

Security Guide

Yeastar S-Series VoIP PBX

Version:

Date: 2024-08-01



Contents

Security Guide.....	1
PBX Service Security.....	1
Network Security.....	2
Web Access Security.....	3
Extension Security.....	5
Trunk Security.....	7
International Call Limit.....	8
Firewall Rules.....	12
Examples of Firewall Rules.....	14
IP Auto Defense.....	17
Contingency Plan.....	18

Security Guide

Security suggestions and measures of your PBX.

PBX Service Security

The PBX provides various services that use different protocol. To secure your PBX, you need to configure and manage the services on the PBX.

PBX Service

Go to **Settings > System > Security > Service** to check all the service status and port.




Note:

We suggest you to change the default port.

Table 1. Description of PBX Services

Service	Default Port	Description
HTTPS	8088	Web access protocol.
HTTP	8088	Web access protocol.
SSH	8022	Access the PBX via SSH to debug the system. Important: Do not enable SSH if you don't need to debug the system.
FTP	21	Access the PBX via FTP to download files from the PBX or upload files to the PBX. Important: Do not enable FTP if you don't need it.
TFTP	/	Yeastar S-Series VoIP PBX works as a TFTP server when auto provisioning phones. Important:

Table 1. Description of PBX Services (continued)

Service	Default Port	Description
		 You can disable TFTP if you don't need to provisioning the phones.
IAX	4569	IAX (Inter-Asterisk Exchange Protocol)
SIP UDP	5060	Registration port of SIP UDP.
SIP TCP	5060	Registration port of SIP TCP.
SIP TLS	5061	Secure SIP packets with TLS encryption. TLS allows safe transactions over untrusted networks and with authenticated parties.
AMI	5038	AMI (Asterisk Manager Interface): Monitor and control Asterisk system through the interface. You can connect a third-party software to the PBX via AMI interface.

Network Security

Separate Voice Traffic and Data Traffic

For some VoIP ISPs, they provide dedicated SIP trunks that supports NGN ports (Next Generation Network). NGN can separate data, voice and video networks or any combination of the three to form a converged network.

You can also set up VLAN (Virtual Local Networks) on the PBX. VLAN can improve the call quality, but also can secure your PBX.

The voice traffic and data traffic can be logically separated by a VLAN switch. If one VLAN is penetrated, the other will remain secured. Also, limiting the rate of traffic to IP telephony VLANs can slow down an outside attack.

Use VPN - Avoid Port Forwarding

We strongly recommend you to set up VPN network for your PBX. Avoid port forwarding on your router and do not enable DMZ on your router.

VPN can secure communications between remote devices and your PBX.

Yeastar S-Series VoIP PBX can be set as an OpenVPN server and also can be an OpenVPN client.

Web Access Security

Secure the web access of your PBX.

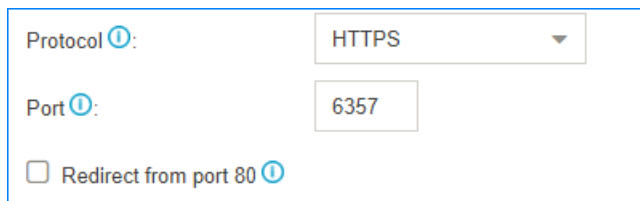
Web Access Protocol

Yeastar S-Series VoIP PBX supports `HTTPS` and `HTTP` protocol of web access. You can go to **Settings > System > Security > Service** to change the web access settings.

To secure transactions and prevent unauthorized access, we suggest you:

- Use `HTTPS` protocol
- Disable **Redirect from port 80**.
- Change the default web access port.

Avoid using well known port, such as 80 and 443.



