ShareTech Security Gateway

SG-100N Administrator Manual

Version 6.1.9

LAN default IP and Password	
IP Address	192.168.1.1
Account / Password	admin / admin

Table of Contents

Conventions Used in This Book

The following typographical conventions are used in this book

Content Style

Menu > Submenu > Right Side Banner Selections

e.g. Configuration > Administrator > System Setup

Constant width bold

Indicates chapter and section

"Italic"

"Indicates user input examples."

This icon indicates a tip, or suggestion. I would like to tell users a special point on the Internet.

This icon indicates a limited or caution. Pay attention to these to avoid running into system.

This icon indicates an example. Give users examples and to show how to use.

Chapter 0：Description

In this chapter, it will not only tell you how to install and connect your network system but also configure and monitor it. Many explanations in detail functions are shown as well as the examples of the operation for interface. In the description chapter you can enable the following lists：

- 0-1 Hardware Overview
- 0-2 Front Panel
- 0-3 Rear Panel
- 0-4 System Setting
- 0-5 Setting internal and external network
- 0-6 Homepage Information

0-1 Hardware Overview

Integration between firewall and NAS

Unlike the traditional way building a gateway firewall and then installing shared storage space via NAS or Network Neighborhood, ShareTech SG-100N is a gateway device integrated NAS into firewall, protecting user's network against threats from web activities with URL filtering. Users can define search by keywords and sort options. Filtering conditions can be applied by time to control over network access and usage to avoid threats from external networks. SG-100N simplifies SMB network environments and provides IT staff a cloud-managed networking solution.

SG-100N Dimensions(wide*long*high) :232*152*44mm Custom Port (Fixed LAN & WAN1), 2G memory 320G HDD 	SG-100N with WiFi Dimensions(wide*long*high) : 232*152*44mm Custom Port (Fixed LAN & WAN1), 2G memory, 320G HDD 2dBi, 3T3R, 802.11b/g/n 

0-2 Front Panel

Figure 0-2. 1 Front Panel

■ Model Name：please see the Figure 0-2.1(Figure 0-2.1)

Appliance LED Behavior

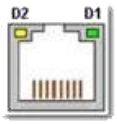
LED	State	Description
POWER	Blinking	ShareTech appliance is activity
	Green	ShareTech appliance in ON
	Off	Take off adapter power(+12V DC)
HDD	Flashing Amber	Activity going on
	Off	No activity
Ethernet Ports	Flashing Green(Right)	The port is linking and active in data transmission.
	Green(Left)	Correct cable is used and power is on port
	Off	Power is not on port.

0-3 Rear Panel

Figure 0-3. 1 Rear Panel

- Power supply: +12 DC in
- Console Port: By using RJ-45 to DB-9 Female cable, you can connect to a computer terminal for diagnostic or configuration purpose. Terminal Configuration Parameters: 115200 baud Rate, 8 data bits, 1 stop bit, no parity, XON/XOFF flow control. A console port for inspecting settings remotely or, if needed, resetting the device to factory default.
- USB 2.0 Ports: It can connect to any USB devices, for example, a USB flash drive.
- Reset Button: It is a button to reset system.
- Ethernet Ports:
  1. LAN: Connects to the intranet.
  2. WAN: Connects to the perimeter router.

Appliance Ethernet Ports Behavior:

LED	State	Description
Ethernet Ports 	Flashing Amber(Left)	The port is linking and active in data transmission.
	Amber(Left)	Correct cable is used and power is on port
	Off(Left)	Power is not on port.
	Amber(Right)	Port is connected at the 100 Mbps
	Green(Right)	Port is connected at the 1000 Mbps
	Off(Right)	Power is not on port.

Please confirm the correct installation and connection. If power LED light does not glow, please shut down the appliance. After several minutes had passed, please reboot the appliance again. If LED light is still not lit, please feel free to call **+886-4-27050888 / Skype: sharetech_tc** and contact with us while the appliance is still under warranty.

How to use condole cale:

The SG-100N can be configured via the "Console" port located on the SG-100N's Rear panel using a terminal-emulation program (e.g. HyperTerminal). (Figure 0-3.3)

Please purchase USB to RS232/DB9 Serial Cable and download its driver (Figure 0-3.2)

Here is an example,

USB to RS232/DB9 Serial Cable Driver, please note your OS before download.

http://www.tri-plc.com/USB-RS232/drivers.htm

Figure 0-3. 2 RS232/DB9

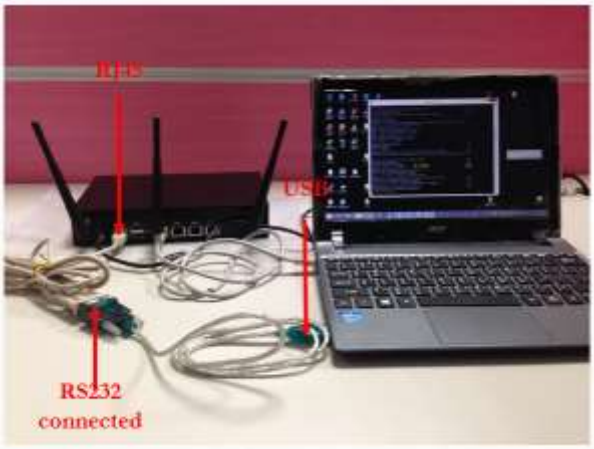


Figure 0-3. 3 using console

Downlaod PuTTY:

http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

Use the following configuration settings for terminal-emulation programs: (Figure 0-3.4)

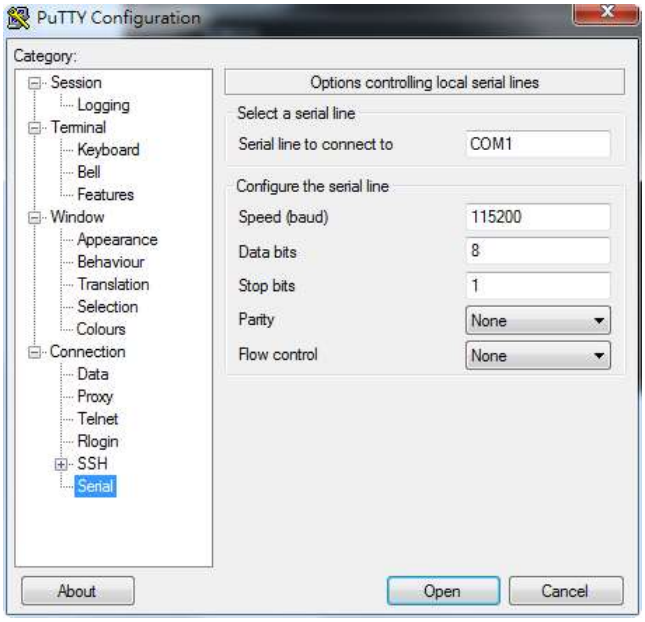


Figure 0-3. 4 PuTTY Configuration

Please check your COM and LPT(Figure 0-3.5)

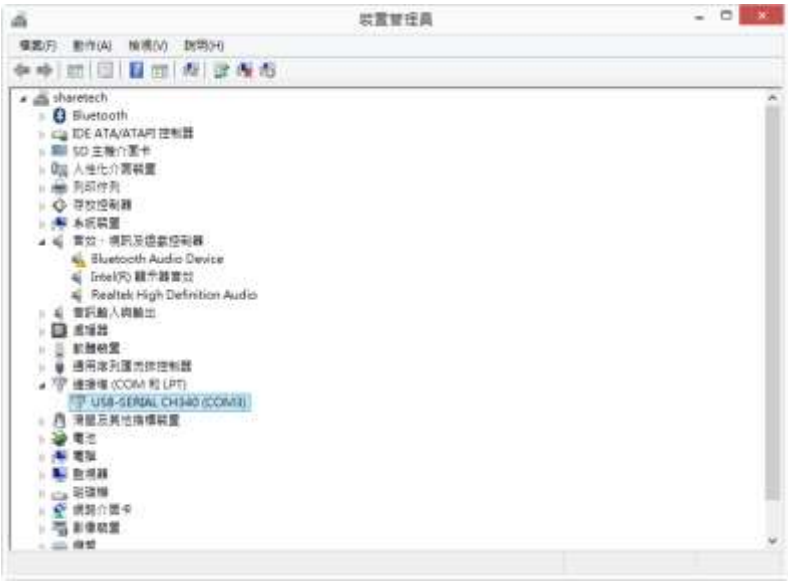


Figure 0-3. 5 USB-SERIAL

Enter Information: (Figure 0-3.6)

- Choose "serial"
- Serial line: COM(?), please refer to Figure 0-3.5, and enter your COM number.
- Speed : 115200
- Choose "Open"

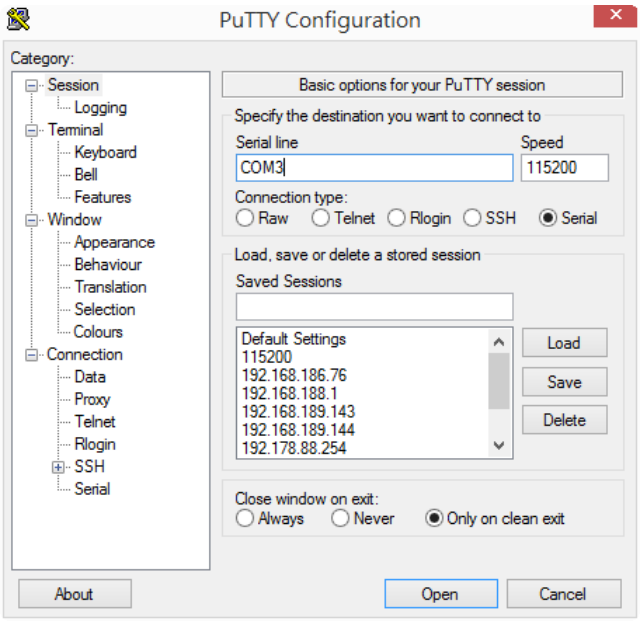


Figure 0-3. 6 Serial line

Console Screen: (Figure 0-3.)

MY LAN IP IS 192.168.1.1: it shows current LAN IP

- admin_pw_def: reset your login User Name and Password to be default(admin/admin)
- admin_ip_def: reset your IP to be 192.168.1.1
- Apache_port: shows http and https port
- Restart: reboot SG-100N and every setting still exist on equipment.
- Poweroff: shutdown SG-100N.

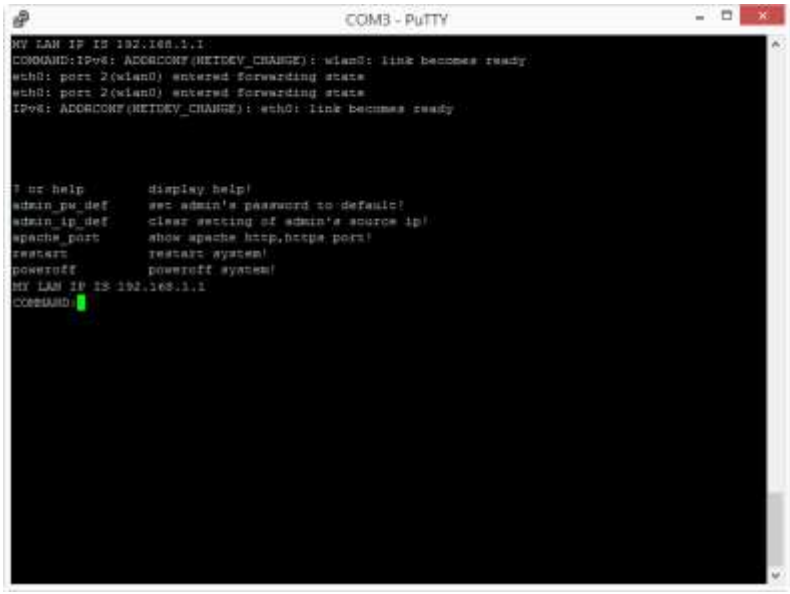


Figure 0-3. 7 Console Screen

0-4 System Setting

Deployment

Your PC connect the device's LAN port directly or, with the same hub / switch, and launch a web browser (ex. Internet Explorer, Mozilla Firefox, or Chrome) to access the management interface address which is set to *http://192.168.1.1* by default. Therefore, the IP addresses of LAN PCs must be configured within the range between 192.168.1.2 and 192.168.1.254 inclusively, and assigned the subnet mask of 255.255.255.0. (Figure 0-4.1)

Figure 0-4. 1 Deployment

Start Browser and Enter Login User Name / Password

Open the IE browser; enter 192.168.1.1 in the address bar. (Figure 0-4.2)

Browser will pop up for authentication, please enter **admin** (username) / **admin** (password) to login.

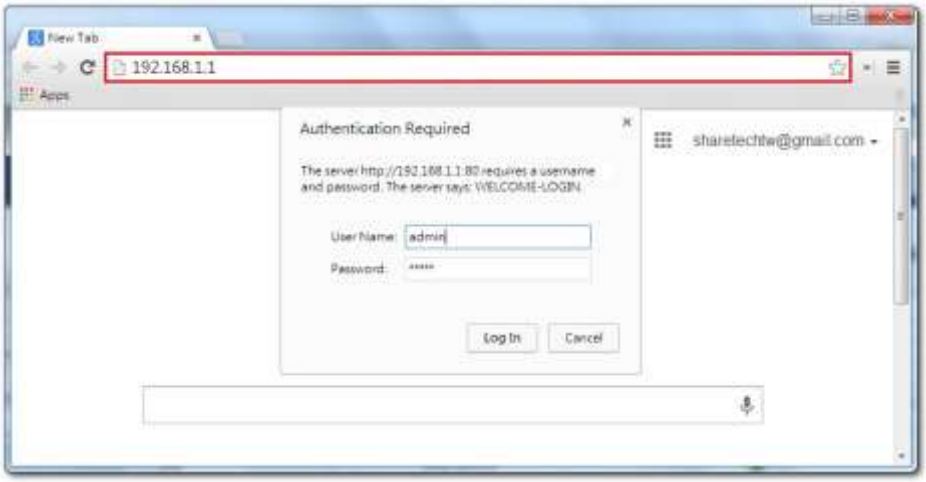


Figure 0-4. 2 Start Browser and Enter Login User Name / Password

Login completed (Figure 0-4.3)

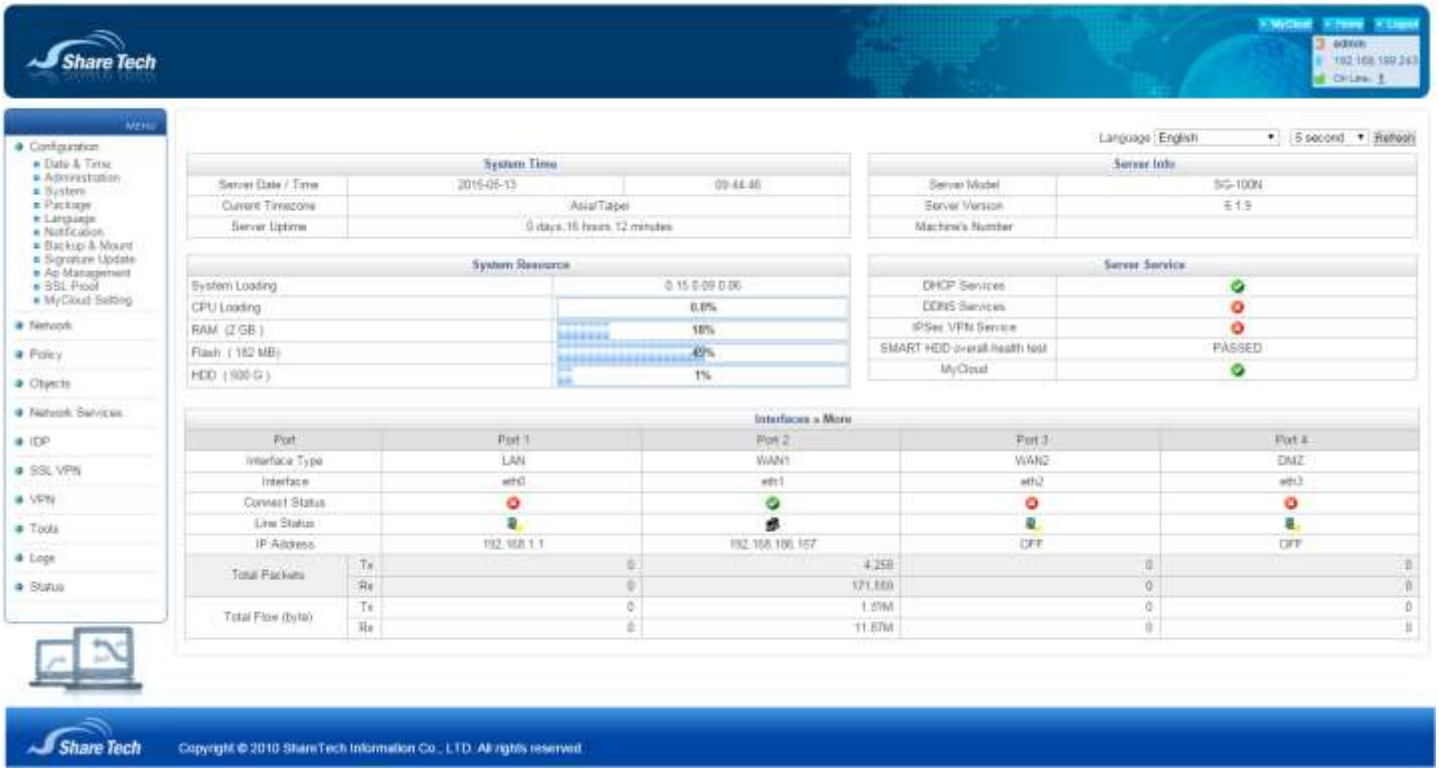


Figure 0-4. 3 Login completed

Change Language

Default management interface language is English. Select Configuration > Language > Language. Then, there are three languages, English, Traditional Chinese, and Simplified Chinese. Select one language which belongs to you. Click on Save. (Figure 0-4.4)

Figure 0-4. 4 Change Language

0-5 Setting internal and external network

In this section, follow two parts below, LAN setup and WAN setup, and to start machine up.

When configure a new LAN interface address accordingly. If the company's LAN IP address is not belong to subnet of 192.168.1.0/24 (default), and then the Administrator must add/change PC IP address to be within the same range of the LAN subnet. (Figure 0-5.1)

For example, to add multiple IP address (192.168.1.2) in "LAN connection" you're your computer.

Figure 0-5. 1 Advanced TCP/IP settings

For your reference, you may configure your management address based on the available subnet ranges below: 10.0.0.0 ~ 10.255.255.255,
172.16.0.0 ~ 172.31.255.255,
192.168.0.0 ~ 192.168.255.255

Setting Internal Network

Select Network > Interface > Port 1, and Interface Type is LAN. (Figure 0-5.2)

Administrator clicks on Network > Interface > Port 1 (LAN) to enter internal network information. At last, click on “save” to complete the setup.

Figure 0-5. 2 LAN Interface

Note: If the management interface is assigned with a different IP address, the management interface will only become accessible from a web browser using the new IP address.

Setting External Network

Select Network > Interface > Port 2, and Interface Type is WAN1. (Figure 0-5.3)

Administrator clicks on Network > Interface > Port 2 (WAN) to enter external network information. At last, click on “save” to complete the setup.

Figure 0-5. 3 external Network

Step 1: Network > Interfaces > Port 2 (WAN) (Figure 0-5.4) (Figure 0-5.5)

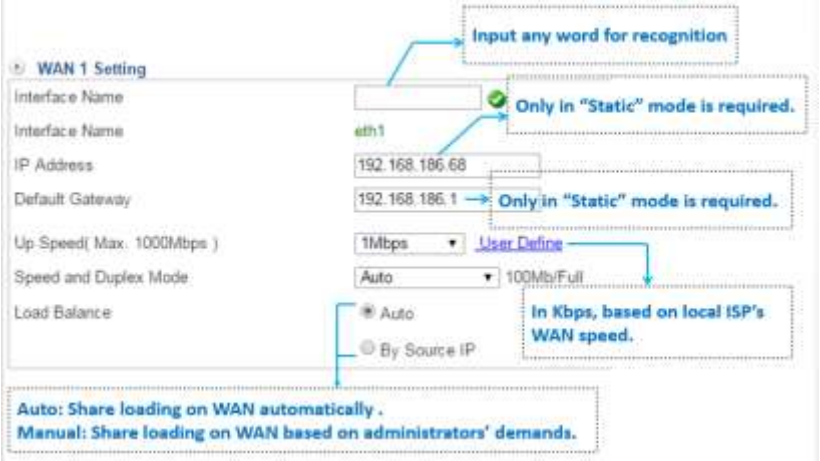


Figure 0-5. 4 WAN 1 Setting

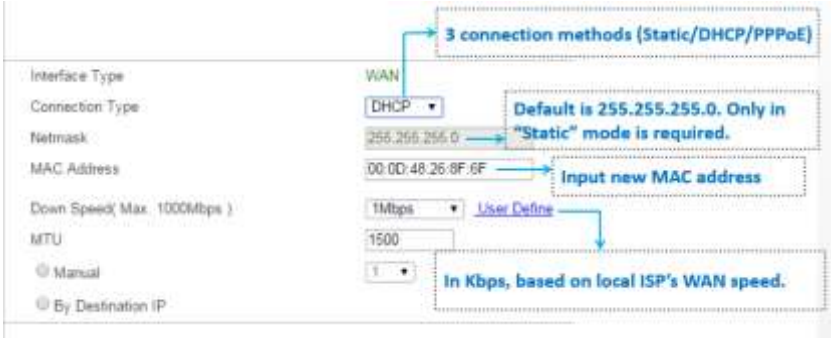


Figure 0-5. 5 WAN1 Connection Type

Step 2: Port 2 (WAN) Alive Detection(Figure 0-5.6)

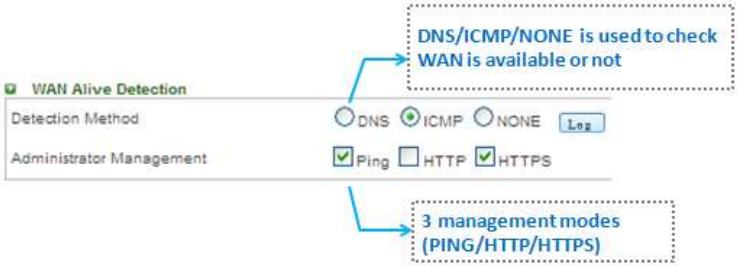


Figure 0-5. 6 WAN1 Alive Detection

Step 3: General Setting on Port 2 (WAN) (Figure 0-5.7)

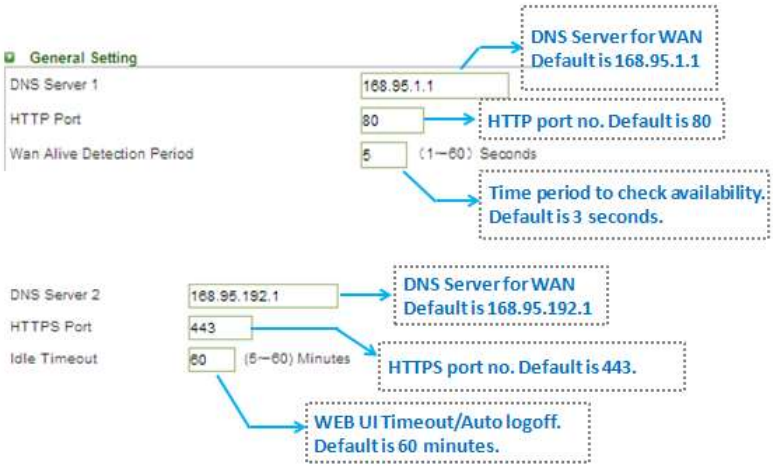


Figure 0-5. 7 General Setting on Port 2

Step 4: After finish configuring LAN and WAN, SG-100N setup is successful.

0-6 Homepage Information

Menu Bar

From top of the screen, menu bar, you can know different models depend on the different colors. SG series is Blue color. (Figure 0-6.1)

Figure 0-6. 1 Menu Bar

MENU

On the other hand, from the left side of the screen, MENU, it shows difference depend on the different models.

Figure 0-6. 2 Menu

System Time and System Resource

It shows Server 1-1 Date & Time and 11-1 Performance. In addition, it displays the CPU, Memory, Flash, and HDD simultaneously. (Figure 0-6.3)

System Time		
Server Date / Time	2015-05-08	14:33:31
Current Timezone	Asia/Taipei	
Server Uptime	5 days 22 hours 19 minutes	

System Resource	
System Loading	0.06 0.12 0.13
CPU Loading	3.0%
RAM (2 GB)	25%
Flash (182 MB)	48%
HDD (500 G)	1%

Figure 0-6. 3 System Time and System Resource

System Information and Server Service

The Server Model and Server Version of the machine (Figure 0-6.4)

- : Service works.
- : Service does not work.

Server Info	
Server Model	SG-100N
Server Version	6.1.9
Machine's Number	

Server Service	
DHCP Services	
DDNS Services	
IPSec VPN Service	
SMART HDD overall-health test	PASSED
MyCloud	

Figure 0-6. 4 System Information and Server Service

Interface

Equipment Interface details: (Figure 0-6.5)

- Name: The system catches network contact surface name.
- Connect Status: Whether the network is unimpeded
  1. : Connect up.
  2. : It does not connect the Internet.
- Line Status: Whether the judgment network does connect
  1. : Connect up.
  2. : It does not connect the Internet.
- IP Address: System binding IP address
- Total Packets: Each network interface transmission, receive wrapped packets quantity. (Bytes)
- Total Flow: Each network interface transmission, receive current capacity. (Bytes)

Interfaces > More					
Port		Port 1	Port 2	Port 3	Port 4
Interface Type		LAN	WAN1	WAN2	DMZ
Interface		eth0	eth1	eth2	eth3
Connect Status					
Line Status					
IP Address		192.168.1.1	192.168.186.157	OFF	OFF
Total Packets	Tx	4	240,887	0	0
	Rx	10,799	3,391,926	0	0
Total Flow (byte)	Tx	408	71.30M	0	0
	Rx	1.43M	334.27M	0	0

Figure 0-6. 5 Interface

Click » More (Figure 0-6.6)

Interfaces » More

Port		Port 1	Port 2	Port 3	Port 4
Interface Type		LAN	WAN1	WAN2	DMZ
Interface		eth0	eth1	eth2	eth3
Connect Status					
Line Status					
IP Address		192.168.1.1	192.168.186.157	OFF	OFF
Total Packets	Tx	4	241,066	0	0
	Rx	10,799	3,392,494	0	0
Total Flow (byte)	Tx	408	71.37M	0	0
	Rx	1.43M	334.38M	0	0
Packet (packet/s)	Tx	0	1	0	0
	Rx	0	6	0	0
Flow (bit/s)	Tx	0	4K	0	0
	Rx	0	13K	0	0
Error Packet	Tx	0	0	0	0
	Rx	0	0	0	0

Figure 0-6. 6 Interface more detailed

Chapter 1：Configuration

In this chapter, you will know how to configure your machine of Date, Time, Administrator, Backup, Notification, and Language. In the Description chapter you can enable the following lists：

- 1-1 Data & Time
- 1-2 Administration
- 1-3 System
- 1-4 Package
- 1-5 Language
- 1-6 Notification
- 1-7 Backup & Mount
- 1-8 Signature Update
- 1-9 CMS
- 1-10 Ap Management
- 1-11 SSL Proof
- 1-12 MyCloud Setting

1-1 Date & Time

Your current time zone setting can also be changed in this section. The first form in this section gives you the possibility to manually change the system time. Second, the system time synchronized to time server hosts on the internet by using the network time protocol (NTP[1]). A number of time server hosts on the internet are preconfigured and used by the system. This makes sense if the system clock is way off and you would like to speed up synchronization. Finally, this might be necessary if you are running a setup that does not allow ShareTech to reach the internet. You can add a host on User Defined Time Server field. In the Date & Time section you can enable the following lists: (Figure 1-1.1)

Figure 1-1. 1 Date & Time

Setting

Select Configuration > Date & Time > Setting. There are three methods you are able to set up, Timezone and time and Network Time Retrieval.

Method 1: Synchronize to the local computer.

- Time Zone: Select your country time zone.
- Time: Select the local time.
- Date: Select the local date.
- Click on Save.

Method 2: The date and time settings can be configured by either synchronizing to an Internet Network Time Server.

- Select Enabled in Network Time Retrieval.
- Selected Time Server: Select your country time server.

[1] Network Time Protocol

- Click Refresh. Click on Time Log to check time log information, and it keeps within three days log information.
- Click on Save.

Method 3: This might be necessary if you are running a setup that does not allow ShareTech to reach the internet.

- Select Enabled in Network Time Retrieval.
- User Defined Time Server: Enter a time server you know.
- Click on Refresh. Click on Time Log to check time log information, and it keeps within three days log information.
- Click on Save.

1-2 Administration

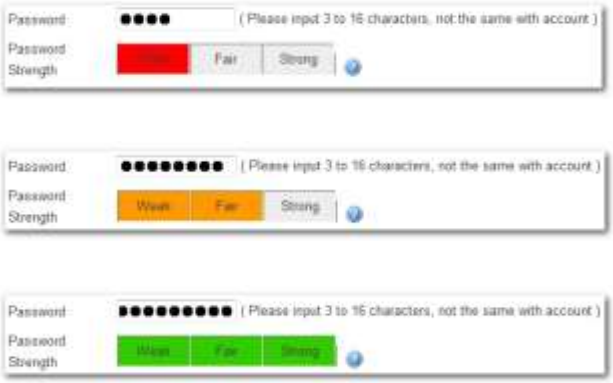
This section mainly explains the authorization settings for accessing. It covers the subjects of Administrator Setup, System Setup, Manage IP Address, Clear Data, and SMTP Server Setting. In this section you can enable the following lists:

Administrator

Select Configuration > Administration > Administrator.

The default account and password are both "admin." IT administrator can create several sub-administrators with different permission and menu customization. In addition, default "admin" is permitted using all privileges and all menus, such as the privileges of packets that pass through the equipment and monitoring controls. "Admin"(system manager) can manage monitor and configure setting of functions. For some sub-administrations (account) are set "Read," it is "read-only" for that account that is not able to change any setting of the machine. (Figure 1-2.1)

- Account: Enter account name.
- Password: The password for authentication.
- Password Strength:



- Confirm Password: The confirmation of password
- Notes: Easy to know who is it.
- Privilege: Sub-administrators can be granted with Read, Write, or All Privileges to determine the right of system. Besides, sub-administrators can be created, edited or deleted.
- User Defined Menu: IT administrator could customize MENU by selecting. (Figure 1-2.1)

Figure 1-2. 1 User Defined Menu

System

Select Configuration > Administration > System. This function shows view of the screen and system default setting.

General Setting: (Figure 1-2.2)

- Login Message: Enter a name, and then click on Sure. The name you enter will be showed when you login. (Figure 1-2.3)
- Homepage Message: Enter a name, and then click on Sure. The name you enter will be showed next to the logo picture. (Figure 1-2.4)
- Browser Message: Enter a name, and then click on Sure. The name you enter will be showed on the top of browser. (Figure 1-2.5)
- Upload Logo: Click on Browse... to upload resolution of 150x90 gif figure file, and then click on Save. The image will automatically appear in the upper left corner of the screen. (Figure 1-2.6)
- Memory Release: How often check memory when memory usage up to what you set %. System will release memory if it has high memory. (Please see memory status in Homepage Information.)
- Pass-Through Protocol: System supports H-323 and SIP.
- Session timeout of established:
- WatchDog timer: When the system is crashed, watchdog will immediately restart the system.

Figure 1-2. 2 System Setup

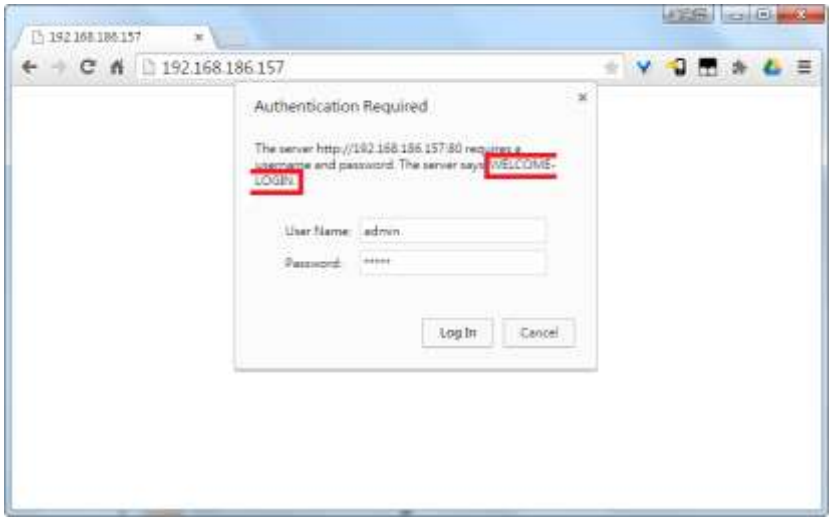


Figure 1-2. 3 Login Message

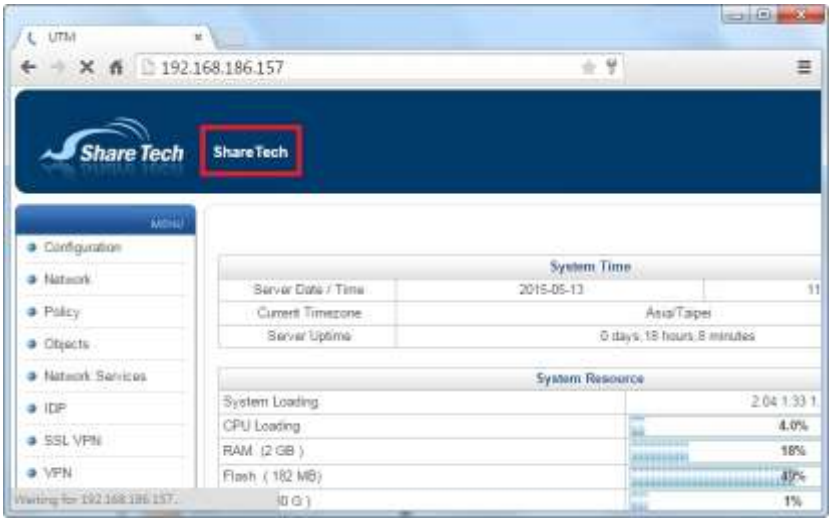


Figure 1-2. 4 Homepage Message

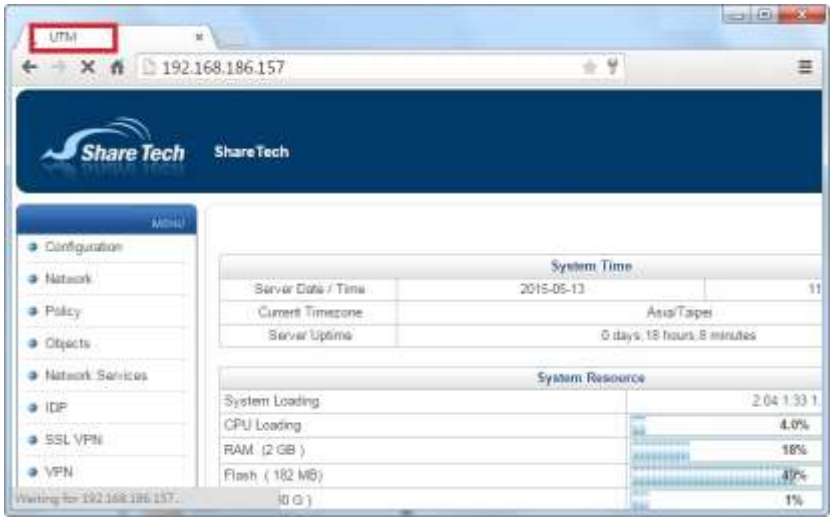


Figure 1-2. 5 Browser Message

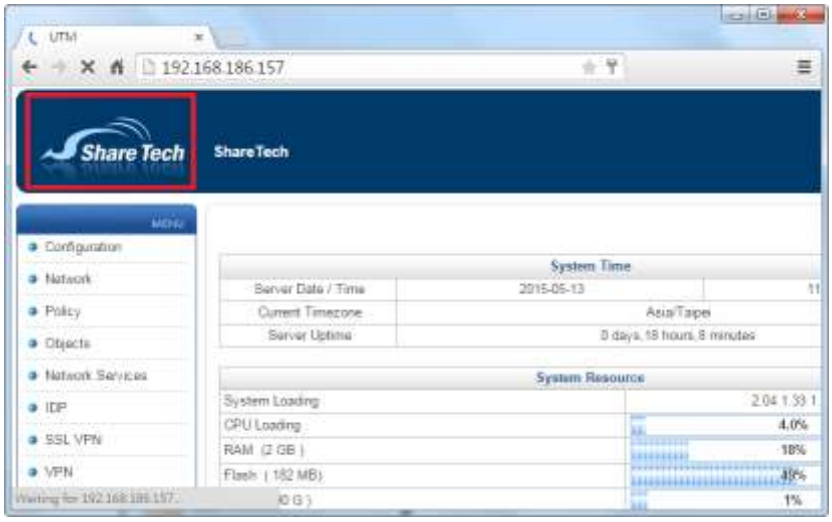


Figure 1-2. 6 Upload Logo

Login Failure Block Settings: (Figure 1-2.7)

- Temporarily block when login failed more than:
- IP blocking period:
- Unblocked IP: (Figure 1-2.9)

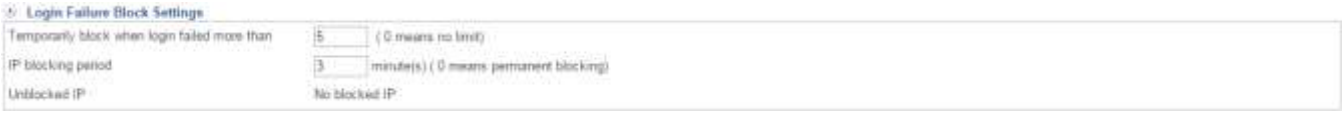


Figure 1-2. 7 Login failure block Settings

Here is an example: enter wrong username and password more than five times, and browser shows the following figure. (Figure 1-2.8) (Figure 1-2.9) (Figure 1-2.10)

Figure 1-2. 8 someone login fail more than 5 times

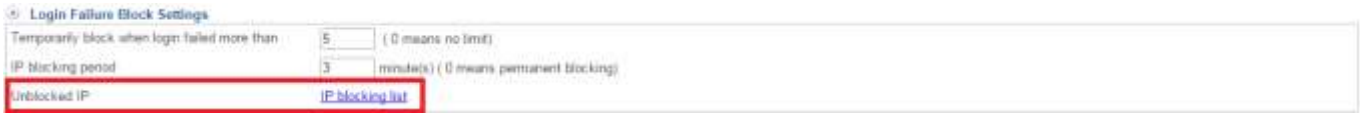


Figure 1-2. 9 IP blocking list

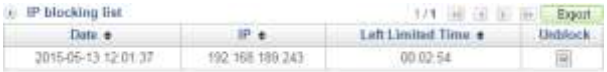


Figure 1-2. 10 IP blocking list and unblock it

Reset/Reboot Setting:

- Reset to Default Setting: If you need keep LAN, WAN and DMZ IP setting or you need to format hard disk, please select what you need. If you do not select, it means that you just want to reset to default setting.
- Reset to MyCloud Default Setting: Delete all settings and logs to be default setting.
- Reboot System: Click on reboot for reboot system.

Figure 1-2. 11 Reset/Reboot Setting

Fsck Hard Disk

Select Configuration > Administration > Fsck Hard Disk. (Figure 1-2.12)

As implied by its name, fsck is used to check and optionally repair one or more Linux file systems. This tool is important for maintaining data integrity, especially after an unforeseen reboot (crash, power-outage). At some point your system unusual crash, improperly shut-down, or be struck by lightning, we advise you must using fsck Confirm Run in order to repair of your file system. Normally, the fsck program will try to handle file systems on different physical disk drives in parallel to reduce the total amount of time needed to check all of the file systems.

Scheduling conditions are match, the system will reboot!

Figure 1-2. 12 Fsck Hard Disk

IP Address

If don't set up any IP address here (Figure 1-2.13), system would follow Network > Network > IP Address > Ports what you set up. (Figure 1-2.14) (Figure 1-2.15)

Figure 1-2. 13 Administrator Management

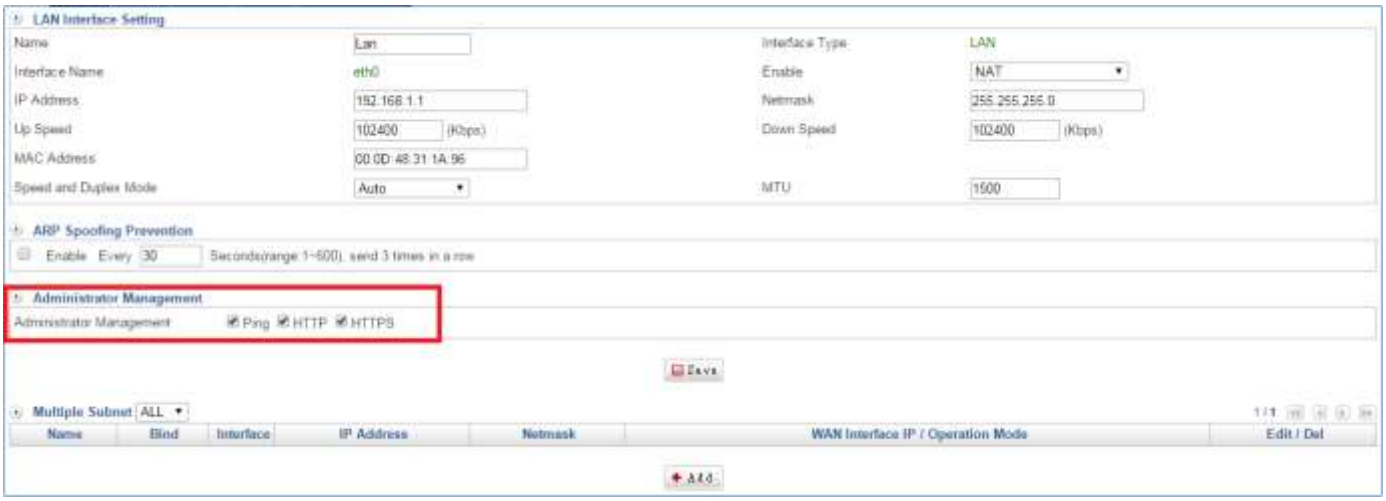


Figure 1-2. 14 Port 1 Administrator Management

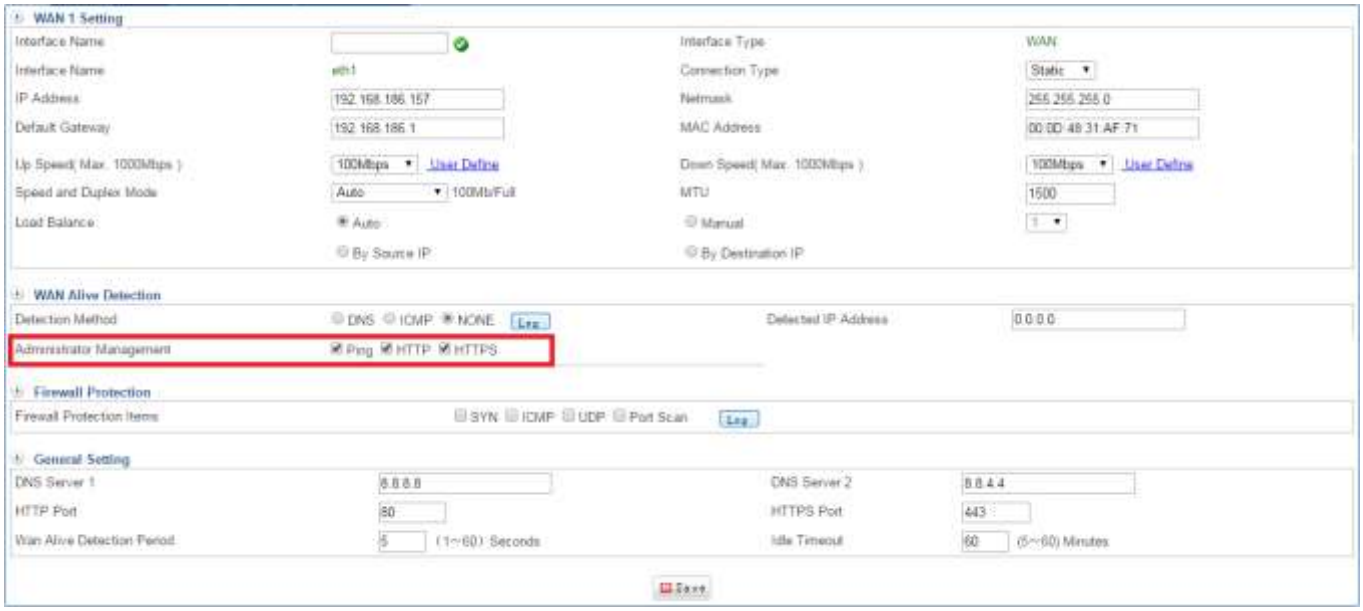


Figure 1-2. 15 Port 2 Administrator

Here is an example:

Please note Action should ne “Allow all of the Following.”

Click on Add to create a new IP and Netmask for Interface management. (Figure 1-2.17)

Figure 1-2. 16 IP Address

Then, others which are not among the IP range don’t have permission to access the server even if server works fine. (Figure 1-2.18)

Figure 1-2. 17 You don’t have permission to access this server

Clear Data

Select Configuration > Administration > Clear Data.

There are two methods, manually or system clear it auto.

Clear Data: In order to more space for Hard Dish, delete some records & logs which are not necessary. Click on Clean. It is also possible to check all connections by clicking on the Select All pane. (Figure 1-2.19)

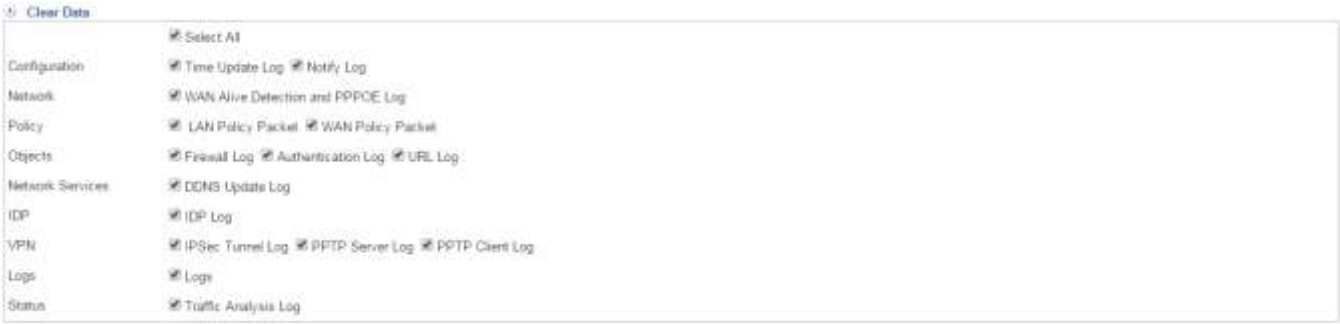


Figure 1-2. 18 Clear Data

Data Storing time: Select numbers. Otherwise, enter how many days you want to keep. Click Change signatures if you modify numbers. (Figure 1-2.20)

Figure 1-2. 19 Data Storing Time

SMTP Server

Select Configuration > Administration > SMTP Server. (Figure 1-2.21) (Figure 1-2.22) (Figure 1-2.23)

- Customize: Default is Admin if you don't enable it.
- Sender Name: Enter email address
- Mail Server IP Address: Enter SMTP server address or domain
- Account: Enter account
- Password: Enter right password of account.
- Authentication: Please select if your SMTP server of mail server has been enabled it.

- TLS: The TLS protocol allows client-server applications to communicate across a network in a way designed to prevent eavesDropping and tampering.
- Delivery Domain Name: If Delivery Domain Name is the same with the domain of receiver, the email will be sent from this SMTP setting; if not, the email will be sent from the first SMTP setting.

Figure 1-2. 20 Add SMTP Server

Figure 1-2. 21 SMTP Server List

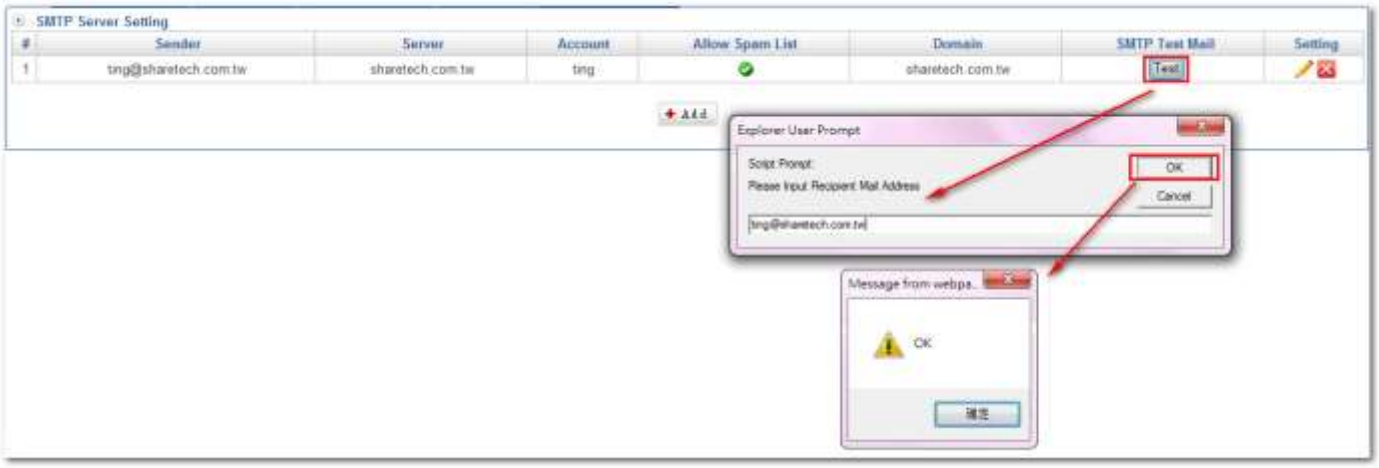


Figure 1-2. 22 SMTP Test Mail

If users got email as blow, your setting is correct, or else, user has to check users' SMTP server setting again. (Figure 1-2.24)

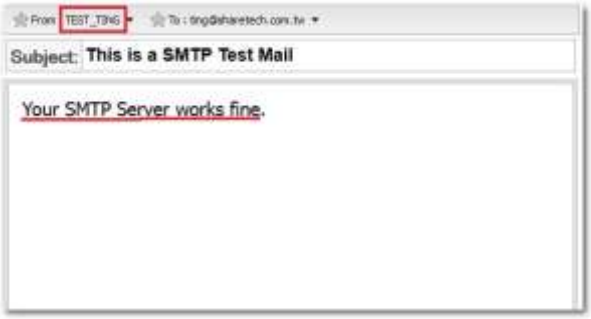


Figure 1-2. 23 Got SMTP TEST Email

1-3 System

In the System section you can enable the following lists:

System Backup

Select Configuration > System > System Backup, you will see two parts, System Backup and System Recovery. (Figure 1-3.1)

Clear Data: System Backup: Click on Backup, and then please wait a minute. You will see another window. Click on OK, and do not forget where you save file.

System Recovery: If you feel system is stranger than last week, you are able to download backup file on Configuration > System > Schedule Backup, and click on Choose File, and then select the file. After you select the file, please click on OK.

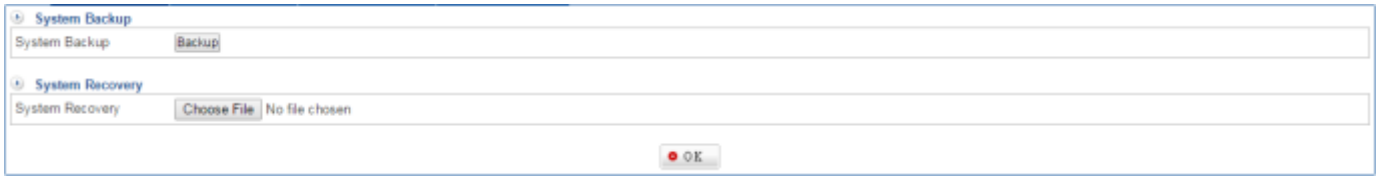


Figure 1-3. 1 System Backup

Schedule Backup

Select Configuration > System > Schedule Backup. There are two methods. (Figure 1-3.2)

Method 1:

- Starting: Select Starting to turn machine on.
- When to Backup: Set information to When to Backup
- Backup Reserved Quantities: Fill out number in the Field. The number should be a positive number in Backup Reserved Quantities field.
- Click on OK.

Method 2:

- Backup Right Now: Click on Backup Right Now, the data will show below of the screen.

Figure 1-3. 2 Auto Backup

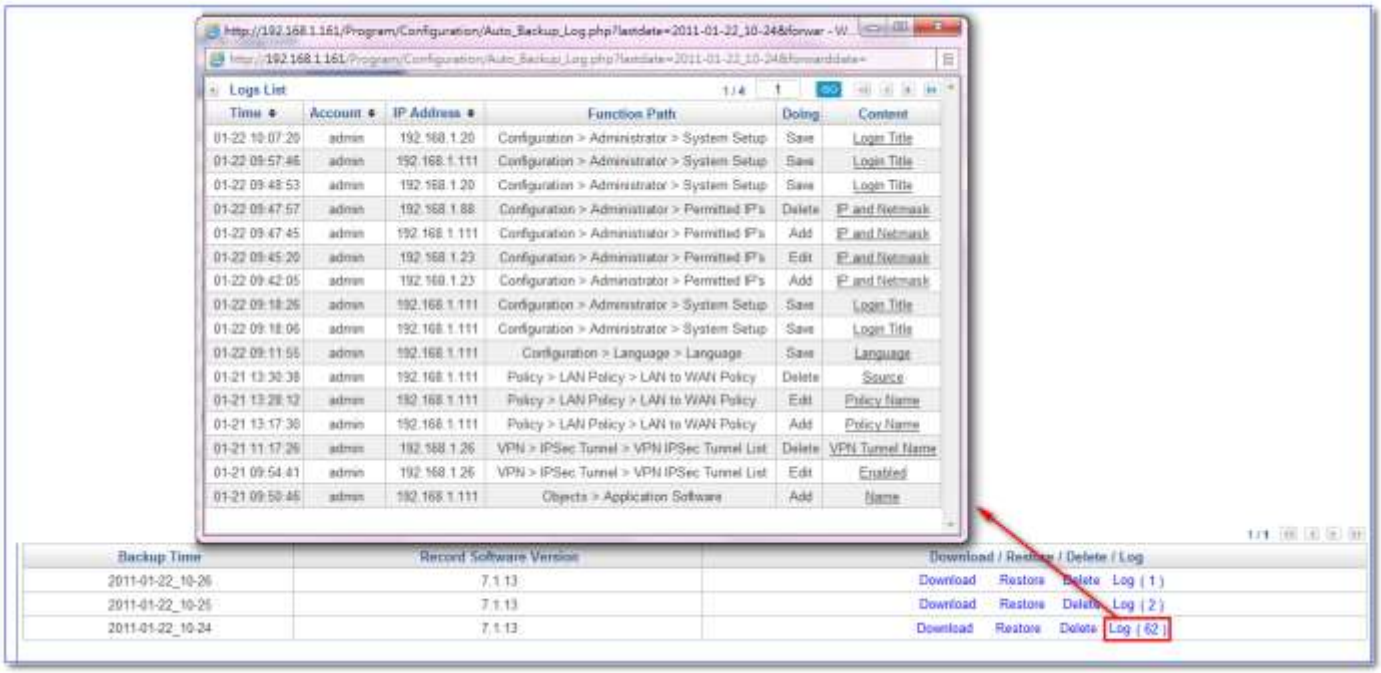


Figure 1-3. 3 Backup Logs

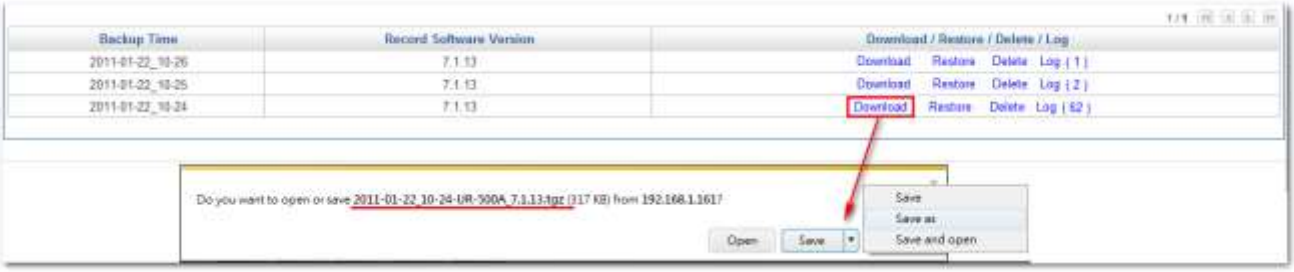


Figure 1-3. 4 Backup Download

Firmware Message

Figure 1-3. 5 Firmware Message

Firmware Upgrade

Select Configuration > System > Firmware Upgrade, you will see two parts, Software Upgrade and Upgrade Record. (Figure 1-3.6)

- Firmware Upgrade: You could know information about server model and current Firmware Version. Besides, ShareTech offer Software Upgrade file constantly on the ShareTech website. Therefore, you could follow the link below to download the most new one on the Internet. http://www.sharetech.com.tw/web_eng/contact-download.htm. After download it, click on Browse... to find out the file where you have just download. Then, remember to click on Upgrade.
- Upgrade Log: It shows all of upgrade information you had even done before.

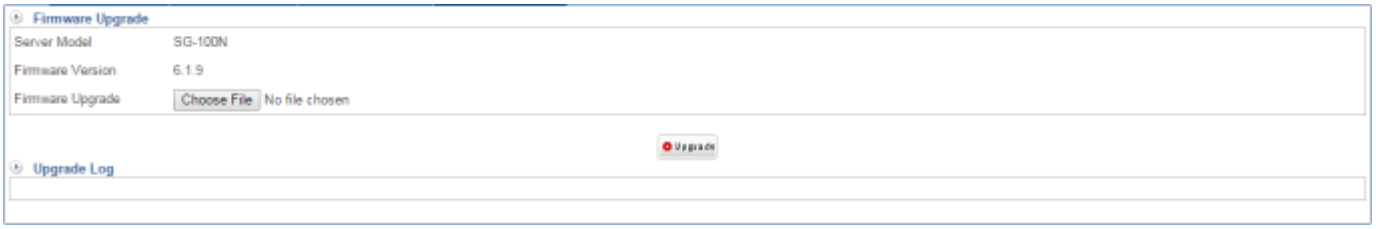


Figure 1-3. 6 Software Upgrade

1-4 Package

Package

It's an optional item. (Figure 1-4.1)

- WiFi: 802.11 b/g/n wireless. (2.4Ghz, 3T3R, 2dBi)

Figure 1-4. 1 Package

1-5 Language

Language

Select Configuration > Language > Language. It offers three languages that you are able to select, English, Traditional Chinese, and Simplified Chinese. Select a language which belongs to you. (Figure 1-5.1)

Figure 1-5. 1 Language

1-6 Notification

This function is in order to remind users if items are strange or happened. This advance notification helps administrator plan for effective deployment of security problems, and includes information about the number of security happened and information about any detection tools relevant to the updates. In the Notification section you can enable the following lists:

Notification

Select Configuration > Notification > Notification. (Figure 1-6.1)

- Sender Account: Default selection is "Auto." Select one SMTP server which you have ever set in Configuration > Administration > SMTP Server.
- Current Setting: After users select SMTP Setting, system will shows current SMTP server setting automatically.
- Recipient: Enter receiver email addresses.
- Click on Save to save setting what you selected.

