Mizutech VoIP Tunneling and Encryption

Quick Setup

About

The Mizu VoIP tunneling solution is a set of client and server side software capable to bypass voip blockades, firewalls, NAT's, SOCKS and HTTP proxies.
For a detailed presentation please visit this link: https://www.mizu-voip.com/Software/VoIPTunnel.aspx
Technical details: https://www.mizu-voip.com/Portals/0/Files/MizuTunnelingGuide.pdf

The mizu tunneling service can be enabled in any softswitch (VoIP Encryption module) or run as a separate gateway (VoIP Tunneling module).

Important: if you are using the SaaS license, then all server side services are fully managed by Mizutech for you. This means that most of the details described in this document doesn't apply. You will receive customized client side software ready to use as-is (mtunnelclient, webphone and softphone for all the major platforms).

All configuration and management can be done by Mizutech support. However you can use this guide and the softswitch admin guide to manage the VoIP tunneling server yourself.
Once the server is installed, you will usually need to perform only a few management tasks which are the followings:

- edit your registrar, inbound and outbound server(s) settings (all these settings can point to a single server)
- monitoring (running calls, CDR records, statistics)
- backup and cloning

Server requirements

- OS: Windows Server 2003/2008/2012/2016/2019 (Windows XP, Vista or 7/8/10 for testing)
- CPU: depending on the usage (the server can take advantage from up to 32 cpu core)
- RAM: depending on the usage (minimum 1 GB for 200 simultaneous calls)
- Disk: 40 GB with logs turned off and or 192 GB for maximum trace level
- Network: ~10 Mbit/s for 300 simultaneous calls (depending on the transport protocol and the codec used)

Typical recommended configuration for VoIP service providers between 500 and 5000 simultaneous calls: 2 servers with 4 or 8 CPU core, 4 GB RAM, and 256 GB disk space. By using 2 servers you can separate the application server from the database server and also you will have a hot backup.

Install

Most of the install and configuration steps are similar as described in the Mizu VoIP Server tutorial: https://www.mizu-voip.com/Portals/0/Files/mizu_voip_server_tutorial.pdf
Download the server install package from the MizuTech webpage: https://www.mizu-voip.com/webinstaller/MizuVoIPServer.exe.
Launch the install wizard and follow the instructions.

Once the install is finished you should download the last fixes from here: https://www.mizu-voip.com/F/serverupgrade.zip
Unpack the zip file and overwrite the existing files with the new ones.
The latest MizuManage install package is always available from here: https://www.mizu-voip.com/Portals/0/Files/MizuManagement_Setup.exe

Verify

When the install wizard is ready you should check the followings:

- ✓ The database is installed correctly. Otherwise you can download the express edition from here. Make sure to install with mixed mode authentication and enable the TCP/IP access from the SQL Server Configuration Manager on port 1433 or 2223.
- ✓ Create a database using the MS SQL Management Studio. You can name it to "mserver" than create the basic database structure with the MDBSetup.exe tool or by running the mserverscript.sql script.

- ✓ mserver is registered as a windows service (otherwise run “mserver.exe /install” from the command prompt). Make sure that the service startup type is set to automatic.
- ✓ Enable the mserver.exe and the TLSProxy if you have enabled the windows built-in firewall.
- ✓ Make sure that port 80 is not used by other software (the tunnel will work also without this, but better if you allocate this port for the tunnel server)
- ✓ For remote administration you need to enable also the database engine executable (sqlservr.exe)
- ✓ Server basic configuration: Edit the [database] section in mizuserver.ini configuration file. Add the newly created database access here (ip, port, database name, username, password)
- ✓ Start or restart the Mizu VoIP service (stop/start.bat or from Services)
- ✓ Check the log file if any startup error exists. (Open the last “log_xxx.dat” files near the mserver.exe with notepad or TotalCommander F3 or using the logviewer application from the Tools directory if you have installed it). Search for “CRITICAL”, “ERROR”, “catch” and “WARNING” messages.