Protocol ⓘ: HTTPS ▼

Port ⓘ: 6357

☐ Redirect from port 80 ⓘ

Password of Web Login

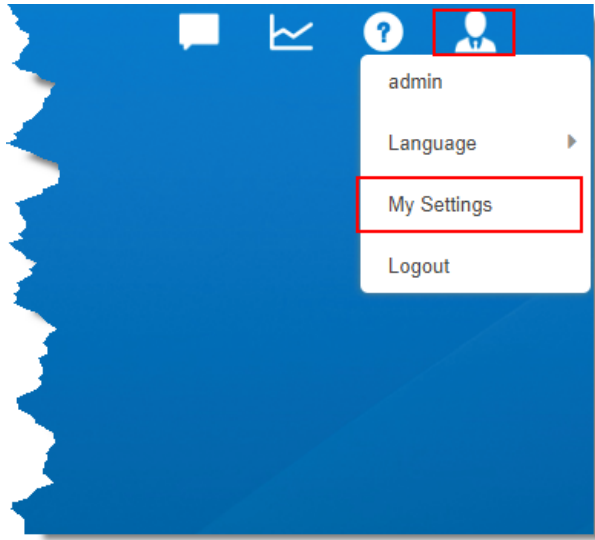
After you log in the PBX web interface for the first time, we suggest you to change the web login password.

Click **Option** icon at the top-right corner, then click **My Settings** to change the login password and enter your email address.



Note:

- The email address can be used to reset the password of web login.



The Password should meet all the following requirements:

- At least 8 characters
- At least 1 number
- At least 1 uppercase letter
- At least 1 lowercase letter
- Avoid word or name

For example, avoid word like `yeastar`, `password`, `carol` etc. Use random password like `81sS*!08k_s922`.

Login Settings

Go to **Settings > System > Security > Service** to change the login settings.

- **Auto Logout Time:** The PBX will logout automatically after the period of inactivity.
- **Login Mode:** By default, the PBX allows **Extension** login mode. We suggest you to choose **Email** login mode.
 - **Extension:** Users can use extension number as the username of web login.
 - **Email:** Users can use their email addresses as the username of web login.



Note:

The super administrator should use `admin` as the username of web login.

Login Attempts

For login protection, the PBX will block an web address after 3 login attempts.

The blocked user should try to log in the PBX web interface after 10 minutes.

Extension Security

Secure the VoIP extensions.

SIP Registration Port

To prevent malicious registration of SIP extensions, go to **Settings > PBX > General > SIP > General** to change the **UDP Port**.

UDP Port ⓘ: 5682

TCP Port ⓘ: 5060

RTP Port ⓘ: 10000 -- 12000

Local SIP Port ⓘ: 5062 -- 5082



Note:

After you change the SIP UDP registration port, you need to change the relevant auto defense rules for the SIP port.

Auto Defense Rules		Blocked IP Address			
Add Delete		Set to the changed SIP UDP port			
<input type="checkbox"/>	Port	Protocol	Rate	Edit	Delete
<input type="checkbox"/>	5682	UDP	120/60s		
<input type="checkbox"/>	5682	UDP	40/2s		
<input type="checkbox"/>	8022	TCP	10/60s		

Extension Password

The PBX will generate a random password for a new extension. If you want to set the password manually, the password should meet the following requirements:

- At least 8 characters
- At least 1 number
- At least 1 uppercase letter

- At least 1 lowercase letter
- Avoid word or name

For example, avoid word like `yeastar`, `password`, `carol` etc. Use password like `81sS*!08k_s922`.

Restrict Extension Registration

You can limit which IP address or which User Agent is allowed to register a certain extension.

Go to **Settings > PBX > Extensions** to edit the extension's **Advanced** setting.

• User Agent Registration Authorization

By default, the PBX allows phones to register extensions without user agent limit. To enhance the extension security, you can restrict which user agent is allowed to register the extension.

When a phone is trying to register the extension, the phone will send SIP packets that contain the user agent. If the user agent is not allowed, the registration will fail.

