS for SIP which is known as SIPS)
- ftpserverport TCP (for remote access for voice recording . Default so 9710)
- UDP: 44444 ("voice-here" functionality in MManage)
- TCP: 9885, 9886, 9889 (optional ports for admin console and logs)

Make sure to enable these ports if you are using a port based firewall.
Make sure that the ports used by the SBC are not used also by some other application such as a local web server (in this case either change the SBC ports or the third party app port or bind them to separate IP address).

SBC behind NAT

The SBC can be used also behind NAT (located behind NAT or router, even without internet access).

If your SIP SBC is behind a NAT or Router, make sure to forward the ports above correctly if you need connectivity also from external network (SIP clients or SIP server on the internet. If both of these are behind NAT, then there is no need to enable these ports).
In this case make sure to set the "**Offer services for**" option correctly on the "Network" page of the Configuration Wizard.
- Both LAN and internet: select this if SIP clients might connect also from the public internet (make sure to set proper port forward on your router in this case)
- LAN: means all SIP clients will connect from local LAN, but the SIP traffic might be sent to the public internet (your SIP server is outside)
- Force LAN Only: means that all peers (including your SIP server and all clients) are located on the local LAN

In other words, here are the **possible uses-cases**:
- SBC on the public internet:

You can just skip this chapter as you don't need to take care about NAT in this case. (SIP clients connecting from behind NAT are handled automatically)
Set the "Offer services" option to "Internet only" if your SIP server is also located on the public internet or "Both LAN and Internet" of your SIP server or other SIP device is located on the same box or network.
Your "Public IP" and "Bind IP" can be the same public address in this case.

- SBC, SIP server and SIP clients all on local LAN:
  In this case you don't need to set any port forwarding in this case as all peers will be reachable directly.
  Set the "Offer services" option to "Force LAN only" in this case.
  Your "Public IP" and "Bind IP" can be the same private address in this case.
- SBC and SIP clients behind NAT, SIP server on the internet:
  If the SIP server or SIP service has good NAT handling capability, then everything should work just fine by default. Otherwise setup proper port forwarding on your NAT/router for the above mentioned ports.
  Set the "Offer services" option to "LAN" in this case.
- SBC behind NAT, SIP clients on the public internet:
  Set the "Offer services" option to "Both LAN and Internet" in this case and setup proper port forwarding on your NAT/router for the above mentioned ports.
  Also set the "Public IP" to your network external IP.

Calls between endusers/extensions

Calls between endusers can be routed directly, without the need to route them via your upper SIP server(s), thus saving your server resources (CPU/memory).

This direct routing is enabled by default and it can be easily changed by the following global config values (from the "Configurations" form):
alloweuserusercalls: 0=no (don't check if local target),1=yes,2=disable (drop) call to endusers

To enable direct routing, set the alloweuserusercalls to 1.
To disable direct routing, set the alloweuserusercalls to 0.

Multiple registrations and call fork

One user can be registered from multiple locations at the same time and calls can be routed to all of its devices.
Use the following global configurations to modify this behavior:
allowforkforsignaling: 0: no,1: partial,2: yes,3: yes and remember old addresses (send sip request to multiple recipients at once)

Codec

The SIP SBC has support for all the commonly used audio and video codecs:
G.711, OPUS, G.729, G.723, GSM, iLBC, Speex, G.722, VP8, H.264
The codec is negotiated automatically for each call depending on SIP client and SIP server capabilities.
The codec used for calls can be also influenced by the "choosecodecs" user configuration (which can be also set on the "Users and devices" form -> Functions page -> Allowed codec setting).

Transcoding

By default, the SBC will try to avoid transcoding when possible by negotiating a common codec between caller and called parties. If necessary, it can convert automatically between the SIP client and server by sending a re-INVITE with all supported codec's when a 488 answer is received from the caller.

If one of your peers has limited codec capabilities or the accepted codec(s) doesn't match with the sender codecs, then set its "needcodecconversion" to 1 (for the target user which is usually a SIP Server user or Enduser). This can be also controlled on the "Functions" page of the "Users and devices" form.
Change the "convertcodecs" global config value to the target codec payload list. The default value is 0,8,18 which means PCMU,PCMA and G.729.
The server is able to transcode between the following codecs: G.711 A-law , G.711 A-law ,G.729, G.723.1, GSM, OPUS, Speex 2,3,4,5,6 (narrowband, wideband and ultrawideband), G.726 and G.722.
You might also have to set the "choosecodecs" field for the target user (same as the "convertcodecs" global config value) and the "convertcodecsforced" global config option to true.

