mPBX Security Configuration Guide

Version: V1.4

Date: March 25th, 2013

Yeastar Technology Co., Ltd.

Contents

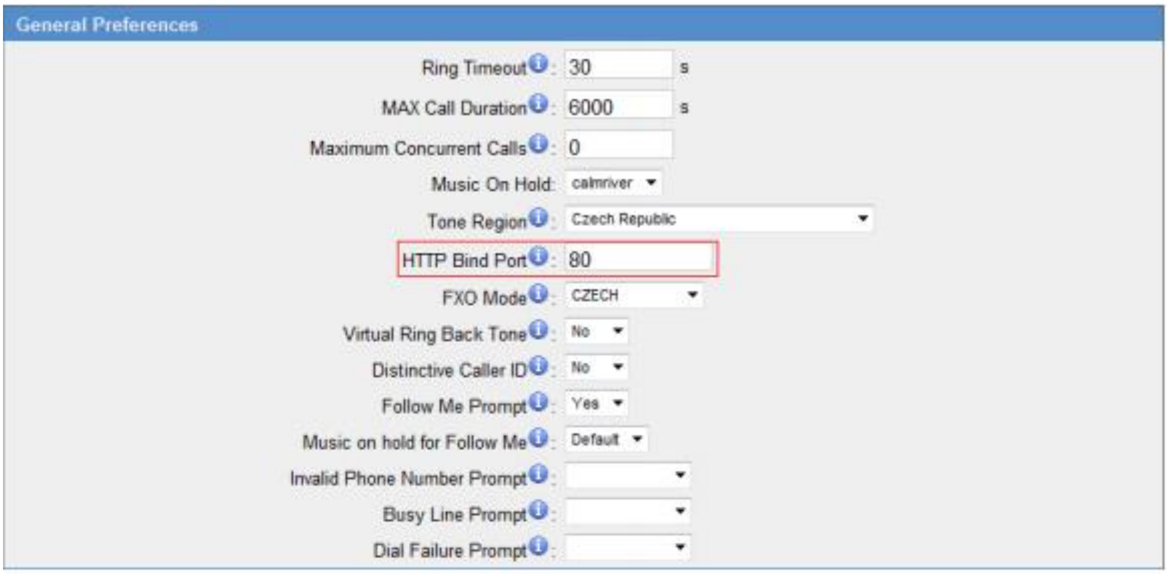
VoIP attacks, although it is not an everyday occurrence, it does exist. While using VoIP, system security is undoubtedly one of the issues we care about most. But with the appropriate configuration, and some basic safety habits, we can improve the security of the telephone system. Moreover, the powerful built-in firewall function in mPBX is adequate to enable the system to run safely and stably .

This guide will introduce the highest defense level in mPBX, and we strongly recommend that you configure firewall and other security options according to this guide, to prevent the attack fraud and the system failure or calls loss. Note: In this guide, the configuration options marked with '*' only exist in 2.17.XX.XX and above versions, namely, 3.2 guest calls option, 3.3 remote registered option, and 5 alarm settings.

1. Security Configuration for Web GUI

1.1. Change the default access port for HTTP on Options page

Select Internal Settings -> Options -> General Preferences -> HTTP Bind Port



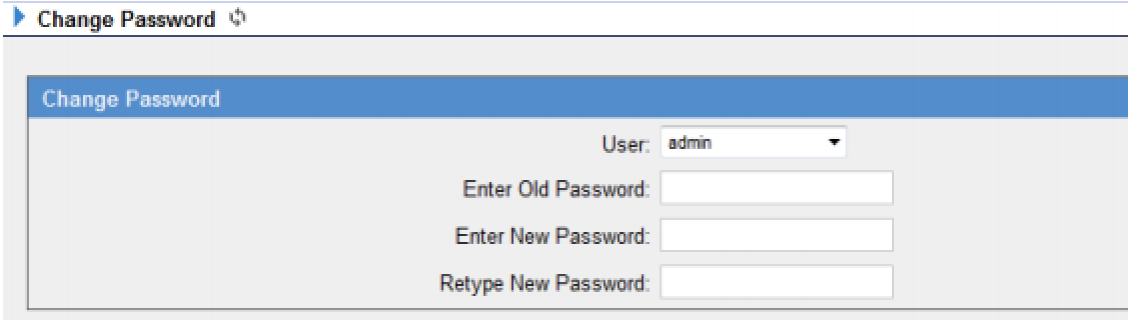
General Preferences

Ring Timeout:	30	s
MAX Call Duration:	6000	s
Maximum Concurrent Calls:	0	
Music On Hold:	calmriver	
Tone Region:	Czech Republic	
HTTP Bind Port:	80	
FXO Mode:	CZECH	
Virtual Ring Back Tone:	No	
Distinctive Caller ID:	No	
Follow Me Prompt:	Yes	
Music on hold for Follow Me:	Default	
Invalid Phone Number Prompt:		
Busy Line Prompt:		
Dial Failure Prompt:		

Figure 1-1

1.2. Change the default password for the web GUI

Select System Settings -> Change Password



Change Password

Change Password

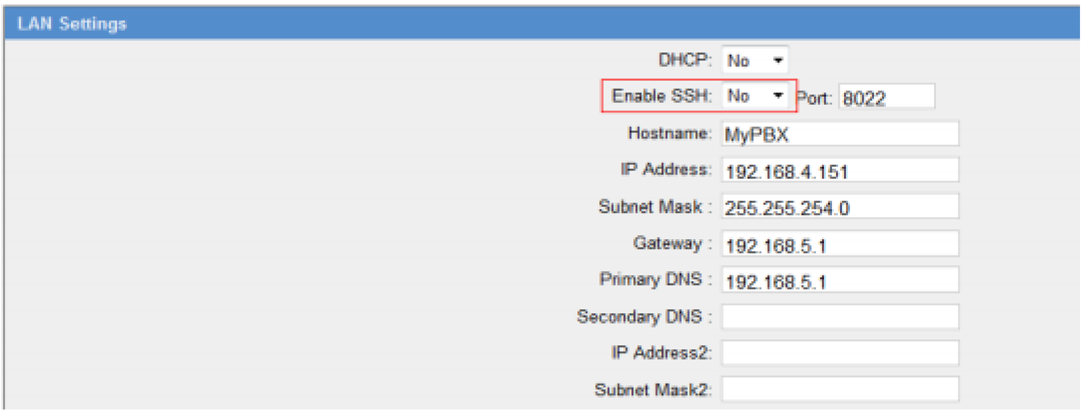
User:	admin
Enter Old Password:	
Enter New Password:	
Retype New Password:	

Figure1-2

2. Disable SSH on LAN Settings Page

2.1. Disable SSH

Select LAN Settings -> Enable SSH. If external debugging isn't required, please select "No" .



