MyPBX 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 MyPBX is adequate to enable the system to run safely and stably.

This guide will introduce the highest defense level in MyPBX, 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

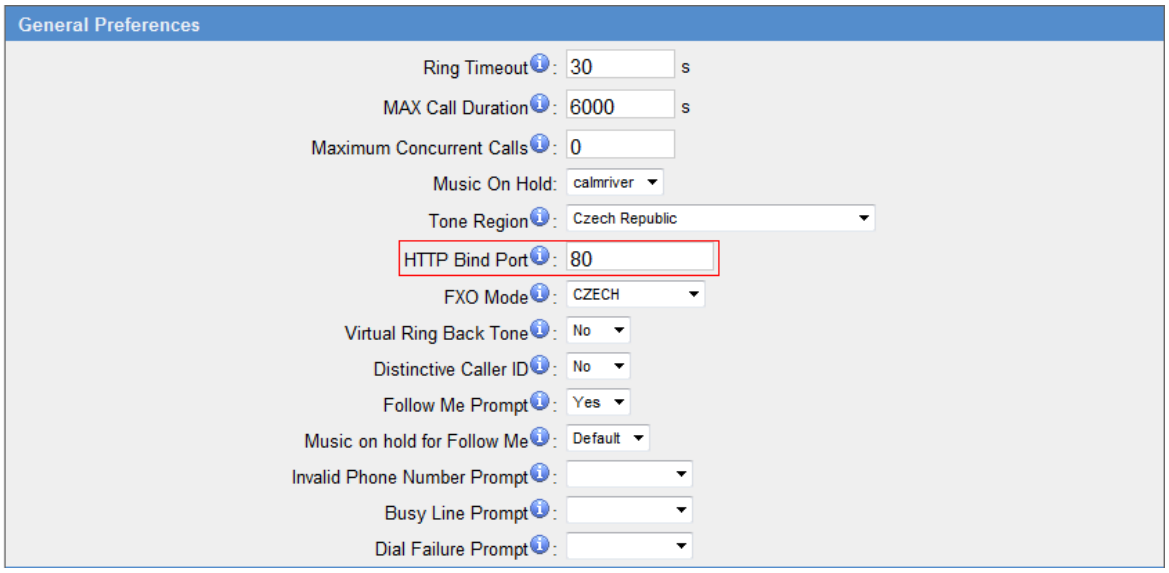

Figure 1-1

1.2 Change the default password for the web GUI

Select System Settings→Change Password

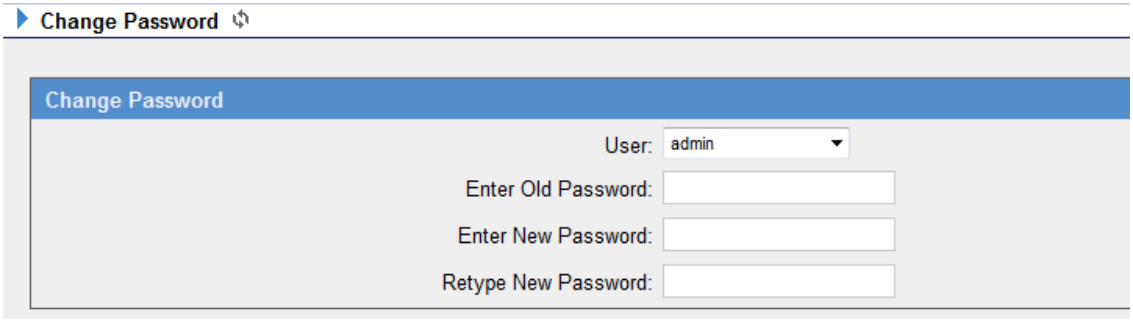

Figure1-2

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".