Valid payload values are the followings:

- PCMU (G.711 u-Law): 0
- PCMA (G.711 A-Law): 8
- GSM (GSM 06.10): 3
- G.722: 9
- G.723: 12

- G.729: 18
- iLBC: 97,
- Speex: 104
- Speex wideband: 105
- Speex ultra wideband: 106
- Opus: 110
- Opus wideband: 111
- Opus ultra wideband: 112

Example: If your SIP Server has support for G.729 and PCMU, then you should enter “18,0” for the choosecodecs user field (or in the “Users and devices” form -> “Functions” tab -> “Allowed codec” field.

Be aware that codec transcoding requires a high amount of CPU usage. For example one CPU (core) can handle around maximum 20-200 simultaneous transcodings between PCMU and G729 on full load (depending on your CPU type).

Codec transcoding should be avoided whenever possible because it will increase the CPU usage and also will degrade the quality a bit. By default the SIP SBC will try to negotiate a common codec between the endpoints and transcode only when strictly necessary.

Example configuration if (caller A has only G.711 codec and) called B accepts only G.729:
For the B user set the user convertcodecs field to 18 and the needcodecconversion field to 1 (The same can be done also from the SBC GUI -> Users and devices -> Functions tab).

To disable all kind of transcoding on your server, run the following queries:

```
update tb_users set needcodecconversion = '', choosecodecs=''
update tb_settings set valstr = 'false' where keystr = 'convertcodecsforced'
update tb_settings set valstr = 'false' where keystr = 'enabletranscoding'
update tb_settings set valstr = '0' where keystr = 'fs_transcode'
update tb_settings set valstr = '0' where keystr = 'autocodecconvert'
```

Call recording

The voice recording option can be set for any user by checking the “Voice Record” checkbox on the user configuration form in MManage (Users and Devices -> Functions tab).
Conversations will be saved in the directory specified by the “serverftpvoice” global config option.

The exact location will be: serverftpvoice\databasename\currentday\voice.xxx
A separate backup can be created in the directory specified by the “voicebackupdir” global config option.
Out of date recorded files can be deleted by setting the “keeprecorded” option accordingly (days to keep).
Recorded files are compressed and encrypted by default.
Recorded conversations can be played on the "CDR" form (Select the "Recorded Conversations" radio item, select the desired record and click on the Play button) or from the “Voice Record” form.
You can also export the files as wav or mp3.
Users can replay the last record by the following DTMF digits: *4*
Note: call recording can make the routing and media path longer, disabling peer to peer calls and also will increase your server I/O and CPU usage.

To disable recording for all users, execute the following SQL’s in the “Direct Query” form:

```
update [tb_users] set record = 0, RouteRTPCaller = 1, RouteRTPCalled = 1 where type in (0,5,9)
ALTER TABLE [tb_users] DROP CONSTRAINT [DF_tb_users_record]
ALTER TABLE [tb_users] ADD  CONSTRAINT [DF_tb_users_record]  DEFAULT 0 FOR [record]
Update tb_settings, set valstr = ‘1’ where keystr = ‘defroutertp’
```

If you wish to enable call recording for all users, execute the following SQL’s in the “Direct Query” form:

```
update [tb_users] set record = 1, RouteRTPCaller = 7, RouteRTPCalled = 7 where type in (0,5,9)
ALTER TABLE [tb_users] DROP CONSTRAINT [DF_tb_users_record]
ALTER TABLE [tb_users] ADD  CONSTRAINT [DF_tb_users_record]  DEFAULT 1 FOR [record]
update tb_settings, set valstr = ‘7’ where keystr = ‘defroutertp’
```

To force recording for all calls (even those where the media would be routed peer-to-peer otherwise), set the following global config options:

```
defroutertp=7 (force RTP routing by default)
alloweuserusercalls=0 (disable upper server routing and media path bypass)
disablep2prtprouting=1 (disable peer to peer media path detection)
```

Chat recording

The users IM history can be recorded and stored in server database, tb_messages table.
For this set the “logmessenger” global config option: 0=no,1=on low load,2=always
You might also disable fast message forwarding by setting the “fastmessagequeue” configuration option to 0.
The recorded messages can be seen on the “Chat Logs” form MManage.