☒ Enable User Agent Registration Authorization ⓘ

User Agent: ⓘ

• IP Restriction

To enhance the extension security, you can restrict which IP is allowed to register the extension.

IP Restriction

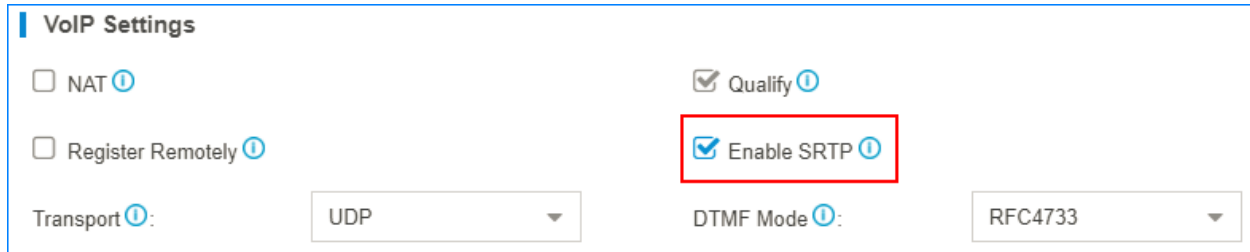
☒ Enable IP Restriction ⓘ

Permitted IP/Subnet mask: / ⓘ

SRTP

SRTP is used to encrypt audio streams. If SRTP is enabled for an extension, the extension will support SRTP and will allow negotiation with calls without SRTP.

Go to **Settings > PBX > Extensions** to edit the extension's **Advanced** setting.



VoIP Settings

☐ NAT ⓘ

☒ Qualify ⓘ

☐ Register Remotely ⓘ

☒ **Enable SRTP ⓘ**

Transport ⓘ: UDP ▼

DTMF Mode ⓘ: RFC4733 ▼

Trunk Security

Secure the trunks on the PBX.

To prevent unauthorized international calls and long-distance calls through the PBX trunks, you need to take steps to protect your trunks on the PBX.

Outbound Route Permission

When you are setting up outbound routes on your PBX, you need to consider outbound route permission for different users.

We suggest you to set up different outbound routes for different trunks, and assign outbound route permission to the users.

For example, you can set up outbound routes as below:

- **Outbound route for local calls**

Select the trunk that is least-cost for local calls, and set the outbound route permission for all the users.

- **Outbound route for long-distance calls**

Select the trunk that is least-cost for national calls, and set the outbound route permission for all the sales and managers.

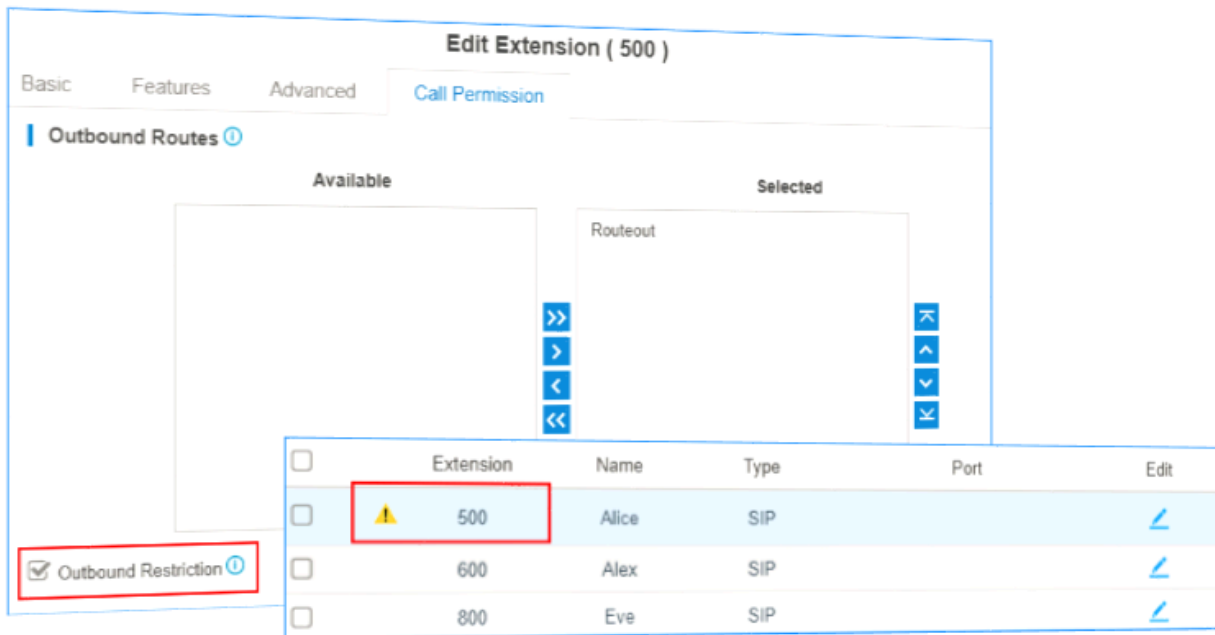
- **Outbound route for international calls**

