

# **Active Wall User Manual**

**U  
S  
E  
R**

**M  
A  
N  
U  
A  
L**

**Active Network CO., Ltd**

# Table of Contents

<b>Chapter 1.</b>	<b>Preface.....</b>	<b>3</b>
1.1.	Version introduction .....	3
1.2.	User .....	3
1.3.	Rules in the manual .....	3
<b>Chapter 2.</b>	<b>Product introduction.....</b>	<b>4</b>
2.1.	Overview .....	4
2.2.	System features .....	6
<b>Chapter 3.</b>	<b>Install and Uninstall.....</b>	<b>7</b>
3.1.	System requirements .....	7
3.2.	Network environments .....	7
3.3.	Installation guide.....	11
3.4.	Uninstall guide .....	14
<b>Chapter 4.</b>	<b>System administration .....</b>	<b>16</b>
4.1.	Getting started .....	16
4.2.	User login.....	16
4.3.	Start/Stop service.....	17
4.4.	User log out.....	17
4.5.	Modify password.....	17
4.6.	Exit the program.....	17
4.7.	Computer management .....	17
4.8.	Group management .....	20
4.9.	Time range management .....	22
4.10.	Policy management .....	23
4.11.	Select a network adapter .....	25
4.12.	Setting option .....	26
4.13.	Plug-in management.....	27
<b>Chapter 5.</b>	<b>Plug-in operation.....</b>	<b>28</b>
5.1.	Authorization.....	29
5.2.	Time Filter.....	30
5.3.	Port Filter .....	30
5.4.	Bandwidth Control .....	31
5.5.	Show Flux .....	32
5.6.	MAC Filter .....	33
5.7.	IP Filter.....	35
5.8.	DNS Filter .....	36
5.9.	HTTP Filter .....	37
5.10.	SMTP Filter.....	39
5.11.	POP3 Filter.....	40
5.12.	IM Filter .....	41
5.13.	FTP Filter .....	42
5.14.	HTTPS Filter.....	44
5.15.	Redirect to Proxy.....	45

5.16.	Log to Files .....	47
5.17.	Log to Database.....	47
5.18.	Log to Mail.....	48
5.19.	Log to Message .....	49
<b>Chapter 6.</b>	<b>Upgrade and Registration .....</b>	<b>50</b>
6.1.	Upgrade online .....	50
6.2.	Registration .....	50
<b>Chapter 7.</b>	<b>FAQ.....</b>	<b>51</b>
7.1.	Frequently answered questions .....	51
7.2.	Known problems .....	54
<b>Chapter 8.</b>	<b>Contact us .....</b>	<b>54</b>
8.1.	Technical support .....	54
8.2.	Advice and Suggestions .....	55
8.3.	Contact .....	55
<b>Chapter 9.</b>	<b>Protocols and standards.....</b>	<b>55</b>
9.1.	Protocols.....	55

# Chapter 1. Preface

## 1.1. Version introduction

This manual is for Active Wall V2.0

## 1.2. User

This manual is for the following users:

- Network engineer
- Network administrator
- Users who master basic knowledge of networking

## 1.3. Rules in the manual

### General format

Font format	Meaning
Times New Roman	The main text and the first-class captions.
Arial Bold	The other captions except the first-class captions.
Courier New Italic	Notes or tips which are separated from the main text by rectangle frames.

### Graphical format

Graph format	Meaning
<>	A button name, for example: "Press the button <OK>".
[]	A window/dialog name, a menu item name, a database name, a plug-in name or a defined string, for example: "Show the window [New user]".
/	A hierarchical menu is separated by "/", for example: "[File/New/Folder]" means one of the [File] menu items is [New], one of the [New] menu items is [Folder].

### Keyboard mapping

Keyboard mapping	Meaning
<Key>	A key name, for example: "<Enter> means the Enter key. <Tab> means the tab key. <Backspace> means the backspace key and <a>

	means a lowercase <a> key".
<Key 1+Key 2>	Press several keys on the keyboard at the same time, for example, <Ctrl+Alt+A> means to press <Ctrl>, <Alt>, <A> at the same time.
<Key 1, Key2>	Firstly press Key 1 down and release. Secondly press Key 2. For example, <Alt, F> means to press <Alt> and release, then to press <F>.

#### Mouse rules

Mouse action	Meaning
Click	Press down a mouse button quickly and release it.
Double click	Repeat the click action twice in a hurry.
Drag drop	Move the mouse while keeping one mouse button pressed down, and then release it.

#### Signs

Some signs are used to inform the users to pay more attention to some operations:



Note: warn the user of the events which should be care.



Tip: some additional information about the current operation.

## Chapter 2. Product introduction

### 2.1. Overview

What's the <Active Wall>? It's a professional network monitoring and filtering software, which supports all kinds of network topology. It can be used without installing any client applications. It can log all the communication activities of computers in LAN, including emails, web-surfing, FTP file transferring, and the instant messenger chatting. It can control all the users in LAN to visit the defined network resources by the defined rules.

By the use of the most up-to-date network technology, <Active Wall> can monitor and authenticate all the network communications in LAN. The main features are shown below:

1. User authentication:  
Only the correct account and password can enable the user to access the Internet. <Active Wall> supports various authentication ways.
2. Time filtering:  
<Active Wall> sets different time sections for different groups to access Internet in different time period.
3. Port filtering:  
Enable or disable ports will control the users to access Internet services. <Active Wall> can

effectively block the online games, chat, video or audio services which do not match the office work by port filtering.

4. Bandwidth control:  
<Active Wall> can control the flow rate of a user or a group, and set the maximum bytes which a user or a group can use in a day. This can save the band width resource and prevent some users from using high bandwidth consume applications, such as P2P tools.
5. Real-time flow rate statistics:  
<Active Wall> can demonstrate the current statistics of flow rate in various protocols, which network blocks or protocols usages.
6. MAC filtering:  
All the computers in LAN can be bind with MAC and IP address. <Active Wall> can prevent the IP address illegal usages by using MAC filtering.
7. IP filtering:  
By setting up a blacklist, <Active Wall> can help the administrators filter and block defined IP addresses from the outside. Therefore, the users in LAN will not be able to visit the sites or hosts in the IP blacklist.
8. DNS filtering:  
<Active Wall> can filter the DNS requests from the users in LAN, in order to block the DNS names used for pornography, gambling, games, etc.
9. HTTP filtering:  
By setting up a series of rules about URL, web content, post keyword or upload file, <Active Wall> can filter the web surfing from all users in LAN. Meanwhile, it can log all webs the user has visited, in case that the administrator can check them in some other day.
10. SMTP filtering:  
<Active Wall> can filter all the users' emails sent by the rules of subject, mail body, from address, to address, attachment and mail size. Meanwhile it can log the emails in order to provide the business data loss or betray with evidence.
11. POP3 filtering:  
<Active Wall> can filter all the users' emails received by the rules of subject, mail body, from address, to address, attachment and mail size. Meanwhile it can log the emails in order to provide the business data loss or betray with evidence.
12. IM filtering:  
<Active Wall> can monitor all kinds of Instant Messenger applications, Internet chat tools and P2P tools.
13. FTP filtering:  
<Active Wall> can filter the file upload or download through FTP protocols and logs the files transferred.
14. HTTPS filtering:  
<Active Wall> can filter the https protocol by IP address, server side certificate, SSL version and deny https tunnel.
15. Proxy redirect:  
<Active Wall> can build up a transparent proxy service with general proxy servers. This can enable the gateway anti-virus or anti-spam emails.
16. Log output:

<Active Wall> can save the entire network monitoring statistics and the alarm information in define folders.

17. Email alerts:

By setting a keyword, <Active Wall> can send email alerts informing users about various events.

18. Message alerts:

By setting a keyword, <Active Wall> can transmit some messages to the administrating computer when the key event happens.

19. Log database:

<Active Wall> can save the entire network monitoring statistics and the alarm information into a database, for the convenience of administration.

## 2.2. System features

1. Stronger filter engines

<Active Wall> uses the middle layer drivers developed independently as the filter engines, which are more low-leveled than other software which uses WinPCap. Because WinPCap is a protocol-type driver, it can only monitor but not block. The other software which uses WinPCap can only block TCP communications, but cannot block UDP, ICMP, IGMP data packets. It has been proved that <Active Wall> is more stable, correct and effective after working online for a long time.

2. More monitoring modes

Most similar software support the only one mode- Passby monitoring mode. Besides the Passby mode, <Active Wall> supports more modes including Gateway mode, Bridge mode and Single mode. It is recommended that the users should use the Gateway mode or the Bridge mode. When using the Passby mode, <Active Wall> can only block TCP data packets for the limit of the network topology. However, the Gateway mode or the Bridge mode enables the <Active Wall> to block all kinds of data packets.

3. Better system performance

Based on the most optimized algorithm in the filter module, <Active Wall> has better system performance than the other similar software does. <Active Wall> can support 10,000 computers surfing on net in a time. It can process over 100M packets flow rate.

4. More flexible monitoring configuration

There are more and more configurations about the web content examinations in <Active Wall>. For example, the HTTP filters enable the administrators to filter the URL, web content, post keyword, upload file and content size. The POP3/SMTP filters can filter the from address, to address, subject, mail body, attachment and mail size. At the same time, a wildcard function is invited to help the administrators with more flexible filtering.

5. More detailed logs

<Active Wall> not only logs the URL, mail subject of the users in LAN, but also saves the web contents, submit files, upload files and emails if needed. The copies saved will enable you to investigate the business privacy revelations.(simplified Chinese version only)

6. Intelligent upgrade

Similar to the anti-virus software, <Active Wall> enables automatic check for new versions on the website. Whenever a new version is detected, is download and installation is offered. And you do not need to restart the computer after the upgrade because the new version works immediately.

## Chapter 3. Install and Uninstall

### 3.1. System requirements

Hardware requirements:

	CPU: Intel x86 or compatible; 266 MHz
	Memory: 64M RAM
	Network adapter: 10~1000M Ethernet adapter
	Hard Disk: 10 MB of disk space for installation
	Display: 800*600 resolution

Software requirements:

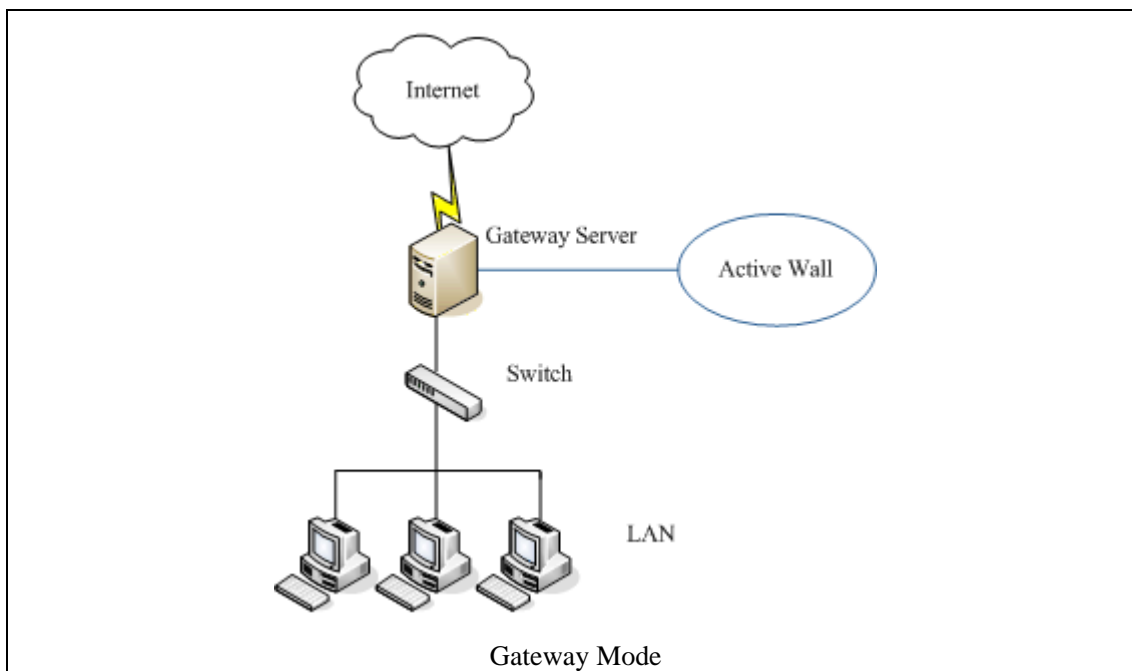
	Microsoft 32-bit Windows 2000/XP/2003 OS
	NDIS compatible driver
	TCP/IP protocols installed

### 3.2. Network environments

Gateway mode: (Recommended)

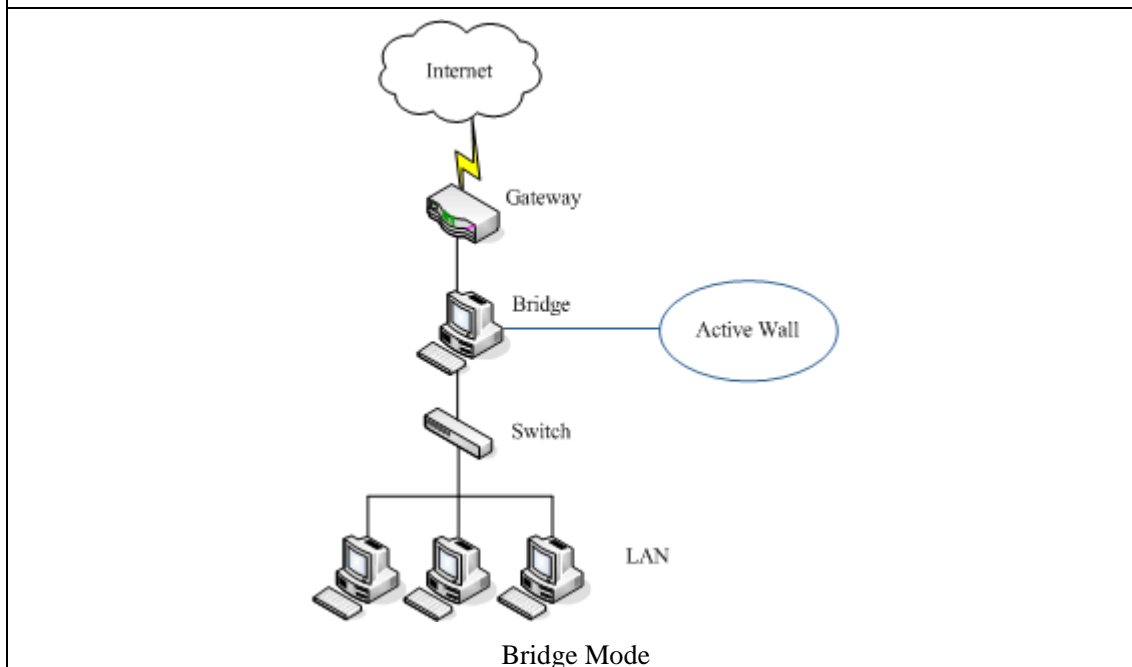
<Active Wall> are required to install on the gateway server station when using a Windows server as a gateway in LAN. It is recommended that <Active Wall> is accompanied by RRAS or ICS provided in the Windows OS.





Bridge mode:

If the gateway server is not the Windows OS, Bridge mode is recommended. In the Bridge mode, a computer with 2 net adapters should be deployed between the gateway and the switch (also connected with them). And the computer will serve as a network bridge, where <Active Wall> needs to be installed in. Please refer to [How to configure a network bridge] for more details.

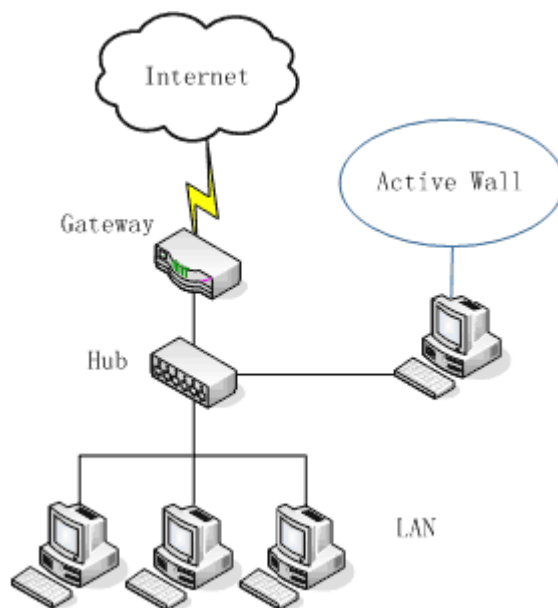


Passby mode:

Passby mode supports 4 kinds of network topology:

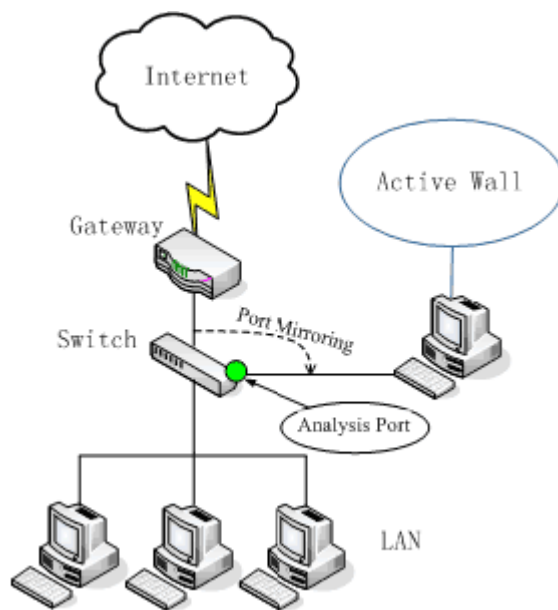
1. When the computers in LAN are connected with a shared hub, <Active Wall> can be

installed in any one of the computers.