MizuManage

Install and start the admin client software on the server or on any remote PC. It is part of the server install package or a separate install can be found at https://www.mizu-voip.com/Portals/0/Files/MizuManagement_Setup.exe

Login to MizuManage:

- Server: ip address of the server (database port followed after a comma if not using the default port)
- Instance: database name (“mserver” by default)
- Username: database username (“sa” by default)
- Password: database password (“srEgtknj34f” by default)

Example:

App server: mserver (127.0.0.1,1433)
DB server: default
DB: mserver
Username: sa
Password: srEgtknj34f

Basic settings

Launch Config menu -> Configuration wizard if not already started. Don’t change any setting that you don’t fully understand (leave default values) and click on Finish.

Take care of the following settings:

- For encryption for local server, enable “VoIP encryption” on the “Roles and features” tab
- For encryption for other server(s) enable “VoIP tunneling” on the “Roles and features” tab
- On the company tab use your company name and fill in the admin username and password to receive a daily report about the usage
- On the network tab enter the IP address you wish to use if your server has multiple interfaces. Use the bindip to restrict the usage to only one interface. Enable the tcp and http tunneling. Enable private ip / local ip if your outbound server(s) are located on the same server/LAN
- On the “Tunneling” page enter your upper server details (where the traffic is sent and accepted). More can be added in routing or configured on client side.

Tunneling specific settings

The voip tunneling specific configuration options are the followings (Configurations form -under the “Other” section):

-userautoaddwithowner: -1: auto (will def to 10 for enc), 0=no, other=max channels for owner (auto enable new tunnel users. maybe useful for trial users ...but we also add them from auto trial server)

-maxlineforautotunnelusers: specify def max simultan count for auto added tunnel users. default is 5

-allowupperserverselection: 0=no,1=yes (def), 2=yes only if found as sipserver allow client softphone to specify upper server. default is true. the upper server can be an id string (rdport from tb_users) or address

-alloweuserusercalls = 1; //0=no (don't check if local target),1=yes (default),2=disable (dropp) call to endusers route calls directly between endusers or all calls have to go trough upperserver

- fwdregistrations=2 //0=no,1=only from alternate port, 2=always
- fwdregistrations_domain=registrar sip domain

- fwdregistrations_ip=registrar ip or FQDNS
- fwdregistrations_port=registrar port
- autocreatereguser=1 //0=no,1=when fwd authenticated ok register, 2=always (when we receive the register)
- forwardauthentifications=1 //will forward invite (regarding routing setup)
- alternatelocalport=xxx (use any port except 5060 which is the standard SIP signaling port)
- alternatelocalportencrypt=3
- normalize_clean=1
- normalizenumbers=0
- usehttp=true
- usetcptunnel=true
- localtcpport=443
- localhttpport=80
- alloweuserusercalls (true or false) whether to allow local calls to bypass your server
- autonewusersencrypt (optional)

```
-checkoldencryption = true;  //set to false if old enc is not used
-disableencryption = false;  //will disable all encryption checks (if we are using separate tunnel server, then this would speedup a lot)
-hideserver = 0;   //0=no,1=most,2=completely hide (allow only encrypted)    server should not respond to any simple/weak request (otherwise very easy to block by just sending a verify message and blocking if certain response received)
-v2mode = 2;    //new version with api, forward, encv2, etc. todo: maybe use db version for this
-encv2 = 0;  //0=don't use,1=auto. not implemented ,2=yes,3=exclusive (accept only encrypted calls from clients. not implemented yet)
-encv2_inithashtype = 2; //0=fix username + salt only, 1=username + salt only, 2=username+pwd+salt (def)  //should be always 2
-encv2_keyhashtype = 2; //0=fix username + salt only, 1=username + salt only, 2=username+pwd+salt (def)   //should be always 2
-encv2_defusername = "tuaxaqplbty";   //should be different on each server
-encv2_defpassword = "v4gz9laq2nggt"; //should be different on each server
-encv2_initsalt = "cpa8gnawgttycmaz5nng";
-encv2_keysalt  = "ih1nd0ann7axr4hj2fh";
-encv2_dhheader = "rfaxh";
-encv2_initpacketxor = 75;  //should be between 10 and 125
-encv2_clientsaltminlen = 5; //5. max: 60
-encv2_clientsaltmaxlen = 60; //5. max: 60
-encv2_headerxor = 117;  //117 not used
-encv2_longkeylength = 2000; //2000
-encv2_maxpadding = 255;  //11
-encv2_cachingthreshold = 4; //min simultan call from client for caching
-encv2_usetls = true;
-encv2_usedh = 2; // (0=no,1=sometimes,2=usually,3=yes,4=force always)
-encv2_strenc = 254;  //mod to convert bigint to bytearray
-encv2_dh_l = 1023;
-encv2_dh_p = rsa key
-encv2_dh_g = rsa key
```