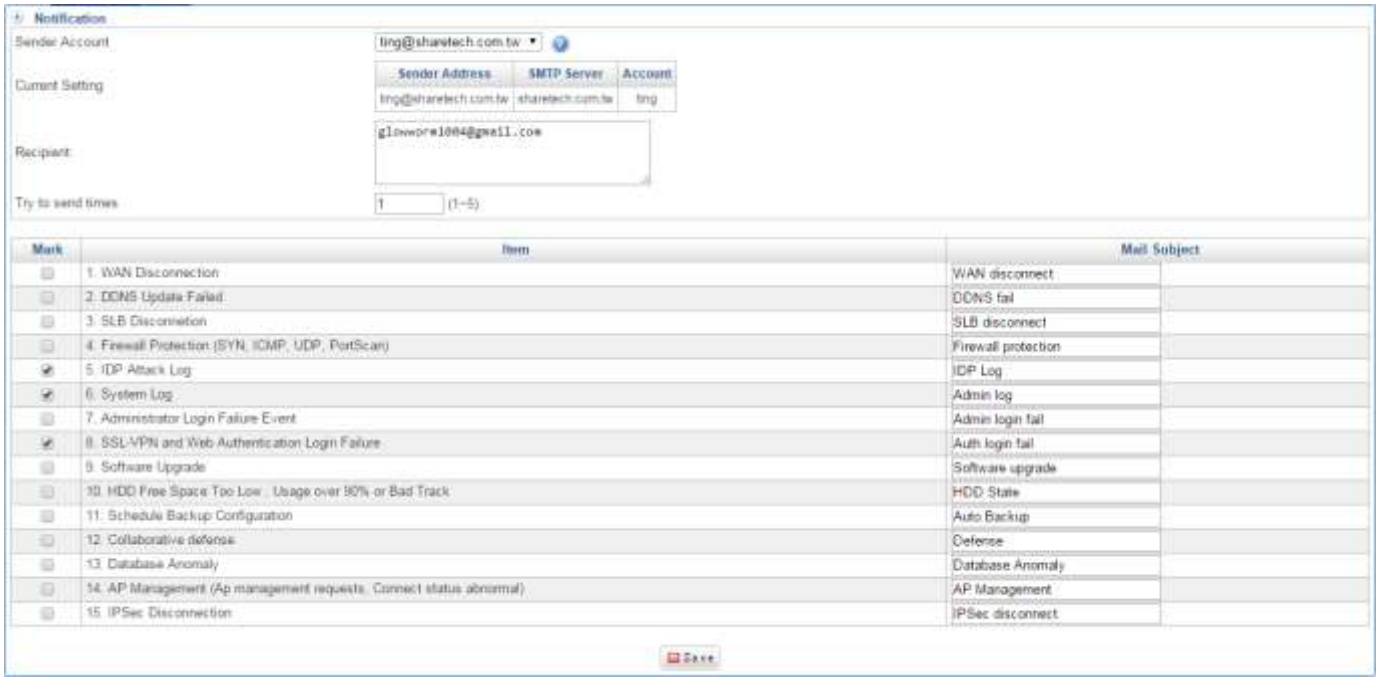


Figure 1-6. 1 Notification

Users will get email as below. (Figure 1-6.2) (Figure 1-6.3)

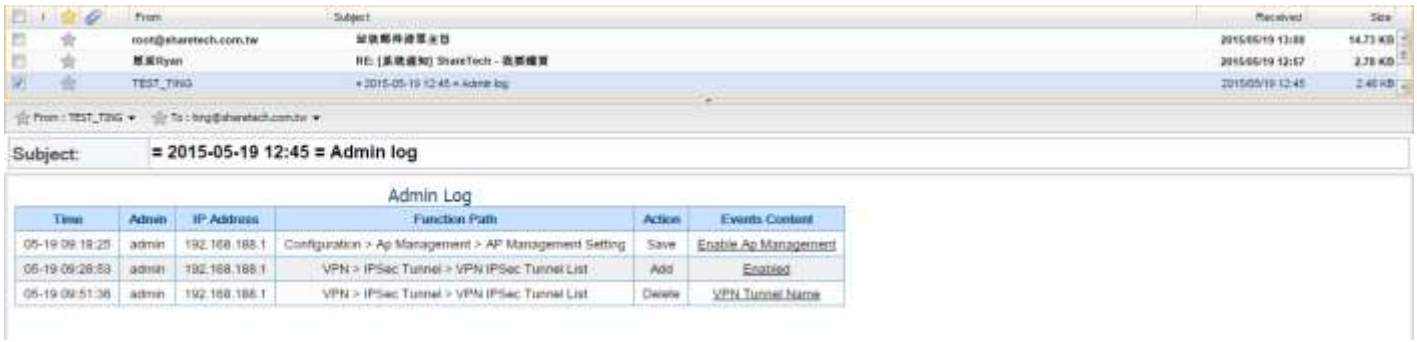


Figure 1-6. 2 notification mail-1

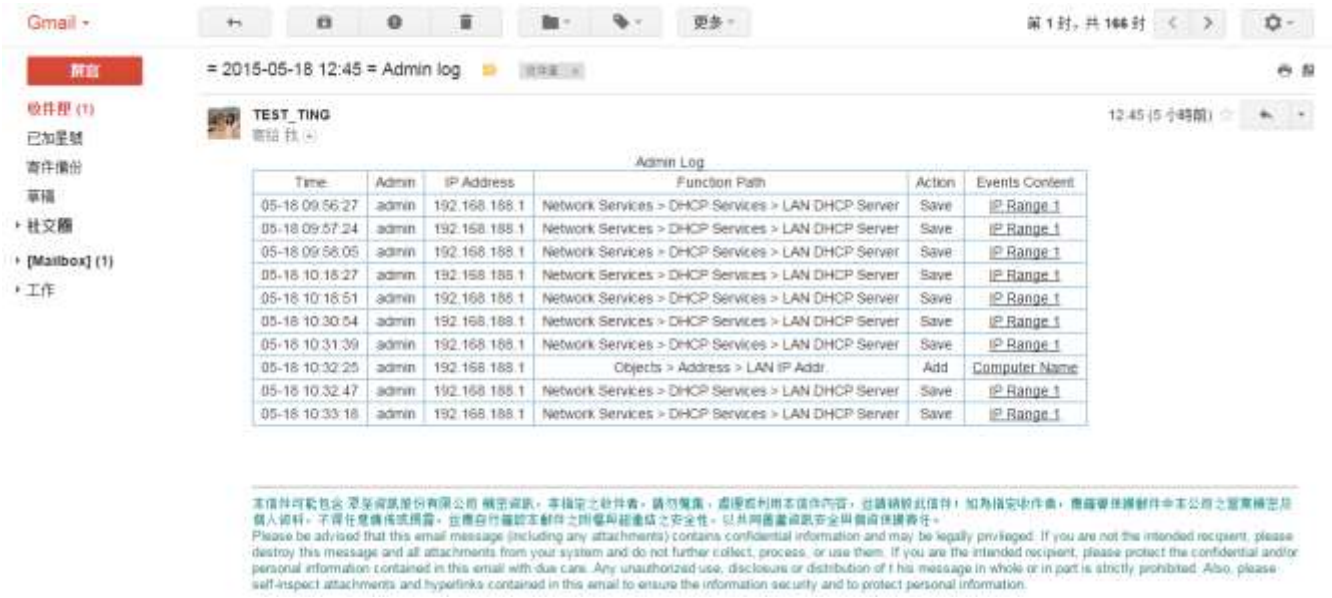


Figure 1-6. 3 notification mail-2

Log

Select Configuration > Notification > Log. (Figure 1-6.4)

- Date: Set date and time.
- Event: Set information what you want to search.
- Recipient: The mail receiver
- Record / Page: Select how many data would be shown on the screen.
- After you click on Search, you will see the result below of the screen.

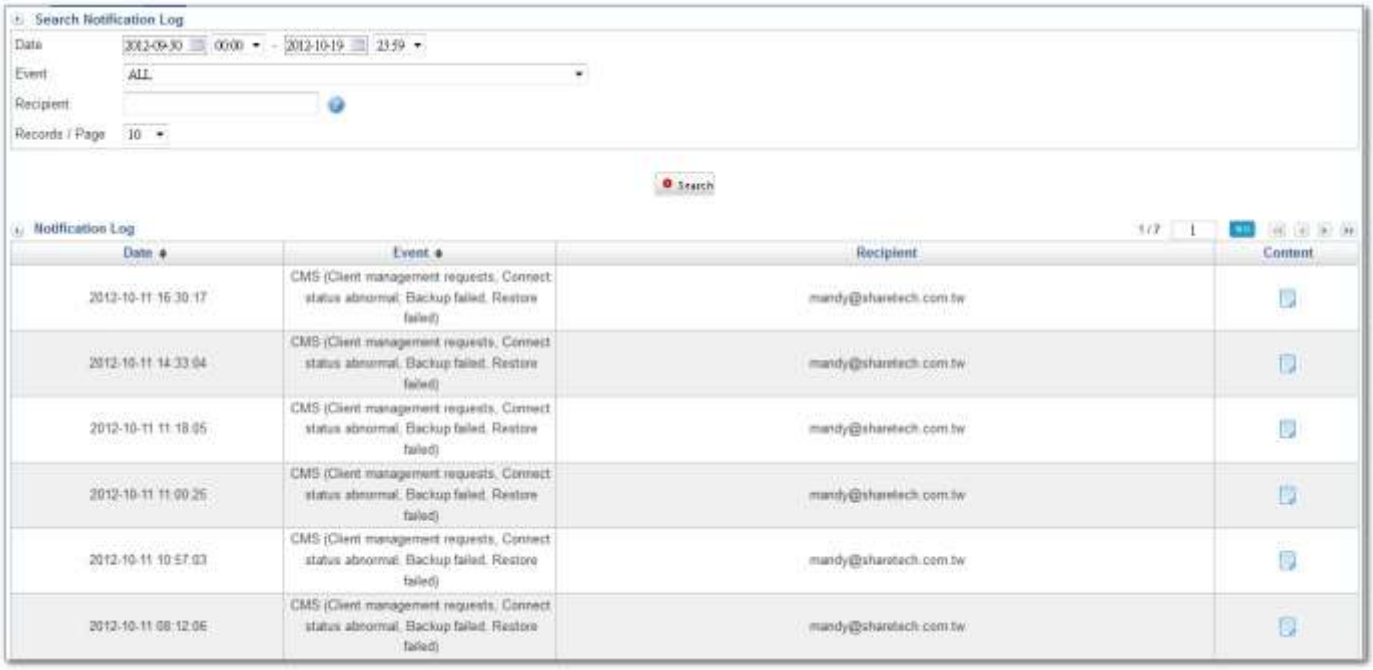


Figure 1-6. 4 Notification Log

Click on to see logs. (Figure 1-6.5)

Figure 1-6. 5 content of Notification Log

1-7 Backup & Mount

Some of IT administrators are afraid of the hard disk which is belonging to SG-100N broken; even through IT administrators do backup system usually or users forget where those files location are. Otherwise, users are also afraid of the device doesn't have enough free space to store those files. Therefore, users would like this function because system has schedule to do data backup automatically.

Data Backup

Select Configuration > Backup & Mount > Data Backup

Backup Destination

- Backup Method: Samba only
- IP address: Enter an IP address.
- Folder Name: Enter a Folder Name you like.

Please create this Folder Name in C: and share it before you set up this

- Username: Enter user's computer name.
- Password: The password for user own computer authentication.
- Confirm Password: The confirmation of password.

Click on Connection Test in order to check whether settings are right or not. (Figure 1-7.1)

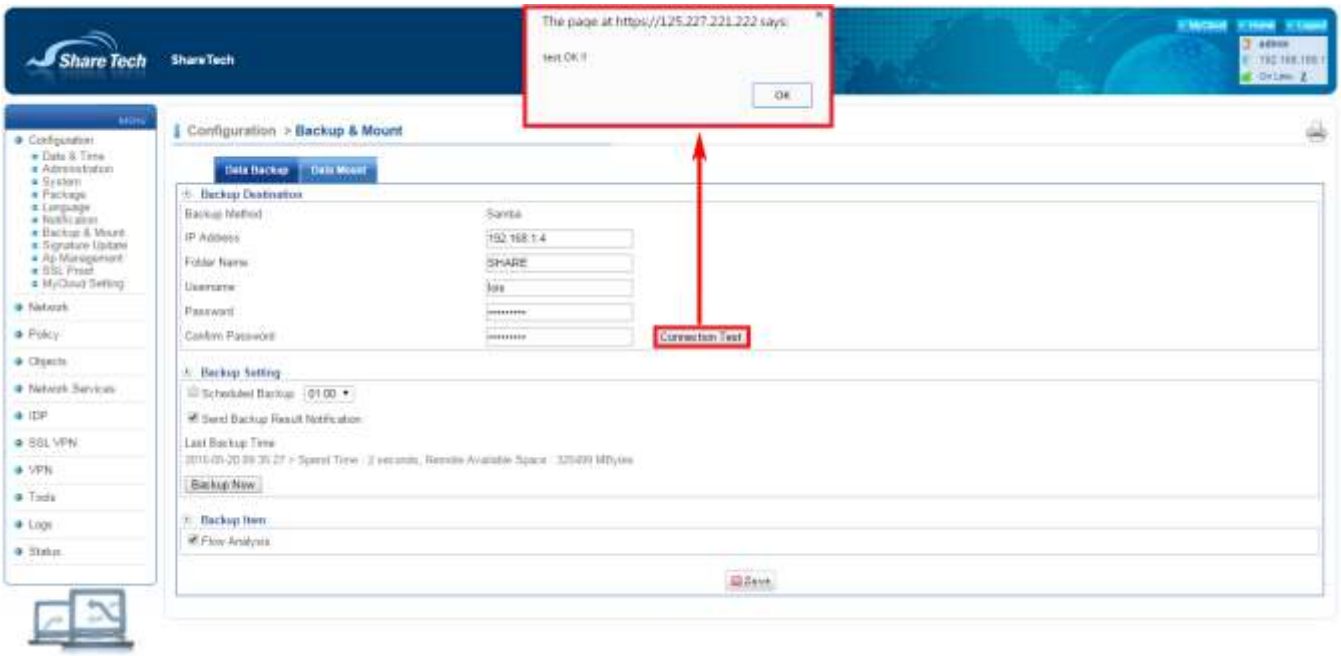


Figure 1-7. 1 Backup & Mount

Backup Setting

- Scheduled Backup: Select when does the system backup data?
- Send Backup Result Notification: User has to go to Configuration > Notification > Notification to set your information first. Then, you will get mail after system backup successfully. (Figure 1-7.3)

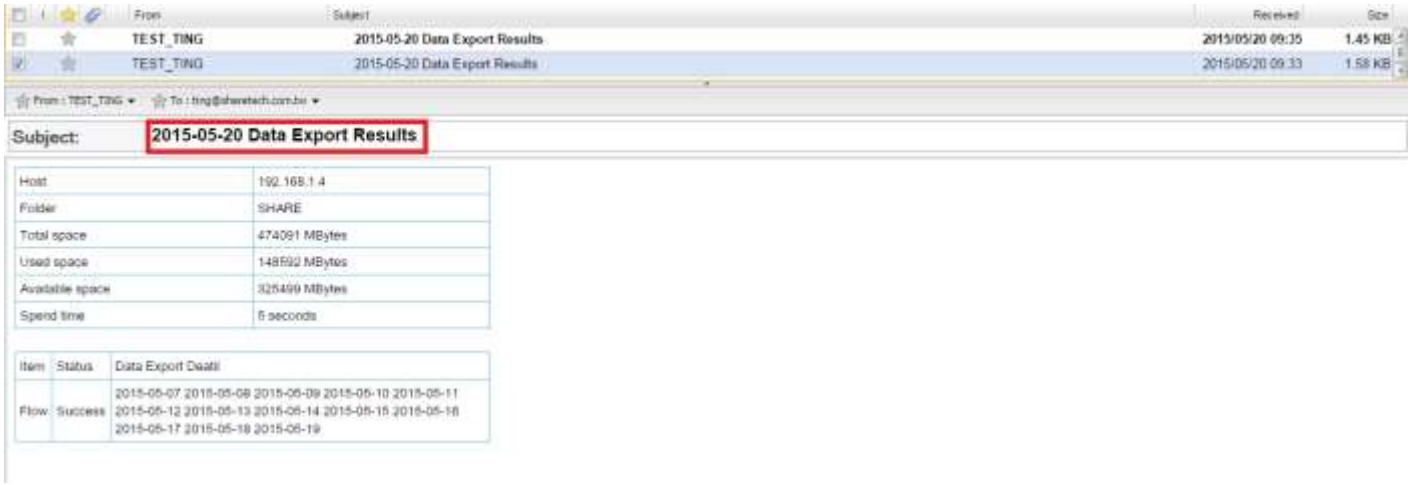


Figure 1-7. 2 Send Backup Result Notification

Click on Backup Now you will see the information as below. (Figure 1-7.4) (Figure 1-7.\53)

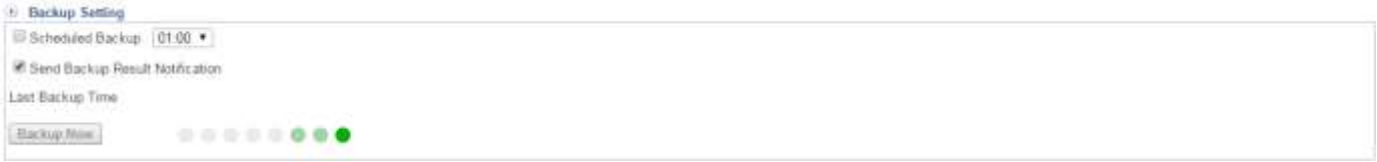


Figure 1-7. 3 Backup Now

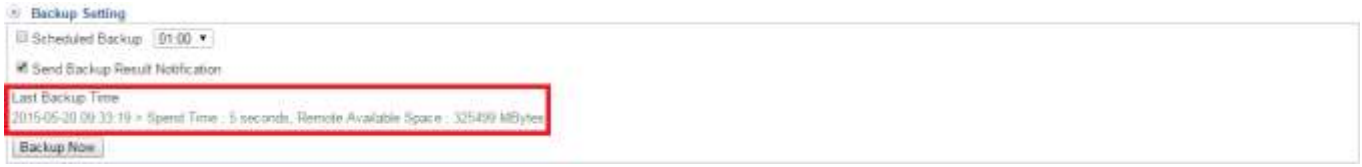


Figure 1-7. 4 backup completed

Backup Item: Flow Analysis (Figure 1-7.6)

Figure 1-7. 5 Backup Item

Data Mount

If you want to see previous contents, but you have ever reset machine to default setting or have ever Clear Data, for these reasons, there are no data contents in this machine hardisk. Fortunately, you have ever use Backup & Mount application to backup contents to another server or computer. Then, you can mount these contents to search Content Record items.

First please click on Access to External Storage, you will see data items that you have ever backup. (Figure 1-7.7)

Figure 1-7. 6 Data Mount

Click on Mount Remote Data (Figure 1-7.8)

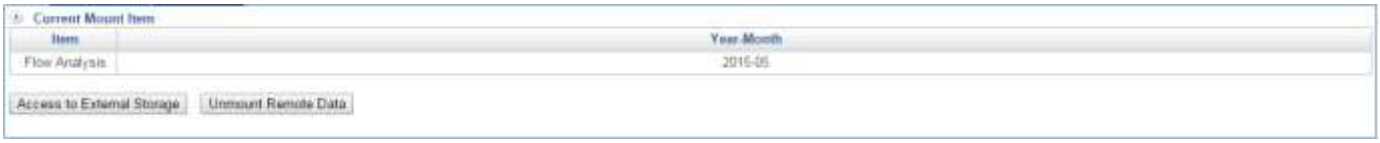


Figure 1-7. 7 Mount Remote Data

User is able to click on Unmount Remote Data if user does not these contents for searching in needed. (Figure 1-7.9)

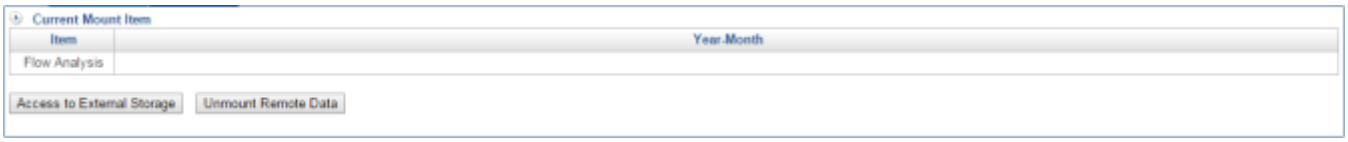


Figure 1-7. 8 Unmount Remote Data

1-8 Signature Update

Signature Update

Select Configuration > Signature Update > Signature Update. (Figure 1-8.1)

Default is manual update.

■ Automatic Update(Figure 1-8.1)

Please select check box, and then system automatically updates the signature version.

Figure 1-8. 1 Signature Update

■ Manual Update(Figure 1-8.2)

To manually update the signature version you can click Check Now to detect signature version.

There are three situation.

1. Already have a new version whether update to a newest version
2. Signature is already the newest version
3. Error→Please check your internet, or allow it through Windows Firewall by opening 80 port.

Figure 1-8. 2 check signature version

1-9 CMS

CMS is Central Management System. This application allows you to view the each ShareTech SG-100N equipment over the network and Internet, but also allows you to backup each configure setting or update firmware from head office. For example, you have 4 sets of SG-100N in one building or different places, and be able to view the each SG-100N interfaces from all of them on the same screen or monitor.

CMS Setting

Select Configuration > CMS > CMS Setting. (Figure 1-9.1)

If Head office WAN IP is 111.252.72.198, and LAN IP is 192.168.1.163
Head office-A office WAN IP is192.168.1.161, and LAN IP is 192.168.99.161
Branch office WAN IP is 60.249.6.184, and LAN IP is 10.10.10.50

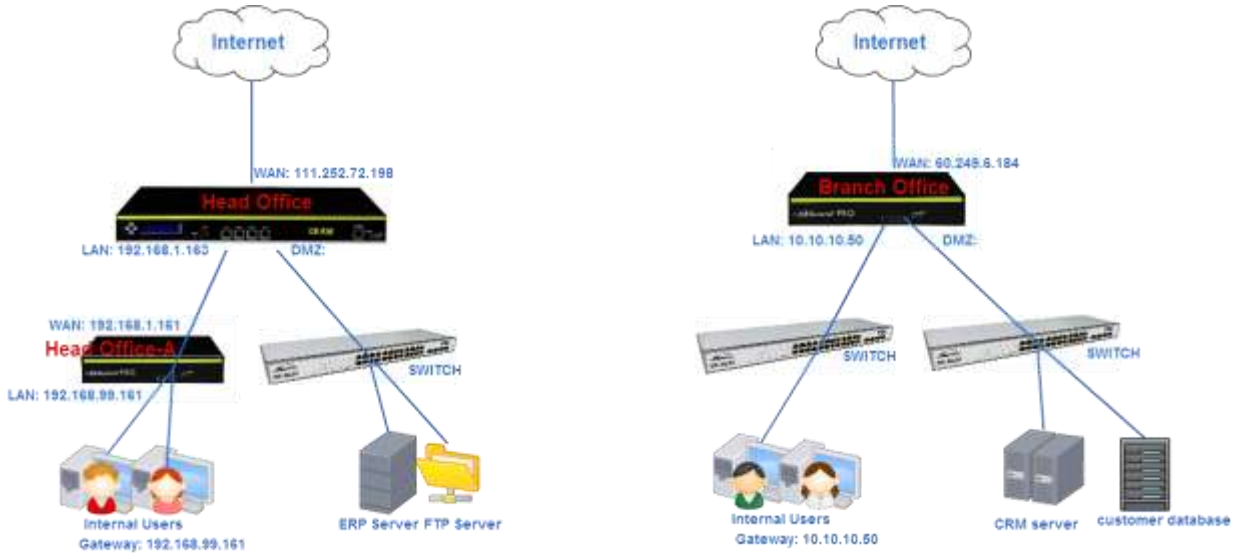


Figure 1-9. 1 CMS Network Architecture

Client site

- Branch office (Figure 1-9.2)
  1. Mode: Client
  2. Server: Enter head office WAN IP 111.252.72.198 or domain
  3. Alias: Enter a name for recognition
  4. Click Save

Figure 1-9. 2 Branch CMS Client setting

- Head office-A (Figure 1-9.3)
  4. Mode: Client
  5. Server: Head office and Head office-A at the same Internal subnet, so enter Head office LAN IP 192.168.163 or domain
  6. Alias: Enter a name for recognition
  7. Click Save

Figure 1-9. 3 Head office-A CMS Client setting

- Head office-Server site
  1. Enable it (Figure 1-9.4)
  2. Choose "server"
  3. Click "New client requests (1) "(Figure 1-9.5)

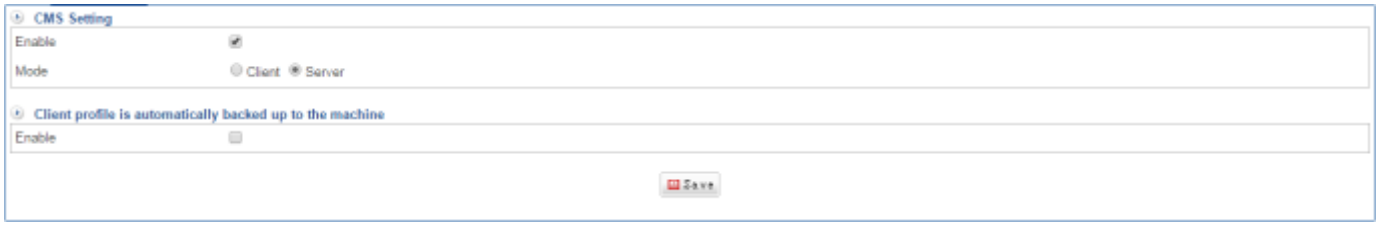


Figure 1-9. 4 CMS server

Figure 1-9. 5 Click “New client requests (1)

4. Click "Accept. " (Figure 1-9.6)

Figure 1-9. 6 it shows CMS client(s)

5. Set up group(Figure 1-9.7)

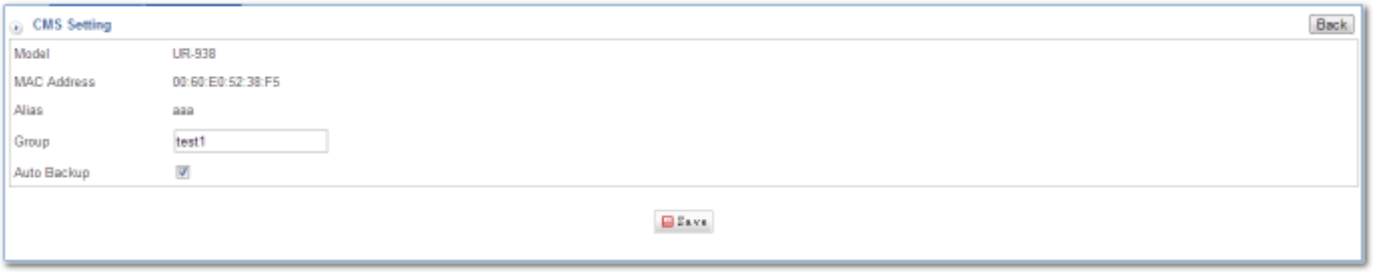


Figure 1-9. 7 it shows CMS client site information

：Connect succeed.

：Connections fail.

Figure 1-9. 8 CMS Lists

1-10 Ap Management

The rise in popularity of smartphones and tablets, combined with enterprise Bring Your Own Device (BYOD) programs, has sent the demand for enterprise Wi-Fi connectivity in many organizations. Wi-Fi becomes as popular and easy to access as cellular is now. You can connect your smartphone or laptop wirelessly at public locations (airports, hotels, coffee shops) to the establish Internet service. The ability to manage network infrastructure from the cloud is likely to be a key technology in coming years. (Figure 1-10.1)

Figure 1-10. 1 AP control

AP Management Setting

Select Configuration > Ap Management > AP Management Setting. (Figure 1-10.2)

- AP Management: Start

Figure 1-10. 2 AP management Setting

■ HiGuard SOHO/HOME : (Figure 1-10.3) (Figure 1-10.4)

1. System > Overview

Figure 1-10. 3 HiGuard SOHO/HOME AP mode

2. Network > AP Management: enable it and enter SG-100N LAN IP

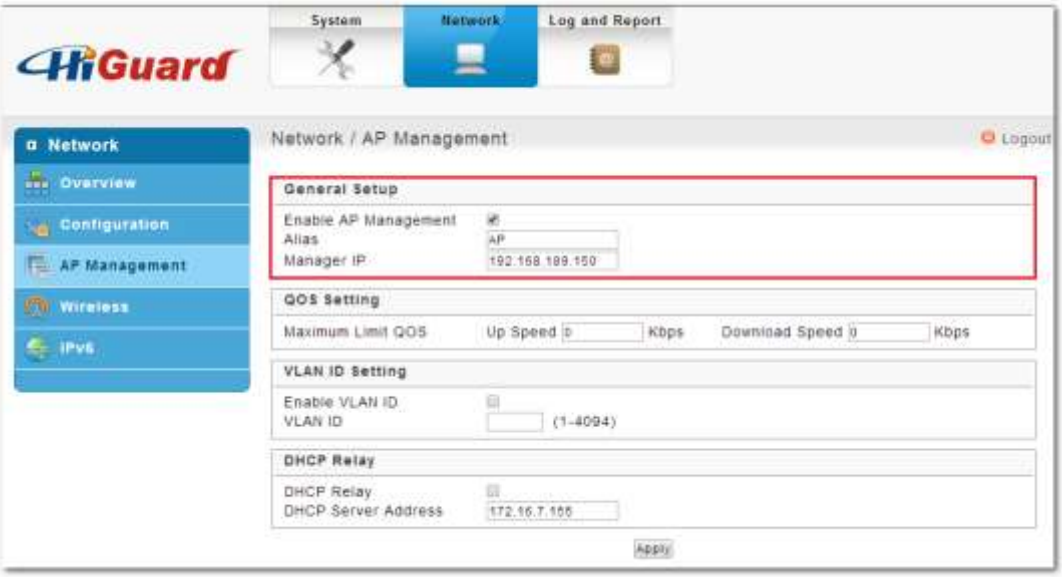


Figure 1-10. 4 HiGuard SOHO/HOME manager IP

■ AP-200: (Figure 1-10.5)

Service > UTM Client: Enable it and enter SG-100N LAN IP

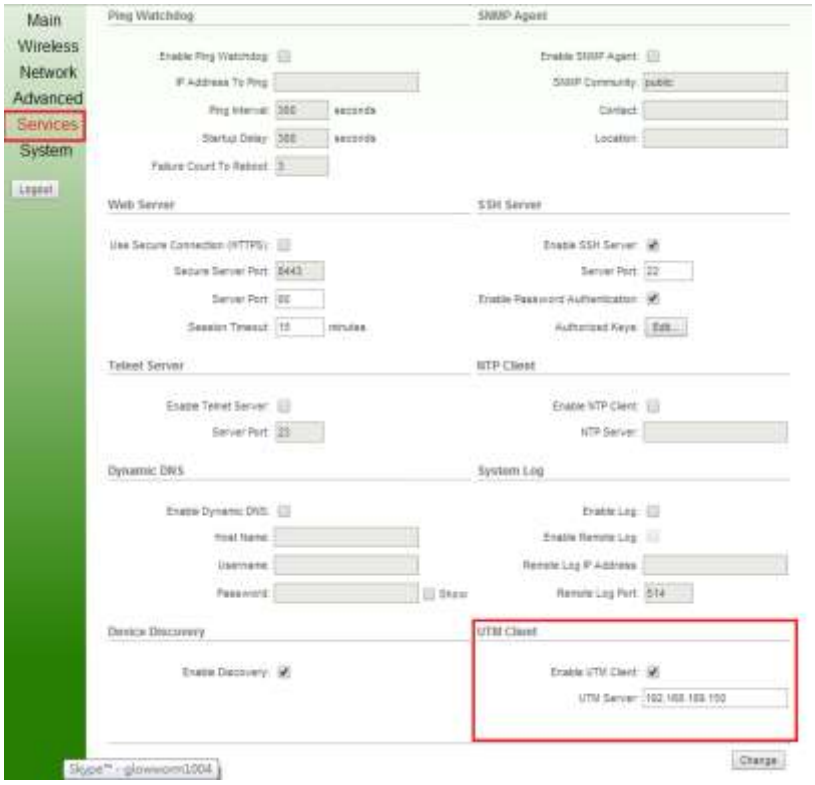


Figure 1-10. 5 AP-200 SG-100N Client

Ap Management

Before “Start” Ap management, please enable DHCP on **Network Services** > **DHCP** (Figure 1-10.6)

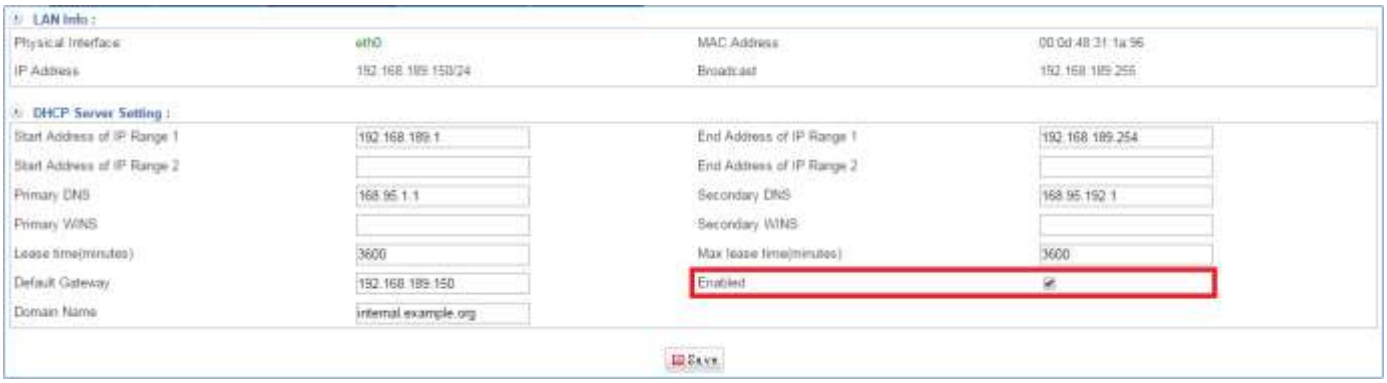


Figure 1-10. 6 DHCP

Select Configuration > Ap Management > Ap Management. (Figure 1-10.7)

■ AP Management Requests

Figure 1-10. 7 Ap Management

Increasing adoption of Wi-Fi service fastens business' Wi-Fi Deployment.

Although Wi-Fi and 3G can be considered complementary technologies, sometimes we choose Wi-Fi service for either budget reasons (especially for multiple devices, can be costly), or technological limitations. Small/medium-sized businesses can be satisfied with a wireless router relying on IT's help, but for larger scale of enterprises, only an integrated management platform can reach the goal of securely connecting all wireless networks.

Easy and efficient management over multi Aps

Centralized architectures have gained popularity recently. Without a single unified controller, it is very difficult for administrators to configure, manage, and rapidly discover which AP is the problematic one among other 20 APs, or even more. ShareTech provides a total AP management solution- HiGuard HOME/SOHO (2 antenna wireless 802.11N/B/G Router supports 2.4 GHz WLAN networks) which prevent from being attacked by malicious softwares, together with a secure, steady, and instant wireless management platform, UR series (SG-100N, including HiGuard PRO) that highly integrate wired and wireless connections. ShareTech SG-100N, a unified platform, is not only a comprehensive firewall solution to the wired enterprises—all frames from WLAN clients have to pass through the WLAN switches to the enterprise network, but also substantially reduces the cost. It centralized wireless network management, monitor flows of each AP, and conclude AP operation details.

ShareTech SG-100N, a wireless AP management platform

ShareTech SG-100N is a single unified controller that is responsible for configuration, control, and management of several HiGuard HOME/SOHO (wireless routers) and AP-200. With these two elements, enterprise can expand their Wi-Fi environment without worries. Each HiGuard wireless

router integrates flows to ShareTech SG-100N which independently manages as a separate network entity on the network. (Figure 1-10.8)

Figure 1-10. 8 ShareTech SG-100N AP Control Platform

On ShareTech SG-100N AP management interface, administrators can easily monitor and manage operation (functioning or malfunction), upload/download flow, and concurrent users on every AP ShareTech wireless AP management platform provides complete and efficient Wi-Fi network security to protect Wi-Fi users from being attacked. (Figure 1-10.9)

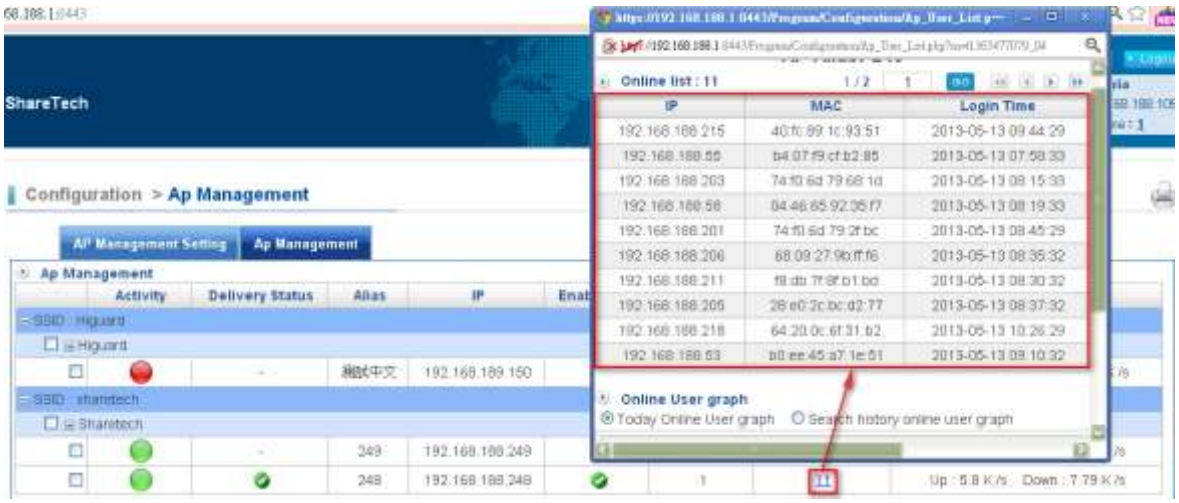


Figure 1-10. 9 Detailed User List on Every AP

1-11 SSL Proof

If you don't like to show kinds of SSL notification web page, please apply for your own SSL Certification at local SSL Certification organizations. It depends on company domain, your company WAN IP, company logo, and others. (Figure 1-11.1)

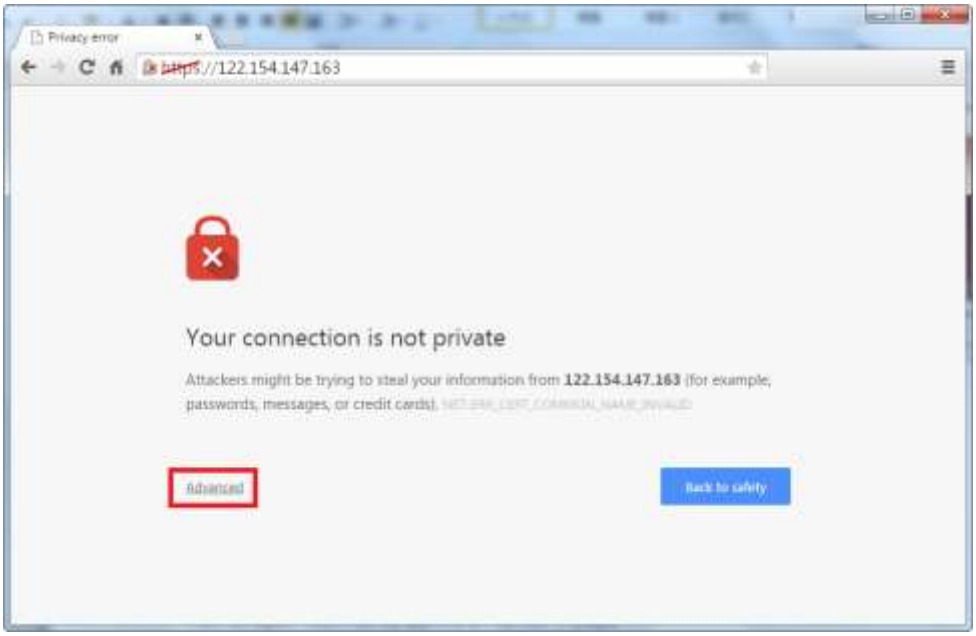


Figure 1-11. 1 Privacy error

SSL Proof Set

Noted: ShareTech doesn't suggest and guarantee any one of SSL Certification organizations, the following are examples.

GeoTrust: https://www.geotrust.com/

Symantec: http://www.symantec.com/verisign/ssl-certificates?inid=us_ps_flyout_prdts_ssl

StartSSL PKI: http://www.startssl.com/

Select Configuration > SSL Proof > SSL Proof Set.

1. Please import three files (server.Key, server.crt, and intermediate certificate) which you apply for your own SSL Certification from organizations. (Figure 1-11.2)

Figure 1-11. 2 import SSL Proof

2. Sometimes, organizations will ask for server.cst and server.key. Therefore, please enter information and download files. Offer these two files to SSL Certification organization. (Figure 1-11.3)

Figure 1-11. 3 Enter SSL Proof

It will be green browser if install SSL Certification. (Figure 1-11.4)

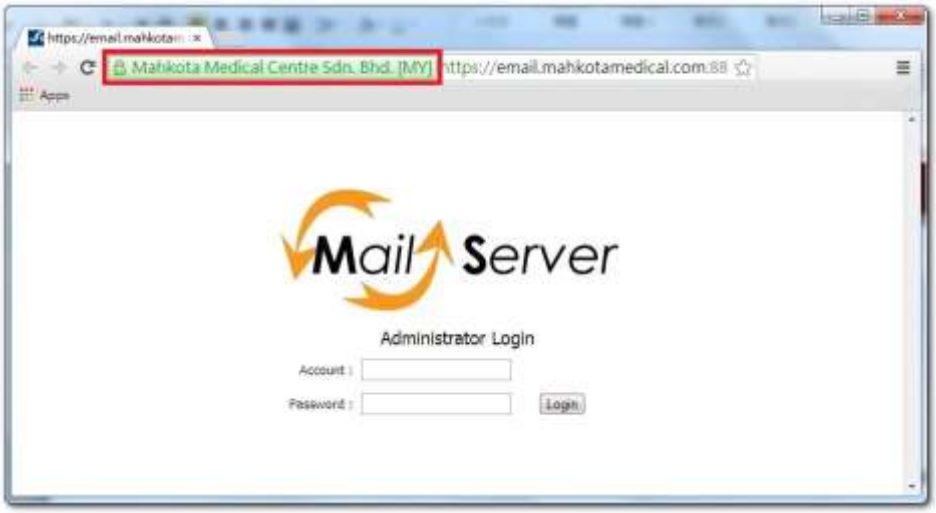


Figure 1-11. 4 green browser

1-12 MyCloud Setting

SG-100N comes with a slick cloud storage solution for SMB to have their own private cloud ensuring safety, integrity and real-time availability. My Cloud satisfies users with easy access, multi-language support, real-time file synchronization, group accounts management, priority-based control, and online data storage of all type of files. Employees can store, share and access their important business files anytime, anywhere using any number of compatible devices and almost any browser. Best of all, SG-100N is a firewall with effective protection which can greatly reduce important business data leakage. (Figure 1-12.1)

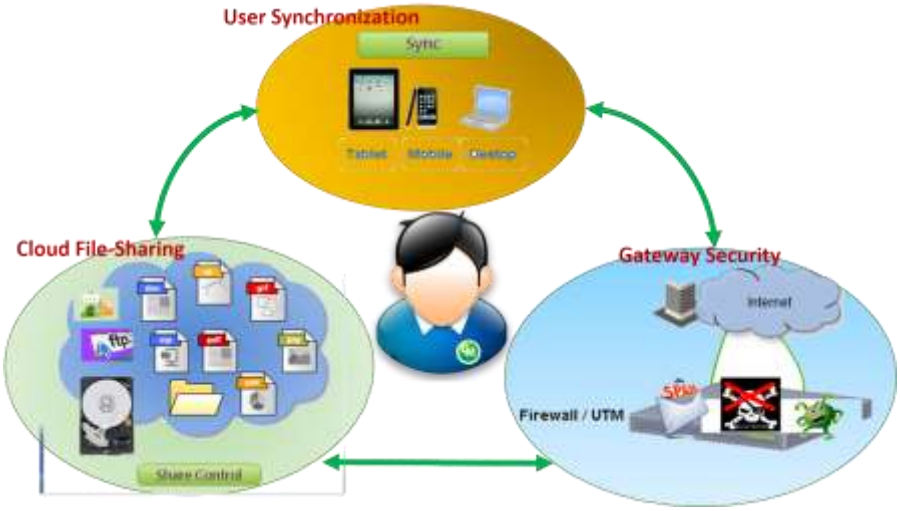


Figure 1-12. 1 My Cloud

MyCloud Setting

Select Configuration > My Cloud Setting > MyCloud Setting (Figure 1-12.2)

MyCloud Setting

- Http Port Setting: allow Http when you enabled it
- Https Port Setting: allow Https when you enabled it

Restart MyCloud service

- Restart MyCloud service:

Reset MyCloud admin password

- Reset MyCloud admin password: enter a password for admin

Default password is "admin"

Figure 1-12. 2 MyCloud Setting

You are able to login MyCloud as the following steps:

1. Administrator can click on MyCloud to login MyCloud system. (Figure 1-12.3)

Figure 1-12. 3 Menu Bar

2. Or open the browser; enter Port 1, or Port 2 IP in the address bar. (Figure 1-12.4)
   Default username / Password: admin/ admin

Figure 1-12. 4 enter IP to login My cloud

Login completed (Figure 1-12.5)

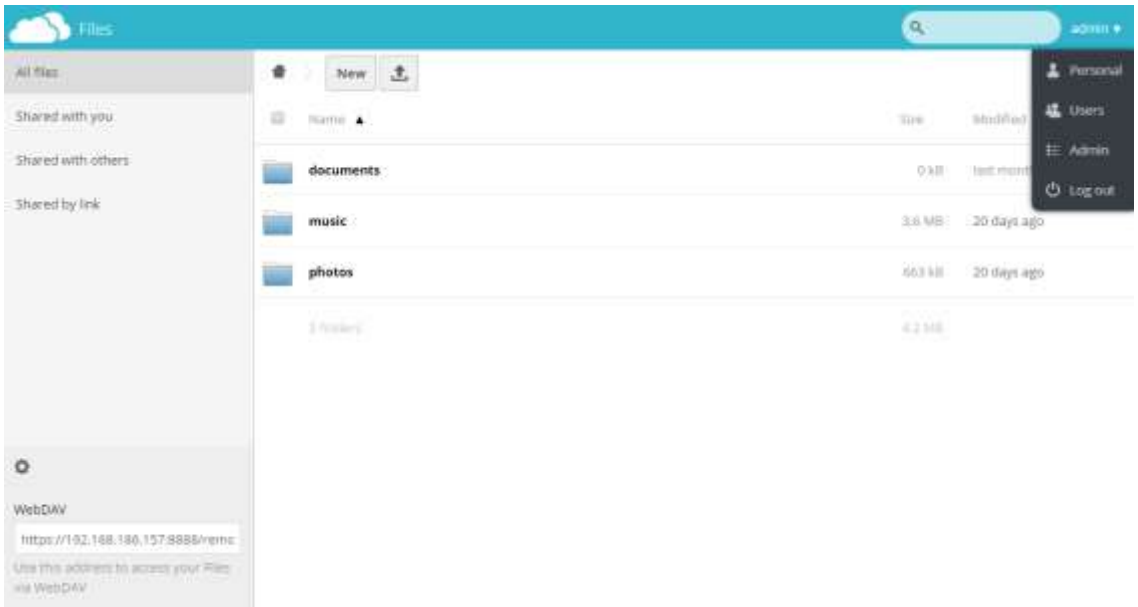


Figure 1-12. 5 MyCloud Homepage Information

Personal

- Password: set up Adminisrtator's password (Figure 1-12.6)
- Full Name: set up Adminisrtator's username (Figure 1-12.6)
- Language: Choose your native language (Figure 1-12.6)

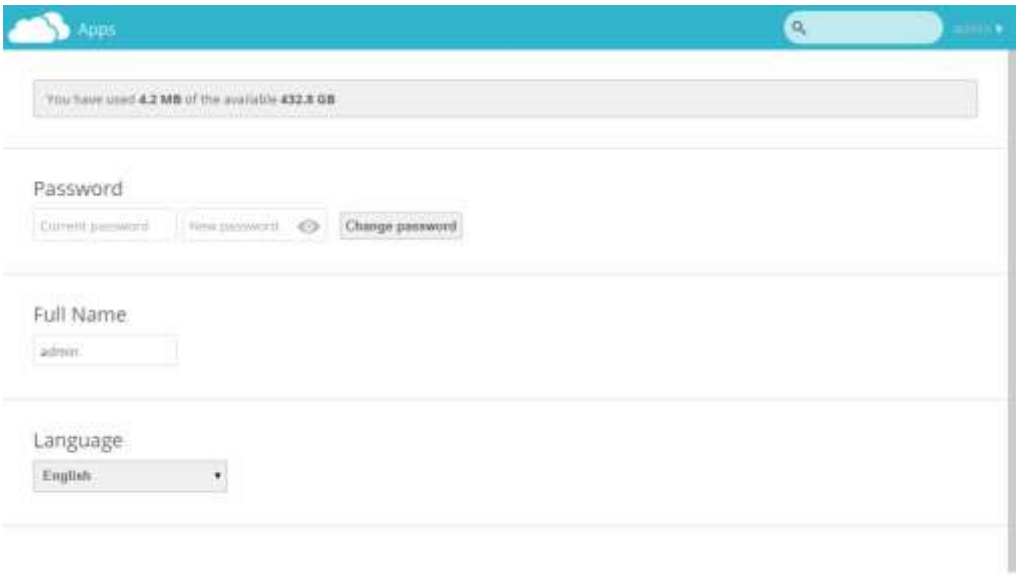


Figure 1-12. 6 Password, Full Name, and Language

Users

Shows every group and its members

Members who are in Group (admin) have high permission to manage settings. (Figure 1-12.7)

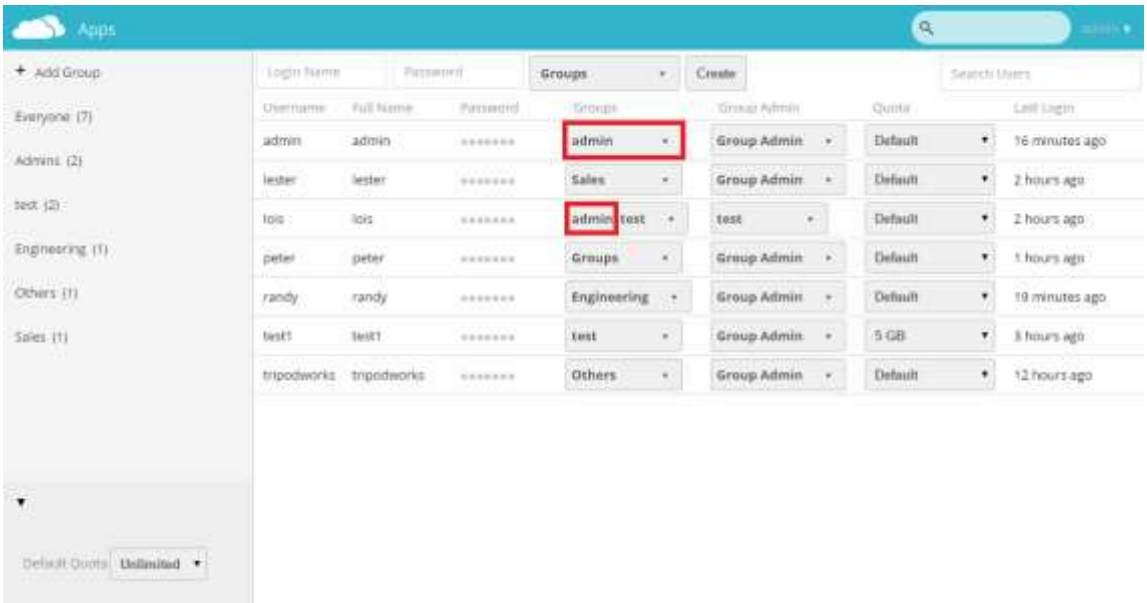


Figure 1-12. 7 High Permission to manage settings.

■ Add a New Group(Figure 1-12.8)

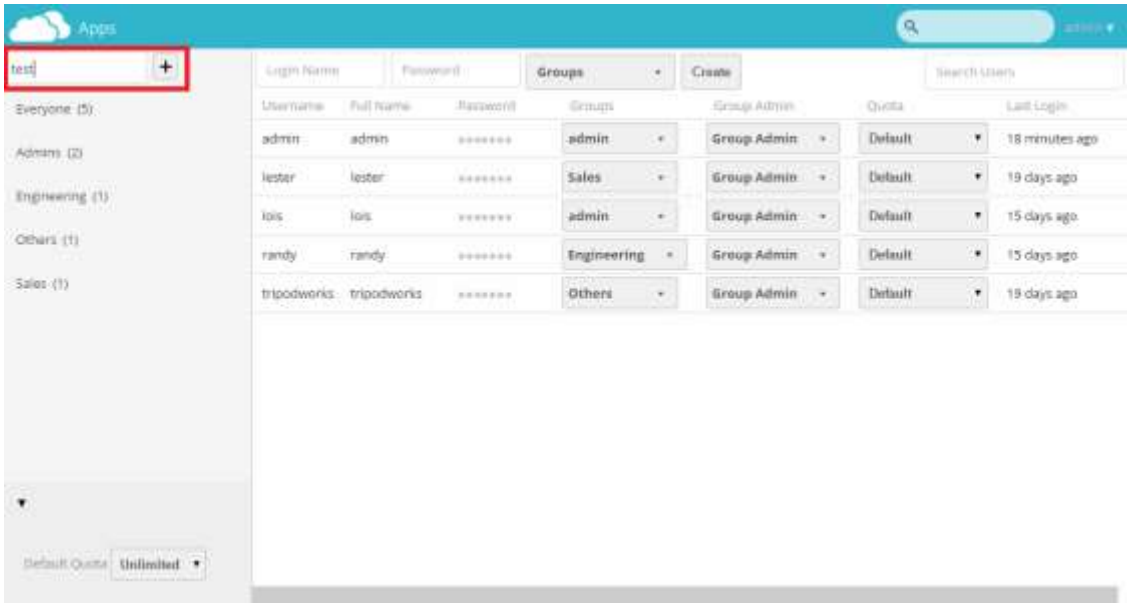


Figure 1-12. 8 Add a new GroupAdd a new member into the group. (Figure 1-12.8)

■ Add a New member into a group (Figure 1-12.9)

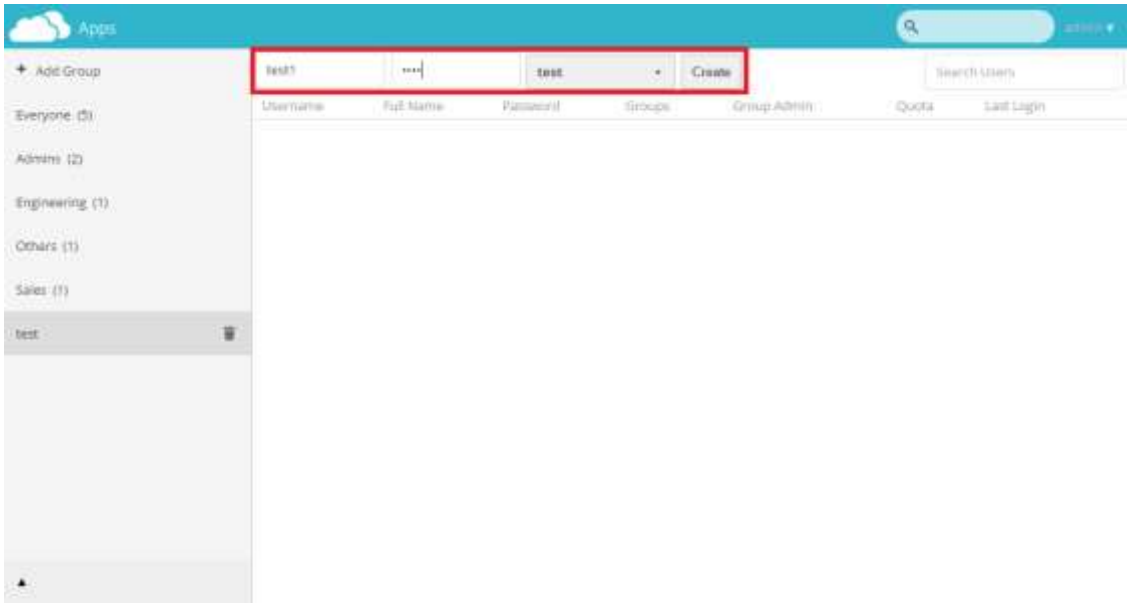


Figure 1-12. 9 Add a new member

■ Set up users' Quota (Figure 1-12.10)

Default Quota: unlimited

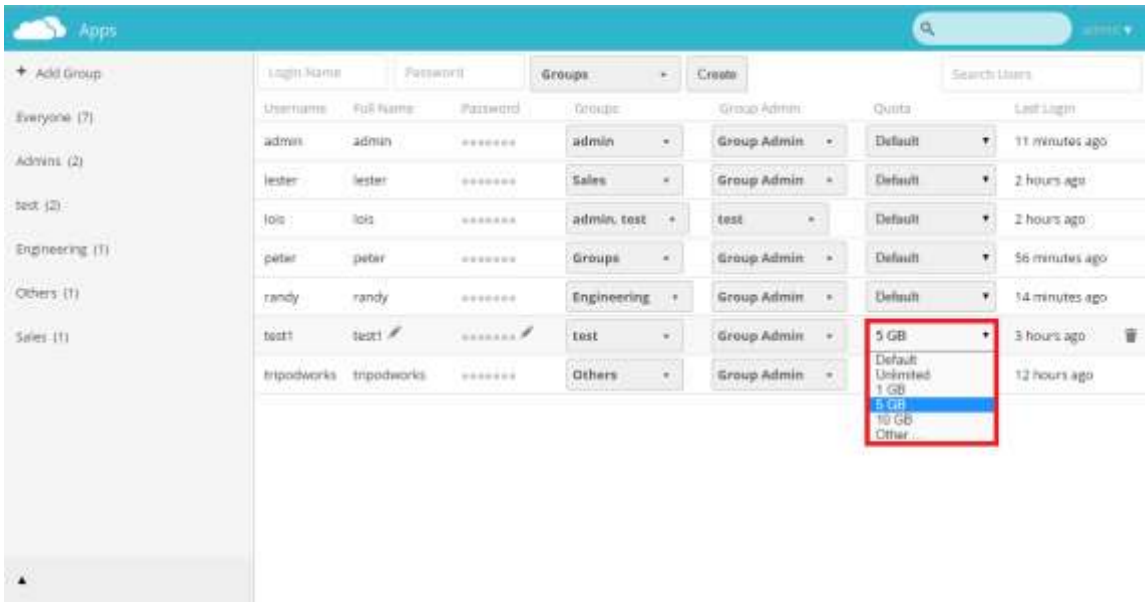


Figure 1-12. 10 Set Up user's Quota

■ A member is able to be with more than a group (Figure 1-12.11)

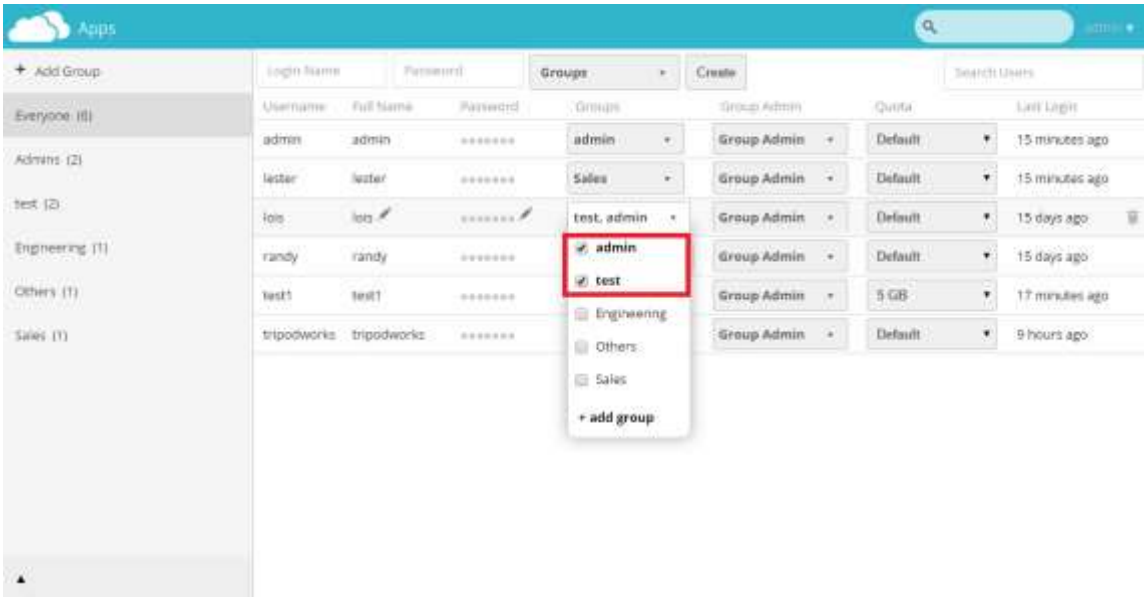


Figure 1-12. 11 a member within two groups

Group Admin: group leader (Figure 1-12.11) Others are its' members.

