Mizu VoIP server security and account limiting

Contents

The Mizu VoIP server is secure by default however with also usability in mind. For common usage you can leave everything with the default settings and you still have a high level protection as the Mizu server has security constrains and built-in automatic attack prevention mechanisms at multiple levels enabled by default. The Mizu VoIP server has very few dependencies of third-party components (including OS services) which also improves security.
Please note that regardless of the server side security, there are still a room for hackers to exploit client endpoints such as stooling SIP username/passwords from softphones/devices. You can't prevent these to happen as it depends on client environments and third party software/hardware however you can still reduce its impact by leveraging strength server side restrictions (max lines, max daily/monthly limits and others).
For extra security, read through this this document and fine-tune your settings, however please note that most of these settings will have direct effect on usability. (Your service might work incorrectly if security restrictions are too strength. Don't change setting unnecessarily)

OS security

The Mizu VoIP server uses only core windows services (networking, file access and other resources with no security implications) so it is not vulnerable for the usual windows related vulnerabilities, because kernel/core ip networking vulnerabilities are very rare and hard to exploit (and windows is no worse in this then other systems such as like linux).
For maximum security just use a clean windows install, with no any unneeded services enabled and see the OS security checklist at the end of this document.
You might further secure / lock down your OS. Usefult links:

- https://www.netwrix.com/windows_server_hardening_checklist.html
- https://serverfault.com/questions/170973/what-is-the-best-way-to-harden-windows-server-2008-r2
- https://help.1and1.com/security-c85142/server-protection-c85157/windows-server-security-tips-a752361.html
- https://technet.microsoft.com/en-us/security/cc184923
- https://support.microsoft.com/af-za/help/278295/how-to-lock-down-a-windows-server-2003-or-windows-2000-terminal-server
- https://www.upguard.com/blog/the-windows-server-hardening-checklist
- https://technet.microsoft.com/en-us/library/2005.05.lockdown.aspx
- https://www.eurovps.com/blog/how-to-secure-your-windows-server/

DB security

The database contains ALL the data used by the Mizu server including user details and CDR records so a special care has to be taken to protect your database.
With a regular SQL install using a strong password you are already secure by default without any special action to be taken.
SQL injection attacks are prevented on multiple layers: all input data are properly filtered and sanitized. SQL parameters are passed by query parameters and not with SQL query string manipulation using stored procedures whenever practicable.
Note: the MManage admin client is treated as a trusted component with few restrictions once the user is logged in.
Make sure to have working backups (incremental/full) to be able to recover your database from a disaster at any time.
Best practices:

- Set a good complex password
- Change the default listen port to filter out most scrip kiddies and commong SQL server attack tools

- Completely disable access to the SQL server from outside (allow only local apps and/or whitelist your other servers which might need access to database)

Socket/stream level network protection

All streams are rate limited in the server to avoid all DoS or overflow attempts.
To fine-tune, you might change the "maxnetworkspeed" global config option which is set to 800000 by default (this means 0.8 gbits so it is optimized for a gigabit NIC with some room for IP/TCP/UDP headers)
For example if your NIC is only 100 mbits, then you might set this to 80000.
These and other extra protections are also applied for media streams for RTP/RTCP flood protection.

Address level network attack preventions:

- DOS attack prevention: when there are too many messages received from an IP address, the address will be blacklisted automatically. Controlled by MAXSUBSMSGCOUNT (default is 39000) and MAXSUBSMSGPERIOD (default is 3 minute) global configuration settings.
- when there are too many "wrong" or meaningless messages from an IP, the address will be blacklisted automatically. Is controlled by MAXWRONGMSGALLOWED (default is 4000) and MAXWRONGMSGPERIOD (default is 1 hour) global configuration setting.
- when there are too many unauthorized request from an IP, the address will be blacklisted automatically. Is controlled by MAXWRONGAUTHFROMIP (default is 2500) and MAXSUBFAILAUTHPERIOD (default is 1 hour) global configuration setting.
- when there are too many unauthorized request from an IP:port, the address will be blacklisted automatically. Is controlled by MAXFAILEDAUTHENABLEDIPPORT (default is 50)/ MAXFAILEDAUTHENABLEDIP (default is 800) and MAXSUBFAILAUTHPERIOD (default is 1 hour) global configuration setting.
- You might set the "checkrtpaddr" configuration option to 2 to force the server to accept rtp packets only from known media sources. (the default setting is false)
- All counters are reset periodically controlled by the REENABLEDOSBLOCKED (default is 6 hours) global configuration setting.
- For the new registrar module the "fastauthsubswrongusermsg" setting will be applied: not authenticated messages from same ip or all messages in 90 sec. (also X*10 for any IP). Default value is 300.

Session level protection

Session level limits are enabled for all services provided by the Mizu VoIP server. This includes the core VoIP services (SIP/H323) but also the enduser web portal and the API.
The server will close the session on the following circumstances:

- absolute timeout, call timeout, media timeout, ring timeout, call init timeout, timeout on session timers (all these are configurable from MManage -> Configurations form)
- too many incoming messages (dynamically based on frequency and number of requests)
- too many authentication failures (dynamically based on frequency and number of requests)
- too quick (abnormal) message receptions (dynamically based on frequency and number of requests)

- subsequent invalid signaling messages (DDOS protection)
- some known scanners are blocked by default. You can add more with the "**blockua**" global config option

Blocked devices and users can be re-enabled by issuing the “delbanned,ip” or “delbanned,all” command on the Console port.

Web security

The Mizu VoIP server uses a native embedded engine for web interfaces so it is not vulnerable for the exploits against the common web servers.
The web engine implements the best current practices including proper authentication, input filtering, rate limiting and XSS attack prevention with secured default settings.

IIS is not required for the Mizu server. Avoiding IIS will lower your server vulnerability. Host your webpages elsewhere, not on your VoIP server.

API access security

The API is secured by default and each sensitive API requires proper authentication to be executed. All data received from the network or user input are properly filtered and sanitized.
Optionally you can harden its security by setting up HTTPS access, setting a random httpapikey key and by fine-tuning the API access.
See the "Security", "Authentication" and the “Hardened access” sections in the VoIP_Server_API documentation.

Payment security

User payments security are completely offloaded to payment gateways (for example PayPal), which must comply for PCI requirements.
This means that the Mizu Server doesn't process any confidential data such as user or credit card details, just forwards the user to the configured payment processor.
Once the transaction is completed (or failed) the Mizu server will receive a message from the payment processor to handle the result (increase user credit).
Various frauds are not uncommon with online payments which are handled by both the payment processor and the mizu server. Suspicious transaction can be left to be approved manually instead to be accepted automatically.
Check your PayPal related settings to enforce proper verifications and limits. (See the PayPal related section in the documentation and search for “paypal” in the MManage configuration form)

Encrypted VoIP

The Mizu VoIP server provides a complete solution for secured communication. See the "Encryption and tunneling" section and the VoIP tunnel documentation for the details.

SSL/TLS/WSS/HTTPS setup

You can use the TLS proxy module to apply secured transport. This module can be used to encrypt all services offered by the mizu voip server, automatically handling each built-in protocols separately regarding to its requirements, including:

- SIPS (Secure SIP protocol. Default port is 5061. Unencrypted port: 5060)

- VoIP tunneling (tunneling over TLS. Default port is random)
- HTTPS (Secure HTTP protocol. Default port is 443. Unencrypted port: 80). This is used for the following services:
    - enduser web portal (default internal unencrypted port is 8080)
    - API (default internal unencrypted port is 80)
    - mmq service (default internal unencrypted port is 80)
    - websocket (for API, WebRTC and mmq)
    - the universal port 80 (unified maina port)