These settings are already preconfigured by the configuration wizard so no further actions are required unless for specific needs.

Inbound/outbound routing

- Open the Users and Devices form and add your existing server(s) as “SIP Server” and “Traffic sender” user(s)
- Open the Routing form and add your server(s) to the default routing pattern.

Inbound traffic for gateways:
If you are connecting a gateway then for the inbound calls you can setup the routing rules either on your VoIP server (by routing calls to the gateway account) or on the tunnel server (MManage -> Routing). Otherwise the device will be presented on your VoIP server as usually, registered with the provided username/password. Please note that you can’t use IP based routing rules in this case (because the IP on your server will be seen as the tunnel server IP) except from the tunnel server, where a SIP Server user can be linked to a Enduser by setting the PRManager field of the enduser to the SIP Server IP.

Monitoring

You can use your old favorite tools for server monitoring since all traffic is sent to your existing servers.
However if you wish to monitor only the tunneling server instances, then you will find all the tools within the MizuManage remote admin client:

- running calls
- CDR
- various statistics (SL, ASR, ACD, etc by peer, by time, etc)
- disconnect reasons
- etc

Detailed trace files can be found in the server directory (*debuglog.dat files). The amount of the logs can be controlled with the "loglevel" global configuration option.

Backup

Reload the configuration or restart the server.

The VoIP tunneling server will store it's configuration in a MS SQL database. For a complete backup you need to save the followings:

- the application files (all files required are found in the program directory. The mizu VoIP server doesn't install any file in the system directory and there are no registry settings)
- the database backup file: to backup the database you can use the MS SQL Studio. You can also setup periodic and differential backups.

Use the cloning guide for more details: https://www.mizu-voip.com/Portals/0/Files/Cloning_Mizu_VoIP_server.pdf

FAQ

How can I change my tunneling server address

Whenever you change the IP address for the tunneling server, open the Configuration form and make sure that the following entries are set up correctly:

-LocalIP
-InternalIP
-bindip
-autodetectlocalip

(search for IP in the Configurations form)

How can I change my upper server address

For this you have to modify the following settings:

1. Change the registrar address:

Open the Configuration form then search for "fwd". Change the value for the following settings accordingly: fwdregistrations_domain, fwdregistrations_ip, fwdregistrations_port

2. From the Users and Devices form modify the settings for both your SIP server an Traffic sender (ip, port and domainname fields)

Make sure that your SIP server is selected in the routing (Routing form)

How can I force a codec from the server side

Fill in the "choosecodecs" field for your Traffic Sender and SIP Server users with the desired payload type(s).
For example 0 for PCMU, 18 for G729 or 0,18 for PCMU and G729

Bandwidth optimization / Compression / Bitsaver

The tunnel can be highly optimized for bandwidth reduction. In this case the app will always select the codec with the less bandwidth usage, will optimize all other parameters (for example optimizing the frame rate and enabling silence suppression) and will not add header padding (which is to improve obfuscation). No functionality loss and codec conversion is involved in this process (the full RTP functionality is kept). Codec conversion can be optionally turned on but requires a lot of server cpu and again usually hurts the quality because of the non-standard narrow band codec usage.

Another set of optimizations is applied when you have multiple calls.