LAN Settings

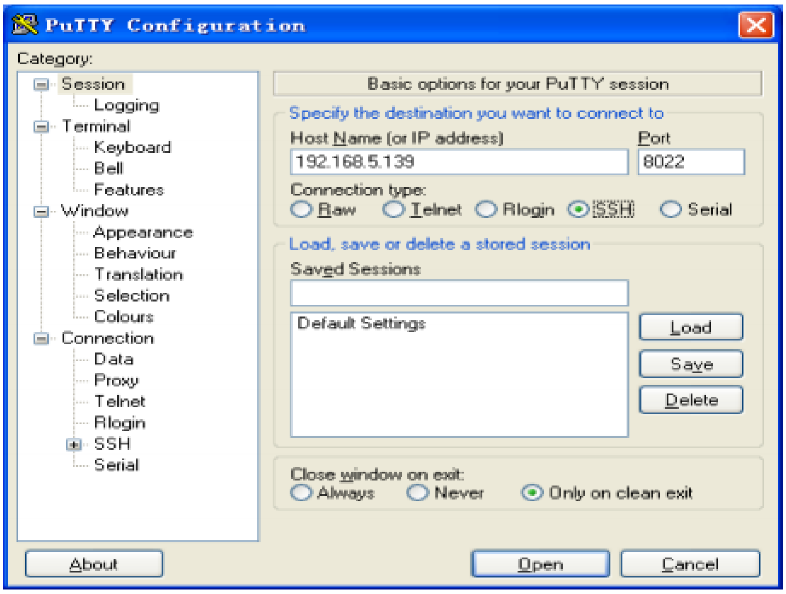
DHCP:	No
Enable SSH:	No Port: 8022
Hostname:	MyPBX
IP Address:	192.168.4.151
Subnet Mask :	255.255.254.0
Gateway :	192.168.5.1
Primary DNS :	192.168.5.1
Secondary DNS :	
IP Address2:	
Subnet Mask2:	

Figure 2-1

2.2. Change the default password for SSH

We can use the Linux command passwd to change root password of mPBX.

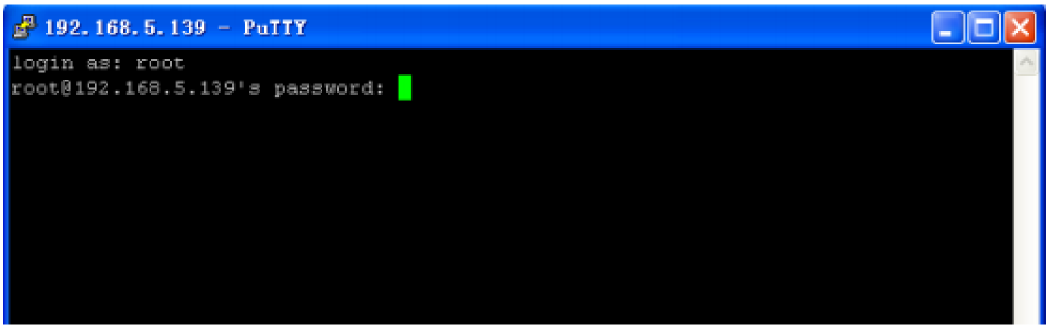
1. Login via putty.exe



Host Name (or IP address): 192.168.5.139
Port: 8022
Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial
Close window on exit: ○ Always ○ Never ● Only on clean exit

Figure 2-2

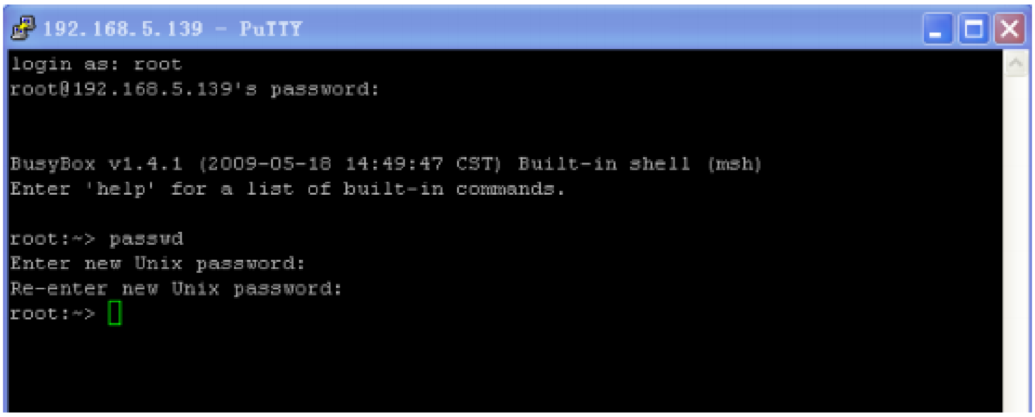
2. The default username is root and the default password is ys123456.



```
login as: root
root@192.168.5.139's password:
```

Figure 2-3

3. Step 2 use command passwd to change the root ’ s password



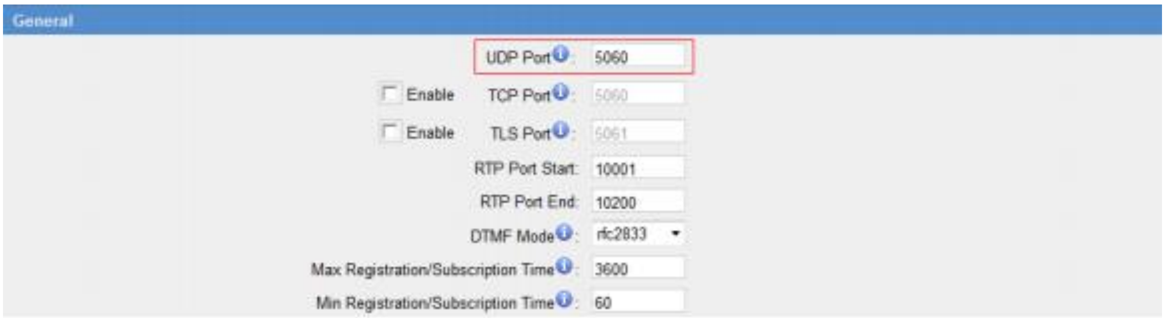
```
login as: root
root@192.168.5.139's password:


BusyBox v1.4.1 (2009-05-18 14:49:47 CST) Built-in shell (msh)
Enter 'help' for a list of built-in commands.

root:~> passwd
Enter new Unix password:
Re-enter new Unix password:
root:~>
```