Select the trunk that is least-cost for international calls, and set the outbound route permission for the international sales who need to make international calls.

Outbound Restriction

Yeastar S-Series VoIP PBX has a default rule to limit users to make maximum 5 outbound calls in 1 minute. You can add an Outbound Restriction rule to define how many outbound calls the extension users can make during a period of time.

If a user makes outbound calls over the limit, the extension will be locked and has permission to make internal calls only.



Go to **Settings > PBX > Call Control > Outbound Restriction** to edit the rule or add a rule.

Add Outbound Restriction

Name ⓘ:

Time Limit(min) ⓘ:

Number of Calls Limit ⓘ:

Member Extensions: ☒ All Extensions ☐ Selected Extensions

International Call Limit

To prevent toll fraud, you need to pay particular attention to the trunk that is used to make international calls.

Limit Call Credit

Before you set up the trunk on your PBX, ask the trunk provider to limit the credit of international calls.

If you don't need to make international calls, ask the provider to disable international call service on the trunk.

Set Password for the International Outbound Calls

Set a single PIN for the outbound route that allows international calls, when the users dial international numbers, the PBX will ask the users to enter a PIN.



Note:

You can also set a PIN list for the outbound route, and assign different PIN numbers to the users who have permission to make international calls.

- If the PIN is correct, the PBX will call the international number.
- If the PIN is incorrect, the PBX will drop the call.

Edit Outbound Routes (International_Calls)

Member Extensions ⓘ:

Available

900 - Cindy

902 - Ina

903 - Alan

904 - Henry

905 - James

906 - Jay

907 - 907

908 - 908

>>

>

<

<<

Selected

500 - Alice

600 - Alex

800 - Eve

901 - Carol

<

<

>

>

Password ⓘ:

Single Pin ▼

685247

Disable International Calls on the PBX

If the trunk provider cannot disable international calls for the trunk, you can add an invalid outbound route on the PBX to disable international calls.

1. Create an invalid SIP trunk like the following figure.

The screenshot shows the 'Add VoIP Trunk' configuration page with the 'Basic' tab selected. The configuration is as follows:

Add VoIP Trunk			
Basic Codec Advanced DOD Adapt Caller ID			
Trunk Status ⓘ:	Enabled ▼		
Protocol:	SIP ▼	Trunk Type:	Peer Trunk ▼
Provider Name:	Invalid_International		
Transport ⓘ:	UDP ▼		
Hostname/IP ⓘ:	127.0.0.1 : 5060		
Domain ⓘ:	127.0.0.1		
Caller ID Number ⓘ:			
Caller ID Name ⓘ:			
<input type="checkbox"/> Enable SLA ⓘ If enabled, this trunk will not be available in routes or other channels.			