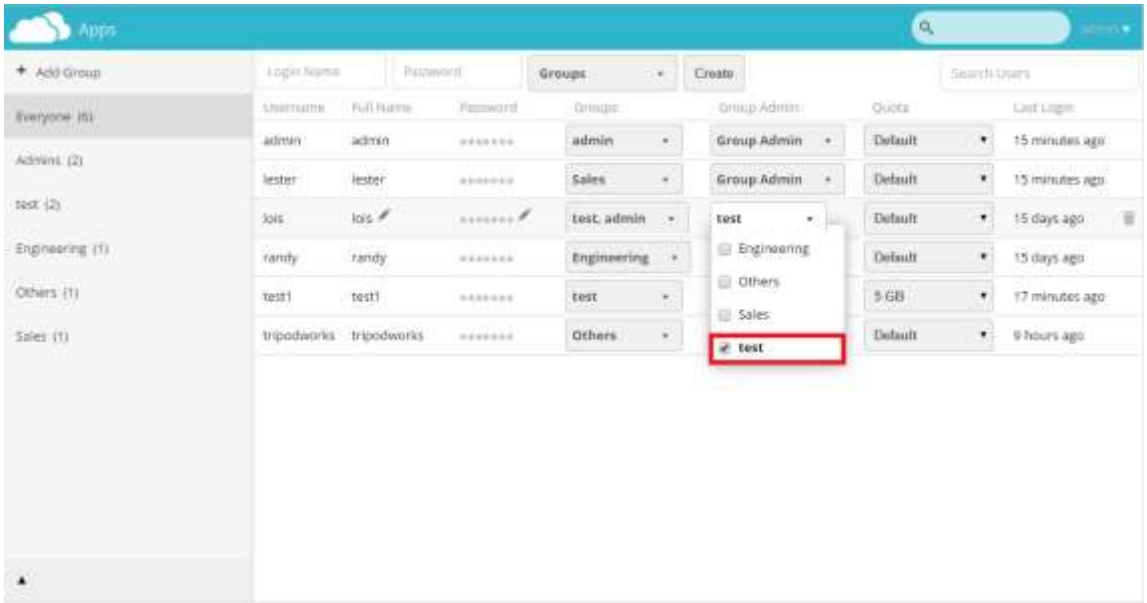
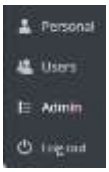


Figure 1-12. 12 Group admin

Admin



HDD usage: it shows total HDD usage (Figure 1-12.13)

Depend on your HDD usage. Default is 320G

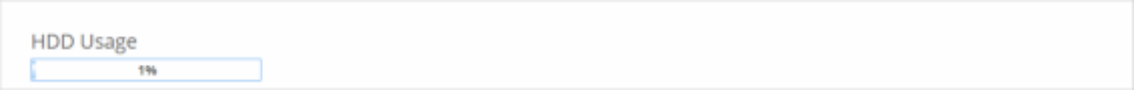


Figure 1-12. 13 HDD usage

File handling (Figure 1-12.14)

maximum Upload possible: 2 GB

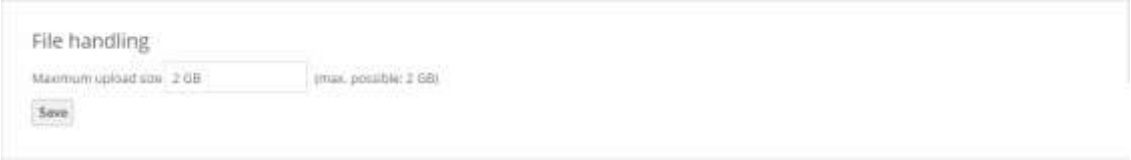


Figure 1-12. 14 File handling

Remote Shares

- Allow other instances to mount public links shared from this server
- Allow users to mount public link shares

Upload Logo

- Login Logo (Figure 1-12.15)

Figure 1-12. 15 Login Logo

- Logined Logo(Figure 1-12.16)

Figure 1-12. 16 Logined Logo

■ Share Link Logo(Figure 1-12.17)

When you copy your file link and share it with your friends, your friends will

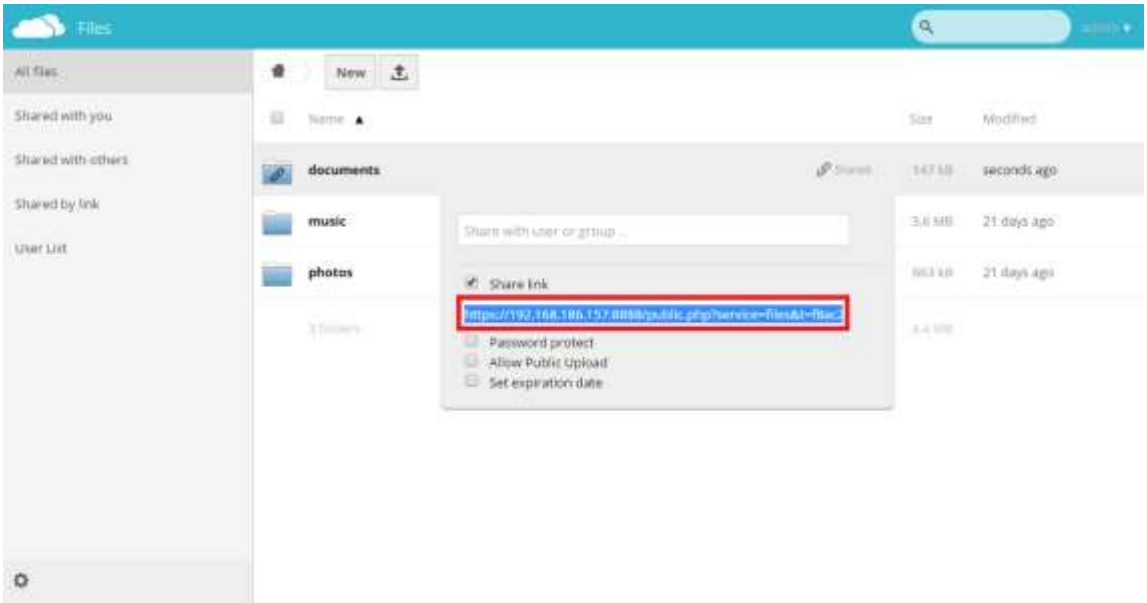


Figure 1-12. 17 Copy Link

Your friends will open the browser; enter share link in the address bar, (Figure 1-12.18) will see this logo which you uploaded

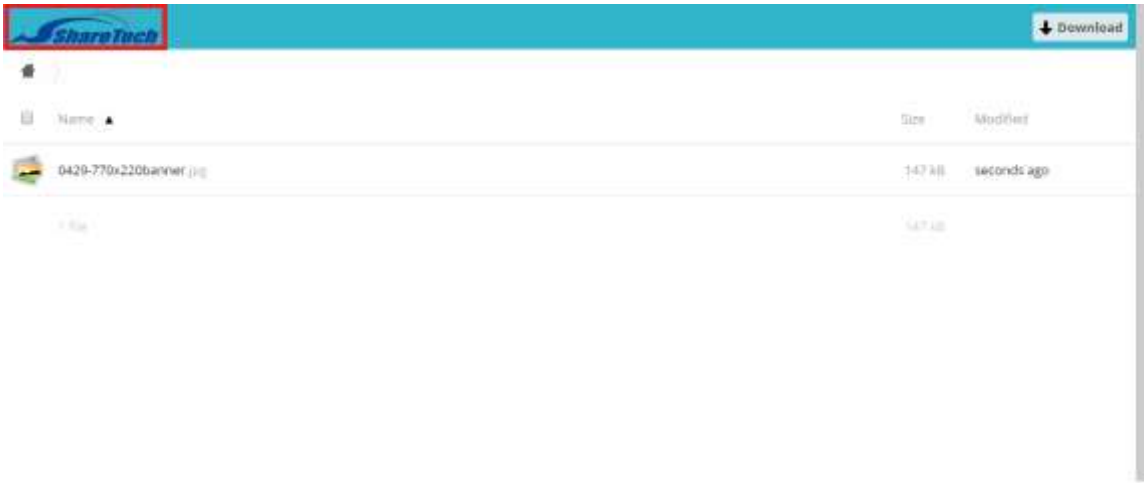


Figure 1-12. 18 Share Link Logo

■ Page icon (Figure 1-12.19)

Figure 1-12. 19 Page icon

■ Page icon(iPad, iPhone)

Background Color (Figure 1-12.20)

Figure 1-12. 20 Background Color

■ Login BackGround: Default is #5ED8EE and #17A4BE

Example: #E9EE5E #BE1717(Figure 1-12.21)

Figure 1-12. 21 Login BackGround

- Logined Logo BackGround: default #31B5CD

Example: #4B31CD(Figure 1-12.22)

Figure 1-12. 22 Logined logo BackGround

Upload User Manual

- Upload User Manual: upload a file which guide user how to use their cloud files. (Figure 1-12.24)

File extension: pdf, and only one file existed (Figure 1-12.23)

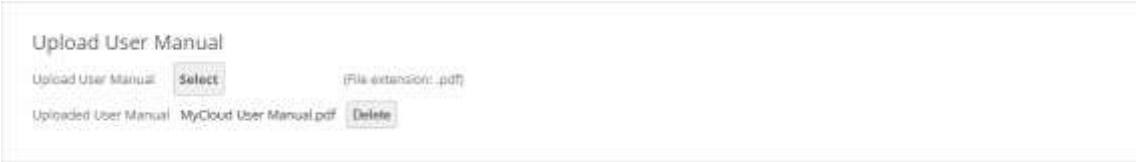


Figure 1-12. 23 Uploaded User Manual

Figure 1-12. 24 I User Manual

User List (Figure 1-12.25)

- Enable User List: every users has permission to see each other

Members who are in Admin Group have high to manage settings.

Default: disable

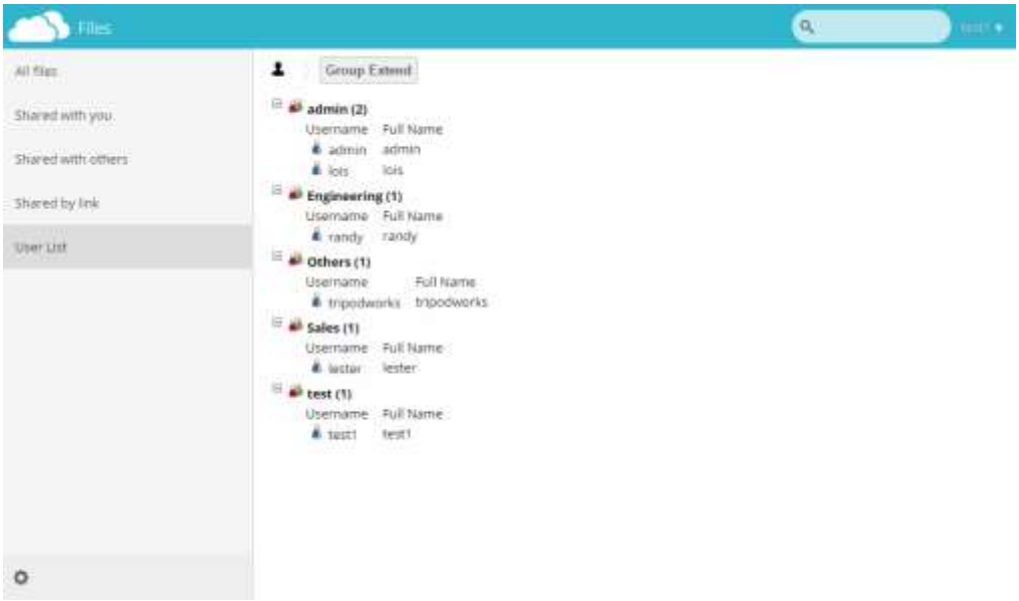


Figure 1-12. 25 User List

Sharing

- Allow apps to use the Share API
- Allow users to share via link

Enable (Figure 1-12.26) (Figure 1-12.27)

Disable (Figure 1-12.28) (Figure 1-12.29)

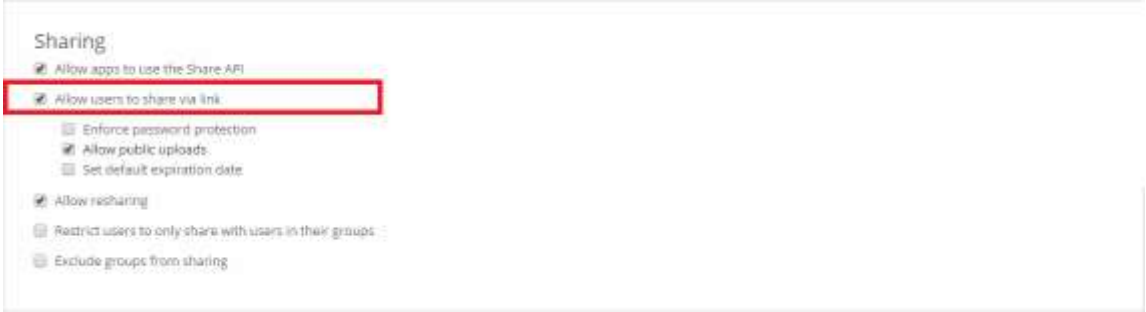


Figure 1-12. 26 Allow users to share via link-1

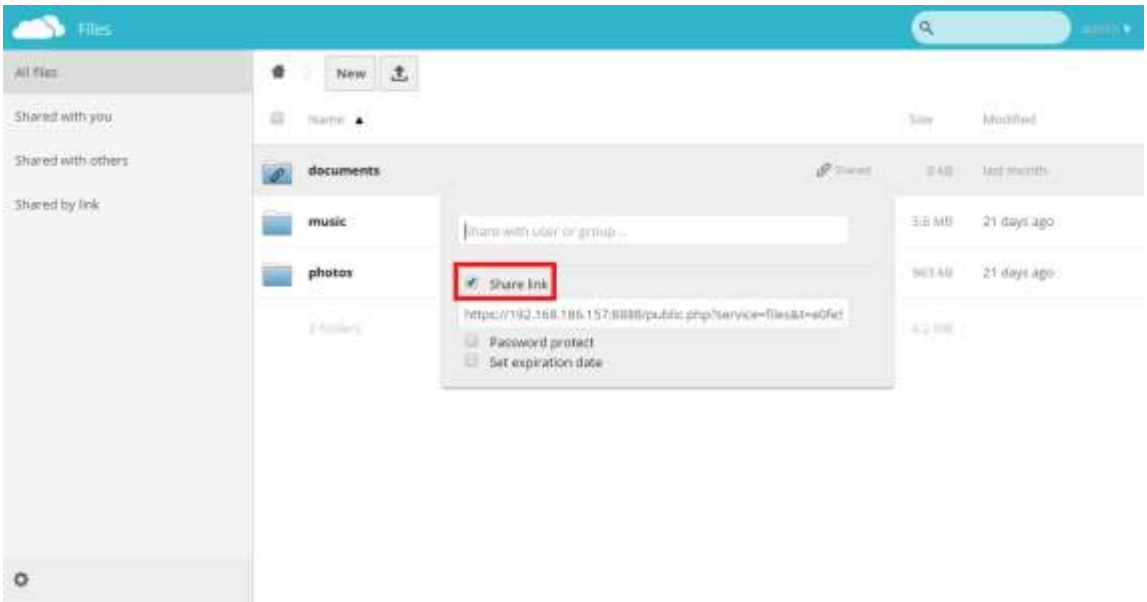


Figure 1-12. 27 Allow users to share via link-2

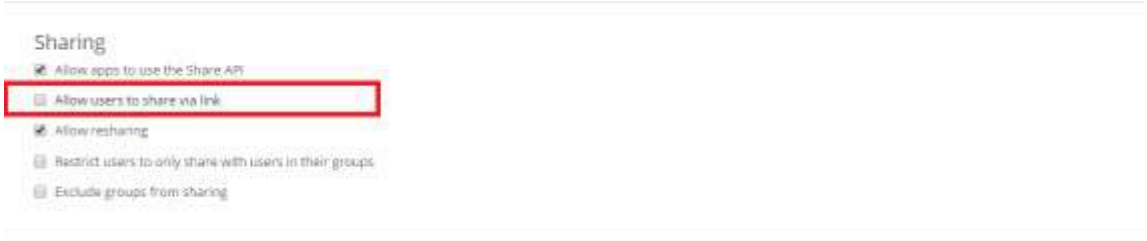


Figure 1-12. 28 disable “Allow users to share via link”-1

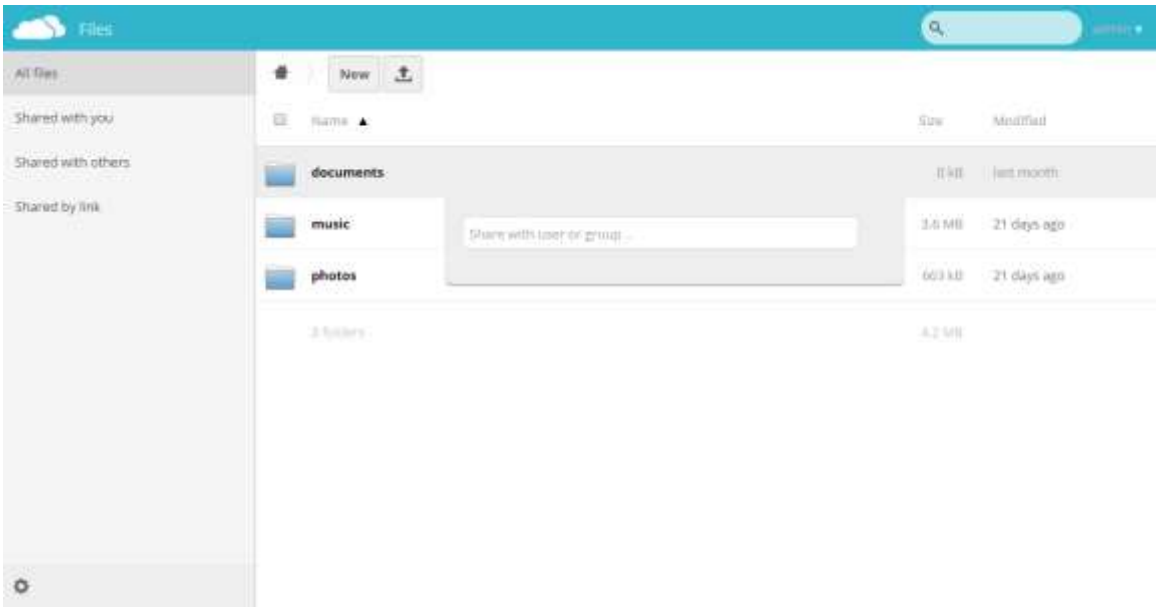


Figure 1-12. 29 disable “Allow users to share via link”-2

1. Enforce password protection: must enter password for protecting. (Figure 1-12.30)

Default: Disable

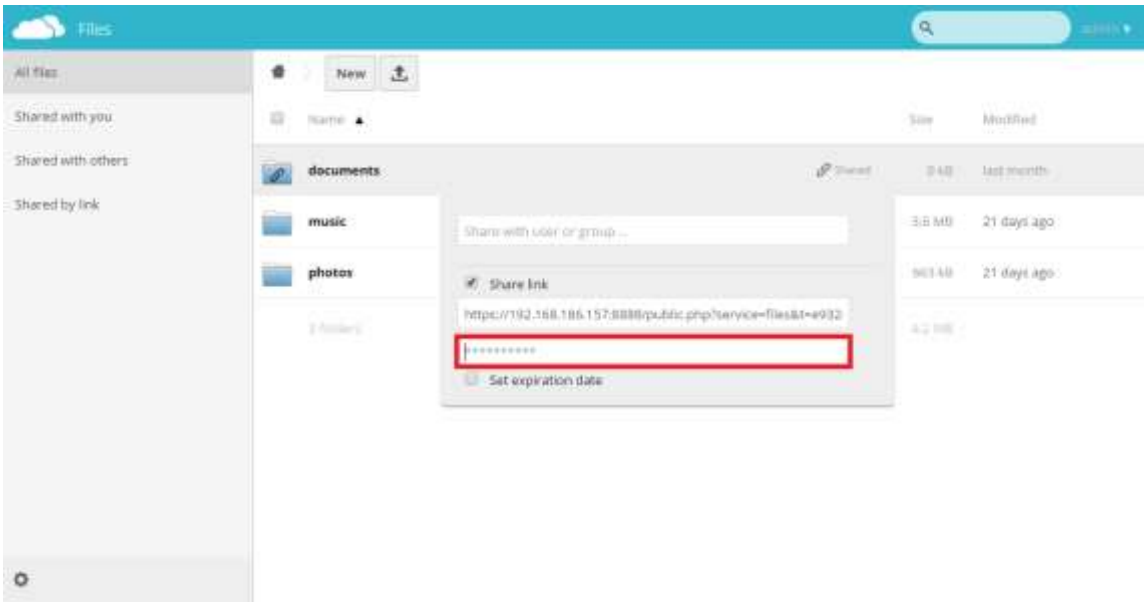


Figure 1-12. 30 Enforce password protection

2. Allow public uploads: users are able to decide whether others upload files or not (Figure 1-12.31)

Default: Enabled

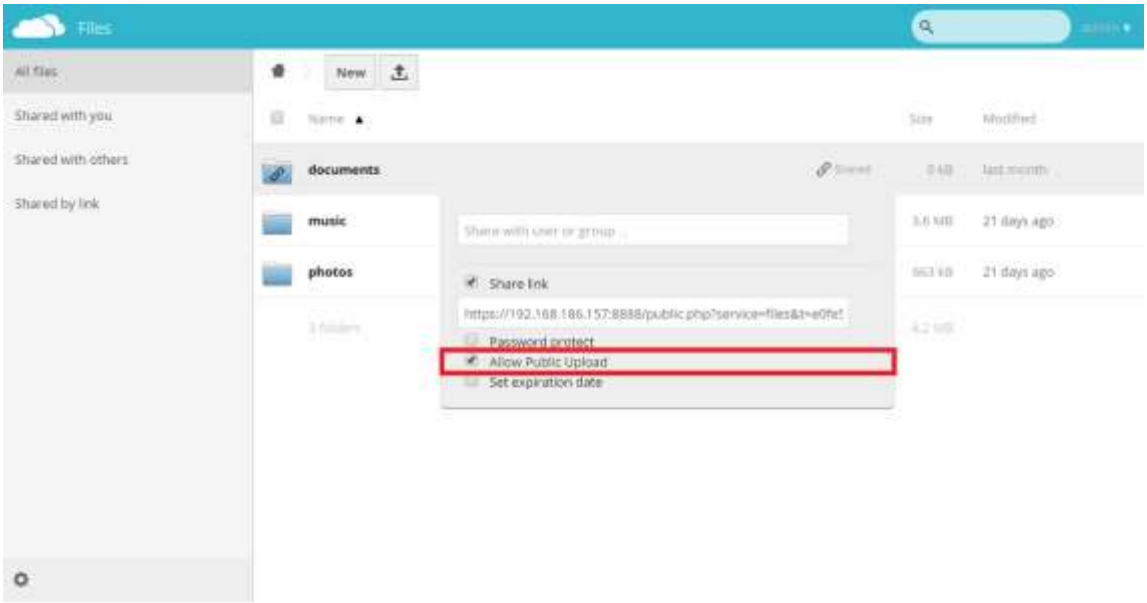


Figure 1-12. 31 Allow public upload

3. Set default expiration date: The public link will expire no later than 7 days after it is created(Figure 1-12.32)

Default: Disable

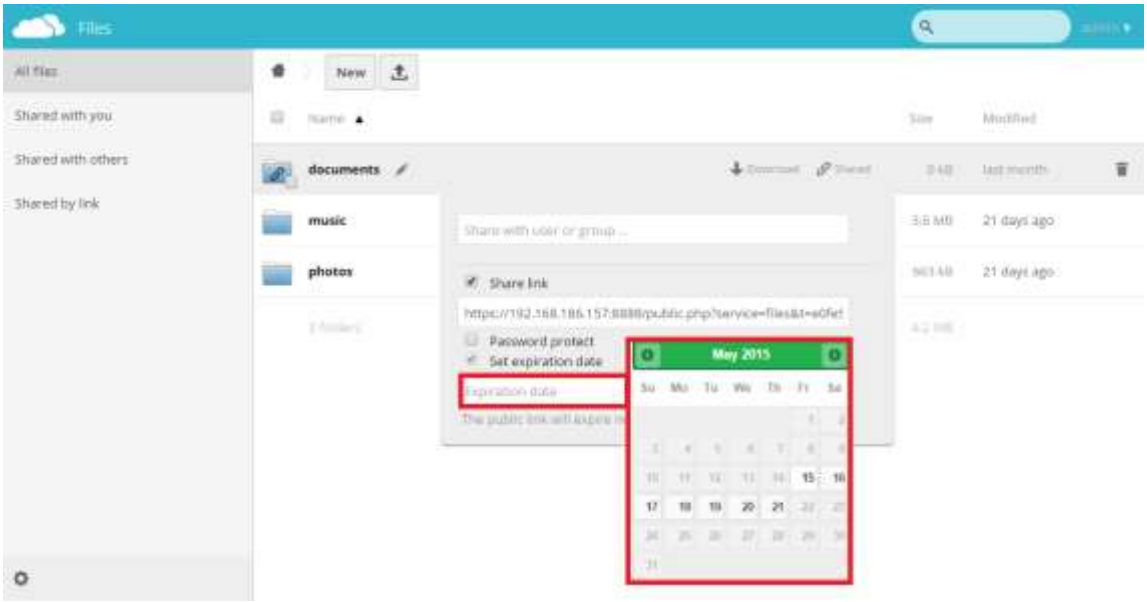


Figure 1-12. 32 Set default expiration date

■ Allow resharing

Default: Enabled

■ Restrict users to only share with users in their groups

Default: Enabled(Figure 1-12.33)

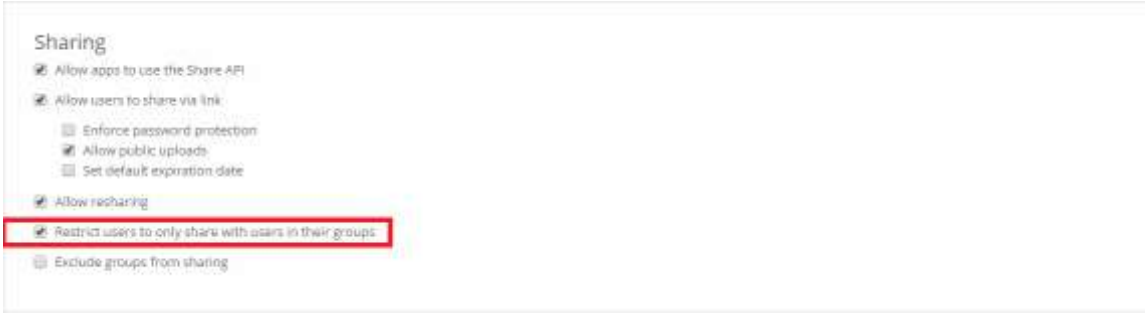


Figure 1-12. 33 Restrict users to only share with users in their groups-1

admin and lois are in the same group so that they can share files each other only. However, both admin and lois are not able to share files to others. (Figure 1-12.34)

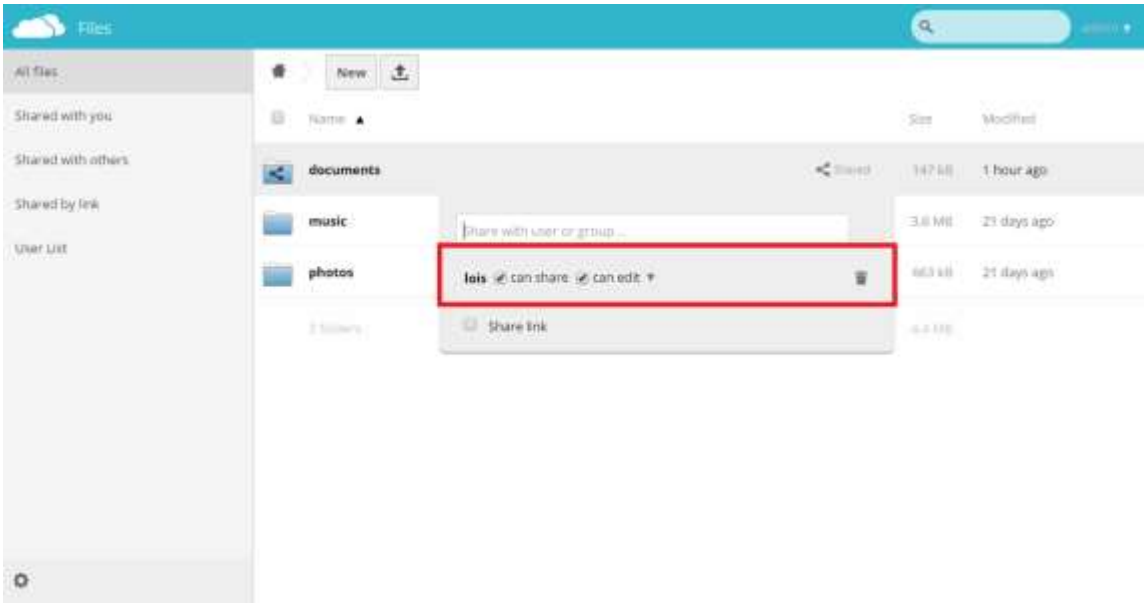


Figure 1-12. 34 Restrict users to only share with users in their groups-2

Here is the other example, Disable(Figure 1-12.35)

Figure 1-12. 35 Disable “Restrict users to only share with users in their groups”

admin is able to share its files with others even if different groups. (Figure 1-12.36)

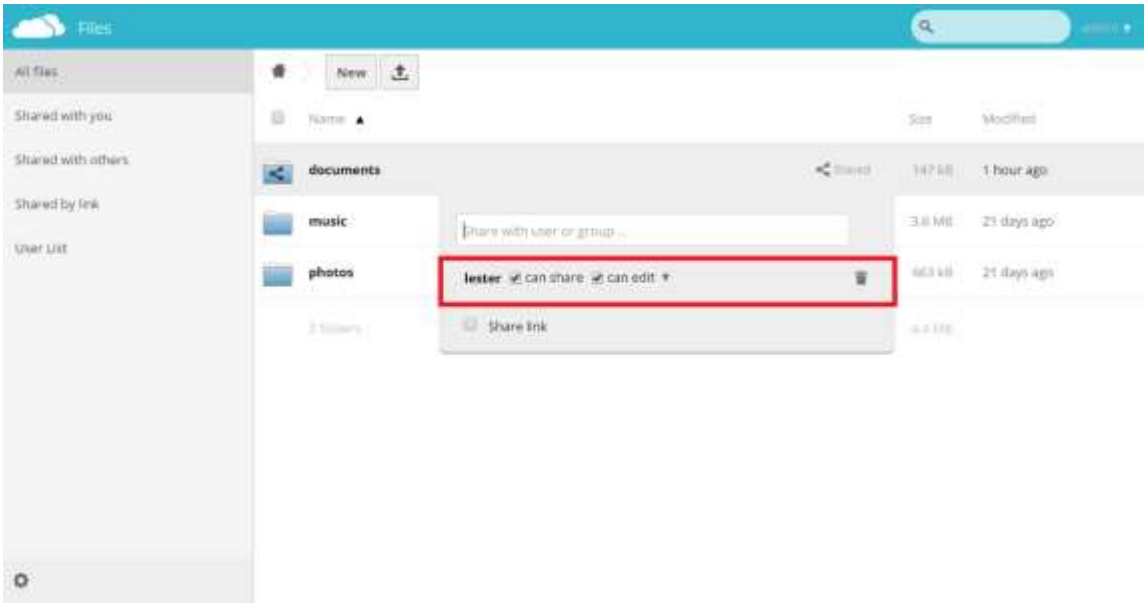


Figure 1-12. 36 admin able to share its file with others

- Exclude groups from sharing: These groups will still be able to receive shares, but not to initiate them. (Figure 1-12.37)

Default: Disable

Example: Enable it, let's see what's happened.

Figure 1-12. 37 Enable "Exclude groups from sharing"

So others are still share their own file with Randy, however, Engineering group members who are not able to share their files to others. (Figure 1-12.38)

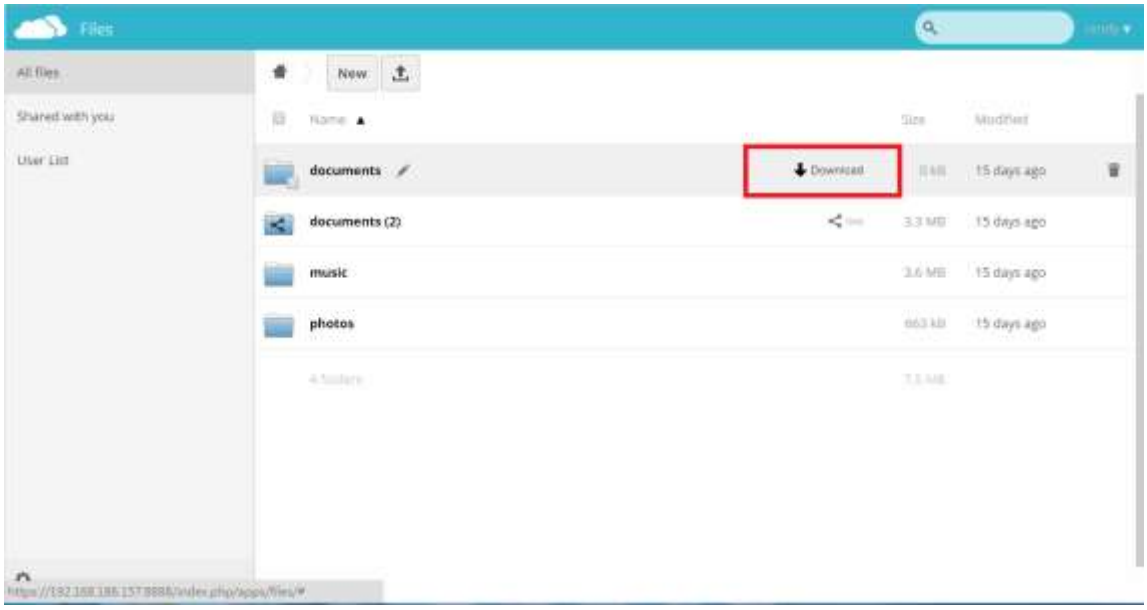


Figure 1-12. 38 Exclude groups from sharing

Security

- Enforce HTTPS: Forces the clients to connect to via an encrypted connection.

My Cloud Homepage Information:

All files (Figure 1-12.39)

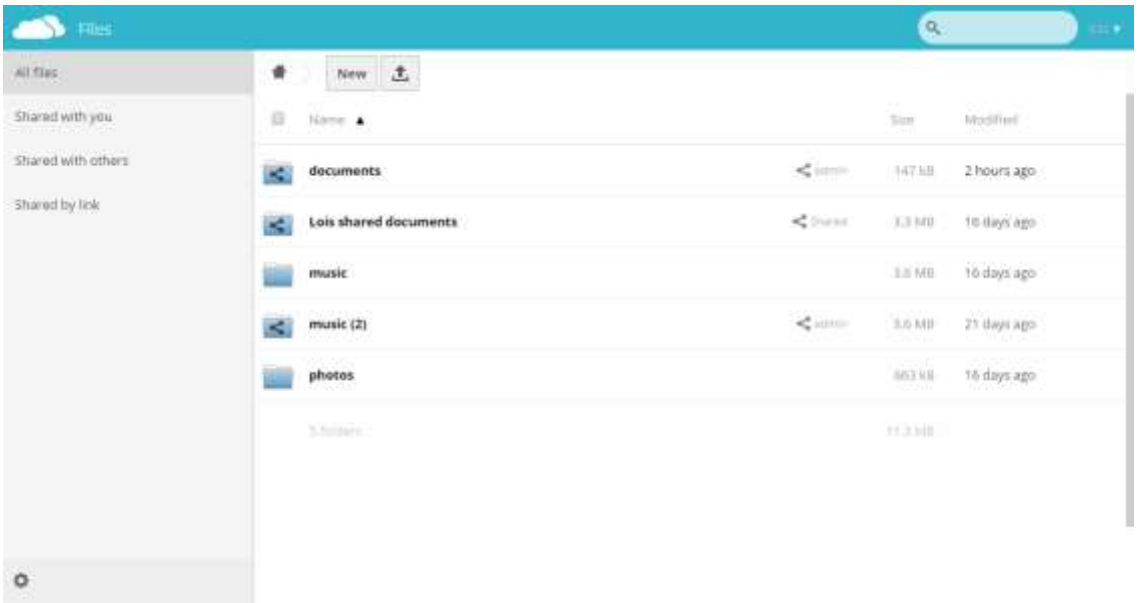


Figure 1-12. 39 All files

Shared with you (Figure 1-12.40)

you are able to click on Unshare to unshare it.

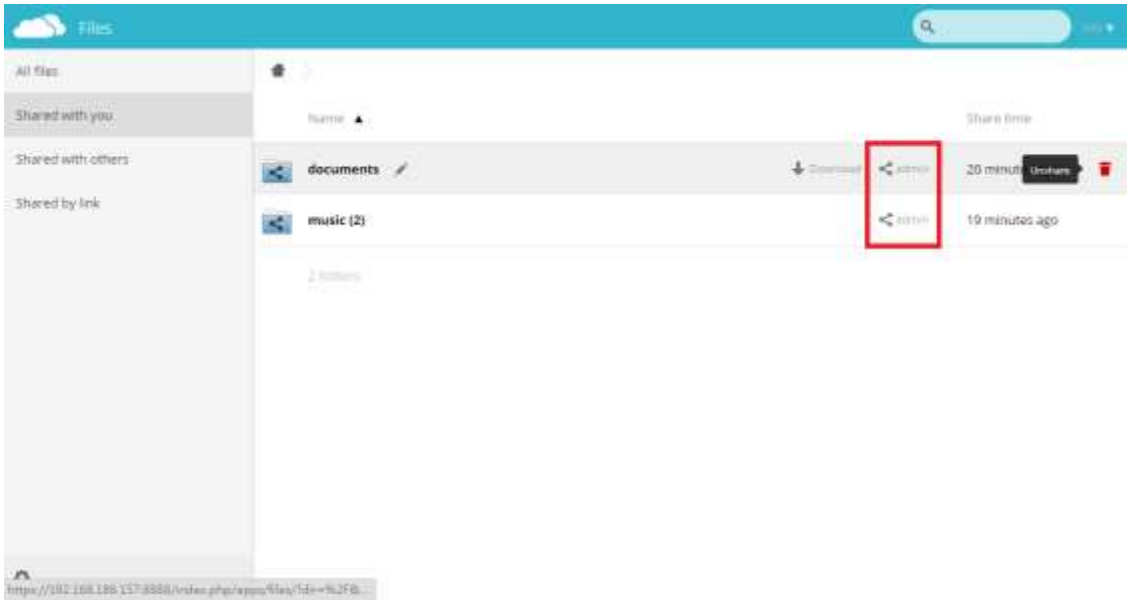


Figure 1-12. 40 Shared with you

Shared with others

You have shared this documents with randy(Figure 1-12.41)

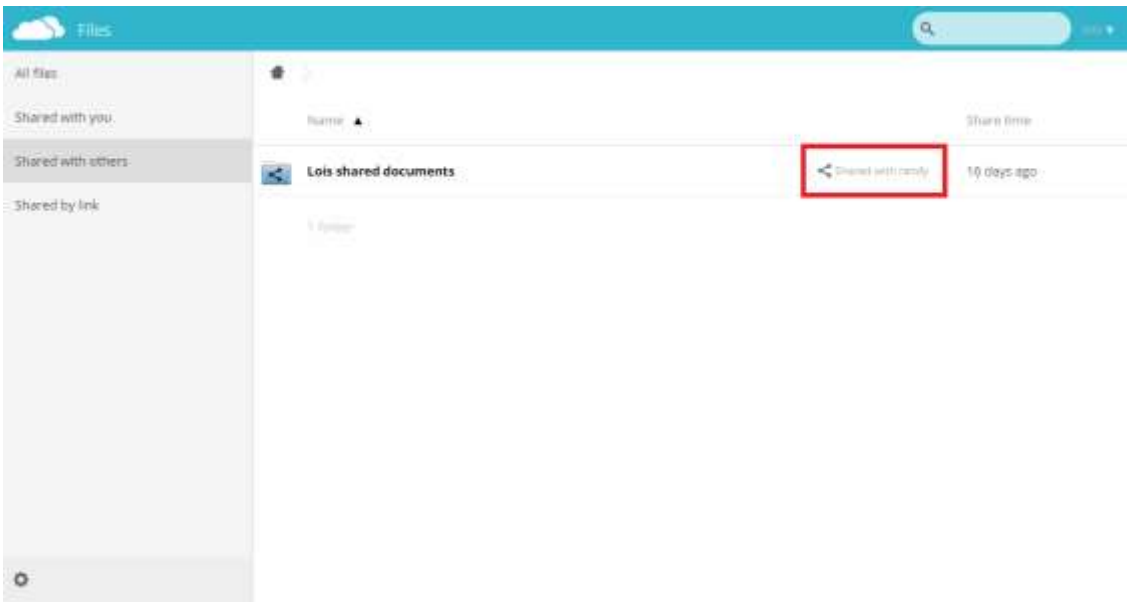


Figure 1-12. 41 Shared with others

Shared by Link

You haven't shared any files by link yet. (Figure 1-12.42)

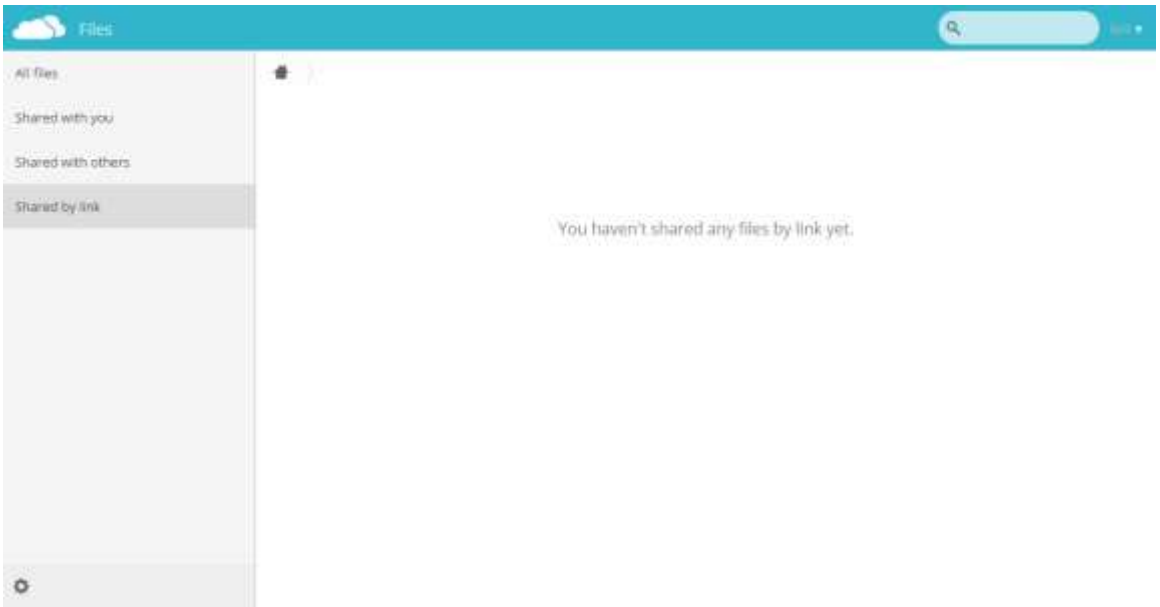


Figure 1-12. 42 Shared by Link

Chapter 2：Network

In this chapter, the Administrator can set the office network. There are two sections, Interfaces and Routing. The Administrator may configure the IP address of the LAN, the WAN, and the DMZ. Besides, not only IPv4 address setting, but also IPv6 address settings.

- 2-1 Interface
- 2-2 Interface (IPv6)
- 2-3 Routing
- 2-4 802.1Q

2-1 Interface

In the Interface section you can enable the following lists:

Port 1

Select Network > Interface> Port 1.

LAN Interface Setting: (Figure 2-1.1)

- Name: Enter any words for recognition.
- Interface Name: eth0
- IP Address: Enter an IP address.
- Up Speed: Define a suitable Max. Upstream bandwidth for each for them in order that the device may use it as a basis for operating
- MAC Address: Enter a MAC Address.
- Speed and Duplex Mode: Usually, it sets on Auto. You also can select another setting.
- Interface Type: LAN
- Enable: NAT mode only because it without bypass
- Netmask: Enter a Netmask.
- Down Speed: Define a suitable Max. Downstream bandwidth for each for them in order that the device may use it as a basis for operating.
- MTU: Nearly all IP over Ethernet implementations use the Ethernet V2 frame format.

  Click on Save.

Figure 2-1. 1 Port1 (LAN) Setting

Table of MTUs of common media

Note: the MTUs in this section are given as the maximum size of IP packet that can be transmitted without fragmentation - including IP headers but excluding headers from lower levels in the protocol stack. The MTU must not be confused with the minimum datagram size

that all hosts must be prepared to accept, which has a value of 576 for IPv4 and of 1280 for IPv6.

Media	Maximum Transmission Unit (Bytes)	Notes
Internet IPv4 Path MTU	At Least 68	Practical path MTUs are generally higher. IPv4 links must be able to forward packets of size up to 68 bytes. Systems may use Path MTU Discovery to find the actual path MTU. This should not be mistaken with the packet size every host must be able to handle, which is 576.
Internet IPv6 Path MTU	At least 1280	Practical path MTUs are generally higher. Systems must use Path MTU Discovery to find the actual path MTU.
Ethernet v2	1500	Nearly all IP over Ethernet implementations use the Ethernet V2 frame format.
Ethernet with LLC and SNAP, PPPoE	1492	
Ethernet Jumbo Frames	1500-9000	The limit varies by vendor. For correct interoperation, the whole Ethernet network must have the same MTU. Jumbo frames are usually only seen in special purpose networks.
WLAN (802.11)	7981	
Token Ring (802.5)	4464	
FDDI	4352	

ARP Spoofing Prevention: (Figure 2-1.1)

Figure 2-1. 2 ARP Spoofing Prevention

What Is ARP Spoofing[2]?

ARP spoofing is a type of attack in which a malicious actor sends falsified ARP (Address Resolution Protocol) messages over a local area network. This results in the linking of an attacker's MAC address with the IP address of a legitimate computer or server on the network. Once the attacker's MAC address is connected to an authentic IP address, the attacker will begin receiving any data that is intended for that IP address. ARP spoofing can enable malicious parties to intercept, modify or even stop data in-transit. ARP spoofing attacks can only occur on local area networks that utilize the Address Resolution Protocol.

Administrator Management

There are three multiple-choice modes, ping, HTTP, and HTTPS.

- Ping: The network can be detected by Ping commands when ticked.
- HTTP: The management interface is available for access via HTTP protocol when ticked.
- HTTPS: The management interface is available for access via HTTPS protocol when ticked.

Administrator is able to login via Port 1's HTTPS and ping Port 1's IP. (Figure 2-1.3)

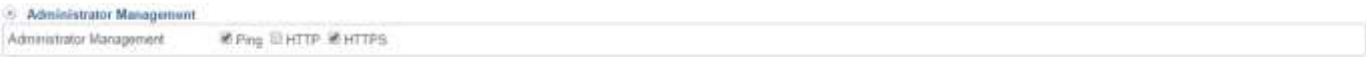


Figure 2-1. 3 Administrator Management

Multiple Subnet: (Figure 2-1.4)

- Name: Enter any word for recognition.
- IP Address: The multiple Subnet range of IP addresses.
- Interface: LAN only because it without bypass
- Bind: it depends on your network condition.
- Netmask: Enter Netmask
- WAN Interface IP Address / Operation Mode Setting: The WAN IP addresses that the subnet corresponds to WAN.
- Forwarding Mode：Allows the internal network to accommodate multiple subnets and enables Internet access through various external IP addresses. It displays using modes of WAN interface IP.

[2] ARP Spoofing: http://www.veracode.com/security/arp-spoofing

1. NAT mode
2. Routing

For example, a company, divided into Engineering department, Marketing Department, Sales Department, Purchasing Department and Accounting Department has a lease line with multiple Public IP addresses; 168.85.88.0/24. In order to facilitate the network management, the IT administrator may designate a subnet to each department respectively. The subnet distribution is as follows: (Figure 2-1.6)

Engineering Department: 192.168.1.1/24 (Internal) > 168.85.88.253 (External) (Figure 2-1.4)

Marketing Department: 192.168.2.1/24 (Internal) > 168.85.88.252 (External) (Figure 2-1.5)

Sales Department: 192.168.3.1/24 (Internal) > 168.85.88.251 (External)

Purchasing Department: 192.168.4.1/24 (Internal) > 168.85.88.250 (External)

Accounting Department: 192.168.5.1/24 (Internal) > 168.85.88.249 (External)

Network segment is the same as LAN IP range, so please disable "Bind."

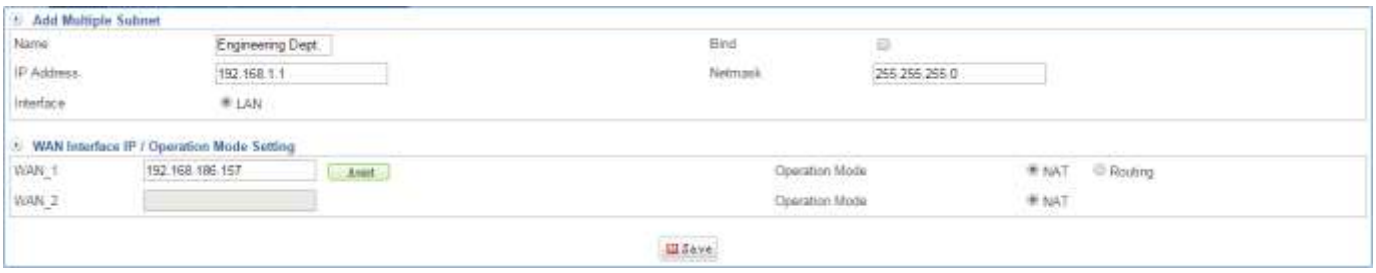


Figure 2-1. 4 set up Engineering Department multiple subnet

Network segment is not within LAN IP range, so please enable "Bind."

Figure 2-1. 5 set up Marketing Department multiple subnet

Completed

Multiple Subnet ALL

Name	Bind	Interface	IP Address	Netmask	WAN Interface IP / Operation Mode	Edit / Del
Engineering Dept.		–	192.168.1.1	255.255.255.0	WAN1 : 192.168.186.157 (NAT) WAN2 : (NAT)	
Marketing Dept.		LAN	192.168.2.1	255.255.255.0	WAN1 : 192.168.186.157 (NAT) WAN2 : (NAT)	
Sales Dept.		LAN	192.168.3.1	255.255.255.0	WAN1 : 192.168.186.157 (NAT) WAN2 : (NAT)	
Purchasing Dept.		LAN	192.168.4.1	255.255.255.0	WAN1 : 192.168.186.157 (NAT) WAN2 : (NAT)	
Accounting Dept.		LAN	192.168.5.1	255.255.255.0	WAN1 : 192.168.186.157 (NAT) WAN2 : (NAT)	

Figure 2-1. 6 Multiple Subnet

The IT administrator must renew his / her own PC's IP address upon using a DHCP server. It is to assure the access validity of the management interface after the change of LAN interface IP address. To renew the IP address distributed by a DHCP server, you may simply follow two steps:

Step 1. Reboot computer.

Step 2. Enter "cmd" in the Run window, and enter "ipconfig /release," and then enter "ipconfig /renew," the IP address is successfully retrieved.

There is another example to show whether should be bind or not. (Figure 2-1.7)

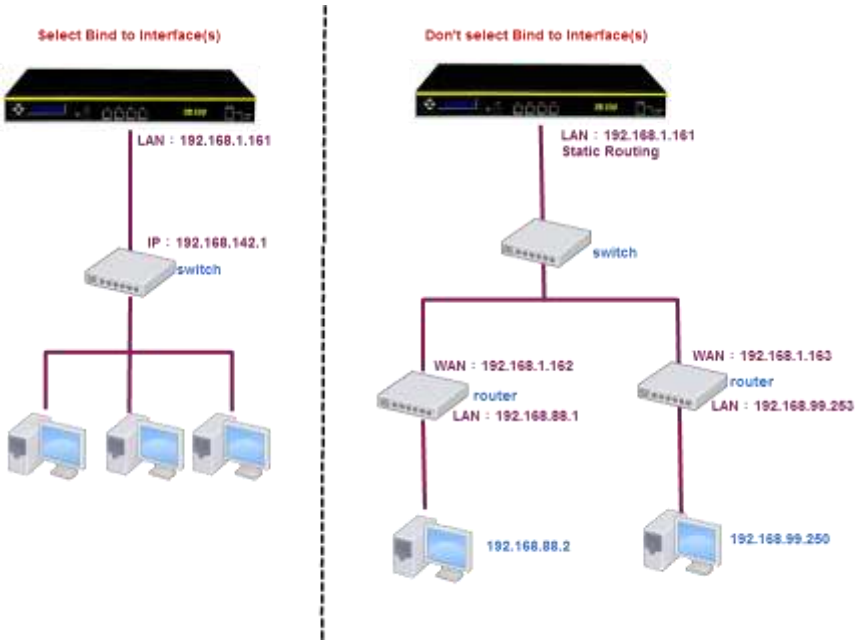


Figure 2-1. 7 Bind selection

Port 2

Select Network > Interface> Port 2. (Figure 2-1.8)

- Interface Name: Enter any word for recognition.
- Interface Name: eth1
- IP Address: Depend on the Connection Method. DHCP and PPPoE mode do not need to set IP address. Only Static mode needs to setup IP address.
- Default Gateway: Depend on the Connection Method. DHCP and PPPoE mode do not need to set Default Gateway. Only Static mode needs to setup Default Gateway.
- Up Speed (Max. 1000Mbps): The IT administrator must define a proper bandwidth for each of them in order that the device may use it as a basis for operating. The Kbps is a unit of Speed. You can click on Custom Define link to set your speed according to ISP's WAN Speed.
- Speed and Duplex Mode: Usually, it sets on Auto. You also can select another setting.
- Load Balancing: It offers four methods.
  1. Auto: Distributes the outward sessions by the usage status of each WAN port.
  2. By Source IP: For services that require using the same IP address throughout the process, such as online game and banking, ShareTech UR helps user retain the same WAN port (i.e. IP address) over which the session was created to avoid disconnection caused by the variation of the user's IP address.
  3. Manual: According administrator demand to share loading on the WAN.
  4. By Destination IP: Once a session is created between the ShareTech SG-100N and a specific host, then the following sessions linking to that host will be automatically distributed to the same WAN port.
- Interface Type: WAN
- Connection Method：There are three Connection methods.
  1. Static: Static IP address
  2. DHCP: Using DHCP to get IP address from ISP
  3. PPPoE: PPPoE
- Netmask: Enter a Netmask. Default setting is 255.255.255.0
- MAC address: Enter a MAC Address.
- Down Speed: The IT administrator must define a proper bandwidth for each of them in order that the device may use it as a basis for operating. The Kbps is a unit of Speed. You can click on Custom Define link to set your speed according to ISP's WAN Speed.
- MTU: Nearly all IP over Ethernet implementations use the Ethernet V2 frame format.
- Click on Save.

Figure 2-1. 8 WAN 1 Setting

WAN Alive Detection (Figure 2-1.9)

- Detection Method: Using DNS, ICMP or NONE to check WAN is on or off. Both DNS and ICMP need to setup IP address for test. In addition, you can click on Log to see more detail Logs.
  1. DNS: Tests the validity of Internet connection by requesting the domain name.
  2. ICMP: Uses ping command to test the validity of Internet connection.
  3. NONE: Line is not detected; the connection status is always on line.
- Administrator Management: There are three multiple-choice modes, ping, HTTP, and HTTPS.
  1. Ping: The network can be detected by Ping commands when ticked.
  2. HTTP: The management interface is available for access via HTTP protocol when ticked.
  3. HTTPS: The management interface is available for access via HTTPS protocol when ticked.

Figure 2-1. 9 WAN Alive Detection

Firewall Protection (Figure 2-1.10) (Figure 2-1.11)

- Firewall Protect Items: There are four multiple-choice, SYN, ICMP, UDP, and Port Scan. It offers currently available protection. In addition, you can click on Log to see more detail Logs.

Figure 2-1. 10 Port 2 Firewall Protection

You are able to see attack logs which through Port2 of SG-100N machine on Objects > Firewall Protection > Attack Log. (Figure 2-1.11)

Figure 2-1. 11 Firewall Protection Port Scan

General Setting (Figure 2-1.12)

- DNS Server 1: The IP address of the DNS server used for the bulk of DNS lookups.

For example: Google DNS are 8.8.8.8 and 8.8.4.4

- HTTP Port: HTTP port number for manage.

Default: 80

- WAN Alive Detection Period: System administrators can enter the system every interval of time to do much testing, unit calculated in seconds.

Default: 5 second

- DNS Server 2: The IP address of the backup DNS server, used when the Primary DNS Server is unreachable.
- HTTPS Port: HTTPS port number for manage.

Default: 443

- Idle Timeout: The device may be configured to automatically disconnect when idle for a period of time upon using PPPoE connection.

Default: 60 minutes

Figure 2-1. 12 Port 2 General Setting

Port 3

Please note that Interface Type depend on what you set up on Network > Interface > Interface Config (Figure 2-1.13) (Figure 2-1.14)

Figure 2-1. 13 Interface Config

Figure 2-1. 14 Port 3 setting

Port 4

Please note that Interface Type depend on what you set up on Network > Interface > Interface Config

For example: Configure the IP address and subnet mask of your demilitarized zone (DMZ) here. Select Network > Interface > Port4. (Figure 2-1.15)

- Name: Enter any word for recognition.
- Interface Name: eth3
- IP Address: Enter an IP address.
- Up Speed: The IT administrator must define a proper bandwidth for each of them in order that the device may use it as a basis for operating. The Kbps is a unit of Speed.
- MAC Address: Enter a MAC address.
- Speed and Duplex Mode: Usually, it sets on Auto. You also can select another setting.
- Interface Type: DMZ
- Enable: It offers three modes.
  1. NAT: In this mode, the DMZ acts an independent subnet from the LAN, from which the IT administrator may configure.
  2. OFF: It means Disable.

3. Transparent Bridging: A mode that allows a SG-100N (firewall, router, switch) to be inserted into an existing network without the need for IP reconfiguration similar with the Transparent Mode but providing more transparency(the firewall acts as a Layer 2 bridge) and versatile functionality. An optional mode of L2 Bridge which prevents traffic that has entered an L2 bridge from being forwarded to a non-Bridge-Pair interface, ensuring that traffic which enters an L2 Bridge exits the L2 Bridge rather than taking its most logically optimal path.
4. Transparent Routing: A mode that allows a SG-100N (firewall, router, switch) to be inserted into an existing network without the need for IP reconfiguration by spanning a single IP subnet across two or more interfaces.

- Netmask: Enter a Netmask.
- Down Speed: The IT administrator must define a proper bandwidth for each of them in order that the device may use it as a basis for operating. The Kbps is a unit of Speed.
- MTU: Nearly all IP over Ethernet implementations use the Ethernet V2 frame format.
- Click on Save after you finish setting.

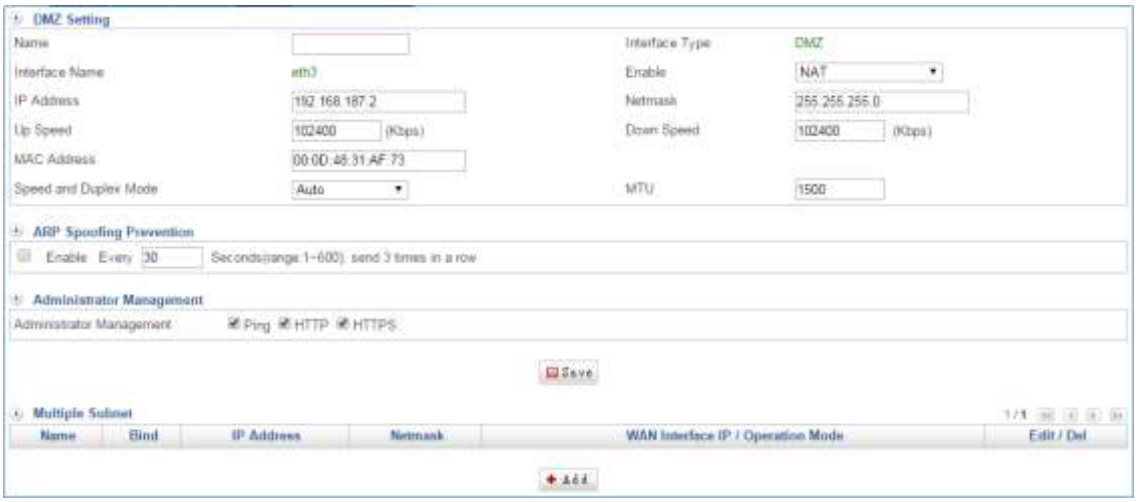


Figure 2-1. 15 Port 3 Setting

What's the difference between DMZ (Transparent Routing) and DMZ (Transparent Bridge)?

In the past, most of SG-100N supports NAT and Transparent mode usually in order to satisfy customers with different network framework requirement. DMZ is an independent virtual (internal) network within NAT mode. If some enterprise doesn't have enough public IP, they would like to use Port Mapping or IP Mapping, and make DMZ Internal IP to be a WAN public IP in order to make Internet service work fine. On the other hand, transparent mode means routing mode, so that DMZ should be Public (real) IP.

Fortunately, ShareTech research and development team creates and improves multi-features constantly. After the firmware 7.1.3, ShareTech DMZ port supports three flexible modes: NAT, Transparent Routing, and Transparent Bridge. We better know what the difference between NAT and Transparent mode from the first paragraph is. Therefore, that's go on to see what's the difference between Transparent Routing and Transparent Bridge

1. Transparent Routing: (Figure 2-1.16)

   When DMZ packets pass through ShareTech SG-100N, system follows routing table rule and then deliver packets to their destination.

   Network Environment: When enterprise has more than two WANs, and must do load balance necessarily. System follows the WAN load balance rule and divide packets which from DMZ among each WAN Port.

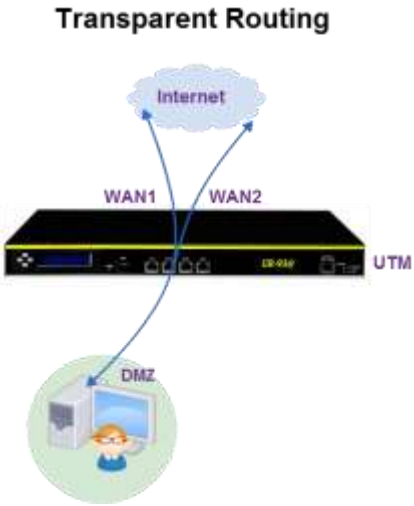


Figure 2-1. 16 Transparent Routing

2. Transparent Bridge: (Figure 2-1.17)

   System doesn't follow routing table rule to deliver packets to their destination, and delivery destination based on MAC. Therefore, the operation is similar to Switch.

   Network Environment: When enterprise only has one WAN or only allow DMZ packets must go pass static WAN.

   Even though Transparent Bridge cannot support load balance, however, sometimes it's very practical method and conscientious. Please see the following figure, if we put gateway in front of SG-100N, and then gateway bind DMZ's IP and MAC. So, as we know the packets is allowed pass out if having the same IP and MAC. On the other hand, the packets will be block if it's with Transparent Routing mode, because gateway just analyze DMZ IP but bind WAN port MAC. (Figure 2-1.17) (Figure 2-1.18)

Transparent Bridge

Figure 2-1. 17 Transparent Bridge

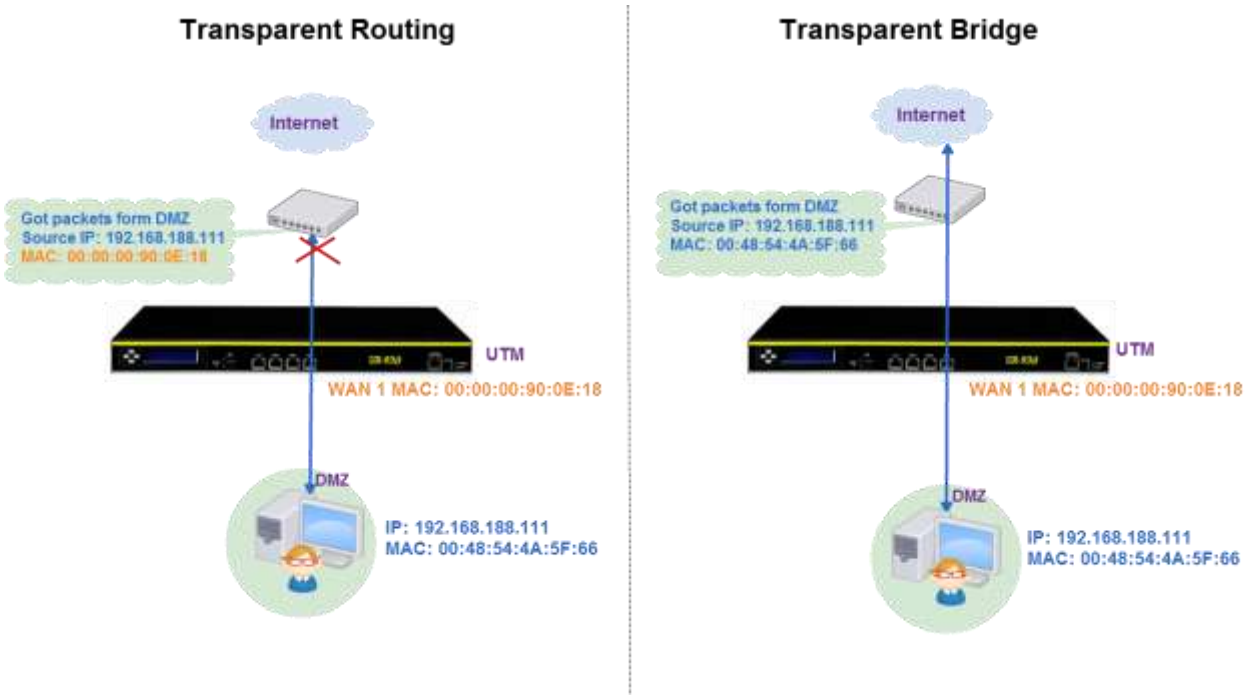


Figure 2-1. 18 Transparent Routing / Transparent Bridge

Compare Transparent Routing with Transparent Bridge		
	Transparent Routing	Transparent Bridge
Load Balance	YES	NO
Environment	More than two WANs	Only one WAN
The packets form DMZ	WAN Port MAC	Original MAC

Figure 2-1. 19 Compare Transparent Routing with Transparent Bridge

WiFi

It's an optional item. If you never purchase WiFi on **Configuration** > **Package**, you will not see this (Figure 2-1.20) Please enable one of SSID.

Figure 2-1. 20 WiFi

Interface Config

Custom Port (Fixed LAN & WAN1) (Figure 2-1.21)

Please note systme will reboot after modify

Figure 2-1. 21 Custom Port

2-2 Interface (IPv6)

IPv4 is not enough anymore until 2021, and previously technical administrators are used to rely on IPv4 with NAT mode. As for now, IPv6 which offer more flexible for distributing IP address and routing table turn up. Compared to IPv4, the most obvious advantage of IPv6 is its larger address space. IPv4 addresses are 32 bits long and number about 4.3 × 10 9 (4.3 billion). IPv6 addresses are 128 bits long and number about 3.4 × 10 38 (340 Undecillion).