WebRTC

If you are interested in WebRTC-SIP protocol conversion then you should use the MRTC gateway which is actually an SBC with the WebRTC module included by default.
However WebRTC support can be easily added also into any existing SIP SBC. Contact Mizutech to perform the upgrade.

Push notifications

The SIP SBC has support also for VoIP push notifications. This is a useful feature to improve the availability of mobile SIP clients by sending a push notification on incoming call or text message which will wake-up the client app, thus the call/chat can be delivered even if the app is closed or the device is sleeping.

Follow this documentation to enable push notification and integrate push support into your Android/iOS/Web app.

Logs

You can find the SIP SBC logs from View menu -> Dir -> Server log directory. Use a fast text reader to work with the files such as F3 from Total Commander.
The logs files are managed automatically by the SBC (auto deleting old log files or if you are low on disk-space).
You can change the server log level from Tools menu -> Utilities -> Set server loglevel.

Security

The SBC is based on our Softswitch core which implements a long list of security measurements which are also applicable for the SIP SBC. See the details here.

Extra features

Class 5 features should be handled on your IP-PBX or Softswitch, however the SBC also has some built-in features which might be useful for you (for example voicemail or call forward). Also for some functionalities there are no direct mapping between the SIP client and SIP server so they can be solved

only by extra features provided from the SIP SBC or on your Softswitch (for example conference). Other features don't depend on SIP but might be implemented on the server side using some separate protocol (usually via a HTTP API exposed to clients).
Here are a few of the extra features:
IM/Chat: fast chat routing between SIP clients based on SIP MESSAGE RFC 3428.
DTMF: For DTMF to work your SIP server and SIP client must have support for RFC 2833 or SIP INFO. The SBC can also perform the conversion between these if needed. In-band DTMF conversion is not supported, however, it is routed as-is, so this method will also work if both your SIP server and SIP client use this method.
Call forward: can be enabled from users and devices form -> functions tab. For call forward to work via your server, it needs to support SIP response code 301 (Moved Permanently) and/or 302 (Moved Temporarily).
Call transfer: available as specified SIP standards (via all devices with support for transfer). For call transfer you will need support for SIP REFER as described in RFC 3515.
Video: Fast video stream routing between endpoints
Special numbers and IVR's such as music, record/playback, vide record/playback and others
Presence: Fast presence routing between SIP clients. For presence to work via your server your software needs support for PUBLISH/SUBSCRIBE/NOTIFY as specified in RFC 3856.
Barge in: via the "Voice here" form in MManage
Softphones: Mizutech can also offer customized/branded softphones which works with the SBC or directly with your SIP server: Browser webphone, Windows softphone, Android softphone, iOS softphone, Symbian dialer, Other softphones
IVR: The IVR module can be used for various tasks like access numbers, callback, customer support etc. You can assign different IVR's to different access numbers by using the "**Campaigns**" form. To create a new campaign, just click on the + sign and enter a "name" for the new record. The most important configuration for an IVR campaign is the script. Switch to the "details" tab to select a "Script".
Scripts can be created by using the "IVR" form. The SBC is shipped with several preconfigured script examples, but you should easily add new scripts or modify the existing ones by following the admin guide or the IVR documentation.
SMS: by default the SBC is capable to route SMS message as SIP MESSAGE (RFC 3428). However, it is also possible to use an external service which can be accessed by a HTTP API. Just set the "smsurl" smsurl global config option or create SMS GW endpoints if you wish to use more than one provider. A guide can be found here.
API: the SBC also has a HTTP API which can be used for various tasks. See the API documentation for the details.
Many others features are enabled for you by default and some of them can be changed/fine-tuned from configurations, such as caller-id, ring groups, call hold, call waiting/park/pickup and others.
The SIP SBC is based on the VoIP Server core thus you can also access almost all of the Softswitch features. See the Softswitch documentation for the details.

The SBC also does its best to compensate on missing support. For example the basic presence might work without SUBSCRIBE/NOTIFY support by using the peer registrar state.

If you are not sure where to find a specific configuration option, search for your keyword in:

1. “Configurations” form within MManage
2. This guide
3. VoIP server guide (most of the settings can be applied also for the SIP SBC)
4. Check the other documentations (some of them are relevant also for SIP SBC)
5. Or ask Mizutech support

Resources

- SIP SBC Home Page
- Download
- Contact