Red boxes highlight the 'Peer Trunk' dropdown, the 'Invalid_International' text, and the '127.0.0.1 : 5060' and '127.0.0.1' fields. A blue box highlights the 'Invalid_International' text.

2. Create an outbound route for the invalid SIP trunk.

- Set **Patterns** to 00.
- Select the invalid SIP trunk
- Select all the extensions

Edit Outbound Routes (Invalid_International)

Name ⓘ:

Invalid_International

Dial Patterns ⓘ:

+

Patterns	Strip	Prepend	Edit	Delete
00.				

Member Trunks ⓘ:

Available

FXO3 (FXO)

FXO4 (FXO)

International (SIP-Register)

Local (SIP-Peer)

>>

>

<

<<

Selected

Invalid_International (SIP-Peer)

<<

<

>

>>

Member Extensions ⓘ:

Available

>>

>

<

<<

Selected

500 - Alice

600 - Alex

800 - Eve

901 - Carol

900 - Cindy

902 - Ina

903 - Alan

<<

<

>

>>

3. Place the invalid outbound route to the top.

Inbound RoutesOutbound RoutesAutoCLIP RoutesTime Conditions								
<div>AddDelete</div>								
<input type="checkbox"/>	Name	Dial Pattern	Edit	Delete	Move			
<input type="checkbox"/>	Invalid_International	00.						
<input type="checkbox"/>	pstnout	X.						

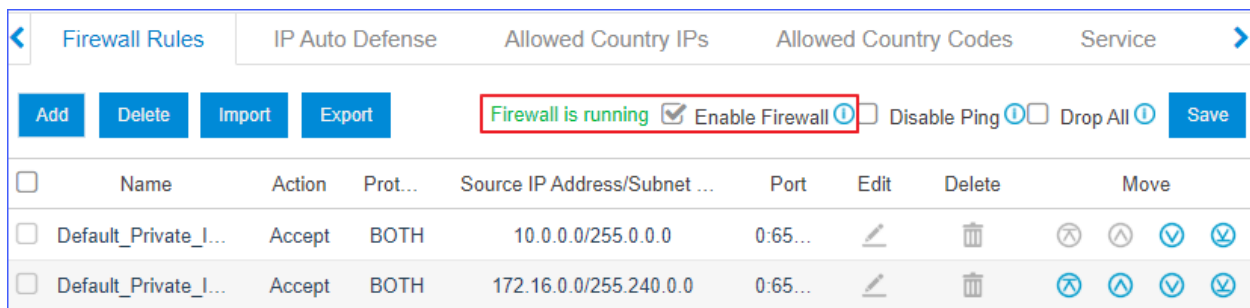
Firewall Rules

We strongly recommend you to enable and configure firewall on the PBX to prevent the attack fraud or calls loss.

Enable Firewall on the PBX

Go to **Settings > System > Security > Firewall Rules**, check the option **Enable Firewall**.

If firewall is enabled, the page will show "Firewall is running", and the firewall rules will work to protect your PBX.



Firewall Rules

Firewall rules are pre-configured rules to control and filter traffic that are sent to the PBX. Yeastar S-Series VoIP PBX has default firewall rules to accept access of your local network. You can also create new rules according to your needs.

Default firewall rules

By default, the following types of IP address or domain are included in Yeastar S-Series VoIP PBX firewall rules:

- **Local network**
 - 10.0.0.0/255.0.0.0
 - 172.16.0.0/255.240.0.0
 - 192.168.0.0/255.255.0.0
 - 169.254.0.0/255.255.0.0
- **Domain related with Yeastar**
 - appcenter.yeastar.com
 - update.yeastar.com
 - mgt.yeastar.com
 - stund.yeastar.com
 - cwmp.yeastar.com
 - lcstunnel.yeastar.com

- image.yeastar.com
- **IP address of phones that are auto provisioned**

Create firewall rules

Besides the default firewall rules, you can create other rules to filter specific source IP address or domain name, ports, MAC address.