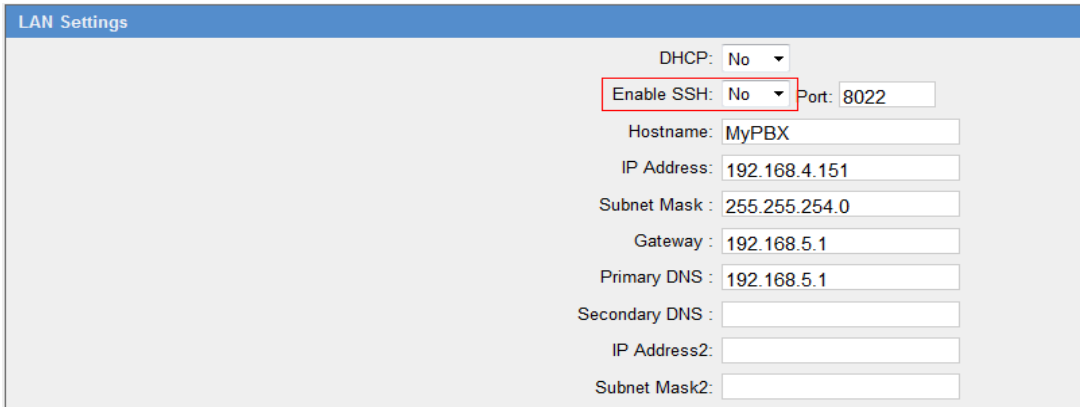

Figure 2-1

2.2 Change the default password for SSH

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

1. Login via putty.exe

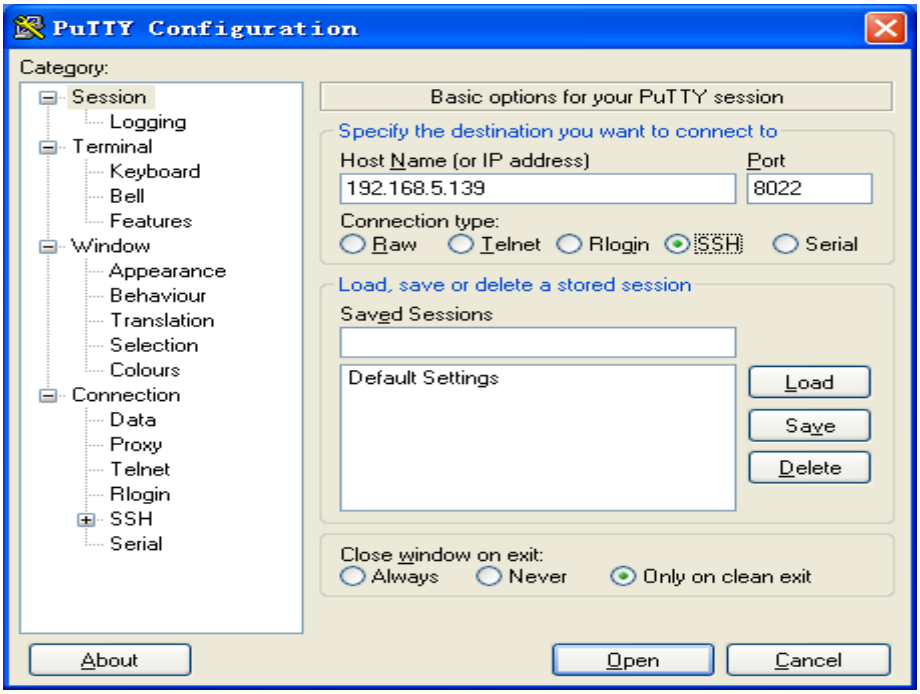

Figure 2-2

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

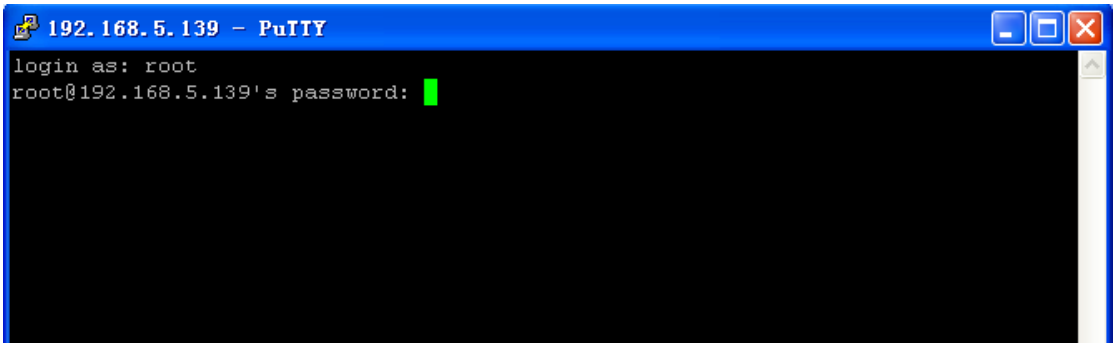

Figure 2-3

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

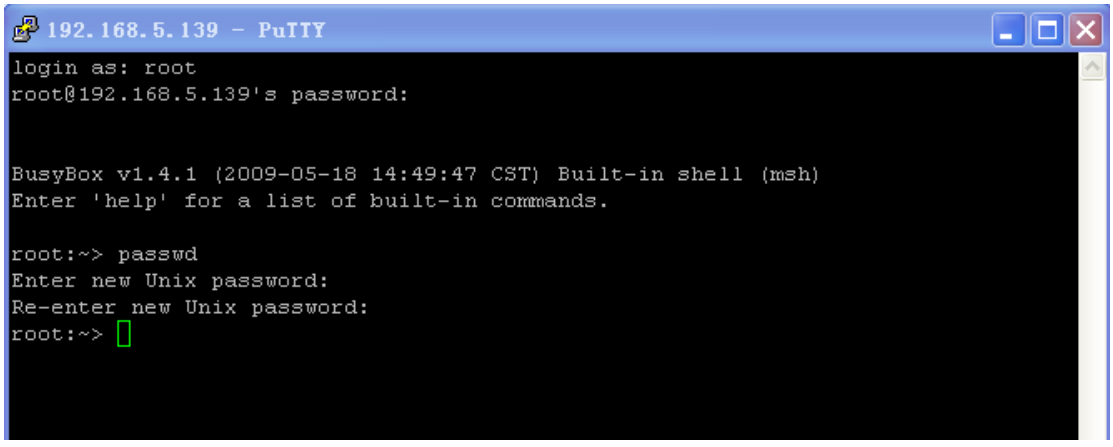

Figure 2-4

3. Security Configuration for Extensions

3.1 Change the default SIP Port

Select SIP settings→General→UDP Port

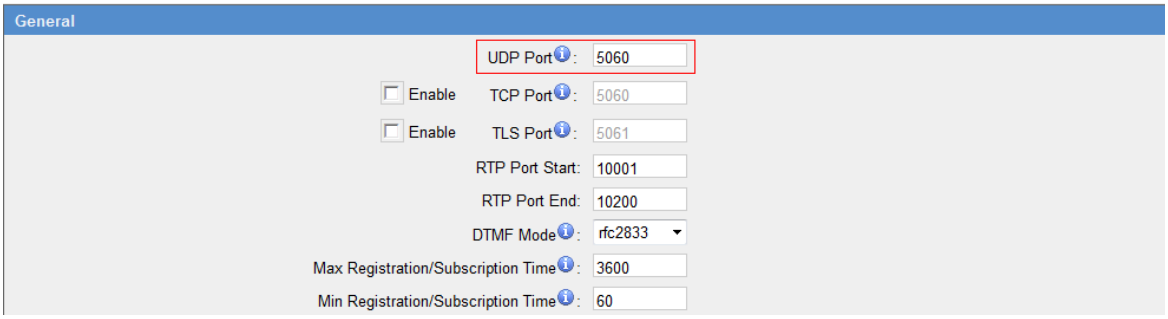

Figure 3-1