By default it is shipped with a self-signed certificate. This can be used for VoIP tunnel encryption, but not for authentication/identity and if used for the webportal, the browsers will present a warning.
Follow the following steps to setup to enable TLS on your server with a valid certificate:

1. You need a (sub)domain name assigned to your server IP (you should also set it in "LocalDomain" global config).
   If you already have a domain name (such as company.com/www.company.com) then with most of the DNS providers you can create sub-domains for free from their control panel. Create a subdomain like sip.company.com for your VoIP server IP. If you don't have a domain name yet, then you can purchase for any DNS providers at around $10/year. For example at GoDaddy.
2. Get a valid certificate for your domain from a reputable CA
   For example you can get free certificate from Let's Encrypt (~~or from StartSSL by following these steps~~).
3. Make sure the tlsproxy.exe, tlsproxy_mserver.exe or tlsproxy_servicename.exe exists in your app directory (contact us if you can't find this app in your server directory)
4. Add your SSL certificate. For this you just have to copy the following files in the server directory:
    - cert.pem: the certificate file (your certificate as received from the CA)
    - key.pem: the key file (which you have generate on cert request
    - root.pem (the CA root certificate)
    - dh.pem and/or dh2.pem (this is optional)
      This is used for DH key exchange and it can be generated with the following commands:
      -fast: openssl dhparam -dsaparam -out dh.pem 1048
      -slower/better: openssl dhparam -out dh2.pem 2048

   All these are clear text files. If you haven't received your certificate in similar format from your CA, then convert (convert , convert) them and create these files (copy content using notepad). If these files are not set, then it will use a self-signed certificate (which will result in browser warnings).
5. Set server settings (search for "tls" in the global configuration)
    - usetls: set to true for SIPS (SIP signaling encryption)
    - encv2_usetls: set to true if you wish to use TLS for VoIP tunneling (if you are using the VoIP tunneling module)
    - usetlsforweb: for internal webportal
    - usetlsforall: will auto set TLS for mainaport, web, voip tunnel, sips (recommended)
    - forcetls: runtime http -> https rewrite: 0=force no, 1=def, 2=force tls,3=extra

- localtlsport: SIPS TLS port (default is 5061)
- sslcertpwd: if your certificate is password encypted, set the password here
- set the domain name assigned to your VoIP server to the "localdomain" global config
- you might also set the cfg_baseurl webportal setting to https:\\yourdomain

6. Reload or restart the service (restart recommended)
7. Test:
    - Example request for enduser webportal over the unified port: https://yoursipdomain.com/webvoip
    - For api: https://yoursipdomain.com/mvapireq/?apientry=apitest1

Other tools:

- SSLBuddy
- OpenSSL (win binaries)
- Test

User authentication

The mizu server provides flexible user authentication services which can be set per user by the "AuthType" config option from MManage. See the "Users" and the "User authorization" section for more details. On the IVR the users can be authenticated also by PIN code or A number authentication. See the "IVR" section or the IVR documentation for the details.
For speed considerations, the mizu server can cache device login information for a time so it will not ask again for authorization for every REGISTER or INVITE request. This means that it can happen that you change the user credentials and the user is still able to login with its old username/password or inverse: the user enters the correct credential but will be still blocked for a time. This can be controlled by the "cacheregistrations" global config variable.
The server will periodically recheck the password for all accounts and will change to a random strong password when weak password is found (enforcestrongauth global config option). Password storage can be encrypted/hashed as set by the securepasswords global config option (on by default).

Per IP call limits

You can restrict the maximum number of calls or call duration from a source address by the following global settings:

- maxcallperip: max number of calls from the same IP
- maxdurationperip: max call duration from the same IP
- maxcostperip: max call cost per IP
- maxcallperperiod: the period for the above (1.0 means one day)
- maxcallperuserid: the above will be set to this user only (set to -1 for all users)

Additionally to IP restriction you should set as much other restrictions as possible to restrict your server attack surface, such restricting the usage to one user (maxcallperuserid), set user as prepaid, set max lines and daily/monthly limits on the account as other best practices discussed in the documentation.