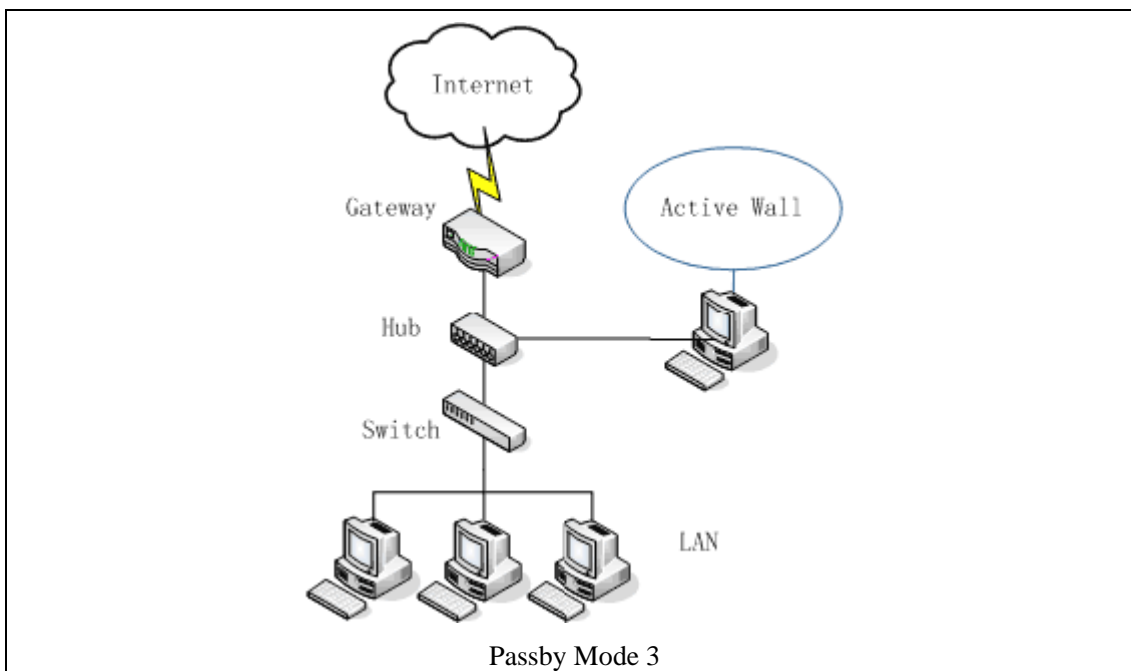
Passby Mode 1

2. When the computers in LAN are connected with a managed switch which can do mirror configurations, just configure a mirror port in the switch and connect the port to a computer which installs <Active Wall>.

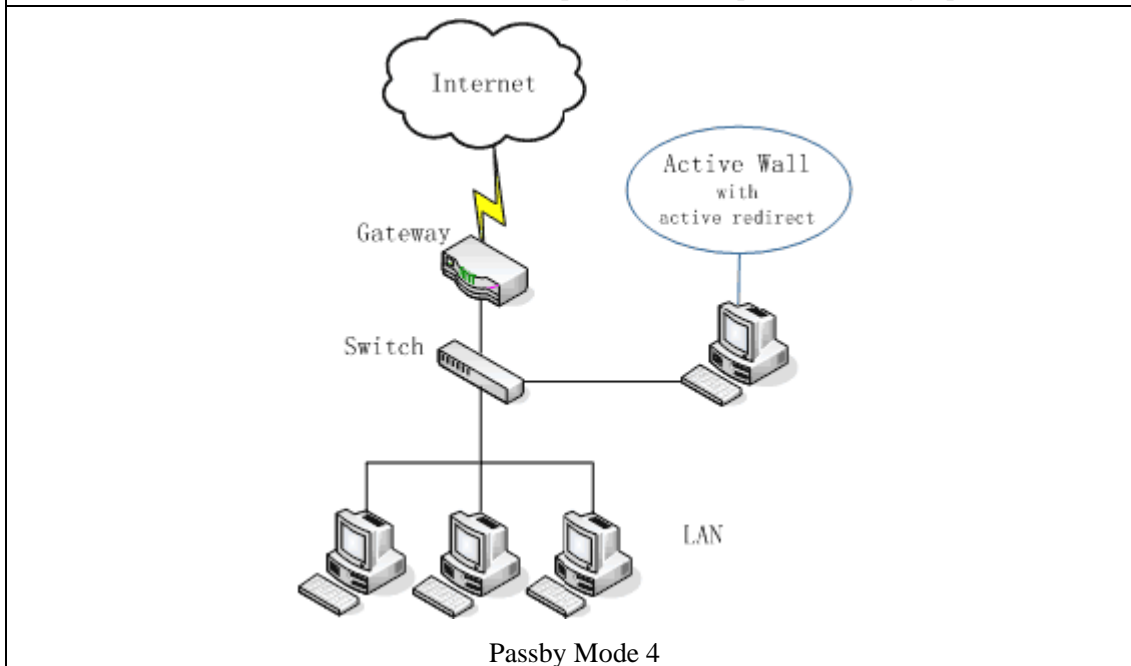


Passby Mode 2

3. When the computers in LAN are connected with an unmanaged switch which cannot do mirror configurations. You need to deploy a new hub between the gateway and the switch and connect a new computer to the hub. <Active Wall> can be installed in the new computer.



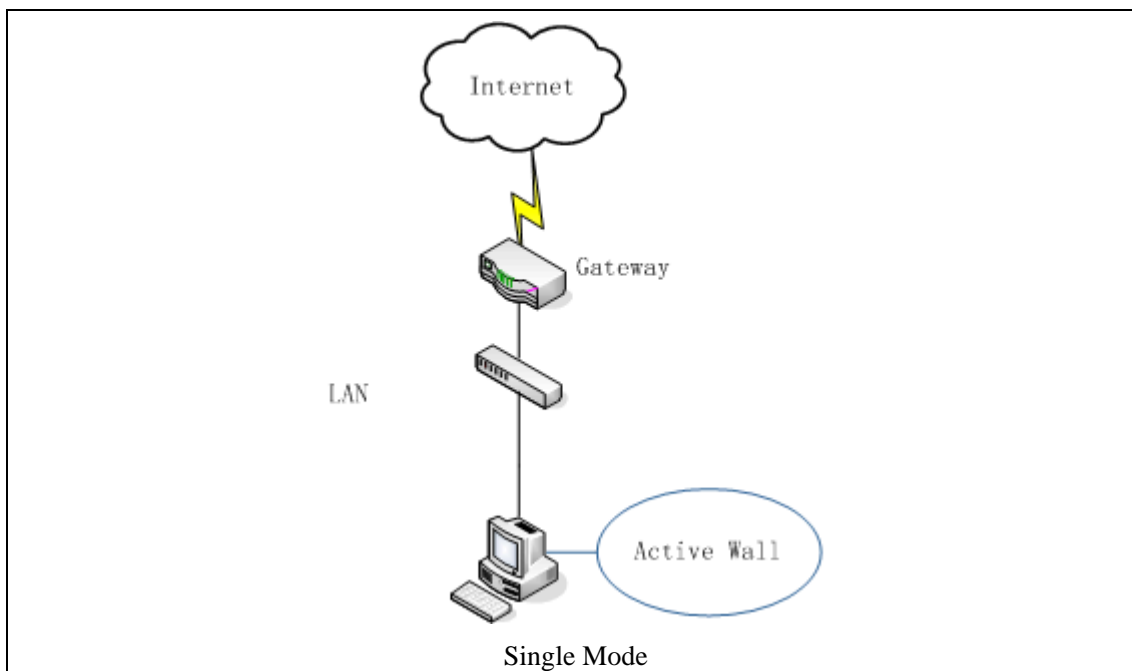
4. When the computers in LAN are connected with an unmanaged switch which cannot do mirror configurations, and if you do not deploy one more hub, you can select the Passby mode and check [Enable active redirect on passby mode] option in [Setting Option] menu.



*Note: There is some limit in Passby mode. Not all the filters can function well as usual. For details, please refer to Known problems.*

**Single mode:**

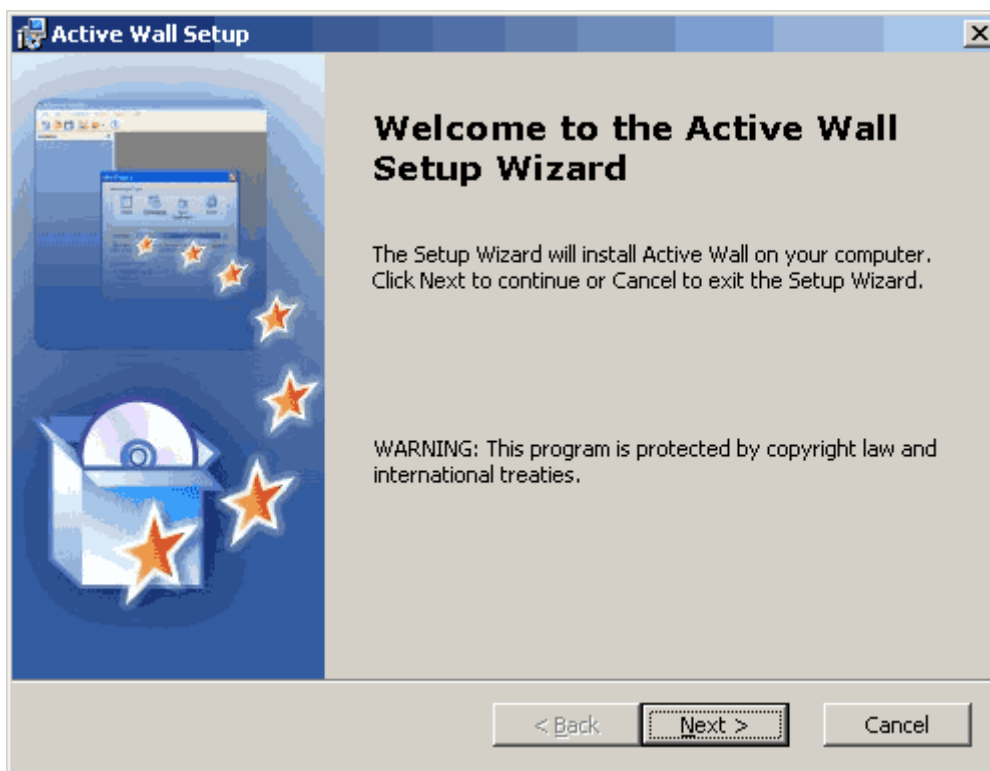
<Active Wall> can be installed in the single computer directly. All the filters will only filter the network actions of this computer.



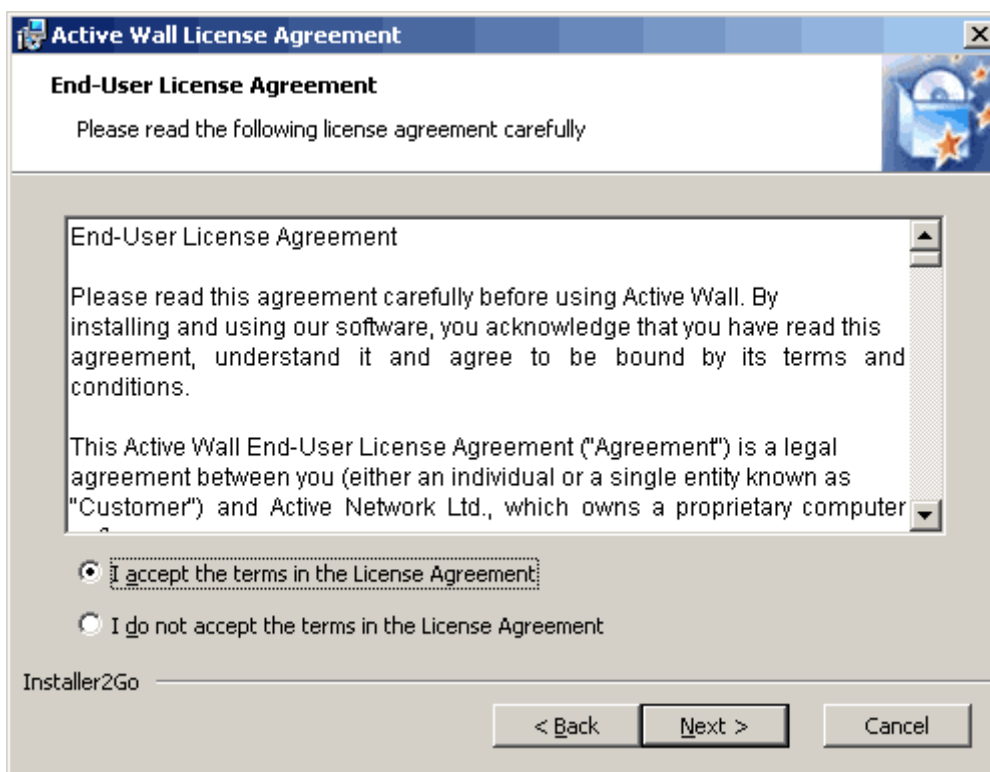
*Note: The monitor mode should be selected as a match with the current network topology. Otherwise, this software may not function well.*

### 3.3. Installation guide

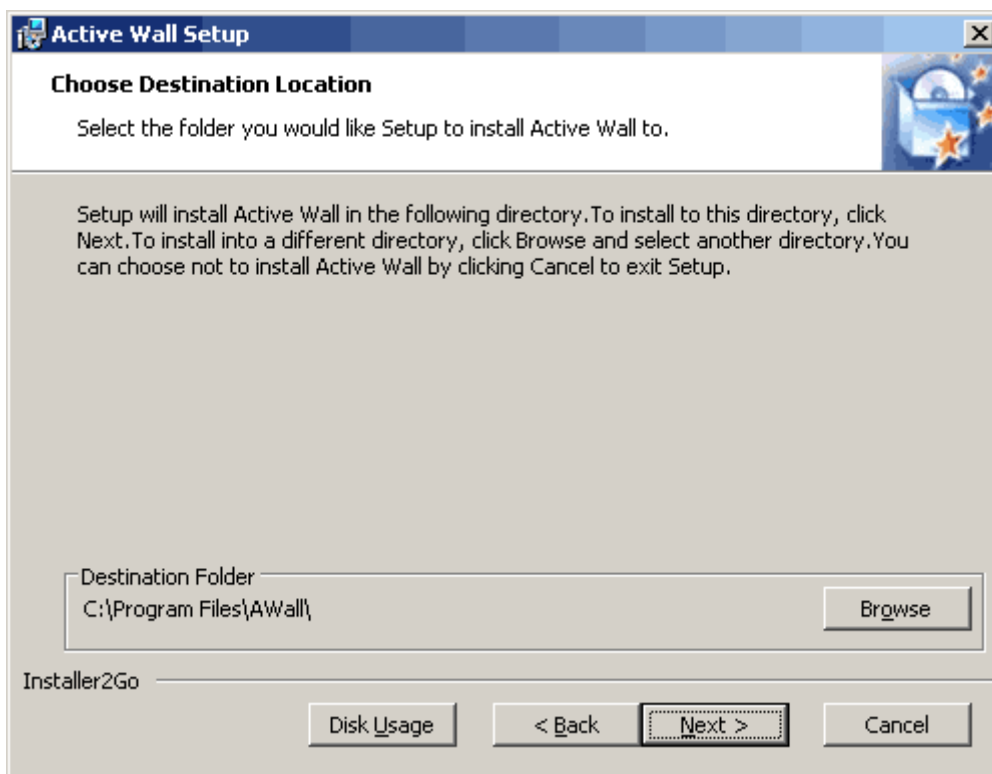
Run the installation program. Firstly you will get a welcome page. Press <Next>.



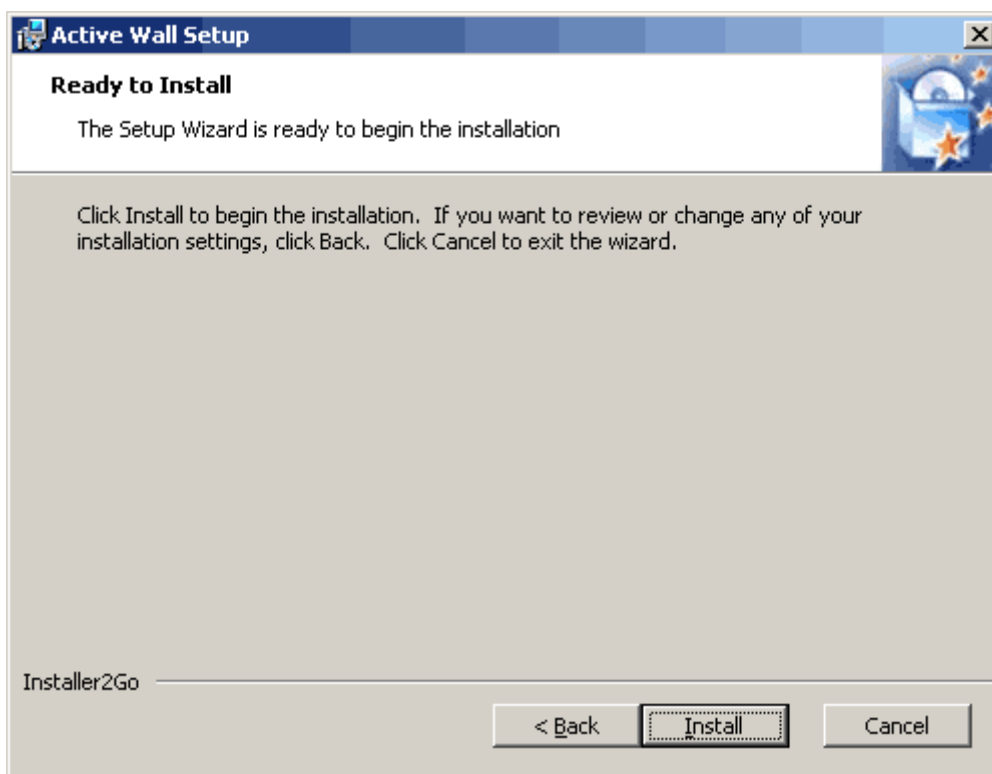
Please read the end user license agreement thoroughly. If you agree with it, please select [I accept] and press <Next>. If you do not agree, just press <Cancel>, it will terminate the installation at once.



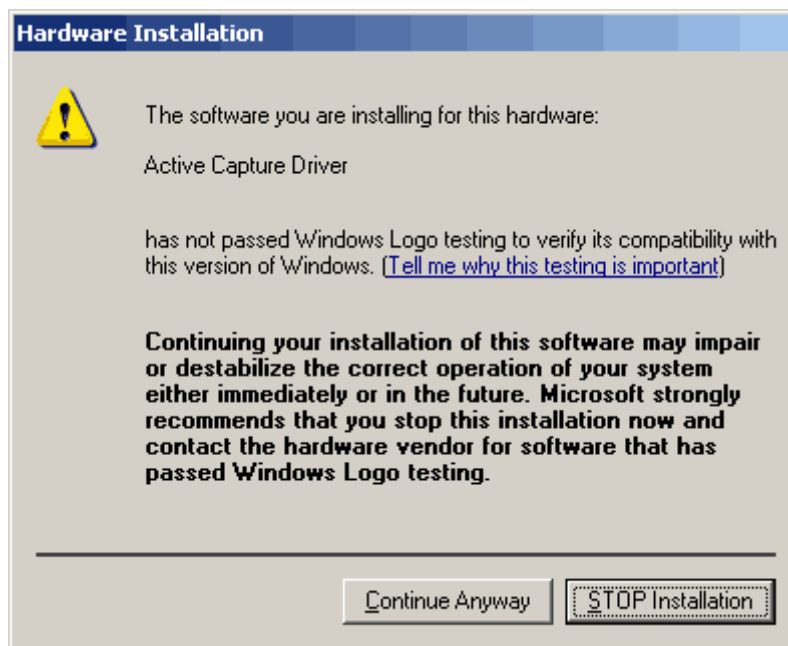
Set a path for the installation. The default path is "C:\Program Files\AWall"; other directories can also be selected by pressing <Browse>. Press <Next> after you set up the path.



