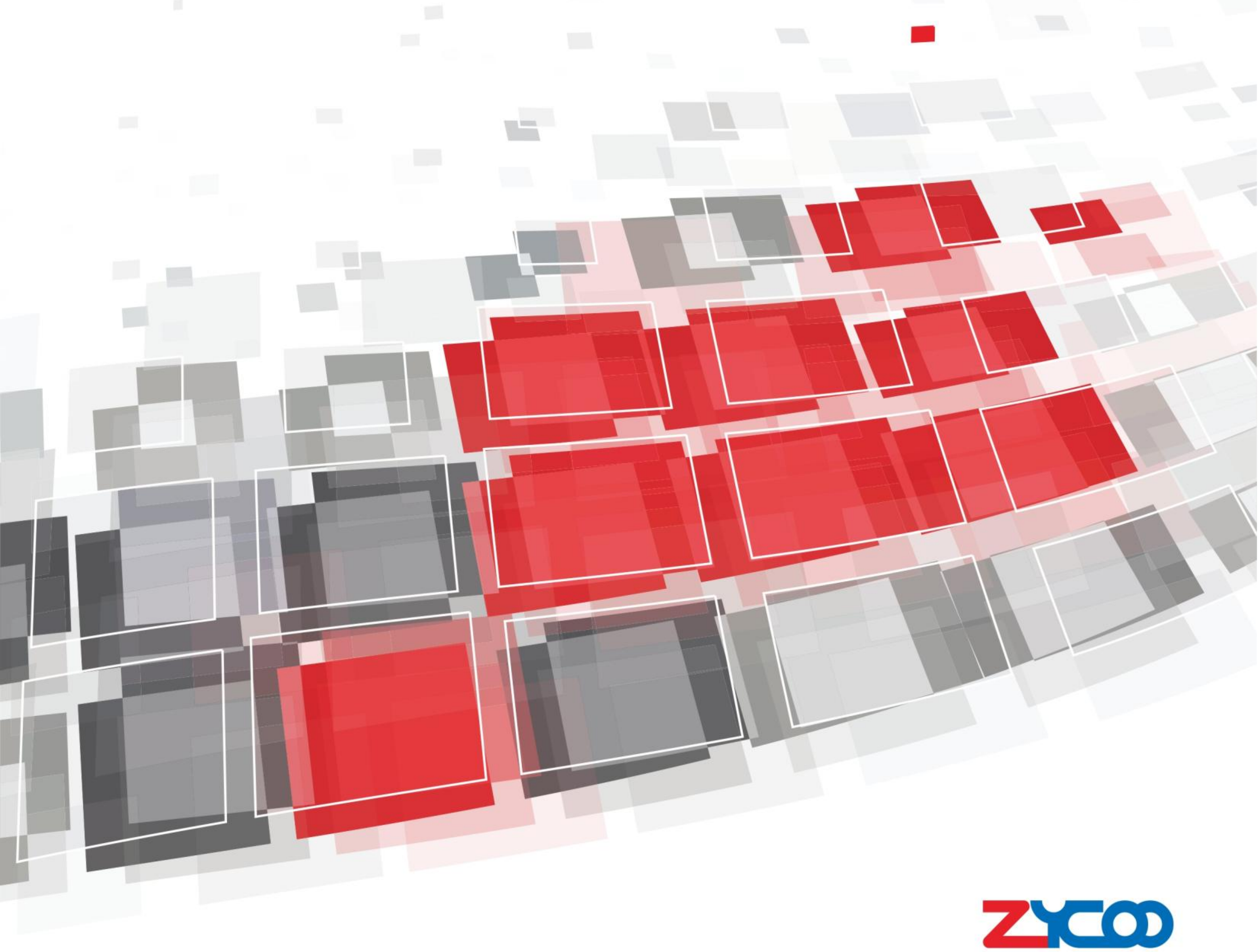
IP Phone System Security Guide

CooVox-U20/U50



We Focus · We Deliver

Contents

1. Introduction

In recent years, with VoIP solutions deeply and prevalently applied in various fields thus security requirements have been changing all the time. ZYCOO, as one of VoIP solutions provider and IP PBX manufacturer, also focus on improving its quality and security to meet with global customers' standards.

In order to prevent insecurity issues happening then reduce economic loss, this documentation helps and guides users how to configure ZYCOO PBX to cope with several insecurity factors. In addition, it would popularize some tips for common types of attack for users.

During this guide, we won't promise you that your system will not be hacked by following this guide. Continue working on this side of things, learning more about security, implementing your system security as you need is the only thing you need to do.

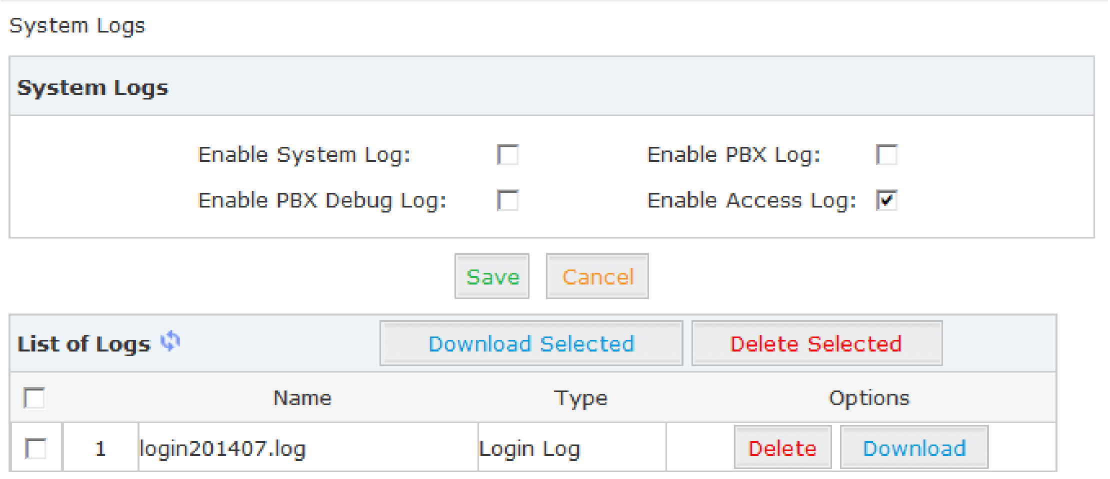
2. Embedded Security Solutions

In the first section, it will introduce four methods which have been implanted in ZYCOO IP PBX systems.

2.1 SSH Access

For U20/U50, default setting contains one solution that system itself would automatically reject the user who input wrong password over eight times and it will not allow user to register again in 20 minutes. Basically, the IP address in the same segment with IP of WAN port would directly skip detection. In other words, those IP are trusted.

It is convenient to check access log, go to 【Reports】→【System Logs】 and tick the **Enable Access log** option.