3.2* Disable guest calls

Select SIP settings→Advanced Settings→Allow Guest

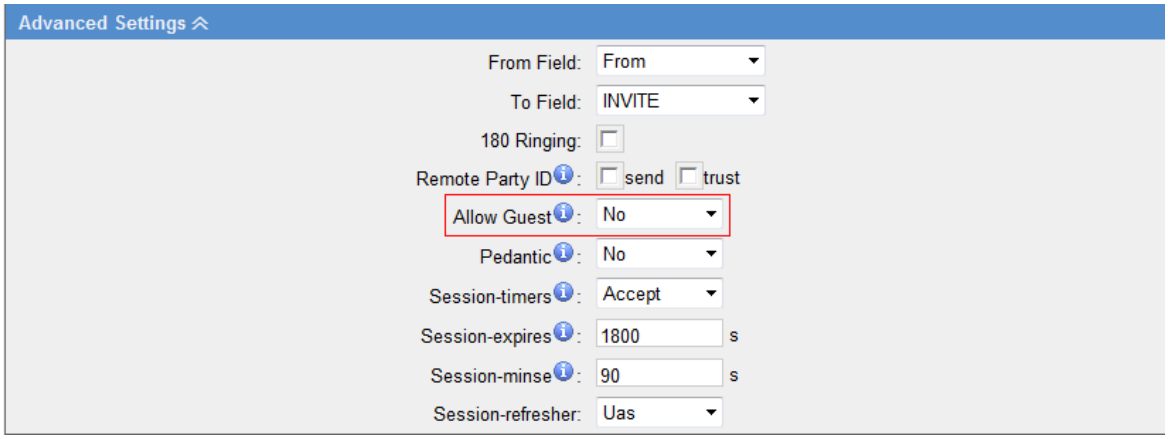

Figure 3-2

3.3* Security Configuration for remote extensions

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

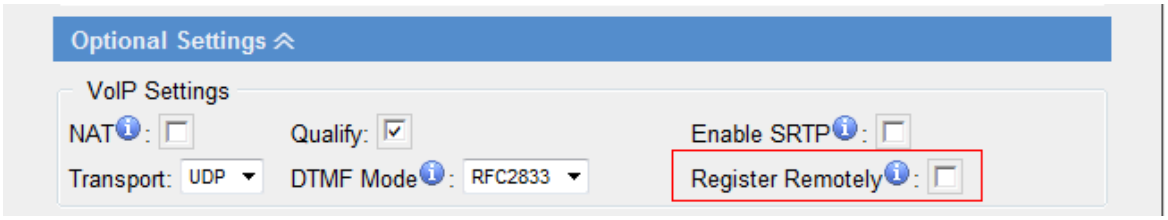

Figure 3-3

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.

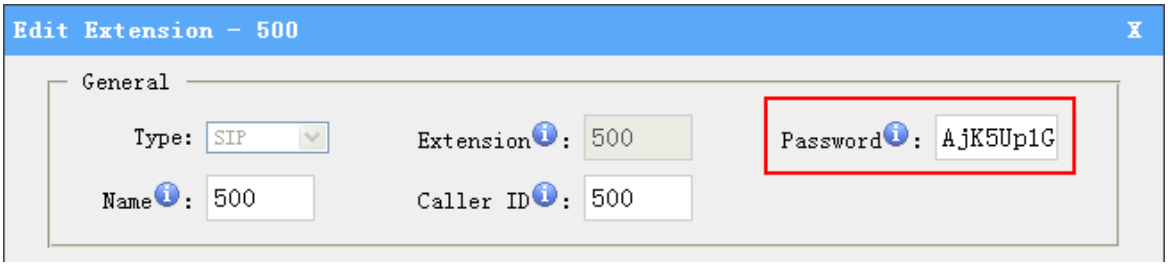

Figure 3-4

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

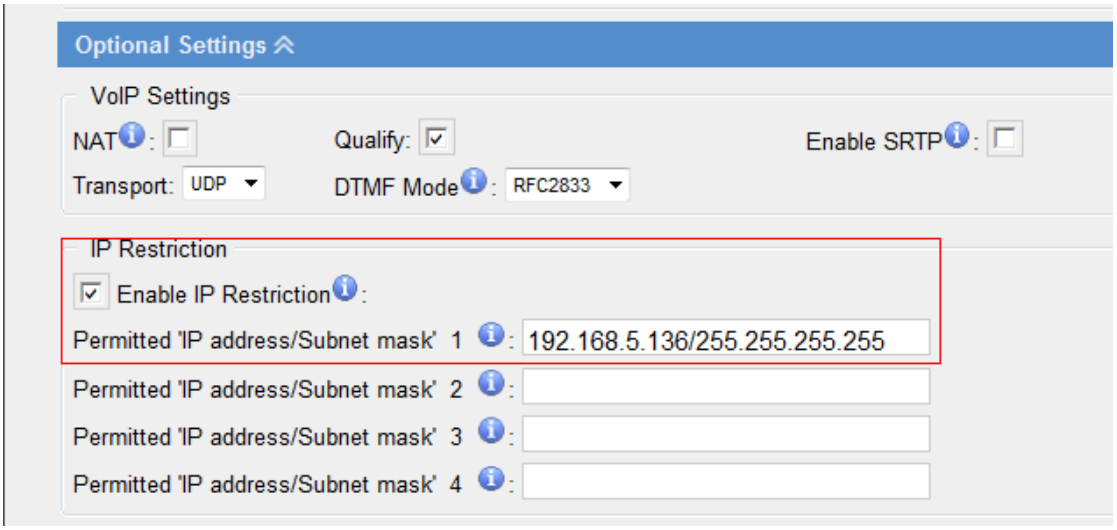

Figure 3-5

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 MyPBX firmware version 2.15.xx.xx or higher versions.