Press <Install> to begin the installation.



When the installation program is copying files and installing drivers, the Windows OS may pop up a security dialog as follows. Just press <Continue Anyway>.



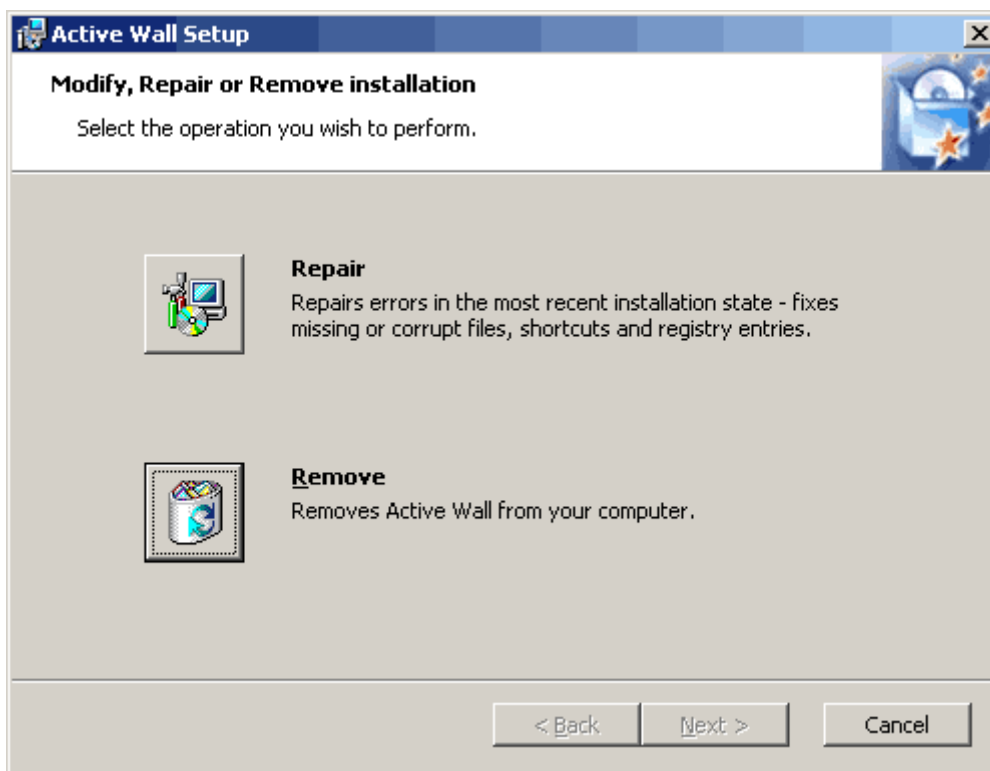
After the installation, the software will run automatically.



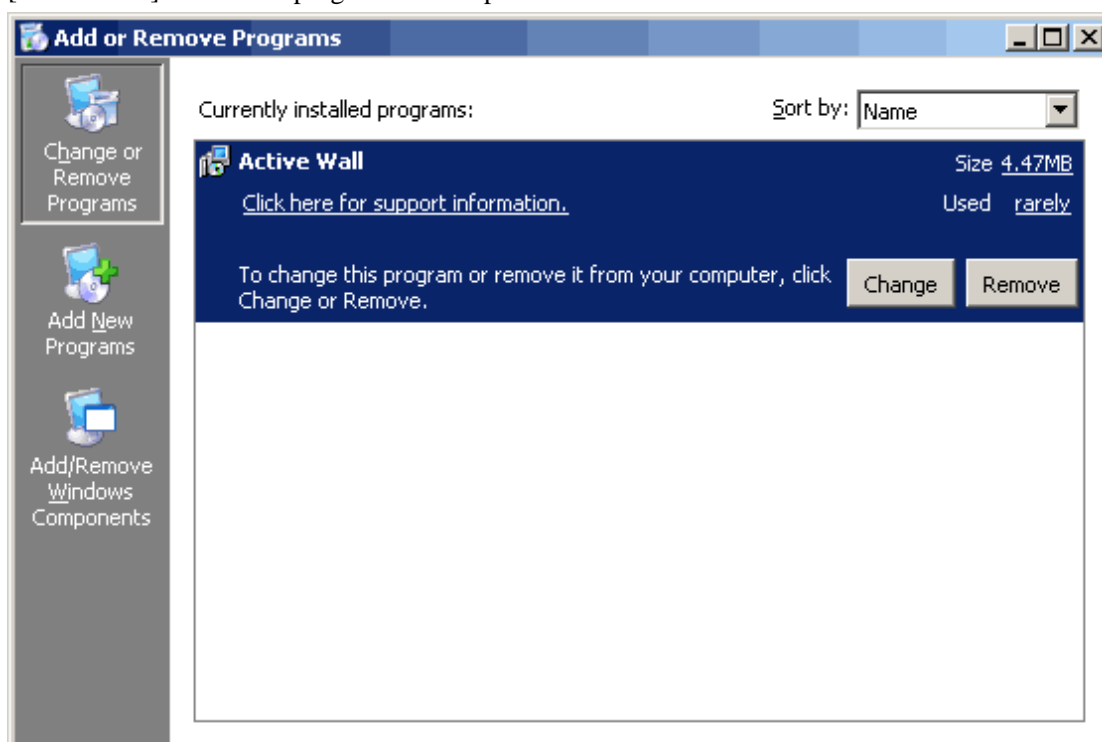
*Note: The network will be suspended for a little while during the installation. If you have some important network connections or applications, please save them before the installation.*

### 3.4. Uninstall guide

Run the installation program again. Press <Remove> to uninstall the software.



Also you can uninstall the software through Windows [Control panel/Install Remove programs]. Open the [Control panel], double click the [Install Remove programs]. Find out the [Active Wall] item in the program list and press <Remove>.



After the uninstall, please restart the computer at once.



*Note: The network will be suspended for a little while during uninstall. If you have some important network connections or*

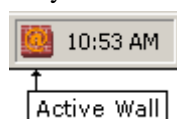


*applications, please save them before the uninstall.*

## Chapter 4. System administration

### 4.1. Getting started

After the installation, go to the Windows [Start] menu, click [Program/Active Wall/Start Service] to start this program. Active Wall tray icon will appear in the task bar:



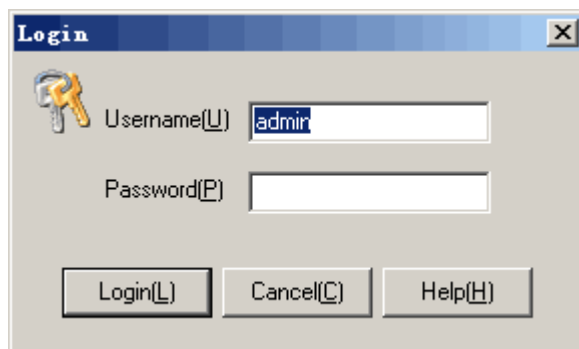
The other way to launch Active Wall is to enter "net start activewall" in the command line.



*Tip: the software is running as a service named "Active Wall" in Windows OS. And it is set to be launched automatically by default when the operating system is started.*

### 4.2. User login

Double-click the <Active Wall> tray icon in the task bar, the login dialog will be displayed.





Enter the username, password and press <Login> to authenticate. Only accountants authenticated successfully can enter the administration pages.



*Tip: Because the default account "admin" has no password set, please modify the password after the first successful login when using "admin".*

### 4.3. Start/Stop service

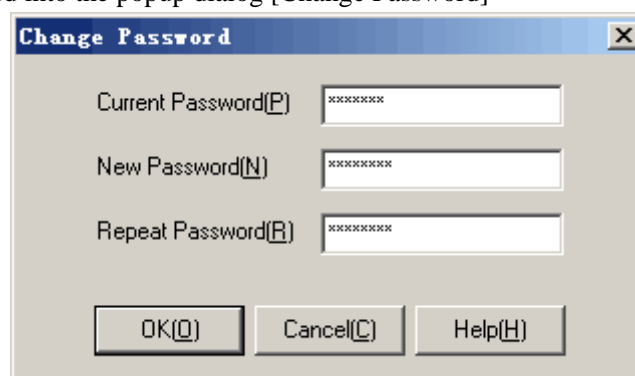
The software automatically monitors the system after starting. When you want to pause monitoring, click the menu [System/Stop service] or press the button [Stop service] . When restarting the monitoring, click menu [System/Start service] or press the button [Start service] .

### 4.4. User log out

When the user finishes the operation, the user should log out of the software by clicking the menu [System/Log Out]. After the user logs out, the program does not exit but goes into the task bar.

### 4.5. Modify password

The administrator password can be modified. Click the menu [System/Change Password], enter a new password into the popup dialog [Change Password]



### 4.6. Exit the program

Click the menu [System/Exit System] to exit the program. Or click [Program/Active Wall/Stop Active Wall] in the Windows start menu. Or execute a command line "net stop activewall" to exit.

### 4.7. Computer management

<Active Wall> identifies each computer in LAN by a unique IP address. It can find the online computers automatically and log all the sent and received data, which will be viewed in the computer list. If the user selects [Auto Find], the software will detect all new computers' MAC

addresses and computer names, and add them into "Default" group. Here are the icons which show the computer online status:



Online and sending data



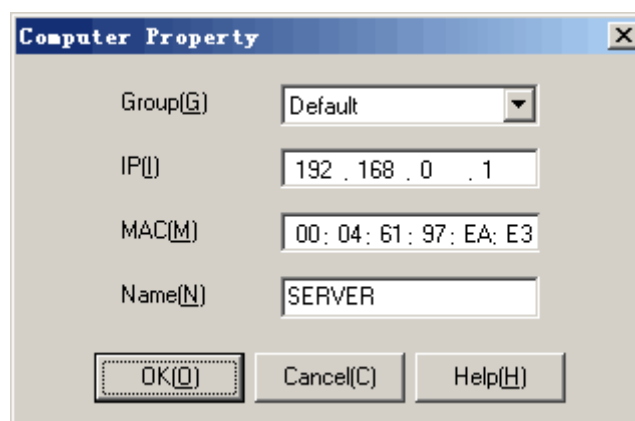
Online but sending no data



Offline, or can not be detected any data transferring in a defined time

### 4.7.1. Add a new computer

Click the menu [Computer/New Computer]. Or right click in the computer list and select [New Computer] in the popup menu. Enter the information of a new computer, and then press <OK>.



### 4.7.2. Modify a computer

In the computer list, select a computer and click the menu [Computer/Computer Property]. Or right click the computer icon in the computer list and select [Computer Property] in the popup menu. Modify the information of the computer, and then press <OK>.

### 4.7.3. Delete a computer

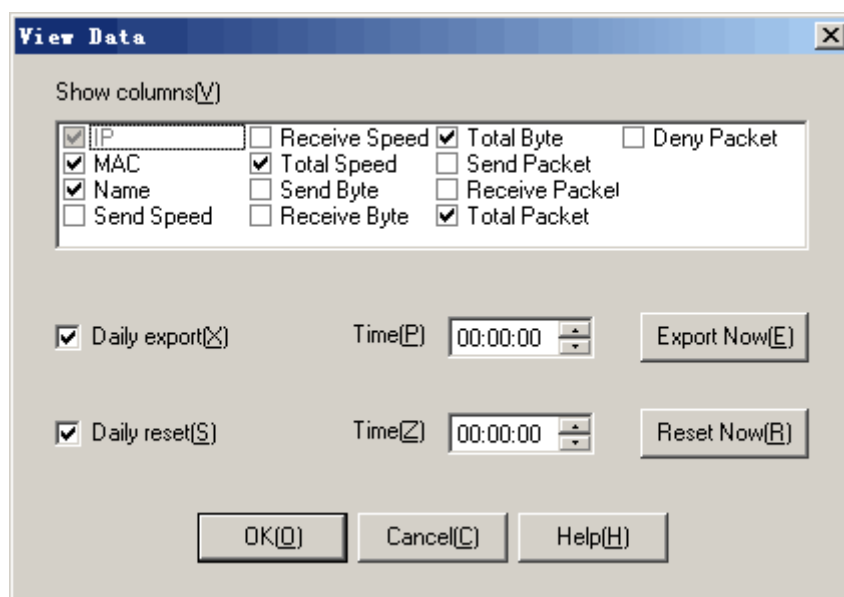
In the computer list, select a computer and click the menu [Computer/Delete Computer]. Or right click the computer icon in the computer list and select [Delete Computer] in the popup menu. You can multi-select more computers in order to delete them at one time.

### 4.7.4. View data

<Active Wall> can do data transferring statistics for each computer in LAN. It also supports a timer of exporting data.

You can choose to display the following items in the computer list, including IP address, MAC address, computer name, send speed, receive speed, total speed, send byte, receive byte,

total byte, send packet, receive packet, total packet and deny packet.



To configure the data items in the computer list, click the menu [Computer/View Data], and select the data items in the popup dialog, then press <OK>.

Export data: Press <Export Now>, fill up a file name then press <Save>. All the current data statistics will be exported into files in hard disk used to analyze later.

Reset data: Press <Reset Now> to clear all the current data statistics.

Daily export: Check [Daily export], fill up a time then press <OK>. After this setting, the system will export the data statistics at the defined time everyday. The default directory for exporting data is the "Report" directory.

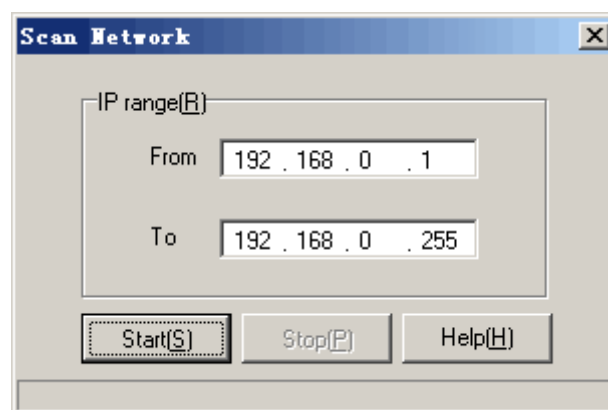
Daily reset: Check [Daily reset], fill up a time then press <OK>. After this setting, the system will reset the data statistics at the defined time everyday.




*Tip: The exported data statistics represents the current data statistics, which means the same to the data displayed in the computer list. It is recommended that both [Daily export] and [Daily reset] are checked if the user wants to do everyday statistics. What's more, the software will reset the statistics after restarting.*

## 4.7.5. Scan network

You can define a range to be scanned. The result of the computers found will be added into "Default" group automatically. Click the menu [Computers/Scan Network]. Or right click in the computer list and select the menu [Scan Network] in the popup menu. Enter the IP address range, and then press <Start>.

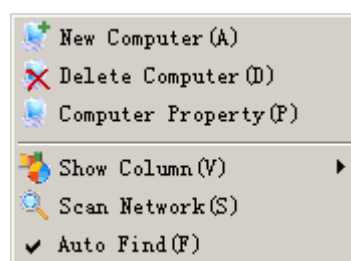


The "Scan network" function can find the computers in the same network range, including the new computer's MAC address and computer name. If it finds a new IP, it will add it into the group "Default".


 *Tip: "Scan Network" only scans the IP addresses in the same subnet. Therefore, it is recommended that "Auto Find" is enabled in case that the system gains a higher speed.*

## 4.7.6. Auto find

When [Auto Find] is enabled, the system can automatically detect the network activity, finds new computers and adds them into the group "Default". Click the menu [Computers/Auto Find]. Or right click in the computer list and select the item [Auto Find] in the popup menu. Then the menu item will be checked by a right mark which means the function is enabled. Otherwise, none means disabled. It is demonstrated as follows:



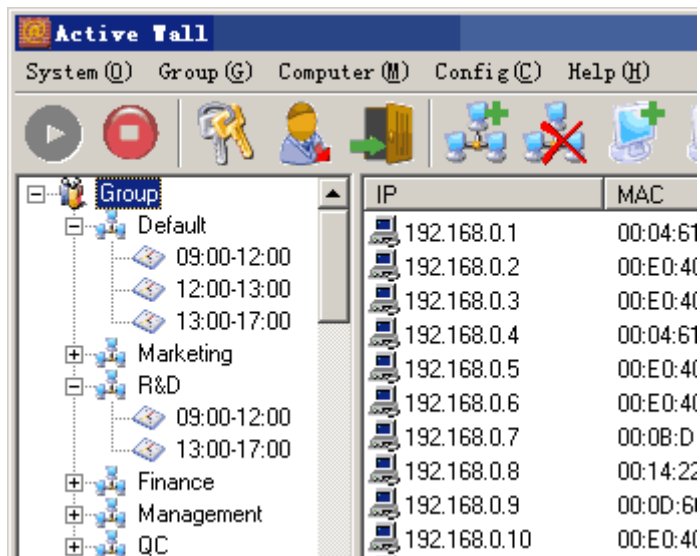
Once you enable the auto find function, new computers in the network will be found and their IP addresses, MAC addresses, computer names will be added into the group "Default" automatically. This operation is equal to the function [Config/Setting Option/Auto find computer].

 *Tip: After a successful installation, the [Auto Find] function is enabled by default.*

## 4.8. Group management

Computer groups are used to manage each computer. The administrator can configure various

monitoring policies on various groups. When selecting a defined group in the group list, the computer list will display all the computers in that group.



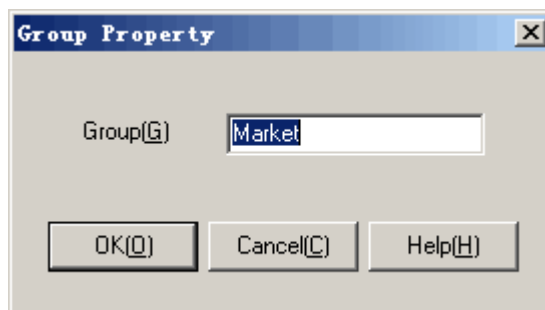
After a successful installation, the system will create a "Default" group, which cannot be modified or deleted by anyone. All the computers found or detected by the scanner will be added into the "Default" group. When you want to modify the group property of a computer, just drag the computer icon into a new group and drop it.



*Tip: The "Default" group includes not only the computers already defined, but also the computers unknown or not displayed. So the computers unknown will be affected by default policies in the network activity.*

### 4.8.1. Add a new group

Click the menu [Group/New Group]. Or right click in the group list and select the menu [New Group] in the popup menu. Enter a group name, and then press <OK>.