System Logs

System Logs

Enable System Log: □ Enable PBX Log: □

Enable PBX Debug Log: □ Enable Access Log: ☑

List of Logs

□		Name	Type	Options
□	1	login201407.log	Login Log	Delete Download

Figure 1_1

2.2 Brutal SIP Flood

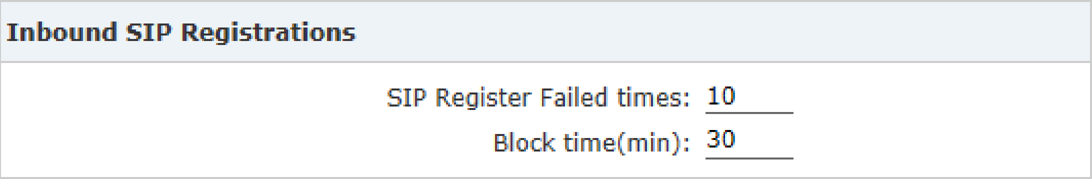
It’s produced by hackers who use the so-called SIP methods, which generates so many requests to the PBX that the system eventually has to end up serving the attacker. This causes that valid users can no longer use the service, in addition to generating excessive system processing and memory usage.

In ZYCOO PBX, system defends this with iptables. For example, if system receives over

10 packets then it would reject the IP to access. Usually, add suspicious dynamical IP in iptables list, then activate changes of PBX, and all the suspicious IP will be cleared.

2.3 SIP Register Limitation

Go to【Advanced】→【Options】→【Global SIP Settings】:



Inbound SIP Registrations

SIP Register Failed times: 10

Block time(min): 30

Figure 1_2

SIP register failed times: the maximum failed times for users can reach to 10 times Failure reasons as follows:

1. Wrong password
2. Wrong username
3. Device has banded fixed IP with phone in the extension
4. Users select improper protocol to register extension. For example, they choose TCP or TLS, but on the PBX, the default protocol is UDP, so it would not match to right protocol

Once over the register times, system will block this user unless his IP address is trusted (default WAN port IP or IP in the same segment which belongs to trusted IP of PBX) . Add suspicious IPs in the iptables list and activate changes of IP PBX, then these IPs would be cleared from the dynamic iptables list.

Blocked time: During the blocked time, the user is rejected to register since the sip register failed over the attempts.

2.4 Guest calls

We have disabled the guest calls from outside by default; that is useful to protect system receive the anonymous calls or calls without authentication.

3. Manually configure system to raise security level

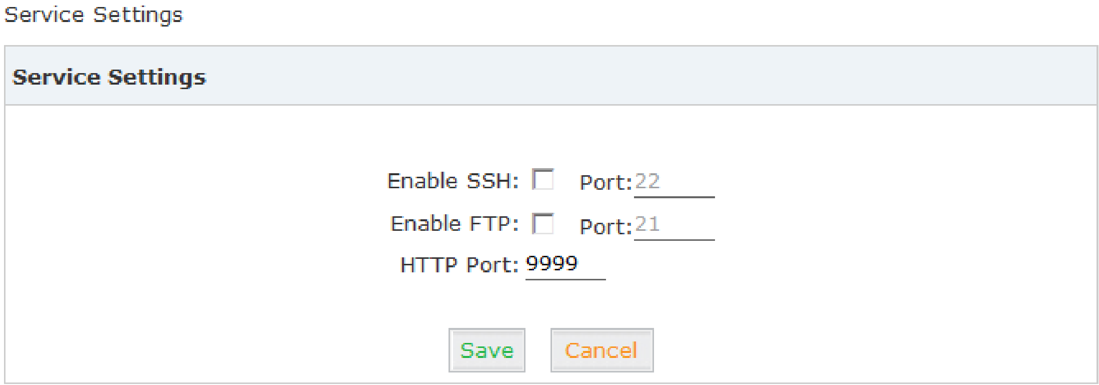
In the second section, it will guide users more methods to keep safety of system. Moreover, it requires customers to configure it according to specific situations.

3.1 Security of GUI accessing

The first part of this section is the security of entrance of system.

- **Change the default ports**

Click 【Security】→【Service】to see the following diagram:



Service Settings

Service Settings

Enable SSH: ☐ Port: 22

Enable FTP: ☐ Port: 21

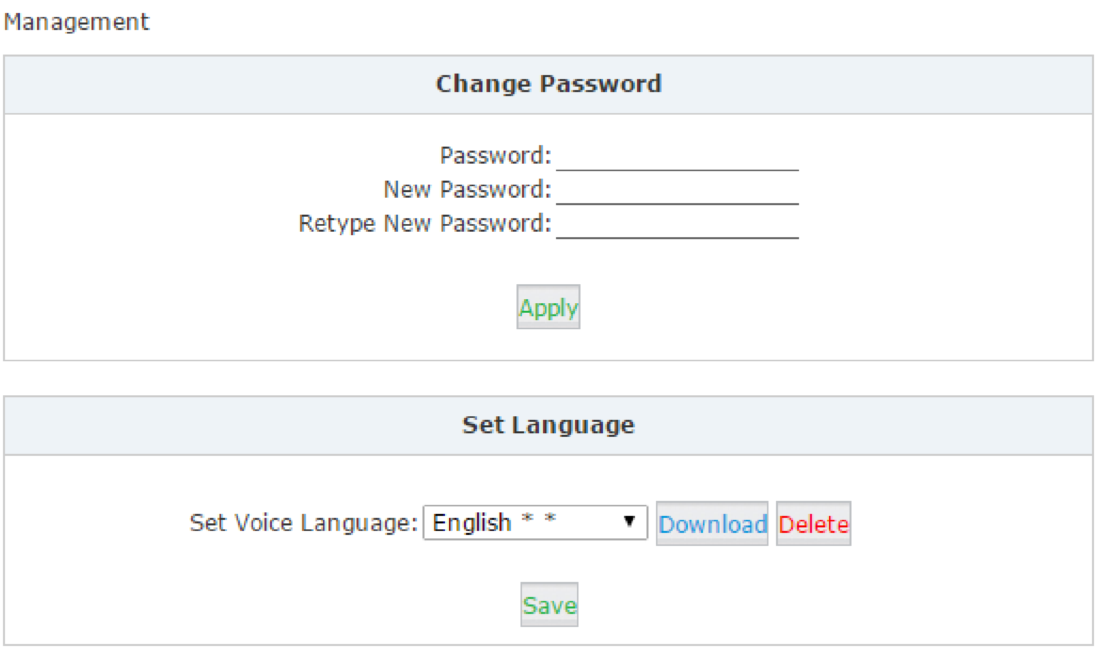
HTTP Port: 9999

Figure 2_1

Except '9999', it can be changed to other numbers. Usually, SSH port can be turned off; it allows customers to upload file via FTP port.

- **Change the default password**

Go to 'System' option then choose 'Management', which allows administrator to change password for entering into GUI. Consequently, prevent attacker to access system. Much more complicated the password is, the system is much more safe.