Figure 2-4

3. Security Configuration for Extensions

3.1. Change the default SIP Port

Select SIP settings -> General -> UDP Port



General

UDP Port: 5060

□ Enable TCP Port: 5060

□ Enable TLS Port: 5061

RTP Port Start: 10001

RTP Port End: 10200

DTMF Mode: rfc2833

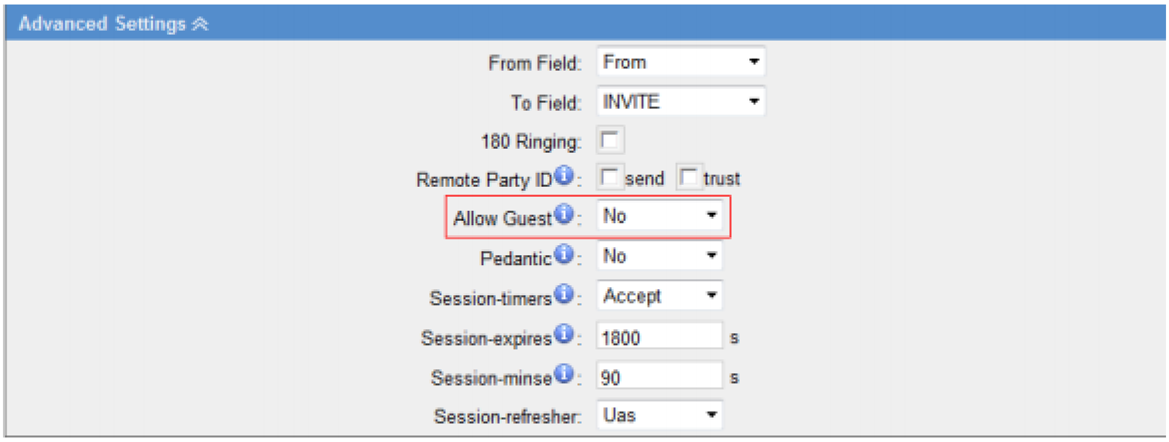
Max Registration/Subscription Time: 3600

Min Registration/Subscription Time: 60

Figure 3-1

3.2. Disable guest calls

Select SIP settings -> Advanced Settings -> Allow Guest



Advanced Settings

From Field: From

To Field: INVITE

180 Ringing: □

Remote Party ID: □ send □ trust

Allow Guest: No

Pedantic: No

Session-timers: Accept

Session-expires: 1800 s

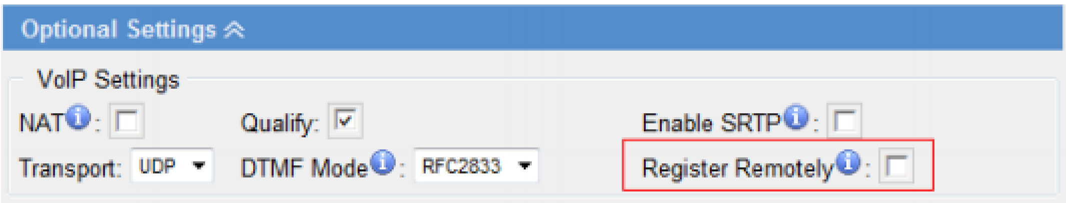
Session-minse: 90 s

Session-refresher: Uas

Figure 3-2

3.3. Security Configuration for remote extensions

If remote registration isn't required, please disable it.



Optional Settings

VoIP Settings

NAT: □

Qualify: ☑

Enable SRTP: □

Transport: UDP

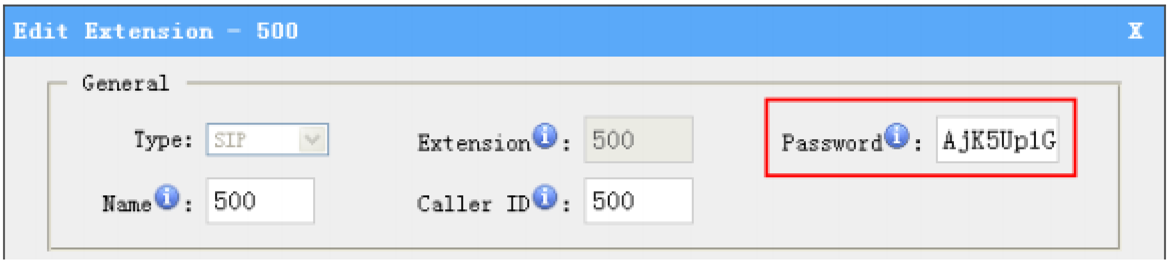
DTMF Mode: RFC2833

Register Remotely: □

Figure 3-3

3.4. Set an enhanced password and enable IP restriction for extensions

1) Set a new extension password at the higher security level, e.g. AjK5Up1G.



Edit Extension - 500

General

Type: SIP

Extension: 500

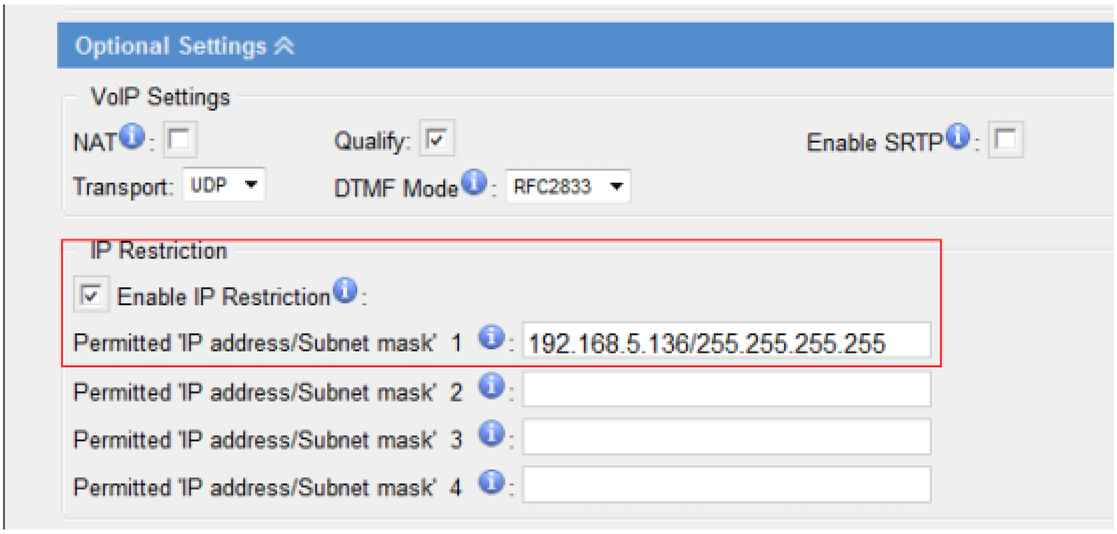
Password: AjK5Up1G

Name: 500

Caller ID: 500

Figure 3-4

2) Enable IP restriction and enter the permitted "IP address/Subnet mask", e.g. 192.168.5.136.