## 4.8.2. Modify a group

Select the group which you want to modify and click the menu [Group/Group Property]. Or right click in the group list and select the menu item [Group Property] in the popup menu. Enter a new group name, and then press <OK>.

## 4.8.3. Delete a group

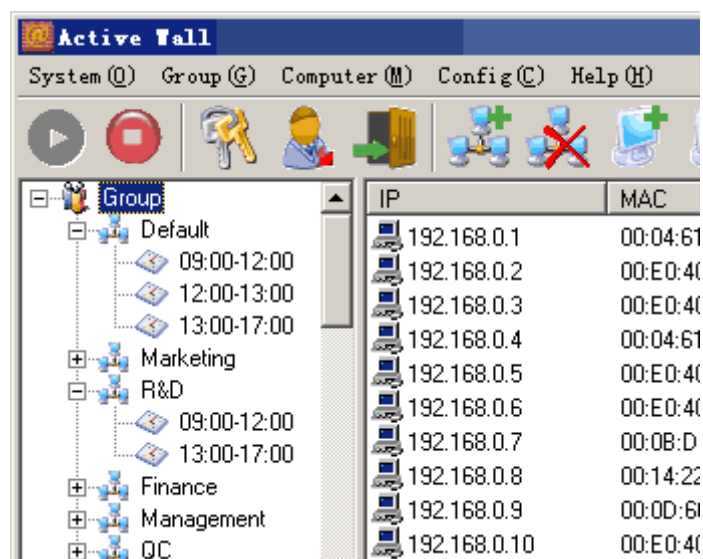
Select the group which you want to delete and click the menu [Group/Delete Group]. Or right click in the group list and select the menu item [Delete Group] in the popup menu.



*Tip: Once a group is deleted, the computers in the group will be moved into the "Default" group. However the "Default" group can not be deleted by anyone.*

## 4.9. Time range management

<Active Wall> allows the administrator to set a time period when each rule will be applied. These time ranges are actually groups that can consist of any number of various intervals and single actions.



### 4.9.1. Add a new time range

Select the group which you want to add a new time range and click the menu [Group/New Time Range]. Or right click the group list and select the menu item [New Time Range]. Enter a time range, and then press <OK>.



*Tip: A new time range will inherit the group policies once it's been created.*

## **4.9.2. Modify a time range**

Select a time range which you want to modify in the group list and click the menu [Group/Time Range Property]. Or right click the group list and select the menu item [Time Range Property]. Enter a new time range, and then press <OK>.

## **4.9.3. Delete a time range**

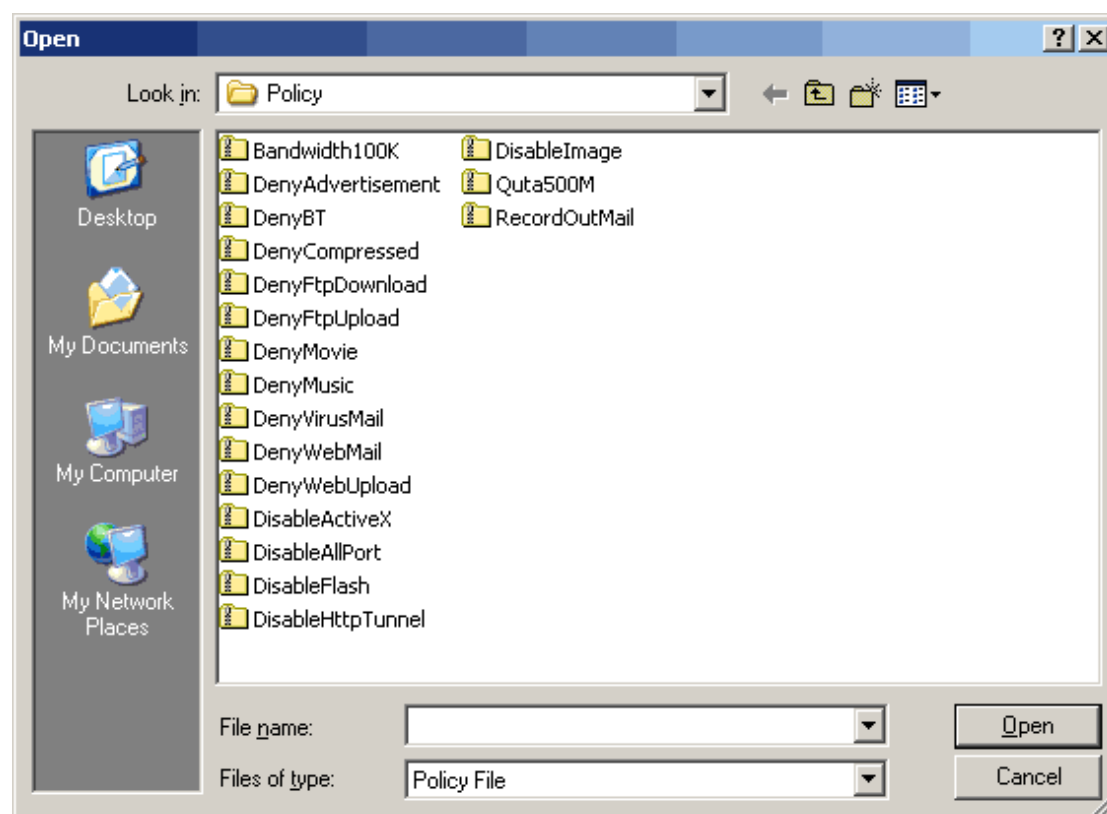
Select a time range which you want to delete in the group list and click the menu [Group/Delete Time Range]. Or right click the group list and select the menu item [Delete Time Range].


## **4.10. Policy management**

### **4.10.1. Import policy**

Select a group or a time range which you want to import a policy and click the menu [Group/Import Policy]. Or you can right click the group list and select the menu item [Import Policy]. Select a policy, and then press <Open>.

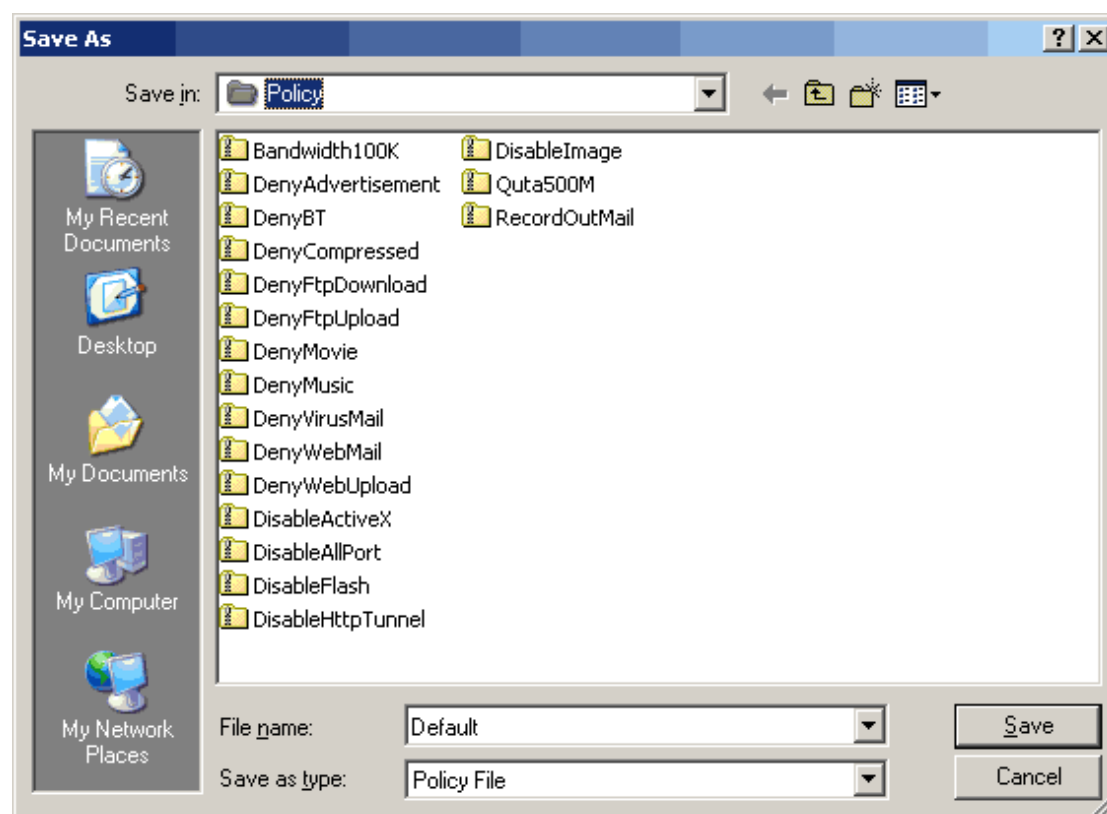




 *Tip: The new policies imported will be added into the end of the group policies. The administrator may need to configure each module and adapt a new order of the policies in order to use them. For more policies, please visit the Active Wall site.*

## 4.10.2. Export policy

Select a group or a time range which you want to export a policy and click the menu [Group/Export Policy]. Or right click the group list and select the menu item [Export Policy]. Enter a new policy name, and then press <Save>.



### 4.10.3. Clear policy

Select a group or a time range which you want to clear a policy and click the menu [Group/Clear Policy]. Or right click the group list and select the menu item [Clear Policy].



*Note: [Clear Policy] will delete all the policies of the group/time range, and the group/time range returns to an initial state without any policies.*

## 4.11. Select a network adapter

<Active Wall> provides 4 kinds of work mode to configure, including Gateway mode, Bridge mode, Passby mode and Single mode. Select a proper mode according to the current network connection (for details, please refer to [Network environments]). Click the menu [Config/Select Adapter]. Select a proper working mode in the popup dialog [Select Adapter]. Select an adapter connected to LAN in the [MAC] list and fill in [Subnet] and [Mask]. If no LAN scope is specified, the application will detect the IP address range automatically. Finally press <OK>.



*Note: The work mode must match the current network environment. If the adapter which is used is not in LAN, the program may corrupt.*

## 4.12. Setting option

<Active Wall> provides several options to set the running program state. Click [Config/Setting Option], a dialog shows as follows:

Option instruction:

### 4.12.1. Auto start with Windows

With this option checked, <Active Wall> will start running with the Windows OS (without user authentication). Without this option checked, the administrator has to start <Active Wall> manually.

## **4.12.2. Enable active redirect on passby mode**

This option only works in the passby mode. Limited in the network topology, the passby mode may not work completely. With this option checked, the ARP spoofing function is enabled to redirect the data packets transferring in other computers in LAN. Without this option checked, no data packets will be redirected. It is recommended that the ARP spoofing function is used only in small-sized LAN, for the reason that this function does some impacts on performance of the whole network.

## **4.12.3. Auto find computer**

This option equals the menu [Auto Find]. With this option checked, <Active Wall> detects new computers automatically and adds them into the "Default" group. Without this option checked, new computers will not be added into the "Default" group, but still be affected by the "Default" group policies.

## **4.12.4. Computer idle detect**

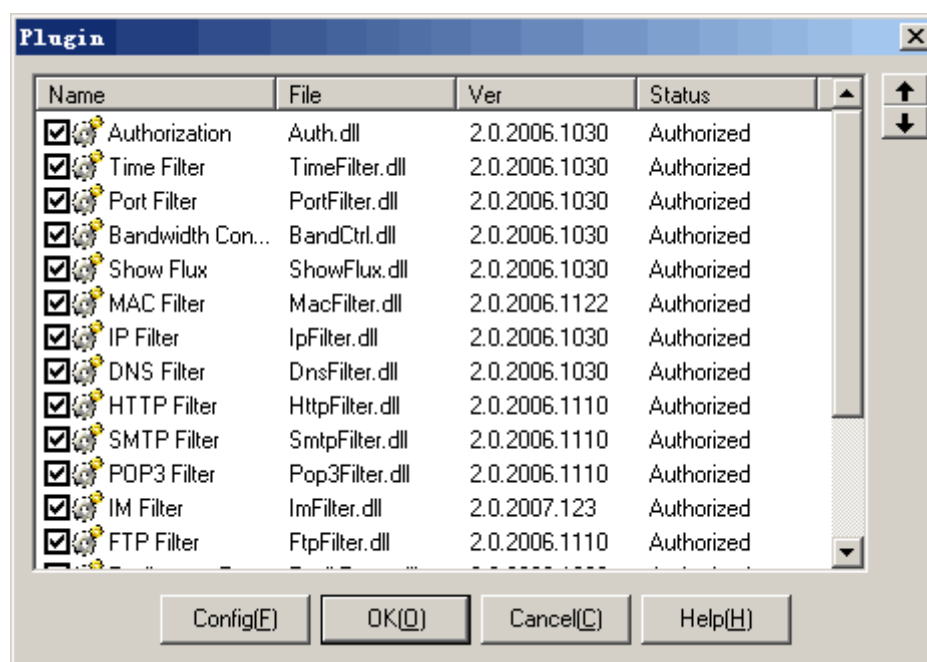
The administrator can adjust this option in order to detect the computer idle time interval. When <Active Wall> can not detect any data packets transportation in a computer in the defined time interval, this computer will be regarded as offline.

## **4.12.5. Max log in screen**

The administrator can adjust this option in order to display the lines in the log on the computer screen. <Active Wall> will rotate to show the newest events. When the log accumulates to a number, the oldest events will be removed from the list displayed.

## **4.13. Plug-in management**

<Active Wall> provides all functions in the way of Plug-ins. The administrator can load or unload some of the Plug-ins. Click the menu [Plugin List], it shows a dialog as below:



The Plug-in is loaded when it is checked, otherwise it is unloaded. The sequence of all the Plug-in modules means the sequence of all the filters which work in the program.

It is recommended that only the required modules be loaded in order to speed up the filtering performance. All the modules which are not required should be unloaded. Also the software provides an optimized sequence after a successful installation.

Select a Plug-in module and press <Config>. Or double click the Plug-in to pop up a configuration dialog. After configuration, press <OK>. The Plug-in module works immediately.

## Chapter 5. Plug-in operation

### Policy instruction

Network activity can be monitored by defining various kinds of policies. The following operations are defined in policies:

1. Pass: data packets can pass the filters, without any events logging;
2. Deny: data packets are blocked or denied to pass, without any events logging;
3. Pass Record: data packets can pass the filters, with events logging;
4. Deny Record: data packets are blocked or denied to pass, with events logging.

### Wildcard matching instruction

<Active Wall> support two kinds of wildcard: "\*" and "?". An asterisk (\*) represents any number of characters. A question mark (?) represents only one character. For example:

1. "comput\*" represents "computer" (\*=er), "computation" (\*=ation), "computing" (\*=ing).
2. "wom?n" represents "woman" (?=a), "women" (?=e).
3. "\*" and "?" can be used together. "\*.?bc.\*" matches "www.abc.com" (\*=www, ?=a, \*=com),  
www.bbc.co.uk (\*=www, ?=b, \*=co.uk).

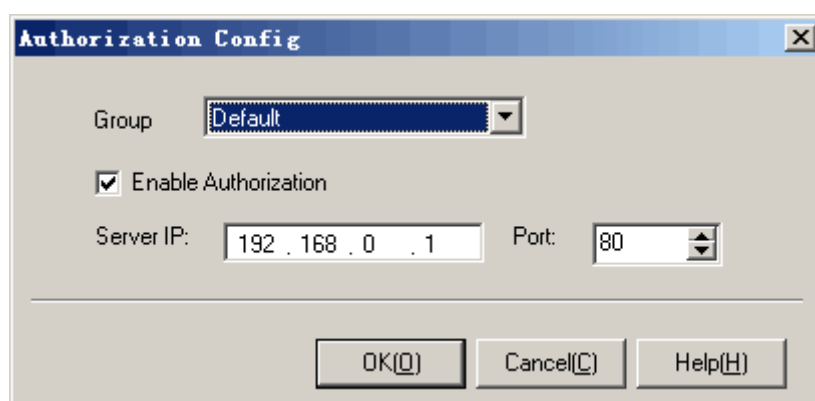
### Event log instruction

Logs are files where history of certain events performed through or detected by <Active Wall> are recorded and kept. Each log is displayed in a window in the Logs section. When the log export module and log database module are loaded, the events will be recorded in files or database. The log saved can be used for analysis later.

## 5.1. Authorization

The authorization function requests correct usernames and passwords to visit Internet. <Active Wall> supports several ways of authorization:

1. IIS based authorization, Windows integrated authorization, digest authorization.
2. Apache based, Netscape based, kinds of web servers authorizations.
3. Web page authorization like ASP, PHP, CGI, Java, .NET.
4. Customized authorization C/S based.



Operation Instruction:

1. Select a group which you want to configure in list [Group].
2. Enter the server IP address and port number.
3. Check [Enable Authorization] option, which means this group needs to be authorized; if not checked, this group do not need.
4. Press <OK> or <Cancel> to save the configuration or cancel.

Additional instruction:

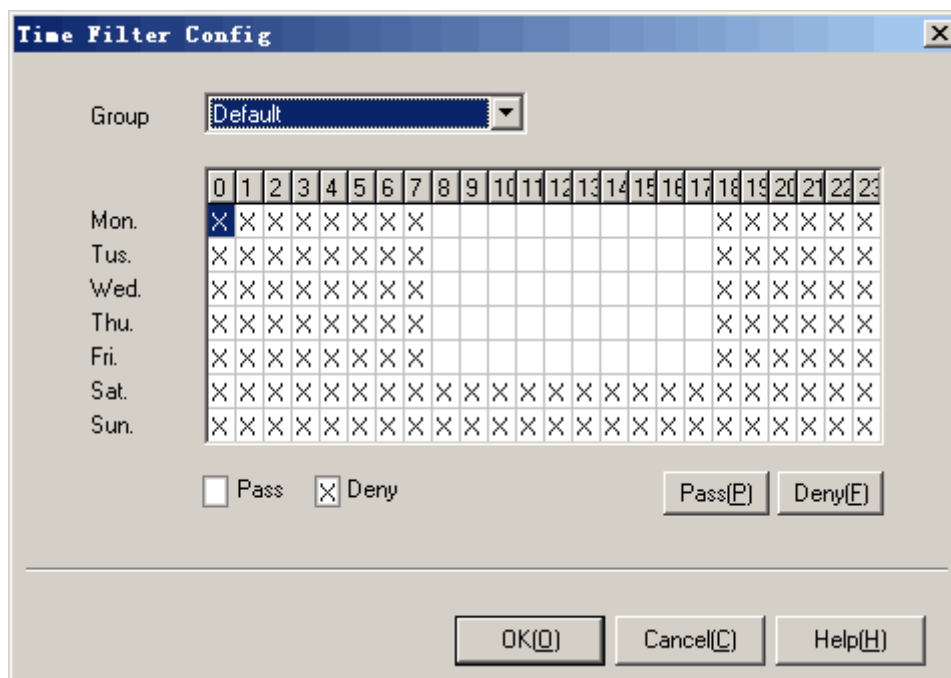
1. [Server IP]: the server's IP address which does the authorization, but it can not be 127.0.0.1, it must be recognizable by other computers in LAN.
2. [Port]: the server's port number used for authorization usually is set to 80.
3. [Server IP] and [Port] are global parameters. Once the server's IP address or port number is changed, all groups will be authorized in a new server.
4. The computers in LAN should go through the gateway configured by <Active Wall> before a successful authorization.
5. Authorization server configuration: since there are many ways of authorization, which can not be listed here, for details please visit our support forum.