Management

Change Password

Password:

New Password:

Retype New Password:

Apply

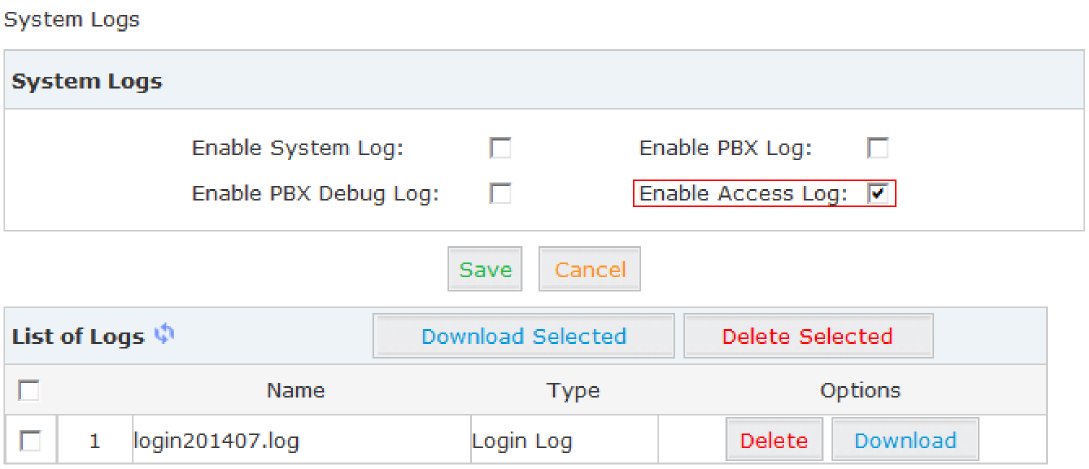
Set Language

Set Voice Language: English * * ▼ Download Delete

Save

Figure 2_2

Go through access log to check out who had logged in. Enable Access Log via 【Reports】→【System Logs】:



System Logs

System Logs

Enable System Log: □ Enable PBX Log: □

Enable PBX Debug Log: □ Enable Access Log: ☑

Save Cancel

List of Logs Download Selected Delete Selected

□		Name	Type	Options
□	1	login201407.log	Login Log	Delete Download

Figure 2_3

3.2 Extension Security

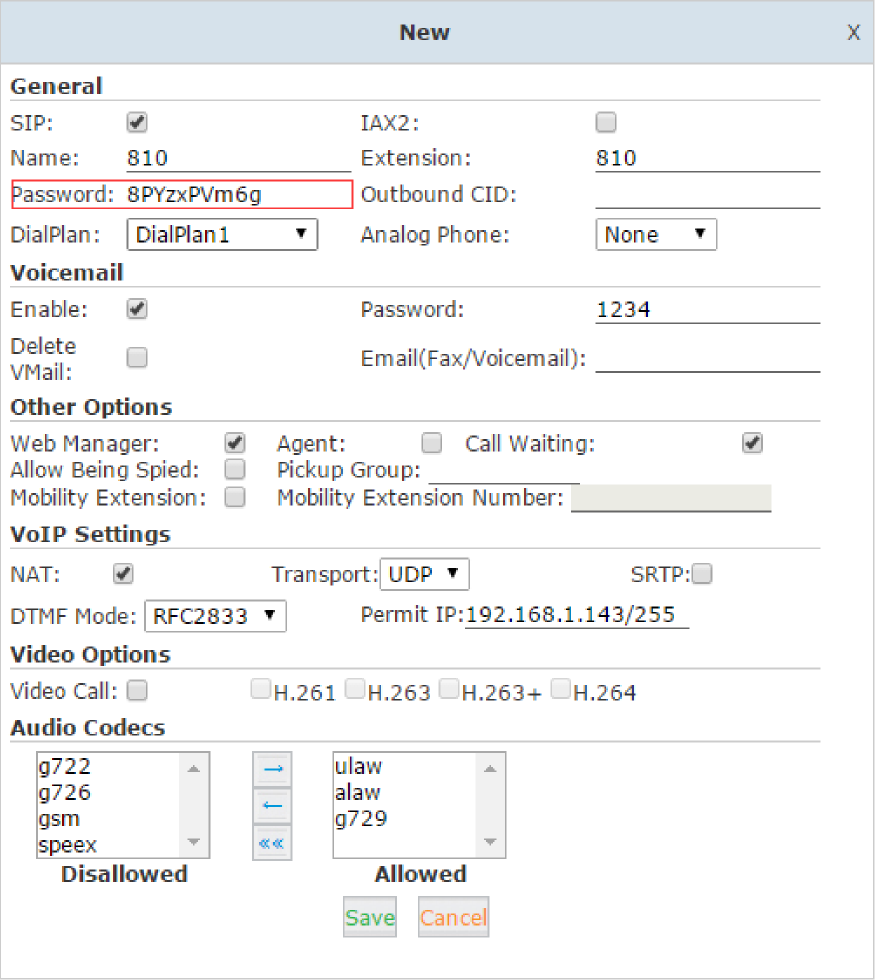
The second part in this section is to guarantee safety of extension on PBX, extension's security is also critical. It always be attacked by Hackers. Aim at this, ZYCOO PBX provides several solutions.

- **Make extension password stronger**

  It is recommended to apply default password generated by system, cause the password is generated randomly with higher coefficient than common password. Let's compare some examples as below:

Passwords	Applicability
201	basically useless - one of the first passwords that they try
94993	still poor - Script Kiddies will use a rolling number generator and try again
holiday2	Poor - Script Kiddies use a database of common words and add numbers
H883ksd3	Good - a mixture of upper and lower characters and numbers
_eK5B2hwAN	Great - probably this and the one before would be suitable

Table 1



New

General

SIP: ☑ IAX2: □

Name: 810 Extension: 810

Password: 8PYzxPVm6g Outbound CID:

DialPlan: DialPlan1 ▼ Analog Phone: None ▼

Voicemail

Enable: ☑ Password: 1234

Delete VMail: □ Email(Fax/Voicemail):

Other Options

Web Manager: ☑ Agent: □ Call Waiting: ☑

Allow Being Spied: □ Pickup Group:

Mobility Extension: □ Mobility Extension Number:

VoIP Settings

NAT: ☑ Transport: UDP ▼ SRTP: □

DTMF Mode: RFC2833 ▼ Permit IP: 192.168.1.143/255

Video Options

Video Call: □ □H.261 □H.263 □H.263+ □H.264

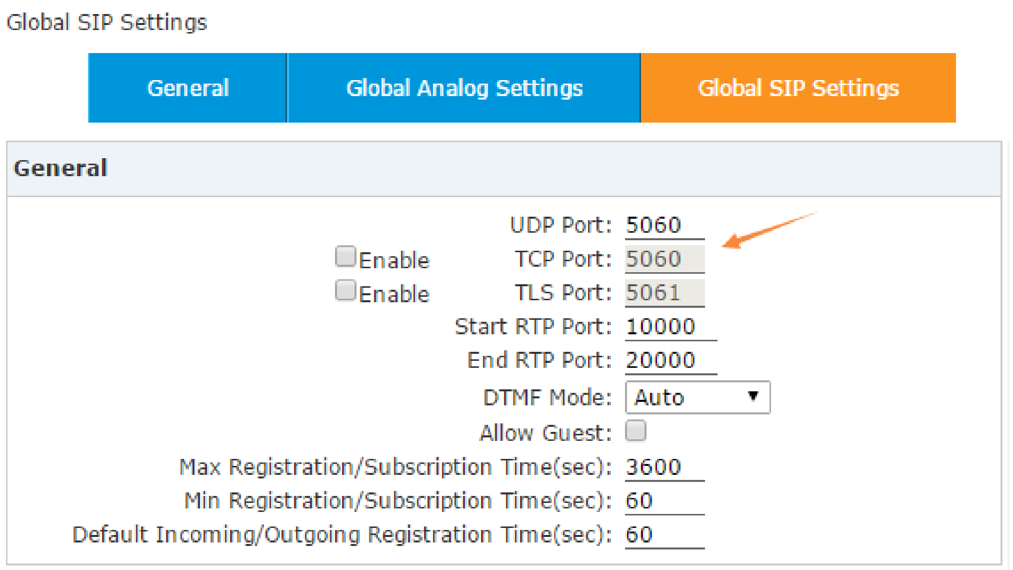
Audio Codecs

Disallowed	Allowed
g722 g726 gsm speex	ulaw alaw g729

Figure 2_4

- ## Change the default SIP port

As we know, the default port for SIP protocol is 5060. Then once this is changed, it would result in failures for hackers to register SIP account on server.



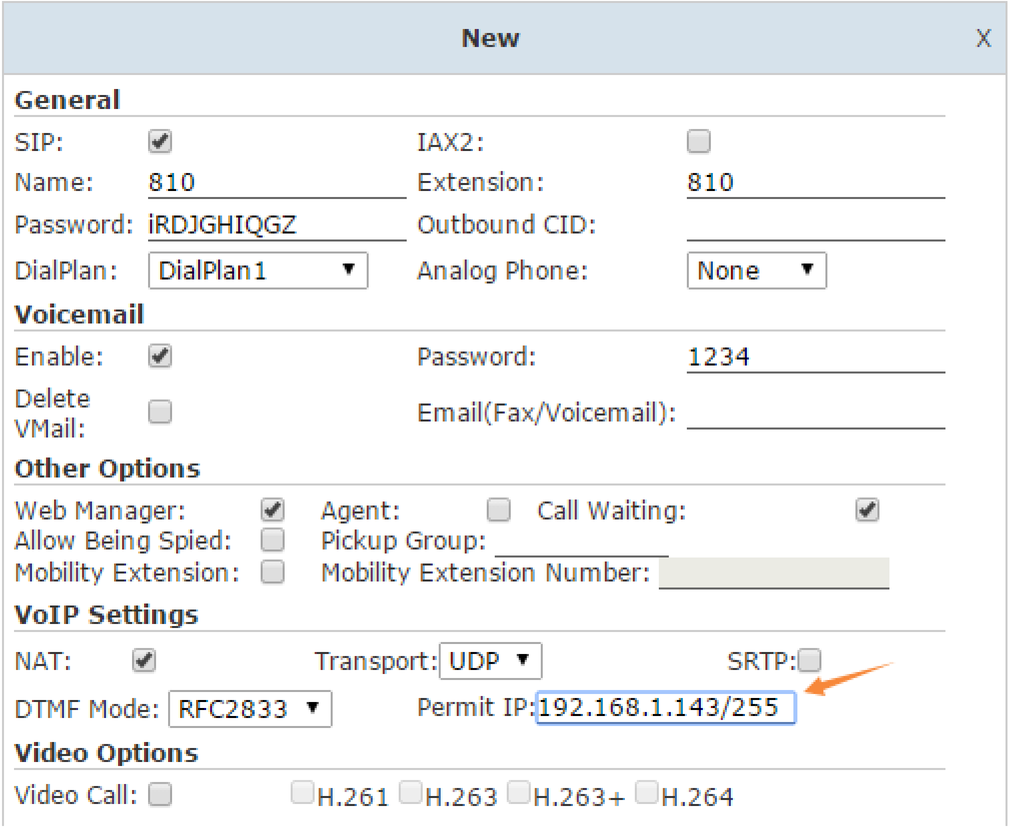
General

UDP Port: 5060
□Enable TCP Port: 5060
□Enable TLS Port: 5061
Start RTP Port: 10000
End RTP Port: 20000
DTMF Mode: Auto ▼
Allow Guest: □
Max Registration/Subscription Time(sec): 3600
Min Registration/Subscription Time(sec): 60
Default Incoming/Outgoing Registration Time(sec): 60

Figure 2_5

- ## IP Restriction for Extension

This function permits the specific IP or network segment for register. In a sense, it restricts range of IP addresses for register on this given extension.



General

SIP: ☑ IAX2: □
Name: 810 Extension: 810
Password: iRDJGHIQGZ Outbound CID:
DialPlan: DialPlan1 ▼ Analog Phone: None ▼

Voicemail

Enable: ☑ Password: 1234
Delete VMail: □ Email(Fax/Voicemail):

Other Options

Web Manager: ☑ Agent: □ Call Waiting: ☑
Allow Being Spied: □ Pickup Group:
Mobility Extension: □ Mobility Extension Number:

VoIP Settings

NAT: ☑ Transport: UDP ▼ SRTP: □
DTMF Mode: RFC2833 ▼ Permit IP: 192.168.1.143/255

Video Options

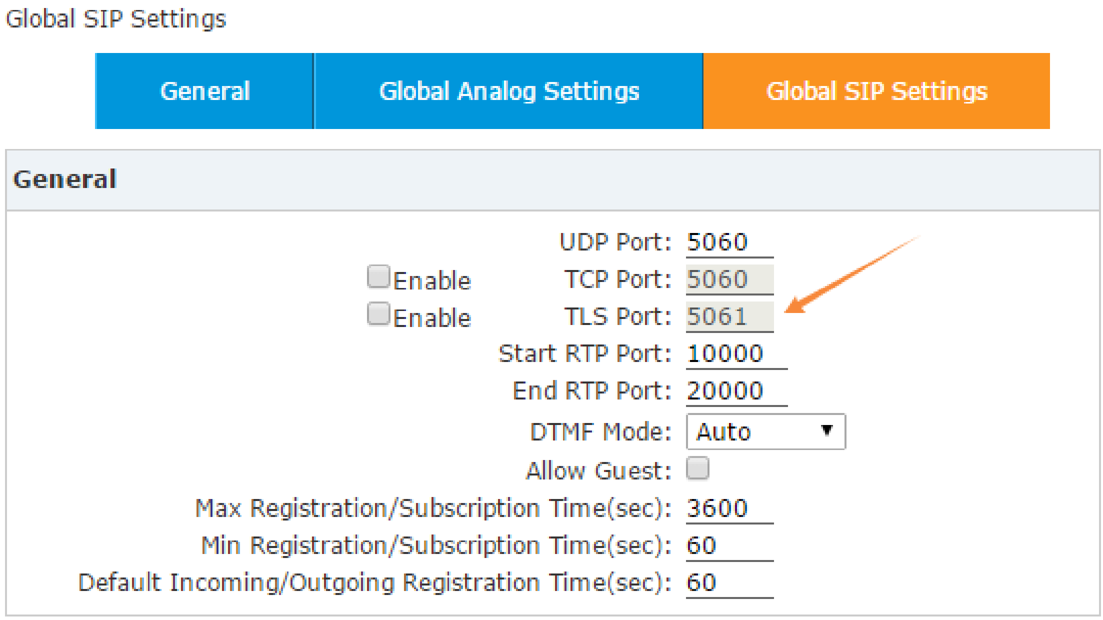
Video Call: □ □H.261 □H.263 □H.263+ □H.264