Go to **Settings > System > Security > Firewall Rules** to configure the firewall rules.

Add Firewall Rule

Name ⓘ:

Description ⓘ:

Action ⓘ:

Accept ▼

Accept the connections from the configured address.

Protocol ⓘ:

BOTH ▼

MAC Address ⓘ:

Type ⓘ:

☐ IP
☒ Domain Name

Domain Name ⓘ:

Port ⓘ:

0

:

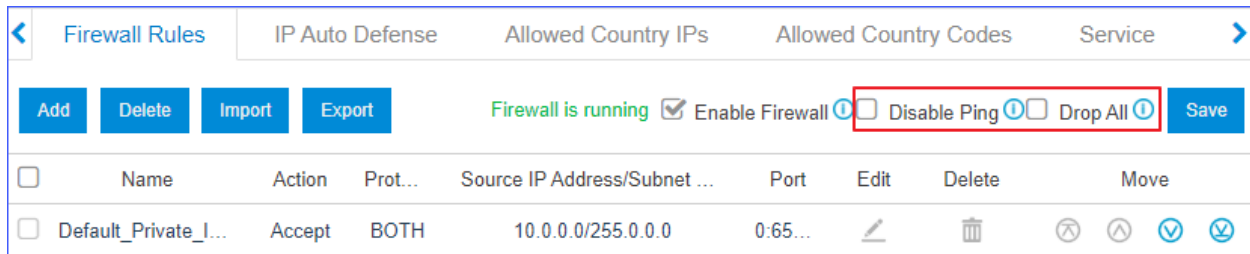
65535

- **Name:** Set a name to identify the firewall rule.
- **Description:** Optional. Description for this firewall rule.
- **Action:** Choose the action for the firewall rule.
 - **Accept**
 - **Drop**
 - **Reject**
- **Protocol:** Choose the protocol that is applied to the rule.
 - **UDP**
 - **TCP**
 - **BOTH:** Both TCP and UDP.
- **MAC Address:** Optional. The MAC address that is applied to the rule.
The format of MAC address is xx:xx:xx:xx:xx:xx.
- **Type:** Choose the network type of the source traffic.

- **Source IP Address/Subnet Mask:** The IP address and subnet of the source traffic.
- **Domain Name:** The domain name of the source traffic.
- **Port:** The port of the source traffic.

Additional Firewall Settings

The PBX provides additional firewall settings to enhance the system security.



- **Disable Ping:** The PBX will disable Ping response (ICMP echo).
- **Drop All:** The PBX will drop all the packets and connections from other hosts except the accepted/trusted IP address/domain that is defined in the firewall rules.



Note:

We recommend that you create a backup on the PBX before you enable **Drop All**.

Examples of Firewall Rules

In this topic, we provide configuration examples of firewall rules under different scenarios. We recommend that you configure firewall rules according to the network environment of your PBX.

Log in PBX, go to **Settings > System > Security > Firewall Rules**, and configure firewall rules as follows.

- Add a trusted IP address to allowlist, or PBX may block the IP address as it frequently sends packets.
- Add an untrusted IP address to blocklist to prevent the IP address from accessing PBX.

Accept remote extensions and remote web access

If you want to remotely access PBX web page or register extensions, you can add the public IP address to the allowlist, or PBX may block the public IP address as it frequently sends packets.

For example, the trusted public IP address is 1.2.3.4. Set the firewall rule as follows.



Note:

- The subnet mask 255.255.255.0 indicates that all IP addresses under the same network segment are allowed to access the PBX.
- If the remote place doesn't have a static public IP address, you can set a firewall rule for the trusted domain name.