*Tip: If you need web authorization, please don't use static web page in case that IE cache prevents <Active Wall> detecting correct data packets.*

## 5.2. Time Filter

Time range filter can configure time intervals in a week, a day, or an hour. Following dialog shows:



Operation instructions:

1. Select a group which you want to configure in list [Group].
2. Each rectangle in the frame means an hour in some day in a week. If you change the rectangle to an "X" by left clicking, in this hour the software will deny any Internet access. If you change the rectangle to a blank by left clicking, in this hour the software will allow Internet access.
3. Press <OK> or <Cancel>.

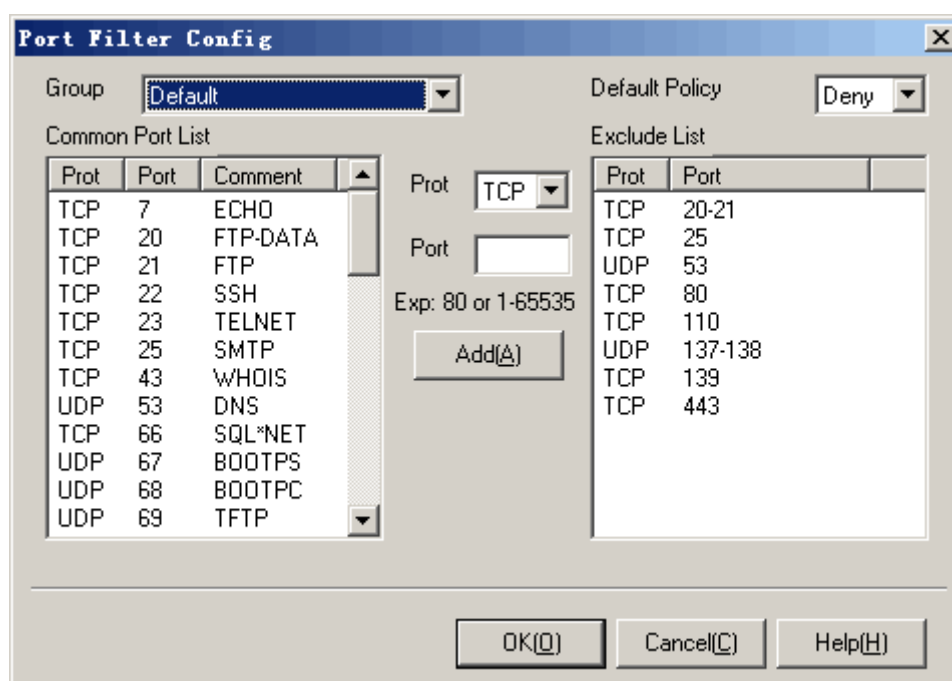
Additional instructions:

1. Time range view: the view is a rectangle frame which consists of 24\*7 rectangles. The x axis means hours, range from 0 to 23; the y axis means days, range from Monday to Sunday (ISO-8601 standards). Each rectangle in the frame means an hour in some a day. For example, (x: 0, y: Mon) means 0:00-1:00 on Monday; (x:17, y: Fri) means 17:00-18:00 on Friday.
2. Time range filtering can only restrict users with some hours during internet surfing. If you want to configure more specific policies, you can choose the time range management function.

## 5.3. Port Filter

Port filter module can open or close some ports defined, in order to pass or block some

services used by users in LAN. Following dialog shows:



Operation instructions:

1. Select a group which you want to configure in list [Group].
2. Select a default policy in the list [Default Policy].
3. In the left list [Common Port List], double click the port number then it will be sent into the right list [Exclude List].
4. If there is no port you want to select, please select a protocol type in the list [Prot]. Then enter a port number in the text box [Port]. Press <Add> to add the customized port into the right list.
5. In the right list [Exclude List], select a port or several ports and right click the mouse. In the popup menu, click the menu [Delete] to delete the ports.
6. Press <OK> or <Cancel>.

Additional instructions:

1. If [Default Policy] is "Deny", the ports in the list [Exclude List] are "Pass". If [Default Policy] is "Pass", the ports in the list [Exclude List] are "Deny".
2. When adding some ports, if the ports are in the same protocol and sequential, the software will combine them into a port range.



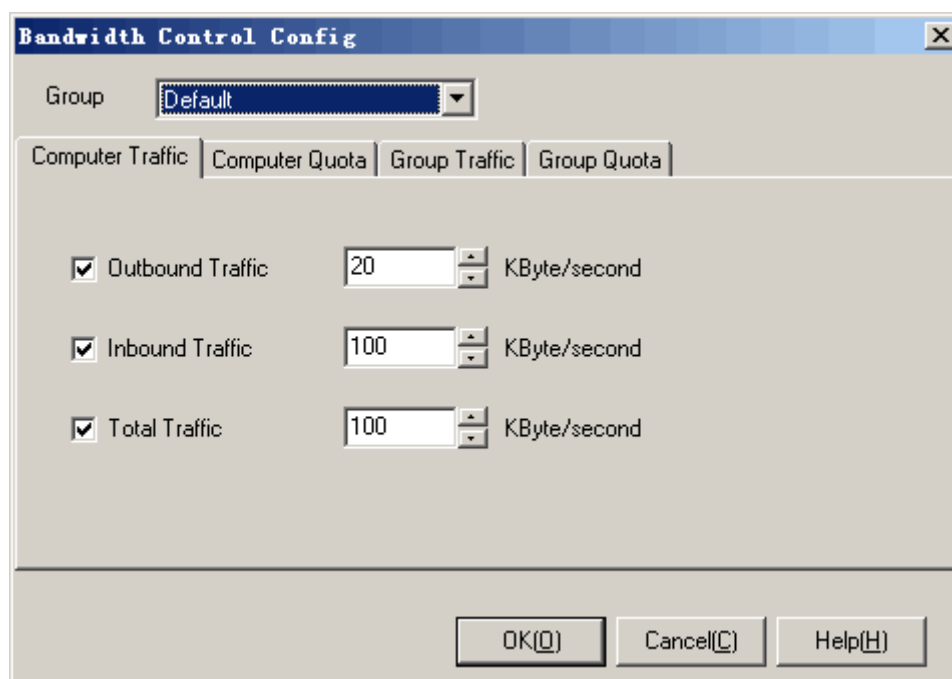
*Note: UDP Port 53 is used for DNS service. When it is blocked, some other services may work abnormally.*

## 5.4. Bandwidth Control

The bandwidth control module is used to control the transportation speed of each computer in LAN and the maximum volume of data transferring every day. Following show a [Bandwidth



Control Config] dialog:



Operation instruction:

1. Select a group which you want to configure in list [Group].
2. In the tab [Computer Traffic]: limit each computer in the selected group with bandwidth. Enter a digit in each blank to limit the inbound, outbound and total traffic.
3. In the tab [Computer Quota]: limit each computer in the selected group with quota in a day. Enter a digit in each blank to limit the inbound, outbound and total quota.
4. In the tab [Group Traffic]: limit the group with bandwidth which is the total of bandwidth of all the computers in the group. Enter a digit in each blank to limit the inbound, outbound and total traffic.
5. In the tab [Group Quota]: limit the group with bandwidth which is the total of quota of all the computers in the group in a day. Enter a digit in each blank to limit the inbound, outbound and total quota.
6. Press <OK> or <Cancel>.

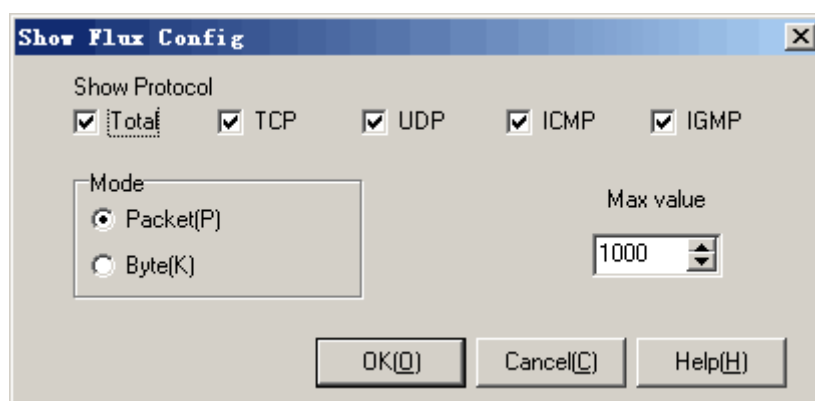
Additional instruction:

1. Bandwidth: Unit KB/s, network transportation speed.
2. Quota: Total volume of data every day, Unit MB/day.
3. Outbound: Data transferred from LAN to Internet.
4. Inbound: Data received from Internet to LAN.
5. Total: The sum of outbound and inbound.
6. The bytes here include not only the TCP, UDP contents, but also Ethernet headers, IP headers and TCP headers.

## 5.5. Show Flux

The Show flux module is used to configure the view of the [Flux View]. The administrator

can select a favorite way of statistics display. Following shows a [Config] dialog:



Operation instruction:

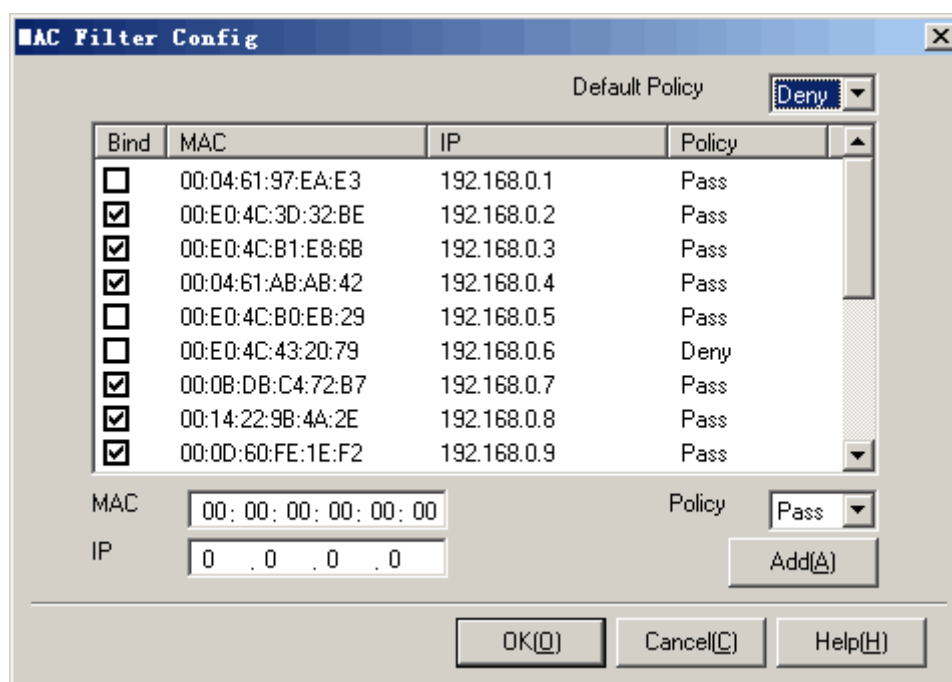
1. In the list [Show Protocol], choose which one to display.
2. In the frame [Mode], choose which unit is used for measuring.
3. In the text box [Max Value], enter a digit to display the maximum value.
4. Press <OK> or <Cancel>.

Additional instructions:

1. Total flow volume: total of all protocols.
2. TCP: total of Transmission Control Protocol.
3. UDP: total of User Datagram Protocol
4. ICMP: total of Internet Control Message Protocol.
5. IGMP: total of Internet Group Management Protocol.
6. In the frame [Mode], "Packet(P)" means flow is measured by a unit of packet; "Byte(K)" means flow is measured by a unit of byte.
7. The bytes here monitored include not only the TCP, UDP contents, but also Ethernet headers, IP headers and TCP headers.

## 5.6. MAC Filter

MAC filter can filter each computer through MAC address in LAN; can also bind one MAC address with a static IP address. Following shows a [MAC Filter Config] dialog:



Operation instruction:

1. In the option list [Default Policy], select a default policy "Pass" or "Deny".
2. In the list below, select an item which you want to modify. Right click the mouse, and then a menu shows. Press [Bind] to bind the current MAC address. Press [Unbind] to unbind the current MAC address. Press [Delete] to delete the current MAC address item. Press [Import] to import all the MAC and IP address in the computer list of the main frame.
3. Double click one MAC address which you want to modify. Edit the policy including [MAC], [IP], and [Policy], and then press <Add>.
4. If you want to add one new policy, just fill in the blanks below, including [MAC], [IP], and [Policy], and then press <Add>.
5. Press <OK> or <Cancel>.

Additional instruction:

1. [Default Policy]: it means that all the other MAC addresses which are not in the list will be served as this policy.
2. When setting "Pass" in the MAC address list, it means that this MAC is permit to pass.
3. When setting "Deny" in the MAC address list, it means that this MAC is not permit to pass.
4. [Bind] means that the selected item MAC and IP address are bind together. It will pass the match of MAC and IP address together.
5. This filter can only be used in single subnet.



*Tip: In order to ban the users modifying IP address, it is recommended to bind MAC and IP together.*

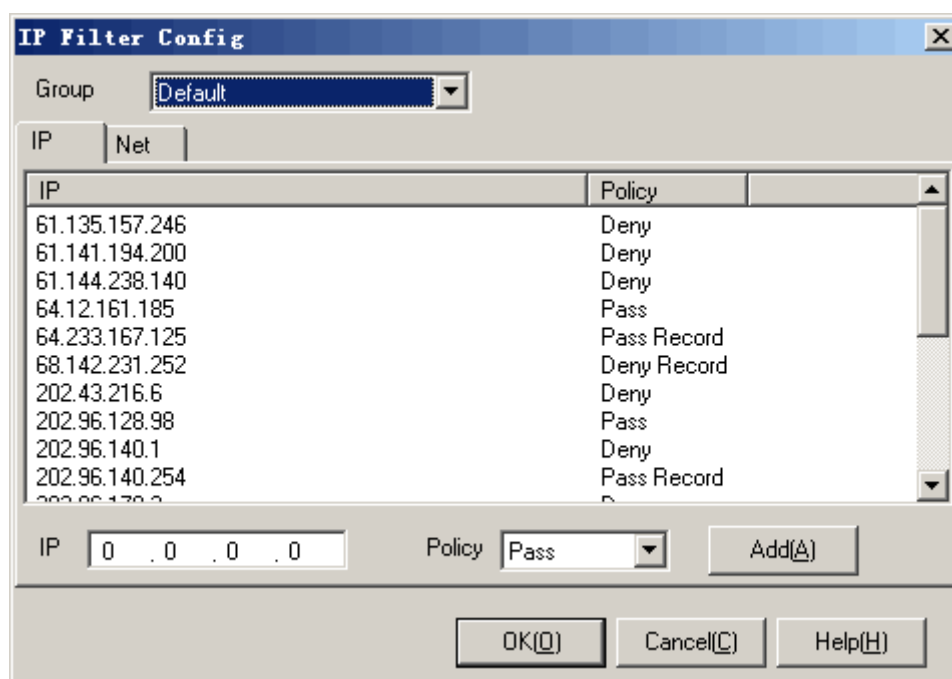


*Note: When you start a DHCP server in LAN in order to automatically dispatch the IP addresses, please set the static IP address for the*

*MAC address in the DHCP server and then start MAC-IP binding function.*

## 5.7. IP Filter

It can filter the IP destination address on the Internet which visited by users in LAN. Following shows a [IP Filter Config] dialog:



Operation instruction:

1. Select a group which you want to configure in list [Group].
2. Double click in the list, edit the content of the item, and then press <Add>.
3. Add IP filtering: select [IP] tab, input IP address, select a policy and then press <Add>.
4. Add subnet filtering: select [Net] tab, input a network number and a length of mask, select a policy, and then press <Add>.
5. Select the item which you want to modify, right click the mouse, select [Delete] in the popup menu to delete the item in the list.
6. Press <OK> or <Cancel>.

Additional instruction:

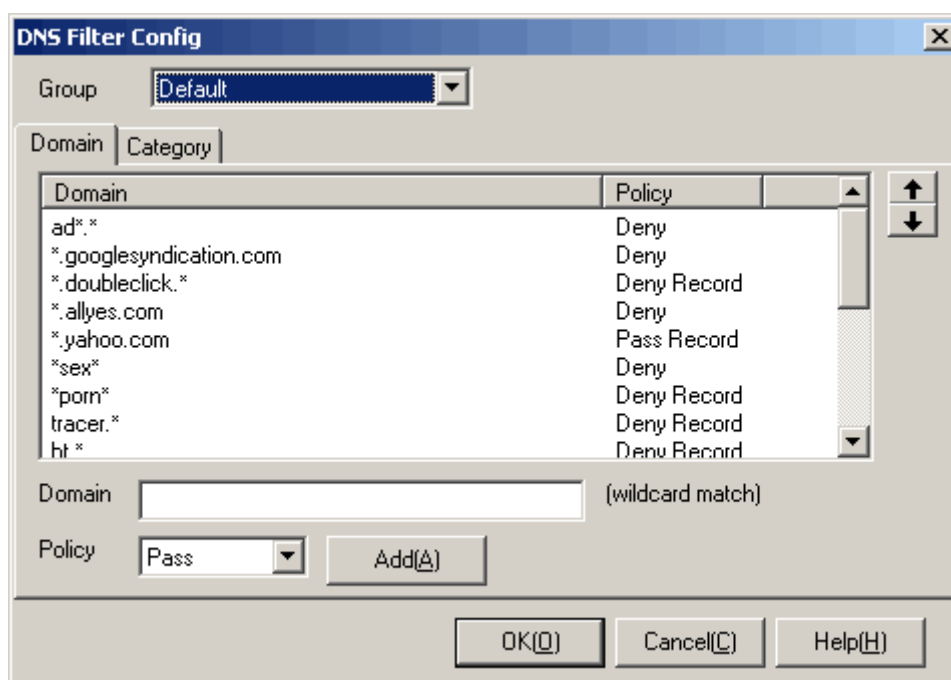
1. [Subnet]: CIDR network prefix presentation (RFC 1878) is used for recording IP address. For example, a network address 210.31.233.0, with its mask 255.255.255.0, can be recorded as 210.31.233.0/24; a network address 166.133.0.0, with its mask 255.255.0.0, can be recorded as 166.133.0.0/16; a network address 192.168.0.0, with its mask 255.255.255.240, can be recorded as 192.168.0.0/28, etc.
2. The order of IP/Net filtering is from narrow to wide range. For example, IP "61.141.238.1" policy is "Pass", and subnet "61.141.238.0/24" policy is "Deny", which means that the only IP "61.141.238.1" can be passed in the subnet "61.141.238.0/24", all the other IP addresses are denied.