Figure 2_6

- **TLS Registry**

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide communication security over the Internet. They use asymmetric cryptography for authentication of key exchange, symmetric encryption for confidentiality and message authentication codes for message integrity. Several versions of the protocols are in widespread use in applications such as web browsing, electronic mail, Internet faxing, instant messaging and VoIP. TLS is supported in ZYCOO PBX for security SIP registry; you can also register SIP trunks to VoIP providers via TLS.

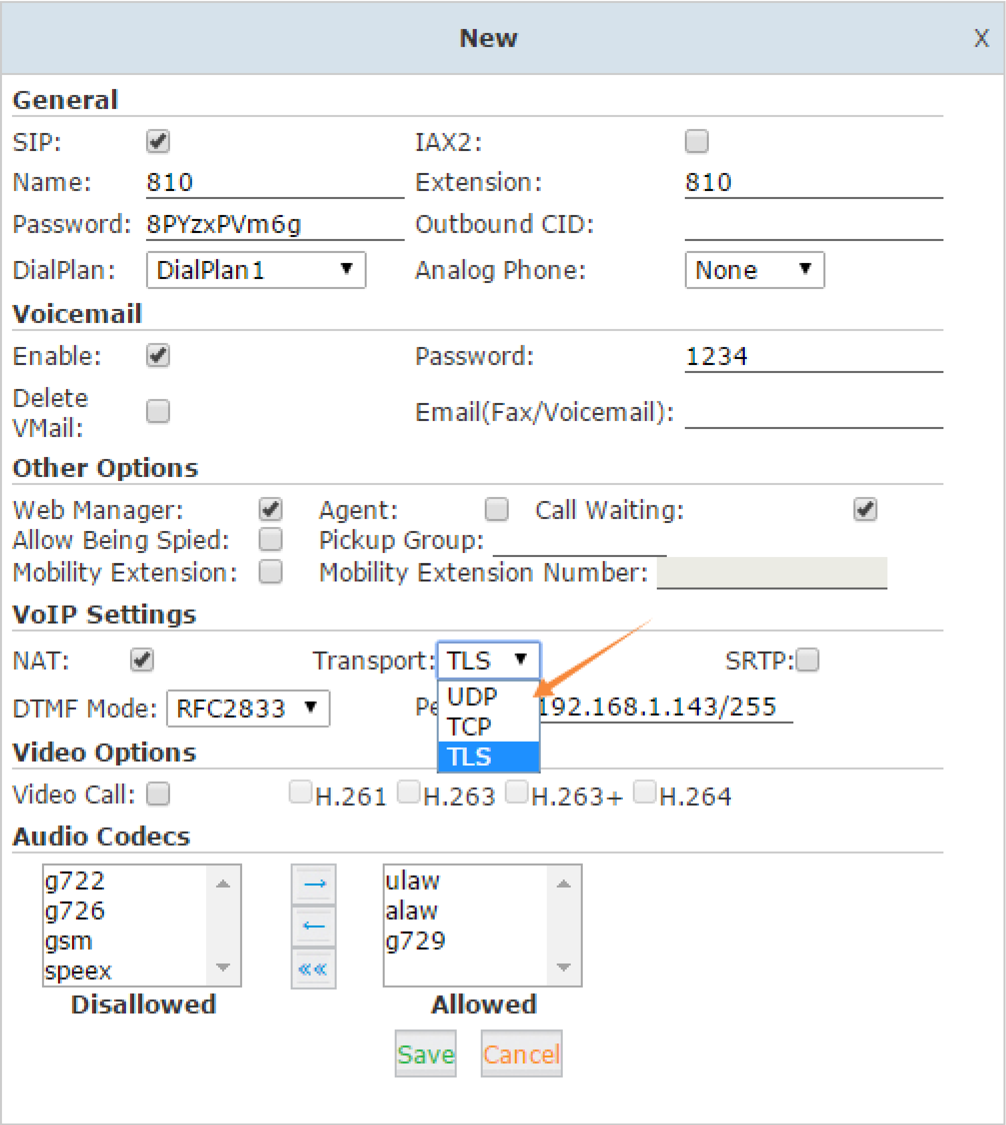
Step 1 Enable TLS port in 【Advanced】→【Options】→【Global SIP Settings】, also the port number is changeable (the default port is 5061).



UDP Port: 5060
□Enable TCP Port: 5060
□Enable TLS Port: 5061
Start RTP Port: 10000
End RTP Port: 20000
DTMF Mode: Auto
Allow Guest: □
Max Registration/Subscription Time(sec): 3600
Min Registration/Subscription Time(sec): 60
Default Incoming/Outgoing Registration Time(sec): 60

Figure 2_7

Step 2 Create or edit the 'Extensions' option to change 'Transport' to TLS.



New

General

SIP: ☑ IAX2: □

Name: 810 Extension: 810

Password: 8PYzxPVm6g Outbound CID:

DialPlan: DialPlan1 Analog Phone: None

Voicemail

Enable: ☑ Password: 1234

Delete VMail: □ Email(Fax/Voicemail):

Other Options

Web Manager: ☑ Agent: □ Call Waiting: ☑

Allow Being Spied: □ Pickup Group:

Mobility Extension: □ Mobility Extension Number:

VoIP Settings

NAT: ☑ Transport: TLS SRTP: □

UDP
TCP
TLS

DTMF Mode: RFC2833 Pe 192.168.1.143/255

Video Options

Video Call: □ □H.261 □H.263 □H.263+ □H.264

Audio Codecs

Disallowed: g722, g726, gsm, speex

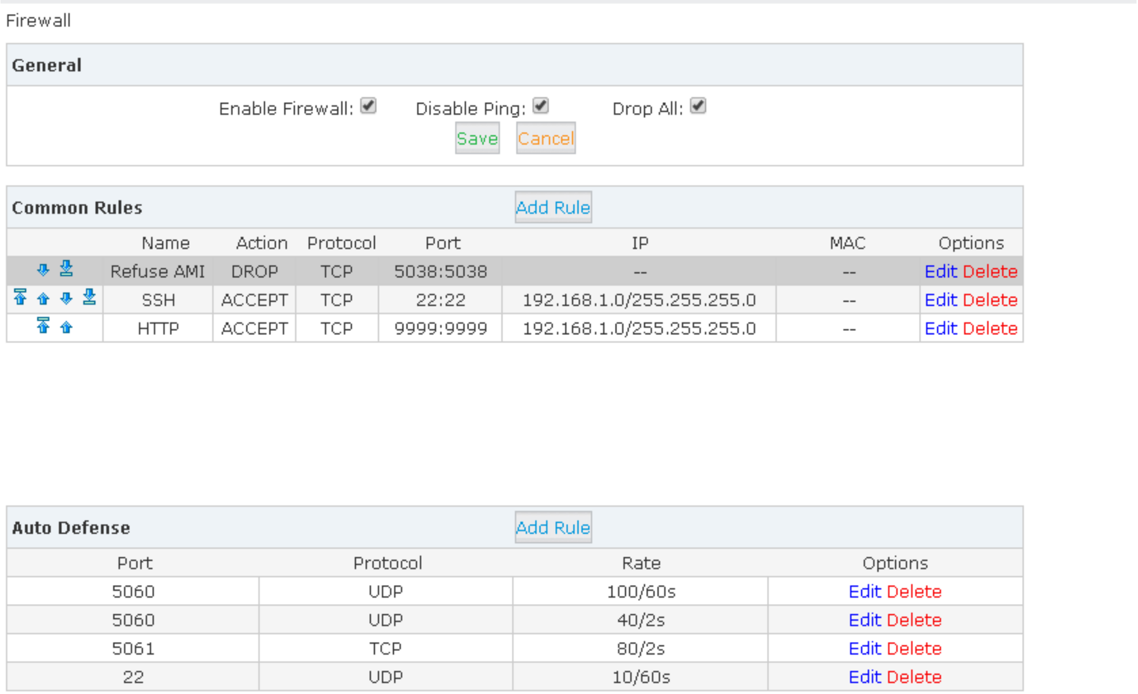
Allowed: ulaw, alaw, g729

Figure 2_8

Step 3 Register it on your phone, no need to download the TLS certificate from ZYCOO IP PBX.

3.3 Firewall configuration

Firewall is based on the iptables, it is a powerful tool and you can set it on the GUI directly as the following picture:



Firewall

General

Enable Firewall: ☑ Disable Ping: ☑ Drop All: ☑

Common Rules

	Name	Action	Protocol	Port	IP	MAC	Options
↓ ⤓	Refuse AMI	DROP	TCP	5038:5038	--	--	Edit Delete
⤒ ↑ ↓ ⤓	SSH	ACCEPT	TCP	22:22	192.168.1.0/255.255.255.0	--	Edit Delete
⤒ ↑	HTTP	ACCEPT	TCP	9999:9999	192.168.1.0/255.255.255.0	--	Edit Delete

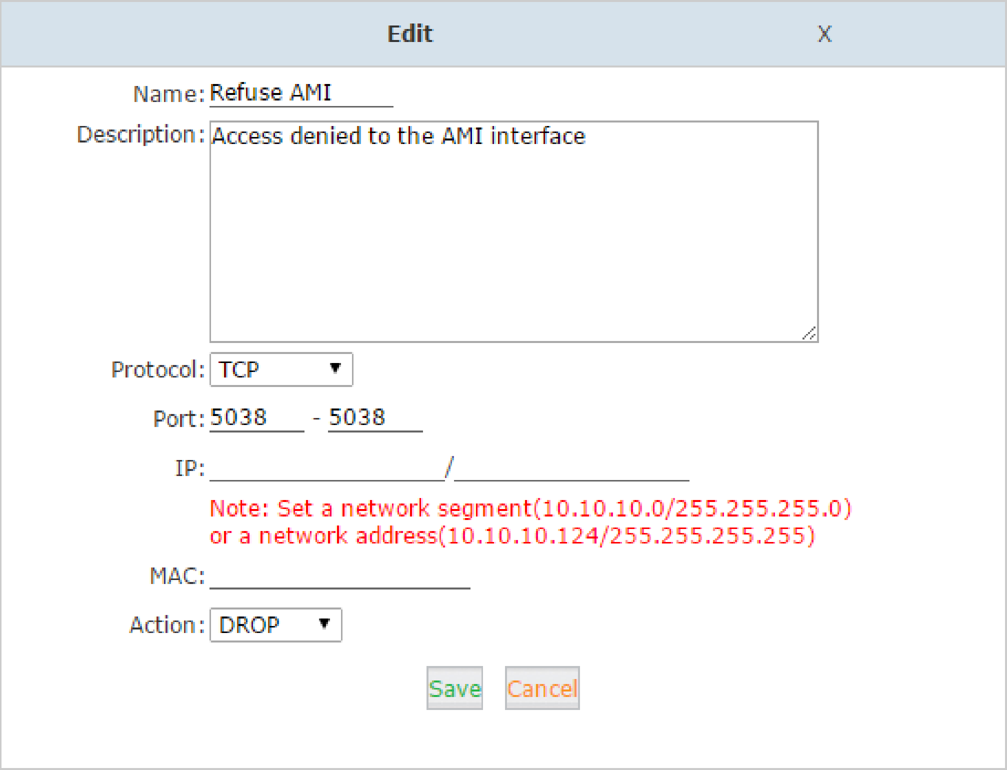
Auto Defense

Port	Protocol	Rate	Options
5060	UDP	100/60s	Edit Delete
5060	UDP	40/2s	Edit Delete
5061	TCP	80/2s	Edit Delete
22	UDP	10/60s	Edit Delete

Reference:

Item	Explanation
Enable Firewall	Enable to use firewall function
Disable Ping	deny to ping the IPPBX IP
Drop All	deny all to access except the “Accept” in the “Action” of Common Rule” list
Refuse AMI	deny all IP to access AMI interface to protect port 5038