Step 1. Enable firewall on firewall page of MyPBX.

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 MyPBX 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

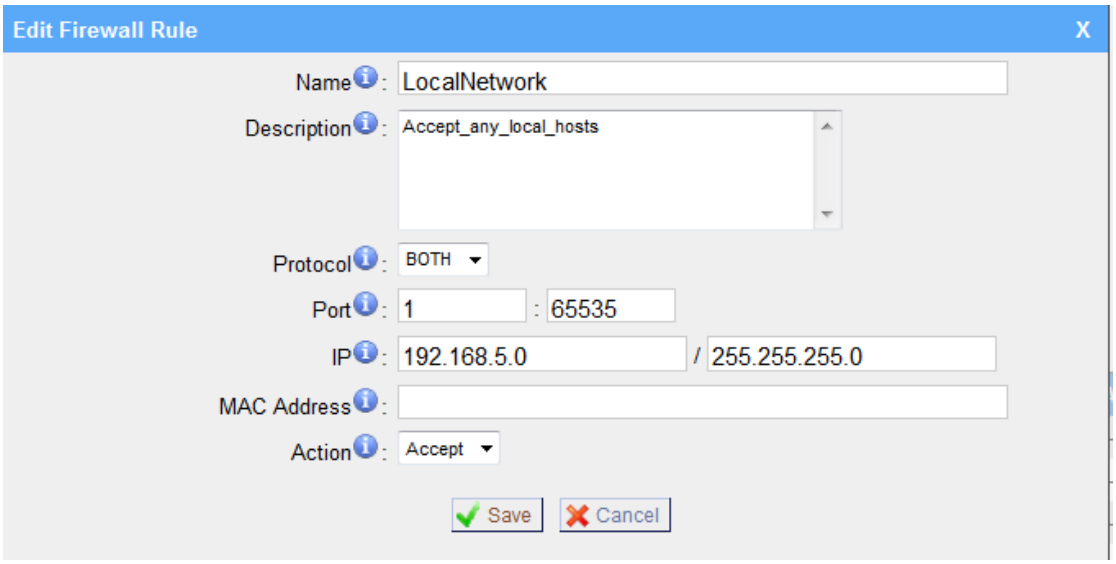

Figure 4-1

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 MyPBX 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

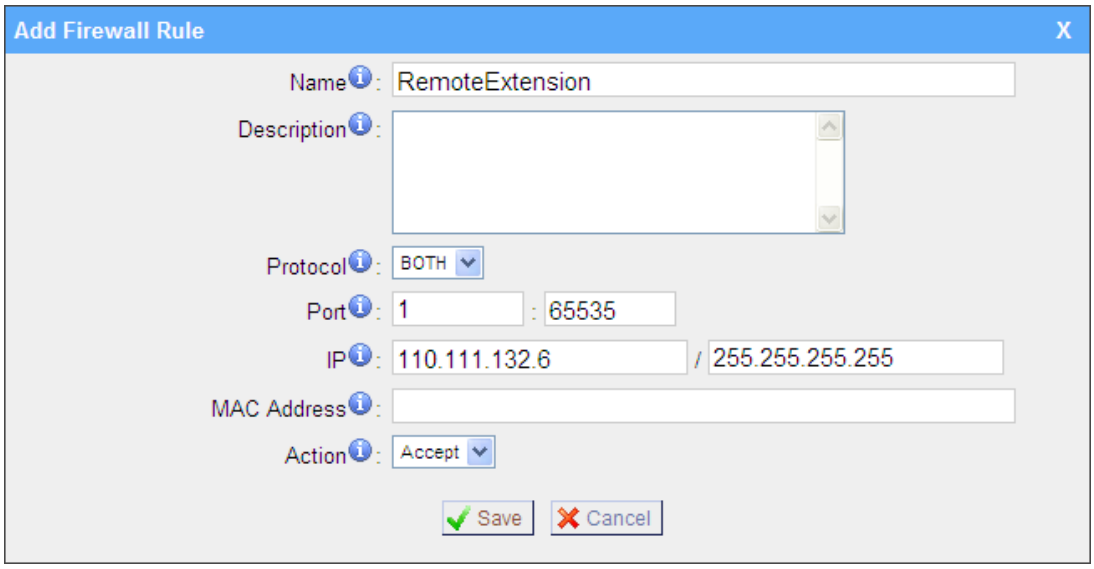

Figure 4-2

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

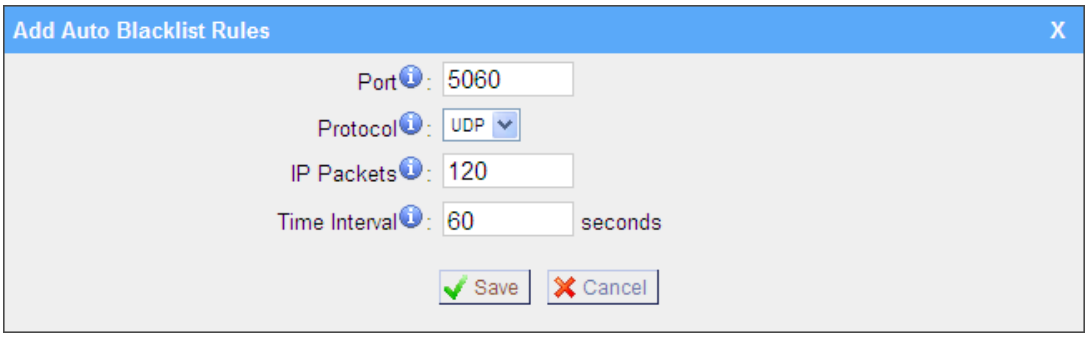

Figure 4-3

Rule No.2:

Port: 5060

Protocol: UDP

IP Packets: 40

Time Interval: 2 seconds

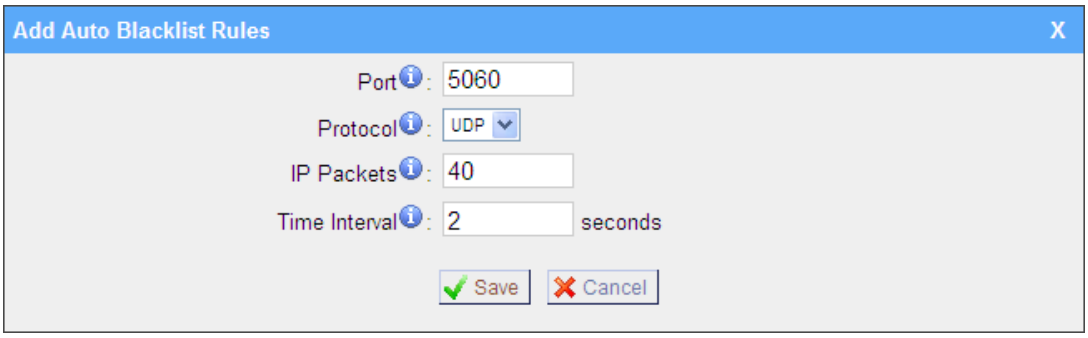

Figure 4-4

2) Add an auto blacklist rule for Port:8022

Rule No.3

Port: 8022

Protocol: TCP

IP Packets: 5

Time Interval: 60 seconds

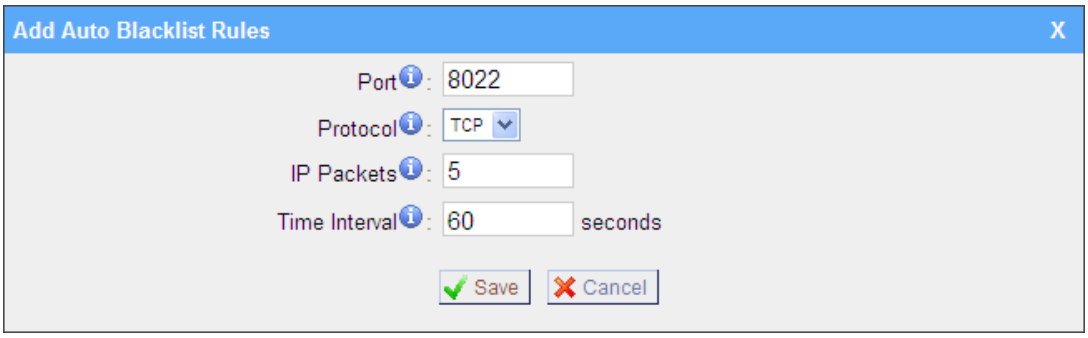

Figure 4-5

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 MyPBX 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