*Tip: All the IP and subnet mentioned in this filter are address or site on the Internet, not in LAN. For LAN IP filtering, please deliver them to different groups and set policies in the main frame.*

## 5.8. DNS Filter

The DNS filter module can filter all domain required in the Internet by computers in LAN. Following shows the dialog [DNS Filter Config]:



Operation instruction:

1. Select a group which you want to configure in list [Group].
2. Fill the [Domain] edit blank, select a policy, and then press <Add>.
3. In the domain list, select what you want to modify, press <Up> or <Down> to move the order of the items.
4. In the domain list, select what you want to modify, right click the mouse, press <Delete> in the popup menu to delete the item.
5. [Domain]: Input domain into [Domain] blanks, select a policy, and then press <Add>. When the computers in this group request the domain which matches this item, the policy will be applied. [Domain] filter applies wildcard match.
6. [Category]: In the category list select one item which you want to modify, select a policy, and then press <Update>. Or select an item, right click the mouse and select a policy. When the computers in this group request the domain which matches this item, the policy will be applied.
7. Press <OK> or <Cancel>.

Additional instruction:

1. [Domain]: The order of filtering is ascending. All the domain items apply wildcard match. For

example, in the first item, domain is "www.google.com", policy is "Pass"; meanwhile, in the second item, domain is "\*.google.\*", policy is "Deny", this will pass only one domain visited "www.google.com", and all the other domains "\*.google.\*" will be denied.

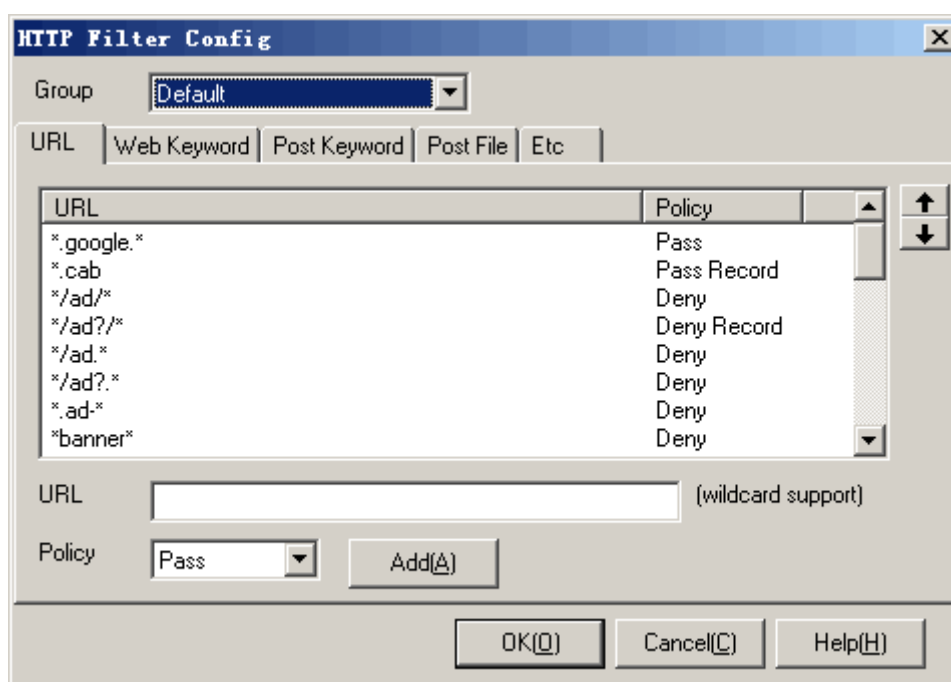
- The order of filtering is from [Domain] to [Category]. If a domain requested matches one item in the [Domain] list, the filter will not query the [Category] list.



*Tip: When querying a domain name, the computer will automatically query the DNS name list in the cache in local host. If it does not get a domain name, it will send a domain request to the Internet. If it does, it will retrieve the DNS name from cache directly. Therefore, there will be a little latency in the DNS query procedure, a new policy may not effect at once until the DNS cache expires in the computers in LAN.*

## 5.9. HTTP Filter

HTTP filter module is used for filtering HTTP, including URL, web page contents, post contents, post files and so on. Following shows a [HTTP Filter Config] dialog:



Operation instruction:

- Select a group which you want to configure in list [Group].
- Fill the edit blanks, select a policy, and then press <Add>.
- Select an item in the list, press <Up> or <Down> to adjust the order of the filters.
- Select an item in the list, right click the mouse and press [Delete] in the popup menu to delete the item.
- [URL]: Input an URL into the [URL] blank. The URL does not include a prefix "http://".

Select a policy in the [Policy] list, and then press <Add>. When the computers in this group

request an URL which matches this item, the policy will be applied. [URL] filter applies wildcard match.

6. [Web Keyword]: Input a keyword into the [Keyword] blank, select a policy in the [Policy] list, and then press <Add>. When the computers in this group visit a web page including the keyword which matches this item, the policy will be applied.
7. [Post Keyword]: Input a keyword into the [Keyword] blank, select a policy in the [Policy] list, and then press <Add>. When the computers in this group post some content including the keyword which matches this item, the policy will be applied.
8. [Post File]: Input a file name into the [File] blank, select a policy in the [Policy] list, and then press <Add>. When the computers in this group post a file through web browser which matches this item, the policy will be applied. [Post file] filter applies wildcard match.
9. [Deny http proxy tunnel]: When selecting this option, it will ban the users from using http proxy or http tunnel. Only the standard HTTP GET and POST method can pass through.
10. [Deny IP host]: When selecting this option, it will ban the users from visiting web server through IP address (for example, http://64.233.189.22), and it will only pass the URL request with domain name (for example, http://www.google.com).
11. [Output size limit]: When selecting this option, you should fill the edit blank in the same line. When it works, the exceeding bytes will be denied to post.
12. [Download size limit]: When selecting this option, you should fill the edit blank in the same line. When it works, the exceeding bytes will be denied to download.
13. Press <OK> or <Cancel>.

Additional instruction:

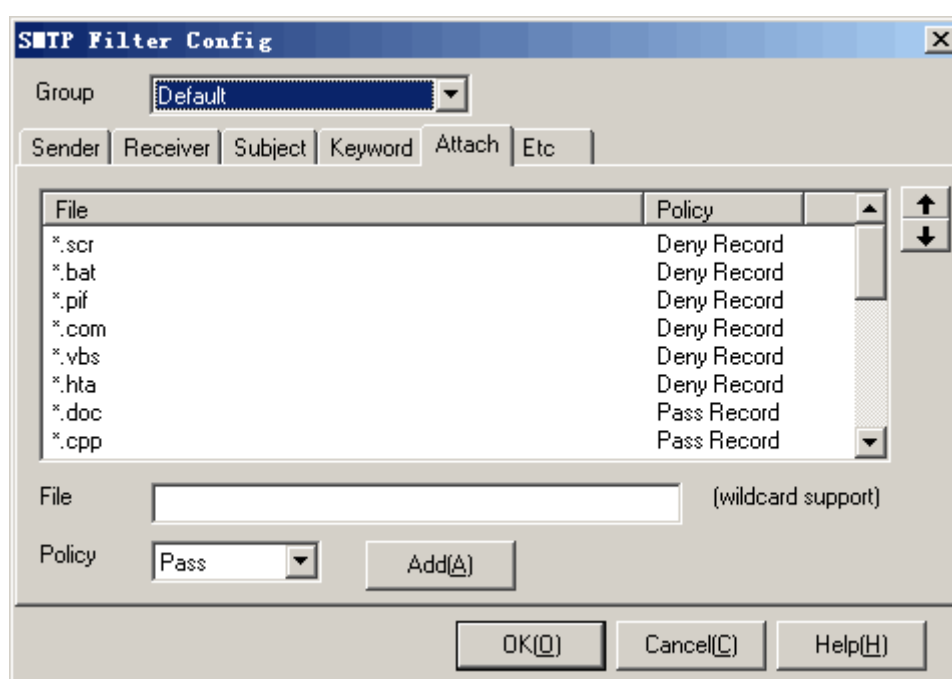
1. [URL] filters are running in the order of top-down and apply wildcard match. For example, in the first policy (URL is "admin.\*", policy is "Pass"), in the second policy (URL is "ad\*", policy is "deny"), it means that all the web sites including "admin.\*" will be passed, but all the other web sites including "ad" will be denied.
2. [Web Keyword] filters are running in the order of top-down. For example, in the first policy (keyword is "medical", policy is "Pass"), in the second policy (keyword is "sex", policy is "Deny"), it means that all the web pages including "medical" will be passed, but all the other web pages including "sex" will be denied.
3. [Post Keyword] filters are running in the order of top-down. For example, in the first policy (keyword is "contract", policy is "Deny"), in the second policy (keyword is "=", policy is "Pass Record"), it means that all the post requests including "contract" will be denied, and the other requests will be passed and record.
4. [Post File] filters are running in the order of top-down and apply wildcard match. For example, in the first policy (file name is "\*.doc", policy is "Deny"), in the second policy (file name is "\*", policy is "Pass Record"), it means all the posted files with postfix "\*.doc" will be denied, and the other files will be passed and recorded.
5. Post keyword filters only works in the "HTTP-POST" method. For "HTTP-GET" method, please use URL filters.
6. When a post filter or a URL filter works, the <Active Wall> will identify ANSI and UTF8 formats automatically.
7. When a HTTP request is transferred in one time, it may go through several filters. If one of the filters is "Deny" or "Deny Record", the connection will be terminated at once.



*Tip: Since HTTP is the most common protocol on the Internet, many software go through HTTP tunneling to contact with outside in order to transpierce a firewall. Please enable the option [Deny http proxy tunnel] to deny http tunnel.*

## 5.10. SMTP Filter

The SMTP filter module can filter all the mails sent through SMTP. This module works on sender address, receiver address, mail subject, mail main text, mail attachment and mail size. Following shows a [SMTP Filter Config] dialog:



Operation instruction:

1. Select a group which you want to configure in list [Group].
2. Fill the edit blanks, select a policy, and then press <Add>.
3. Select an item in the list, press <Up> or <Down> to adjust the order of the filters.
4. Select an item in the list, right click the mouse and press [Delete] in the popup menu to delete the item.
5. [Sender]: in the [Sender] tab, add a sender address, select a policy, and then press <Add>. When the mail's sender address matches this item, the policy will be applied. [Sender] filter applies wildcard match.
6. [Receiver]: in the [Receiver] tab, add a receiver address, select a policy, and then press <Add>. When the mail's receiver address matches this item, the policy will be applied. [Receiver] filter applies wildcard match.
7. [Subject]: in the [Subject] tab, add a subject, select a policy, and then press <Add>. When the mail's subject matches this item, the policy will be applied. [Subject] filter applies wildcard match.



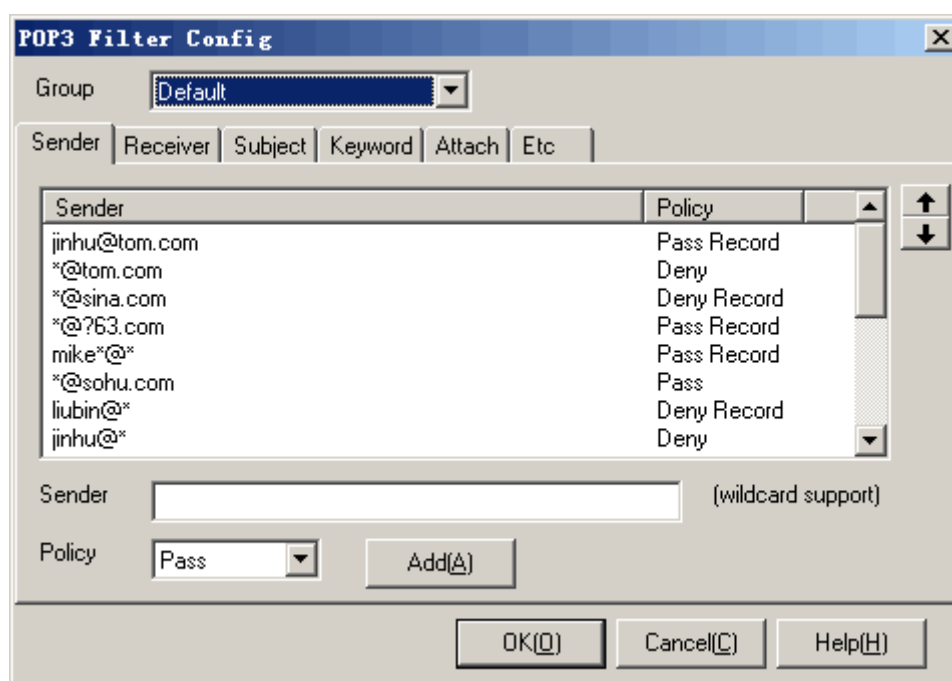
8. [Keyword]: in the [Keyword] tab, add a keyword, select a policy, and then press <Add>. When the mail's main text including the keyword matches this item, the policy will be applied.
9. [Attach]: in the [Attach] tab, add a file, select a policy, and then press <Add>. When the mail's attachment matches this item, the policy will be applied. [Attach] filter applies wildcard match.
10. [Send mail size limit]: in the [Etc] tab, when selecting this option, the user can not send a mail which has more than the limit number (Kbytes).
11. Press <OK> or <Cancel>.

Additional instruction:

1. This module works only for the SMTP protocol. If you want to filter mails through HTTP, please refer to the HTTP filter module.
2. All the following tabs are ordered top-down: [Sender], [Receiver], [Subject], [Keyword] and [Attach].
3. If a mail through SMTP protocol goes into several filters, in which only one filter's policy is "Deny" or "Deny Record", this mail will be denied.

## 5.11. POP3 Filter

The POP3 filter module can filter all the mails received through POP3. This module works on sender address, receiver address, mail subject, mail main text, mail attachment and mail size. Following shows a [POP3 Filter Config] dialog:



Operation instruction:

1. Select a group which you want to configure in list [Group].
2. Fill the edit blanks, select a policy, and then press <Add>.
3. Select an item in the list, press <Up> or <Down> to adjust the order of the filters.
4. Select an item in the list, right click the mouse and press [Delete] in the popup menu to delete

the item.

5. [Sender]: in the [Sender] tab, add a sender address, select a policy, and then press <Add>. When the mail's sender address matches this item, the policy will be applied. [Sender] filter applies wildcard match.
6. [Receiver]: in the [Receiver] tab, add a receiver address, select a policy, and then press <Add>. When the mail's receiver address matches this item, the policy will be applied. [Receiver] filter applies wildcard match.
7. [Subject]: in the [Subject] tab, add a subject, select a policy, and then press <Add>. When the mail's subject matches this item, the policy will be applied. [Subject] filter applies wildcard match.
8. [Keyword]: in the [Keyword] tab, add a keyword, select a policy, and then press <Add>. When the mail's main text including the keyword matches this item, the policy will be applied.
9. [Attach]: in the [Attach] tab, add a file, select a policy, and then press <Add>. When the mail's attachment matches this item, the policy will be applied. [Attach] filter applies wildcard match.
10. [Receive mail size limit]: in the [Etc] card, when selecting this option, the user can not receive a mail which has more than the limit number (Kbytes).
11. Press <OK> or <Cancel>.

Additional instruction:

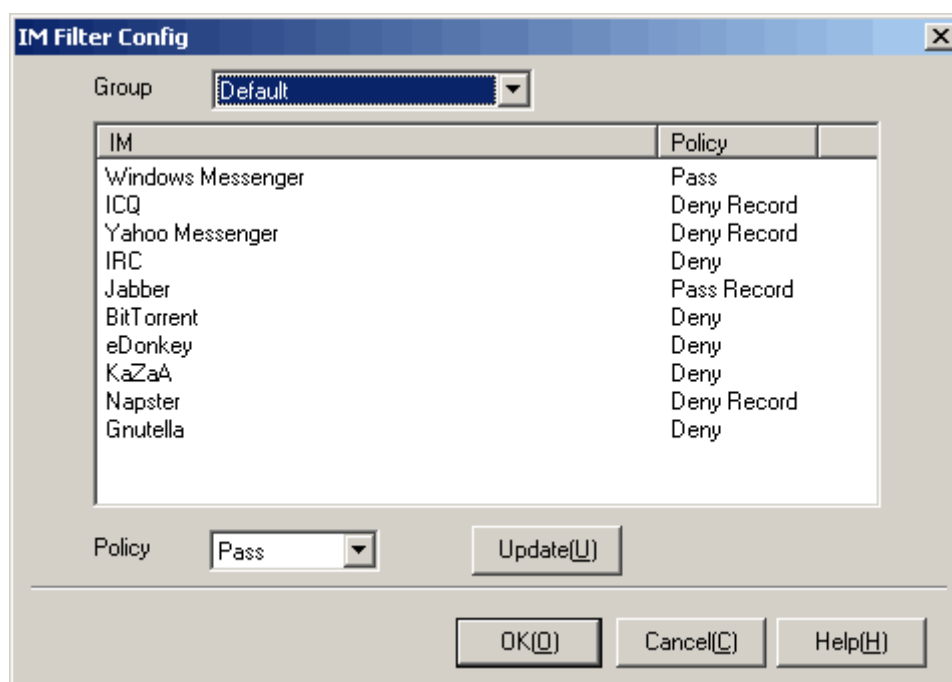
1. This module works only for the POP3 protocol. If you want to filter mails through HTTP, please refer to the HTTP filter module.
2. All the following tabs are ordered top-down: [Sender], [Receiver], [Subject], [Keyword] and [Attach].
3. If a mail through POP3 protocol goes into several filters, in which only one filter's policy is "Deny" or "Deny Record", this mail will be denied.