IPv6 Auto Configuration is a new concept with IPv6. It gives an intermediate alternative between a purely manual configuration and stateful auto configuration.

Port 1

Select Network > Interface (IPv6) > Port 1 (Figure 2-2.1)

- IPV6 LAN (eth0) IP: Enter IPv6 address.
- IPv6 Auto Configuration: It's like IPv4 DHCP. It automatically distributes IPv6 address to among LAN internal users.

The following is LAN IPv6 figure

Figure 2-2. 1 Port 1 IPv6

Port 2

Select Network > Interface (IPv6) > Port 2

- IPv6 model: you are able to choose static, Tunnel, or PPPoE IPv6 ways. (Figure 2-2.2)

The following is WAN1 IPv6 figure

Figure 2-2. 2 Port 2 IPv6

Port 3

Select Network > Interface (IPv6) > Port 3. (Figure 2-2.3)

Please note that Interface Type depend on what you set up on Network > Interface > Interface Config. (Figure 2-1.9)

The following is WAN2 IPv6 figure, so you are able to choose static, Tunnel, or PPPoE IPv6 ways.

Figure 2-2. 3 Port 3IPv6

Port 4

Select Network > Interface (IPv6) > Port 4. (Figure 2-2.4)

Please note that Interface Type depend on what you set up on Network > Interface > Interface Config. (Figure 2-1.9)

The following is DMZ IPv6 figure, so please enter DMZ's IPv6 address.

Figure 2-2. 4 Port 4 IPv6

DNS Server

The current IETF recommendation is to use AAAA (Quad A) RR for forward mapping and PTR RRs for reverse mapping when defining IPv6 networks. (Figure 2-2.5)

The Google Public DNS IPv6 addresses are as follows:

2001:4860:4860::8888

2001:4860:4860::8844

Figure 2-2. 5 DNS IPv6

2-3 Routing

Routing tables contain a list of IP addresses. Each IP address identifies a remote router (or other network gateway) that the local router is configured to recognize. For each IP address, the routing table additionally stores a network mask and other data that specifies the destination IP address ranges that remote device will accept. In the Routing section you can enable the following lists:

Routing Table

Static routing is simply the process of manually entering routes into a device's routing table via a configuration file that is loaded when the routing device starts up. As an alternative, these routes can be entered by a network administrator who configures the routes manually. Since these manually configured routes don't change after they are configured (unless a human changes them) they are called 'static' routes.

Select Network > Routing > Routing Table. Click on Add to create a new routing table. (Figure 2-3.1)

- Comment: Enter any words for recognition.
- Destination IP: The IP address of the packet's final destination.
- Netmask: Enter Netmask
- Gateway: Enter Gateway
- Interface: Select your internal interface.(The outgoing network interface the device should use when forwarding the packet to the next hop or final destination)

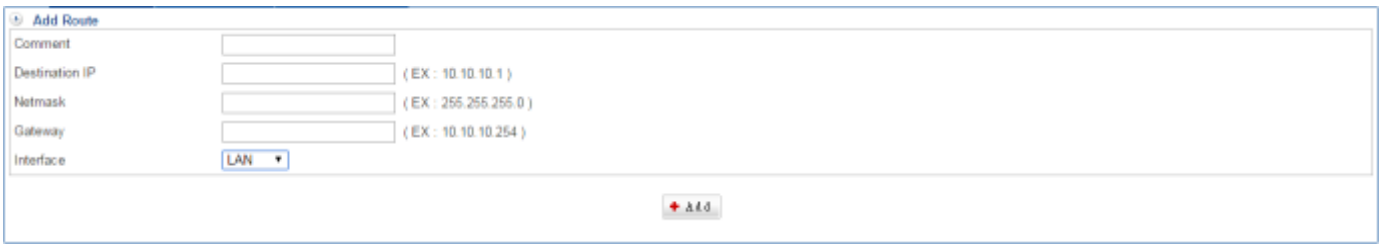


Figure 2-3. 1 Routing Table

For exemple : A leased line connects Company A's Router 1 (10.10.10.1) with Company B's Router 2 (10.10.10.2)

Company A : Connect WAN port 1 (61.11.11.11) to ATUR; Connect WAN port 2 (211.22.22.22) to ATUR; LAN subnet ranges 192.168.1.1/24；The LAN subnet that Router 1 (10.10.10.1, RIPv2 supported) connected to ranges from 192.168.10.1/24.

Company B: The LAN subnet that Router 2 (10.10.10.2, RIPv2 supported) connected to ranges from 192.168.20.1/24.

- Setting Routing Table completed. The network subnets of 192.168.20.1/24 and 192.168.1.1/24 now not only communicate with each other, but as well use NAT mode to access the Internet. In addition, select Mark tick box, and click on Add to create a new sub-content, Edit to modify contents, or Del to cancel list. (Figure 2-3.2)

Figure 2-3. 2 Routing Table List

Two hypothetical, partial routing table entries are shown below:
IP Address: 172.48.11.181 - Network Mask: 255.255.255.255
IP Address: 192.168.1.1 - Network Mask: 255.255.255.0
In this example, the first entry represents the route to the ISP's primary DNS server. Requests made from the home network to any destination on the Internet will be sent to the IP address 172.48.11.181 for forwarding. The second entry represents the route between any computers within the home network, where the home router has IP address 192.168.1.1.

Dynamic routing

A router using dynamic routing will 'learn' the routes to all networks that are directly connected to the device. Next, the router will learn routes from other routers that run the same routing protocol (RIP, RIP2, etc.). Each router will then sort through its list of routes and select one or more 'best' routes for each network destination the router knows or has learned.

Select Network > Routing > Dynamic routing. Select interface(s) and click on Save (Figure 2-3.3)

Figure 2-3. 3 Dynamic routing Table

Viewing the Contents of Routing Tables, please select Tools > Connection Test > IP Route. (Figure 2-3.4)

Figure 2-3. 4 IP Route

On Windows and Unix/Linux computers, the *netstat -r* command also displays the contents of the routing table configured on the local computer.

IPV6 Routing Table

IPV6 Routing Table setting way is the same as Routing Table section. (Figure 2-3.5)

Figure 2-3. 5 IPV6 Routing Table

2-4 802.1Q

IEEE 802.1Q is the networking standard that supports Virtual LANs (VLANs) on an Ethernet network. The standard defines a system of VLAN tagging for Ethernet frames and the accompanying procedures to be used by bridges and switches in handling such frames. The IEEE's 802.1Q standard was developed to address the problem of how to break large networks into smaller parts so broadcast and multicast traffic wouldn't grab more bandwidth than necessary. The standard also helps provide a higher level of security between segments of internal networks.In this section you can enable the following lists:

802.1Q

Select Network > 802.1Q > 802.1Q Click on + Add to add VLAN ID.

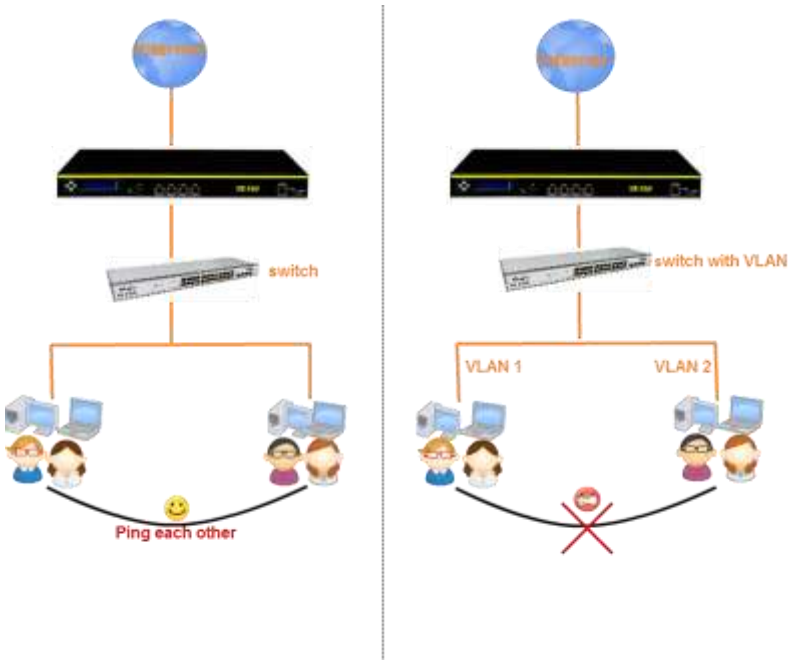


Figure 2-4. 1 difference no VLAN between VLAN

Here I use ML-9324 switch for testing, and let's create some VLANs. (Figure 2-4.2)

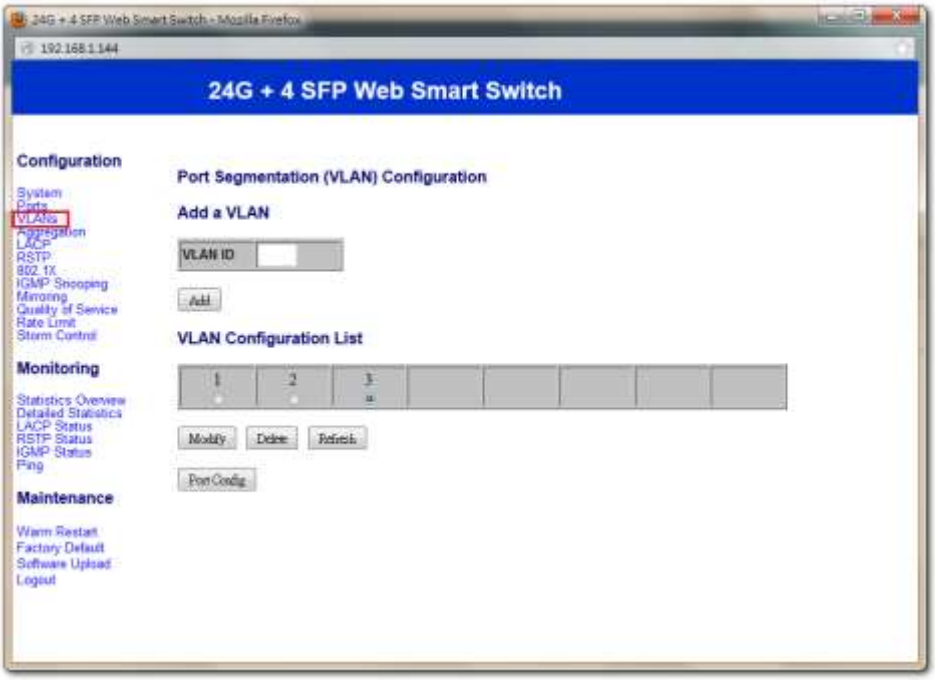


Figure 2-4. 2 switch VLANs

Then, distribute some ports among one group. (Figure 2-4.3)

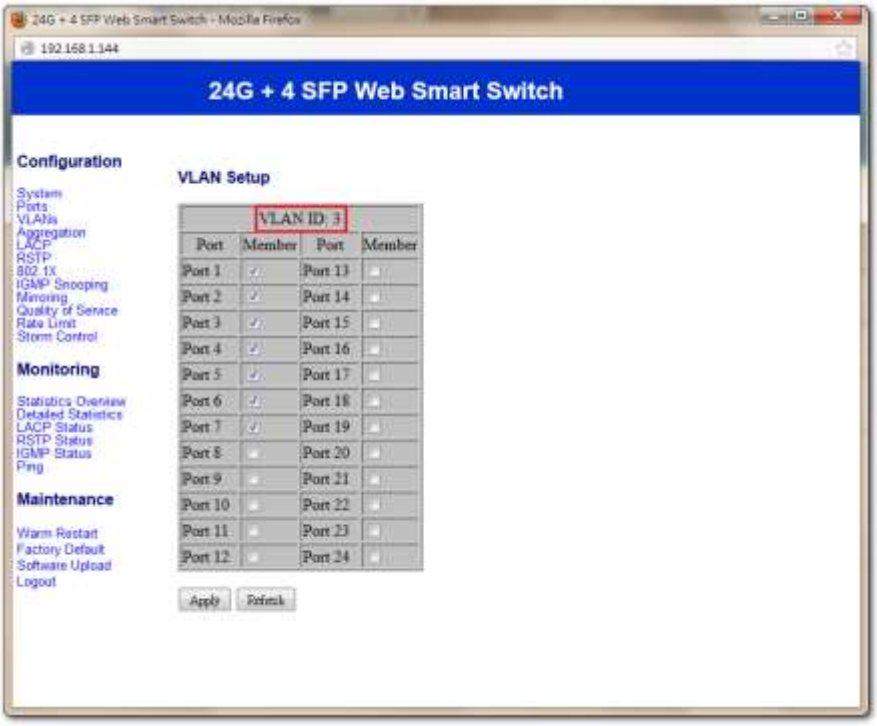


Figure 2-4. 3 VLAN Setup

Select Port 1 to Port7 of packets should be with Tagged 3.(Figure 2-4.4)

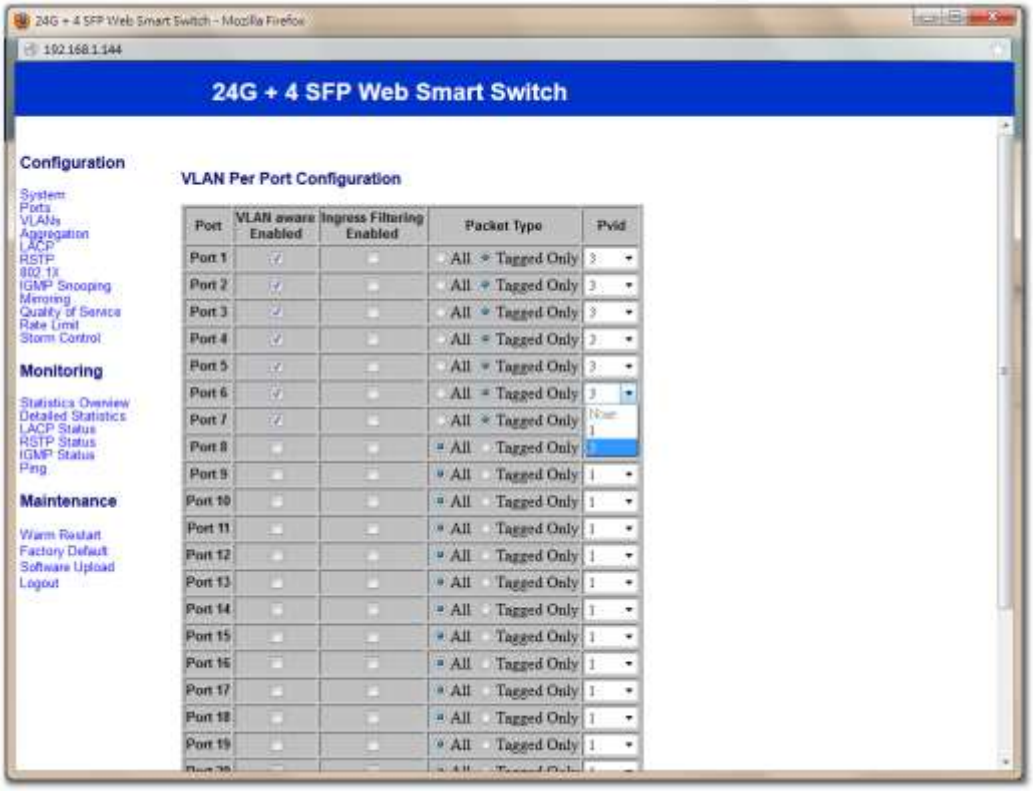


Figure 2-4. 4 VLAN per Port Configuration

As your port is like the following figure. (Figure 2-4.5)

Figure 2-4. 5 switch status

- Comment: Enter any word for recognition
- Multiple Subnet: choose one
- IP Address: Enter an IP address.
- Netmask: Enter Netmask
- Interface: Select interface, LAN or DMZ.
- VLAN ID: It is the identification of the VLAN, which is basically used by the standard 802.1Q.

Add "VLAN ID 3" now, otherwise, the port 6 cannot surf Internet. (Figure 2-4.6)

Figure 2-4. 6 Add VLAN ID

Finished 802.1Q setting, and the Port 6 is able to surf Internet. (Figure 2-4.7)

Figure 2-4. 7 Completed 802.1Q setting

Chapter 3：Policy

ShareTech SG-100N inspects each packet passing through the device to see if it meets the criteria of any policy. Every packet is processed according to the designated policy; consequently any packets that do not meet the criteria will not be permitted to pass. The items of a policy include Policy Name, Source Address, Destination Address, Action, Protocol, Service Port or Group, Software Access Control, QoS, Schedule, URL Policy, Internet Auth, Using Which WAN, Maximum Concurrent Sessions per IP Address, IDP, Packet tracing, and Traffic Analysis. The IT administrator could determine the outgoing and incoming service or application of which data packets should be blocked or processed by configuring these items. On the other hand, IDP belongs to AW models.

3-1 WiFi Policy

It's an optional item. If you don't purchase WiFi on **Configuration** > **Package**, you will not see this. Please check whether enable WiFi SSID or not

It allows all packets if you set up nothing (Figure 3-1.1)

Figure 3-1. 1 WiFi to WAN

3-2 LAN Policy

In this section you can enable the following lists：

Basic Setting

- Policy Name: Enter any word for the description of the policy.
- Source: Source address is based around using the device as a point of reference. The initiating point of a session is referred to as the source address.
- Destination: Destination address is based around using the device as a point of reference. The initiating point of a session is referred to as the source address.
- Action：It offers two kinds, Permit and Drop. When it Permit, the policy will be pass. On the other hand, Drop means the policy will be stop.
  1. Drop: Deny the Policy.
  2. Permit: Allow the Policy.

Policy

- Protocol:
  1. ALL
  2. TCP
  3. UDP
  4. ICMP[3]
- Service Port or Group: The services are regulated. Available options are the system default services and the services that are customized in the section of 4-2 Services.

[3] ICMP = Internet Control Message Protocol

- Software Access Control: It can restrict the use of application software. Set this function in the section of 4-5 Software Blocking
- QoS: The guaranteed and maximum bandwidth settings (The bandwidth is distributed to users. Setting this in the section of 4-4 QoS)
- Schedule: Activate as per the configured scheduled time. Set this function in the section of 4-3 Schedule.
- URL Access Control: It can restrict the access to any URL websites specified. Set this function in the section of 4-6 URL Filter.
- Authentication: This requires users to be authenticated to create a connection. Set this function on the section of 4-9 Authentication.
- Bulletin Board:
- WAN: It determines over which WAN interface's packets are permitted to pass through.
  1. All: Packets are granted to pass through all interfaces once approved by the configured policy.
  2. WAN 1: Policy approved packets may access WAN 1.
  3. WAN 2: Policy approved packets may access WAN 2.
- Maximum Concurrent Sessions for Each Source IP Address: It determines the maximum number of concurrent sessions of each IP address. If the amount of sessions exceeds the set value, new sessions will not be created.
- IDP: It can identify intrusion packets and react to them in a timely manner.
- Packet Tracing:
- Traffic Analysis:
- Pause：Temporarily disable the policy.
- Start: Start the Policy.
- Delete: Delete the Policy.
- Edit: Edit the Policy.

- Traffic Analysis: Click on this button, you can see the detail illustration of traffic analysis.
- Log Packet tracing: Record Logs of packet transmissions managed by the policy. You can click on Log button to see packet logs.

Fire wall Protection

- SYN attack
- ICMP attack
- UDP Attack
- Port Scan

Figure 3-1. 2 LAN to WAN Policy

3-3 DMZ Policy

The way of DMZ Policy settings are the same as LAN Policy, and it allows all packets if you set up nothing (Figure 3-3.1)

Figure 3-3. 1 DMZ Policy

3-4 WAN Policy

The way of WAN Policy settings are the same as LAN Policy, and it allows all packets if you set up nothing (Figure 3-4.1)

Figure 3-4. 1 WAN Policy

Chapter 4：Objects

In the Objects chapter you can enable the following lists：

- 4-1 Address Table
- 4-2 Services
- 4-3 Schedule
- 4-4 QoS
- 4-5 Application Control
- 4-6 URL Filter
- 4-7 Virtual Server
- 4-8 Firewall Protection
- 4-9 Authentication
- 4-10 Bulletin Board

4-1 Address Table

In Address section, the IT administrator may configure network settings of LAN, WAN and DMZ, as well as designate specific addresses in a network as a group. An IP address might represent a host or a domain, in either case, the IT administrator may give it an easily identifiable name for better management. According to the network in which an IP address resides, it can be categorized into three kinds, LAN IP address, WAN IP address and DMZ IP address. Each of the three can be organized into an address group comprising several addresses. Simply by applying the address group to a policy, the IT administrator may easily manage a group of users with merely one policy. In this section you can enable the following lists:

LAN IP Address

Select Objects > Address Table > LAN IP Address. (Figure 4-1.1)

Select IP Mode: IPv4 or IP v6

- Computer Name: Enter any words for recognition.
- IP Address: It is recommended to configure some desirable address names within Address first so that they are ready to use for the Source Address or Destination Address setting of a policy. In addition, you may click on Assist to add to create an entry.
- Mode:
  1. Only set IP Address
  2. IP and MAC Address
- Please click on Get Mac

Click on + Add to create one LAN IP Address first.

Figure 4-1. 1 LAN IP Address

Setting LAN IP Address completed. In addition, select ☑checkbox, and click on + Add to create a new sub-content, Edit to modify contents, or ✖ Del to cancel list. (Figure 4-1.2) (Figure 4-1.3)

Figure 4-1. 2 LAN IP Address List

Figure 4-1. 3 Static IP

LAN Group

Select Objects > Address Table > LAN Group.

- Select IP Mode: It offers two modes.
  1. IPv4 Mode: IPv4 address.
  2. IP v6 Mode: IPv6 address.
- Click on +Add button to create a LAN Group rule.
- Group Name: Enter any word for recognition. (Figure 4-1.4)

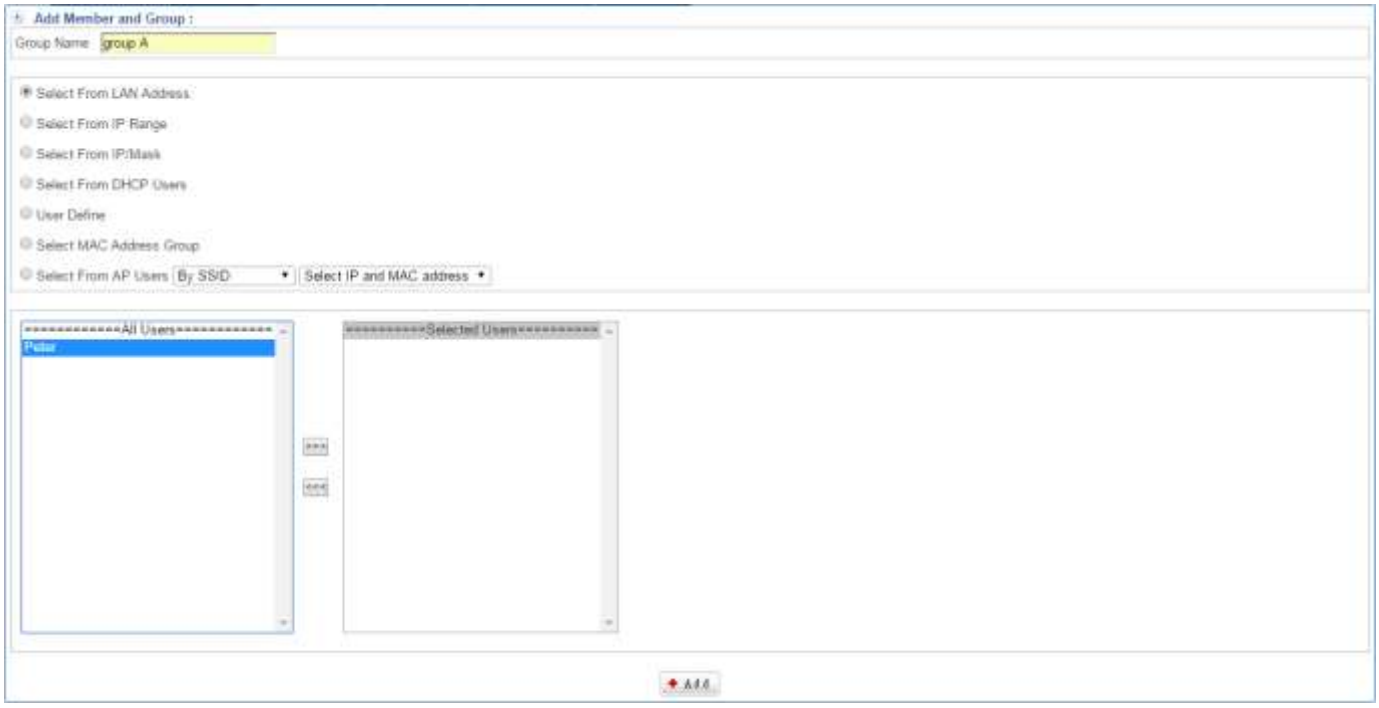


Figure 4-1. 4 LAN Group

1. Select From LAN Address: The left user lists which you add in LAN IP Address. (Figure 4-1.5)

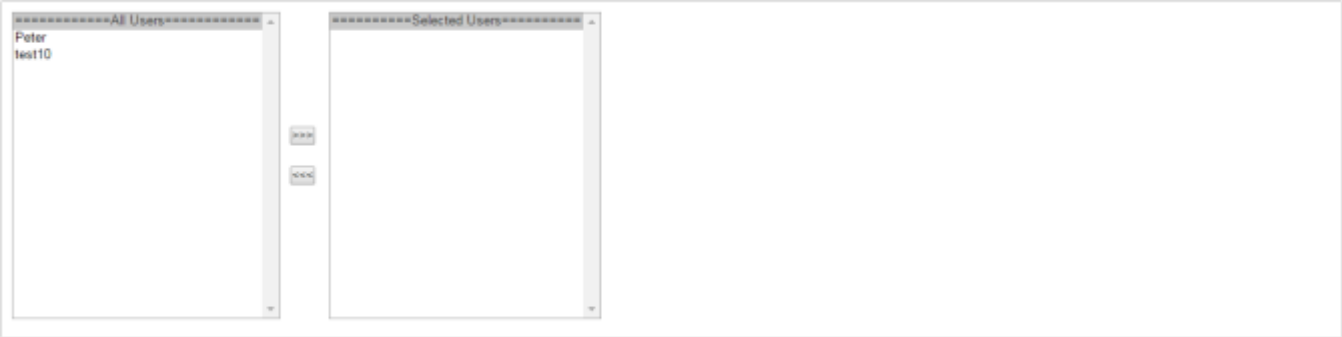


Figure 4-1. 5 Select from LAN Address

2. Select From IP Rang: Enter the range IP addresses which you want to restrict to. (Figure 4-1.6)

Figure 4-1. 6 Select from IP Range

3. Select From IP/Mask: (Figure 4-1.7)

Figure 4-1. 7 Select from IP/Mask

4. Select From DHCP Users: It shows range of DHCP users, and these will be restricted. If you select IP-MAC Binding tick box, it will show list of IP MAC. (Figure 4-1.8)

Figure 4-1. 8 Select from DHCP Users

5. Users Define: Please enter an IP address or subnet. (Figure 4-1.9)

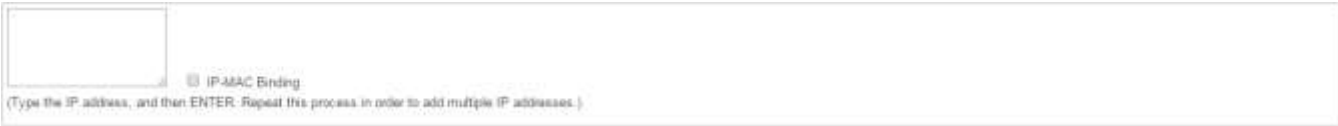


Figure 4-1. 9 Select Users Define

6. MAC Address Group: Please enter an MAC address or subnet. (Figure 4-1.10)

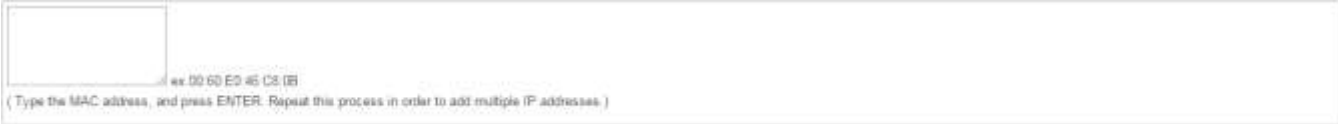


Figure 4-1. 10 Select MAC Address Group

Setting LAN Group completed. In addition, select Mark tick box, and click on +Add button to create a new sub-content, Edit to modify contents, or Del to cancel list. (Figure 4-1.11)

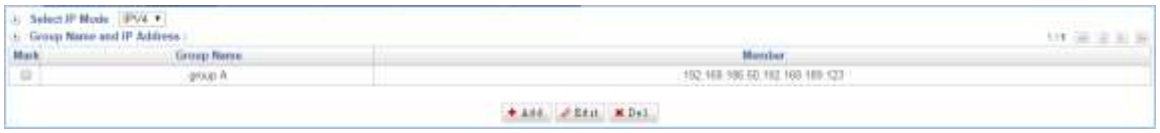


Figure 4-1. 11 LAN Group List

There is an example of how LAN Group is used.

1. Select Policy > LAN Policy > LAN to WAN or LAN to DMZ.
2. Click on ✚ Add, and select Action to DROP or Permit, and then select Source to group A which you have just set in 4-1 Address. (Figure 4-1.12)

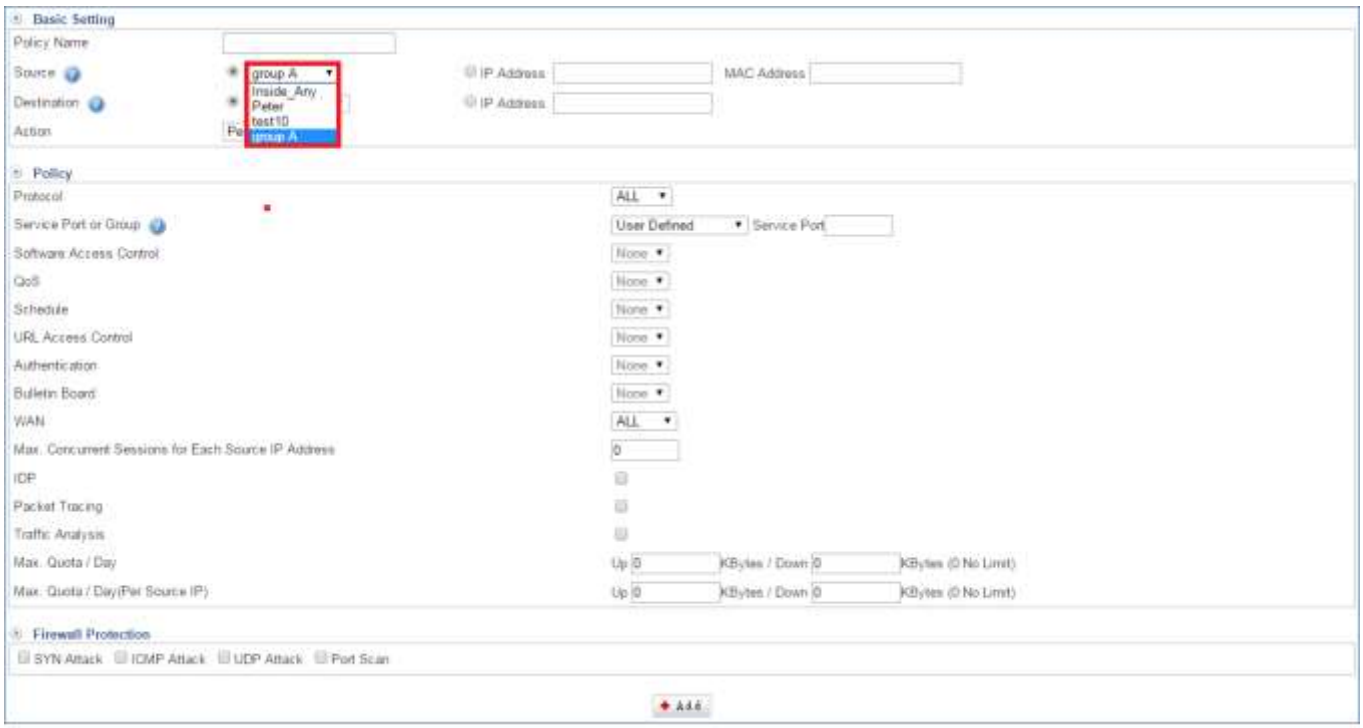


Figure 4-1. 12 Address Policy

3. Setting Address Policy completed. (Figure 4-1.13)

Figure 4-1. 13 Address Policy List

DMZ IP Address

The way of DMZ IP Address settings are the same as LAN IP Address.

Please note that Interface Type depend on what you set up on Network > Interface > Interface Config

DMZ Group

The way of DMZ Group settings are the same as LAN Group. When you want to use DMZ Group, please select Policy > DMZ Policy> DMZ to WAN or DMZ to LAN. Click on Add, and select Action to DROP or Permit, and then select Source to which you have just set in 4-1 Address DMZ Group.

Please note that Interface Type depend on what you set up on Network > Interface > Interface Config

WiFi IP Address

The way of WiFi IP Address settings are the same as LAN IP Address.

Please check whether enable WiFi SSID or not

WiFi Group

The way of WiFi Group settings are the same as LAN Group. When you want to use WiFi Group, just select Policy > DMZ Policy> WiFi to WAN, WiFi to LAN, WiFi to DMZ, and WiFi to WiFi. Click on Add, and select Action to DROP or Permit, and then select Source to which you have just set in 4-1 Address WiFi Group.

WAN IP Address

The way of WAN IP Address settings are the same as LAN IP Address.

WAN Group

The way of WAN Group settings are the same as LAN Group. When you want to use WAN Group, just select Policy > WAN Policy> WAN to LAN or WAN to DMZ. Click on Add, and select Action to Drop, and then select Source to which you have just set in 4-1 Address.

『FQDN』 - What is FQDN?

A Fully Qualified Domain Name (FQDN), sometimes called an absolute domain name, and its consists of a host and domain name, including top-level domain.

For example, www.higuard.com is a fully qualified domain name in the Internet. www is the host, higuard is the second-level domain, and com is the top level domain. In this case, www is the name of the host in the higuard.com domain.

When connecting to a host (using an SSH client, for example), you must specify the FQDN. The

DNS server then resolves the hostname to its IP address by looking at its DNS table. The host is contacted and you receive a login prompt.

This application, such as web browsers, try to resolve the domain name part of a Uniform Resource Locator (URL) if the resolver cannot find the specified domain or if it is clearly not fully qualified by appending frequently used top-level domains and testing the result.

Example application

Usually, most administrator use URL filter application to avoid internal users surfing Internet, however, we may figure out it cannot block "https." Therefore, ShareTech released FQDN application within filter in order to block domain exactly. (Figure 4-1.14)

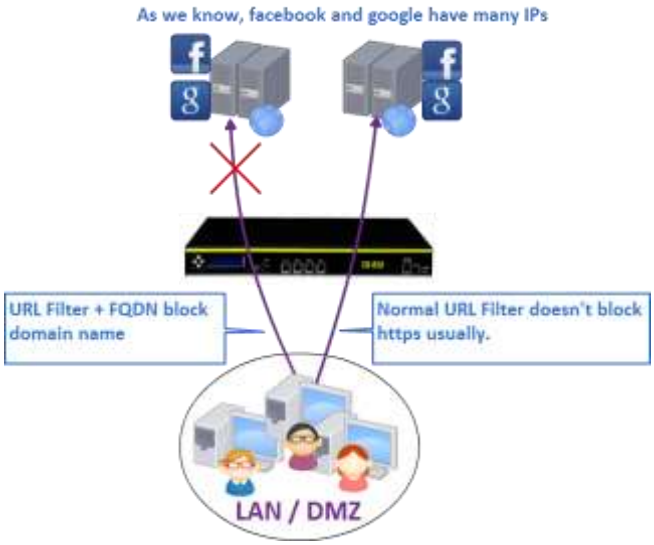


Figure 4-1. 14 FQDN

Select Object > Address Table > WAN Group. Click on + Add to create a WAN group with FQDN. (Figure 4-1.15) (Figure 4-1.16)

Figure 4-1. 15 WAN_User Define Domain

Figure 4-1. 16 WAN Group

Select Policy > LAN Policy > LAN to WAN. Click on Add to create a new policy. (Figure 4-1.17) (Figure 4-1.18)

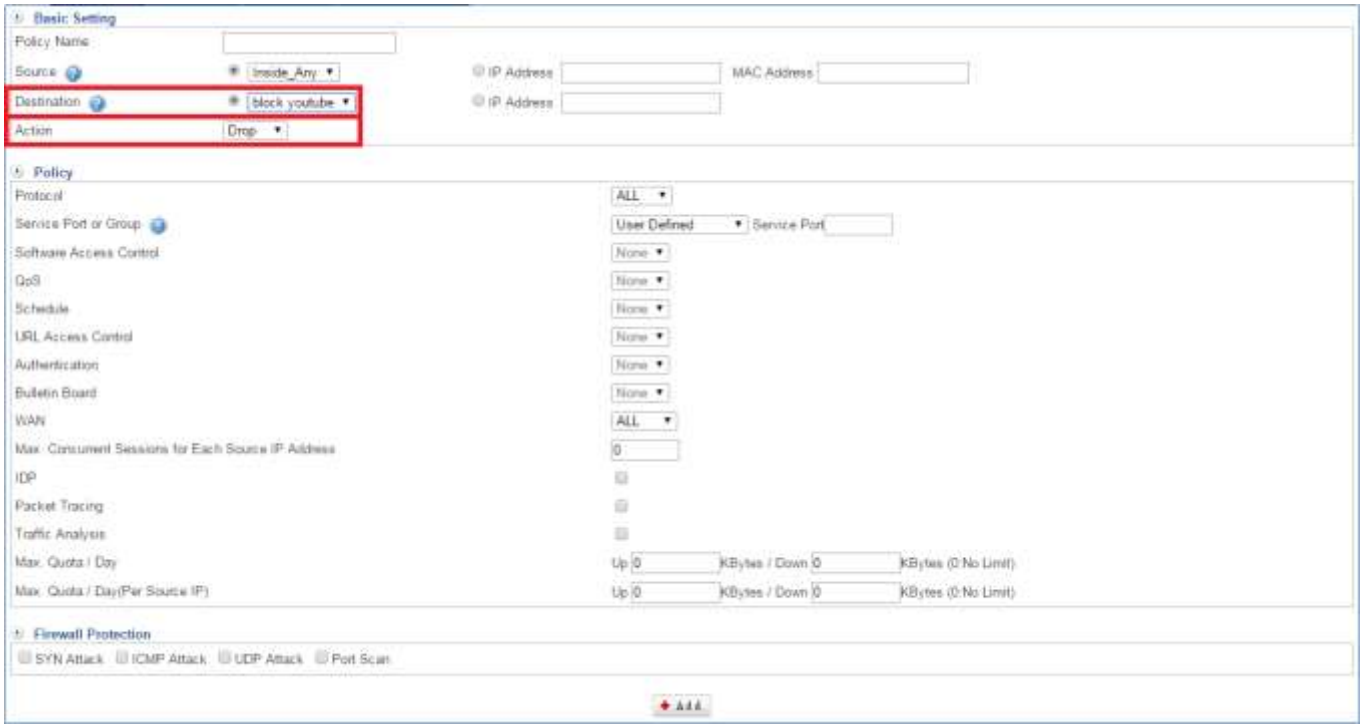


Figure 4-1. 17 setting Policy

Figure 4-1. 18 Completed setting Policy

Now, let's check domain ip. (Figure 4-1.19)

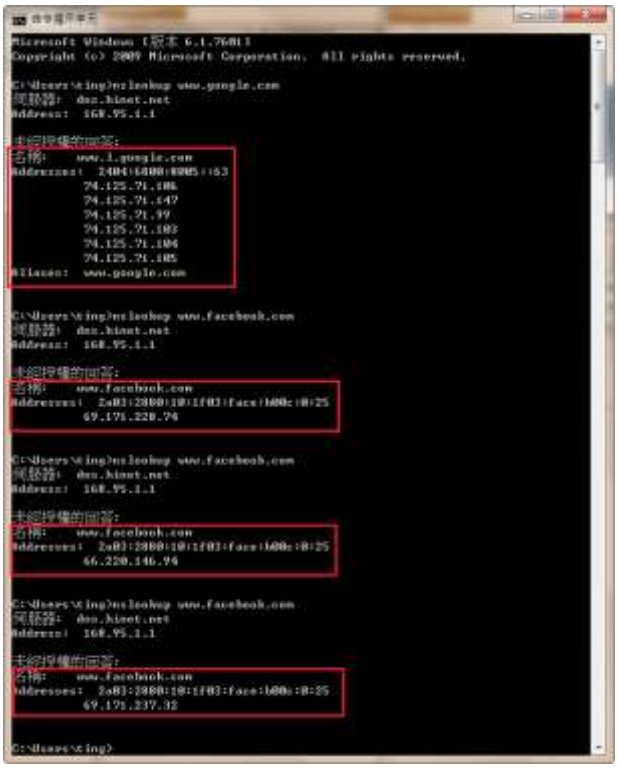


Figure 4-1. 19 ns lookup

As we know, internal user cannot surf facebook even if it go through https . (Figure 4-1.20)

Figure 4-1. 20 block https

4-2 Services

TCP and UDP protocols support a variety of services, and each service consists of a TCP port or UDP port number, such as TELNET (23), FTP (21), SMTP (25), POP3 (110), etc. This section has two types of services, that is, Pre-defined service and Service group. Pre-defined service includes the most common-used services using TCP or UDP protocol. It allows neither modification nor deletion while Custom service allows modification on port numbers based on the situation.

When configuring Custom service, the port number setting for either client port or server port falls between 0 and 65535. The IT administrator merely needs to determine the necessary protocol and port number for each Internet service, and then the client will be able to access different services.

In this section you can enable the following lists:

Basic Service

Select Objects > Services > Basic Service. The symbol and its description used in Pre-defined: (Figure 4-2.1)

- Protocol: The protocol used for communication between two devices. TCP and UDP are the two most frequently seen protocols among others.
  1. ANY: Any Service.
  2. TCP: Services using TCP protocol, Gepher, ICQ, Ident, LDAP, NTTP over SSL, PPTP, SFTP, SSH, Terminal, WINFRAME, AFPoverTCP, FTP, H323 (NetMeeting), L2TP, MSN Messenger, POP2, SMTP over SSL, Yahoo, AOL, Finger, HTTP, IMAP over SSL, LDAP Admin, NNTP, POP3 over SSL, RLOGIN, SMTP, VNC, BGP, GNUTella, HTTPS, IMAP, LDAP over SSL, POP3, Real Audio, Telnet, and WAIS.
  3. UDP: Services using UDP protocol, DNS, IKE, RIP, SYSLOG, UUCP, TFTP, NTP, and SNMP.
- Port: The port number of the client user's PC which is used for connecting to the UTM device.

  Range from 0 to 65535. Using default is recommended.

Figure 4-2. 1 Pre-defined description

Service Group

To facilitate policy management, the IT administrator may create a service group including a group of necessary services.

For example, given that ten users from ten different IP addresses requesting access to five types of services, namely HTTP, FTP, SMTP, POP3 and TELNET, it merely takes one policy with a service group to satisfy the service request of 50 combinations (10 users times 5 services equals to 50 service requests). Select Objects > Services > Service Group. This function regulates the online usage of service. Click on + Add to create a Service rule.

- Service Name: Enter some words for recognition.

Click on Assist to select services. (Figure4-2.2)

Figure 4-2. 2 Service Assist

If you made wrong selection, you want to remove one port. Please blank out the port. (Figure 4-2.3)

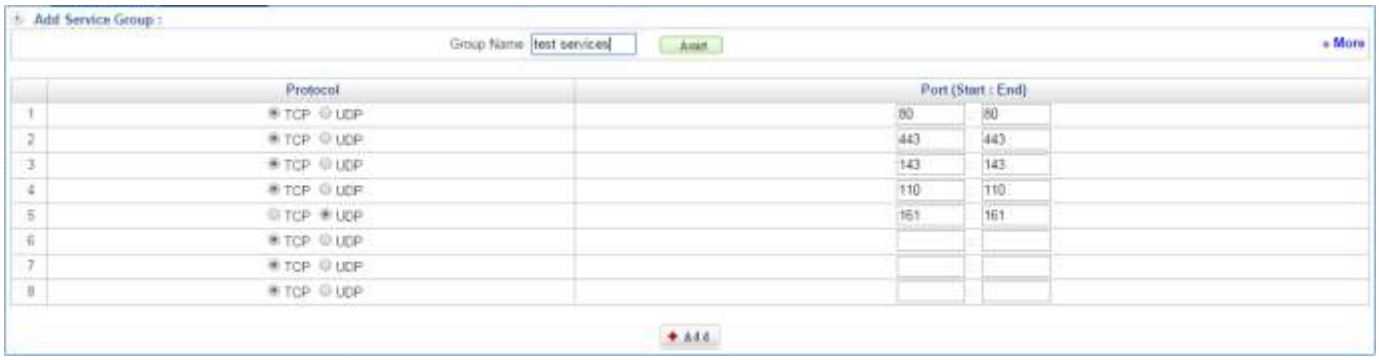


Figure 4-2. 3 Service group

Setting Service group completed. In addition, select ☑checkbox, and click on Add to create a new sub-content, Edit to modify contents, or Del to cancel list. (Figure4-2.4)

Figure 4-2. 4 Service group List

There is an example that administrator deny these services.

1. Select Policy > LAN Policy, DMZ Policy, or WAN Policy. Then, select the function you need on the right side.
2. Click on + Add, and select Action to DROP or Permit, and then select Service Port or Group to test service which you have just set in 4-2 Services. (Figure 4-2.5)

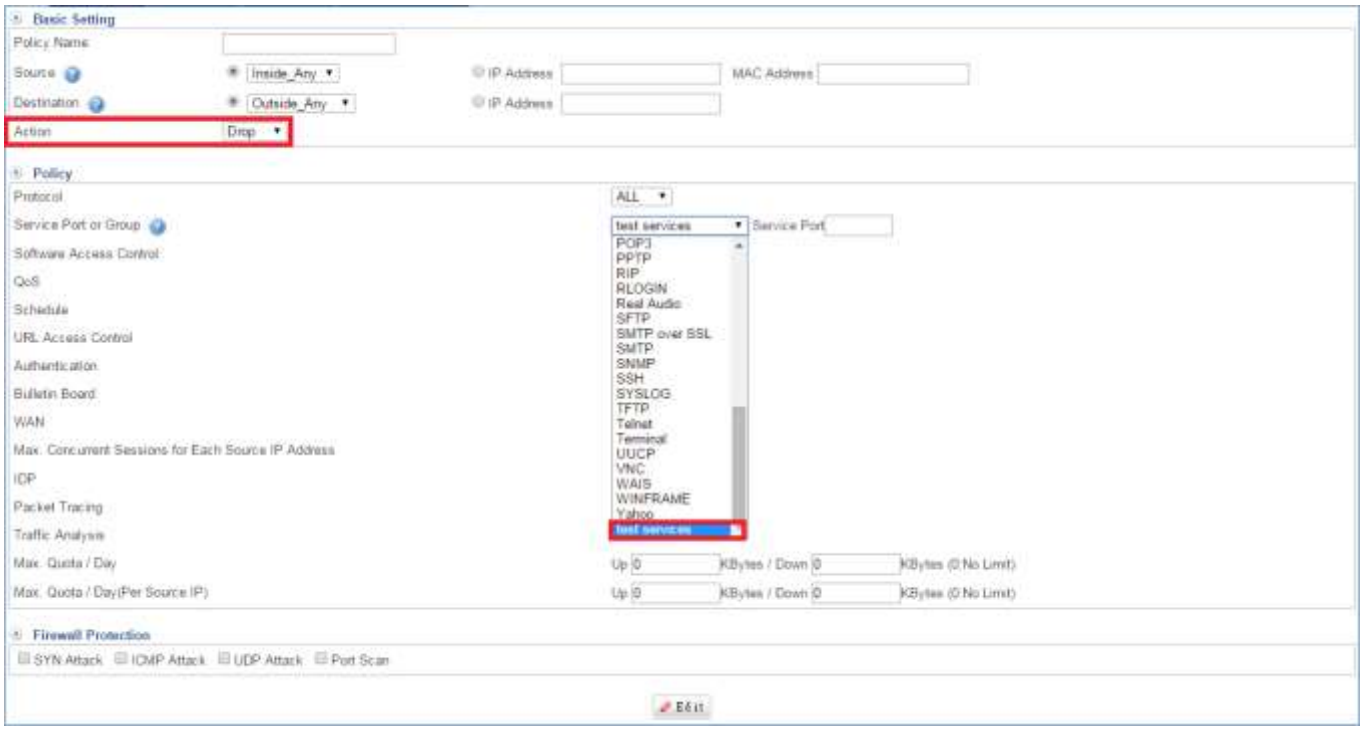


Figure 4-2. 5 Service Policy

3. Setting Service Policy completed, and then internal users are not able to use these services.(Figure 4-2.6)

Figure 4-2. 6 Service Policy List

4-3 Schedule

The IT Administrator to configure a schedule for policy to take effect and allow the policies to be used at those designated times. And then the Administrator can set the start time and stop time or VPN connection in Policy or in VPN. By using the Schedule function, the Administrator can save a lot of management time and make the network system most effective. In this section you can enable the following lists:

Schedule List

The system administrator and IT administrator can use Schedule to set up the device to carry out the connection of Policy or VPN during several different time divisions automatically. Select Objects > Schedule > Schedule List. Click on Add to create a new Schedule rule first.

- Schedule Name: Enter some words for recognition.
- Setting Mode: there are two mdoes.

Mode 1: (Figure 4-3.1)

Figure 4-3. 1 Schedule Mode 1

Mode 2: (Figure 4-3.2)

Figure 4-3. 2 Schedule Mode 2

Setting Schedule List completed. In addition, select ☑checkbox, and click on ✚ Add to create a new sub-content, ✎ Edit to modify contents, or ✖ Del to cancel list. (Figure 4-3.3)

- ✔ : Pass
- ✖ : Disable

Figure 4-3. 3 Schedule List

There is an example of how Schedule List is used.

1. Select Policy > LAN Policy > DMZ Policy, or WAN Policy. Then, select the function you need on the right side. Here, we use LAN to WAN for sample. Click on ✚ Add first.
2. Select Action to DROP or Permit, and then select Schedule to for working time which you have just set in 4-3 Schedule List. (Figure 4-3.4)

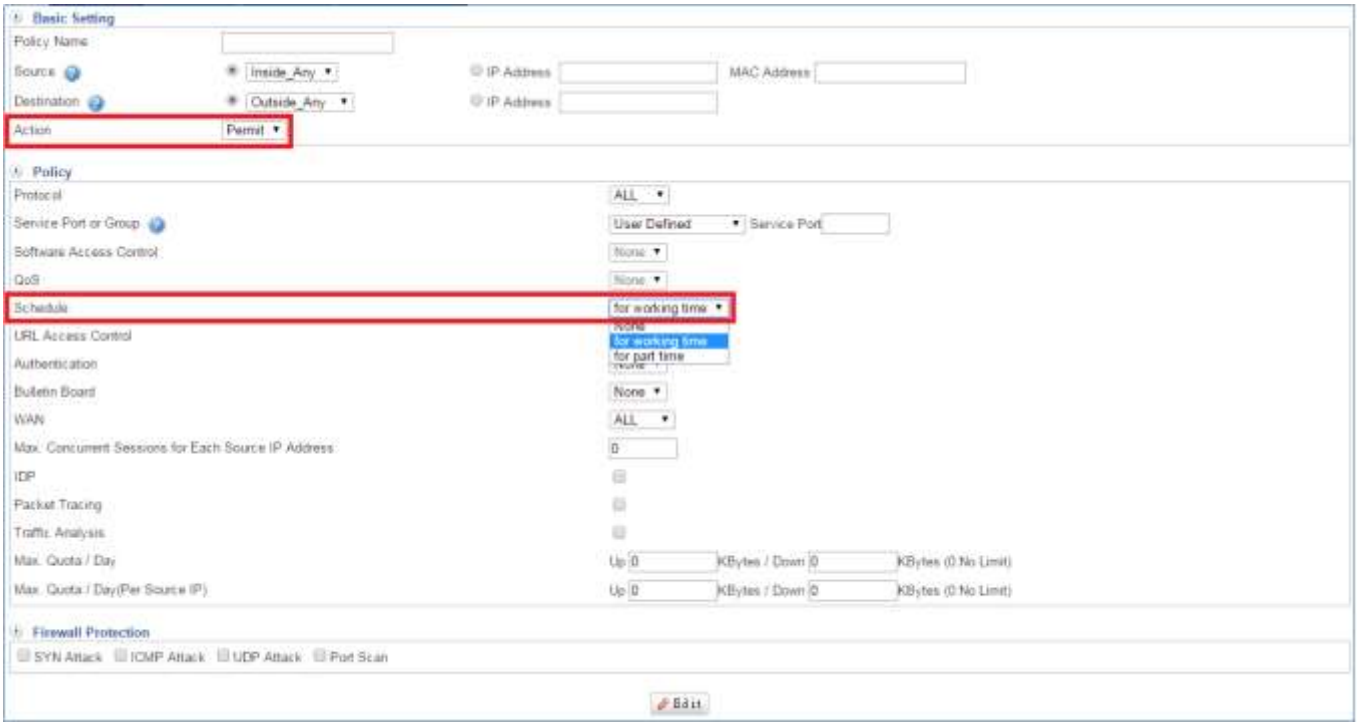


Figure 4-3. 4 Schedule Policy

3. Setting Schedule Policy completed, and it means internal users able to use during period.(Figure 4-3.5)

Figure 4-3. 5 Schedule Policy List

4-4 QoS

By configuring the QoS, IT administrator can control the Outbound and Inbound Upstream/Downstream Bandwidth. The administrator can configure the bandwidth according to the WAN bandwidth. The QoS feature not only facilitates the bandwidth management but optimizes the bandwidth utilization as well. The following two figures indicate the improvement of bandwidth utilization as a result of enforcing QoS by showing before and after comparisons. In this section you can enable the following lists:

QoS Setting

Select Objects > QoS > QoS Setting. Click on Add to create a new QoS rule first. (Figure 4-4.1)

- QoS Name: Enter any word for recognition.
- Prio (Priority): To configure the priority of distributing Upstream/Downstream and unused bandwidth
- Bandwidth Mode: It offers three ways.
  1. By Policy
  2. Inside Per Source IP (It includes Smart QoS application)
  3. Outside Per Source IP
- Interface: Display LAN, DMZ, WAN1, WAN2, WAN3, and WAN4.
- User Down Speed (Downstream Bandwidth): To configure the Guaranteed Bandwidth and Maximum Bandwidth according to the bandwidth range you apply from ISP
- User Up Speed (Upstream Bandwidth): To configure the Guaranteed Bandwidth and Maximum Bandwidth according to the bandwidth range you apply from ISP
- rate (Guaranteed Bandwidth): Specifies the minimum (guaranteed) amount of bandwidth
- max (Maximum Bandwidth): Specifies the maximum amount of bandwidth.

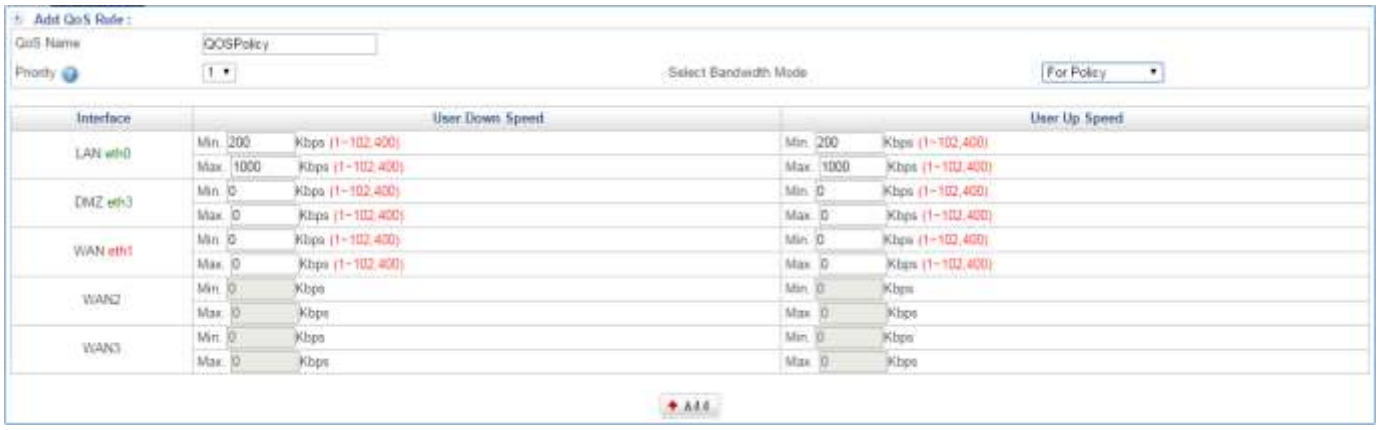


Figure 4-4. 1 QoS Setup

Setting QoS List completed. In addition, select ☑checkbox, and click on Add to create a new sub-content, Edit to modify contents, or Del to cancel list. (Figure 4-4.2)

Figure 4-4. 2 QoS List

There is an example of how QoS List is used.

1. Select Policy > LAN Policy, DMZ Policy, or WAN Policy. Then, select the function you need on the right side. Here, we use LAN to WAN for sample. Click on Add first.
2. Select Action to Permit, and then select QoS to QOSPolicy(Per Souce IP) which you have just set in 4-4 QoS. (Figure 4-4.3)

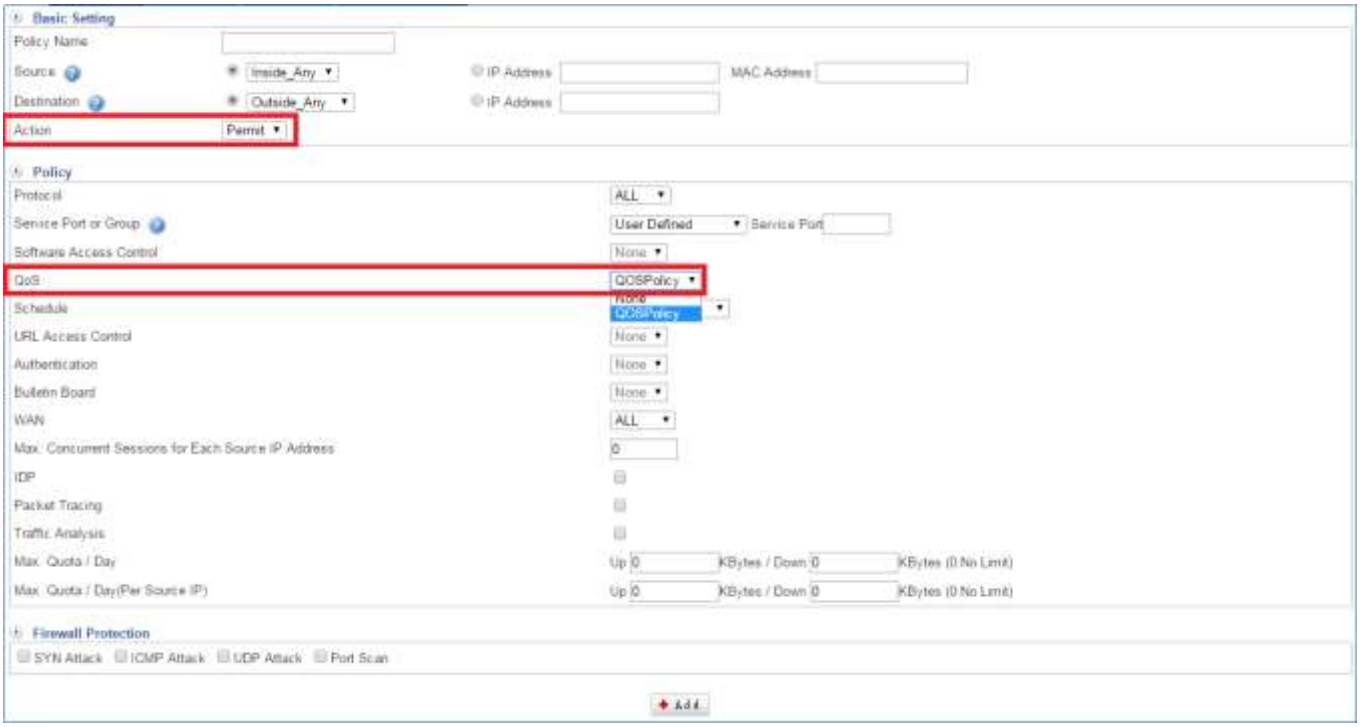


Figure 4-4. 3 QoS Policy

3. Setting QoS Policy completed. (Figure 4-4.4)

Figure 4-4. 4 QoS Policy List

4-5 Application Control

Setting

Select Objects > Application Control > Software Block. It offers five kinds of software blocking, P2P Software, IM Software, WEB Application, Fun Software, and Other Application. Click on Add first.