-multiplexing the calls

-caching the packets (so a bigger packet is sent in every 10-20 msec instead of many small packets and their headers)

In average the tunnel can save around 80% of the bandwidth (between 0% and 300%+ depending on the circumstances).

How to disable the unified port

Leave the access port setting to empty or set the "usemainaport" config to false

In this case you can still access the services on its own ports. For example for webportal set the "runwebportal" to true and set the "cfg_port" for any value you wish

How to force a specified transport

By default the tunnel will always choose the best available transport method with some heuristic. If you wish prioritize or use only one transport method, then the following client settings can be changed:

-encv2_singletransport=transportmethod //other methods are not checked at all
-encv2_onlytransport= transportmethod //whenever possible, this transport will be selected
-encv2_faworizetransport= transportmethod //the priority of this transport will be increased

The “transportmethod” parameter is a number with the following possible values:

-udp: 0
-udp with socks: 1
-tcp with random ports: 3
-tcp via local socks: 4
-tcp on port 443 or 80: 5
-tcp via local http proxy: 6
-tls: 7
-http (fast): 8
-tcp via remote socks: 10
-tcp via remote http proxy: 11
-http (browser): 13

How to force a specified server/peer type

By default the tunnel will always choose the best available server or node to connect to. If you wish prioritize or use only one server then you can use the following settings:

-encv2_onlyserver=servertype //this server type will be forced
-encv2_faworizeserver= servertype //the priority of this server type will be increased

The “servertype” parameter is a number with the following possible values:

-main tunnel server final: 1
-backup tunnel server final: 2
-main tunnel server: 3
-main tunnel server alt ip: 4
-backup tunnel server: 5
-built-in proxy: 6
-dynamic proxy: 7
-distributed network: 8

Direct server connect

The clients can be preconfigured to probe direct connection to the VoIP server (connect directly without encryption with clear sip/rtp).

This can be enabled by (so the client might connect directly when available):

Cantryudpdirectep: true //set to true to enable direct try or false to disable
cfgusetunneling = 1; //0=never,1=automatic,2=always,3=always (never direct)
Directserveraddress: voipserver:port //same as upper server

To disable (always use tunneling only):

Cantryudpdirectep: false //set to true to enable direct try or false to disable
cfgusetunneling = 3; //0=never,1=automatic,2=always,3=always (never direct)
Directserveraddress: ""; //clear this

JProxy Management

JProxies are an important part of the Mizu tunnel distributed network.

This section is mainly for Mizutech Support.

- on new server (and adjust after new proxy was installed):
  - set tunel servers jproxycount in crm db tb_tunnelservers
- after new jproxy install:
  - add jproxy to tb_dynresources if not exists (should be there automatically once launched)
  - set proxy type_sub to 2 (def) or 3 (dyn) or 5 (reserved)
- periodically:
  - check not working proxies every 10 days: select * from tb_dynresources where type_main = 2 and type_sub not in (0,1) and (jplastpresent is not null or jplastpresent < getdate() - 0.2 or (createddatum < getdate() - 5 and ((jplastworking1 is null or jplastworking1 < getdate() -3) or (jplastworking2 is null or jplastworking2 < getdate() -3.1))))
- concept:
  - jproxies will auto add themself to crm db on first run (via http request to licensing service)
  - jproxies will send periodic statistics to crm db (via http request to licensing service)
  - def proxies are configured from mmanage wizard (these are hardcoded into softphones)
  - dyn proxies are dowloaded by tunnel server automatically every night and auto assigned to clients (2 proxy for each client sent by auth ok sip messages)
  - mserver will auto update jproxy stats from data received from webphones (server local db only for now)
- fields:
  - jplastpresent: last message from jproxy (jproxy should send status every hour, so this is ok if in the last hour, otherwise there are some problem)
  - jplastworking1: last message from jproxy with any msg from clients
  - jplastworking2: last message from jproxy with any msg from server

More help

For more details, please consult the Admin Guide and other server related documentations on our website.
Install, configuration and support services are included with each license plan. Contact serversupport@mizu-voip.com