*Note: The POP3 filtering module will not deliberately delete the mails which are denied. Meanwhile, POP3 client software tries to receive mails ordered in a queue. This may lead to a block in the receiving procedure. When this happens, users should delete the "denied" mails manually in POP3 servers.*

## 5.12. IM Filter

The IM filter module works on IM, P2P software including MSN, ICQ, Yahoo! Messenger, IRC, Jabber, BitTorrent, eDonkey and so on. Following shows a [IM Filter Config] dialog:



Operation instruction:

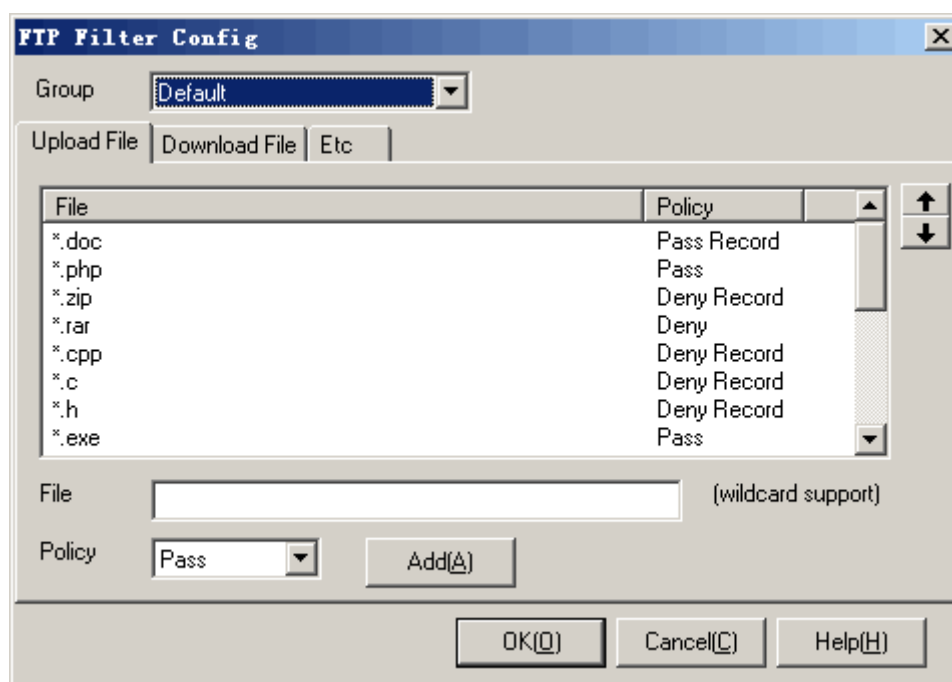
1. Select a group which you want to configure in list [Group].
2. Select an item in the IM list, select a policy, and then press <Update>. When the computers in this group use an IM software which matches this item, the policy will be applied.
3. Press <OK> or <Cancel>.

Additional operation:

1. The IM filtering module works based on server ports, domain names or IP addresses which the IM software use.
2. Many IM software support proxy or HTTP/HTTPS tunneling. In order to completely deny IM software, it is recommended that you should configure other modules with IM filter together. First, close all unused ports in Port filter. Second, enable [Deny http proxy tunnel] option in HTTP filter. Third, enable [Deny https proxy tunnel] and [Deny server without certificate] options in HTTPS filter.
3. Since the IM software upgrade gradually, this filter needs upgrading as well to filter all the IM communications.

## 5.13. FTP Filter

The FTP filter module can filter all the files transferred through FTP. This module works on upload/download file names and file sizes. Following shows a [FTP Filter Config] dialog:



Operation instruction:

1. Select a group which you want to configure in list [Group].
2. Fill the edit blanks, select a policy, and then press <Add>.
3. Select an item in the list, press <Up> or <Down> to adjust the order of the filters.
4. Select an item in the list, right click the mouse and press [Delete] in the popup menu to delete the item.
5. [Upload File]: in the [Upload File] tab, input a file name into [File] blank, select a policy, and then press <Add>. When the computers in this group upload a file by FTP which file name matches this item, the policy will be applied. [Upload File] filter applies wildcard match.
6. [Download File]: in the [Download File] tab, input a file name into [File] blank, select a policy, and then press <Add>. When the computers in this group download a file by FTP which file name matches this item, the policy will be applied. [Download File] filter applies wildcard match.
7. [Upload file size limit]: in the [Etc] tab, when selecting this option, the computers in this group can not upload a file which has more than the limit number (Kbytes).
8. [Download file size limit]: in the [Etc] tab, when selecting this option, the computers in this group can not download a file which has more than the limit number (Kbytes).
9. Press <OK> or <Cancel>.

Additional instruction:

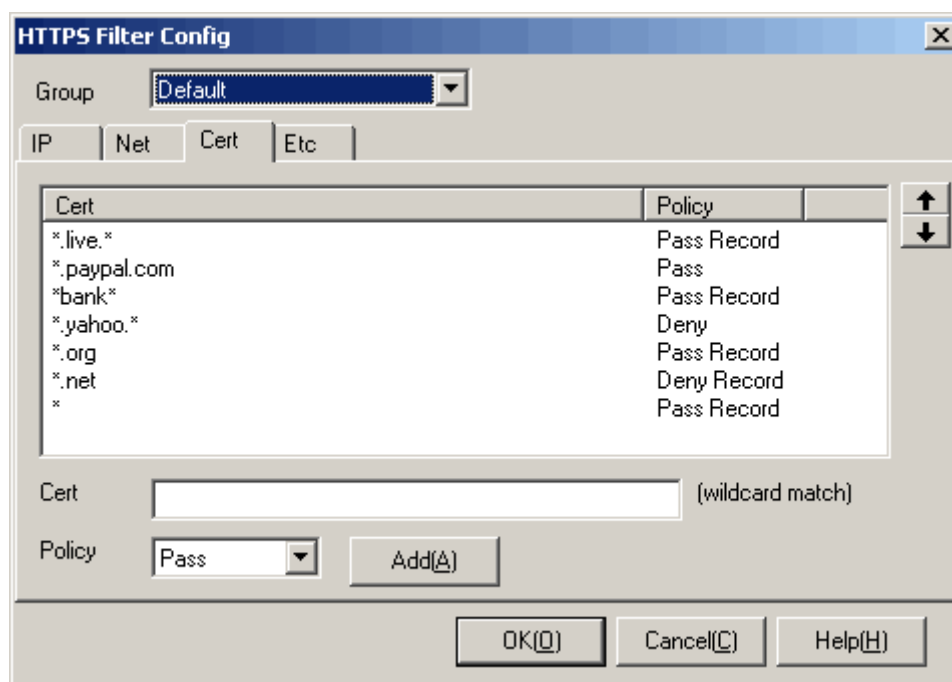
1. [Upload File]: all the filters in this module are ordered top-down. [Upload File] filter applies wildcard match. For example, the first policy (file name "\*.doc", policy "Deny"), the second policy (file name "\*", policy "Pass Record"), these mean that an upload file which has postfix "\*.doc" will be denied, but other files will be passed and recorded as events in log files.
2. [Download file]: all the filters in this module are ordered top-down. [Download File] filter applies wildcard match. For example, the first policy (file name "\*.exe", policy "Deny"), the second policy (file name "\*", policy "Pass Record"), these mean that a download file which has postfix "\*.doc" will be denied, but other files will be passed and recorded as events in log

files.

- FTP filter supports PORT and PASV mode.

## 5.14. HTTPS Filter

The HTTPS filter module is used for filtering HTTP over SSL, including IP address, net address, server side certificate, SSL version and so on. Following shows a [HTTPS Filter Config] dialog:



Operation instruction:

- Select a group which you want to configure in list [Group].
- Fill the edit blanks, select a policy, and then press <Add>.
- Select an item in the list, press <Up> or <Down> to adjust the order of the filters.
- Select an item in the list, right click the mouse and press [Delete] in the popup menu to delete the item.
- Add IP filtering: select [IP] tab, input IP address, select a policy and then press <Add>.
- Add subnet filtering: select [Net] tab, input a network number and a length of mask, select a policy, and then press <Add>.
- [Cert]: in the [Cert] tab, input a certificate into [Cert] blank, select a policy, and then press <Add>. When the computers in this group visit a server which certificate matches this item, the policy will be applied. [Cert] filter applies wildcard match.
- [Deny https proxy tunnel]: When selecting this option, it will ban the users from using https tunnel. Only the standard HTTPS protocol can pass through.
- [Deny server without certificate]: When selecting this option, it will ban the users from visiting a server which use the standard SSL protocol but has no certificate.
- [Disable SSL 2.0]: When selecting this option, it will ban the users from using SSL version 2.0 protocol.

11. [Disable SSL 3.0]: When selecting this option, it will ban the users from using SSL version 3.0 protocol.
12. [Disable TLS 1.0]: When selecting this option, it will ban the users from using TLS version 1.0 protocol.
13. Press <OK> or <Cancel>.

Additional instruction:

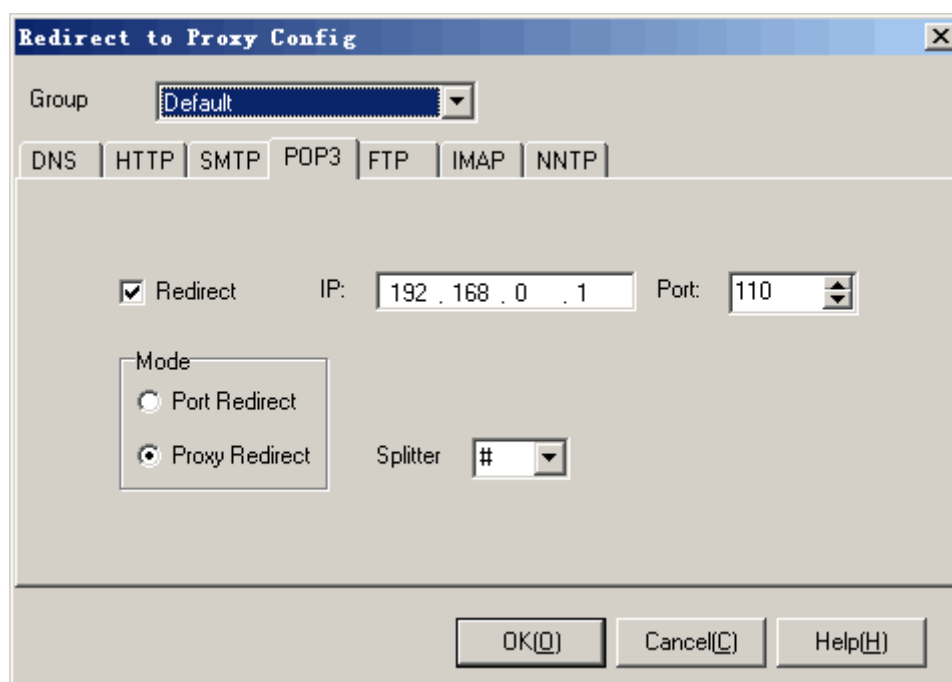
1. [Subnet]: CIDR network prefix presentation (RFC 1878) is used for recording IP address. For example, a network address 210.31.233.0, with its mask 255.255.255.0, can be recorded as 210.31.233.0/24; a network address 166.133.0.0, with its mask 255.255.0.0, can be recorded as 166.133.0.0/16; a network address 192.168.0.0, with its mask 255.255.255.240, can be recorded as 192.168.0.0/28, etc.
2. The order of IP/Net filtering is from narrow to wide range. For example, IP "61.141.238.1" policy is "Pass", and subnet "61.141.238.0/24" policy is "Deny", which means that the only IP "61.141.238.1" can be passed in the subnet "61.141.238.0/24", all the other IP addresses are denied.
8. [Cert] filters are running in the order of top-down and apply wildcard match. For example, in the first policy (certificate is "\*.paypal.\*", policy is "Deny"), in the second policy (certificate is "\*", policy is "Pass Record"), it means all the servers which certificate match "\*.paypal.\*" will be denied, and the other servers will be passed and recorded.



*Tip: Since HTTPS is the most common protocol on the Internet, many software go through HTTPS tunneling to contact with outside in order to transpierce a firewall. Please enable the option [Deny https proxy tunnel] and [Deny server without certificate] to deny https tunnel.*

## 5.15. Redirect to Proxy

This module supports many protocols: DNS, HTTP, SMTP, POP3, FTP, IMAP, NNTP and so on. This module can cooperate with other common proxy servers and implement transparent proxy service, so that there is no need for the users to configure any proxy settings. This proxy redirection module automatically transports a common proxy into a proxy application in order to implement some kinds of high-level applications: Anti-virus in the gateway, Spam mails filtering and so on. Following shows a [Redirect to Proxy Config] dialog:



Operation instruction:

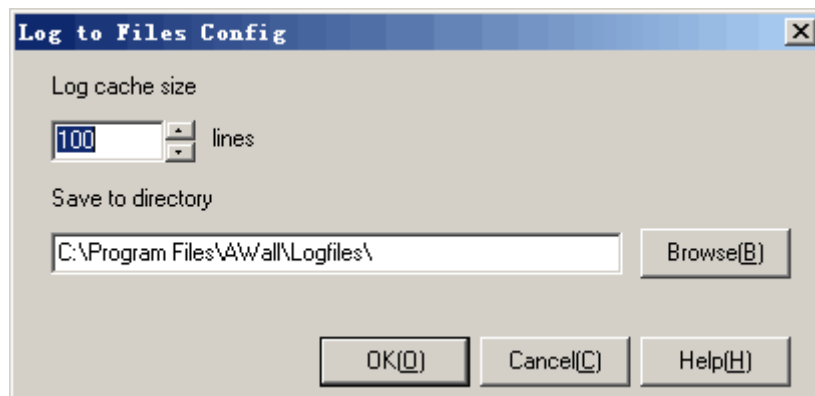
1. Select a group which you want to configure in list [Group].
2. Fill in IP address and port number.
3. In the [Mode] option, select a redirection mode. In DNS tab, there is only one [Port Redirect] option.
4. In the [Splitter] blank, select a splitter between "account" and "server". In DNS and HTTP tabs, you do not need to select [Splitter] option.
5. Please check the [Redirect] option, if you want to redirect the protocol into a proxy server.
6. Press <OK> or <Cancel>.

Additional instruction:

1. In the [IP] blank, please do not use 127.0.0.1. IP address must be recognizable by other computers in LAN.
2. [IP], [Port], [Mode] and [Splitter] are global parameters. It means that if you modify IP address, port number, redirect mode, splitter in one group, it will affect all groups.
3. <Active Wall> must locate between LAN and the proxy server. Otherwise the module does not work.
4. Redirect mode should match the proxy server configuration. Common proxy servers support proxy mode. Some transparent proxy servers can support port redirect mode, for example, http port redirection can work with SQUID transparent proxy mode.
5. Splitters should be defined according to the configuration of the proxy server. Take POP3 protocol as an instance, the original accountant is "user", pop3 server name is pop.server.com. If the proxy server defines a way that users in client should change account to user#pop.server.com, then the splitter should be "#".
6. When this filtering module starts, the client does not configure any proxy servers. This module can redirect all the data in client to proxy server in order to visit internet.

## 5.16. Log to Files

This module can export all the log files into hard disk, including all the records functioned by the policies of all the filtering modules. Following shows a [Log to Files Config] dialog:



Operation instruction:

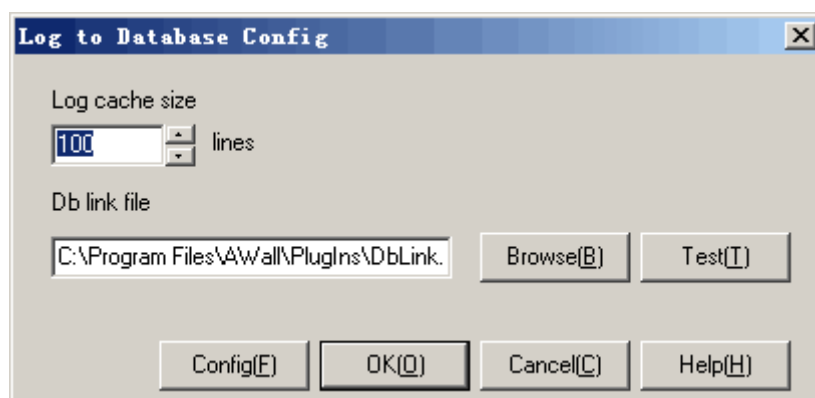
1. In the [Log cache size] blank, fill up a number.
2. Press <Browse> to direct a path where to save the log.
3. Press <OK> or <Cancel>.

Additional instruction:

1. [Log cache size]: This number represents the maximum of the event records in the cache, is 100 by default. A bigger number will cost more memory, while a smaller number will lead to low performance because of too many operations in hard disk I/O.
2. [Save to directory]: The directory is an absolute one which the log file will be stored in. This module will create a file to save the log every day.

## 5.17. Log to Database

This module works on all the records in the other filters and exports the log into a database. Following shows [Log to Database Config] dialog:



Operation instruction:

1. In the [Log cache size] blank, fill up a number.
2. Press <Browse> to direct a database link file.



3. Press <Test> to test the database link whether it works or not.
4. Press <Config> to modify the database information in UDL file.