- Group Name: Enter any word for recognition.
- Block Log: If you want to record the condition of software blocking, please select this.
- Popular Software: File Shareing Application, Instant Messaging Client, VOIP Application Block, WEB Mail Block, Game, and Others. (Figure 4-5.1)

Figure 4-5. 1 Popular Software

- Not Commonly Used Software: File Sharing Application, Instant Messaging Client, WEB File Extension Download Block, WEB File Extension Upload Block, Video Software Block, Game Virus, Worms, Spyware Block , Stock Software Block, and others. (Figure 4-5.2)

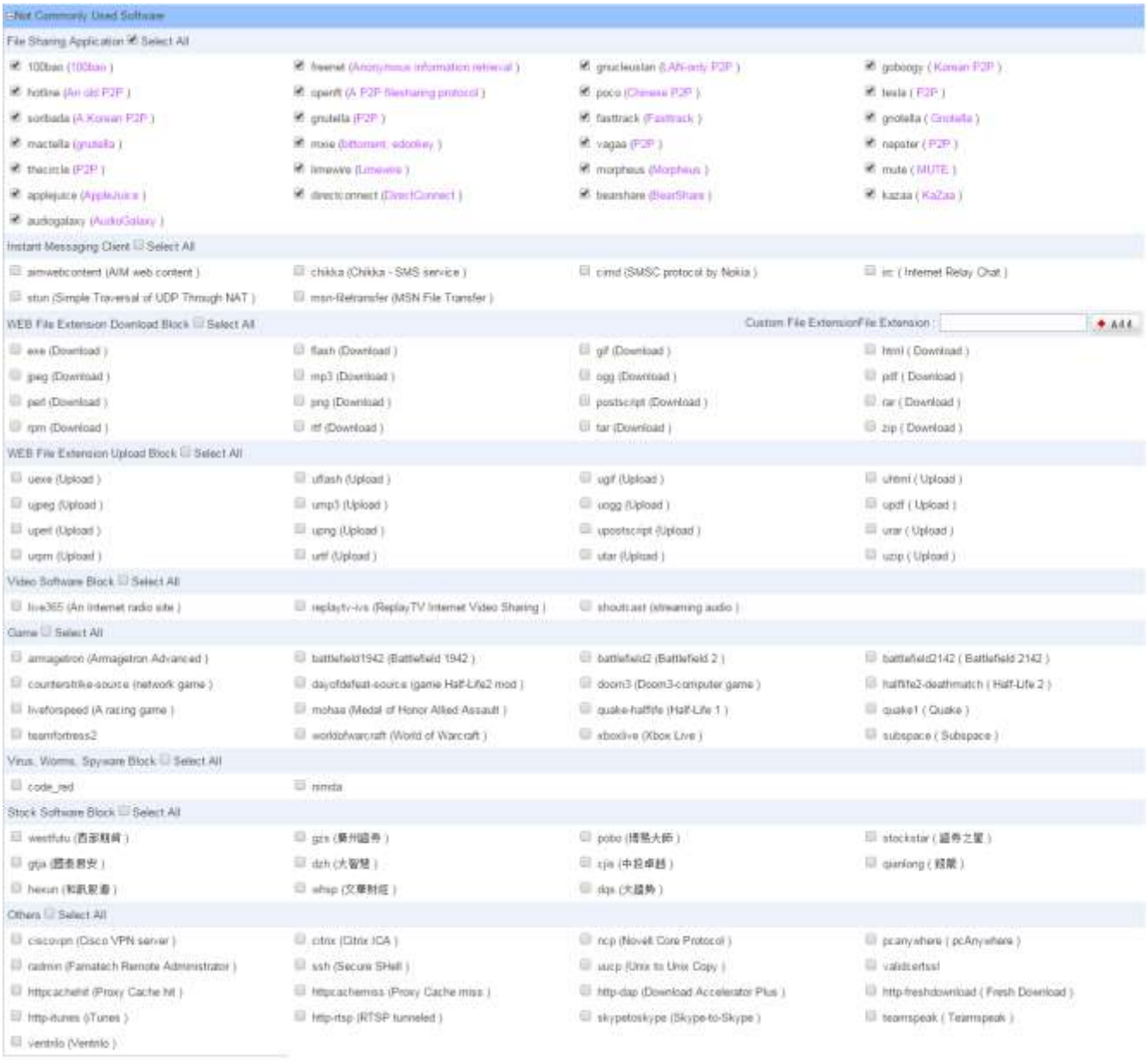


Figure 4-5. 2 Not Commonly Used Software

Setting Software Blocking List completed. In addition, select ☑check box, and click on ✚ Add to create a new sub-content, ✎ Edit to modify contents, or ✖ Del to cancel list. (Figure 4-5.3)

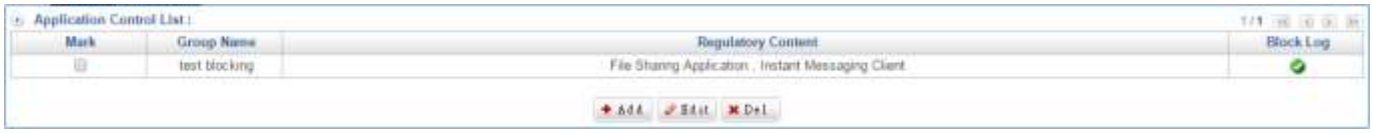


Figure 4-5. 3 Application Control List

There is an example of how Software Blocking is used.

1. Select Policy > LAN Policy or DMZ Policy. Then, select the function you need on the right side. Here, we use LAN to WAN for sample. Click on ✚ Add first.
2. Select Action to DROP or Permit, and then select Software Access Control to test blocking which you have just set in 4-5 Application Control. (Figure 4-5.8)

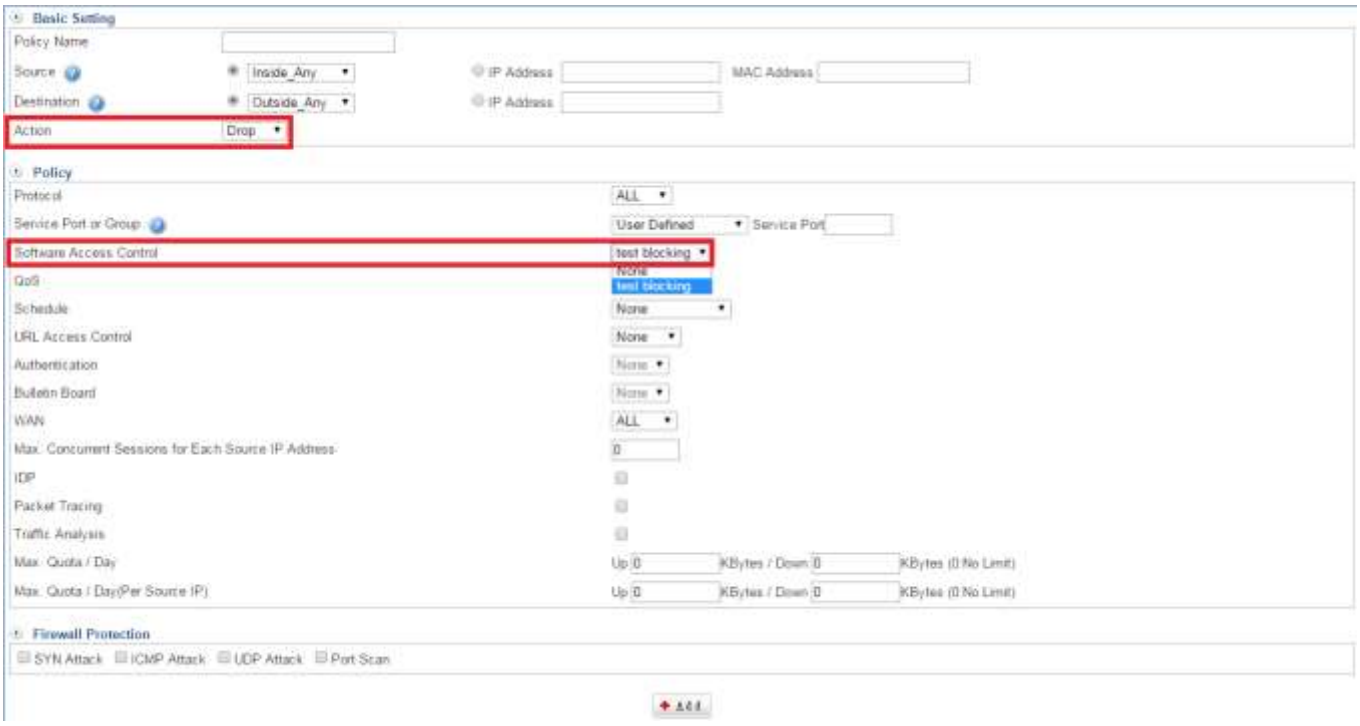


Figure 4-5. 4 Software Blocking Policy

3. Setting Software Blocking Policy completed. (Figure 4-5.5)

Figure 4-5. 5 Software Blocking Policy List

Block Log

Select Objects > Application Control > Block Log (Figure 4-5.6)

Figure 4-5. 6 Block Log

4-6 URL Filter

URL Filtering (URLF) is widely used for parental control, compliance and productivity. In schools, for instance, URLF is used to help deter exposure to inappropriate websites, such as pornography, nudity, aggressive sites, etc. In offices, URL filtering is especially an indispensible tool for web security policy.

According to research, company employees spend a significant proportion of their time surfing non-work-related web during working hours. In addition to productivity, network latency is also an issue when employees surf unnecessary websites, or download bandwidth-intensive files. The greater concern is the threat caused from malicious applications or malware, while surfing some illegitimate or inappropriate websites.

List Settings

Select Objects > URL Filter > List Settings. Then, click on + Add

- Name: Enter any words for recognition.
- List Mode: Select for Blacklist or Whitelist.
- Match Mode: There are two ways, Exact and Fuzzy.
- URL Blacklist: Enter the complete domain name or key word of the website. It is restricted specific website whether user surf Internet or not, however it depends on what you select on List Mode.

For example: "*www.kcg.gov.tw*" "kh.google.com" "*gov*" or "**google**" (Figure 4-6.1)

- IP Blacklist: Enter the complete IP address. It is restricted specific website whether user surf Internet or not, however it depends on what you select on List Mode.

Figure 4-6. 1 List Settings

Setting URL List completed. In addition, select Mark tick box, and click on Add to create a new sub-content, to modify contents, or to cancel list. (Figure 4-6.2)

Figure 4-6. 2 URL List

URL Settings

Select Objects > URL Filter > URL Settings. Then, click on Add

- Group Name: Enter any words for recognition. (Figure 4-6.3)
- Create block warning message: User can create block warning message their own when it's enabled. Besides, you are able to edit your warning message Objects > URL Filter > Other Settings. (Figure 4-6.4)
- List Select: Select one that you have ever added in List settings.

Figure 4-6. 3 URL settings

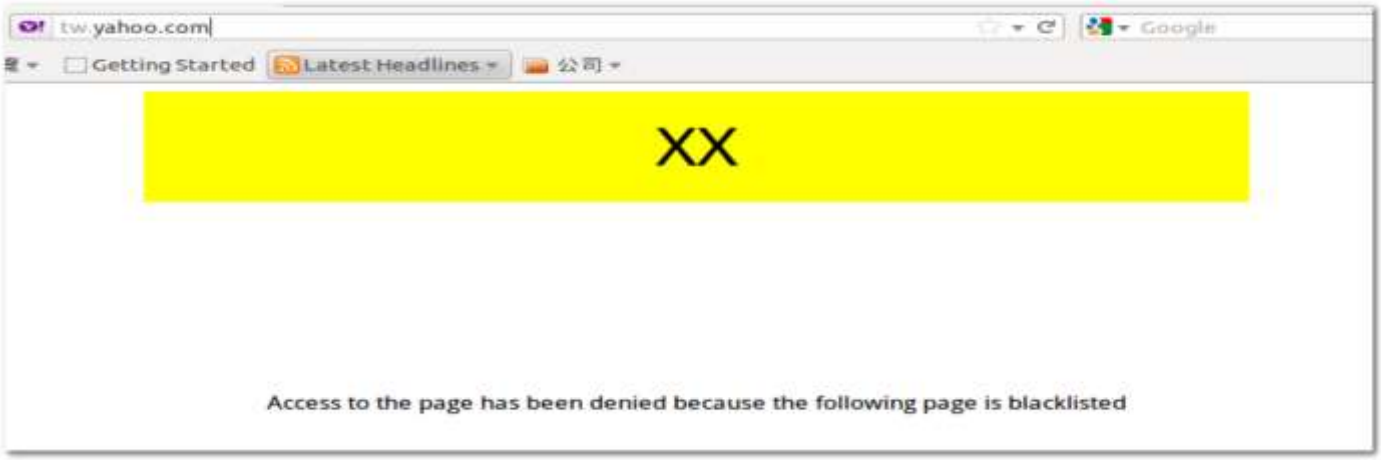


Figure 4-6. 4 Block Warning Message

Setting URL List completed. In addition, select Mark tick box, and click on Add to create a new sub-content, to modify contents, or to cancel list. (Figure 4-6.5)

Figure 4-6. 5 URL Settings

There is an example of how 4-6 URL Filter is used.

1. Select Policy > LAN Policy or DMZ Policy. Then, select the function you need on the right side.
2. Click on Add, and select Action to Permit, and then select URL Access Control which you have just set in 4-6 URL Filter. (Figure 4-6.6)

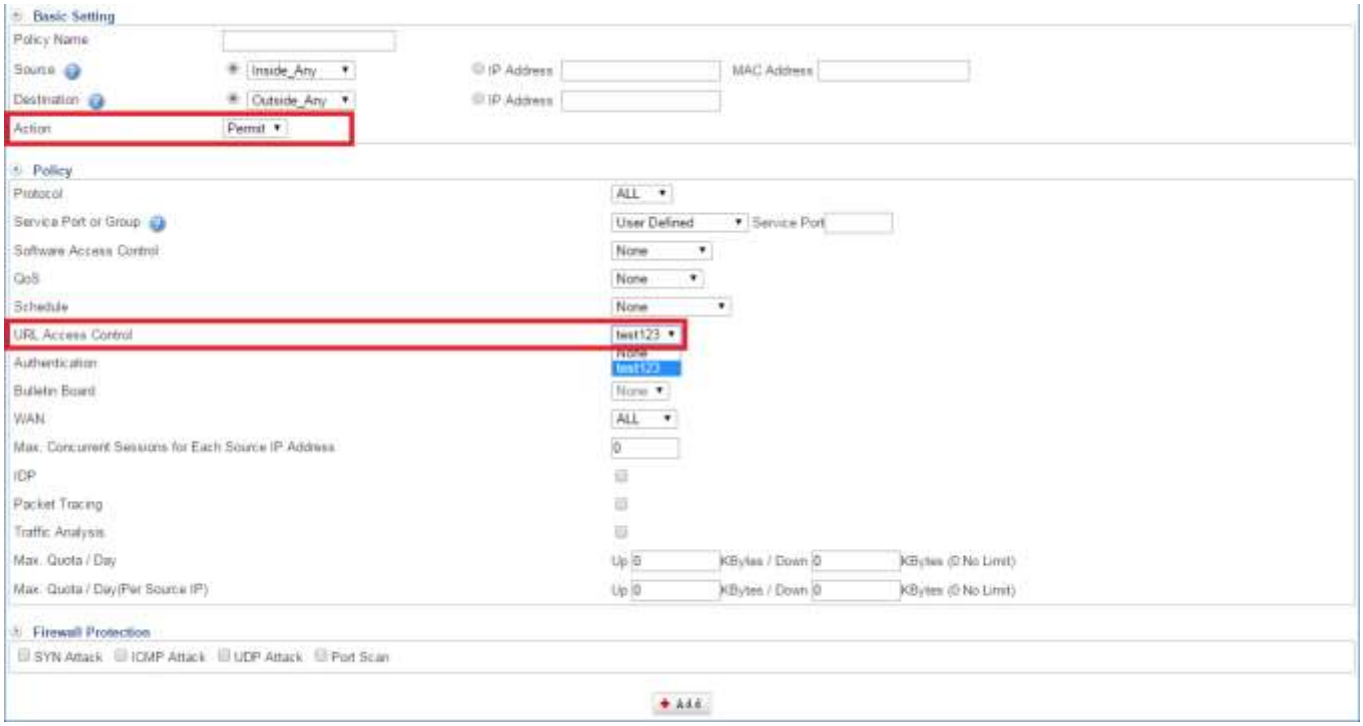


Figure 4-6. 6 URL Policy

Setting URL Policy completed. Afterward the users can browse the website except “youtube,” “google,” and “yahoo” in domain name by the above policy. (Figure 4-6.7)

Figure 4-6. 7 URL Policy List

Other Settings

You are able to modifty your own waring Subject and content here (Figure 4-6.8) (Figure 4-6.9)

Figure 4-6. 8 Other Settings

Figure 4-6. 9 warning Subject

Log

Enter the data that you want to search, and click on Search. (Figure 4-6.10)

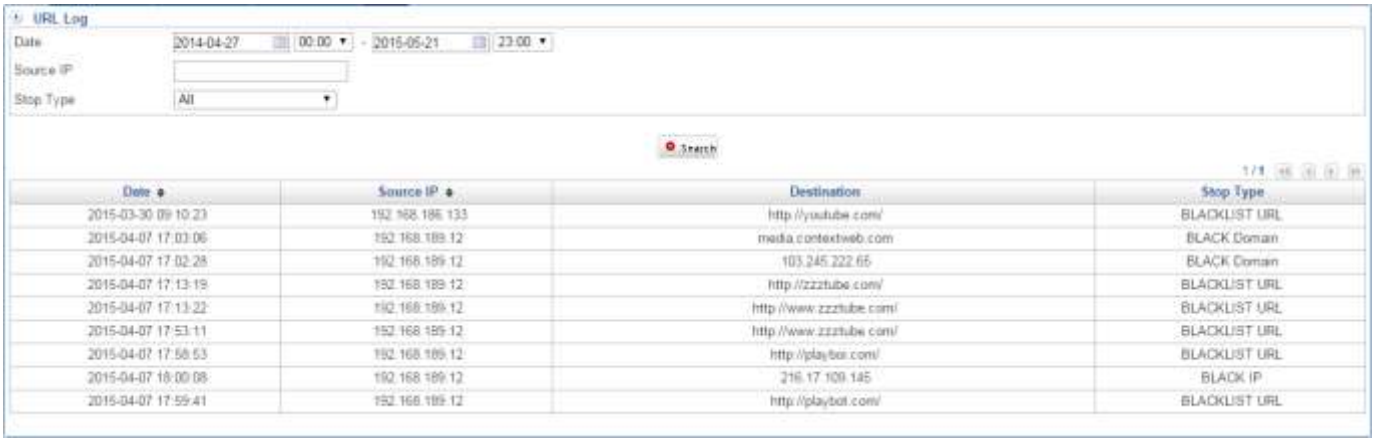


Figure 4-6. 10 URL Filter logs

4-7 Virtual Server

The real IP address provided from ISP is always not enough for all the users when the system manager applies the network connection from ISP. Generally speaking, in order to allocate enough IP addresses for all computers, an enterprise assigns each computer a private IP address, and converts it into a real IP address through UR's NAT (Network Address Translation) function. If a server that provides service to WAN network is located in LAN networks, external users cannot directly connect to the server by using the server's private IP address. The Virtual Server has set the real IP address of the UR's WAN network interface to be the Virtual Server IP. Through the Virtual Server function, the UR translates the Virtual Server's IP address into the private IP address in the LAN network. Virtual Server owns another feature know as one-to-many mapping. This is when one real server IP address on the WAN interface can be mapped into many LAN network servers provide the same service private IP addresses. This section covers the functionality and application of Virtual Server and Mapped IP. In the Virtual Server section you can enable the following lists:

Virtual Server

Its function resembles Mapped IP's. But the virtual Server Maps one-to-many. That is, to map a Real IP Address to LAN Private IP Address and provide the service item in Service. Select Objects > Virtual Server> Virtual Server. Click on + Add button to create a new virtual server.

- Click on Assist to select IP address. It offers two Assist Select. Here, we suggest using "static IP." (Figure 4-7.1) (Figure4-7.2)
  1. WAN 1 Interface
  2. WAN 2 Interface

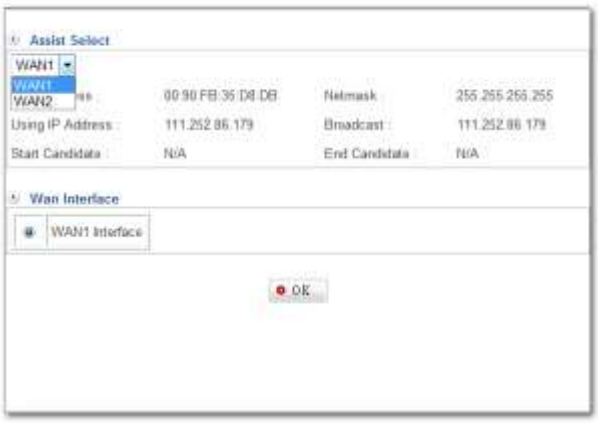


Figure 4-7. 1 Virtual Server Assist Select

■ After selected Virtual WAN IP.

Figure 4-7. 2 Virtual Server

■ Setting Virtual Server WAN IP completed. (Figure 4-7.3)

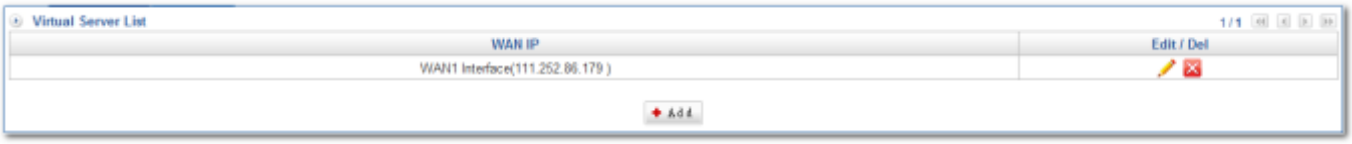


Figure 4-7. 3 Virtual Server List

■ Click on to edit content, and then click on Add, enter Virtual Server IP Address. (Figure 4-7.4)

Figure 4-7. 4 Enter Virtual Server IP

■ User can click on Assist to select External Service Port easily,(Figure 4-7.5) or enter single port. (Figure 4-7.6)

Figure 4-7. 5 Select Service Group

Figure 4-7. 6 Enter single Port

■ Setting Virtual Server completed. In addition, click on + Add to create a new sub-content, Edit to modify contents, or Del to cancel list. (Figure 4-7.7)

Figure 4-7. 7 Virtual Server List

There is an example, how to open mail server port in order to make outside person connect to. Assume your Mail Server IP is 192.168.99.250. Please follow the previous steps, and then create a WAN policy in Policy > WAN Policy > WAN to LAN. (Figure 4-7.8) (Figure 4-7.9)

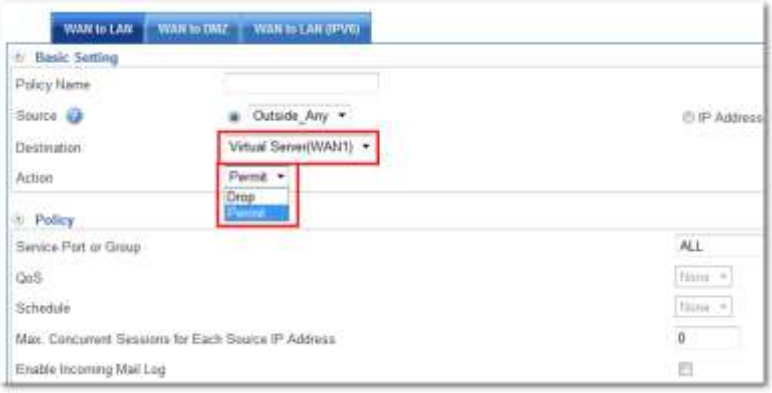


Figure 4-7. 8 WAN to LAN Policy

Figure 4-7. 9 Setting WAN to LAN policy completed

Then, enter WAN IP and port number. For example, http://111.252.76.144:88 (Figure 4-7.10)

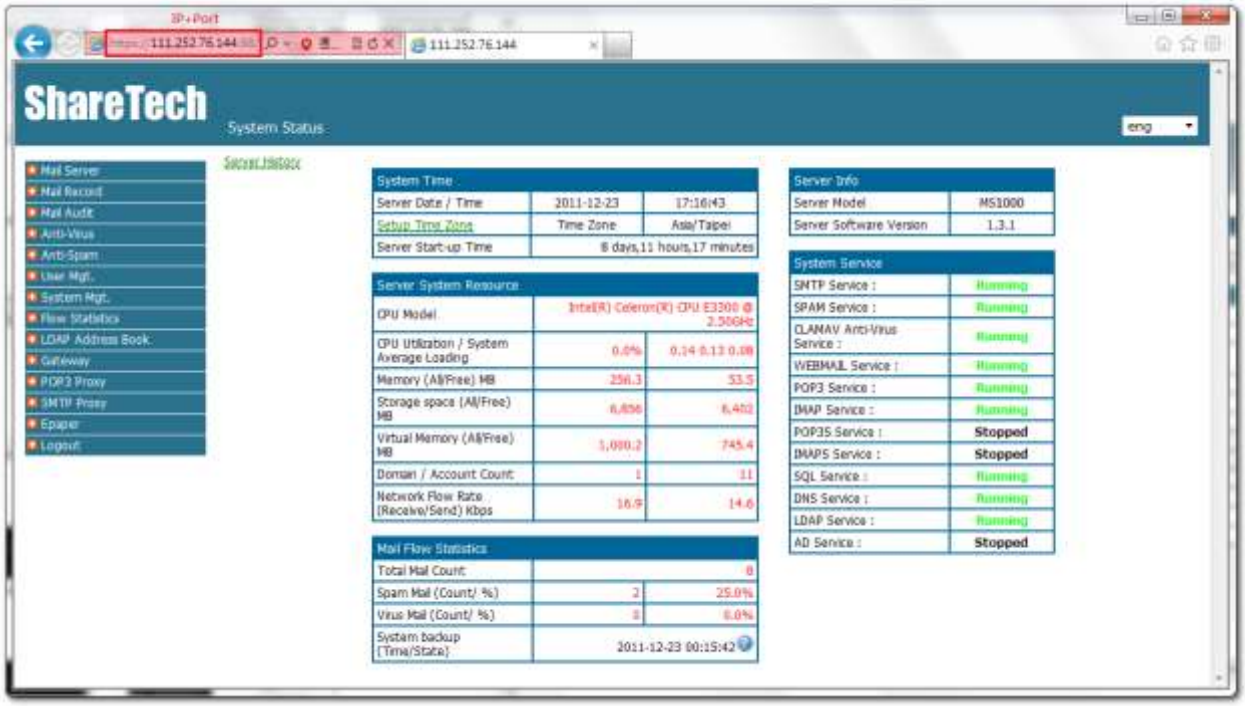


Figure 4-7. 10 WAN Virtual server 88port

Otherwise, enter WAN IP and port number, https://111.252.76.144:888 (Figure 4-7.11)

Figure 4-7. 11 WAN Virtual 888port

Mapped IP

Because of the intranet is transferring the private IP by NAT[4] Mode, so, using NAT to map a wan Real IP address to a LAN Private IP address. It is a one-to-one mapping. That is, to gain access to internal servers with private IP addresses from an external network, mapping is required. Select Objects > Virtual Server> Mapped IP. Click on Add to create a new one.

- Click on Assist button to select WAN IP address. It offers two Auxiliary Select. (Figure 4-7.12)
  1. WAN 1 Interface selections.
  2. WAN 2 Interface
- Map to Virtual IP:

Figure 4-7. 12 Mapped IP

- Setting Mapped IP completed. In addition, click on Add to create a new sub-content, Edit to modify contents, or Del to cancel list. (Figure 4-7.13)

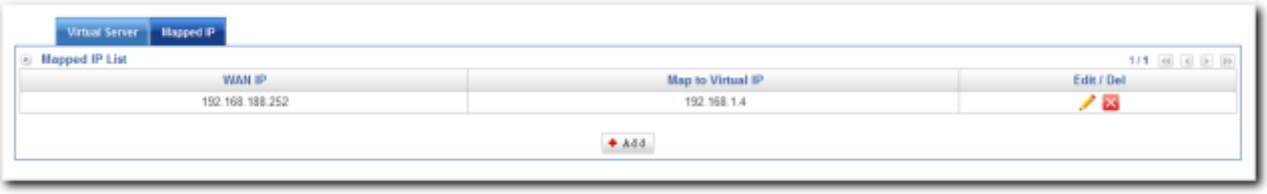


Figure 4-7. 13 Mapped IP List

[4] NAT = Network Address Translation

4-8 Firewall Protection

This section allows setting up the rules that specify if and how IP traffic flows through your UTM Appliance. It offers a standard firewall and creates its firewall rules using firewall function. In the Firewall Function section you can enable the following lists:

Firewall Protection

Firewall protection primarily uses packet filtering to detect and block intruders. Some also include application filtering. In addition, these applications typically generate alerts and log intrusion attempts. Default firewall Protection function is enabled. Select Objects > Firewall Protection > Firewall Protection. (Figure 4-8.1)

- SYN attack detection: SYN Flood is a popular attack way. DoS and DDoS are TCP protocol. Hackers like using this method to make a counterfeit of connection, and the CPU and memory, and so on resource is been consume.
- ICMP attack detection: ICMP is kind of a pack of TCP/IP; its important function is for transfer simple signal on the Internet. There are two normal attack ways which hackers like to use, Ping of Death and Smurf attack.
- UDP attack detection: Hackers use UDP Protocol to make a counterfeit of connection, and the CPU and memory, and so on resource is been consume.

Figure 4-8. 1 Firewall Function

There is an example, how to set up firewall protection. Assume your Mail Server IP is 192.168.99.250. Please follow the previous steps, and then create a WAN policy in Policy > WAN Policy > LAN to WAN or WAN to LAN.

1. Select Policy > LAN Policy, DMZ Policy, or WAN Policy. Then, select the function you need on the right side. Here, we use LAN to WAN for sample. Click on Add first.
2. Select Action to Permit, and then choose protection on Firewall Protection (Figure 4-8.2) (Figure 4-8.3) (Figure 4-8.4)

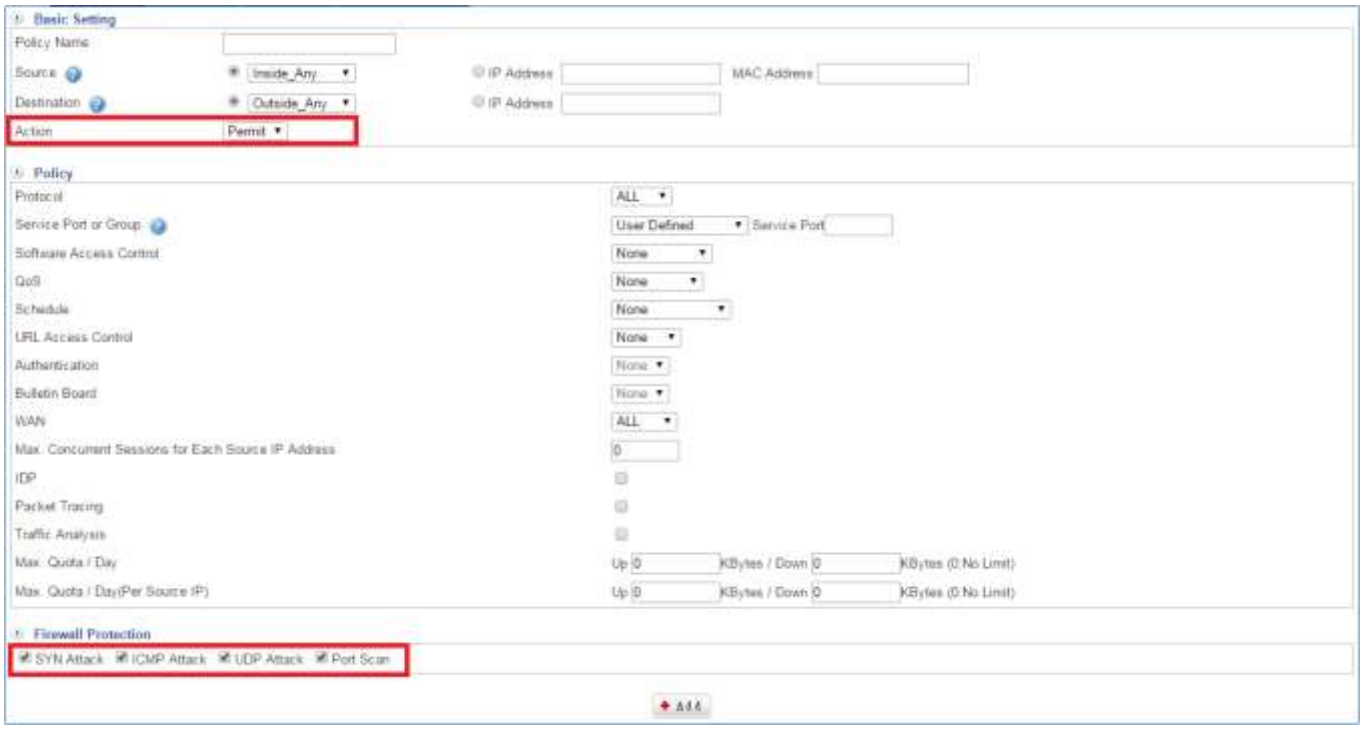


Figure 4-8. 2 Firewall Protection on Policy

Figure 4-8. 3 Completed Policy

Figure 4-8. 4 Firewall Protection Log

■ Other items: (Figure 4-8.5) (Figure 4-8.6)

Figure 4-8. 5 firewall protection other items

After choose other items, you don't have to set up Policy, and then you are able to see the attack log on Objects > Firewall Protection > Attack Log. (Figure 4-8.6)

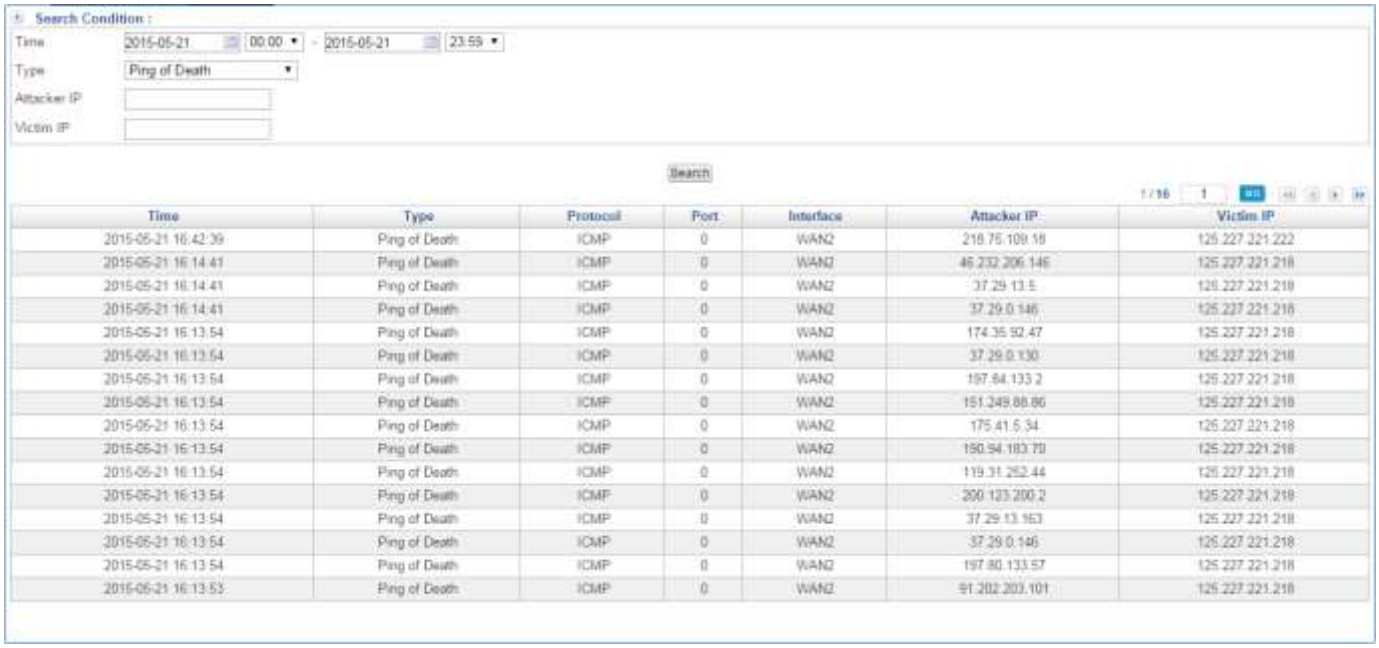


Figure 4-8. 6 Search Condition

Attack Log

Select Objects > Firewall Protection > Attack Log. You are able to search see all of attack logs which through SG-100N machine. (Figure 4-8.7)

Figure 4-8. 7 Attack Log

4-9 Authentication

Internet Authentication serves as a gateway to filter out unauthorized users from accessing the Internet. Configuring the Authentication provides an effective method of managing the network's use. Therefore, IT administration can control the user's connection authority by setting account and password to identify the privilege, and then users have to pass the authentication to access to Internet. In this section, it offers some authentication modes, Local Users, User Group, External Auth Settings which are include AD[5] and POP3, adding flexibility to your choice of authentication method. In addition, it also offers Internet Auth Recorder and Auth Status. The IT administrator can use two methods to know the authentication of LAN's users what they have been done. In the Internet Auth section you can enable the following lists:

Auth Setting

Select Objects > Authentication > Auth Setting. (Figure 4-9.1)

- Authentication port: The port number that authentication requires. Default port is 82.

range: 1 ~ 65535,0 means authentication disabled

- Authentication Connection Protocol: please choose HTTP or HTTPS
- Max Concurrent Connections:

range: 10 ~ 256

- Idle timeout: If an authenticated connection has been idle for a period of time, it will expire. Default is 60 minutes.

range: 1 ~ 1000

- Re-login after user has logged in for: Determines the valid time of an authentication. Authentication expires on the due time.

range: 0 ~ 24,0 means no limit

- Allow change password: Permits users who are using the device's local authentication mechanism to modify their own password
- Deny multi-login: When enabled, once a user has logged in with his / her authentication account no other user is permitted to log in to the same account.
- Temporarily Block when Login failed more than:

0 means no limit

- IP blocking Period:

[5] AD = Active Directory

0 means permanent blocking

- Permanently block when login failed more than:

0 means no limit

- Unblocked IP: here, will show up total blocked IP, and then you are able to see detailed on status.
- Account expiration notification:

0 represents the day

- Delete expired account:

0 means no limit, that is never deleted

- Select authentication mode: Click on Edit button to enter mode. These modes are separated by using comma.
  1. L: Local
  2. A: AD
  3. P: POP3
  4. R: RADIUS

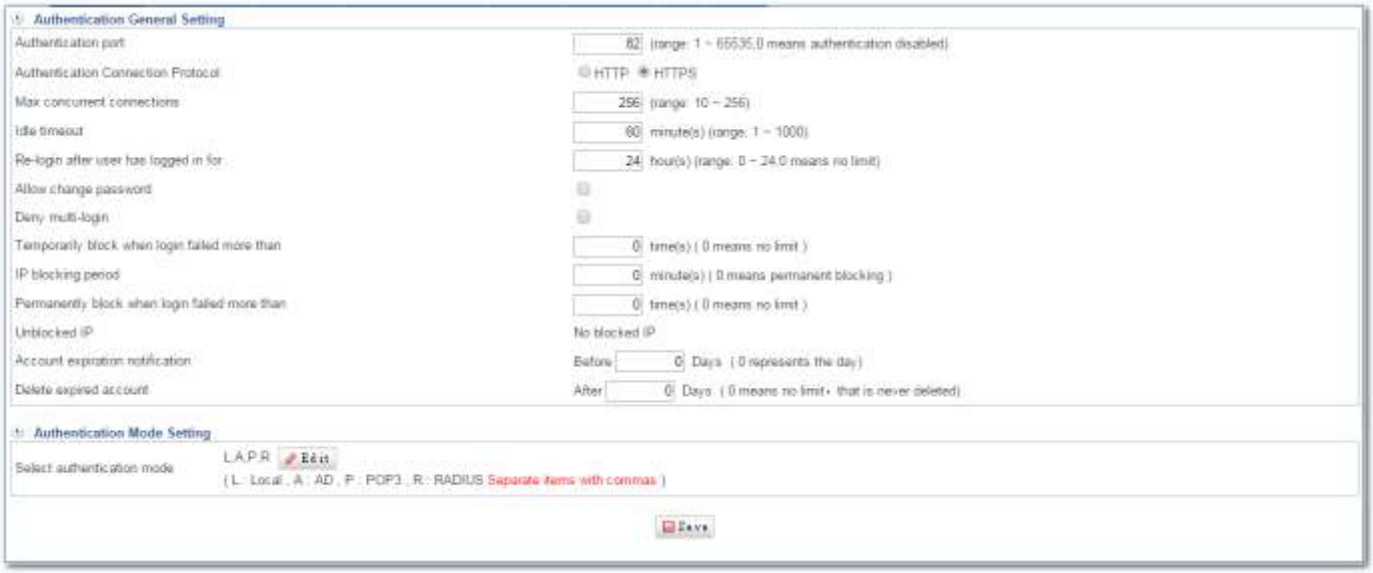


Figure 4-9. 1 Authentication General Setting

Page Settings

Select Objects > Authentication > Page Settings. (Figure 4-9.2)

- Redirect successfully authenticated users to: Authenticated user can be redirected to the designated web site by assigning its address to this field. Leaving it blank means the user will just go directly to their desired web site.

- Subject: Enter some words to be website subject.
- Content: Enter some message which shown in the login screen. Leaving it blank will result in no message be show.
- Upload logo: Click on Browse... . This picture will show when users use Internet by through the Internet authentication way. The Login screen shows before a user accesses a web site.

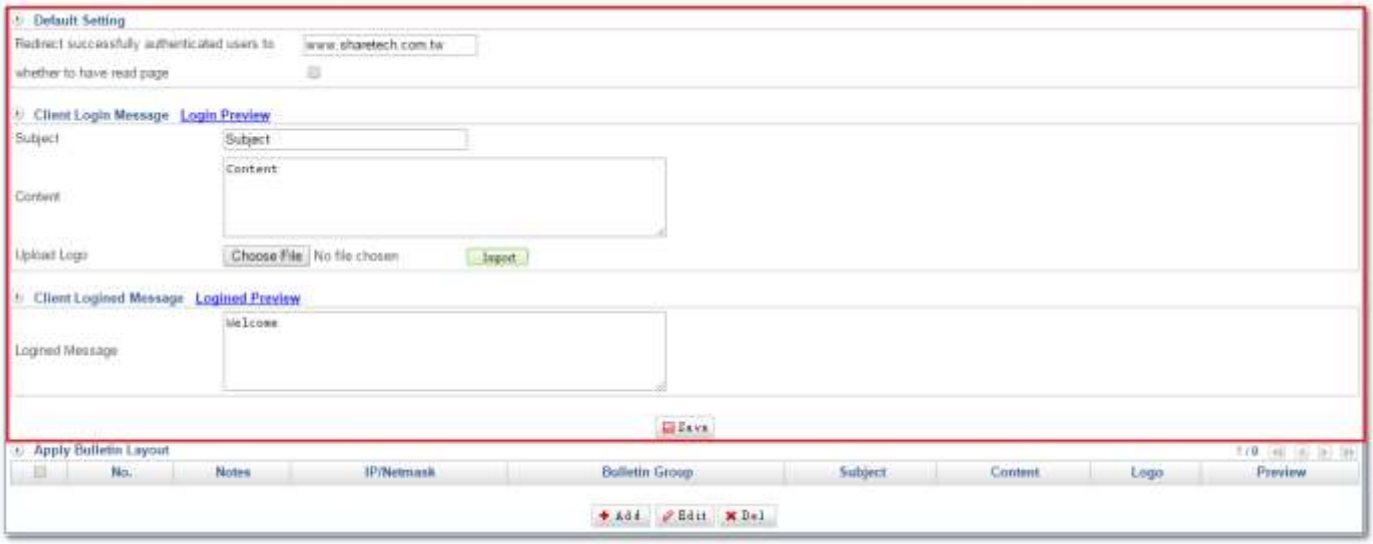


Figure 4-9. 2 Page Default Setting

- You are able to click Login Preview to see login screen which your settings. There is an example figure as below. (Figure 4-9.3)

Figure 4-9. 3 Client Login Message

- You are able to click Login Preview to see screen after user login successfully. There is an example figure as below. (Figure 4-9.4)

Figure 4-9. 4 Client Logined Message

■ Before start to set up "Apply Bulletin Layout" we should set up Bulletin Board first. (Figure 4-9.5)

Figure 4-9. 5 Add user Define Settings

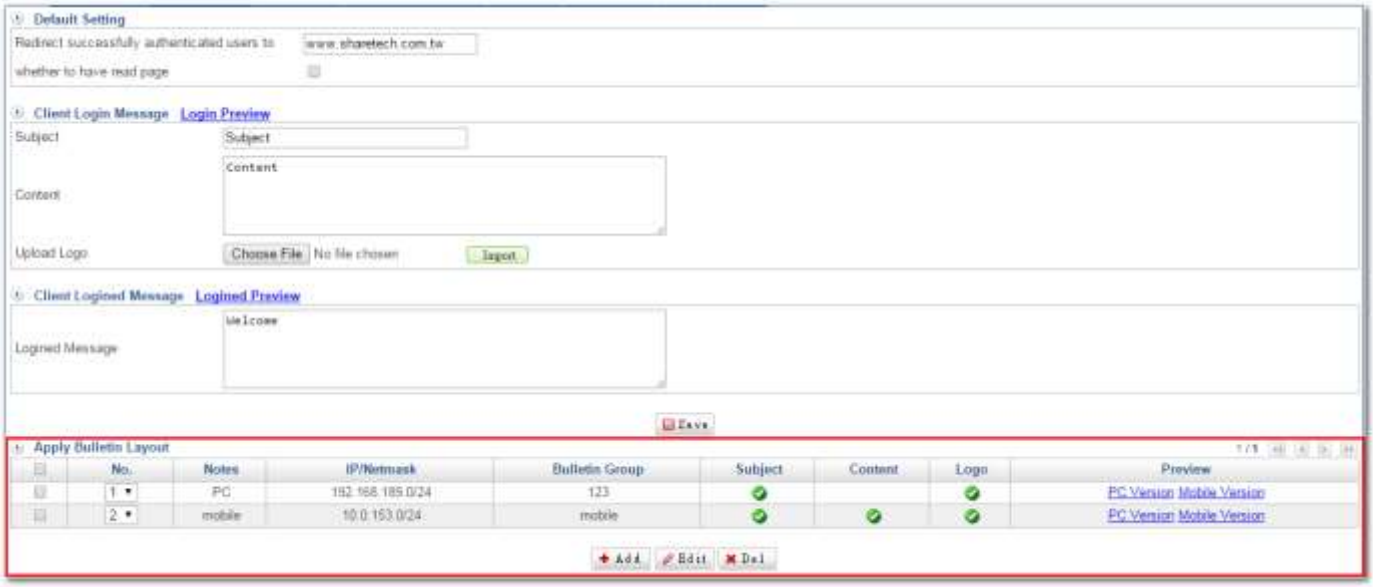


Figure 4-9. 6 Apply Bulletin Layout

You are able to click PC Version and Mobile Version to see login screen which your settings. There are two examples as below. (Figure 4-9.7) (Figure 4-9.8)

Figure 4-9. 7 PC Version

Figure 4-9. 8 Mobile Version

Local User

Select Objects > Authentication > Local User. (Figure 4-9.9)

- User List: If you have many accounts, you can click on Browse... to bring in accounts. After selected, click on Import. Then, you do not have to enter account step by step.

Click on + Add first.

- Name: The user name for authentication
- User Account: The account for authentication
- Password: The password for authentication
- Confirm Password: The confirmation of password
- require users to log on when the next change password: If selected, the local authentication accounts can be forced to change their passwords at their next login attempt.
- user account expiration date: Sets the period of validity for a user's account

Figure 4-9. 9 Add User Account

Setting Local Users completed. In addition, click on Add to create a new sub-content, Edit to modify contents, or Del to cancel list. (Figure 4-9.10)

Figure 4-9. 10 Users list

Then, please see User Group part to see how to use Internet Authentication.

POP3, RADIUS User

Select Objects > Authentication > POP3, RADIUS User. Please check your mail server Network Setting first. (Figure 4-9.11)

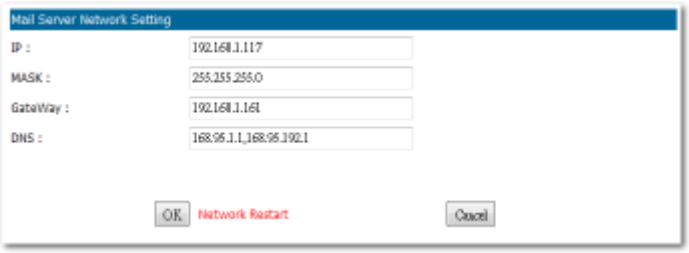


Figure 4-9. 11 POP3 Server

Then, add a POP3 server info. (Figure 4-9.12)

Figure 4-9. 12 Add a server

Second, we suggest importing all of POP3 accounts, it will faster than enter each of accounts. We use "*sharetech01@randoll.com.tw*" for testing here. (Figure 4-9.13)

Figure 4-9. 13 POP3 accounts

Click to edit info. (Figure 4-9.14)

Figure 4-9. 14 Edit POP3 Server

Enter "*sharetech01*" in Account field. (Figure 4-9.15)

Figure 4-9. 15 Enter POP3 Account

Create one account successfully. Also, you are able to import file (Figure 4-9.16)

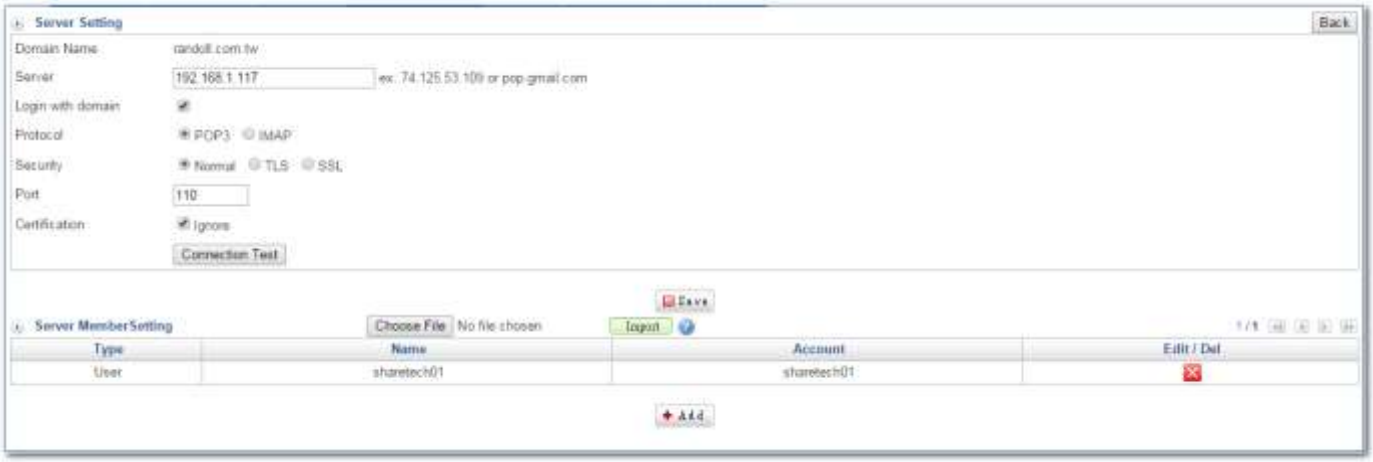


Figure 4-9. 16 Server Member Setting

Then, please see User Group part to see how to use Internet Authentication.

On the other hand, If mail server is internal, and do not allow external personal yet. We advise set up DNS first in UTM. Please refer 5-3 DNS Server chapter.

Let's set up DNS Server in Network Services > DNS Server > Domain Setting. (Figure 4-9.17)

Figure 4-9. 17 DNS Server

Setting DNS Server completed. (Figure 4-9.18)

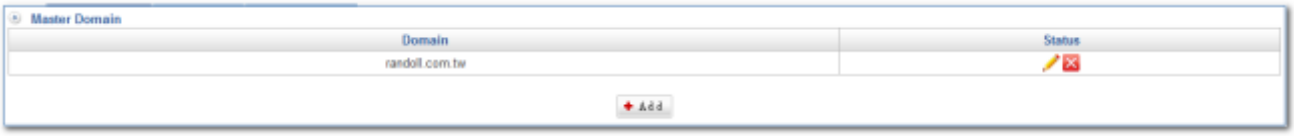


Figure 4-9. 18 Setting DNS Server completed

Click to check A of domain. (Figure 4-9.19)

Figure 4-9. 19 check A of domain

AD User

Select Objects > Authentication> AD User

- AD Settings; After you enter your AD address and AD Domain Name, please click on Save settings first. Then, click on Connect Test to make sure whether it is correct or not. (Figure 4-9.24)

Figure 4-9. 20 AD setting

And then, please see User Group part to see how to use Internal Authentication.

User Group

Select Objects > Authentication > User Group. Click on + Add.

- Group name; Enter some words for recognition.
- Auth Settings:
  1. Use a shared set: It is accord with Auth Settings.
  2. Use custom settings: The settings of When asked how long the idle re-registration, How long after the user logs requested a re-registration, and Select Authentication Mode are defined by yourself. (Figure 4-9.10)

Figure 4-9. 21 Use custom settings

- Choose to edit the user type：There are three ways.
  1. this machine(Local Users) (Figure 4-9.11)

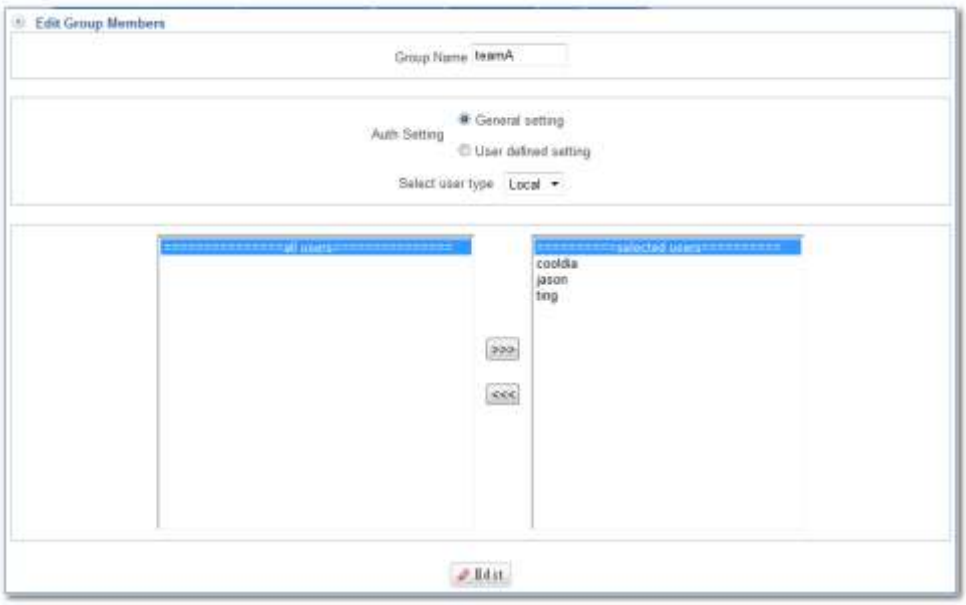


Figure 4-9. 22 Local Users

Setting User Group with Local Users mode completed. In addition, click on Add to create a new sub-content, Edit to modify contents, or Del to cancel list. (Figure 4-9.12)

Figure 4-9. 23 Setting user group with Local Users mode completed

2. POP3 (Figure 4-9.13)

Figure 4-9. 24 POP3

Setting User Group with POP3 mode completed. In addition, click on Add to create a new sub-content, Edit to modify contents, or Del to cancel list. (Figure 4-9.25)

Figure 4-9. 25 Setting user group with POP3 mode completed

3. AD

- AD accounts import：Click on Browse... to bring in accounts. After selected, click on Import.
- Setting User Group with AD mode completed. In addition, click on + Add to create a new sub-content, Edit to modify contents, or Del to cancel list.

There is an example of how User Group is used with Local Users mode.

1. Select Objects > Policy > LAN Policy or DMZ Policy. Then, select the function you need on the right side.
2. Click on + Add, and select Action to ACCEPT, and then select Internet Auth to "*team A*" which you have just set in 4-9 Authentication. (Figure 4-9.26)

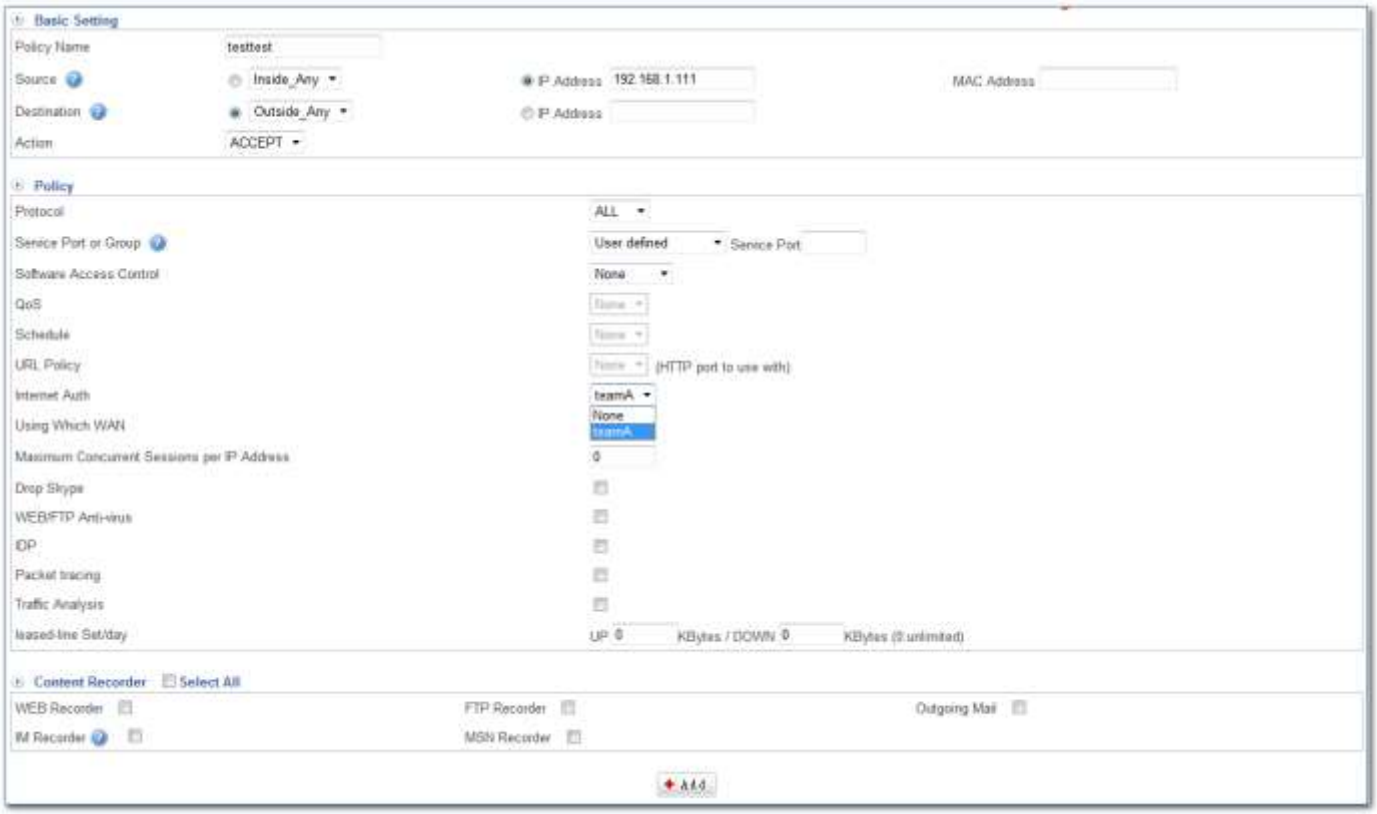


Figure 4-9. 26 Internet Auth Policy

3. Setting Internet Auth Policy completed. (Figure 4-9.27)

Figure 4-9. 27 Internet Auth Policy List

4. Let's login. (Figure 4-9.28)

Figure 4-9. 28 login

There is an example of how User Group is used with POP3 mode.

1. 1 Select Objects > Policy > LAN Policy or DMZ Policy. Then, select the function you need on the right side.
2. Click on Add, and select Action to ACCEPT, and then select Internet Auth to "*testgroup*" which you have just set in 4-9 Authentication. (Figure 4-9.29)

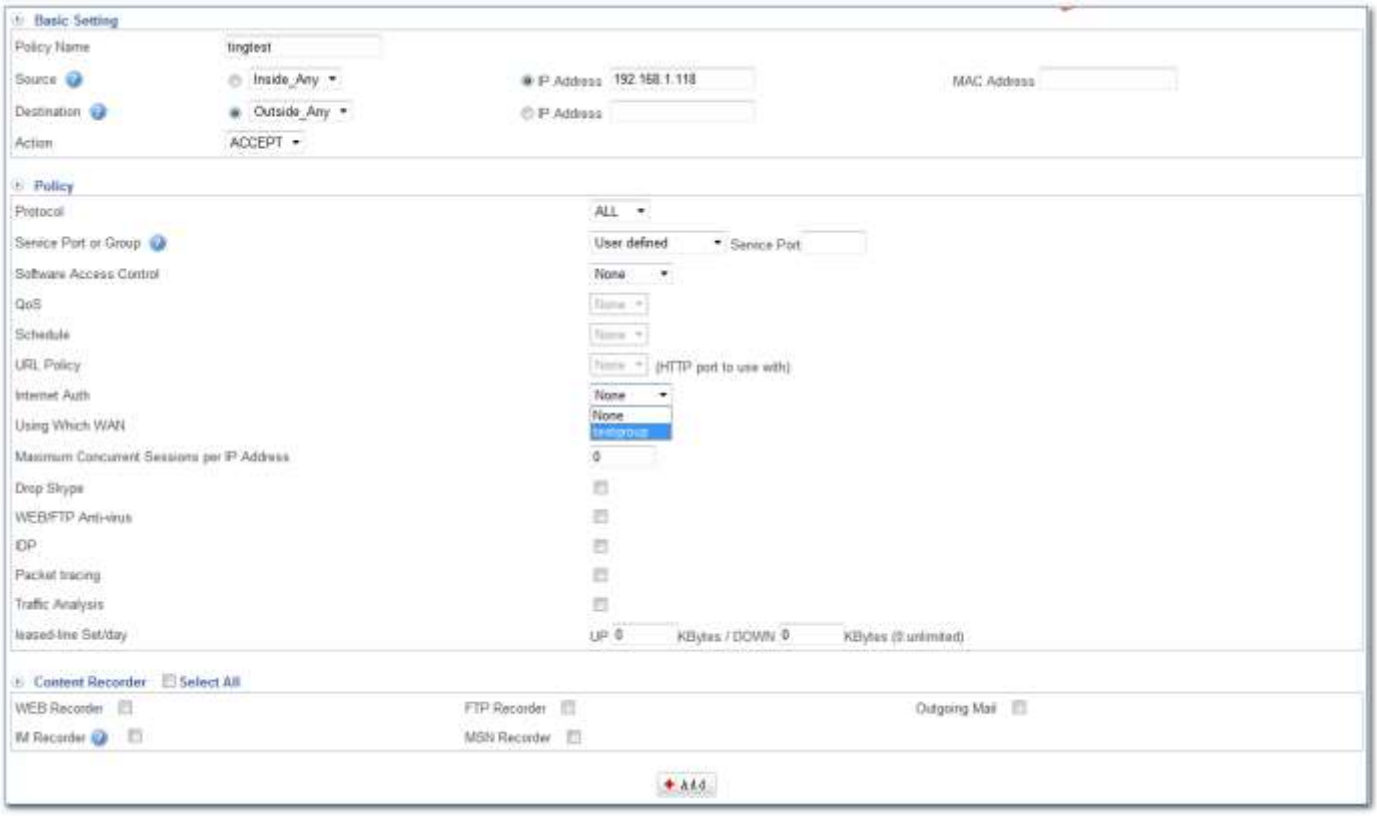


Figure 4-9. 29 Internet Auth policy

3. Setting Internet Auth Policy completed. (Figure 4-9.30)

Figure 4-9. 30 Auth policy

4. Let's login. (Figure 4-9.31)

Figure 4-9. 31 login

Log

This function is accords with the section of Auth Settings, Local Users, User Group, and Policy Chapter. If the user has been Login, the records will be shown. (Figure 4-9.32)

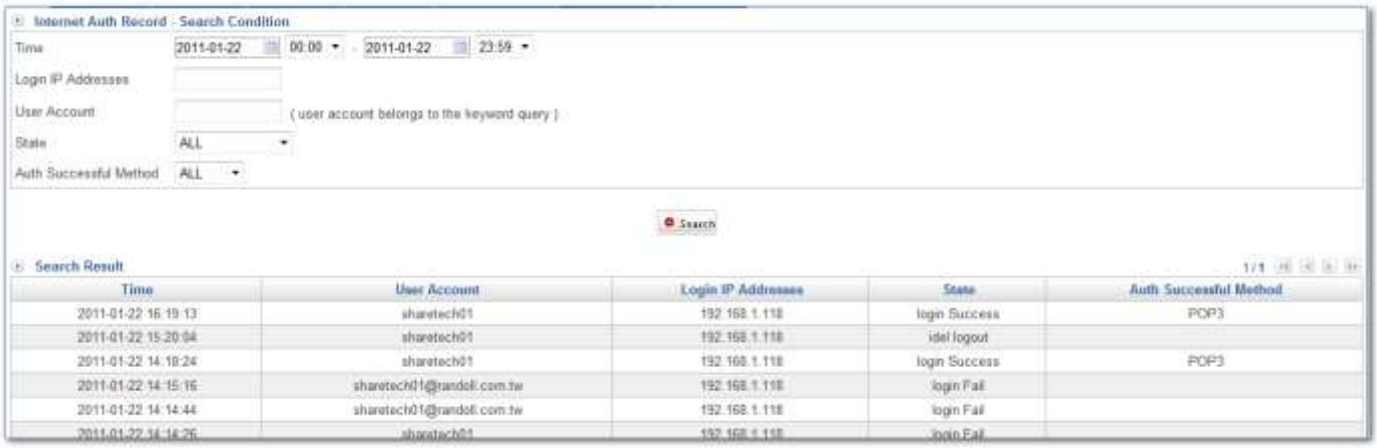


Figure 4-9. 32 Internet Auth Record

Status

It shows the users who is on the Internet at present. You can click on Kick link to kick out the user or user group, and then you cannot use Internet. (Figure 4-9.33) (Figure 4-9.34)

Figure 4-9. 33 login interface

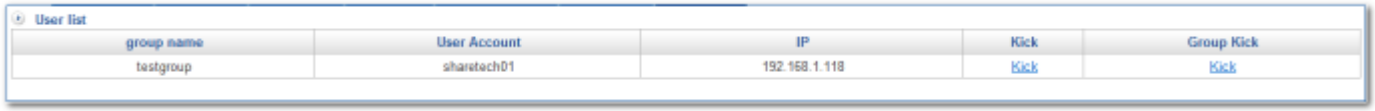


Figure 4-9. 34 Auth Status

4-10 Bulletin Board

In a workplace environment, bulletin boards can save time, promote productivity, and efficiency. The bulletin board offered as part of a company's internal extranet communication systems saves people the hassle of sorting through superfluous emails that aren't work-related. Instead, assignments, memos and messages from clients can be posted on the company's bulletin board.