Refuse AMI



Edit

Name: Refuse AMI

Description: Access denied to the AMI interface

Protocol: TCP

Port: 5038 - 5038

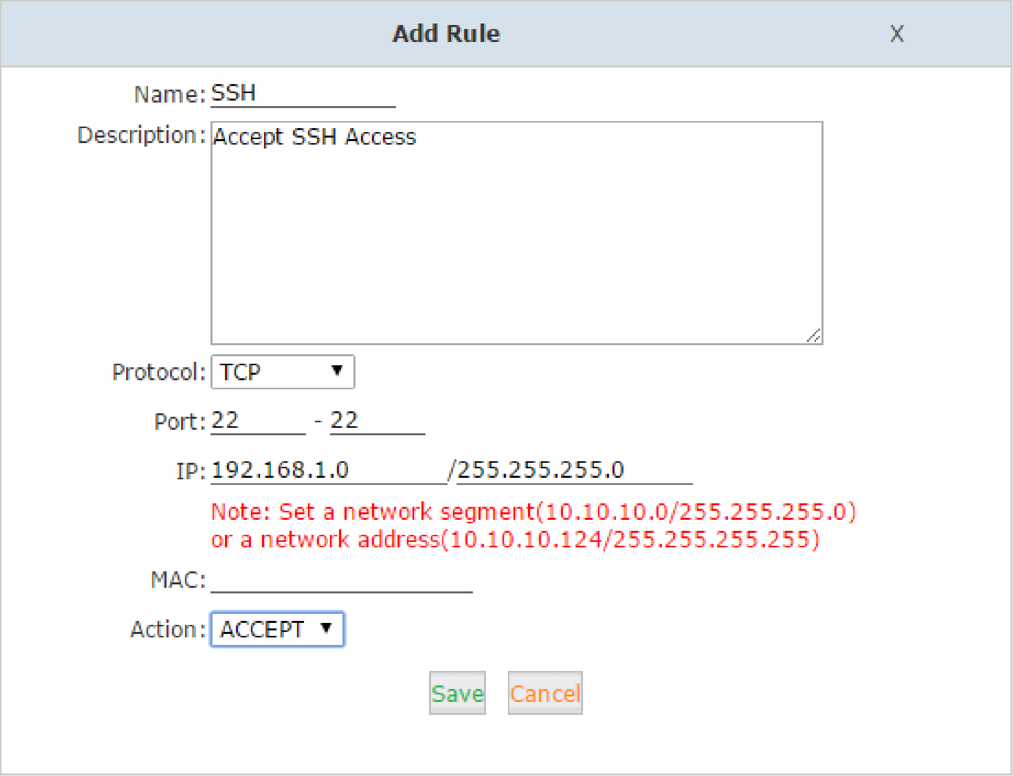
IP: /

Note: Set a network segment(10.10.10.0/255.255.255.0)
or a network address(10.10.10.124/255.255.255.255)

MAC:

Action: DROP

- **SSH**: allow IP with 192.168.1.0 segment to access the SSH



Add Rule

Name: SSH

Description: Accept SSH Access

Protocol: TCP

Port: 22 - 22

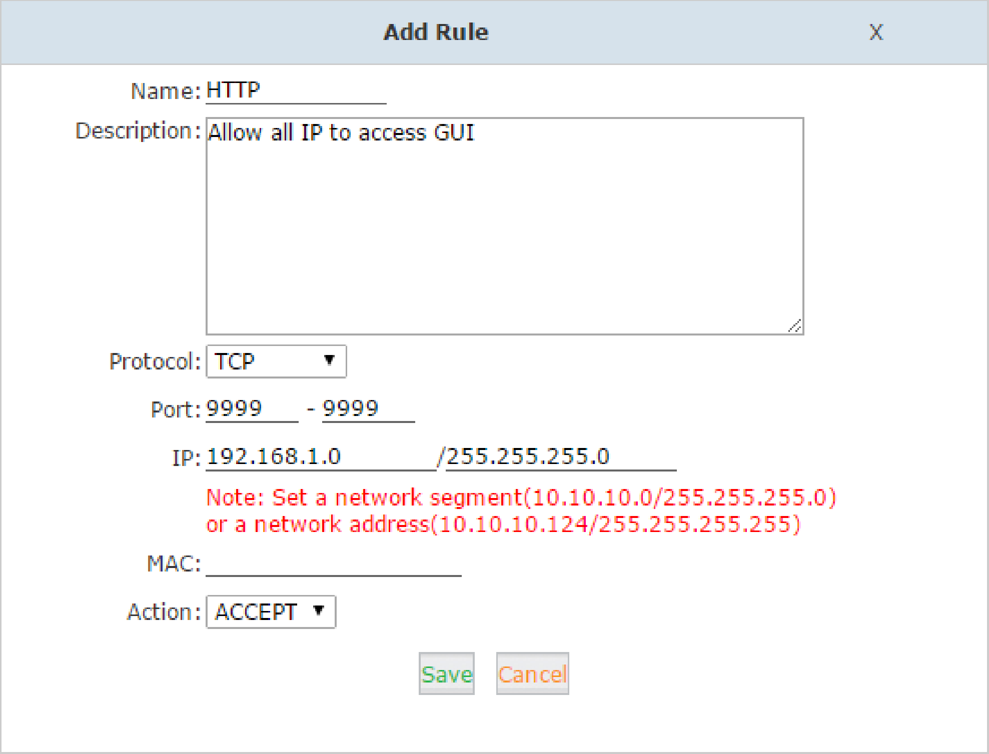
IP: 192.168.1.0 /255.255.255.0

Note: Set a network segment(10.10.10.0/255.255.255.0)
or a network address(10.10.10.124/255.255.255.255)

MAC:

Action: ACCEPT

- **HTTP**: allow IP with 192.168.1.0 segment to access the HTTP



Name: HTTP

Description: Allow all IP to access GUI

Protocol: TCP

Port: 9999 - 9999

IP: 192.168.1.0 /255.255.255.0

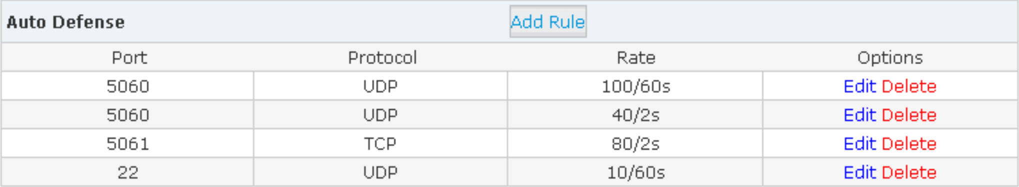
Note: Set a network segment(10.10.10.0/255.255.255.0) or a network address(10.10.10.124/255.255.255.255)

MAC:

Action: ACCEPT

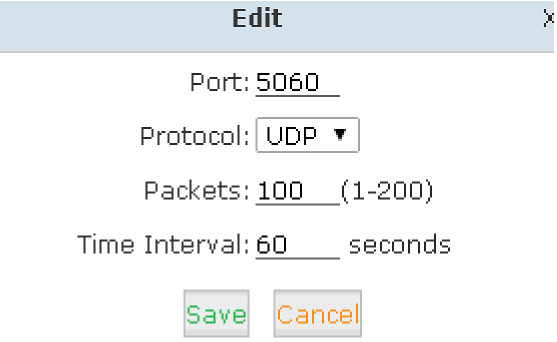
Auto Defense

Allow register packets to be received in a specific time for different port.