IP Spoofing

IP Spoofing means incomgin TCP or UDP packets with false source IP which might be used by attackers to impersonalization. You can avoid this with the following meassurements:

- If you are vulnerable to IP spoofing, make sure to not use IP based authentication.
- Consider using a techprefix also of IP authentication is required for call (NeeAuth user field set to 3 which means IP auth + tech prefix)
- Make sure that your router or gateway performs proper ingress filtering (blocking of packets from outside the network with a source address inside the network).
- Adjust the allowtrustedip global config option after your needs: 0=no,1=my ip only,2=private ip's only,3=yes(def),4=everywhere(including admin console)

Firewall

The server has a built-in static and dynamic firewall to block unwanted sources. See the “Firewall” section in the documentation for more details.

Maximum simultaneous call limits

To avoid overflow with calls you should set the MaxLines/MaxLinesOffpeak settings for each enduser and traffic sender properly.
(For enduser the default Max Line is 5. We don't recommend to be set to 1, since this might disallow services such as call transfer and conference)

Prepaid account credit limits

Prepaid accounts have a hard limit by their credit value.

Postpaid account monthly spend limits

You can also limit postpaid account to prevent unexpected bills.

Set the “creditcheckforpostp” global config to true.
Set a meaningful default and actual value for each user for the followings: maxmonthlycredit, maxmonthlycreditinc, maxmonthlycreditend.

- maxmonthlycredit: max allowed credit/month even if the user is postpaid
- maxmonthlycreditend: max Maxmonthlycredit (because we increase Maxmonthlycredit by maxmonthlycreditinc every month if the user was active)
- onlylocalaccess: traffic sender traffic will not be forwarded (can call only local users from tb_users and tb_numbers)
- maxmonthlycreditinc: determines how much money we add to Maxmonthlycredit every month

To set the default value, you should edit the database default values and then run a query like this:
update tb_users set maxmonthlycredit = X, maxmonthlycreditinc=X, maxmonthlycreditend=X where type = 0 and postpaid > 0

To make it default for new users:

alter table tb_users drop constraint DF_tb_users_maxmonthlycredit
alter table tb_users drop constraint DF_tb_users_maxmonthlycreditend
alter table tb_users drop constraint DF_tb_users_maxmonthlycreditinc

alter table tb_users add constraint DF_tb_users_maxmonthlycredit default X for maxmonthlycredit
alter table tb_users add constraint DF_tb_users_maxmonthlycreditend default X for maxmonthlycreditend
alter table tb_users add constraint DF_tb_users_maxmonthlycreditinc default X for maxmonthlycreditinc

Fix daily credit limits

You can apply a maximum daily limit for all (both prepaid and postpaid) accounts with the following global configurations settings:

- maxdailycreditforenduser (max daily spend for traffic senders)
- maxdailycreditforts (max daily spend for endusers)
- You can also set the limit on user level by setting the "maxdailycredit" field for the respective users. (For this to work you should also set the "maxdailycreditperuser" global config option to 1, but that is auto set at first config reload if at least one user has "maxdailycredit" set)

Dynamic credit/spent limits

Set the "checkmaxdyndailycredit" global configuration option to enable dynamic credit/spent monitoring and call block on threshold.
Once this is turned on, the server will not allow the usage (spending) to grow more than a specified level (maxdyndailycredit_multiplier) within a single day.
(The server will always remember the maximum value spend by a single user in a single day. Then it will block the calls if this value is exceed by the specified multiplier)
Configuration:

- checkmaxdyndailycredit: 0=disabled,1=enabled for enduser,2=enabled for endusers and traffic senders
- maxdyndailycreditforenduser_min: will not block endusers if spend below this value (default is 10)
- maxdynmaxdailycreditforts_min: will not block traffic senders if spend below this value (default is 100)
- maxdyndailycredit_multiplier: max grow allowed within a single day. Default is 7 (you might lower it for better protection, however values below 4 is not recommended because that can be considered as normal calling pattern)

The disconnect reason for such calls can be configured by the “quotadiscreason” global config option. Default is 403.
Admins can receive emails about user blocks if the sendadminemailnotifications global config option is set to 2.