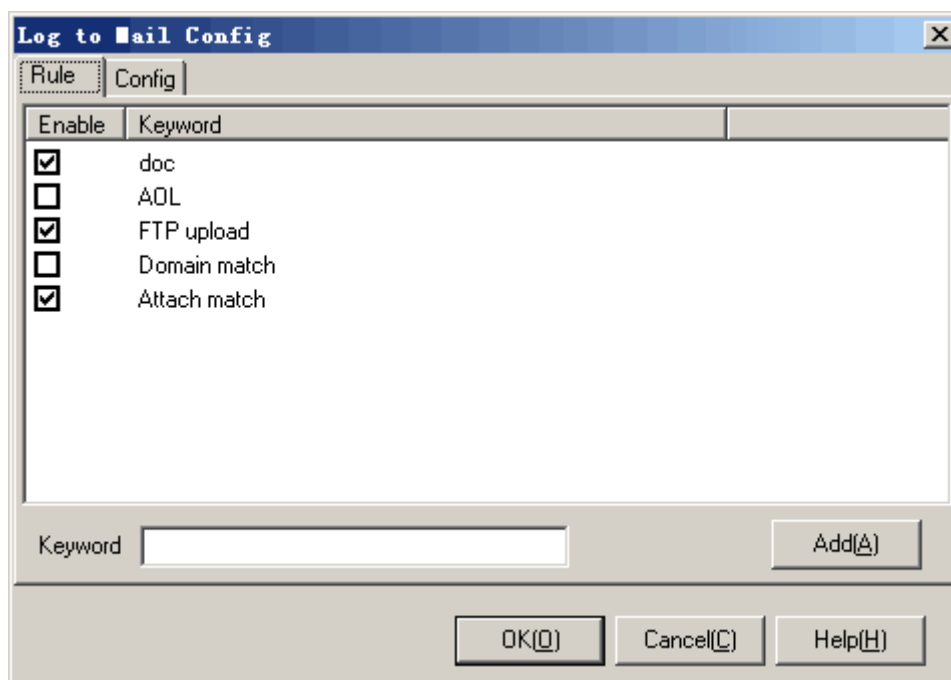
Additional instruction:

1. [Log cache size]: this number represents a maximum number how many records can be stored in cache, is 100 by default. A bigger number will cost more memory, while a smaller number will lead to low performance because of too many operations in hard disk I/O.
2. [Db link file]: UDL file is used for connecting the database. UDL is Usual Database Link file for short, which stores a string which connects the database.
3. The <Active Wall> installation has a database of Access type. Users can export to the database of Access directly, or can create a new database and modify the UDL file.
4. The following statement is used to create a database table structure:

```
CREATE TABLE [EventLog] (  
  [ID] [int] IDENTITY (1, 1) PRIMARY KEY ,  
  [EventTime] [datetime] NOT NULL ,  
  [LanIP] [nvarchar] (15) NOT NULL ,  
  [WanIP] [nvarchar] (15) NOT NULL ,  
  [PlugIn] [nvarchar] (20) NOT NULL ,  
  [Act] [int] NOT NULL ,  
  [Msg] [nvarchar] (255) NOT NULL ,  
  [Res] [ntext] NULL  
)
```

## 5.18. Log to Mail

This module can send urgent message through e-mail to a defined mail-box. Following shows a [Log to Mail Config] dialog:



## Operation instruction:

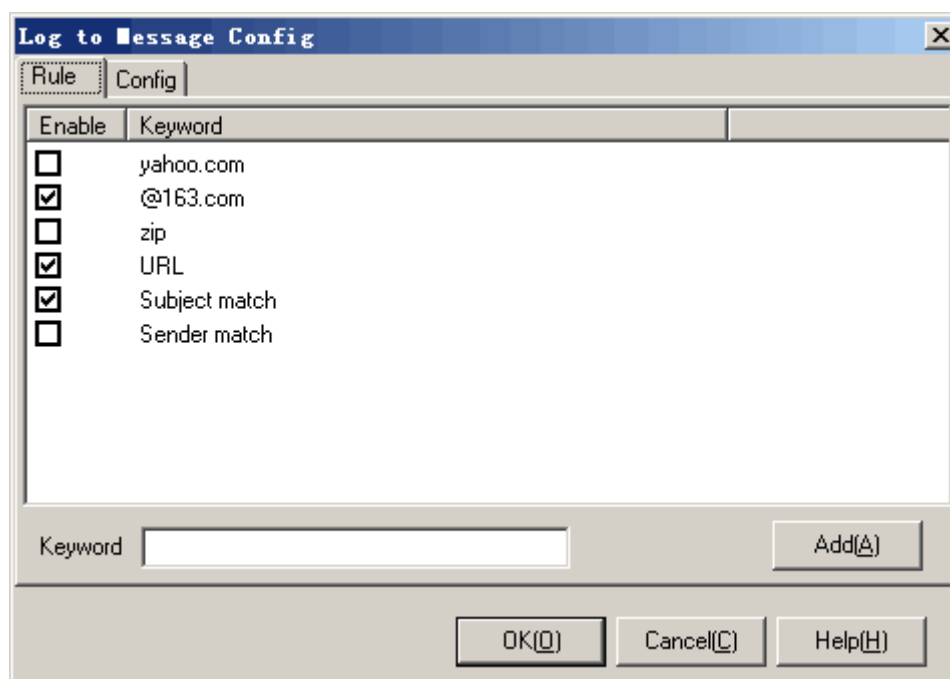
1. [Rule]: Fill in the [Keyword] blank, and then press <Add>. When the event record content includes the keyword, an email will be sent into the defined mail-box.
2. Select an item in the list, right click the mouse and press [Delete] in the popup menu to delete the item.
3. [Config]: Fill the [Config] tab with the defined mailbox address, SMTP server and so on.
4. Press <Test> to verify the configuration whether is OK or not. The verification procedure can send a test mail to the mailbox.
5. Press <OK> or <Cancel>.

## Additional operation:

1. [Mail to]: fill in a mailbox which is used for receiving alert.
2. [Send from]: fill in a mailbox which is used for sending alert.
3. [SMTP server]: server name which is used for sending mail.
4. [SMTP server requires authentication]: some SMTP servers require user authentication to send mails. If that happens, please select this option and fill in the [Account] and [Pass].
5. [Account]: SMTP authentication account.
6. [Pass]: SMTP authentication password.

## 5.19. Log to Message

This module can send urgent message through Windows messenger service to defined computers. Following shows a [Log to Message Config] dialog:

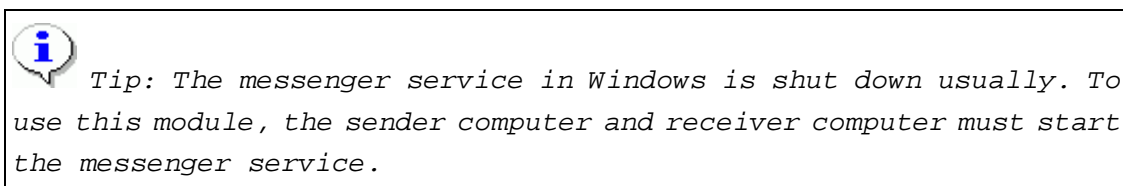


## Operation instruction:

1. [Rule]: Fill in the [Keyword] blank, and then press <Add>. When the event record content includes the keyword, a message will be sent to the defined computer.
2. Select an item in the list, right click the mouse and press [Delete] in the popup menu to delete

the item.

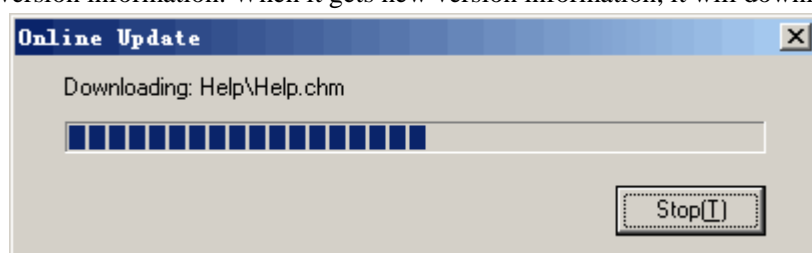
3. [Config]: fill the [Target computer] blank, with a computer which is usually the administrator.
4. Press <Test> to send a test message.
5. Press <OK> or <Cancel>.



## Chapter 6. Upgrade and Registration

### 6.1. Upgrade online

Press menu [Help/Update Online], the software automatically connects the update server and checks new version information. When it gets new version information, it will download:



The software maybe restarts to use the newest version.

### 6.2. Registration

Press menu [Help/Register Info], it shows a [Register] dialog. Unregistered user can read a serial number generated by the software automatically. Registered user can read user name, serial number, license number and register code.

Anyone who wants to purchase licenses, please contact with the local agents or our company directly.

After registering a formal user, you can do the following:

1. Encourage the author and improve the new version.
2. Authenticated to use all the functions of the software.
3. Use technological support and help from our company by Email, telephone, fax and so on.
4. For commercial use or other use.
5. Get user identification information and the other high-level functions.

## Chapter 7. FAQ

### 7.1. Frequently answered questions

#### 7.1.1. Why can't I install the software?

1. Check whether the computer hardware meets the software installation requirements. Please refer to [System requirements].
2. Use administrator account to log in and then run the installation.
3. When it shows a warning dialog while installing the software, press <Continue anyway>.
4. Check the driver signing options, please modify it to ignore or warn.
5. After uninstalling the software, it needs a restart before a new installation.

#### 7.1.2. How can I configure network adapter and work mode?

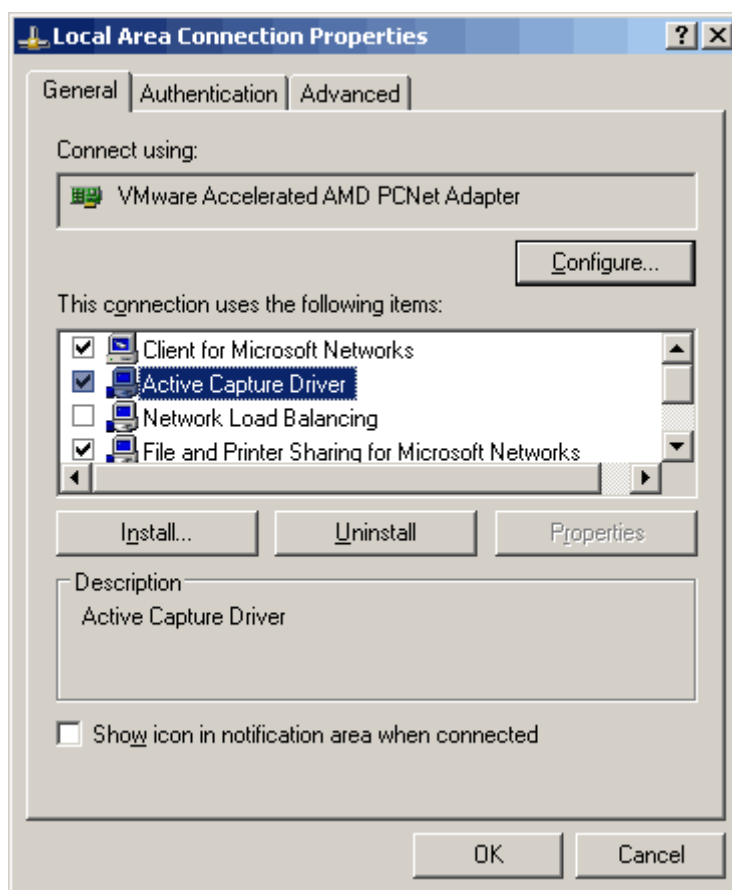
1. Please select a proper work mode according to the current network topology. Please refer to [Network environments].
2. If there is no proper mode which matches the current network topology, please modify the topology.
3. Please select a network adapter which connects the LAN. Please refer to [Select a network adapter].



*Tip: It is recommended that you select the gateway mode, because this mode is more stable and less performance-cost. And all the filtering modules can work normally under the gateway mode.*

#### 7.1.3. Why do I read an empty network adapter list?

1. Please check whether the driver is normally installed, and check the network adapter connection properties. Following shows a service:



2. Please check the [Active Capture Driver] option.
3. If there is no such [Active Capture Driver] option in the general tab, please uninstall the software and restart the system. And then install the software again. When it shows a warning dialog while installing the software, press <Continue anyway>.
4. If there is an option [Active Capture Driver] checked, please try to cancel the check and then check it again. When it shows a warning dialog while installing the software, press <Continue anyway>.

### 7.1.4. Why are there many IP addresses from outside in the [Default] group?

1. Because the user selects an improper work mode which does not match the current network topology. Please refer to [How can I configure network adapter and work mode].
2. Please try to check the correct net adapter you select for LAN connection. Refer to [Select Adapter].
3. Please try to check the IP list configured in [Select Adapter].

### 7.1.5. Does this software support multi-subnet and VLAN?

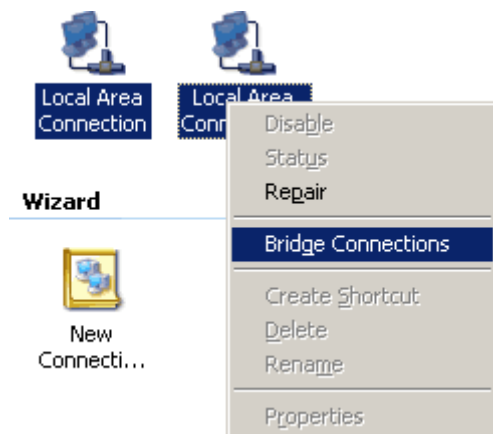
1. <Active Wall> identifies computers by IP addresses, so it supports multi-subnet and VLAN.
2. Computers in multi-subnet or VLAN communicate with each other through routers or switch, the source MAC address in the data packets will be replaced with a router's MAC address. Therefore, MAC filter module may not work in this environment.

### 7.1.6. Why can not I find Active Wall through the Microsoft Remote Desktop connection?

1. Active Wall is running as service in Windows, and only can be operated by the first local accountant (not remote).
2. Execute the command: "mstsc/console", then the user through remote connection can operate Active Wall.
3. VNC is better for remote connection, for details please go to the site: <http://www.realvnc.com>

### 7.1.7. How to configure a network bridge?

1. Open "Network neighborhood" in Windows, select two network adapters in the same time and right click, then in the pop up menu, select the option [Bridge Connections], and Windows will build up a network bridge automatically.



2. When the bridge is built up, the two adapters' IP address will disappear. Select the Network Bridge and configure a new IP address in the [Properties] menu, for LAN connections.

#### Network Bridge



3. When using a bridging mode, you need do step 1 and step2 first of all, and then install  
Active Network CO., Ltd  
Tel: +86 5782519007  
Email: support@lanctrl.com

<Active Wall>. Otherwise, the soft driver can not find a correct adapter. If you install the soft in the computer without a network bridge, please uninstall the soft and repeat step 1 and 2.

4. When completing the installation, you can find in the dialog [Select Adapter] three adapters available. Two of them are real ones for LAN connections, with IP address "0.0.0.0". The other one is a network bridge, which is a dummy. You need to select a real adapter with IP address "0.0.0.0".

## **7.2. Known problems**

### **7.2.1. HTTP filter ignores gzip webpage**

In HTTP filter module, web keyword filtering function can automatically recognize ANSI and UTF8 coding and perform keywords matching. However, the web keyword filtering is overlooked when some web servers use gzip to output compressed webpage content, which cannot be recognized by HTTP filter module.

### **7.2.2. Shortage of passby mode**

When using a passby mode in LAN. Limited with the network topology, Active Wall can not deny UDP/ICMP/IGMP packets. Several filtering modules do not work. If the option [Enable active redirect on passby mode] is checked, Active Wall will start the function ARP spoofing, which will redirect all the data packets in LAN. It is recommended that the ARP spoofing function is used only in small-sized LAN, for the reason that this function does some impacts on performance of the whole network.

### **7.2.3. Delay of domain filtering module**

When a computer in LAN tries to analyze a domain name, it will firstly search in local host DNS cache. If it can find the domain name, it will return at once. Or it will send a DNS query request. So a new policy on DNS filter module may not work at once on the monitored computers. After the local host DNS cache expires, the policy will work.

## **Chapter 8. Contact us**

### **8.1. Technical support**

We provide registered users with free technical support. We suggest you read help document firstly or visit our technical web site to acquire the up-to-date help documents, experience and

Active Network CO., Ltd

Tel: +86 5782519007

Email: support@lanctrl.com

<http://www.lanctrl.com>

Fax: +86 5782536303

Page 54

policy configurations. If you can not handle your problems in the ways above, please contact with our technicians. Be sure the following ways are tried:

1. Upgrade the up-to-date version.
2. Submit a specific description on the problem.
3. Submit the current network topology and monitoring mode.
4. Submit versions of the OS and Active Wall.
5. Try to tell us your problem as specifically as possible.

## 8.2. Advice and Suggestions

Please send us any advice and suggestions which are good for the software improvement. We are glad to get any feedback information from registered or unregistered users. We thank all the advice and suggestions including Bugs, user experiences and remarks. With full heart, we also thank all the friends who used to send us e-mails or mails, not matter they are compliments or criticism.

## 8.3. Contact

Company: Active Network CO., Ltd

Telephone: +86 5782519007

Fax: +86 5782536303

Post code: 323000

Address: No.242, Dengta Street, Lishui City, Zhejiang Province, China

Web site: <http://www.lanctrl.com>

E-mail: [support@lanctrl.com](mailto:support@lanctrl.com)

Support BBS: <http://forum.lanctrl.com>

# Chapter 9. Protocols and standards

## 9.1. Protocols

Following shows all the network protocols which <Active Wall> bases on:

**IEEE 802.3** - 10BASE-T

**IEEE 802.3u** - 100BASE-TX

**IEEE 802.3z** - 1000BaseSX, 1000BaseLX

**RFC 768** - User Datagram Protocol

**RFC 791** - Internet Protocol

**RFC 792** - Internet Control Message Protocol

**RFC 793** - Transmission Control Protocol

Active Network CO., Ltd  
Tel: +86 5782519007  
Email: [support@lanctrl.com](mailto:support@lanctrl.com)

<http://www.lanctrl.com>  
Fax: +86 5782536303  
Page 55



- RFC 821** - Simple Mail Transfer Protocol
- RFC 822** - STANDARD FOR THE FORMAT OF ARPA INTERNET TEXT MESSAGES
- RFC 826** - Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware
- RFC 959** - File Transfer Protocol
- RFC 977** - Network News Transfer Protocol
- RFC 1034** - Domain names - concepts and facilities
- RFC 1035** - Domain names - implementation and specification
- RFC 1112** - Host extensions for IP multicasting
- RFC 1323** - TCP Extensions for High Performance
- RFC 1519** - Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy
- RFC 1521** - MIME (Multipurpose Internet Mail Extensions) Part One: Mechanisms for Specifying and Describing the Format of Internet Message Bodies
- RFC 1522** - MIME (Multipurpose Internet Mail Extensions) Part Two: Message Header Extensions for Non-ASCII Text
- RFC 1631** - The IP Network Address Translator (NAT)
- RFC 1700** - Assigned Numbers
- RFC 1725** - Post Office Protocol - Version 3
- RFC 1738** - Uniform Resource Locators (URL)
- RFC 1866** - Hypertext Markup Language - 2.0
- RFC 1867** - Form-based File Upload in HTML
- RFC 1869** - SMTP Service Extensions
- RFC 1918** - Address Allocation for Private Internets
- RFC 1939** - Post Office Protocol (POP) - Version 3
- RFC 1945** - Hypertext Transfer Protocol -- HTTP/1.0
- RFC 1951** - DEFLATE Compressed Data Format Specification version 1.3
- RFC 1952** - GZIP file format specification version 4.3
- RFC 2044** - UTF-8, a transformation format of Unicode and ISO 10646
- RFC 2045** - Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies
- RFC 2046** - Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types
- RFC 2047** - MIME (Multipurpose Internet Mail Extensions) Part Three: Message Header Extensions for Non-ASCII Text
- RFC 2048** - Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures
- RFC 2049** - Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples
- RFC 2060** - Internet Message Access Protocol (IMAP) - Version 4 Rev 1
- RFC 2068** - Hypertext Transfer Protocol -- HTTP/1.1
- RFC 2070** - Internationalization of the Hypertext Markup Language
- RFC 2131** - Dynamic Host Configuration Protocol
- RFC 2236** - Internet Group Management Protocol, Version 2
- RFC 2279** - UTF-8, a transformation format of ISO 10646
- RFC 2396** - Uniform Resource Identifiers (URI): Generic Syntax

**RFC 2616** - Hypertext Transfer Protocol -- HTTP/1.1

**RFC 2617** - HTTP Authentication: Basic and Digest Access Authentication

**RFC 2818** - HTTP Over TLS