Noted: Bulletin Board and Authentication cannot be used together.

Bulletin setting

Select Objects > Bulletin Board > Bulletin setting. Click on Add to add new bulletin board. (Figure4-10.1) (Figure4-10.2)

- Group Name: Enter any words for recognition.
- How long to alert bulletin: please enter 0~24 hours
- Before read bulletin, deny all outing: Internal users cannot surf Internet if users do not read content of bulletin yet.
- After read bulletin, url redirect: (Figure 4-10.10)

Figure 4-10. 1 add new bulletin board

Figure 4-10. 2 add bulleting completed

Then, click Layout to edit content of bulletin board. (Figure4-10.3)

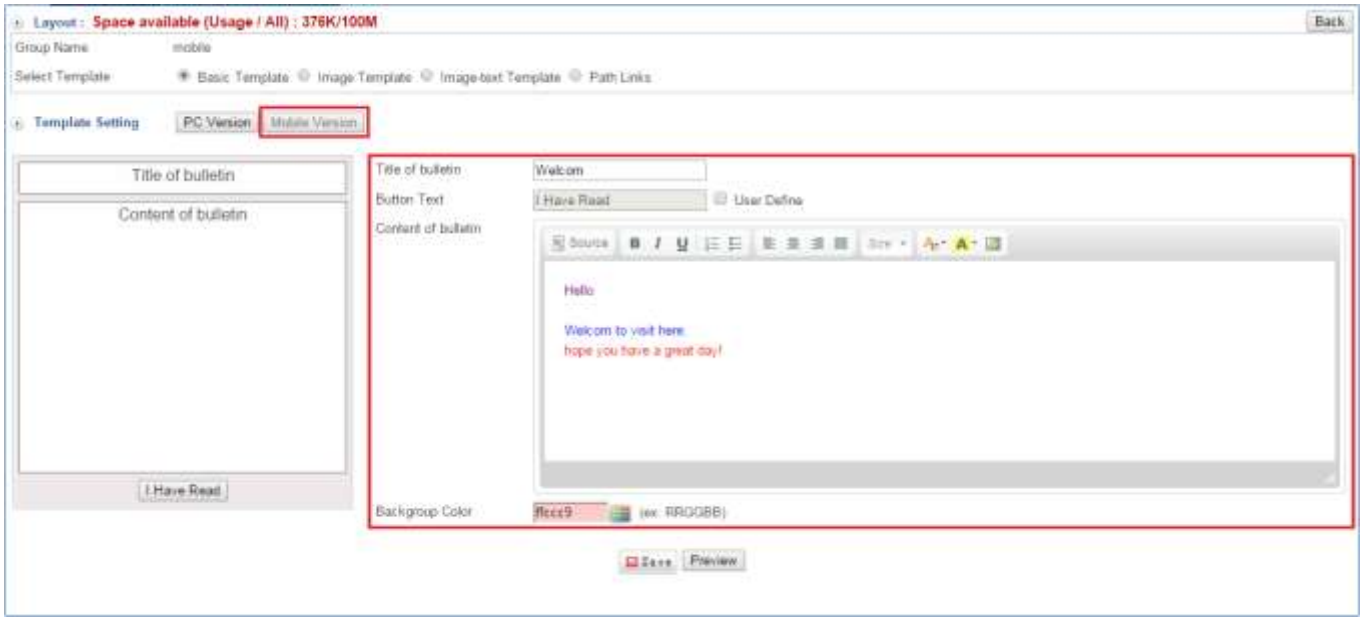


Figure 4-10. 3 edit mobile authentication content

Click on Preview (Figure 4-10.4)

Figure 4-10. 4 Mobile version Bulletin Board Preview

Click Layout to edit content of bulletin board. (Figure 4-10.5)

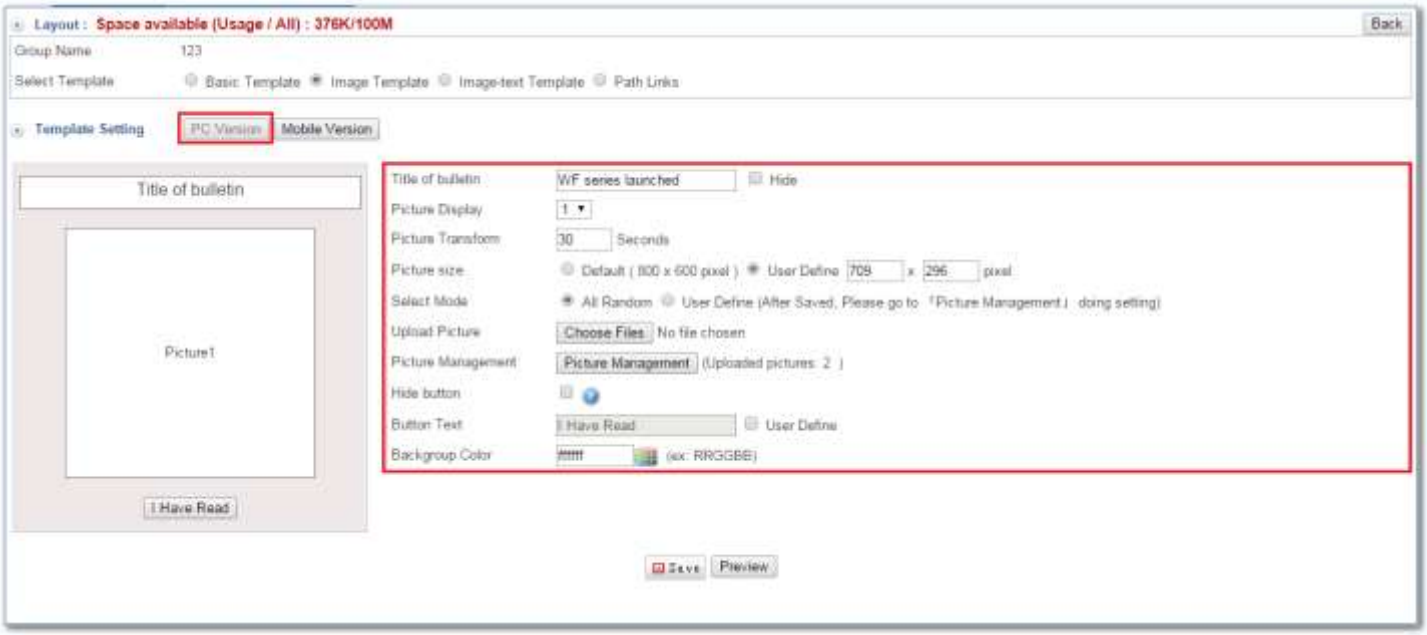


Figure 4-10. 5 edit PC authentication content

Click on Preview (Figure 4-10.6)

Figure 4-10. 6 PC Version Bulletin Board Preview

Select Policy > LAN Policy (or DMZ Policy) > LAN to WAN or LAN to DMZ. Click on + Add to add new policy. (Figure 4-10.7)

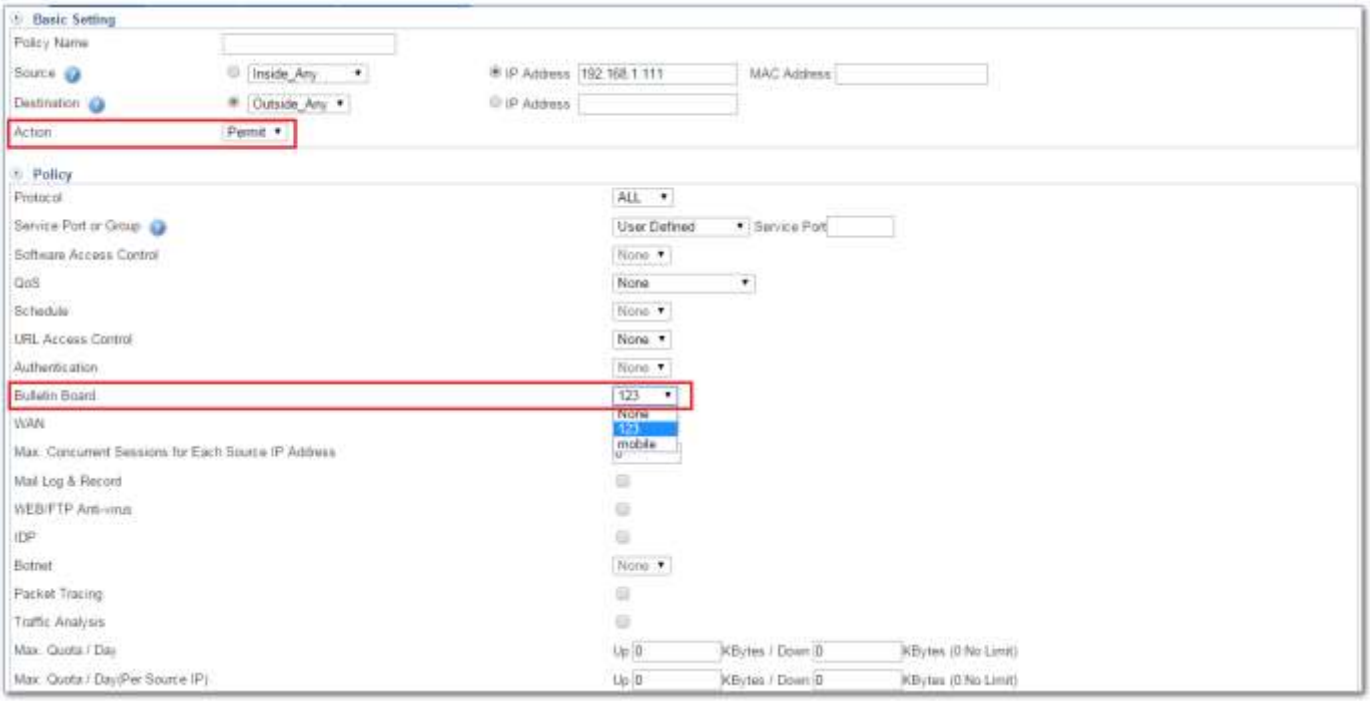


Figure 4-10. 7 add policy

Figure 4-10. 8 add Policy completed

Then, internal users will see bulletin board when they use Web Browser. (Figure 4-10.9)

Figure 4-10. 9 internal users' content bulletin board

After users read bulletin content and click on I Have Read, URL redirect to what Administrator enter. (Figure 4-10.10)

Figure 4-10. 10 URL redirect to

Has read the bulletin board

Select Objects > Bulletin Board > Has read the bulletin board. (Figure 4-10.11)

Administrator sees which IP had read content of bulletin board. Internal user has to read again if Kick out.

Has read the bulletin board :

Group Name	IP Address	Computer Name	When to read the bulletin	Kick	Kick the group
Test Bulletin	192.168.1.111	TING-PC	2012-08-23 14:51:37	kick	kick

Figure 4-10. 11 has read the bulletin board

Chapter 5：Network Services

In the Network Services chapter you can enable the following lists：

- 5-1 DHCP
- 5-2 DDNS
- 5-3 DNS Procy
- 5-4 SNMP
- 5-5 Remote Syslog Server

5-1 DHCP

The DHCP[6]service allows you to control the IP address configuration of all your network devices from ShareTech UR Appliance in a centralized way. When a client (host or other device such as networked printer, etc.) joins your network it will automatically get a valid IP address from a range of addresses and other settings from the DHCP service. The client must be configured to use DHCP, this is something called "automatic network configuration" and is often the default setting. You may choose to provide this service to clients on your LAN only, or include devices on the DMZ or WAN zone. In this section you can enable the following lists:

LAN DHCP Server

Select Network Services > DHCP > LAN DHCP Server

- Physical Interface: eth0
- IP Address: it depends on what you set up on LAN
- Start / End address of IP Range 1 and 2: Specify the range of addresses to be handed out. These addresses have to be within the subnet that has been assigned to the corresponding zone. Primary / Secondary DNS: This specifies the DNS to be used by your clients. Since ShareTech UR Appliance contains a caching DNS server, the default value is the firewall's own IP address in the respective zone.
- Primary / Secondary WINS:
- Lease time (mins) / Max lease time (mins): This defines the default /maximum time in minutes before the IP assignment expires and the client is supposed to request a new lease from the DHCP server. In order to avoid UR use the same IP, how long can we also establish the same IP max lease time.
- Default Gateway: The default gateway of the LAN
  Domain name: This is the default domain name that is passed to the clients. When the client looks up a hostname, it will first try to resolve the requested name. If that is not possible, the client will append this domain name preceded by a dot and try again.
- Enabled: please enable it if you would like to use this feature, and choose Save (Figure 5-1.1)

[6] Dynamic Host Configuration Protocol

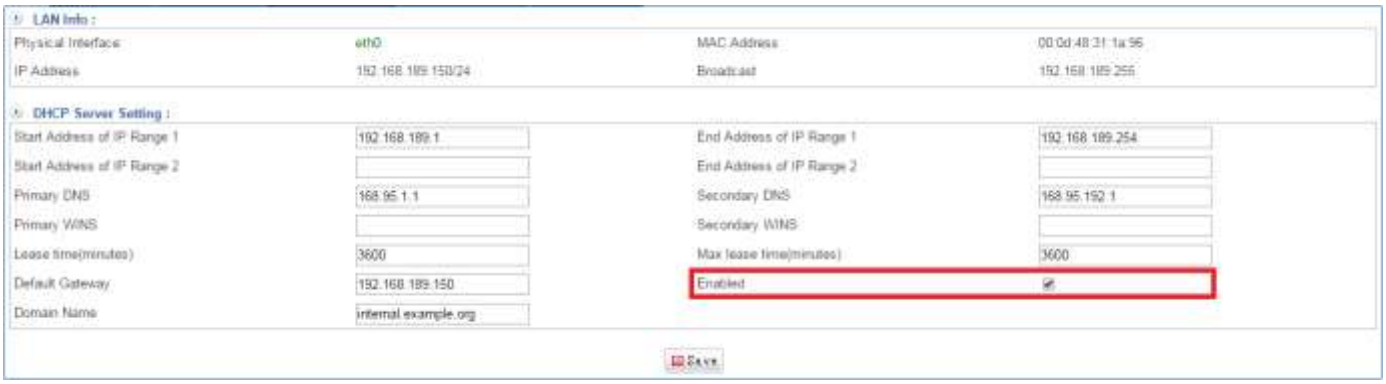


Figure 5-1. 1 LAN DHCP Server

LAN User List

After enable LAN DHCP server, please check your Network Services > DHCP > LAN User List. (Figure 5-1.2)

Figure 5-1. 2 LAN User List

DMZ DHCP Server

Please note that Interface Type depend on what you set up on Network > Interface > Interface Config

- Enabled: please enable it if you would like to use this feature, and choose Save (Figure 5-1.3)

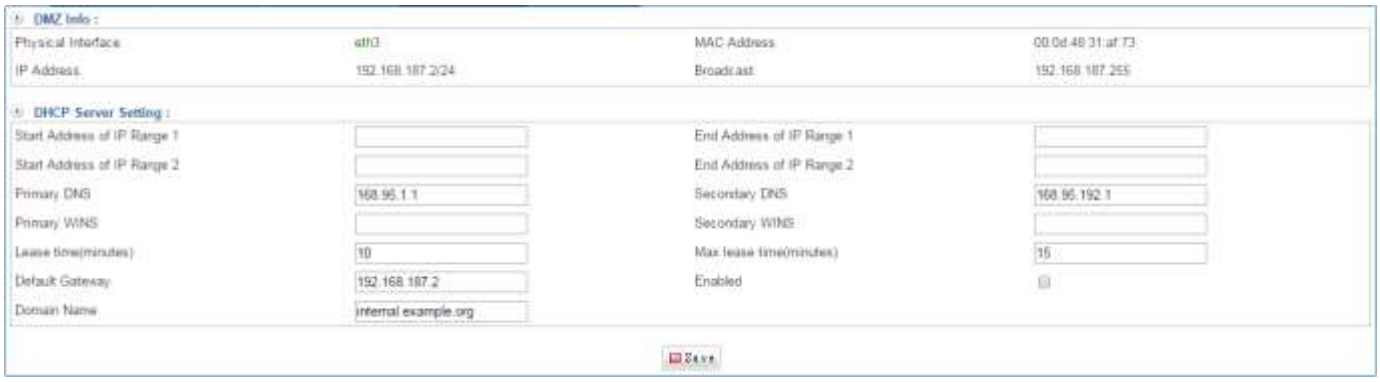


Figure 5-1. 3 DMZ DHCP Server

DMZ User List

After enable DMZ DHCP server, please check your Network Services > DHCP > DMZ User List. (Figure 5-1.4)

3. If you don't enable DMZ DHCP server, and it doesn't show IP list.

Figure 5-1. 4 DMZ User List

DHCP Static IP

Select Network Services > DHCP > DHCP Static IP. If you have been select "Get static IP address" from DHCP Server, you will see DHCP Static IP list here. (Figure 5-1.5)

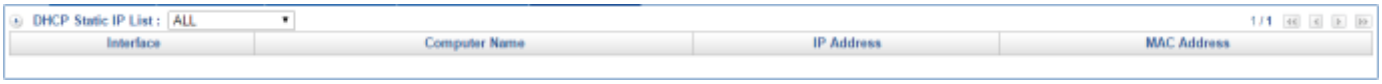


Figure 5-1. 5 DHCP Static IP

5-2 DDNS

DDNS[7], it allows you to make your server available to the Internet even though it does not have a static IP address. To use DDNS you must first register a sub-domain with a DDNS provider. Then whenever your server connects to the Internet and is given an IP address by your ISP it must tell the DDNS server this IP address. When a client machine wishes to connect to your server it will resolve the address by asking the DDNS server, which will answer with the latest value. If this is up to date then the client will be able to contact your server (assuming your firewall rules allow this). EFW makes the process of keeping your DDNS address up to date easier by providing automatic updates for many of the DDNS providers. In this section you can enable the following lists:

DDNS Server

Dynamic DNS providers a service that allows assigning a globally available domain name to IP addresses. This works even with addresses that are changing dynamically such as those offered by residential ADSL connections. For this to work, each time the IP address changes, the update must be actively propagated to the Dynamic DNS provider. Select Network Services > DDNS > DDNS Server. (Figure 5-2.1)

- Click on + Add to create a new one.
- Service Provider: Choose the DDNS provider.

4. For instance, "no-ip.org"
   http://www.noip.com/support/knowledgebase/getting-started-with-no-ip-com/

- Hostname: The hostname and domain as registered with your DDNS provider.

5. For instance, "*ShareTec*" and "*dhs.org*"

- WAN: The real IP address that the domain name corresponds to
  1. WAN 1
  2. WAN 2
- Account: Enter an account for DDNS server.
- Password: Enter a password for DDNS server.
- Comment: Enter any word for recognition.
- Enabled: Select Enabled tick box. If it is not ticked, the Firewall will not update the information on the DDNS server. It will retain the information so that you can re-enable DDNS updates without reentering the data. It contains a DDNS client for 14 different providers - if Enabled, it

[7] Dynamic DNS

will automatically connect to the dynamic DNS provider and tell it the new IP address after every address change.

Figure 5-2. 1 DDNS server

- Setting DDNS Server completed. In addition, click on to create a new sub-content, Edit to modify contents, or Del to cancel list. (Figure 5-2.2)

Figure 5-2. 2 DDNS Server List

5-3 DNS[8] Proxy

The DNS (domain name system) is a network system of servers that translates numeric IP addresses into readable, hierarchical Internet addresses, and vice versa. This is what allows your computer network to understand that you want to reach the server at 192.168.188.186 (for example) when you type into your browser a domain name such as www.ShareTech.com.tw.
ShareTech SG-100N offers a DNS proxy which receives DNS queries from the local networks and forwards them to DNS servers on the Internet. The responses are cached, thus IP addresses of sites frequently accessed are delivered quickly. For example, it's like A computer. (Figure 5-3.1) (Figure 5-3.2) (Figure 5-3.3)

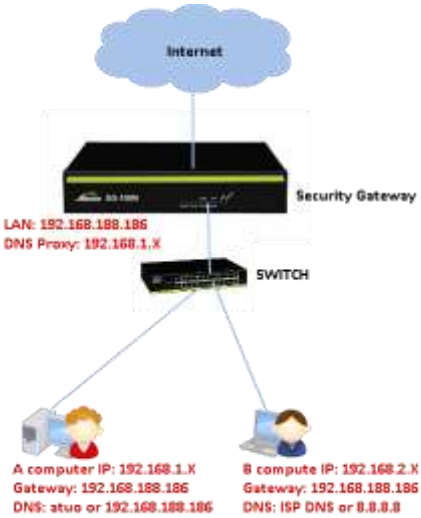


Figure 5-3. 1 DNS Proxy

General Setting

Select Network Services > DNS Proxy > General Setting. Enter the IP that be allowed recursive queries.

Figure 5-3. 2 DNS Proxy General Setting

[8] DNS = Domain Name Servers

Figure 5-3. 3 Allow recursive quires

5-4 SNMP

SNMP[9] is an "Internet-standard protocol for managing devices on IP networks. Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks, and more." It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

- SNMP agents expose management data on the managed systems as variables. The protocol also permits active management tasks, such as modifying and applying a new configuration through remote modification of these variables.
- SNMPv3 primarily added security and remote configuration enhancements to SNMP

Figure 5-4. 1 SNMP

[9] SNMP = Simple Network Management Protocol

Here, IT administrator can use ShareTech SNMP client plus MRTG to see more network status. (Figure 5-4.1) In this section you can enable the following lists:

Please select Network Services > SNMP > SNMP. (Figure 5-5.2)

Figure 5-4. 2 SNMP Agent

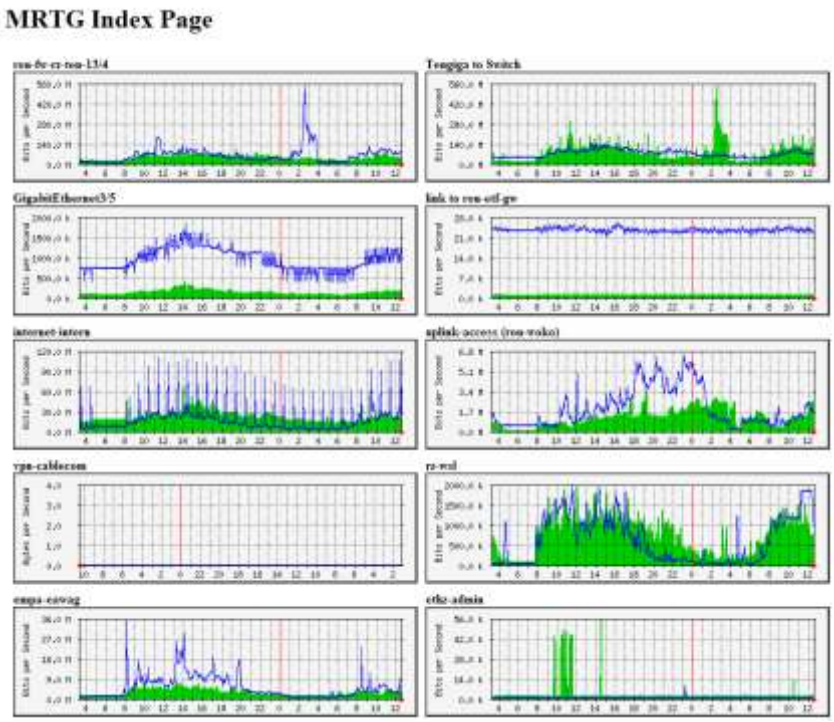


Figure 5-4. 3 MRTG Index page

5-5 Remote Syslog Server

SG-100N logs all its security functions so that you can analyze and do statistics. Also, there is a search function in all these log pages. Some abnormal behaviors of network can be located and then help you to fix. The log function is disabled by default.

Remote Connect Setup

To enable SG-100N sends logs to the external syslog server. Please select Network Services > Remote Syslog Server > Remote Connect Setup.(Figure 5-5.1) Click "Enable" and enter the syslog server information.

Figure 5-5. 1 Remote Syslog Server

6. Syslog is a service for remotely logging data. For example, it allows monitoring video less network equipment. Here, I use Kiwi Syslog, please download the following link：http://www.kiwisyslog.com/downloads/registration.aspx?productType=ks&AppID=876&CampaignID=70150000000Es8J

7. Select "I Agree"(Figure 5-5.2)

Figure 5-5. 2 Select "I Agree"

8. Select "Install Kiwi Syslog Server as a Service," and "Next"(Figure 5-5.3)

Figure 5-5. 3 Select "Install Kiwi Syslog Server as a Service"

9. Select "The localSystem Account," and "Next"(Figure 5-5.4)

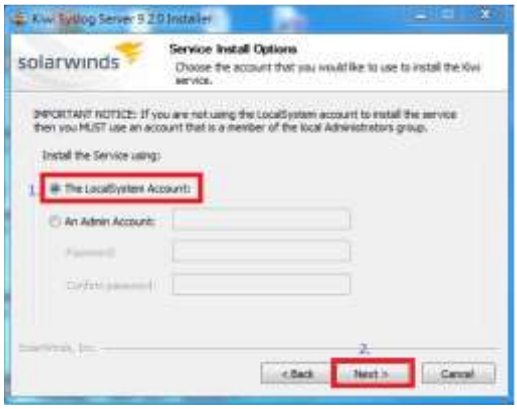


Figure 5-5. 4 Select "The LocalSystem Account"

Don't select "Install Kiwi Syslog Web Access," and "Next"(Figure 5-5.5)

Figure 5-5. 5 Don't select "Install Kiwi Syslog Web Access"

10. Select "Next"(Figure 5-5.6)

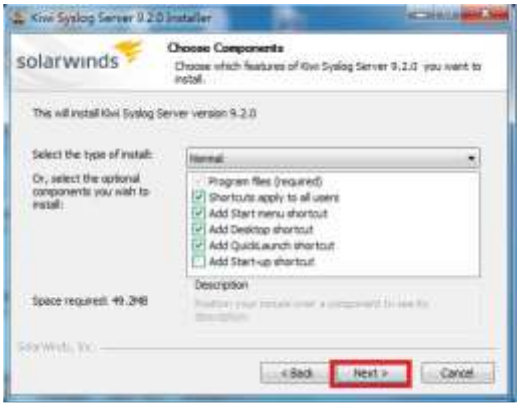


Figure 5-5. 6 Choose Components

11. Select ”Install”(Figure 5-5.7) (Figure 5-5.8)

Figure 5-5. 7 Choose Install Location

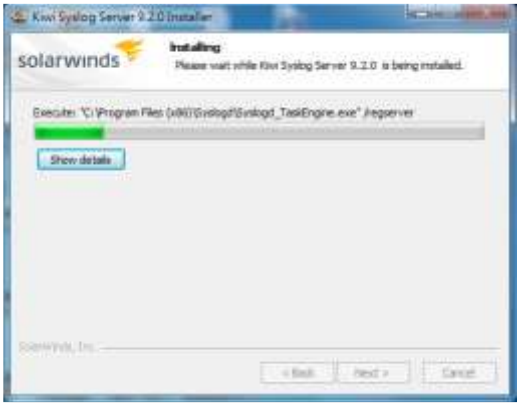


Figure 5-5. 8 Installing

12.Select ”Finish.”(Figure 5-5.9)

Figure 5-5. 9 Completing the Kiwi Syslog server 9.2.0 Setup Wizard

13. Please select Policy.
14. Choose Permit, and must select "Packet Tracing."(Figure 5-5.10) (Figure 5-5.11)

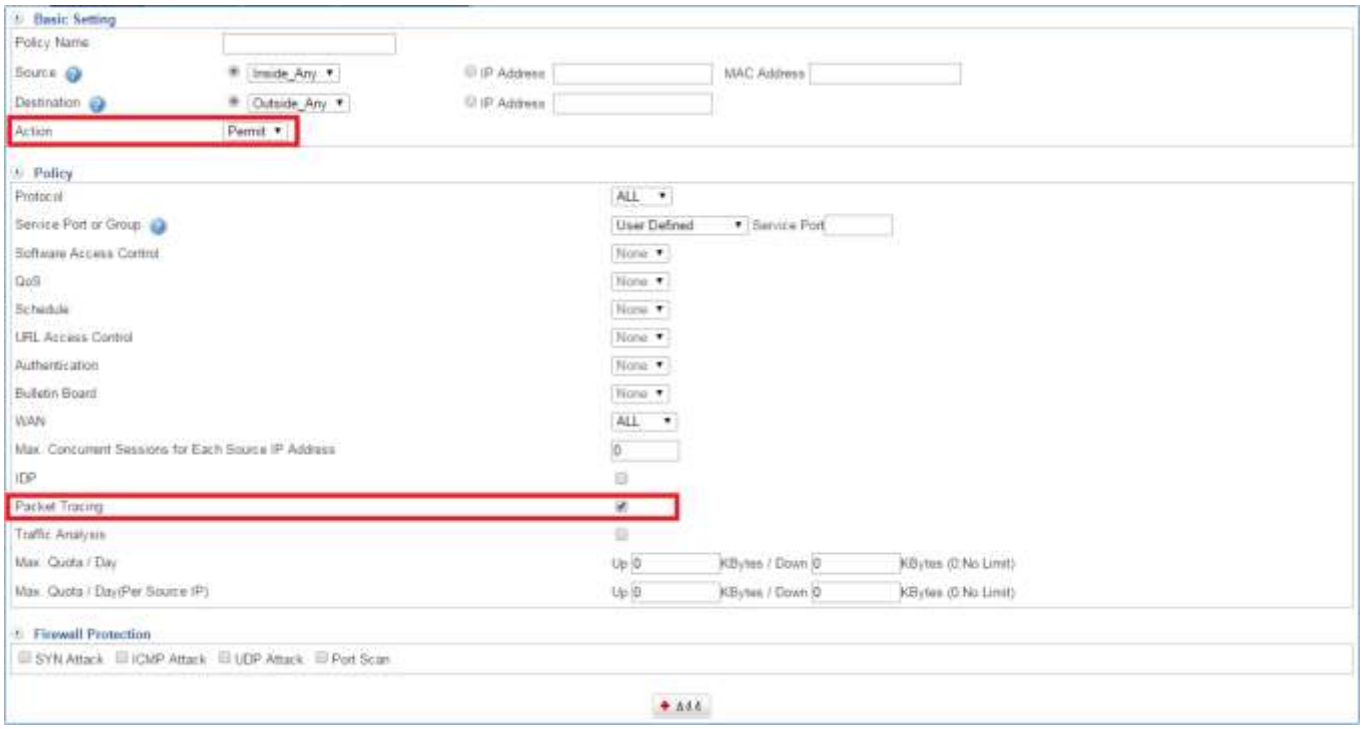


Figure 5-5. 10 Select "Packet Tracing"

Figure 5-5. 11 Policy setting

15. Then, you will see Syslog such as the following figure.(Figure 5-5.12). It's similar like packet Tracing Log (Figure 5-5.13)

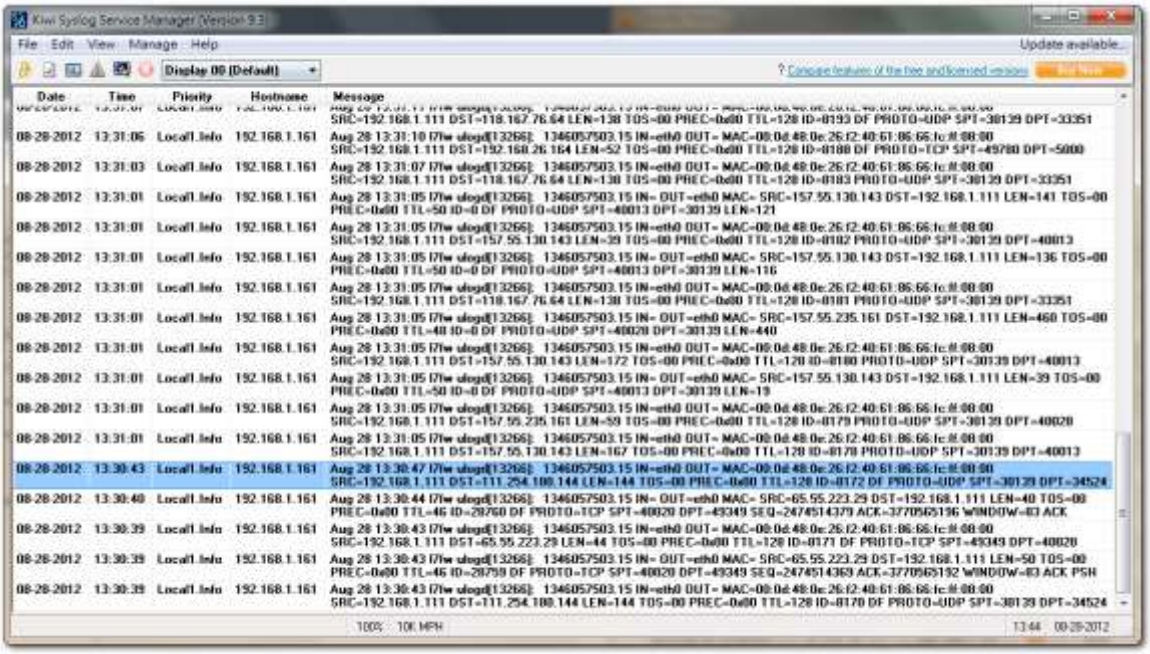


Figure 5-5. 12 Kiwi Syslog Service

16. Please click on Log (Figure 5-5.13)

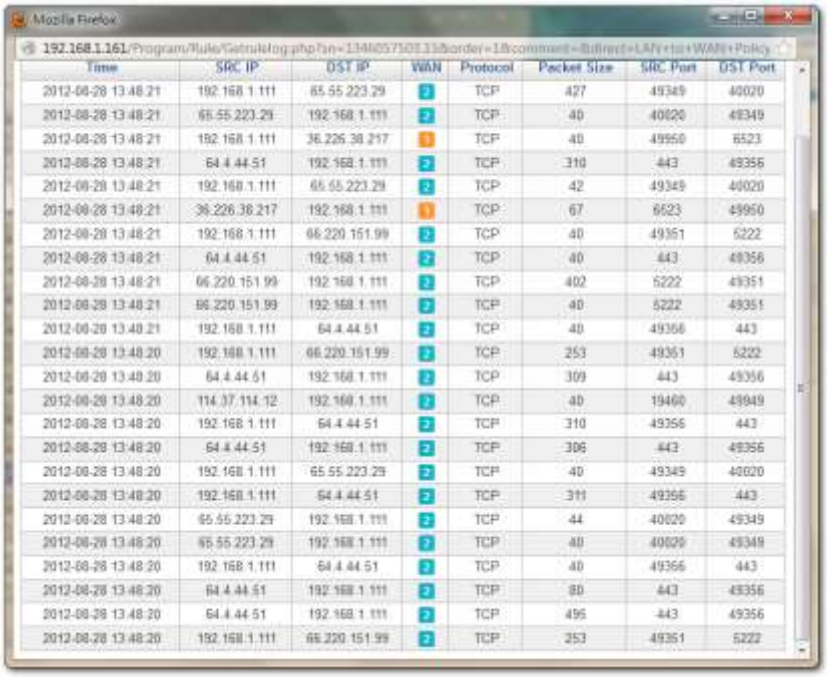


Figure 5-5. 13 Packet Tracing Log

If you want to export syslog to .txt file, please follow the steps. Please select "File > Setup"(Figure 5-5.14)

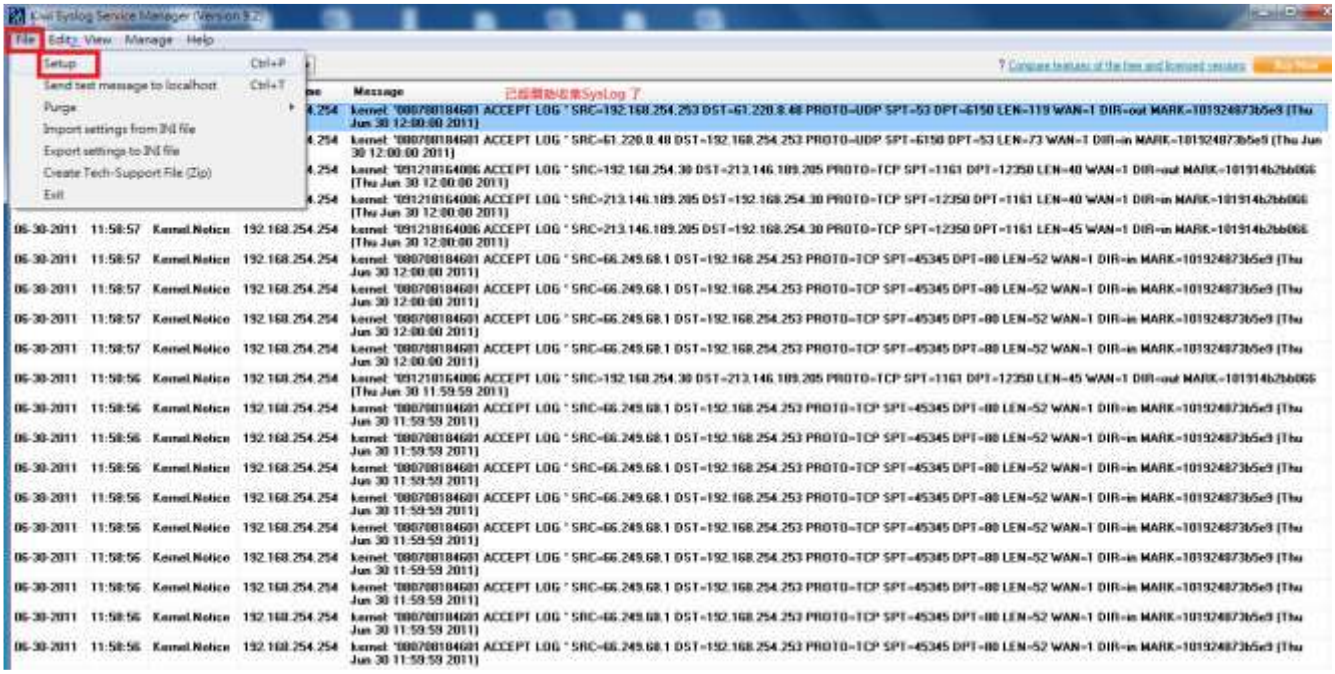


Figure 5-5. 14 Kiwi Setup

Please select "Log to file"(Figure 5-5.15) and depend on how your setting.

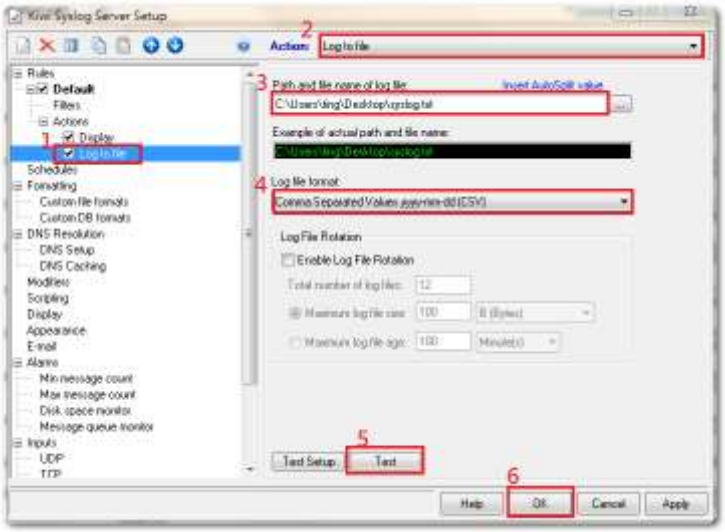


Figure 5-5. 15 Select "Log to file"

Then, completing export syslog file. (Figure 5-5.16)

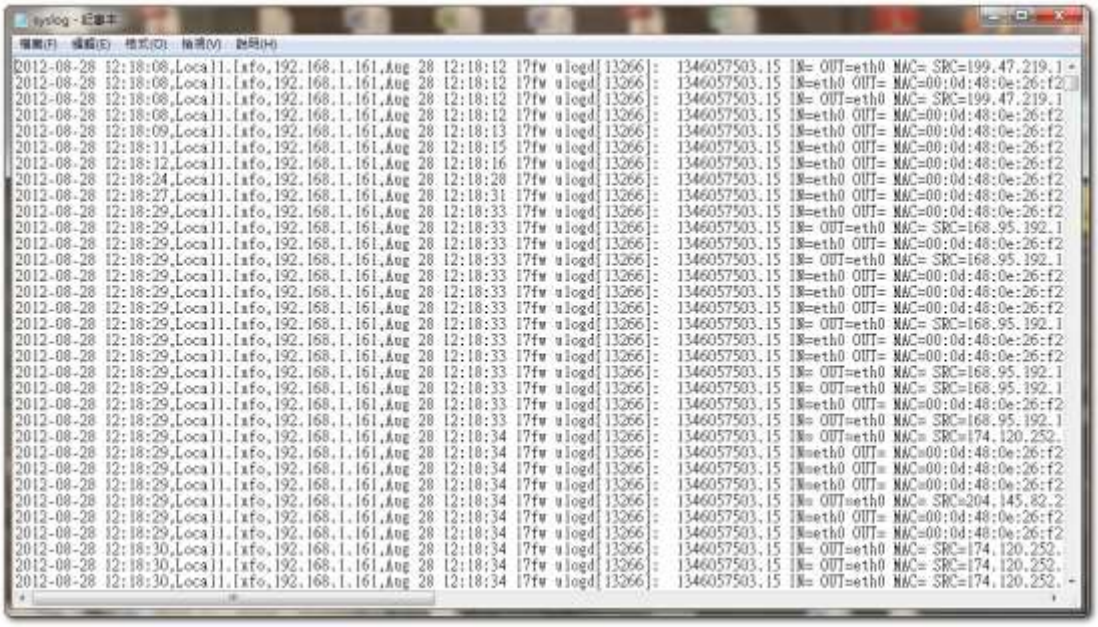


Figure 5-5. 16 export syslogs

Besides, users also can use mail Notification. Please select "E-mail." (Figure 5-5.17)

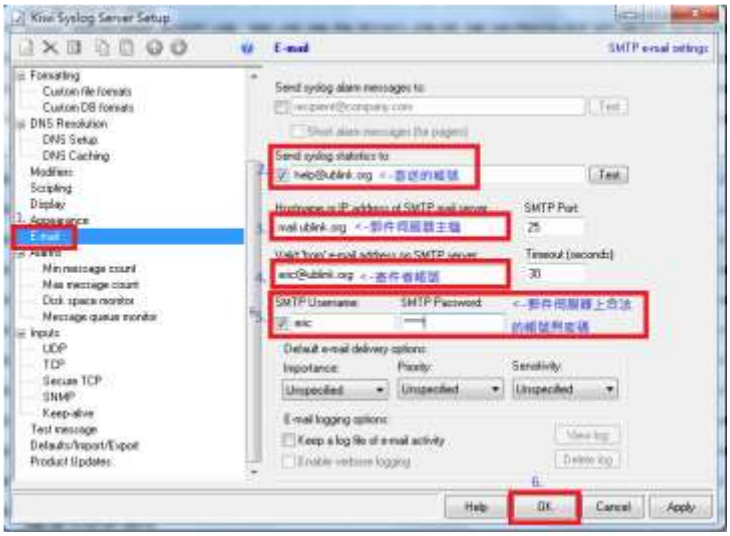


Figure 5-5. 17 syslog E-mail setting

Chapter 6：IDP

Traditional firewall can inspect Layer 2 to Layer 4 of OSI model, such as Source IP Address, Destination IP Address, Source Port Number, Destination Port Number, and Flag Fields. However, traditional defense system cannot protect industry's network from evolving threats and virus anymore.

ShareTech UTM built-in IDP[10] (IDS + IPS) can inspect the packets from OSI layer 4 (transport layer) to OSI layer 7 (application layer) by using Deep Packet Inspection (DPI), and block concealed malicious code, such as worms and buffer overflow attacks. As soon as an attack is suspected, UTM will immediately notify the IT administrator. Moreover, an extensive range of reports is available for the IT administrator to analyze.

Integrated IDP system with attack-signature database protects industries from network threats, such as Trojan horse, virus, worms, buffer overflow etc. Take worm as an example, to protect attack from worm, the only thing for firewall to do is to close ports. As for the file-based virus, it is outside the scope of firewall protection. ShareTech UTM built-in IDP with huge database can inspect all the packets from WEB, P2P, IM, NetBIOS etc.

[10] IDP = Intrusion Detection and Prevention

6-1 IDP Setting

In order to protect your network from various security threats, the device produces timely alerts and blocking mechanisms based upon anomaly flows and the inspection of packet contents. Thus, it ensures that the network's performance remains efficient and uninhibited. This section deals with the configuration settings of IDP. ShareTech AW models include the well-known IDS[11] and IPS[12] system Snort. It is directly built into the IP-firewall (Snort inline). At this time no rules can be added through the web interface, hence Snort is usable only for advanced users that can load their own rules through the command line. Select IDP > IDP Setting > Basic Setting. (Figure 6-1. 1)

Note : we suggest setting High Risk and Medium Risk are OK

Basic Setting

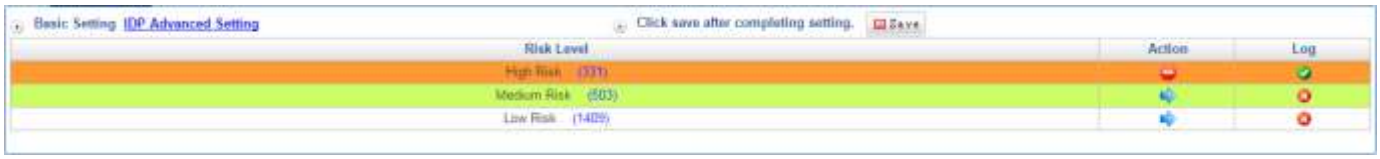


Figure 6-1. 1 IDP Basic Setting

- Risk Name: The level risk name
- Action: Click on Action figure button.
  1. : On.
  2. : Off.
- Log: Click on Log figure button.
  1. : Off
  2. : on
- Save: After completed this model setting, please click on Save.
- Click on IDP Advanced Settings link, you will see a view as below figure. On the other hand, click on IDP Basic Setting to get back previous step. Setting your IDP function, and then do not forget to click on Save. In addition, click rectangular form if you want to see list class name. (Figure 6-1. 2)

[11] IDS = Intrusion Detection System
[12] IPS = Intrusion Prevention System

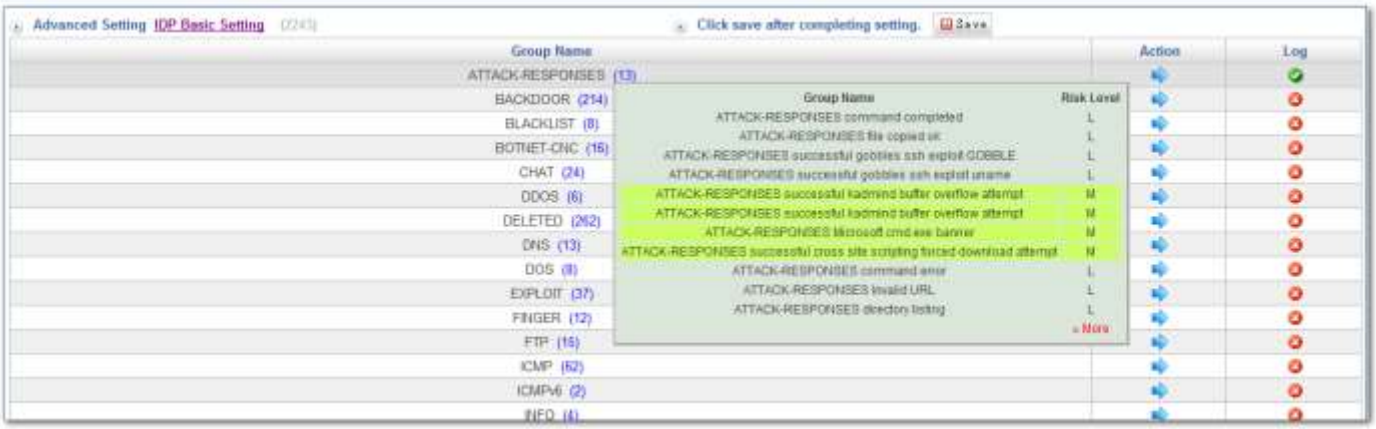


Figure 6-1. 2 IDP Advanced Setting

■ Click on » More to see more detail risk group name. (Figure 6-1. 3)

Group Name	Risk Level
ATTACK-RESPONSES command completed	L
ATTACK-RESPONSES file copied ok	L
ATTACK-RESPONSES successful gobbles ssh exploit GOBBLE	L
ATTACK-RESPONSES successful gobbles ssh exploit uname	L
ATTACK-RESPONSES successful kadmind buffer overflow attempt	M
ATTACK-RESPONSES successful kadmind buffer overflow attempt	M
ATTACK-RESPONSES Microsoft cmd.exe banner	M
ATTACK-RESPONSES successful cross site scripting forced download attempt	M
ATTACK-RESPONSES command error	L
ATTACK-RESPONSES Invalid URL	L
ATTACK-RESPONSES directory listing	L
ATTACK-RESPONSES index of /cgi-bin/ response	L
ATTACK-RESPONSES rexec username too long response	M

Figure 6-1. 3 Risk Group Name

17. Usually, we set up with WAN to LAN or WAN to DMZ(Figure 6-1. 4)

Figure 6-1. 4 Add IDP policy

6-2 IDP Log

IDP Log Search

■ Select or type information you want to search, and click on Search. (Figure 6-2.1)

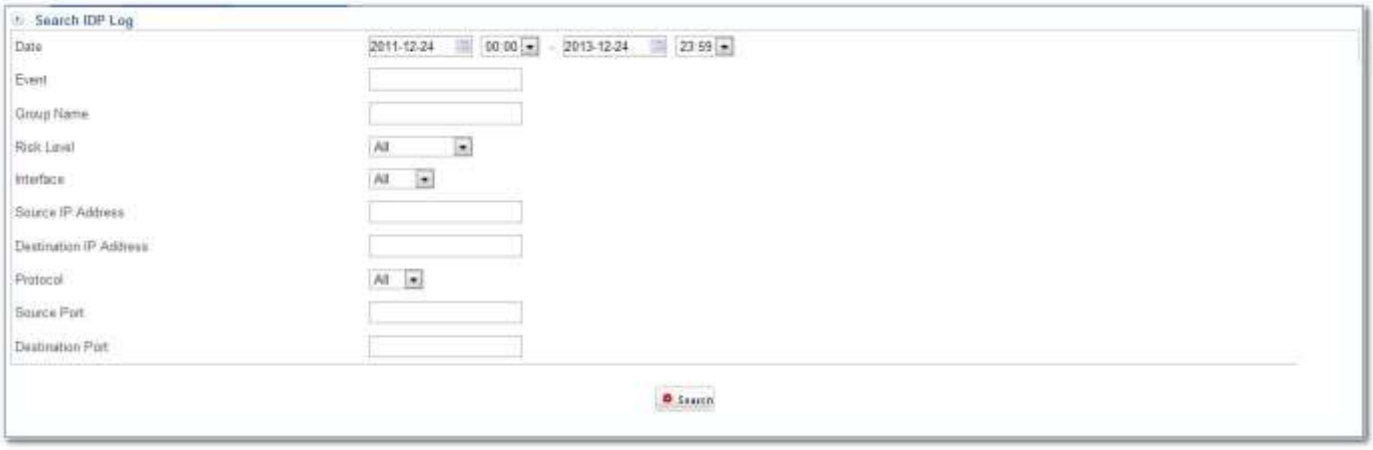


Figure 6-2. 1 IDP Log Search

Search Results

■ After click on Search, you will see logs search result as example below. (Figure 6-2.2)

Date	Event	Group Name	Risk Level	Interface	Source IP Address	Destination IP Address	Protocol	Source Port	Destination Port
2011-11-08 08:35:27	P2P Skype client start up get latest version attempt	P2P	Med	LAN	192.168.99.117	204.9.163.158	TCP	43909	80
2011-10-24 11:09:44	WEB-PHP viewtopic.php access	WEB-PHP	Med	LAN	192.168.99.126	202.39.234.38	TCP	60916	80
2011-10-24 11:09:43	WEB-PHP viewtopic.php access	WEB-PHP	Med	LAN	192.168.99.126	202.39.234.38	TCP	60917	80
2011-10-24 11:09:43	WEB-PHP viewtopic.php access	WEB-PHP	Med	LAN	192.168.99.126	202.39.234.38	TCP	60917	80
2011-10-24 11:09:43	WEB-PHP viewtopic.php access	WEB-PHP	Med	LAN	192.168.99.126	118.215.191.139	TCP	60921	80
2011-10-24 11:09:43	WEB-PHP viewtopic.php access	WEB-PHP	Med	LAN	192.168.99.126	202.39.234.38	TCP	60915	80
2011-10-24 11:09:43	WEB-PHP viewtopic.php access	WEB-PHP	Med	LAN	192.168.99.126	202.39.234.38	TCP	60916	80
2011-10-24 11:09:43	WEB-PHP viewtopic.php access	WEB-PHP	Med	LAN	192.168.99.126	202.39.234.38	TCP	60916	80
2011-10-24 11:09:07	WEB-PHP viewtopic.php access	WEB-PHP	Med	LAN	192.168.99.126	74.125.71.155	TCP	60889	80
2011-10-24 11:09:07	WEB-PHP viewtopic.php access	WEB-PHP	Med	LAN	192.168.99.126	202.39.234.38	TCP	60880	80
2011-10-24 11:09:06	WEB-PHP viewtopic.php access	WEB-PHP	Med	LAN	192.168.99.126	202.39.234.38	TCP	60876	80
2011-10-24 11:09:06	WEB-PHP viewtopic.php access	WEB-PHP	Med	LAN	192.168.99.126	202.39.234.38	TCP	60880	80
2011-10-24 11:08:27	WEB-PHP viewtopic.php access	WEB-PHP	Med	LAN	192.168.99.126	74.125.71.155	TCP	60811	80
2011-10-24 11:08:26	WEB-PHP viewtopic.php access	WEB-PHP	Med	LAN	192.168.99.126	202.39.234.38	TCP	60868	80
2011-10-24 11:08:26	WEB-PHP viewtopic.php access	WEB-PHP	Med	LAN	192.168.99.126	74.125.71.155	TCP	60811	80
2011-10-24 11:08:26	WEB-PHP viewtopic.php access	WEB-PHP	Med	LAN	192.168.99.126	202.39.234.38	TCP	60867	80

Figure 6-2. 2 IDP Log Search Results

Chapter 7：SSL VPN

Since the Internet is in widespread use these days, the demand for secure remote connections is increasing. To meet this demand, using SSL VPN is the best solution. Using SSL VPN and just a standard browser, clients can transfer data securely by utilizing its SSL security protocol, eliminating the need to install any software or hardware.

- An SSL VPN (Secure Sockets Layer virtual private network) is a form of VPN that can be used with a standard Web browser. In contrast to the traditional Internet Protocol Security (IPsec) VPN, an SSL VPN does not require the installation of specialized client software on the end user's computer. It's used to give remote users with access to Web applications, client/server applications and internal network connections. A virtual private network (VPN) provides a secure communications mechanism for data and other information transmitted between two endpoints. An SSL VPN consists of one or more VPN devices to which the user connects by using his Web browser. The traffic between the Web browser and the SSL VPN device is encrypted with the SSL protocol or its successor, the Transport Layer Security (TLS) Protocol.
- An SSL VPN offers versatility, ease of use and granular control for a range of users on a variety of computers, accessing resources from many locations. There are two major types of SSL VPNs:
  1. SSL Portal VPN: This type of SSL VPN allows for a single SSL connection to a Web site so the end user can securely access multiple network services. The site is called a portal because it is one door (a single page) that leads to many other resources. The remote user accesses the SSL VPN gateway using any modern Web browser, identifies himself or she to the gateway using an authentication method supported by the gateway and is then presented with a Web page that acts as the portal to the other services.
  2. SSL Tunnel VPN: This type of SSL VPN allows a Web browser to securely access multiple network services, including applications and protocols that are not Web-based, through a tunnel that is running under SSL. SSL tunnel VPNs require that the Web browser be able to handle active content, which allows them to provide functionality that is not accessible to SSL portal VPNs.

7-1 SSL VPN Setting

In the SSL VPN Settings section you can enable the following lists：

SSL VPN Setup

Users have to click on **Modify the Server Setting** link, to modify SSL VPN settings. In addition, users must select "Start" because default setting is Stop. (Figure 7-1.1)

Note: System will cancel all certificates after modification (except service status). Please Re-generate certificate and download again.

- Service Status: Select Start to on this function, on the other hand, Stop to off this function.

  Note: It will take a few seconds to start, please be patient.
- Local Interface:
  1. Default
  2. Custom
  3. WAN 1
  4. WAN 2
- Local Port: Default setting is 387.
- Max concurrent connections: (Range: 20~256).
- Client IP Range: Client IP ranges need different with LAN, DMZ interface.
- DNS Server 1: The IP address of the DNS server used for the bulk of DNS lookups.
- DNS Server 2: The IP address of the backup DNS server, used when the Primary DNS Server is unreachable
- WINS Server 1: Windows Internet Name Service (WINS) is Microsoft's implementation of NetBIOS Name Service (NBNS), a name server and service for NetBIOS computer names.
- WINS Server 2: All WINS clients should be configured to use a primary WINS server and a different secondary WINS server. The secondary would normally be the hub server.
- Certificate Settings: Enter your computer certificate information for SSL VPN users.
- Do not forget to clink on Save to start SSL VPN.