Optional Settings

VoIP Settings

NAT: □ Qualify: ☑ Enable SRTP: □

Transport: UDP DTMF Mode: RFC2833

IP Restriction

☑ Enable IP Restriction:

Permitted 'IP address/Subnet mask' 1: 192.168.5.136/255.255.255.255

Permitted 'IP address/Subnet mask' 2:

Permitted 'IP address/Subnet mask' 3:

Permitted 'IP address/Subnet mask' 4:

Figure 3-5

4. Set up Proper Firewall Rules

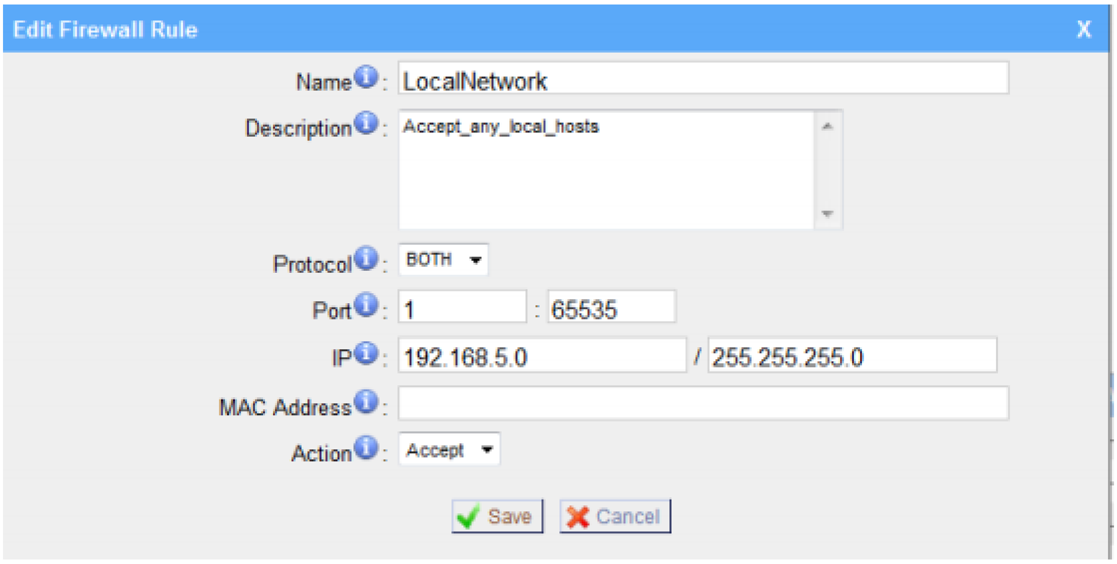
Note: Please backup the configurations on backup and restore page before you go ahead. In the case that you lock the device, you can reset to factory default and restore the previous configurations. Below example rules works with mPBX firmware version 2.15.xx.xx or higher versions.

Step 1. Enable firewall on firewall page of mPBX.

Step 2. Add a common rule to accept local network access.

Create a common rule to allow the all the IP addresses of the local phones to access mPBX server . For example, if the IP addresses of the local network are 192.168.5.1-254, the configurations could be as below:

Name: LocalNetwork
Protocol: BOTH
Port: 1:65535
IP: 192.168.5.0/255.255.255.0
Action: Accept



Edit Firewall Rule

Name: LocalNetwork
Description: Accept_any_local_hosts
Protocol: BOTH
Port: 1 : 65535
IP: 192.168.5.0 / 255.255.255.0
MAC Address:
Action: Accept

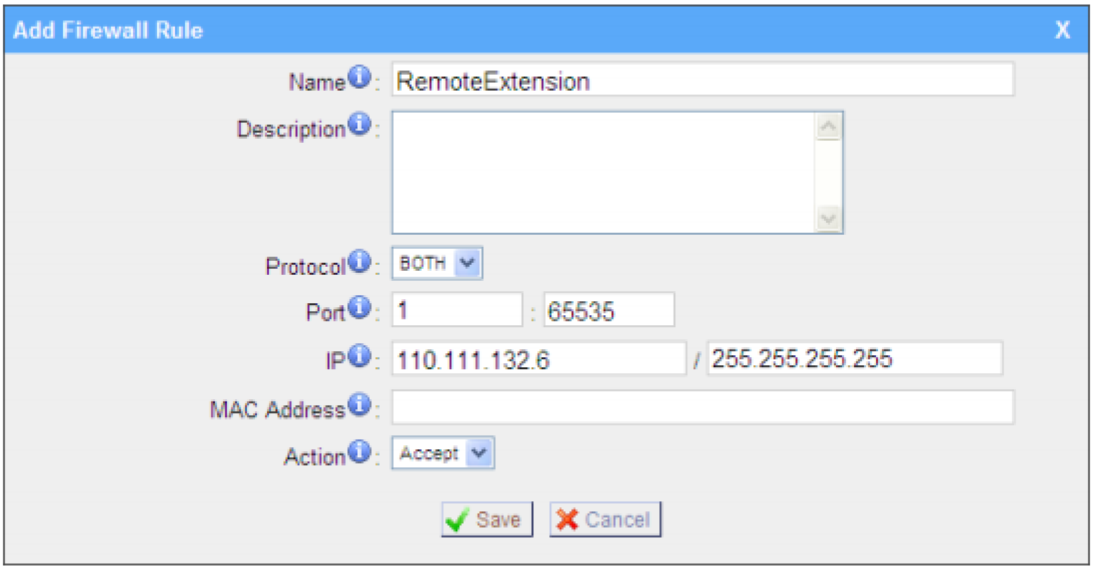
Figure 4-1

Step 3. Create common rules to accept remote extensions or remote administrators, if you use SIP trunk, please accept the provider’s host as well.

Note: If there are no remote extensions, the rule is not required.

1) Set up the firewall rule to allow the public IP address of remote extensions to access mPBX server. e.g.110.111.132.6, the configurations could be as below:

Name: Remote Extension
Protocol: BOTH
Port: 1:65535
IP: 110.111.132.6/255.255.255.255
Action: Accept



Name: RemoteExtension

Description:

Protocol: BOTH

Port: 1 : 65535

IP: 110.111.132.6 / 255.255.255.255

MAC Address:

Action: Accept

Figure 4-2

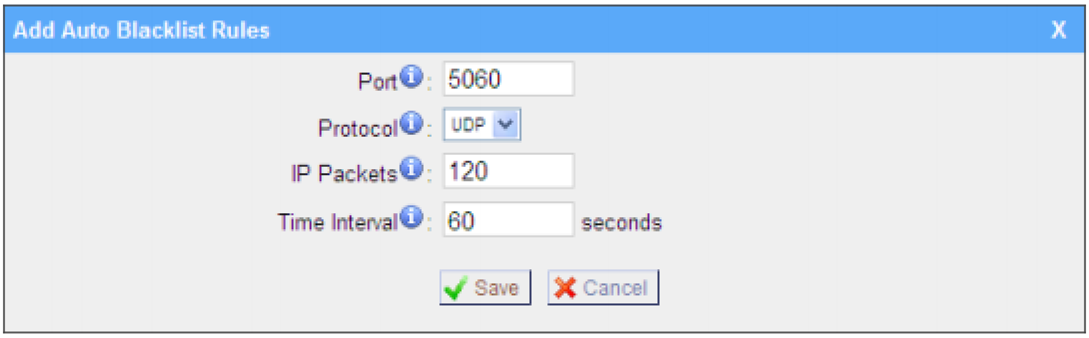
Step 4. Configure auto blacklist rules

Auto blacklist rules: the Server would add the IP address to the blacklist automatically if the number of the packets it sends exceed the rule you configured.