For example if user A normally spend 10 usd maximum per day, and if one day it suddenly reach over 70 usd then calls are blocked. Please note that smooth increase if traffic is still fine (the max allowed grows automatically if the user is below the max grow limit).
Another example:

- Monday (firs day) the user spend 10 usd. Fine, the maxdyndailycredit is set to 10.
- Tuesday the user doesn't make any call. No changes.
- Wednesday the user spends 5 USD. No changes since 5 is lower than the previous max which was set to 10 on Monday.

- Thursday the user spend 30 USD. Fine since 30 is lower the maxdyndailycredit * maxdyndailycredit_multiplier (which is 70). The maxdyndailycredit is set to 30.
- Friday the user (or a hacker which have stolen the user credentials) start to make mass calls or calls to expensive direction. Once his spending reaches 210, the account is blocked (210 = the previous maxdyndailycredit which is 30 multiplied with the maxdyndailycredit_multiplier which is set to 7)

Follow these steps to enable this for old database versions:

change tb_users.todaycredit data type from int to decimal(18, 5)
exec sql: ALTER TABLE tb_users ADD [maxdailycredit] [int] NULL
exec sql: ALTER TABLE tb_users ADD [maxdyndailycredit] [int] NULL
add a.maxdailycredit,a.maxdyndailycredit to [v_checkuser] select list
set globan config:
maxdailycreditforenduser=1
maxdailycreditforts=1
maxdailycreditperuser=1

Fraud calls

By default the mizu server blocks most of the well-known satellite and premium numbers (blocksatellitecalls and blockpremiumnumbers).
You can also block other unwanted destinations from routing or billing

Blacklists

With the fix/dynamic and smart blacklist modules you can efficiently block unwanted numbers. See the Blacklisting/Access Lists chapters in the documentation and/or search for “black” in the Configurations form from MManage for more details.

Billing and profitability

To make the billing strict, you might also set the following global parameters:

- blocknotbilledcalls: 0=no (default),1=if best match packet is not found,2=if no exact packet match with prefix,3=block if not assigned directly for the user,4=check also tariff list prefix,5=check also parent tariff list
- blocknotprofitablecalls 0=no (default),1=yes,2=yes also if equal,3=block also when it is not set
- vgetpriceexactmatch: 0=no (default), 1=yes for resellers, 2= yes for all
- notbilledcallerr=0 0=default (error with 2 priority),1=error,2=critical
- blockhighcostcalls: don't route the call if the cost per minutes is higher than this value (default is 0 which means no limit)

Security checklist

Go through the points below to better secure your VoIP service:

Network security:

- make sure that your router or gateway performs proper ingress filtering (blocking of packets from outside the network with a source address inside the network).
- set proper firewall rules to protect your services (not important for the VoIP service itself, but you might host other services within your network which might require firewall protection)
- set proper packet flood filtering rules
- be avare of DDoS attacks and its mitigation especially if you are a big organization or VoIP is vital for you (while the VoIP service is capable to mitigate DDoS attack by itself, this will not help if your ethernet ports are fully flooded)

OS security:

- do not install any third party software on your VoIP server and don't use it's desktop for your daily work
- enable the embedded windows firewall. It's speed and application level packet filtering is perfect for VoIP. Enable only the needed applications (mserver.exe, mssql.exe, vfpt.exe, tlsproxy.exe, mizuweb.exe)
- disable all unneeded network services (File and Printer Sharing, IIS, FTP, etc. With a clean windows install this is not necessary since not installed/enabled by default)
- disable NetBIOS over TCP/IP and Client for Microsoft Networks on network connections where it is not needed.
- don't install any virus scanner (it is meaningless)
- choose a strong password for your OS accounts (especially for the Administrator account and better if you don't create or disable all unneeded OS user accounts)