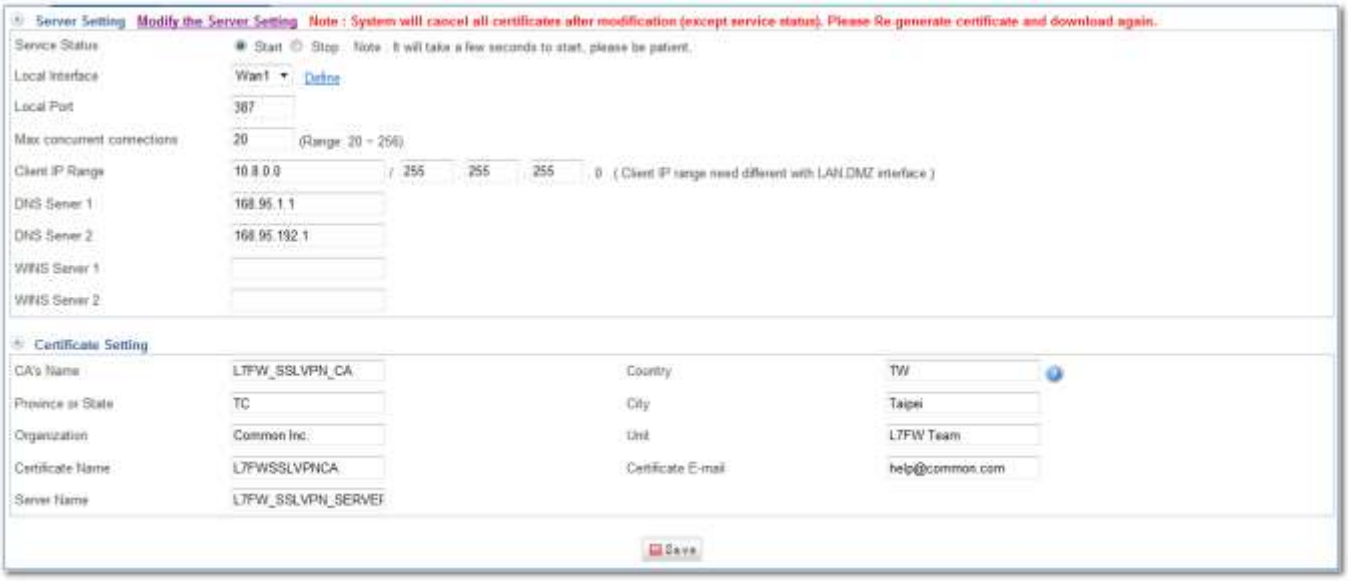


Figure 7-1. 1 SSL VPN Setting

SSL Client List

Please create an account in 4-9 Objects > Authentication > Local User. (Figure 7-1.2)

Figure 7-1. 2 Create Authentication account

Figure 7-1. 3 Authentication User List

Then, select Objects > Authentication > User Group. Click on Add to create a new Authentication User Group. (Figure 7-1.4)

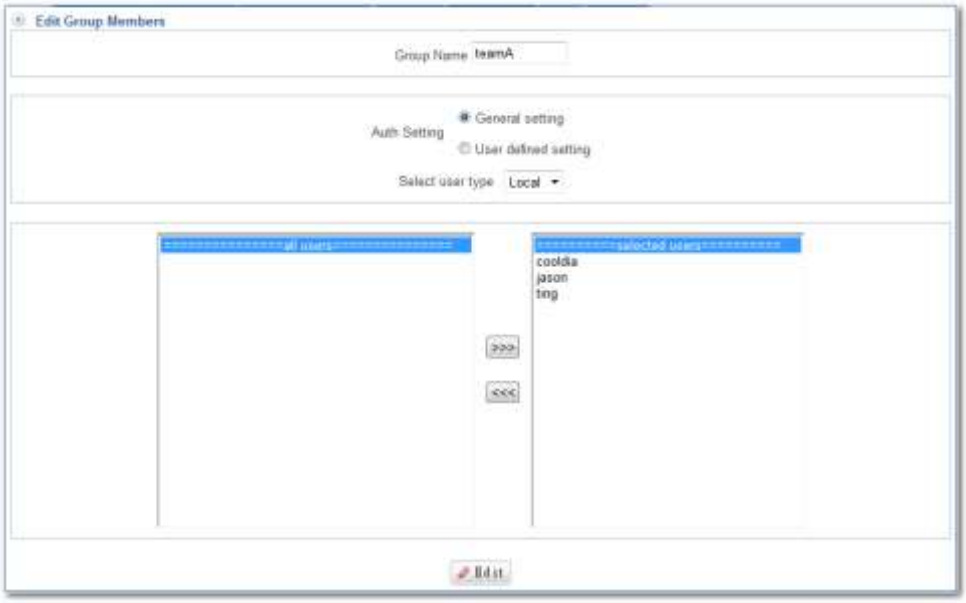


Figure 7-1. 4 Local Users

Setting User Group with Local Users mode completed. In addition, click on Add to create a new sub-content, Edit to modify contents, or Del to cancel list. (Figure 7-1.5)

Figure 7-1. 5 Setting user group with Local Users mode completed

Then, go on SSL VPN > SSL VPN Setting > SSL Client List. Please click on Add to create a new certification SSL VPN Group. (Figure 7-1.6) (Figure 7-1.7)

Figure 7-1. 6 New Certification Group

Figure 7-1. 7 Setting SSL VPN Client with Authentication Local Users completed

IT networking Administrator can click on  to see SSL VPN clinet status. (Figure 7-1.8)

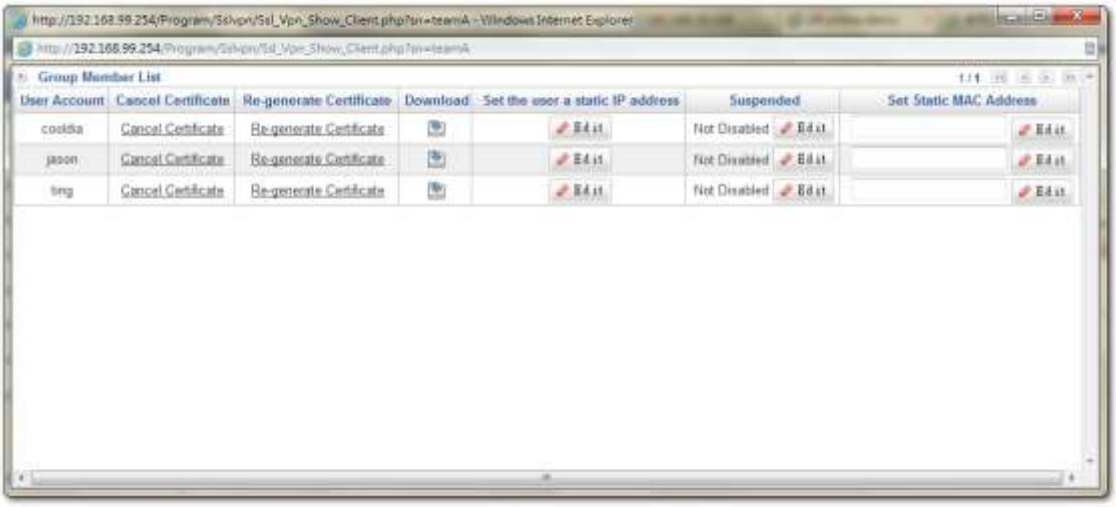


Figure 7-1. 8 SSL VPN clinet status

User should download generate certificate into their computer, laptop, or iPad by using **https:// [Wan IP Address or Domain] : [HTTPS Port] /sslvpn.php**

18. For example, https://111.252.70.234:443/sslvpn.php(Figure 7-1.9)

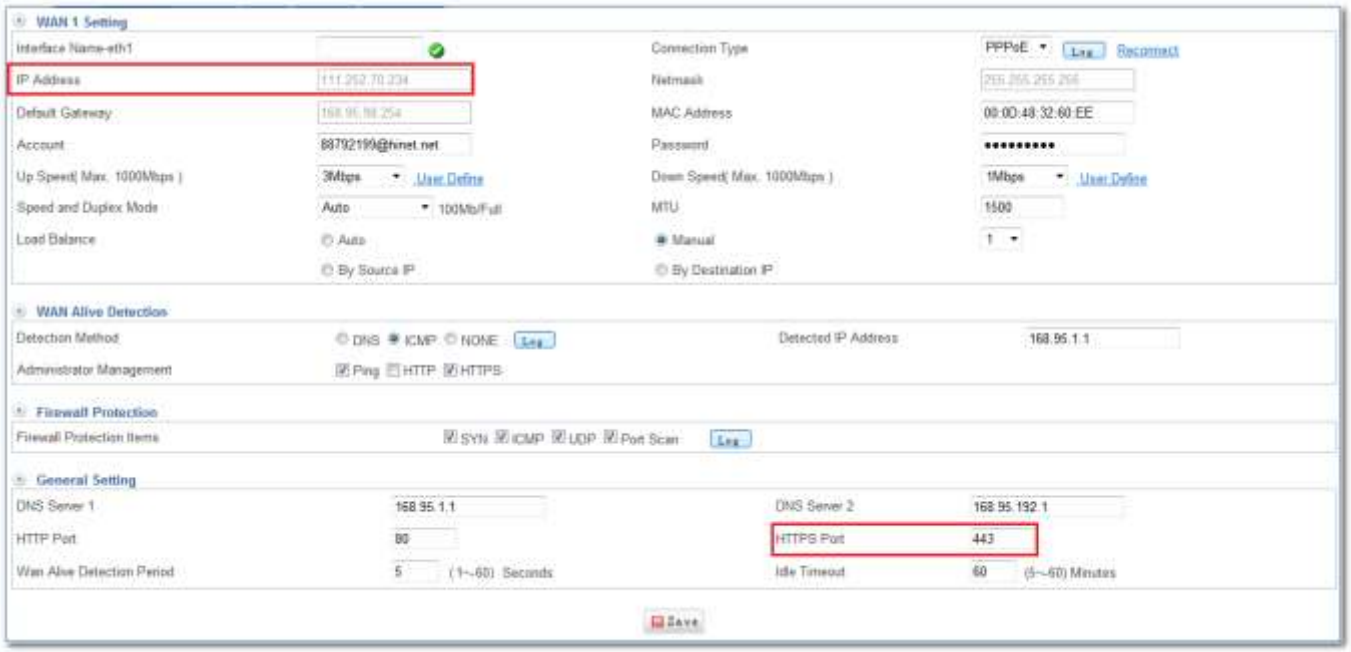


Figure 7-1. 9 check you interface IP and HTTPS Port

Enter https://111.252.70.234:443/sslvpn.php in your browser, and then enter your user account and user password. (Figure 7-1.10)

Figure 7-1. 10 Try to login.

Download generate certificate into their computer, laptop, or iPad. (Figure 7-1.11)

Figure 7-1. 11 Download generate certificate

Open zip file sslvpn_gui_V1.2_ting.zip (Figure 7-1.12), or else update your driver that choose tap-win32 or tap-win64.

Figure 7-1. 12 sslvpn gui

Then, click on , and enter your username and password. (Figure 7-1.13)

Figure 7-1. 13 SSL VPN Connection (Client)

7-2 SSL VPN Log

In this section you can enable the following lists:

SSL Client On-Line Log

- Connection refused to record start: Select Start to on this function, on the other hand, select Stop to off this function. In addition, you can click on Log to see SSL VPN logs. (Figure 7-2.1)

Figure 7-2. 1 SSL Client On-Line Log

7-3 VPN Policy

This section is the same as 8-4 VPN Policy. In this section you can enable the following lists:
SSL VPN on internal control and external control through the SSL VPN connection points connected to internal network, the protocol, Service group port, QoS bandwidth and Schedule, Packet tracing, and Traffic Analysis. Select SSL VPN > VPN Policy > VPN to Internal or Internal to VPN. Click on Add to create a new VPN policy. VPN's policy as follows, policies started from the priority1, will be the implementation of eligible project. If you want to ban non-control information into the internal network, will need to last a total of all the packets into the internal prohibited.

- Policy Name: Enter any word for recognition.
- Source Address and Destination: Source Address (source network) and Destination Address (the destination network) are for the observation points, connect one end of the active source network address, be connected to one end of the network address for the purpose of, apart from the policy choices, users can also directly enter the IP address and MAC address.
  1. Source IP address: VPN_Any will representative of the external section of all VPN tunnels, either with IPSec , PPTP set up Site to Site or the establishment of a single PPTP Server, dial-up account, are in line with the conditions. The default IP address of the PPTP server will also be included in the default source IP address.
  2. The destination IP Address: Inside_Any will representative of the external section of all VPN tunnels, either with IPSec , PPTP set up Site to Site or the establishment of a single PPTP Server, dial-up account, are in line with the conditions. The demand for network administrators can allow or deny specific VPN access other end of the incoming IP address, communication services and even time. The default access control rule is when the VPN is established, both materials are free to communicate with each other to exchange, unless prohibited it from incoming VPN controls.
- Action: It offers two movements.
  1. ACCEPT means any meet the Policy of the packet will be released.
  2. DROP means discarded.
- Protocol: The protocol used for communication between two devices. TCP and UDP are the two most frequently seen protocols among others.
- Service group Port or Group: With service groups, the administrator in setting policy can simplify many processes. For example, there are ten different IP addresses on the server can access five different services, such as HTTP, FTP, SMTP, POP3, and TELNET. If you do not use the service

group functions , need to develop a total of 10x5=50 policies, but use the service group name applied to the service option on , you only need a policy can achieve the function of 50.

- QoS: Select Objects > QoS. Then, the VPN policy set the maxi bandwidth and rate bandwidth (Bandwidth is consistent with the policy of the user to share).
- Schedule: Select Objects > Schedule. Then, set your schedule time.
- Packet Tracing: Select Packet tracing tick box to start function, all records of a VPN tunnel through which packets can view it.
- Traffic Analysis: Select Traffic Analysis tick box to start function.
- NAT

VPN to Internal

Figure 7-3. 1 VPN to Internal

Internal to VPN

Figure 7-3. 2 Internal to VPN

7-4 SSL From your Android phone

Securely Connect Your Android Smartphone via SSLVPN.

ShareTech roll out full SSL VPN support for Android Smartphones for more secure remote access to UTM and other corporate applications because of the Android system support and flexibility.

When you're out on the road with nothing but your phone and desperately need access to a document that's stored on your computer at home or at work, what do you do? Because a modern smartphone is really just a small computer, you can securely connect to your home LAN or company network over a SSL VPN connection.

19. Let's take a look at how you can do this with popular Android phones.

1. Add an authentication account(Figure 7-4.1)

Objects >Authentication > Local User

Figure 7-4. 1 Add an authentication account

2. Objects > Authentication > Local User (Figure 7-4.2)

Figure 7-4. 2 User List

3. Add an authentication group(Figure 7-4.3) (Figure 7-4.4)

Objects > Authentication > User Group

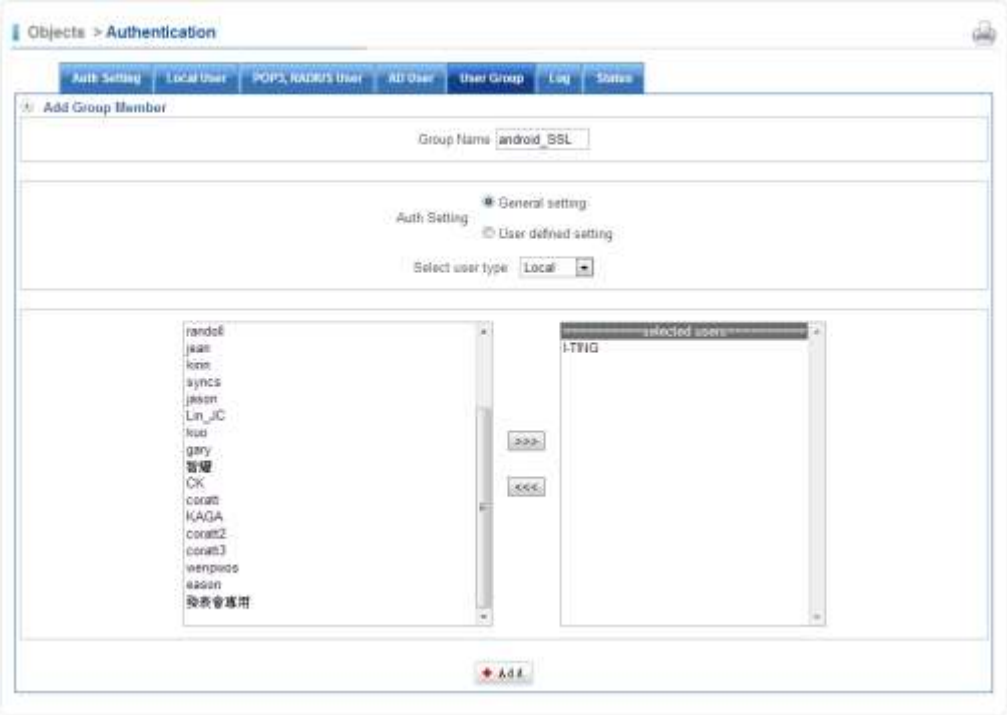


Figure 7-4. 3 add Group Member

Figure 7-4. 4 Group List

4. Add a New Certification Group(Figure 7-4.5) (Figure 7-4.6)

SSL VPN > SSL VPN Setting > SSL Client List

Figure 7-4. 5 Add a New Certification Group

SSL VPN > SSL VPN Setting > SSL Client List

Figure 7-4. 6 SSL Client List

5. Start SSL VPN

SSL VPN > SSL VPN Setting > SSL VPN Setup

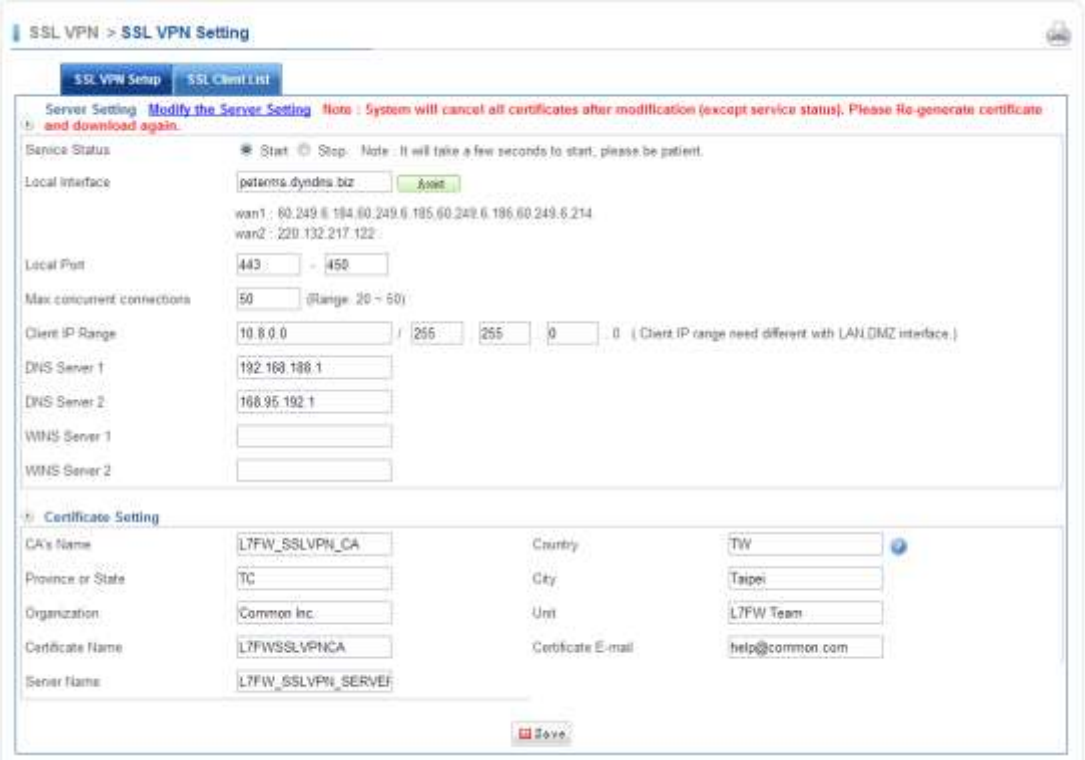
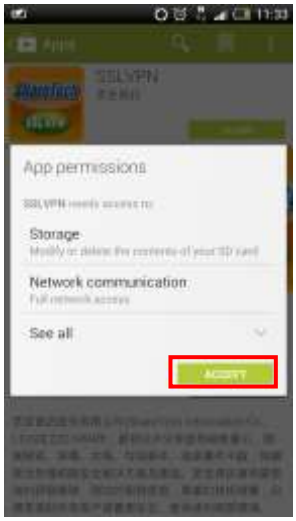


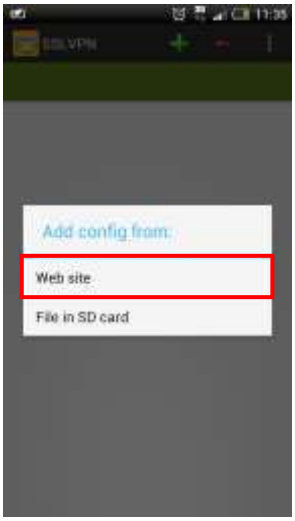
Figure 7-4. 7 Start SSL VPN

20. Configure Your Android Device

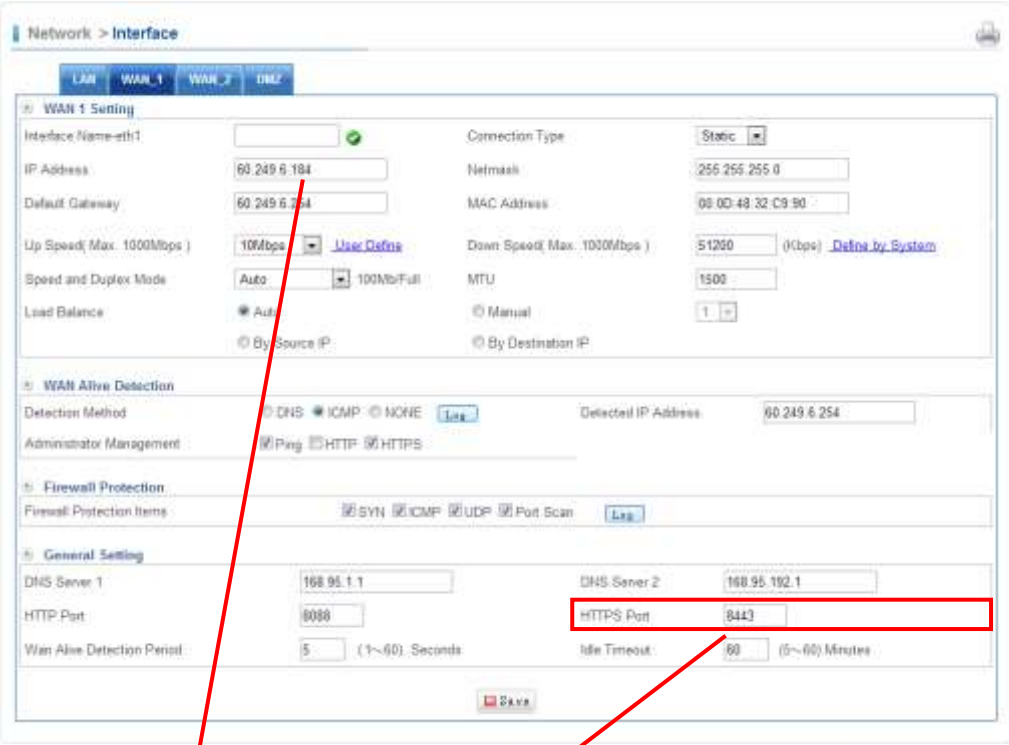
6. Download "ShareTech SSL VPN, " and Install it.

7. Add a new SSL VPN connection.

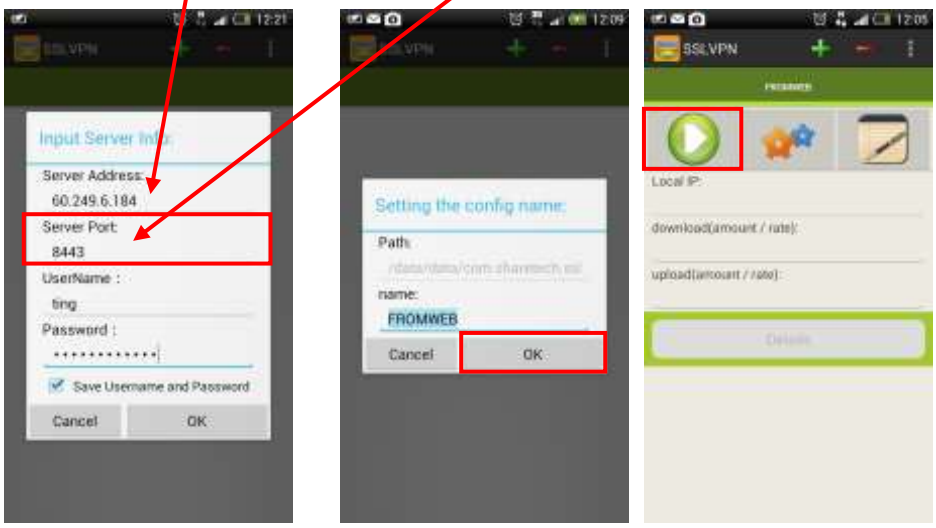




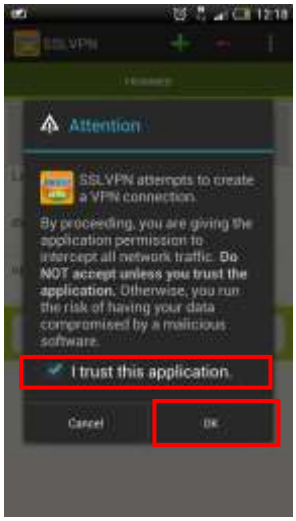
Network > Interface > HTTPS Port

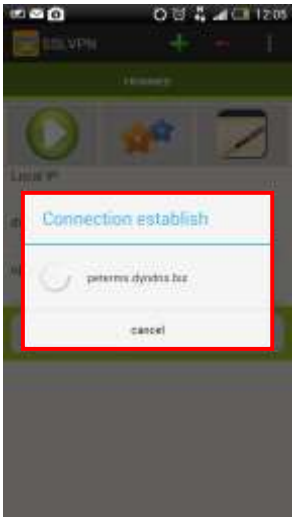


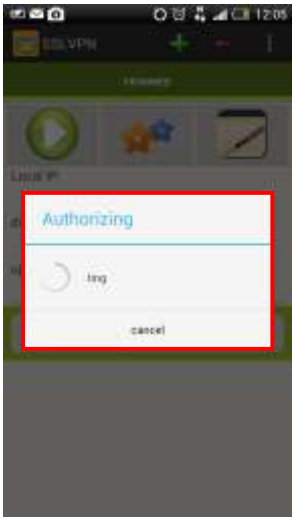
8. Enter Server Information



9. Connection establish and Authorizing



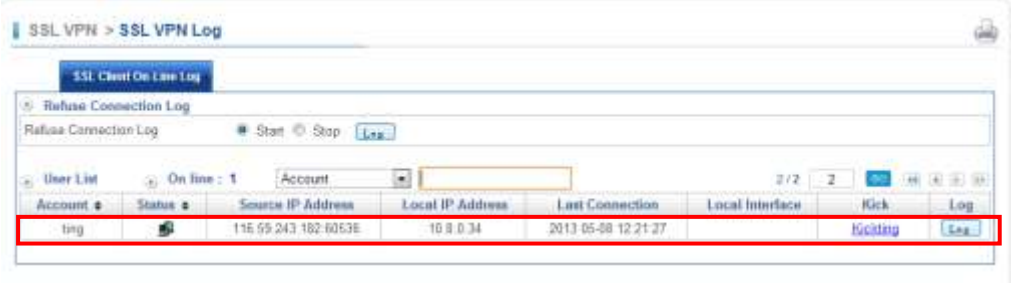




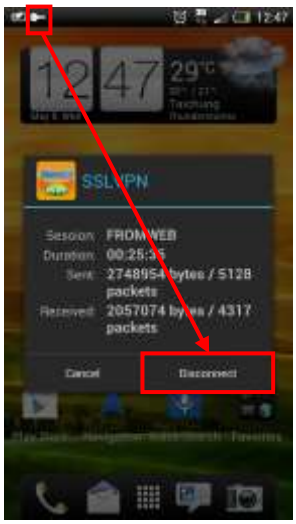
10. Address of information message

11. Your smartphone is now successfully connected to the SSL VPN

12. SSL VPN Log



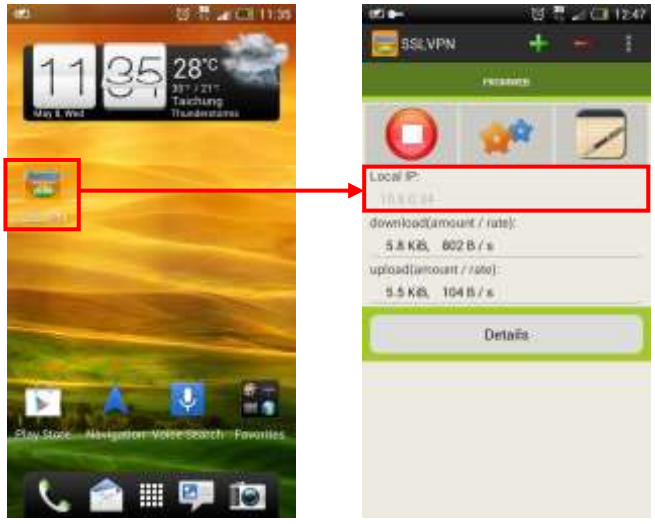
13. How to disconnect SSL VPN?



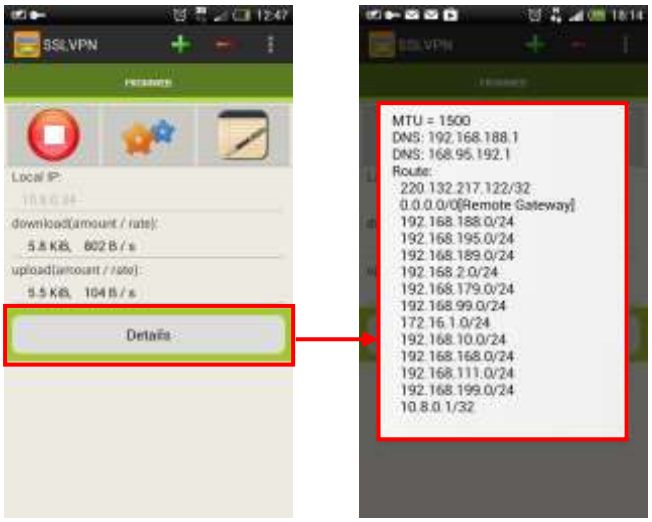
Other Information

Using a SSL VPN to connect your smartphone to your home or work network can expand the usability of your phone and help you to be productive no matter where you are.

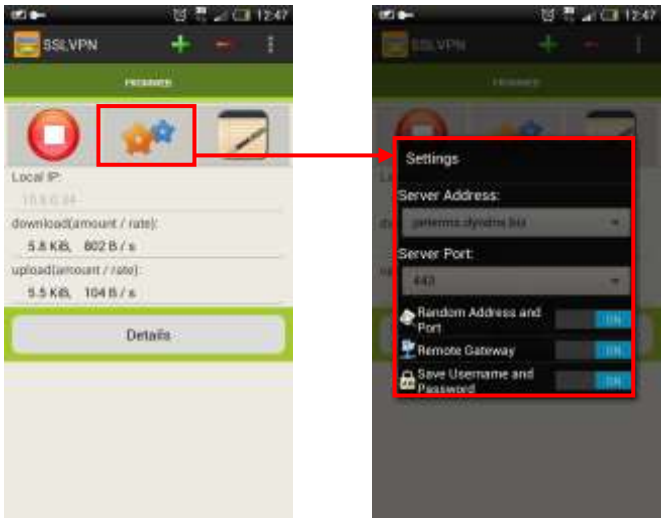
14. What is your internal IP?



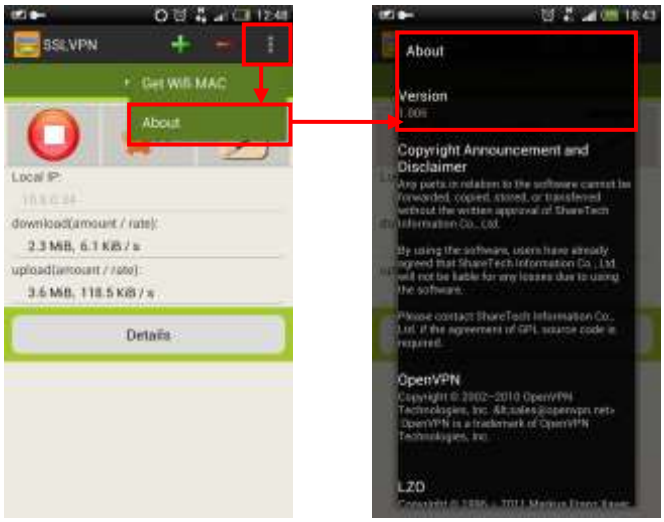
15. What are Details? Route Information



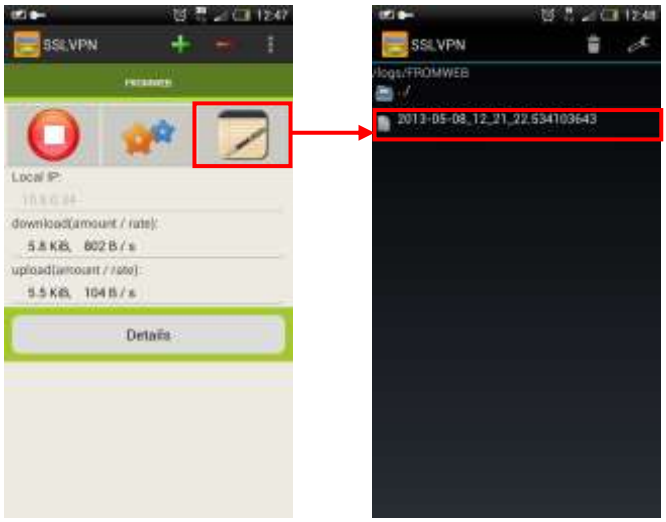
16. Setting



17. SSL Version



18. SSL VPN Connection Logs



Chapter 8：VPN

To obtain a private and secure network link, the UR is capable of establishing VPN connections. When used in combination with remote client authentication, it links the business' remote sites and users, conveniently providing the enterprise with an encrypted network communication method. By allowing the enterprise to utilize the Internet as a means of transferring data across the network, it forms one of the most effective and secures options for enterprises to adopt in comparison to other methods. In the VPN chapter you can enable the following lists:

VPN connections use either Point-to-Point Tunneling Protocol (PPTP) or Layer Two Tunneling Protocol/Internet Protocol security (L2TP/IPSec) over an intermediate network, such as the Internet. By using the Internet as a connection medium, VPN saves the cost of long-distance phone service and hardware costs associated with using dial-up or leased line connections. A VPN solution includes advanced security technologies such as data encryption, authentication, authorization, and Network Access Quarantine Control.

- 8-1 IPSec Tunnel
- 8-2 PPTP Server
- 8-3 PPTP Client
- 8-4 VPN Policy

8-1 IPSec Tunnel

IPSec[13] is a generic standardized VPN solution. IPSec must be implemented in the IP stack which is part of the kernel. Since IPSec is a standardized protocol it is compatible to most vendors that implement IPSec. It allows users to have an encrypted network session by standard IKE[14]. We strongly encourage you to use IPSec only if you need to because of interoperability purposes.When IPSec lifetime is specified, the device can randomly refresh and identify forged IKE's during the IPSec lifetime. In this section you can enable the following lists:

Select VPN > IPSec Tunnel > IPSec Tunnel. Click on + Add button to create a new IPSec Tunnel.

Add IPSec Tunnel

Select VPN > IPSec Tunnel > IPSec Tunnel.

- Enabled: Select it to start the connection.
- IPSec Tunnel Name: Enter any words for recognition.
- Interface: This is only available for host-to-host connections and specifies to which interface the host is connecting.
  1. WAN 1
  2. WAN 2
- Remote IP Address: The IP or fully qualified domain name of the remote host.
  1. IP Address or Domain: Enter an IP Address or Domain.
  2. Dynamic: Follow Dynamic IP address.
- Local Subnet: The local subnet in CIDR notation. For instance, "*192.168.15.0/24*"
- Remote Subnet: This is only available for net-to-net connections and specifies the remote subnet in CIDR notation. For instance, "*192.168.16.0/24*"

[13] IPSec = IP Security
[14] IKE = Internet Key Exchange

- Connection Type: There are two types.
  1. Main
  2. Aggressive
- Preshare Key: Enter a pass phrase to be used to authenticate the other side of the tunnel.
- ISAKMP[15]: It provides the way to create the SA[16] between two PCs. The SA can access the encoding between two PCs, and the IT administrator can assign of which key size or Preshare Key and algorithm to use. The SA comes in many connection ways.
  1. AES[17]: All using a 128-bit, 192-bit and 256-bit key. AES is a commonly seen and adopted nowadays.
  2. 3DES[18]: Triple DES is a block cipher formed from the DES[19] cipher by using it three times. It can achieve an algorithm up to 168 bits.
  3. SHA1: The SHA1 is a revision of SHA[20]. It has improved the shortcomings of SHA. By producing summary hash values, it can achieve an algorithm up to 160 bits.
  4. MD5[21] Algorithm: MD5 processes a variable-length message into a fixed–length output of 128 bits.
  5. DH Group: When the encryption technique is aes, it can be choice2, 5, 14, 15, 16, 17, 18, but the encryption technique is 3des, only can choice 2, 5.
  6. Auto Pairing
- Local ID: An ID for the local host of the connection
- Remote ID: An ID for the remote host of this connection
- IKE SA Lifetime: You can specify how long IKE packets are valid.
- IPSec: It offers aes, 3des, sha1, and md5.
  1. AES; All using a 128-bit, 192-bit and 256-bit key. AES is a commonly seen and adopted nowadays.
  2. 3DES: Triple DES is a block cipher formed from the DES cipher by using it three times. It can achieve an algorithm up to 168 bits.
  3. SHA1: The SHA1 is a revision of SHA. It has improved the shortcomings of SHA. By producing summary hash values, it can achieve an algorithm up to 160 bits.
  4. MD5 Algorithm: MD5 processes a variable-length message into a fixed–length output of 128 bits.

---

[15] ISAKMP = Internet Security Association Key Management Protocol
[16] SA = Security Association
[17] AES = Advanced Encryption Standard
[18] 3DES = Triple-DES
[19] DES = Data Encryption Standard
[20] SHA = Secure Hash Algorithm
[21] MD5 = Message Digest Algorithm 5

5. Auto Pairing

- Perfect Forward Secrecy(PFS)[22]: Set Yes to start the function. DH Group, when the encryption technique is aes, it can be choice2, 5, 14, 15, 16, 17, 18, but the encryption technique is 3des, only can choice 2, 5.
- IPSec SA Lifetime: Set to 1~3 hours. Default setting is 3 hours.
- Dead Peer Detection: When startin DPD function, when VPN detects opposite party reaction time, hold stand for the system will retain IPSec SA, "Clear" stand for the tunnel will clean away and waits for the new sessions, "Restart" will delete the IPSec SA and reset VPN tunnel.
- Drop SMB Protocol: After the closure Network Neighborhood will be prevented.

21. There is an example of utilizes two UR devices. Assume that A Company 192.168.168.51 wants to create a VPN connection with B Company 192.168.99.21 in order to access files. (Figure 8-1.1) (Figure 8-1.2)

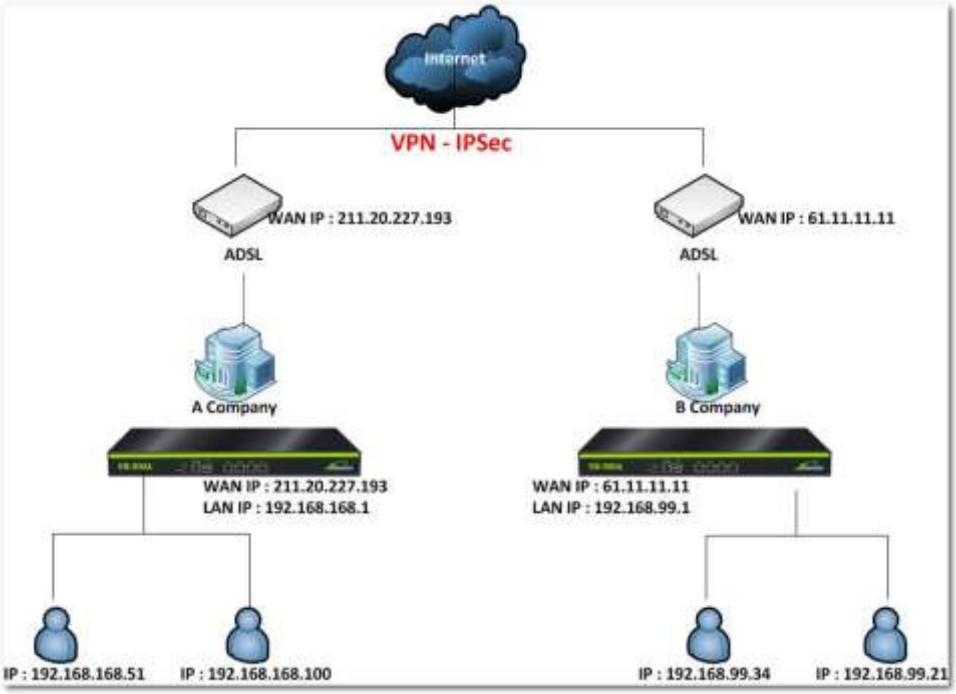


Figure 8-1. 1 example setting

[22] PFS = Perfect Forward Secrecy

For A company: Select VPN > IPSec Tunnel > Add VPN Tunnel. Its WAN IP is 211.20.227.193, and LAN subnet is 192.168.168.0/24. Default gateway for the A company LAN IP 192.168.168.1.

Step 1. VPN Tunnel Name: Enter "*VPN_B*" in the field.

Step 2. Interface: Select "*WAN 1.*"(Suggest using static IP)

Step 3. Local Subnet: Enter "*192.168.168.0 255.255.255.0 (/24)*"

Step 4. Remote Subnet: Enter "*192.168.99.0 255.255.255.0 (/24)*"

Step 5. Preshare Key: Enter numbers for B Company. Should be the same with B Company.(The maximum length of Preshare key is 103 characters.)

Step 6. ISAKMP: Select "*aes*" and "*sha1*," and set "*DH Group*".

Step 7. Local ID: Default is use WAN IP Address as ID, administrator also can use domain as ID. For example "*@1.1.1.1"* or "*@abc.com"*

Step 8. Remote ID: The use way is the same with Local ID.

Step 9. IKE SA Lifetime: The default is 3 hours. After IKE establishment surpasses the system set time, will produce new IKE.

Step 10. IPSec: Select "aes" and"“md5" for IPSec. And select Auto Pairing to start. To start Auto Pairing, the system all calculation combination will converge in the rule, If UTM as SERVE，Will discover the same combination automatically on behalf of the system with the far-end segment.

Step 11. Perfect Forward Secrecy (PFS): Set to Yes. (The default setting is not work), and select DH Group.

Step 12. IPSec SA Lifetime: Set to 1~3 hours. The default setting is 3 hours.

Step 13. Dead Peer Detection: Set up the detection time of DPD, the DPD detection’s gap is 30 seconds, over 300 seconds to think that is the broken line.

Step 14. Drop SMB Protocol: After the closure Network Neighborhood will be prevented.

Step 15. Settings completed.

For B Company: B Company setting steps is similar to A Company setting.
WAN IP is 61.11.11.11, LAN subnet is 192.168.99.0/24

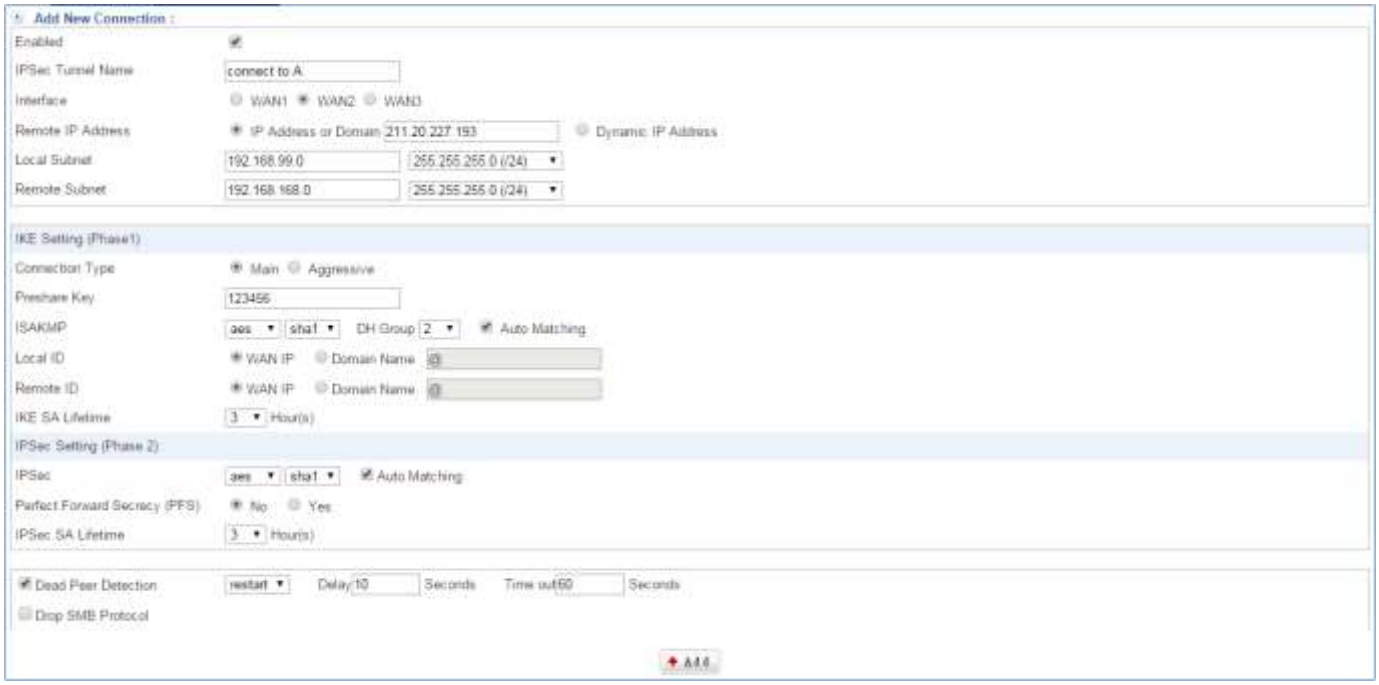


Figure 8-1. 2 How to Add IPSec Tunnel for B company

IPSec Tunnel

Setting IPSec Tunnel completed, and please notices the status. (Figure 8-1.3)

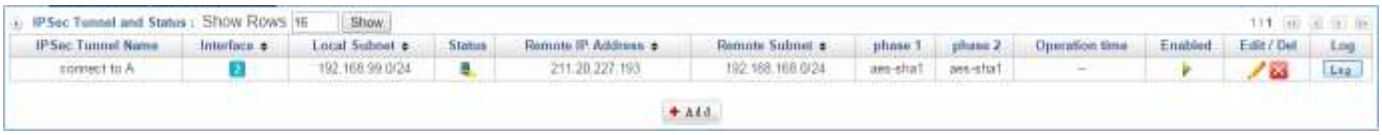


Figure 8-1. 3 Setting IPSec Tunnel completed

- VPN and Status：
  1. Interface: At present IPSec VPN use entity interface.
     a. 1: Represent WAN 1
     b. 2: Represent WAN 2
  2. Status:
     a. : The VPN is not work
     b. : The VPN is on work
  3. Enabled: Control IPSec VPN start and suspension button.

a. : Stand for start

b. : Stand for suspension

4. : Stand for edit the VPN setting

5. Log: This VPN communication record，IPSec VPN channel , if has the communication record with opposite party , select the "Log" will open the new Windows, the data will be according to time sorting, most recent news in last page. (Figure 8-1.4)

Comment : connect to A

TIME	NUMBER	EVENT
2015-05-19 09:28:53		deleting connection
2015-05-19 09:28:53		We cannot identify ourselves with either end of this connection
2015-05-19 09:30:03		deleting connection
2015-05-19 09:30:03		We cannot identify ourselves with either end of this connection
2015-05-19 09:32:02		deleting connection
2015-05-19 09:32:03		We cannot identify ourselves with either end of this connection
2015-05-19 09:34:02		deleting connection
2015-05-19 09:34:02		We cannot identify ourselves with either end of this connection
2015-05-19 09:36:02		deleting connection
2015-05-19 09:36:03		We cannot identify ourselves with either end of this connection
2015-05-19 09:38:02		deleting connection
2015-05-19 09:38:02		We cannot identify ourselves with either end of this connection
2015-05-19 09:40:02		deleting connection

Figure 8-1. 4 IPSec VPN Log

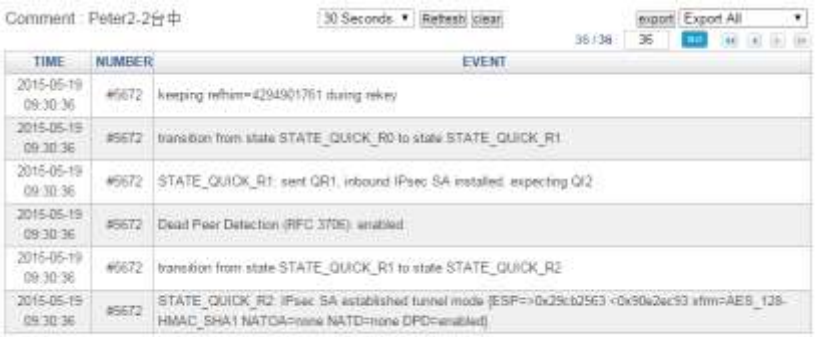
22. You are able to create multiple IPSec VPN(Figure 8-1.5) (Figure 8-1.6)

IPSec Tunnel and Status : Show Rows 16 Show

Tunnel Name	Interface	Local Subnet	Status	Remote IP	Remote Subnet	phase 1	phase 2	Operation time	Enabled	Switch	Edit / Del	Log
	1	192.168.184.0/21		116.231.248.225	192.168.21.0/24	des-md5	des-md5	00:31:59		-		Log
	1	192.168.184.0/21		122.117.136.58	192.168.200.0/24	des-md5	des-md5	15:13:26		-		Log
	1	192.168.188.0/24		60.250.106.211	192.168.100.0/24	3des-md5	3des-md5	00:36:01		-		Log
	1	192.168.196.0/24		60.250.106.211	192.168.100.0/24	3des-md5	3des-md5	00:34:33		-		Log
	1	192.168.188.0/24		220.130.209.67	192.168.1.0/24	des-md5	des-md5	00:11:18		-		Log
	1	192.168.189.0/24		60.250.106.211	192.168.100.0/24	3des-md5	3des-md5	00:28:57		-		Log
	1	192.168.191.0/24		60.250.106.211	192.168.100.0/24	3des-md5	3des-md5	15:11:58		-		Log
	1	192.168.186.0/24		116.231.248.225	192.168.21.0/24	des-md5	des-md5	00:31:59		-		Log
	1	192.168.189.0/24		116.231.248.225	192.168.21.0/24	des-md5	des-md5	00:31:58		-		Log
	1	192.168.186.0/24		123.205.117.19	192.168.202.0/24	aes-sha1	aes-sha1	00:42:59		-		Log
	1	192.168.186.0/24		210.202.56.31	192.168.196.0/24	aes-sha1	aes-sha1	06:55:22		-		Log
	1	192.168.186.0/24		122.117.136.58	192.168.200.0/24	des-md5	des-md5	00:34:31		-		Log
	1	192.168.186.0/24		60.250.106.211	192.168.100.0/24	3des-md5	3des-md5	00:33:13		-		Log
	1	192.168.186.0/24		Dynamic IP	172.16.10.0/24	des-md5	des-md5	-		-		Log
	1	192.168.188.0/24		123.205.117.19	192.168.202.0/24	aes-sha1	aes-sha1	00:05:29		-		Log

Add

Figure 8-1. 5 Multiple IPSec VPN



Comment : Peter2-2台中

TIME	NUMBER	EVENT
2015-05-19 09:30:36	#5672	keeping refhim=4294901761 during rekey
2015-05-19 09:30:36	#5672	transition from state STATE_QUICK_R0 to state STATE_QUICK_R1
2015-05-19 09:30:36	#5672	STATE_QUICK_R1: sent QR1, inbound IPsec SA installed, expecting QI2
2015-05-19 09:30:36	#5672	Dead Peer Detection (RFC 3706): enabled
2015-05-19 09:30:36	#5672	transition from state STATE_QUICK_R1 to state STATE_QUICK_R2
2015-05-19 09:30:36	#5672	STATE_QUICK_R2: IPsec SA established tunnel mode {ESP=>0x25cb2563 <0x90a2ec93 xfrm=AES_128-HMAC_SHA1 NATOA=none NATD=none DPD=enabled}

Figure 8-1. 6 IPSec VPN log

8-2 PPTP Server

This section shows you how to set of VPN-PPTP server.

Uses the IP address and the scope option needs to match the far-end the PPTP server, its goal uses the PPTP channel technology, establishes Site to Site VPN, its function the channel has meaning of the equally good results from different methods with IPSec. In this section you can enable the following lists:

PPTP Server

Starting PPTP Server, Enable the far-end user to be possible to dial using PPTP meets the software with UTM PPTP the server establishment encryption VPN connect. Select VPN > PPTP Server > PPTP Server. (Figure 8-2.1)

- Enabled: Select Enabled tick box to start VPN-PPTP function, but otherwise, it is disable if not select.
- Enable Compression & Encryption: Select Enabled tick box to start compression and encryption, but otherwise, it is disable if not select.
- PPTP User Pass Through Internet: Select tick box to enable user who pass through Internet by VPN-PPTP, but otherwise, it means that PPTP Server is disable.
- Client IP Address Range: The range of IP address for clients using PPTP connection
- The first DNS Server: The IP address of the DNS server used for the bulk of DNS lookups.
- The second DNS Server: The IP address of the backup DNS server, used when the Primary DNS Server is unreachable
- The first WINS Server: When the PPTP clients enter the PPTP Server, assigns for the far-end client WINS Server address.
- The second WINS Server: When the PPTP clients enter the PPTP Server, assigns for the far-end client WINS Server address.
- Click on Save to start PPTP Server.

Figure 8-2. 1 PPTP Server

Add Account

Select VPN > PPTP Server > Add Account. (Figure 8-2.2)

- Enabled: Select Enabled to start this account.
- Account: Enter an account.
- Password: Enter a password.
- Client IP Address Assign: It offers two ways.
  1. Assign By PPTP Server: The UTM will distribute IP address to the VPN-PPTP users automatically.
  2. User Define IP Address: The VPN-PPTP users should use the IP address what you enter..

Figure 8-2. 2 Account Add

How do users create VPN connection in their computer?

Step 1: Create new connection (Figure 8-2.3)

Figure 8-2. 3 create new connection

Step 2: Select VPN connection (Figure 8-2.4)

Figure 8-2. 4 select connect working place by VPN

Step 3: Enter WAN IP address (Figure 8-2.5)

Figure 8-2. 5 Enter WAN IP address

Step 4: Enter your username and password (Figure 8-2.6)

Figure 8-2. 6 Enter username and password

Step 5: Users can check their status in their computer (Figure 8-2.7)

Figure 8-2. 7 check users' computer

Step 6: In addition, user can enter "ipconfig" in cmd (Figure 8-2.8)

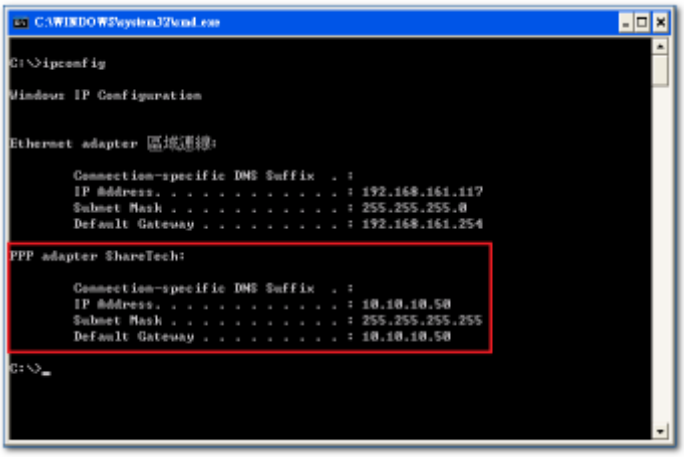


Figure 8-2. 8 ipconfig in cmd

PPTP Account List

Select VPN > PPTP Server > PPTP Account List. It means setting PPTP account completed. (Figure 8-2.9)

- Account: Available VPN-PPTP account
- Status: The symbol and its description used in the VPN connection status.

  1. : It is connecting.

  2. : Disconnected

- Enabled: Click signature again will change to disable.

1. : Enable
2. : Disable

- Edit / Del: Click on the pencil signature to modify contents, and click on another one to delete PPTP account.
  1. : to modify contents
  2. : to delete PPTP account
- Log: Click on Log, it shows the PPTP account connection logs.

Figure 8-2. 9 PPTP Account List

8-3 PPTP Client

In the PPTP Client section you can enable the following lists:

Add PPTP Client

Select VPN > PPTP Client > Add PPTP Client. (Figure 8-3.1)

- Name: The description for PPTP Client
- Account: It displays the name of clients using PPTP to log in to PPTP server.
- Server: Enter a server IP address.
- Remote Mask: The Mask of PPTP Server
- Enabled: Select it to start PPTP Client account.
- Password: It displays the password of clients using PPTP to log in to PPTP server.
- Remote Subnet: PPTP Client enters the IP address of PPTP Server.

Figure 8-3. 1 Add PPTP Client

PPTP Client List

Select VPN > PPTP Client > PPTP Client List. It means setting PPTP Client completed. (Figure 8-3.2)

Figure 8-3. 2 PPTP Client List

8-4 VPN Policy

The intelligence and power behind the Positive Networks VPN service derives from the Positive VPN Policy Manager. The Positive VPN Policy Manager provides the administrator interface that maintains and enforces security policies for all groups and individual users. It is available from an ordinary web browser with a secure login. To create a secure VPN connection, the settings of IPSec Tunnel, PPTP Server or PPTP Client must be set to correlative policies.

The default of VPN Policy do not grant pre-control, as long as the VPN to establish successful, two-way computer can communicate, if only the control of the target was expected through the proposed regulations in the last one against all connections.

The control of the VPN in the past, most were carried out from the policies or is unable to monitor, but ShareTech UTM for the VPN is direct control from the VPN.VPN on internal control and external control through the VPN connection points connected to internal network, the Protocol, Service port, QoS bandwidth and Schedule, Packet tracing, and Traffic Analysis. Select VPN > VPN Policy > VPN to Internal or Internal to VPN. Click on Add to create a new VPN policy. VPN's policy as follows, policies started from the priority1, will be the implementation of eligible project. If you want to ban non-control information into the internal network, will need to last a total of all the packets into the internal prohibited.

- Policy Name: Enter any word for recognition.
- Source Address and Destination: Source Address (source network) and Destination Address (the destination network) are for the observation points, connect one end of the active source network address, be connected to one end of the network address for the purpose of, apart from the policy choices, users can also directly enter the IP address and MAC address.
  1. Source IP address: VPN_Any will representative of the external section of all VPN tunnels, either with IPSec , PPTP set up Site to Site or the establishment of a single PPTP Server, dial-up account, are in line with the conditions. The default IP address of the PPTP server will also be included in the default source IP address.
  2. The destination IP Address: Inside_Any will representative of the external section of all VPN tunnels, either with IPSec , PPTP set up Site to Site or the establishment of a single PPTP Server, dial-up account, are in line with the conditions. The demand for network administrators can allow or deny specific VPN access other end of the incoming IP address, communication services and even time. The default access control rule is when the VPN is established, both materials are free to communicate with each other to exchange, unless prohibited it from incoming VPN controls.

- Action: It offers two movements.
  1. ACCEPT means any meet the Policy of the packet will be released.
  2. DROP means discarded.
- Protocol: The protocol used for communication between two devices. TCP and UDP are the two most frequently seen protocols among others.
- Service group Port or Group: With service groups, the administrator in setting policy can simplify many processes. For example, there are ten different IP addresses on the server can access five different services, such as HTTP, FTP, SMTP, POP3, and TELNET. If you do not use the service group functions , need to develop a total of 10x5=50 policies, but use the service group name applied to the service option on , you only need a policy can achieve the function of 50.
- QoS: Select Objects > QoS. Then, the VPN policy set the maxi bandwidth and rate bandwidth (Bandwidth is consistent with the policy of the user to share).
- Schedule: Select Objects > Schedule. Then, set your schedule time.
- Packet Tracing: Select Packet tracing tick box to start function, all records of a VPN tunnel through which packets can view it.
- Traffic Analysis: Select Traffic Analysis tick box to start function.
- NAT

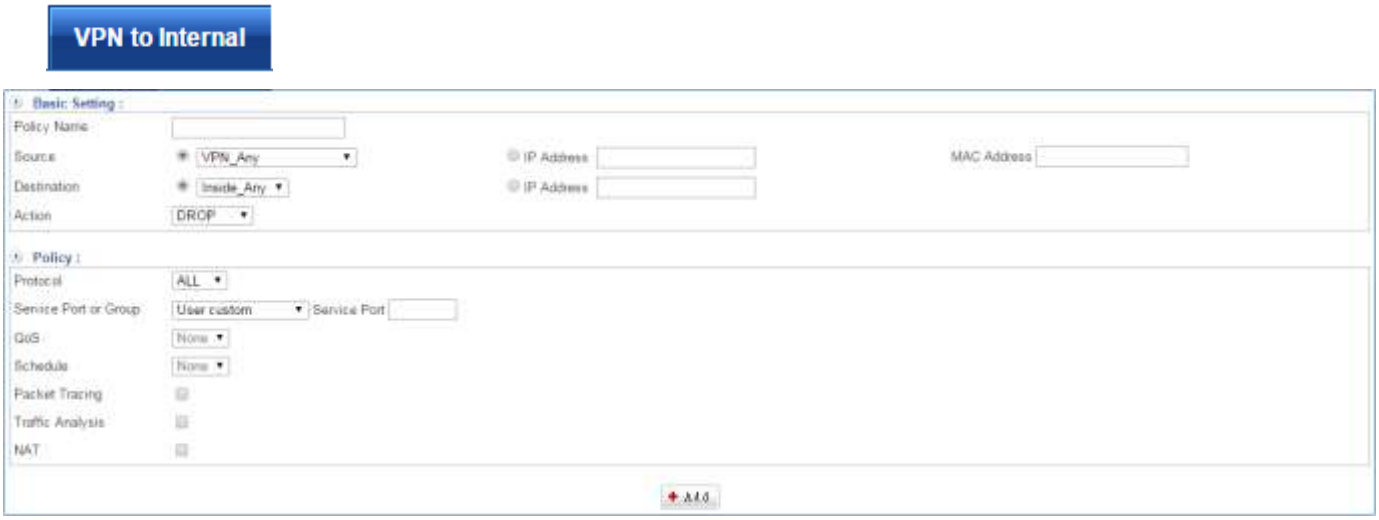


Figure 8-4. 1 VPN to Internal

Internal to VPN

Figure 8-4. 2 Internal to VPN

Chapter 9：Tools

In the Tools chapter you can enable the following lists:

- 9-1 Connection Test
- 9-2 Packet Capture

9-1 Connection Test

In the Connection Test Chapter, UTM provides Ping, Trace Route, DNS Query, Port Scan, IP Route, Interface Information and Wake up utilities to help diagnose network issues with particular external nodes.

Ping

It is an ICMP protocol. Most of people usually use ping to diagnostic Internet between self and other people when Internet disconnected. Select Tools > Connection Test > Ping. Enter some information in the field, and click on OK. Then, you will see Ping Result. (Figure 9-1.1)

- Target IP or Domain: Enter the Target IP or Domain name in the field.
- Package Size: It configures the size of each packet. Default setting is 32 Bytes.
- Times: It configures the quantity of packets to send out. Default setting is 4.
- Wait Time: It specifies the duration to wait between successive pings. Default setting is 1 second.
- Using Interface & IP: Select an interface.

Figure 9-1. 1 Ping

Trace Route

Traceroute command can be used by the SG-100N to send out packets to a specific address to diagnose the quality of the traversed network. Select Tools > Connection Test > Trace Route. Enter some information in the field, and click on OK. Then, you will see Traceroute Result. (Figure 9-1.2)

- Target IP or Domain: Enter the destination address for the packets.
- Package Size: Configure the size of each packet. Default setting is 40 Bytes.
- Max. Next Hop: Enter the maximum number of hops. Default setting is 30 Nodes.
- Wait Time: Specify the duration to wait between successive pings. Default setting is 2 seconds.
- Tracing Methods: There are ICMP, UDP, and TCP.

- Source Interface：Select the interface that the packets will originate from.