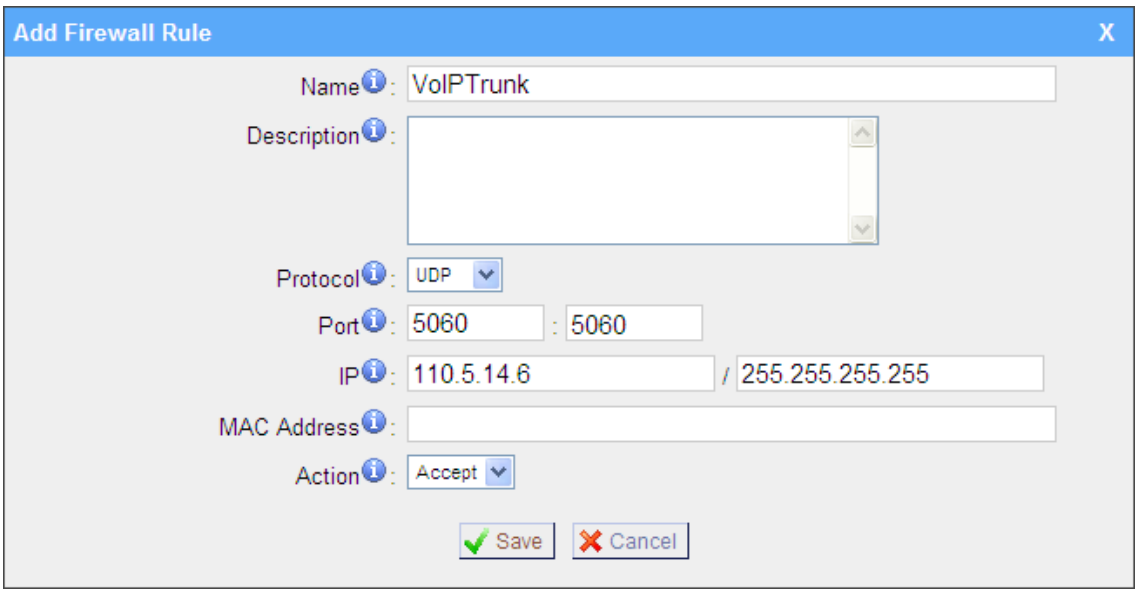

Figure 4-6

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

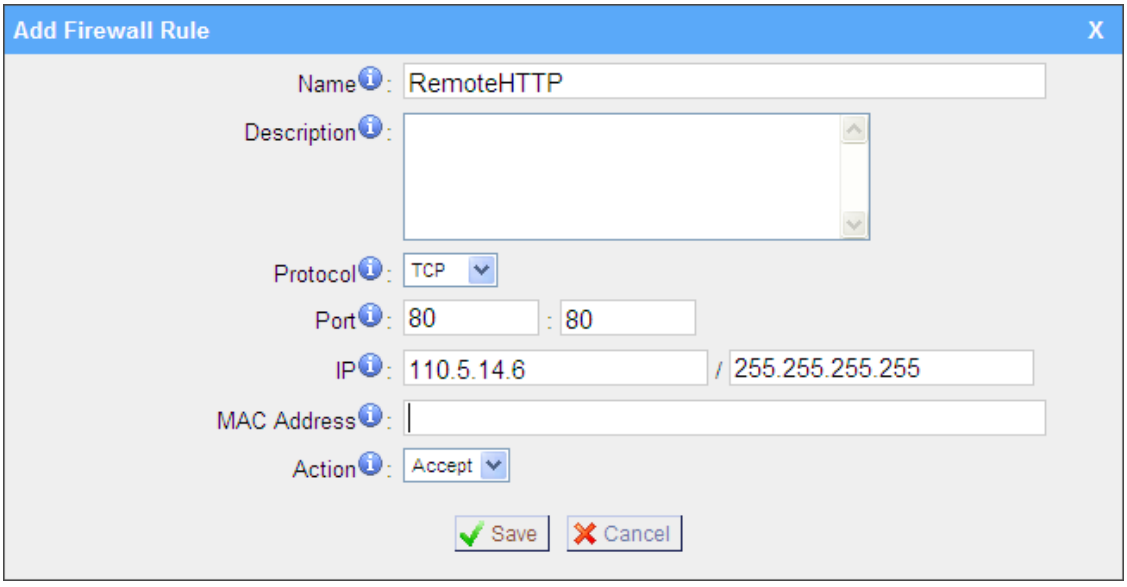

Figure 4-7

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

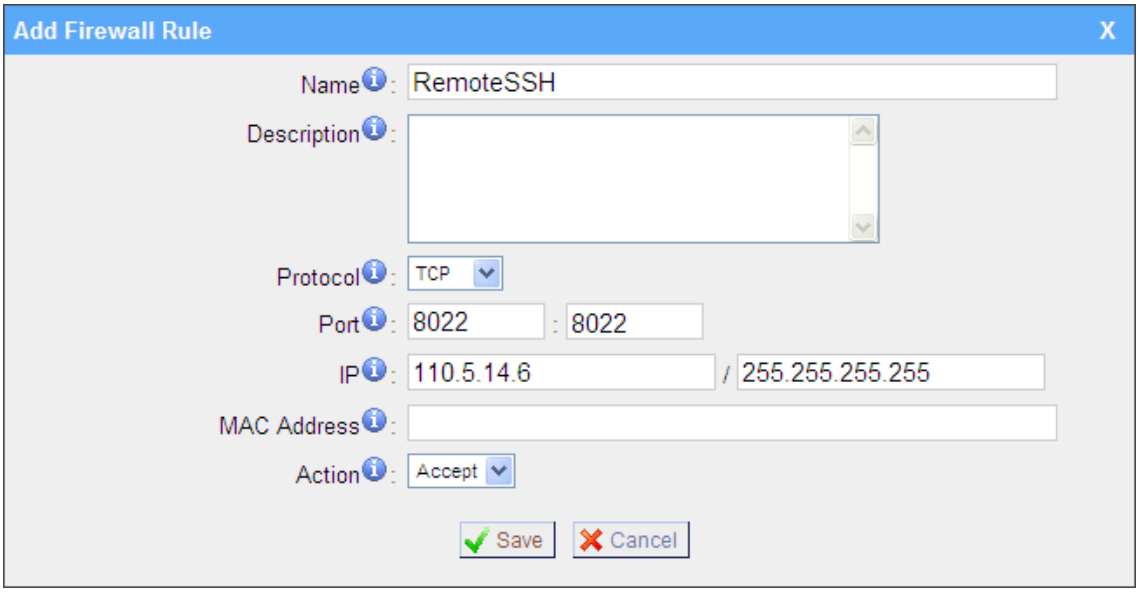

Figure 4-8

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.

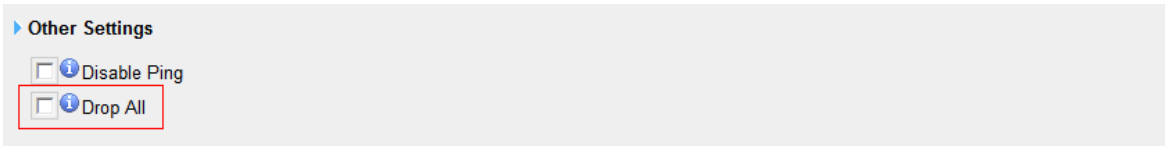

Figure 4-9

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.