DB security:

- choose a strong long password for your database access (also for the sa account).
- change the default MSSQL port from 1433 (this is not a security issue, but when the MS SQL runs on the default ports, you can experience lots of login attempts).
- restrict the SQL service account (and don't use the default system or network accounts; this is important especially if your server is not dedicated to VoIP / you are using the server also for other purposes)
- create users with different roles and set only minimal rights as required (especially if the engine is hosting also other databases)

VoIP service security:

Change only the values which are meaningful for your needs, otherwise you might prevent normal usage also for users which should be otherwise trusted.

- strengthen the above listed configurations (DDoS attack prevention, per IP call limits, max monthly call and credit limits, daily credit limits, max line per user, etc)
- request (and verify) as much data from your subscribers as necessary (country, email address, etc)
- increase minpwdlength (default value is 4)
- set the fwdtootherdomains global config option to 0 to disable arbitrary call routing to other domains

- set the “apiv2key” global config option to a random value (a short 5 digit number will fulfill its reason)
- set the “enforcestrongauth” global config option to true (true by default since v.5.2 2013)
- make sure that all users have a strong password (this should be fulfilled automatically if the rest of the settings are set correctly)
- set max amount, max ports for users
- set maxmonthlycredit per user (as discussed in above sections)
- set callingcardauth to a more strict check (for example set to 9 for pin code strict only)
- configure the maxdyndailycredit global config option and dynamic credit/spend limits as discussed in above sections
- set the securepasswords parameter to 1 or more
- set the uauthverifypwd to 0
- set authfastusers to 1
- set the forwardclientaddress to 0 (to prevent forwarding the peer location)
- set the apisipauth to 1 (to enforce SIP authenthication for API access when appropriate)
- set a random serverapikey (don’t change it if you already have customized softphones)
- set the blocksatellitecalls and blockpremiumnumbers to true
- leverage TLS security (optional)
- set the blockearlymedia and blockearlymedia_in after your needs to mute the communication before full call setup
- disable unwanted directions (unwanted countries, etc)
- check your traffic on a daily basis or setup scheduled tasks to check abnormal traffic amounts and notify you by sms or email. Use the Analyze form regularly.
- setup the allowed ip and trusted ip global config option properly by the “apiv2ipauth” global config option (applied especially for the http api). Disable "trustlanip" from global config if not needed.
- check proper dtmf input in your ivr scripts
- set apidefneedlogin to 3 for nonce verification on API access
- set apideftrustadmin to 4 (0: no, 1: admin if trusted ip (def), 2: always ip only, 3: always pwd only, 4: always ip+pwd)
- check your global configuration parameters related to IP, port, currency, credit amounts and other restrictions
- make sure that the A number authentication is set correctly if you are using IVR call forward. disable if not needed (turn off for each traffic sender at the "Functions" tab and/or set the "anumberhandling" global config option to 0)
- you should verify first payment manually (don’t accept automatically first PayPal payment from not verified users. see the PayPal settings)
- disable JSONP to other servers by setting the "enablejsonp" global config option to 1
- you might set the "autofinetune" to 0 to set consistent service level (but this is not optimal for high-load servers)
- disable http file upload if no file sharing services are used by setting the "allowhttpfileupload" global config option to 0
- you can also apply system level limits by the licensecfg global config option (see the “License limitations” FAQ section)
- set the default credit to 0 by executing the following queries (from the direct query form or from SQL management studio):

```
alter table tb_users drop constraint DF_tb_users_Credit
alter table tb_users add constraint DF_tb_users_Credit default 0 for Credit
```

The most important security related settings where listed in this document.
For more configuration options , consult the documentation.

Links

VoIP server home
Documentation
Email