1) Add two auto blacklist rules for port: 5060.

Rule No.1:

Port: 5060
Protocol: UDP
IP Packets: 120
Time Interval: 60 seconds



Port: 5060

Protocol: UDP

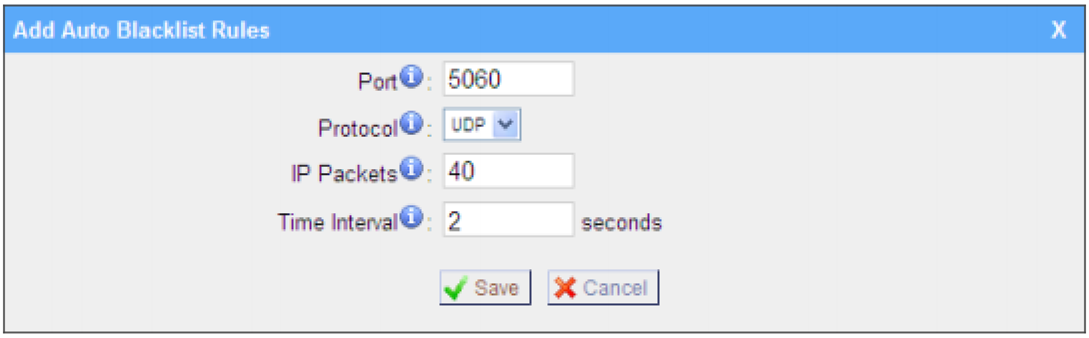
IP Packets: 120

Time Interval: 60 seconds

Figure 4-3

Rule No.2:

Port: 5060
Protocol: UDP
IP Packets: 40
Time Interval: 2 seconds



Add Auto Blacklist Rules

Port: 5060

Protocol: UDP

IP Packets: 40

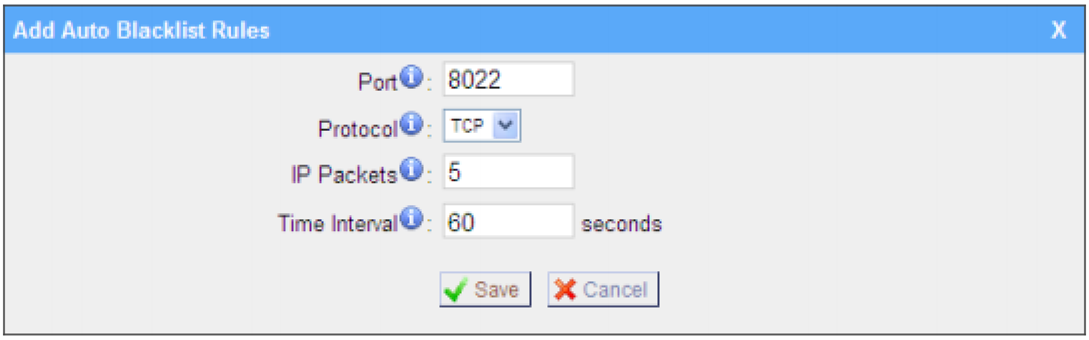
Time Interval: 2 seconds

Figure 4-4

2) Add an auto blacklist rule for Port:8022

Rule No.3

Port: 8022
Protocol: TCP
IP Packets: 5
Time Interval: 60 seconds



Add Auto Blacklist Rules

Port: 8022

Protocol: TCP

IP Packets: 5

Time Interval: 60 seconds

Figure 4-5

Step 5. Add a Firewall Rule for VoIP trunk registration

Note: If there is no VoIP trunk, this rule is not required. And if the RTP IP address of VoIP trunk and Registration IP address of the VoIP trunk are different, we need create a rule to accept the RTP IP address too.

Add a rule to accept the IP address of the VoIP trunk to access mPBX server. For example: If the IP address of the VoIP trunk is 110.5.14.6, Protocol is UDP and Port is 5060, the configuration could be as below:

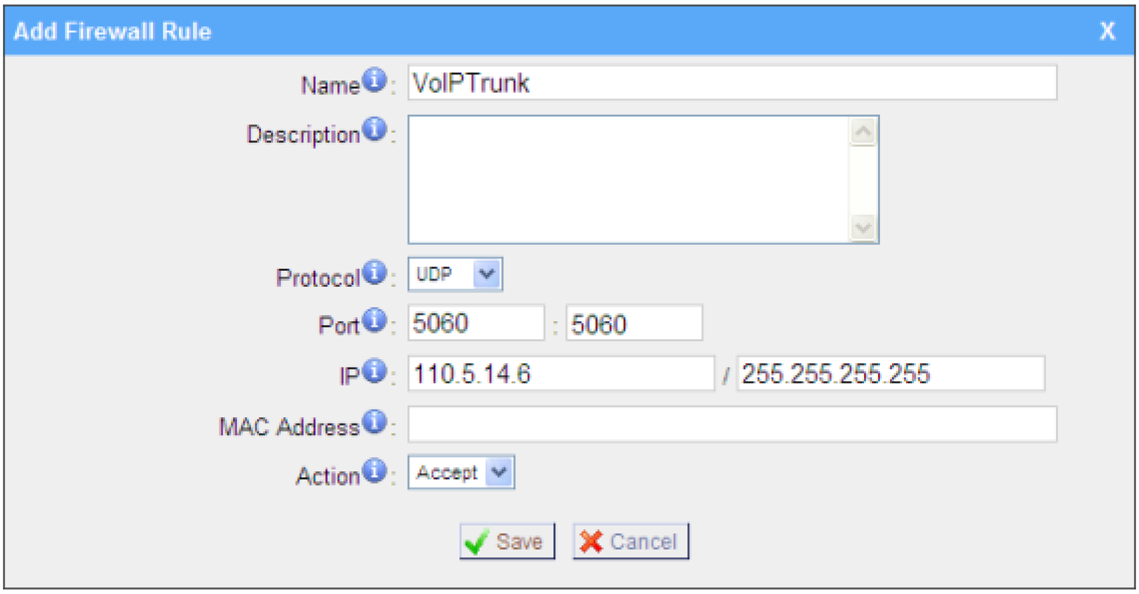
Name: VoIPTrunk

Protocol: UDP

Port: 5060: 5060

IP: 110.5.14.6/255.255.255.255

Action: Accept

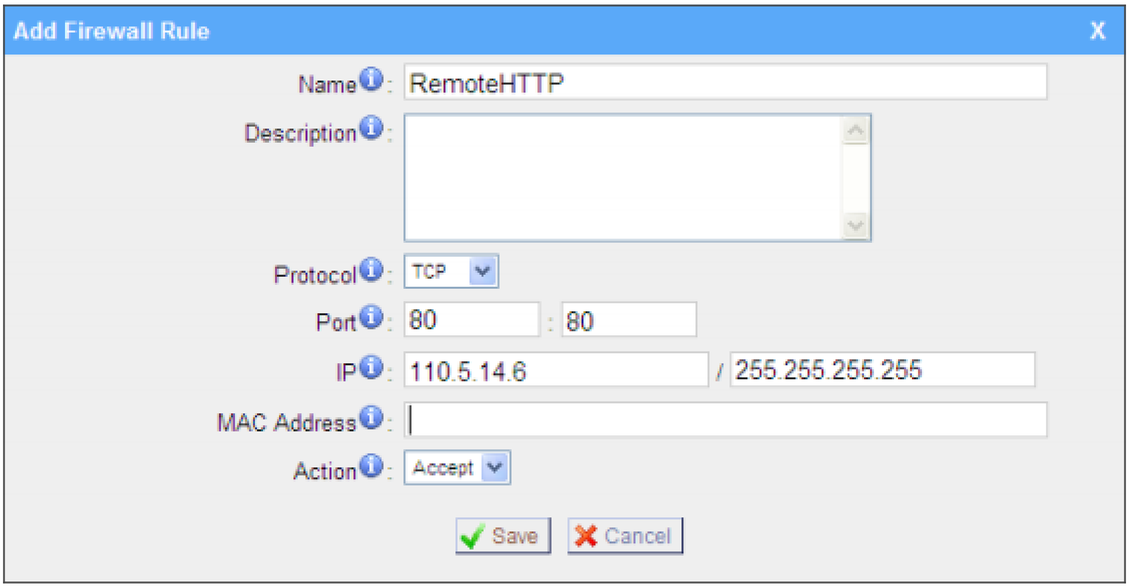


Name: VoIPTrunk
Description:
Protocol: UDP
Port: 5060 : 5060
IP: 110.5.14.6 / 255.255.255.255
MAC Address:
Action: Accept

Figure 4-6

Step 6. Add a firewall rule to accept the remote access of HTTP port. For example, if the remote access IP is 110.5.14.6, and the port is 80, the configuration could be as below .

Name: RemoteHTTP
Protocol: TCP
Port: 80:80
IP: 110.5.14.6/255.255.255.255
Action: Accept



Name: RemoteHTTP
Description:
Protocol: TCP
Port: 80 : 80
IP: 110.5.14.6 / 255.255.255.255
MAC Address:
Action: Accept

Figure 4-7

Step 7. Add a firewall rule to accept remote access of SSH port. For example: if the remote access IP is 110.5.14.6 and the port is 8022.

Note: If the remote access of SSH port is not needed, this rule is not required.

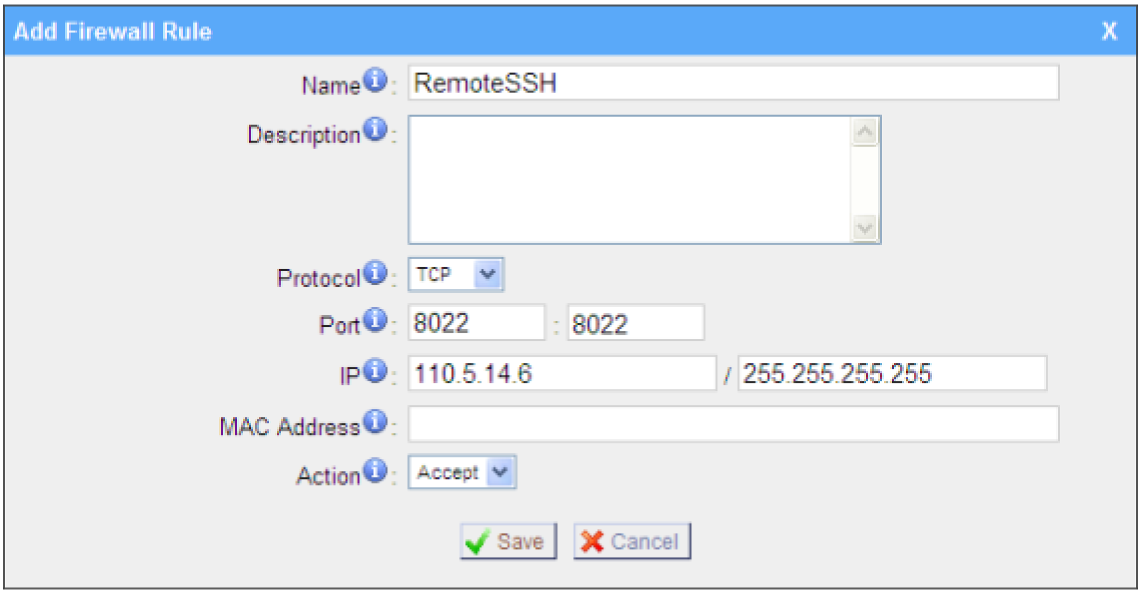
Name: RemoteSSH

Protocol: TCP

Port: 8022:8022

IP: 110.5.14.6/255.255.255.255

Action: Accept



Add Firewall Rule X

Name: RemoteSSH

Description:

Protocol: TCP

Port: 8022 : 8022

IP: 110.5.14.6 / 255.255.255.255

MAC Address:

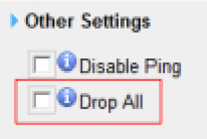
Action: Accept

Figure 4-8

Step 8. Add other firewall rules by yourself. For example, if you are using features about email, you should add the firewall rules for the SMTP server and POP3 server.

Step 9. Enable Drop all (If this feature is enabled, all the packets and connection that do not match the rules would be dropped.)

Note: Before enable this feature, please add a rule to accept the local network access, or the server might not be accessed.