Port	Protocol	Rate	Options
5060	UDP	100/60s	Edit Delete
5060	UDP	40/2s	Edit Delete
5061	TCP	80/2s	Edit Delete
22	UDP	10/60s	Edit Delete

5060: system can receive 100 sip register packets every minute



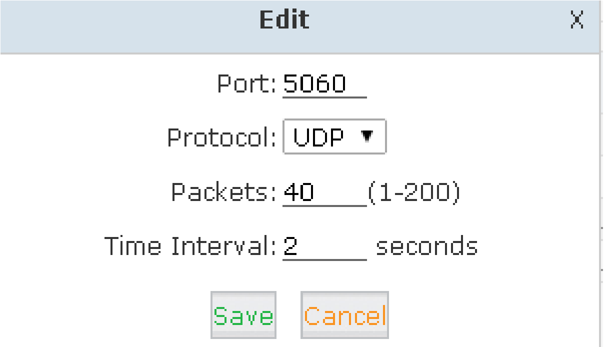
Port: 5060

Protocol: UDP

Packets: 100 (1-200)

Time Interval: 60 seconds

5060: system can receive 40 register packets every 2s



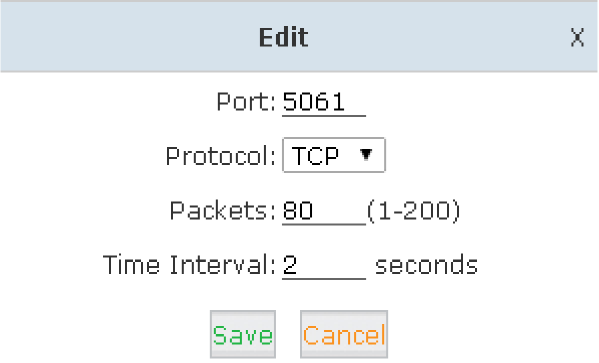
Port: 5060

Protocol: UDP ▼

Packets: 40 (1-200)

Time Interval: 2 seconds

5061: system can receive 80 register packets every 2s



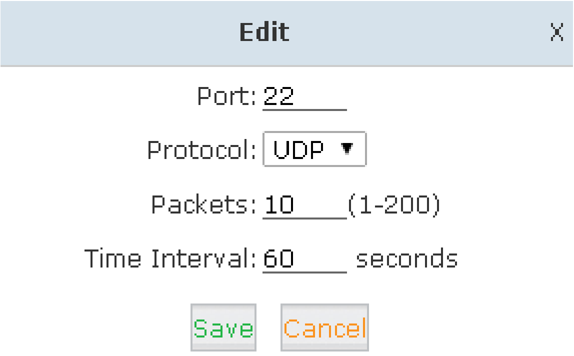
Port: 5061

Protocol: TCP ▼

Packets: 80 (1-200)

Time Interval: 2 seconds

22: system can receive 10 packets every minute



Port: 22

Protocol: UDP ▼

Packets: 10 (1-200)

Time Interval: 60 seconds

4. International Call Limit

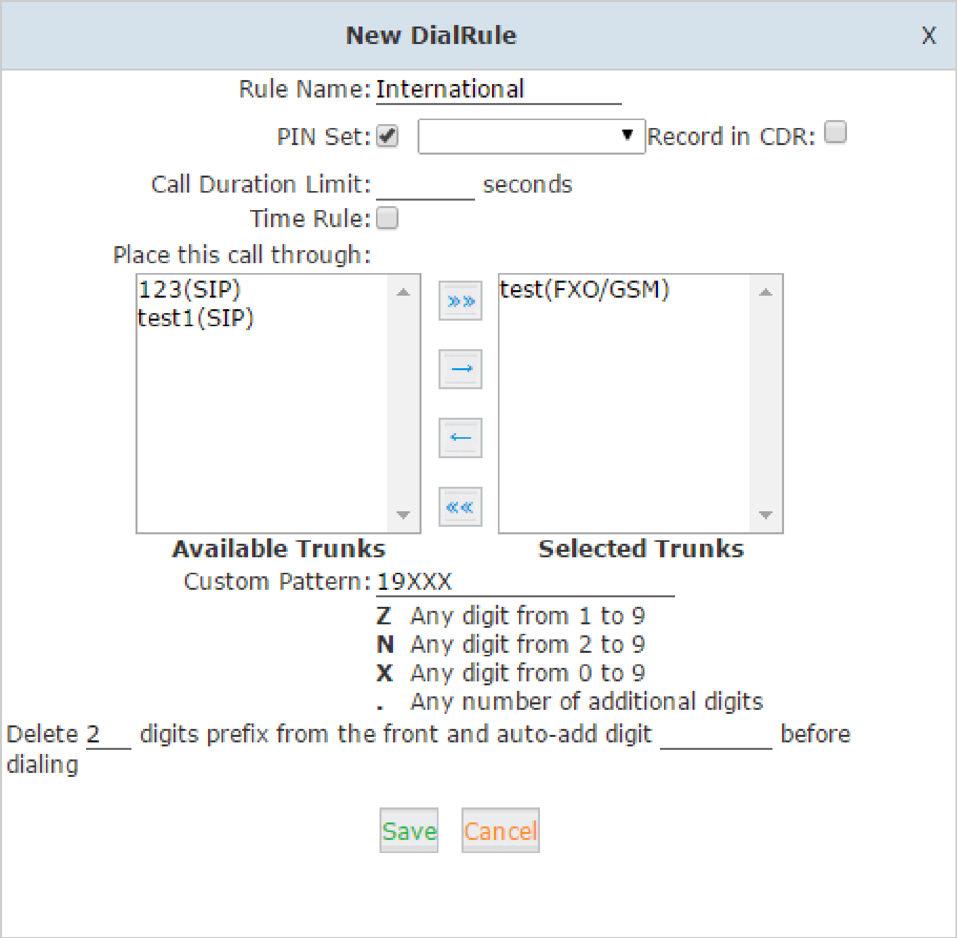
4.1 Limit Call Credit at Provider Side

We can ask VoIP/PSTN/ISDN provider for help to limit the credit of international calls in advance, then the hacker cannot dial international calls. Each provider has its own policy. You can also ask the provider to disable international call if not needed.

4.2 Set PIN or add Prefix for International call

For preventing toll fraud, it has two methods:
1) set PIN for this trunk;
2) add 2 complex digits prefix for this dial rule.

【Basic】→【Outbound Routes】→【DialRules】:



New DialRule

Rule Name: International

PIN Set: ☑ Record in CDR: □

Call Duration Limit: seconds

Time Rule: □

Place this call through:

Available Trunks: 123(SIP), test1(SIP)

Selected Trunks: test(FXO/GSM)

Custom Pattern: 19XXX

Z Any digit from 1 to 9
N Any digit from 2 to 9
X Any digit from 0 to 9
. Any number of additional digits

Delete 2 digits prefix from the front and auto-add digit before dialing

Figure 3_1

5. Appendix

All application port will be probably used in IPPBX

Port	Protocol	Usage
5060	UDP/TCP	SIP
5061	TCP	SIP
514	TCP	System log
22	TCP	SSH
21	TCP	FTP
9999	TCP	HTTP
69	UDP	TFTP
123	UDP	NTP Server
4569	UDP	IAX2
4520	UDP	DUNDI
5038	UDP	AMI
10000-20000	UDP	RTP

<The End>