Name ⓘ:	Allow_Remote_Access	
Description ⓘ:		
Action ⓘ:	Accept ▼	
Protocol ⓘ:	BOTH ▼	
MAC Address ⓘ:		
Type ⓘ:	<input checked="" type="radio"/> IP <input type="radio"/> Domain Name	
Source IP Address/Subnet Mask:	1.2.3.4	/ 255.255.255.255
Port ⓘ:	1	: 65535

Accept traffic of VoIP Provider

Accept the traffic of SIP registration port and RTP media ports from the VoIP provider.

For example, the IP address of the VoIP provider is 2.2.2.2; port of SIP registration is 5630; the range of RTP ports is 10000-12000. You need to set two firewall rules for the VoIP provider.

- **Accept traffic of the SIP registration port**

Name ⓘ:	Accept_SIP_Port	
Description ⓘ:		
Action ⓘ:	Accept ▼	
Protocol ⓘ:	UDP ▼	
MAC Address ⓘ:		
Type ⓘ:	<input checked="" type="radio"/> IP <input type="radio"/> Domain Name	
Source IP Address/Subnet Mask:	2.2.2.2	/ 255.255.255.255
Port ⓘ:	5630	: 5630

- **Accept traffic of the RTP ports**

Name ⓘ:	Accept_RTP_Ports	
Description ⓘ:		
Action ⓘ:	Accept ▼	
Protocol ⓘ:	UDP ▼	
MAC Address ⓘ:		
Type ⓘ:	<input checked="" type="radio"/> IP <input type="radio"/> Domain Name	
Source IP Address/Subnet Mask:	2.2.2.2	/ 255.255.255.255
Port ⓘ:	10000	: 12000

Accept traffic of NTP, SMTP, POP, STUN

We recommend that you accept traffic of NTP, SMTP, POP, STUN, and keep the default [auto defense rules](#).

For example, the IP address of the NTP server is 3.3.3.3. Set the firewall rule as the following figure.

Name ⓘ:	Accept_NTP
Description ⓘ:	
Action ⓘ:	Accept ▼
Protocol ⓘ:	BOTH ▼
MAC Address ⓘ:	
Type ⓘ:	<input checked="" type="radio"/> IP <input type="radio"/> Domain Name
Source IP Address/Subnet Mask:	3.3.3.3 / 255.255.255.255
Port ⓘ:	1 : 65535

IP Auto Defense

Yeastar S-Series VoIP PBX has default auto defense rules to prevent massive connection attempts or brute force attacks.



Important:

- Do NOT delete the default IP defense rules.
- Change the default IP defense rules under the instruction of our support.

Go to **Settings > System > Security > IP Auto Defense > Auto Defense Rules** to configure auto defense rules.



The dialog box titled "Add IP Auto Defense Rule" contains the following fields and controls:

- Port:** Two input boxes separated by a colon (:).
- Protocol:** A dropdown menu currently showing "UDP".
- Number of IP Packets:** A single input box.
- Time Interval (s):** A single input box.
- Buttons:** "Save" and "Cancel" buttons at the bottom.

- **Port:** The auto defense port.
- **Protocol:** The protocol of the auto defense port.
- **Number of IP Packets:** The number of IP Packets permitted within a specific time interval.
- **Time Interval:** The time interval to receive IP Packets.

For example, **Number of IP Packets** is 90 and **Time Interval** is 60; The PBX will block the IP that sends more than 90 IP packets in 60 seconds.

Contingency Plan

There is no absolute safety. Make a contingency plan for your PBX.

In case an attacker successfully forced your PBX to fail, you should have a contingency plan for your PBX.

Event Center

To get informed of the events that occur to your PBX, you need to configure Event Center on the PBX. Enable event notifications and add contacts to receive the notifications by email or phone number.

Hot Standby

Prepare two PBXs that are in the same model and firmware version, and set up Hot Standby. When the primary server cannot work, you can quickly replace the failed server to the secondary server with the same configurations.

Schedule Auto Backup

Set auto backup on the PBX. If the PBX cannot work, you can reset the PBX, and restore the PBX configurations from the backup file.