Other Settings

□ Disable Ping

□ Drop All

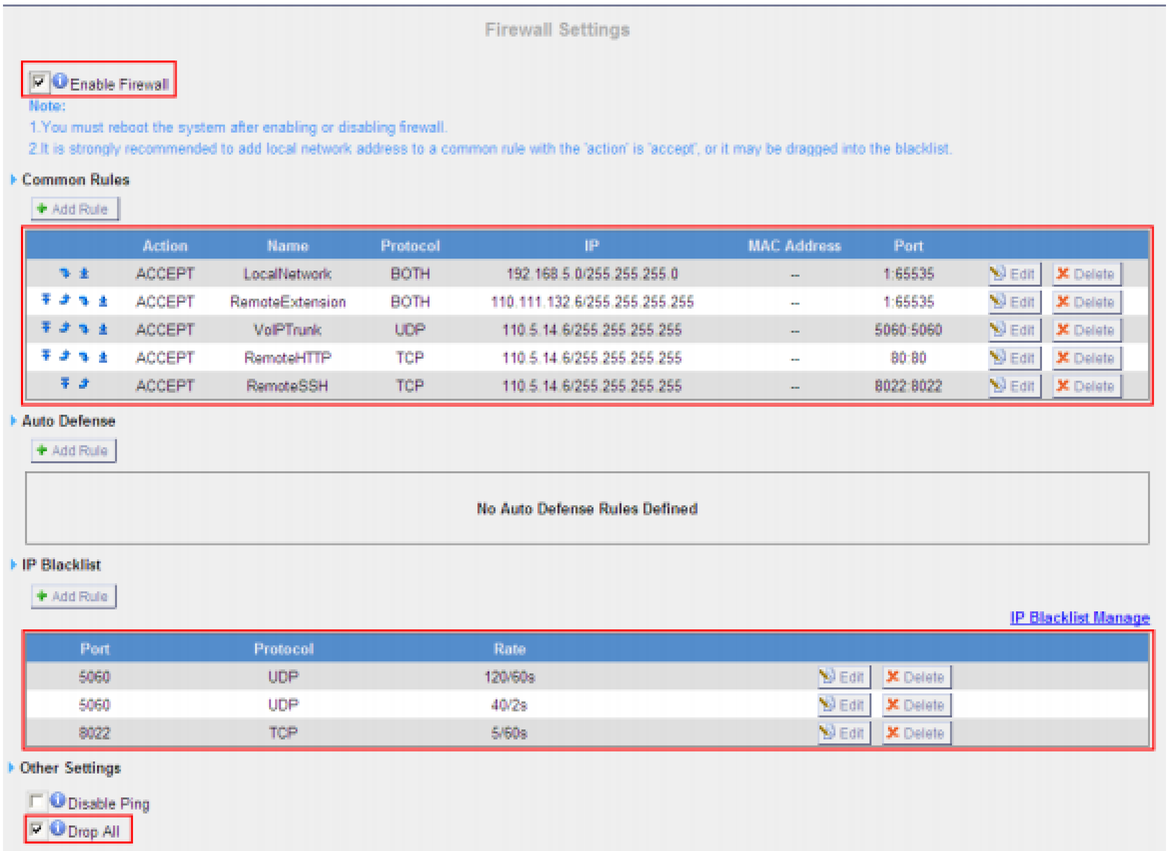
Figure 4-9

Note:

1. After enabling ‘drop all’ , the rules of auto defense and IP blacklist will not take effect. It means except the IPs and packets which are defined as the accept rules, the other connection or packets will be dropped.

2. If ‘drop all’ is not enabled, please don’t remove the IP blacklist rules in case the system security hole.

Step 10. The Configuration of firewall settings is completed. See as below figure.



Firewall Settings

☑ Enable Firewall

Note:

1.You must reboot the system after enabling or disabling firewall.

2.It is strongly recommended to add local network address to a common rule with the 'action' is 'accept', or it may be dragged into the blacklist.

Common Rules

	Action	Name	Protocol	IP	MAC Address	Port		
	ACCEPT	LocalNetwork	BOTH	192.168.5.0/255.255.255.0	--	1:65535	Edit	Delete
	ACCEPT	RemoteExtension	BOTH	110.111.132.6/255.255.255.255	--	1:65535	Edit	Delete
	ACCEPT	VoIPTrunk	UDP	110.5.14.6/255.255.255.255	--	5060:5060	Edit	Delete
	ACCEPT	RemoteHTTP	TCP	110.5.14.6/255.255.255.255	--	80:80	Edit	Delete
	ACCEPT	RemoteSSH	TCP	110.5.14.6/255.255.255.255	--	8022:8022	Edit	Delete

Auto Defense

No Auto Defense Rules Defined

IP Blacklist

Port	Protocol	Rate		
5060	UDP	120/60s	Edit	Delete
5060	UDP	40/2s	Edit	Delete
8022	TCP	5/60s	Edit	Delete

Other Settings

□ Disable Ping

☑ Drop All

Figure 4-10

5. Alert Settings

After enabling alert settings', if the device is attacked, the system will notify users the alert via call or e-mail. The attack modes include IP attack and Web Login.

5.1. IPATTACK

When the system is attacked by some IP addresses, the firewall will add the IP to auto IP mPBX Security Configuration Guide Blacklist and notify the user if it match the protection rule.

Example: Configure to notify extension 500, outbound number 5503301 and E-mail alert@yeastart.com.

Configuration could be as below.

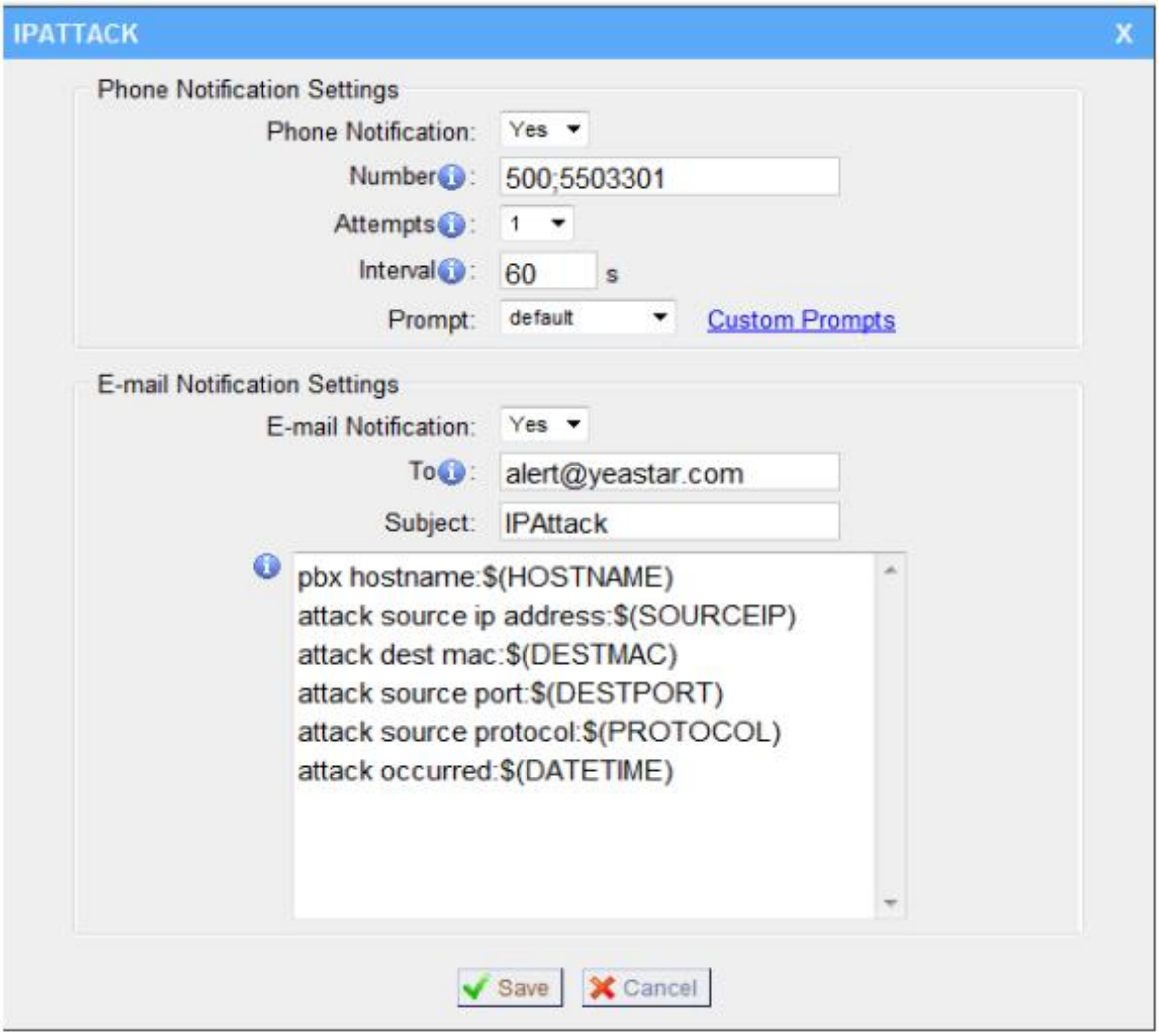
Phone Notification Settings:

Phone Notification: Yes
Number: 500;5503301
Attempts: 1
Interval: 60s
Prompt: default

Note: If there's outbound number to notify, the number should be fit with the dial pattern of outbound route.

E-mail Notification Settings:

E-mail Notification: Yes
To: alert@yeastar.com
Subject: IPAttack



Phone Notification Settings

Phone Notification: Yes
Number: 500;5503301
Attempts: 1
Interval: 60 s
Prompt: default

E-mail Notification Settings

E-mail Notification: Yes
To: alert@yeastar.com
Subject: IPAttack

```
pbx hostname:$(HOSTNAME)
attack source ip address:$(SOURCEIP)
attack dest mac:$(DESTMAC)
attack source port:$(DESTPORT)
attack source protocol:$(PROTOCOL)
attack occurred:$(DATETIME)
```

Figure 5-1

5.2. WEBLOGIN

Enter the password incorrectly five times when logging in mPBX Web interface will be deemed as attack, the system will limit the IP login within 10 minutes and notify the user.

Example: Configure to notify extension 500, outbound number 5503301 and E-mail alert@yeastar.com.

Configuration could be as below.

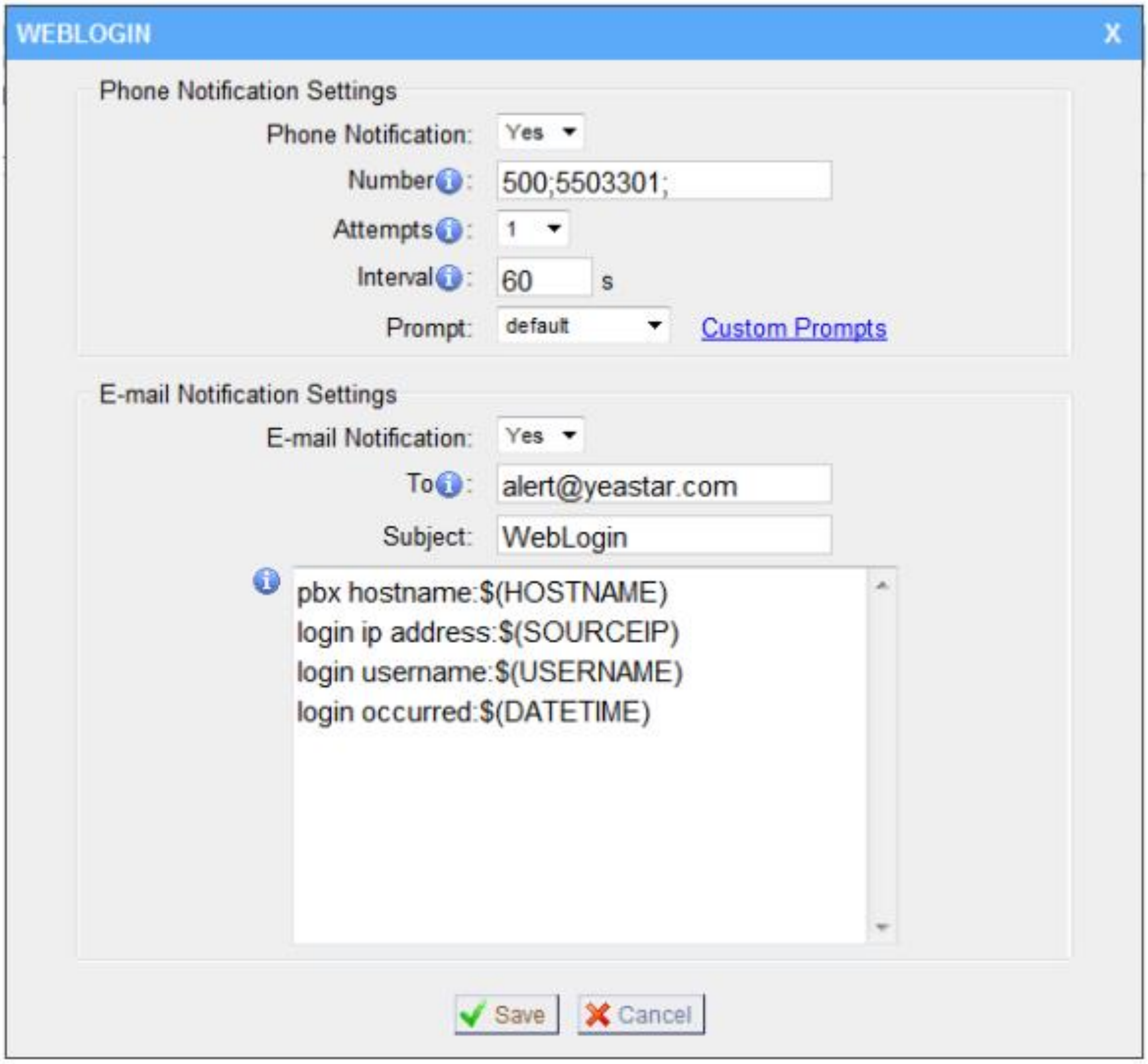
Phone Notification Settings:

Phone Notification: Yes
Number: 500;5503301
Attempts: 1
Interval: 60s
Prompt: default

Note: If there's outbound number to notify, the number should be fit with the dial pattern of outbound route.

E-mail Notification Settings:

E-mail Notification: Yes
To: alert@domainr.com
Subject: WebLogin



WEBLOGIN

Phone Notification Settings

Phone Notification: Yes
Number: 500;5503301;
Attempts: 1
Interval: 60 s
Prompt: default

E-mail Notification Settings

E-mail Notification: Yes
To: alert@yeastar.com
Subject: WebLogin

pbx hostname:$(HOSTNAME)
login ip address:$(SOURCEIP)
login username:$(USERNAME)
login occurred:$(DATETIME)

Figure 5-2

6. Note

If the phenomena of toll fraud have been happened in your mPBX system, we are really sorry about that, then please enhance the protection level of your firewall refer to the above steps.

In addition, please change the all password: Web GUI password, SSH password, and all extensions password.

<The end>