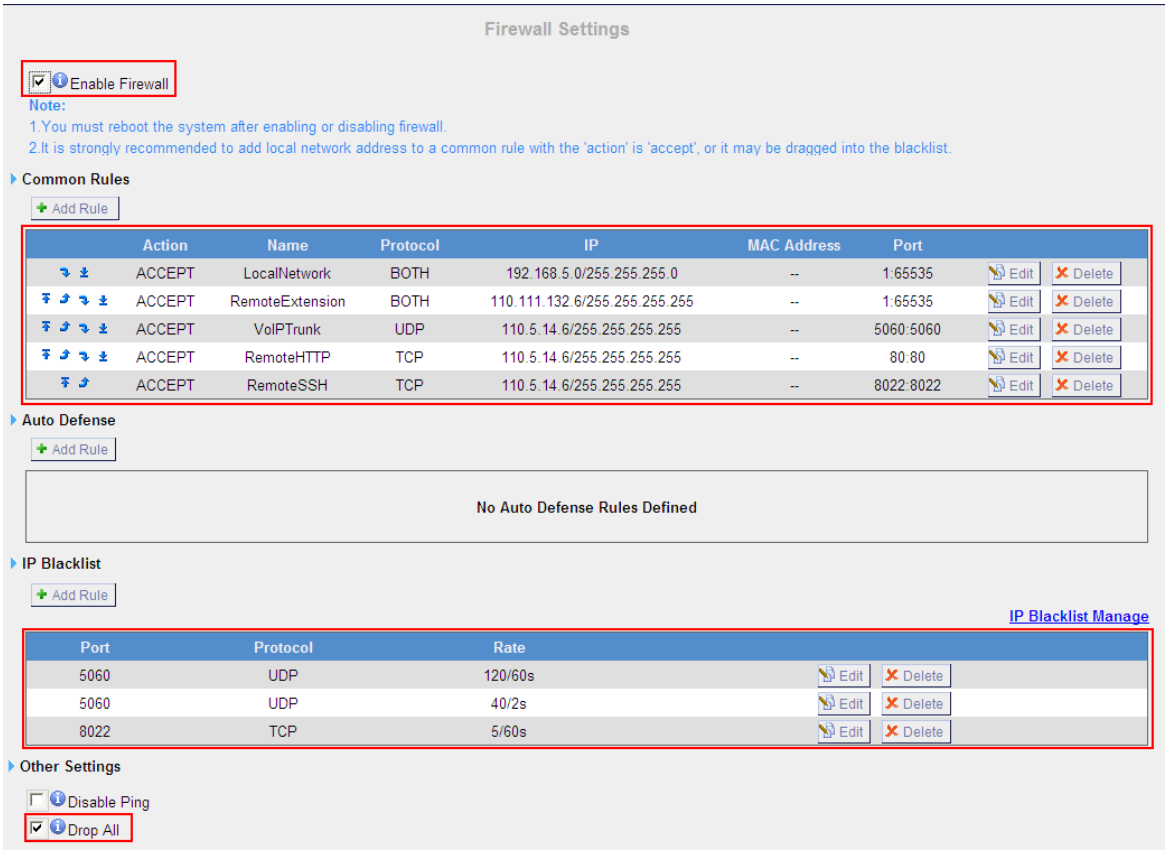

Figure 4-10

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

Blacklist and notify the user if it match the protection rule.

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@yeastar.com

Subject: IPAttack

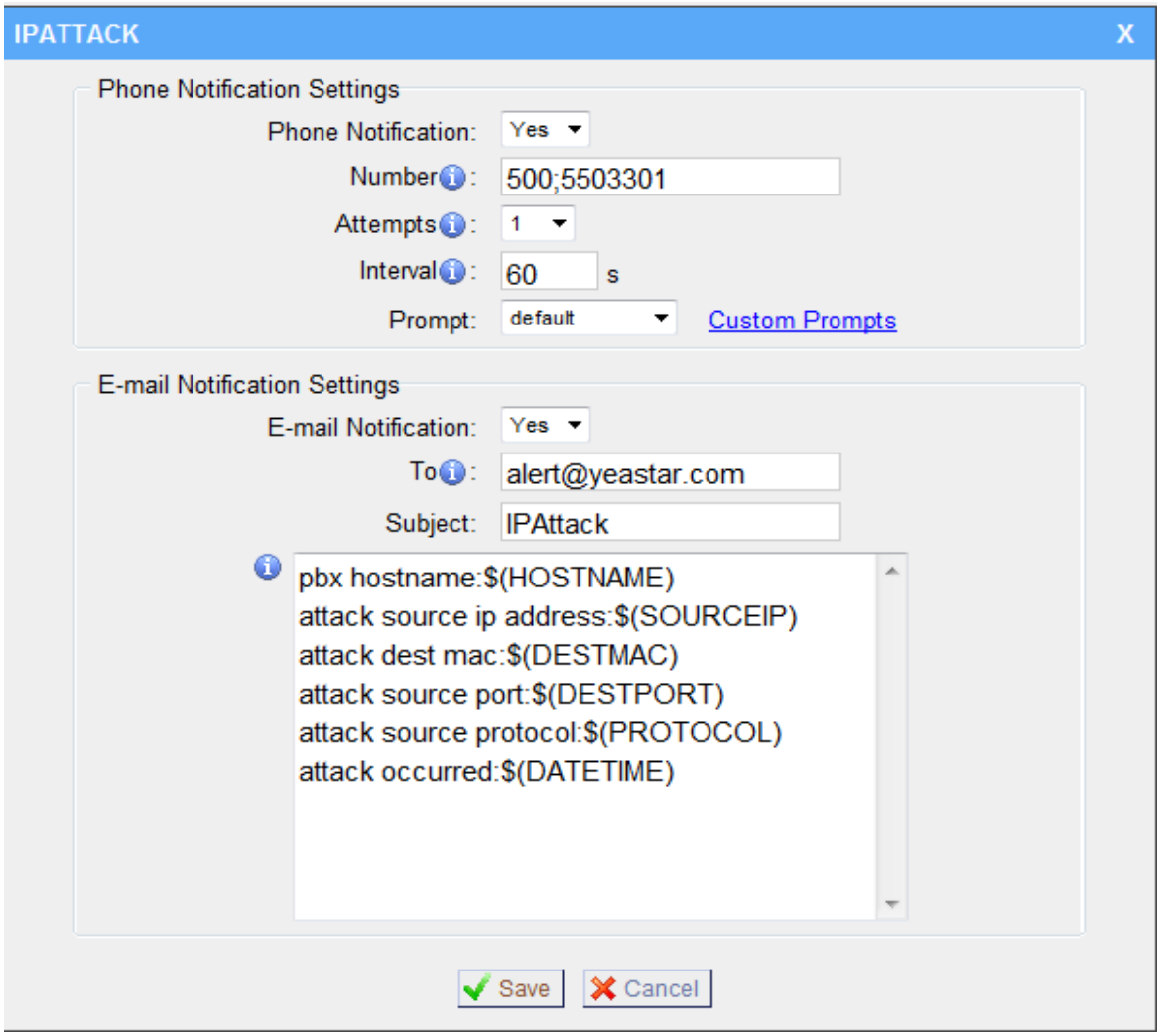

Figure 5-1

5.2 WEBLOGIN

Enter the password incorrectly five times when logging in MyPBX 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@yeastar.com
Subject: WebLogin

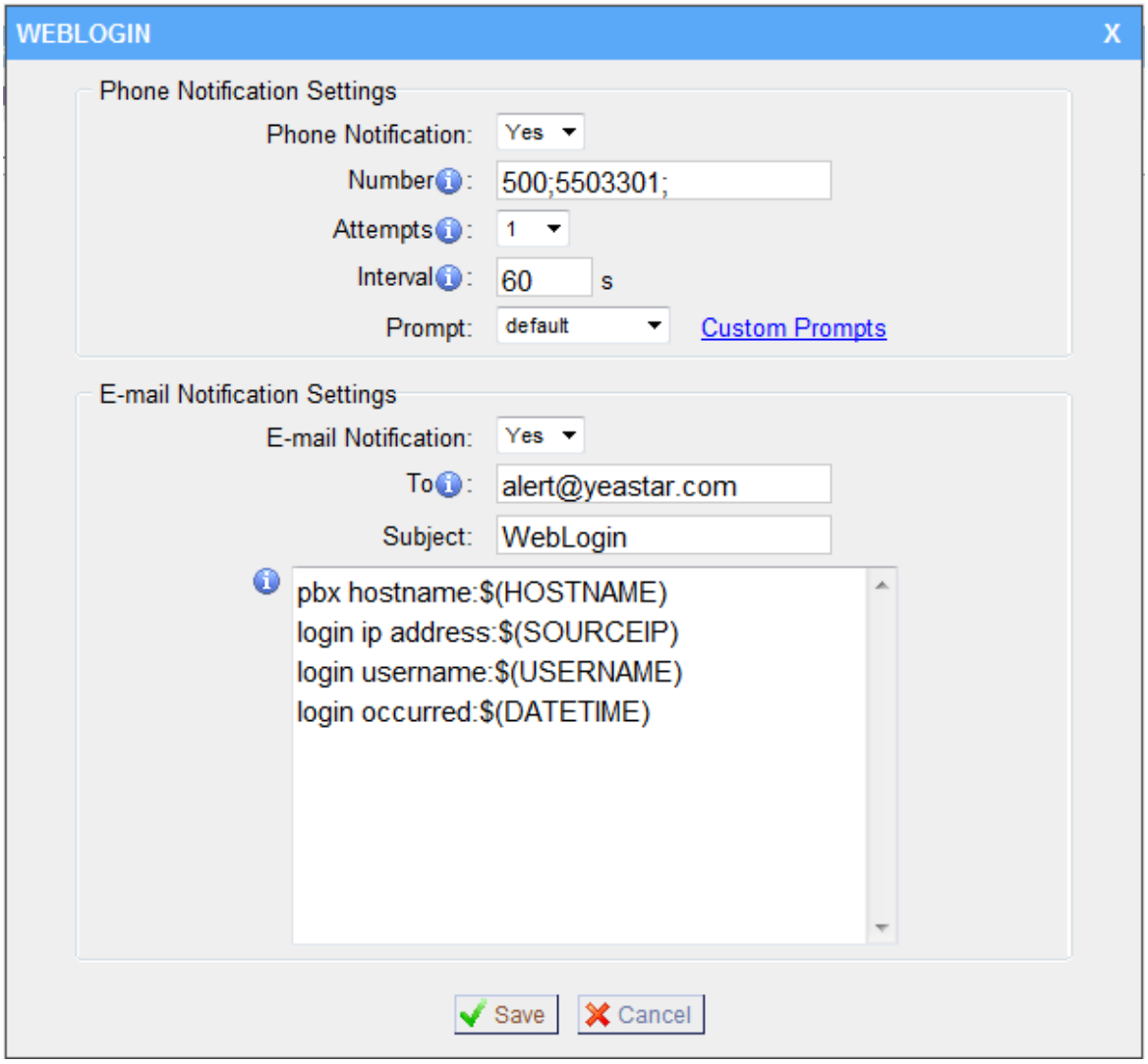

Figure 5-2

6. Note

If the phenomena of toll fraud have been happened in your MyPBX 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>