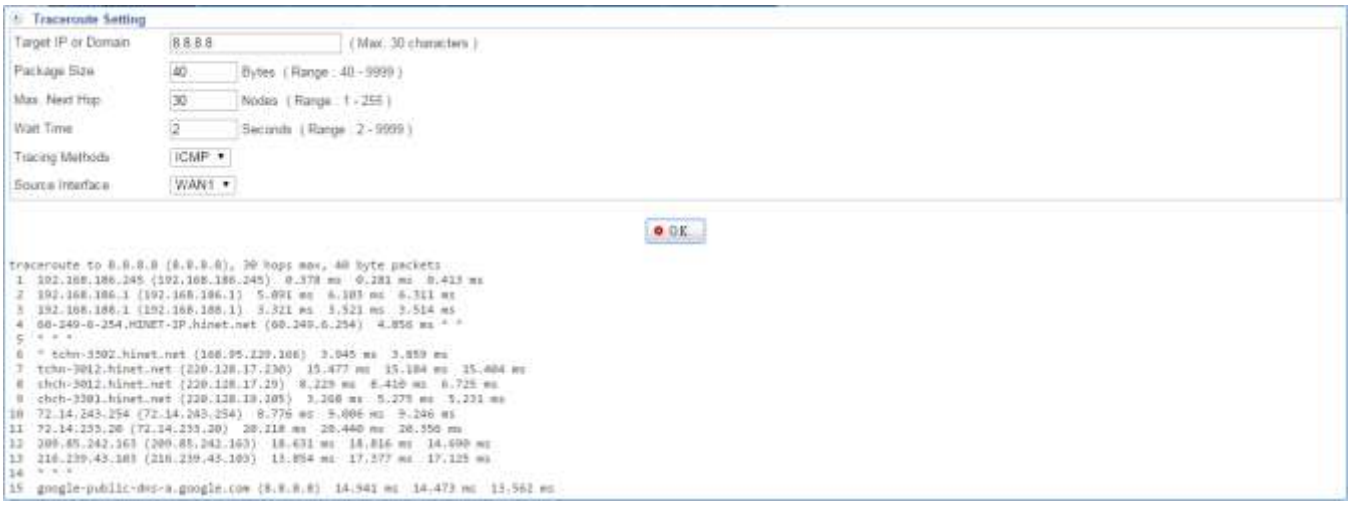


Figure 9-1. 2 Trace Route

DNS Query

Inquires the DNS detailed material, at present may inquire the datas of ANY, SOA, NS, A Record, MX, CNAME, PTR, may user specific DNS server achievement inquires the basis. Select Tools > Connection Test > DNS Query. Enter some information in the field, and click on OK. Then, you will see DNS Query Result. (Figure 9-1.3)

- Using DNS Server: Enter a DNS server IP address or domain name in the field. (Max. 50 Characters)
- Domain or IP to Query: Enter an IP address or domain name in the field. (Max. 50 Characters)
- Query Type: Select the interface from the list. There are ANY, SOA, NS Record, A Record, MX Record, CHAME, and PTR.

Figure 9-1. 3 DNS Query

Port Scan

To inquire the Port Scan detailed material , which at present can inquire the server to open to serve the port, contains FTP, SSH, TELNET, SMTP, DNS, HTTP, POP3, SAMBA, IMAP, SNMP, PROXY, MySQL, SMTPS, IMAPS…etc. Select Tools > Connection Test > Port Scan. Enter domain or IP address in the field, and click on OK. Then, you will see Port Scan Result. (Figure 9-1.4) (Figure 9-1.5)

- Domain or IP to Scan: Enter the domain or IP address for the packets.

Figure 9-1. 4 Port Scan "scan.sharetech.com.tw"

Figure 9-1. 5 Port Scan "www.google.com.tw"

IP Route

IP Route shows router status in order to know router information; it also shows multiple subnet status. (Figure 9-1.6)

Figure 9-1. 6 IP Route

Interface Information

It shows SG-100N of the present interface information. (Figure 12-1.7) (Figure 12-1.8) (Figure 12-1.9) (Figure 12-1.10)

Figure 9-1. 7 LAN Information

Figure 9-1. 8 DMZ Information

Figure 9-1. 9 WAN1 Information

Figure 9-1. 10 WAN2 Information

Wake Up

Select Tools > Connection Test > Wake Up and please click on Assist (Figure 9-1.11) (Figure 9-1.12)

Figure 9-1. 11 wake up

Figure 9-1. 12 wake up

IPv6

Ping your IPv6 in order to check whether LAN/WAN/DMZ Alive Detection. (Figure 9-1.13)

Select Tools > Connection Test > IPv6, and enter your IPv6

- Target IP: Enter IPv6 IP

The Google Public DNS IPv6 addresses are as follows:

2001:4860:4860::8888

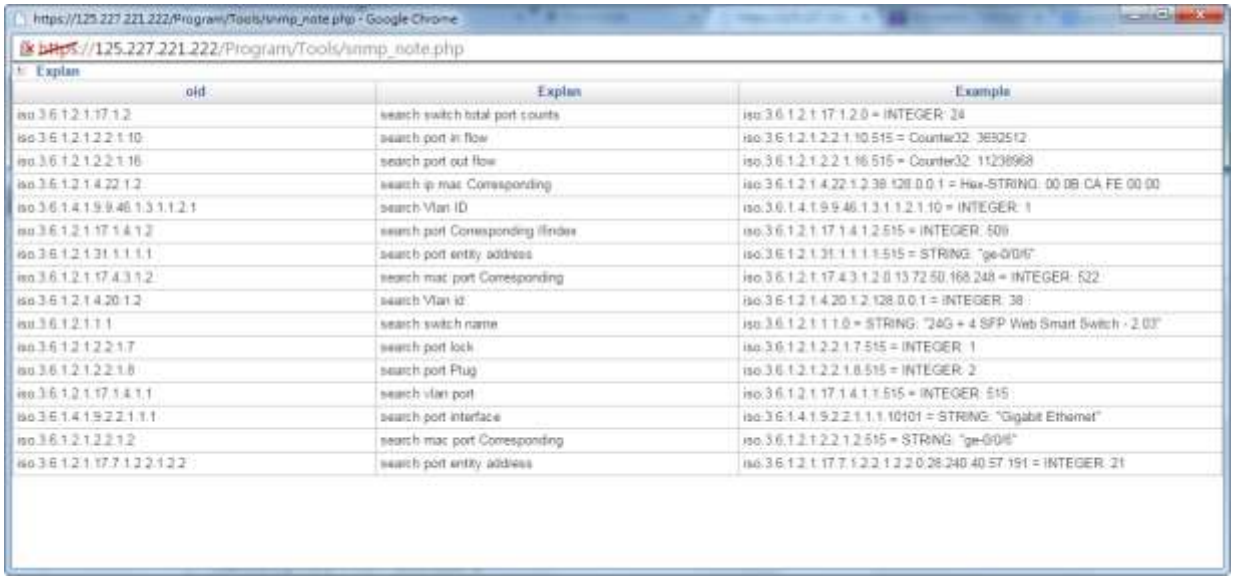
2001:4860:4860::8844

Figure 9-1. 13 IPv6 status

SNMP

This feature helps administrator check issue Switch Status.

Please click to know more SNMP information. (Figure 9-1.14)



oid	Explan	Example
iso.3.6.1.2.1.17.1.2	search switch total port counts	iso.3.6.1.2.1.17.1.2.0 = INTEGER: 24
iso.3.6.1.2.1.2.2.1.10	search port in flow	iso.3.6.1.2.1.2.2.1.10.515 = Counter32: 3692512
iso.3.6.1.2.1.2.2.1.16	search port out flow	iso.3.6.1.2.1.2.2.1.16.515 = Counter32: 11238968
iso.3.6.1.2.1.4.22.1.2	search ip mac Corresponding	iso.3.6.1.2.1.4.22.1.2.38.128.0.0.1 = Hex-STRING: 00 0B CA FE 00 00
iso.3.6.1.4.1.9.9.46.1.3.1.1.2.1	search Vlan ID	iso.3.6.1.4.1.9.9.46.1.3.1.1.2.1.10 = INTEGER: 1
iso.3.6.1.2.1.17.1.4.1.2	search port Corresponding ifIndex	iso.3.6.1.2.1.17.1.4.1.2.515 = INTEGER: 509
iso.3.6.1.2.1.31.1.1.1.1	search port entity address	iso.3.6.1.2.1.31.1.1.1.1.515 = STRING: "ge-0/0/6"
iso.3.6.1.2.1.17.4.3.1.2	search mac port Corresponding	iso.3.6.1.2.1.17.4.3.1.2.0.13.72.50.168.248 = INTEGER: 522
iso.3.6.1.2.1.4.20.1.2	search Vlan id	iso.3.6.1.2.1.4.20.1.2.128.0.0.1 = INTEGER: 38
iso.3.6.1.2.1.1.1	search switch name	iso.3.6.1.2.1.1.1.0 = STRING: "24G + 4 SFP Web Smart Switch - 2.03"
iso.3.6.1.2.1.2.2.1.7	search port lock	iso.3.6.1.2.1.2.2.1.7.515 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.8	search port Plug	iso.3.6.1.2.1.2.2.1.8.515 = INTEGER: 2
iso.3.6.1.2.1.17.1.4.1.1	search vlan port	iso.3.6.1.2.1.17.1.4.1.1.515 = INTEGER: 515
iso.3.6.1.4.1.9.2.2.1.1.1	search port interface	iso.3.6.1.4.1.9.2.2.1.1.1.10101 = STRING: "Gigabit Ethernet"
iso.3.6.1.2.1.2.2.1.2	search mac port Corresponding	iso.3.6.1.2.1.2.2.1.2.515 = STRING: "ge-0/0/6"
iso.3.6.1.2.1.17.7.1.2.2.1.2.2	search port entity address	iso.3.6.1.2.1.17.7.1.2.2.1.2.2.0.28.240.40.57.191 = INTEGER: 21

Figure 9-1. 14 General SNMP information

For instance, select Tools > Connection Test > SNMP, and enter your switch IP, Read permissions, and OID. It shows switch SNMP result. (Figure 9-1.15)

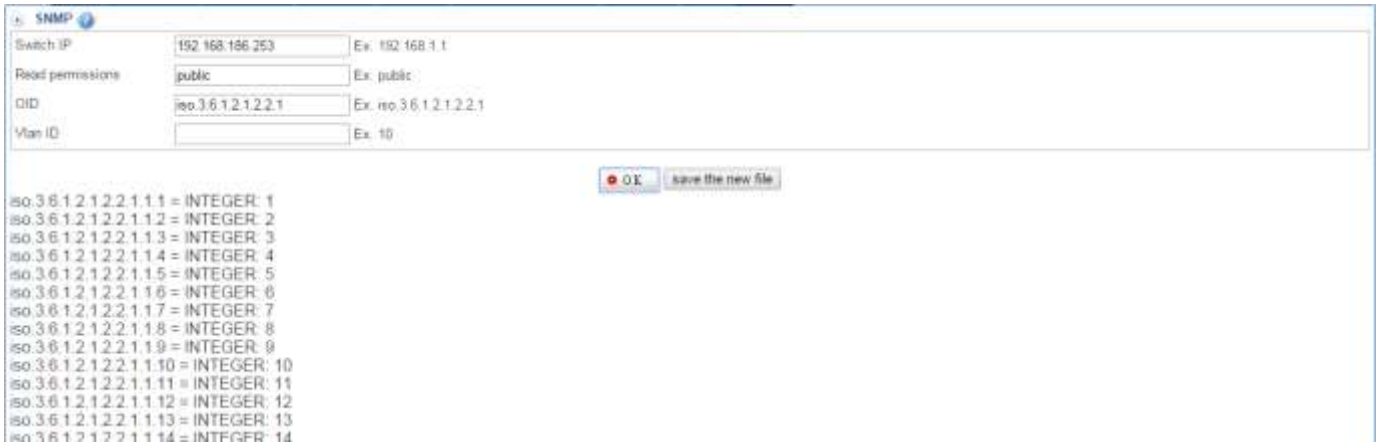
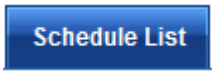


Figure 9-1. 15 SNMP result

9-2 Packet Capture

The following are some examples people uses Packet Capture for network administrators use it to troubleshoot network problems and network security engineers use it to examine security problems.



Select Tool > Packet Capture > Schedule List. Click to create a new schedule.

- Enabled: Enable listen packet.
- Time Range: Select time range
- Interface: Select which interface you are going to listen.
  1. LAN
  2. DMZ
  3. WAN
- Protocol: Select which protocol you are going to listen.
  1. ANY
  2. TCP
  3. UDP
  4. ICMP
  5. ARP
- Filter Condition: please refer the following explanation or read the Wireshark manual http://www.wireshark.org/docs/wsug_html_chunked/
- pcap File Size (MB): default is 5
- pcap Filter Num: default is 10
- Print the link-level header: show MAC information of OSI layer 2

Filter type: host(default), net, port

Type	Description and Example
host 192.168.1.155	Listen 192.168.1.155 host
net 192.168.1.0/24	Listen 192.168.1.0/24 network
port 23	Listen port 23

Transfer Direction: src, dst, src or dst, dst and src

C-like	Type	Description and Example
src 210.27.48.2	source	It means filtering source match 210.27.48.2
dst net 202.0.0.0	distance	It means filtering distance match 202.0.0.0

Filter Logical Operations

English	C-like	Description and Example
and	&&	Logical AND ip.src==192.168.1.111and tcp.glags.fin
not	!	Logical NOT not llc
or	||	Logical OR ip.src==192.168.1.111 or ip.src192.168.1.1

23. There is an example how packet capture is used. (Figure 9-2.1)

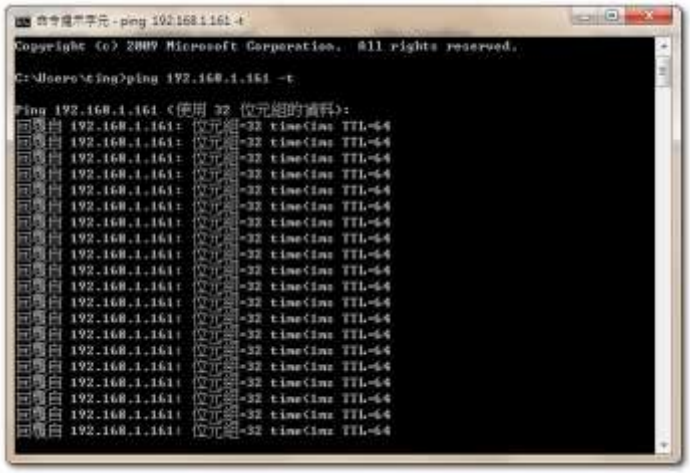


Figure 9-2. 1 ping LAN

24. Ping is ICMP protocol. (Figure 9-2.2) (Figure 9-2.3)

Figure 9-2. 2 Add listen Schedule

Figure 9-2. 3 Listen Schedule List

Completed List

Select Tool > Packet Capture > Completed List. (Figure 9-2.4)

Figure 9-2. 4 Completed List

Click Log, and download pcap file. (Figure 9-2.5)

Figure 9-2. 5 download pcap file

Please install Wireshark software (http://www.wireshark.org/), and open pcap file by Wireshark. As you see the following figure, we may know 192.168.1.111 have been transfer ICMP packets to 192.168.1.161. They have had communication each other. (Figure 9-2.6)

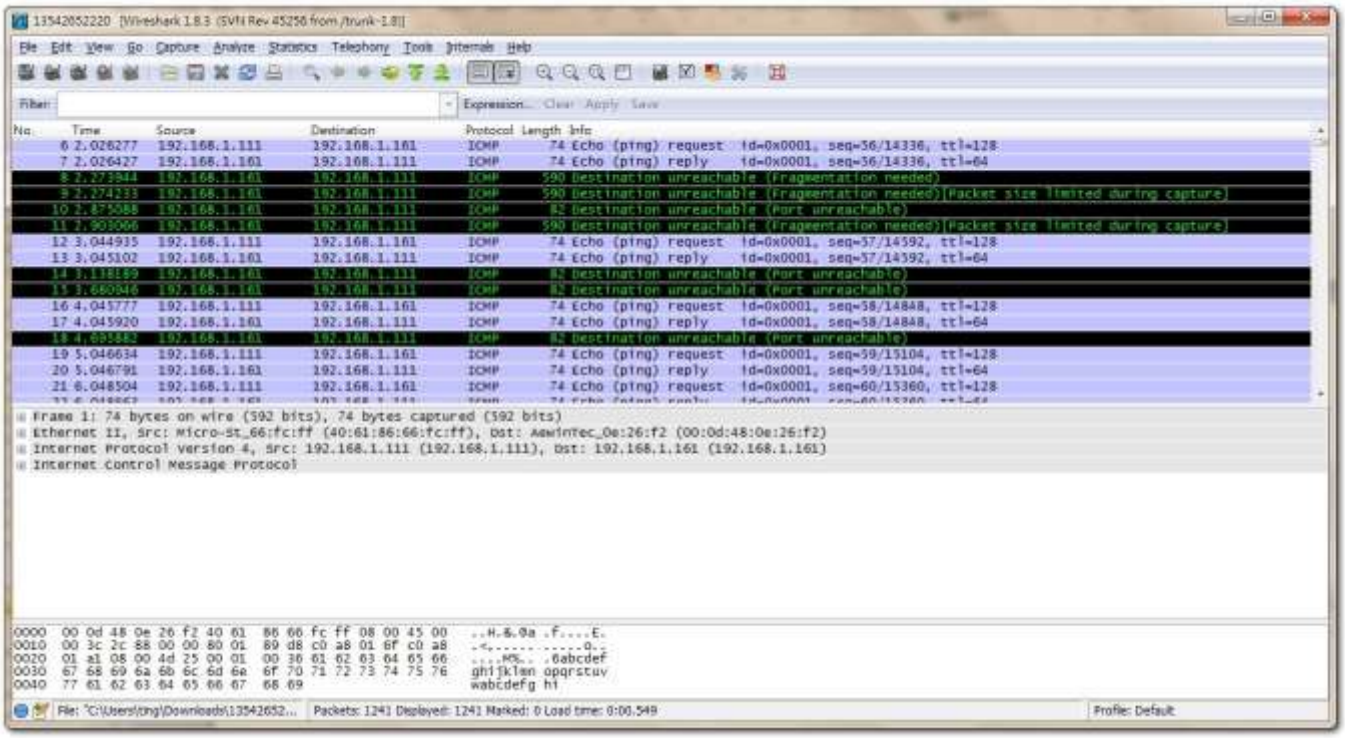


Figure 9-2. 6 open pcap file by Wireshark

What is Wireshark?

Wireshark is a network packet analyzer. A network packet analyzer will try to capture network packets and tries to display that packet data as detailed as possible.

Reference: Wireshark User's Guide (http://www.wireshark.org/docs/wsug_html_chunked/)

Here are some things Wireshark does not provide:

1. Wireshark isn't an intrusion detection system. It will not warn you when someone does strange things on your network that he/she isn't allowed to do. However, if strange things happen, Wireshark might help you figure out what is really going on.
2. Wireshark will not manipulate things on the network, it will only "measure" things from it. Wireshark doesn't send packets on the network or do other active things (except for name resolutions, but even that can be disabled).

25. There is another example to show how wireshark is used. Select Capture > Options…(Figure 9-2.7)

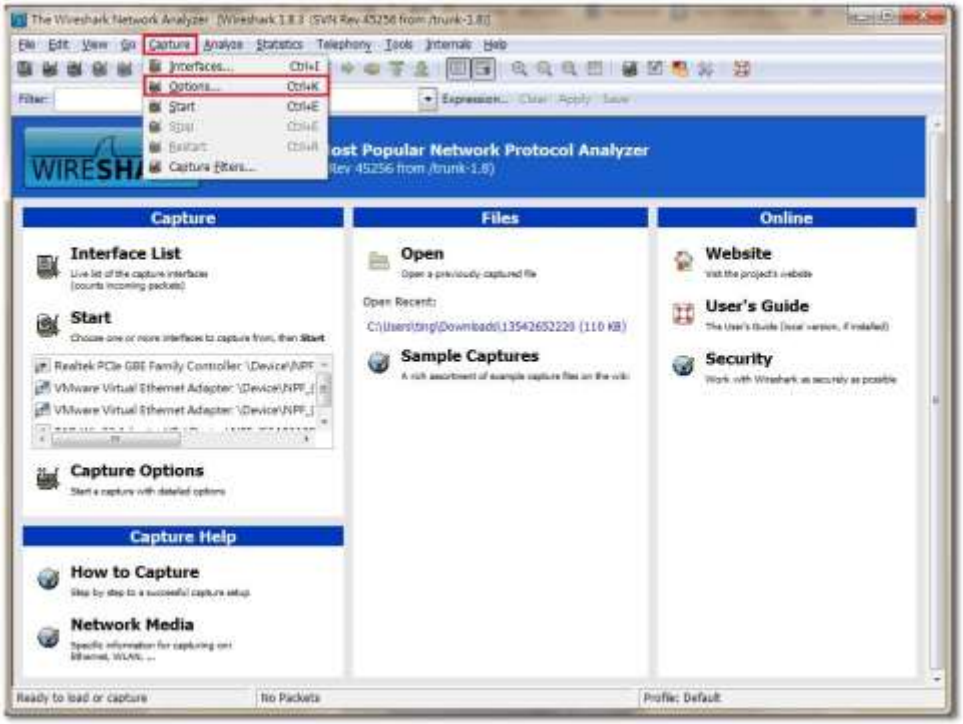


Figure 9-2. 7 Wireshark collection

Select your network card. (Figure 9-2.8)

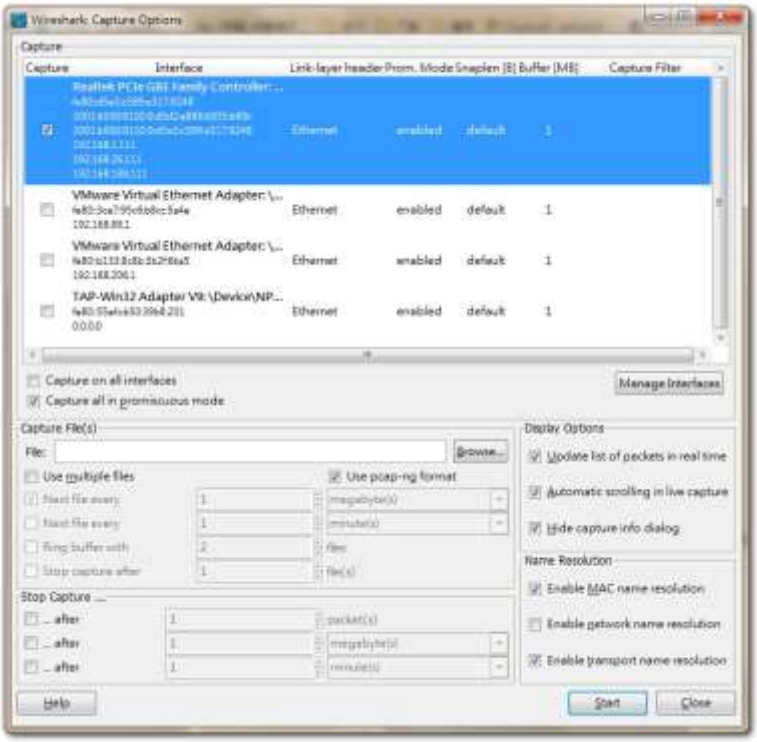


Figure 9-2. 8 select network card

Select FileZilla FTP server after you start collect packets by wireshark. (Figure 9-2.9)

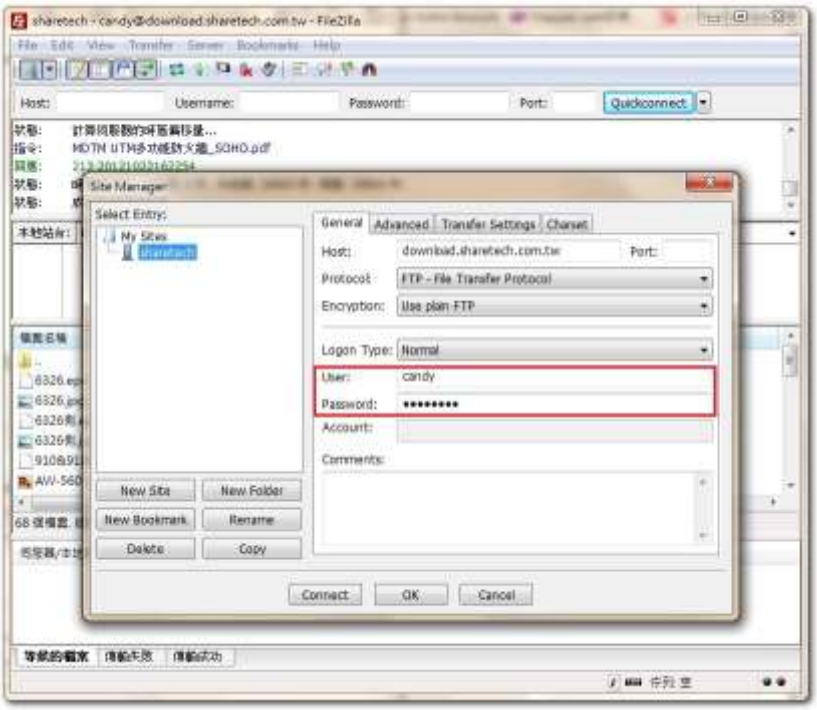


Figure 9-2. 9 connect FTP server

Select "Stop the running live capture" after Disconnected FTP server (Figure 9-2.10)

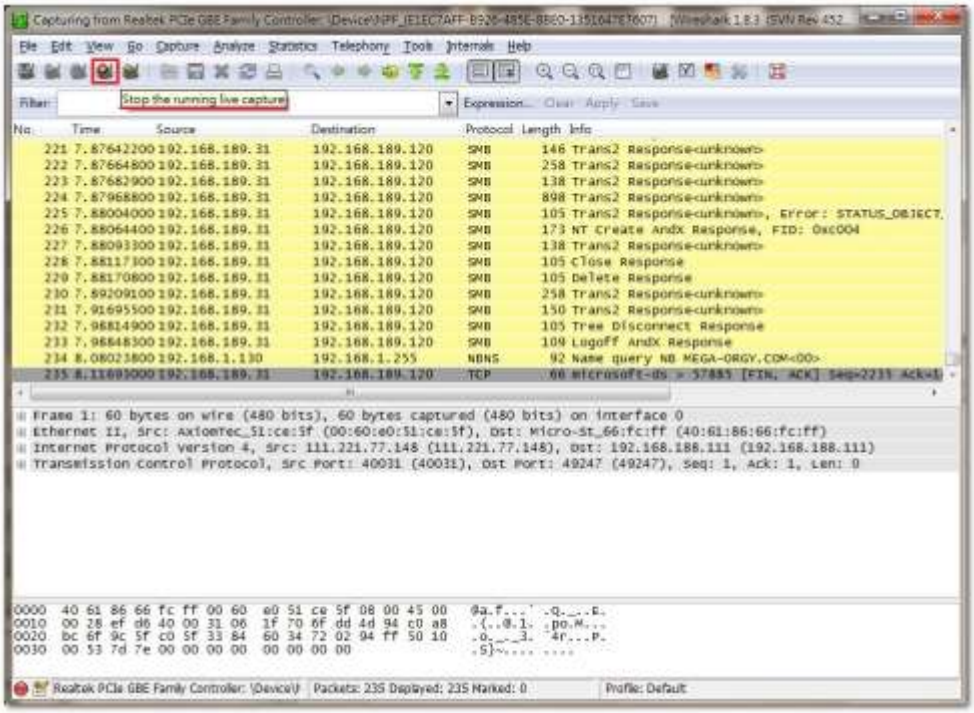


Figure 9-2. 10 stop the running live capture

Because of Wireshark collect wide range packets, and we just need FTP detailed packets information. We have used FTP so that filter type is "FTP Protocol." Select Expression > FTP (Figure 9-2.11)

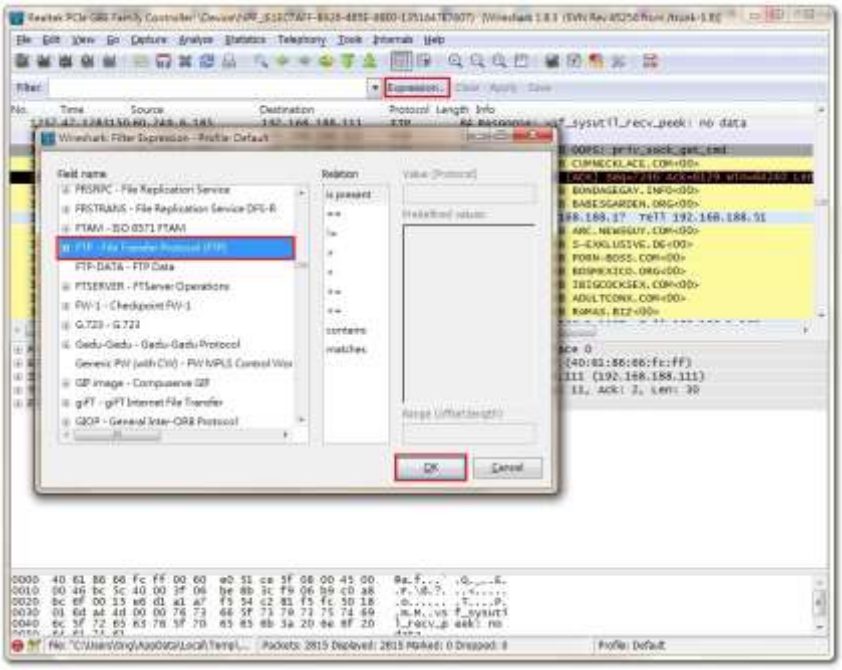


Figure 9-2. 11 Wireshark Expression

You may figure out username/password. (Figure 9-2.12)

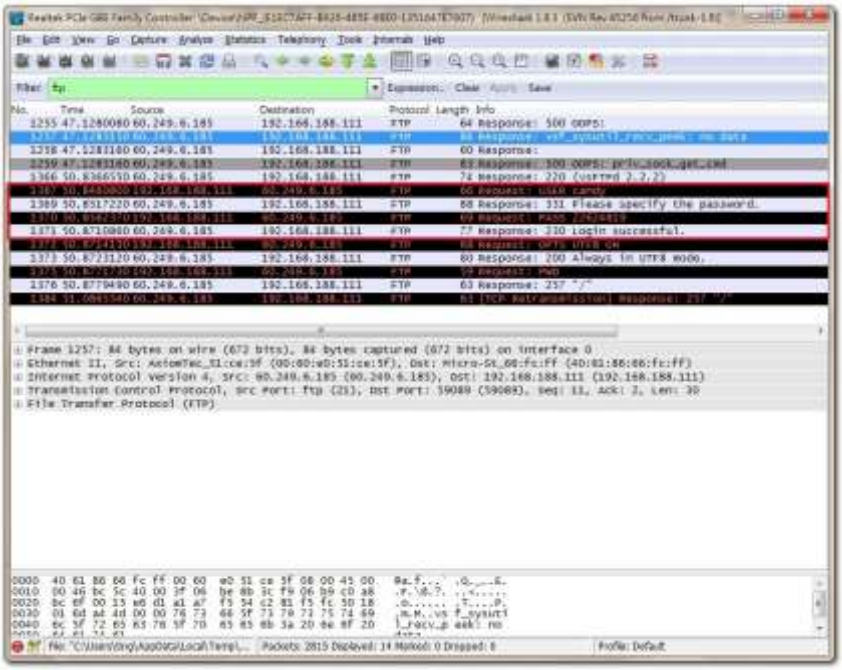


Figure 9-2. 12 Filter:ftp

Chapter 10：Logs

In the Logs chapter you can enable the following lists:

- 10-1 System Operation

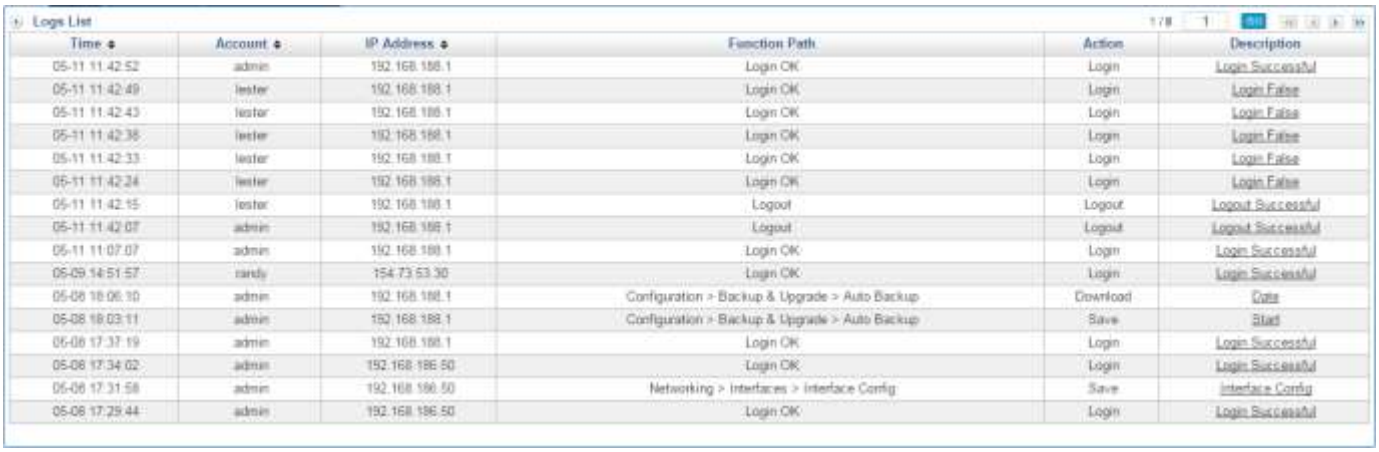
10-1 System Operation

Log records all connections that pass through the SG-100N. The information is classified as Configuration, Networking, Policy, Object, and so on. Event log has the records of any system configurations made. Each log denotes who, when, what and where that a configuration is being modified. The Administrator can view the logged data to evaluate and troubleshoot the network, such as pinpointing the source of traffic congestions. You can see simply information in Logs. If you need more information, you could use Logs Search to search what logs you need. The result shows on Logs Search Result.

Logs

Select Logs > System Operation > Logs. It shows configurations which has been modified with illustration, describe what kinds of action has been modified, describe which IP address has ever done function path. (Figure 10-1.1)

- Time: It shows event time.
- Account: Which account name has ever done event.
- IP Address: It shows IP address with Account.
- Function Path: To record the superintendent events that management.
- Action: The superintendent carries out movement, include login, add, edit, delete, search, refresh, Download, and so on.
- Description: To describe the event.



Logs List

Time	Account	IP Address	Function Path	Action	Description
05-11 11:42:52	admin	192.168.188.1	Login OK	Login	Login Successful
05-11 11:42:49	lester	192.168.188.1	Login OK	Login	Login False
05-11 11:42:43	lester	192.168.188.1	Login OK	Login	Login False
05-11 11:42:38	lester	192.168.188.1	Login OK	Login	Login False
05-11 11:42:33	lester	192.168.188.1	Login OK	Login	Login False
05-11 11:42:24	lester	192.168.188.1	Login OK	Login	Login False
05-11 11:42:15	lester	192.168.188.1	Logout	Logout	Logout Successful
05-11 11:42:07	admin	192.168.188.1	Logout	Logout	Logout Successful
05-11 11:07:07	admin	192.168.188.1	Login OK	Login	Login Successful
05-09 14:51:57	randy	154.73.53.30	Login OK	Login	Login Successful
05-08 18:06:10	admin	192.168.188.1	Configuration > Backup & Upgrade > Auto Backup	Download	Date
05-08 18:03:11	admin	192.168.188.1	Configuration > Backup & Upgrade > Auto Backup	Save	Start
05-08 17:37:19	admin	192.168.188.1	Login OK	Login	Login Successful
05-08 17:34:02	admin	192.168.186.50	Login OK	Login	Login Successful
05-08 17:31:58	admin	192.168.186.50	Networking > Interfaces > Interface Config	Save	Interface Config
05-08 17:29:44	admin	192.168.186.50	Login OK	Login	Login Successful

Figure 10-1. 1 Logs

Logs Search

Select Logs > System Operation > Logs Search. (Figure 10-1.2)

- Account: Available account which administrator you had made before.
- Computer Name: All of available computers which are ever through the SG-100N
- IP Address: Internal IP addresses.
- Login Setting: Recording users login system logs.
- Configuration: It lists out the working connections for the Data & Time, Administration, System, and Language logs.
- Network: It lists out the working connections for the Interface and Routing logs.
- Policy: It lists out the working connections for the LAN Policy, DMZ Policy, and WAN Policy logs.
- Objects: It lists out the working connections for the Address, Services, QoS, Schedule, Application Software, URL, and Virtual Server logs.
- Network Services: It lists out the working connections for the DHCP, DDNS, DNS, WEB/FTP, MSN, Anti-Virus logs.
- Mail Service: It lists out the working connections for the Filter & Log, Anti-virus, Anti-Spam, and Mail logs.
- Content Recorder: It lists out the working connections for the WEB, FTP, MSN, IM, and Mail contents.
- VPN: It lists out the working connections for the VPN Tunnel, PPTP Server, and PPTP Client logs.

Figure 10-1. 2 Logs Search

Logs Search Result

After click on Search, you will see logs search result as example below. (Figure10-1.3)

Search Result

Time	Account	IP Address	Function Path	Action	Description
05-09 14:51:57	randy	164.73.53.30	Login OK	Login	Login Successful
04-29 00:24:54	randy	192.168.188.1	Login OK	Login	Login Successful
04-29 00:20:06	randy	192.168.188.1	Login OK	Login	Login Successful
04-29 00:19:00	randy	192.168.188.1	Login OK	Login	Login False
04-29 00:18:54	randy	192.168.188.1	Login OK	Login	Login False
04-29 00:18:31	randy	192.168.188.1	Logout	Logout	Logout Successful
04-29 00:18:21	randy	192.168.188.1	Logout	Logout	Logout Successful

Figure 10-1. 3 Logs Search Result

Chapter 11：Status

This function provides current information about the device and the network including addresses for LAN / WAN, subnet masks, default gateways, etc. as well as current network connection status and other information. In the Status chapter you can enable the following lists:

- 11-1 Performance
- 11-2 Connection Status
- 11-3 Flow Awalysis

11-1 Performance

There are three parts, System Status, Interface Flow, and History Status. Performance section shows the utilization of CPU Usage, Memory Usage, System Usage, Each interface's on downloads the current capacity also to be possible to inquire the above information historical current capacity.

System Status

Generally speaking, system status shows graphs of resource usage. It shows last 12 hours machine status. Select Status > Performance > System Status. There are three graphs, CPU Usage, Memory Usage, and System Usage. In addition, select System Usage tick box, and click on OK. You will get graphs of System Usage.

- CPU Usage：The CPU utilization of the device(Figure 11-1.1)
- Memory Usage：The Memory utilization of the device(Figure 11-1.2)
- System Usage：The System utilization of the device(Figure 11-1.3)

Figure 11-1. 1 CPU Usage

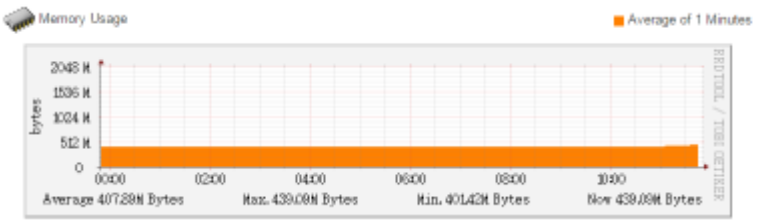


Figure 11-1. 2 Memory Usage

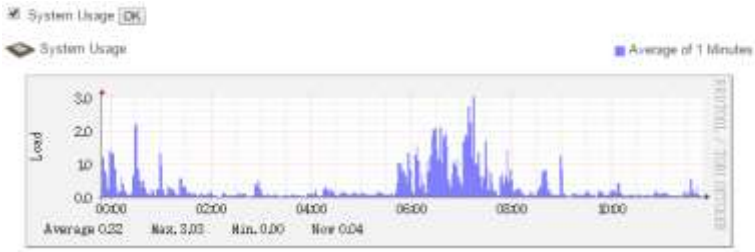


Figure 11-1. 3 System Usage

Interface Flow

Select Status > Performance> Interface Flow. It shows graphs of incoming and outing traffic through that interface.

- LAN: Last 12 Hours LAN Interface Flow Status (Figure 11-1.4)
- WAN 1: Last 12 Hours WAN1 Interface Flow Status (Figure 11-1.4)
- WAN 2: Last 12 Hours WAN2 Interface Flow Status (Figure 11-1.4)
- DMZ: Last 12 Hours DMZ Interface Flow Status (Figure 11-1.5)

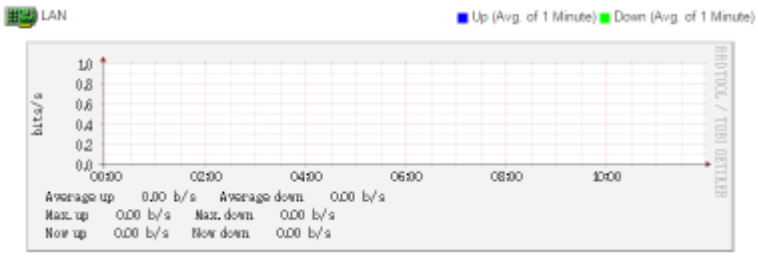


Figure 11-1. 4 Last 12 Hours LAN Interface Flow Status

Figure 11-1. 5 Last 12 Hours WAN Interface Flow Status

Figure 11-1. 6 Last 12 Hours DMZ Interface Flow Status

History Status

Select Status > Performance > History Status. Set information, and click on Search. Then, you will see Search Result. It shows the history system condition. (Figure 11-1.6)

- Search Object(s): There are CPU, System Load, RAM, LAN, DMZ, WAN 1, and WAN 2.
- Date: Select date ranges.

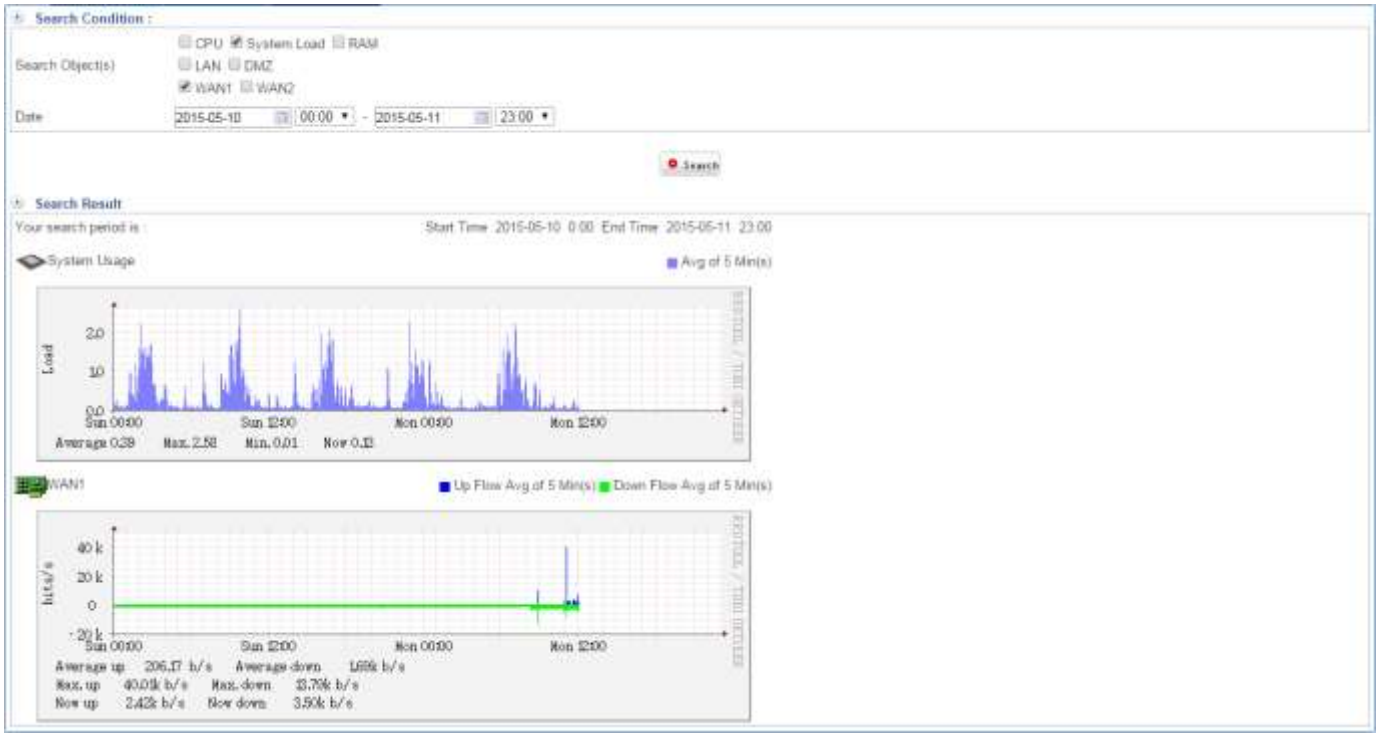


Figure 11-1. 7 History Status Result

11-2 Connection Status

The Connection Status section records all the connection status of host PCs that have ever connected to the SG-100N. It shows computer list and connect tract.

Computer List

Select Status > Connection Status> Computer List. It shows the current connection status information. (Figure 11-2.1)

- OS: It shows different OS system what those computers used after you enable "Client OS Detection", and click on Refresh. You are also able to enter Excluding IP which computer won't be detected. (Figure 11-2.2)

Default: disable

- Computer Name: The computer's network identification name.
- IP Address; The computer's IP address
- MAC Address: The computer's network adapter identification number
- Interface: You could know where the connecter is from, LAN or BRI.
- Status:
  1. On-line:
  2. Off-line:
- Last Update Time: When did users login

(year / month / day / hour / minute / seconds)

You are able to click on Refresh to get the current connection status information.

Figure 11-2. 1 Computer List

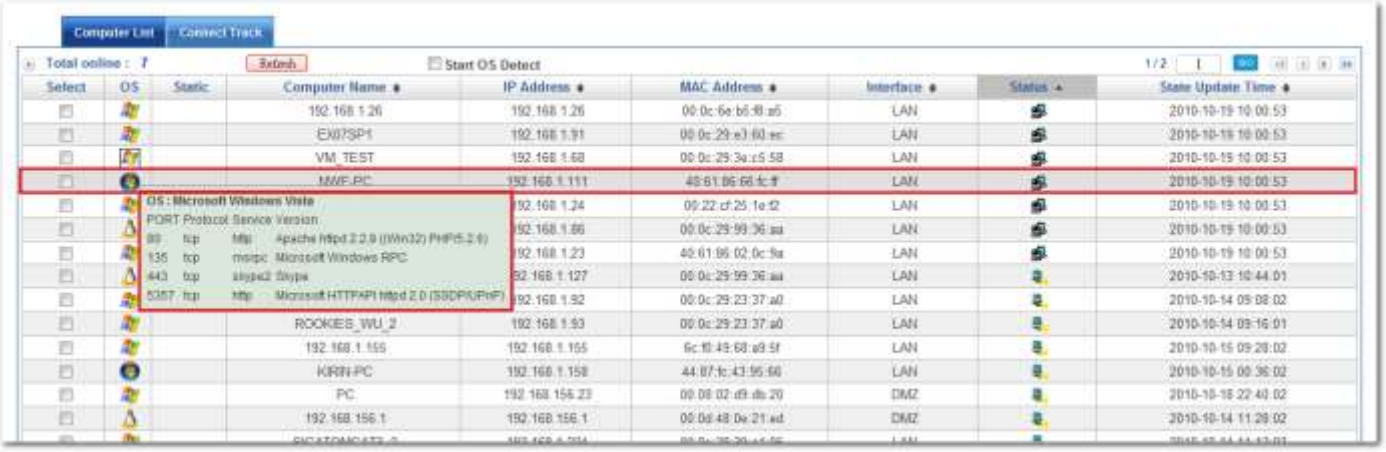


Figure 11-2. 2 Client OS Detection

Wireless Computer List

It's an optional item. If you don't purchase WiFi on **Configuration** > **Package**, you will not see this. (Figure 11-2.3)

Figure 11-2. 3 Wireless Computer List

Ap Management Computer List

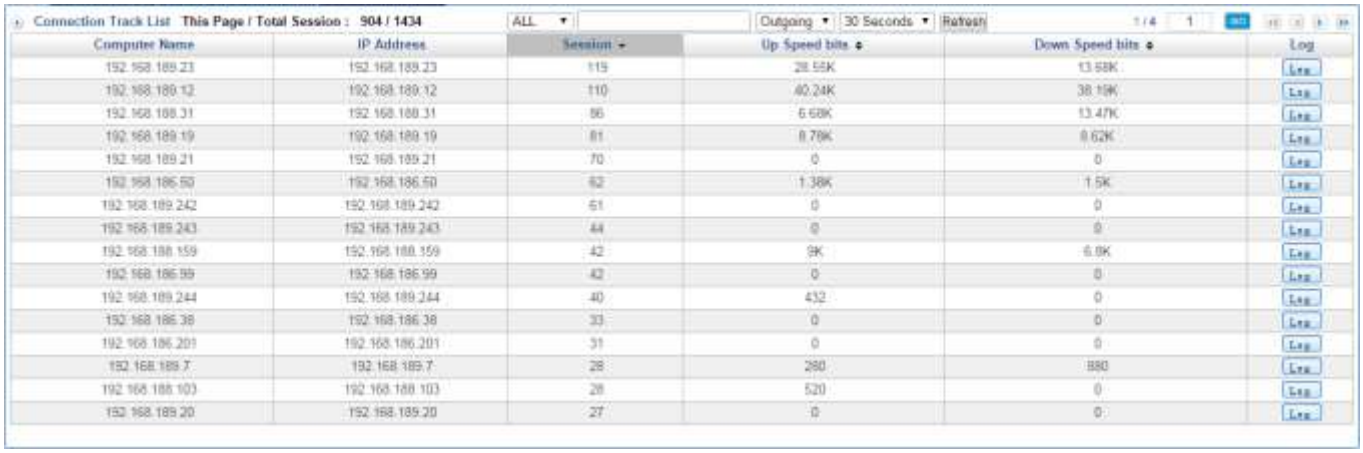
After you "Start" AP Management on 1-10 Configuration > Ap Management > AP Management Setting, you will see the Ap management computer list here as below. (Figure 11-2.4)

Figure 11-2. 4 Ap Management Computer List

Connection Track

According to the network packet analysis and tracing. It analyzes each of users' behavior on the Internet. This function originates the end name to take the classification, demonstrated that record of the present all user, contains the IP address, Session, Up speed bits, Down speed bits, and Log. Select Status > Connection Status> Connect Track. It shows the upload and download flow status of the computer all users at present. (Figure 11-2.5)

- Computer Name: The computer's network identification name.
- IP Address: It shows the computer IP Address.
- Session: It shows the current number of sessions connected to the computer.
- Up Speed bits: It shows the upstream bandwidth for the computer. Eight bits is a unit of a bytes/Second. 1024 bytes = 1 KB.
- Down Speed bits: It shows the downstream bandwidth for the computer. Eight bits is a unit of a bytes/Second. 1024 bytes = 1 KB.

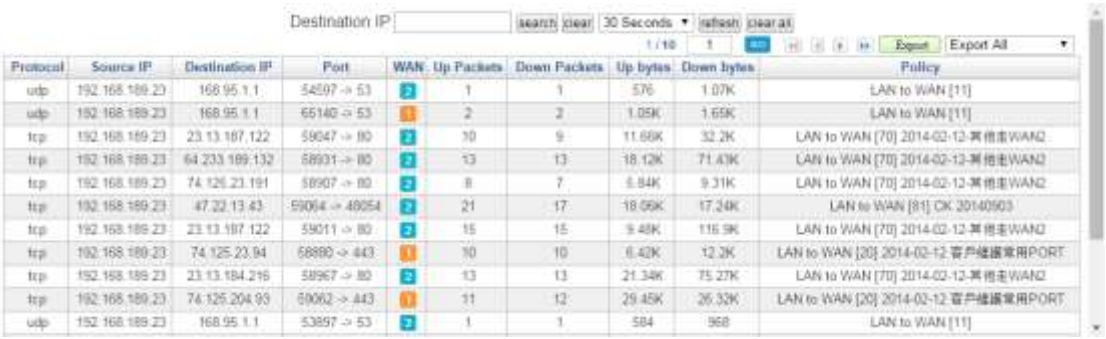

Connection Track List This Page / Total Session : 904 / 1434 ALL Outgoing 30 Seconds Refresh 1 / 4 1 GO

Computer Name	IP Address	Session	Up Speed bits	Down Speed bits	Log
192.168.189.23	192.168.189.23	119	28.55K	13.68K	Log
192.168.189.12	192.168.189.12	110	40.24K	38.19K	Log
192.168.188.31	192.168.188.31	86	6.68K	13.47K	Log
192.168.189.19	192.168.189.19	81	8.78K	8.62K	Log
192.168.189.21	192.168.189.21	70	0	0	Log
192.168.186.50	192.168.186.50	62	1.38K	1.5K	Log
192.168.189.242	192.168.189.242	61	0	0	Log
192.168.189.243	192.168.189.243	44	0	0	Log
192.168.188.159	192.168.188.159	42	9K	6.8K	Log
192.168.186.99	192.168.186.99	42	0	0	Log
192.168.189.244	192.168.189.244	40	432	0	Log
192.168.186.38	192.168.186.38	33	0	0	Log
192.168.186.201	192.168.186.201	31	0	0	Log
192.168.189.7	192.168.189.7	28	280	880	Log
192.168.188.103	192.168.188.103	28	520	0	Log
192.168.189.20	192.168.189.20	27	0	0	Log

Figure 11-2. 5 Connect Track

Click on Log, it shows more detail information. (Figure 11-2.6)

- Destination IP search: Type the specific IP address you want to search.
- Port: It shows the packets go through source port to destination port.
- Up Packets: It shows the upload flows at present.
- Down Packets: It shows the download flows at present.
- UP bps: The accumulation of upload flow. Eight bits is a unit of a bytes/Second. 1024 bytes = 1 KB.
- Down bps: The accumulation of download flow. Eight bits is a unit of a bytes/Second. 1024 bytes = 1 KB.


Destination IP search clear 30 Seconds refresh clear all 1 / 10 1 GO Export Export All

Protocol	Source IP	Destination IP	Port	WAN	Up Packets	Down Packets	Up bytes	Down bytes	Policy
udp	192.168.189.23	168.95.1.1	54597 -> 53	2	1	1	576	1.07K	LAN to WAN [11]
udp	192.168.189.23	168.95.1.1	65140 -> 53	1	2	2	1.05K	1.65K	LAN to WAN [11]
tcp	192.168.189.23	23.13.187.122	59047 -> 80	2	10	9	11.66K	32.2K	LAN to WAN [70] 2014-02-12-其他走WAN2
tcp	192.168.189.23	64.233.189.132	58931 -> 80	2	13	13	18.12K	71.43K	LAN to WAN [70] 2014-02-12-其他走WAN2
tcp	192.168.189.23	74.125.23.191	58907 -> 80	2	8	7	6.84K	9.31K	LAN to WAN [70] 2014-02-12-其他走WAN2
tcp	192.168.189.23	47.22.13.43	59064 -> 48054	2	21	17	18.06K	17.24K	LAN to WAN [81] CK 20140903
tcp	192.168.189.23	23.13.187.122	59011 -> 80	2	15	15	9.48K	116.9K	LAN to WAN [70] 2014-02-12-其他走WAN2
tcp	192.168.189.23	74.125.23.94	58880 -> 443	1	10	10	6.42K	12.2K	LAN to WAN [20] 2014-02-12-客戶端服常用PORT
tcp	192.168.189.23	23.13.184.216	58967 -> 80	2	13	13	21.34K	75.27K	LAN to WAN [70] 2014-02-12-其他走WAN2
tcp	192.168.189.23	74.125.204.93	59062 -> 443	1	11	12	29.45K	26.32K	LAN to WAN [20] 2014-02-12-客戶端服常用PORT
udp	192.168.189.23	168.95.1.1	53897 -> 53	2	1	1	584	968	LAN to WAN [11]

Figure 11-2. 6 Connection Track Log

11-3 Flow Analysis

It shows all main flow of connection. This function not only records the Downstream Flow and Up Flow, but also provides the IT administrator with detailed statistical reports and charts. In this section, it shows Top Flow List, Top Flow List by Port, and Top Flow Search.

Top N Flow

Select Status > Flow Analysis > Top N Flow. (Figure 11-3.1)

- Flow Direction: There are two selections. Default setting is OutBound.
  1. Outgoing
  2. Incoming
- Top N Flow: Select how many lists would be shown. Default setting is 10.
- Statistics Period: system will show period auto.

Click on Search, you will see result as below.

- Computer Name: The computer's network identification name
- IP Address: It shows the computer IP Address.
- MAC Address: The computer's network adapter identification number
- Up Flow (Kbytes): The accumulation of up flow.
  1 bytes = 8 bits kilobytes. 1 kilobytes = 1024 bytes.
- Down Flow (Kbytes): The accumulation of down flow.
  1 bytes = 8 bits kilobytes. 1 kilobytes = 1024 bytes.

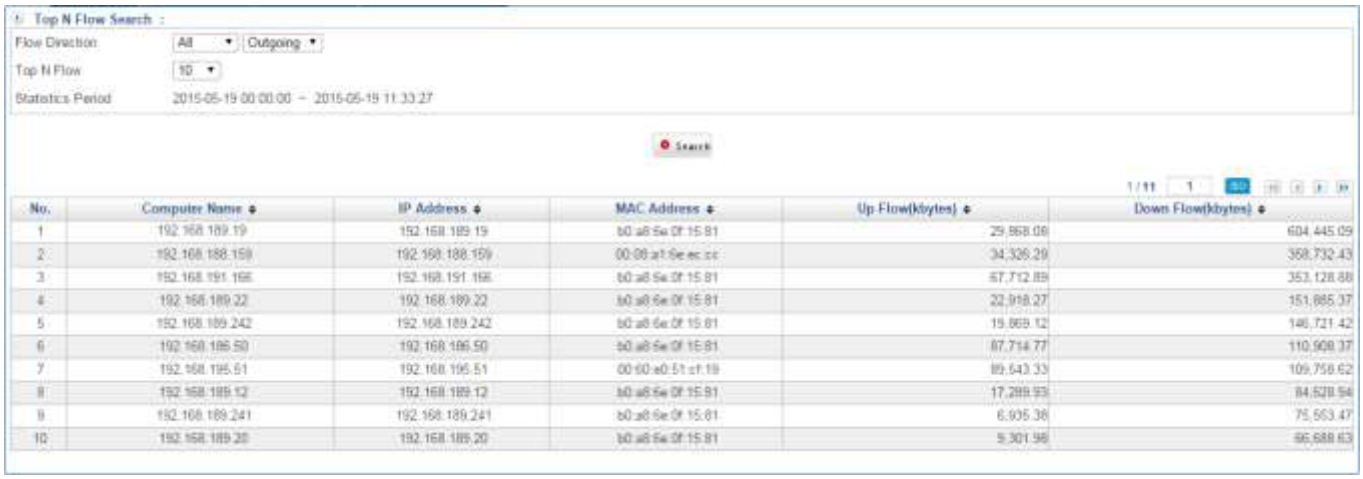


Figure 11-3. 1 Top N Flow

If you want to know which service port is the IP address connecting to, select the rectangular form. You will see a figure as below. (Figure 11-3.2)

IP : 192.168.189.20 Type : Outgoing

Service	Up Flow(kbytes)	Percentage	Down Flow(kbytes)	Percentage	Record
DNS	56.70	1%	128.45	< 1%	Log
HTTP	3,600.89	39%	27,562.16	41%	Log
other	718.30	8%	13,409.91	20%	Log
IMAP	13.21	< 1%	766.21	1%	Log
HTTPS	4,914.02	53%	24,826.23	37%	Log

Figure 11-3. 2 Top N Flow Detail

Click on Log to see a figure as below. (Figure 11-3.3)

IP : 192.168.189.20 Type : Outgoing Service : HTTP Reverse Dst IP Back

1 / 44 1 GO Export Export All

Date	Protocol	Src IP	Dst IP	Port	WAN	Up Flow(kbytes)	Down Flow(kbytes)	Policy
2015-05-19 08:33:59	tcp	192.168.189.20	74.204.71.137	49208 -> 80	2	1.23	2.77	LAN to WAN [70] 2014-02-12-其他走WAN2
2015-05-19 08:34:29	tcp	192.168.189.20	111.221.29.13	49227 -> 80	2	0.98	1.15	LAN to WAN [70] 2014-02-12-其他走WAN2
2015-05-19 08:34:59	tcp	192.168.189.20	178.255.83.1	49199 -> 80	2	1.43	3.18	LAN to WAN [70] 2014-02-12-其他走WAN2
2015-05-19 08:34:59	tcp	192.168.189.20	103.23.108.224	49277 -> 80	2	11.08	15.31	LAN to WAN [70] 2014-02-12-其他走WAN2
2015-05-19 08:34:59	tcp	192.168.189.20	202.39.236.195	49271 -> 80	2	0.86	5.91	LAN to WAN [70] 2014-02-12-其他走WAN2
2015-05-19 08:34:59	tcp	192.168.189.20	178.255.83.2	49206 -> 80	2	1.79	83.47	LAN to WAN [70] 2014-02-12-其他走WAN2
2015-05-19 08:35:30	tcp	192.168.189.20	203.66.213.165	49313 -> 80	2	1.01	7.72	LAN to WAN [70] 2014-02-12-其他走WAN2
2015-05-19 08:36:00	tcp	192.168.189.20	192.229.145.200	49221 -> 80	2	0.55	1.06	LAN to WAN [70] 2014-02-12-其他走WAN2
2015-05-19 08:37:00	tcp	192.168.189.20	103.23.108.119	49318 -> 80	2	1.66	5.54	LAN to WAN [70] 2014-02-12-其他走WAN2
2015-05-19 08:37:00	tcp	192.168.189.20	54.65.184.229	49379 -> 80	2	5.20	14.90	LAN to WAN [70] 2014-02-12-其他走WAN2
2015-05-19 08:37:00	tcp	192.168.189.20	68.232.44.121	49328 -> 80	2	5.21	33.33	LAN to WAN [70] 2014-02-12-其他走WAN2
2015-05-19 08:37:00	tcp	192.168.189.20	203.66.213.166	49312 -> 80	2	3.13	40.47	LAN to WAN [70] 2014-02-12-其他走WAN2
2015-05-19 08:37:00	tcp	192.168.189.20	118.163.170.12	49294 -> 80	2	1.88	22.97	LAN to WAN [70] 2014-02-12-其他走WAN2
2015-05-19 08:37:00	tcp	192.168.189.20	103.23.108.224	49289 -> 80	2	27.50	76.58	LAN to WAN [70] 2014-02-12-其他走WAN2
2015-05-19 08:37:00	tcp	192.168.189.20	103.23.108.184	49316 -> 80	2	0.89	1.16	LAN to WAN [70] 2014-02-12-其他走WAN2
2015-05-19 08:37:59	tcp	192.168.189.20	31.13.87.1	49335 -> 80	2	0.96	1.13	LAN to WAN [70] 2014-02-12-其他走WAN2

Figure 11-3. 3 Top N Flow Log

Top N Port Flow

Select Status > Flow Analysis > Top N Port Flow. (Figure 11-3.4)

- Flow Direction: There are two selections. Default setting is OutBound.
  1. Outgoing
  2. Incomingd
- Top N Flow: Select how many lists would be shown. Default setting is 10.
- Statistics Period: system will show period auto.

Click on Search, you will see result as below.

- Destination Port: It shows what specific port is IP used.
- Up Flow (Kbytes): The accumulation of up flow.
  1 bytes = 8 bits kilobytes. 1 kilobytes = 1024 bytes.
- Down Flow (Kbytes): The accumulation of down flow.
  1 bytes = 8 bits kilobytes. 1 kilobytes = 1024 bytes.

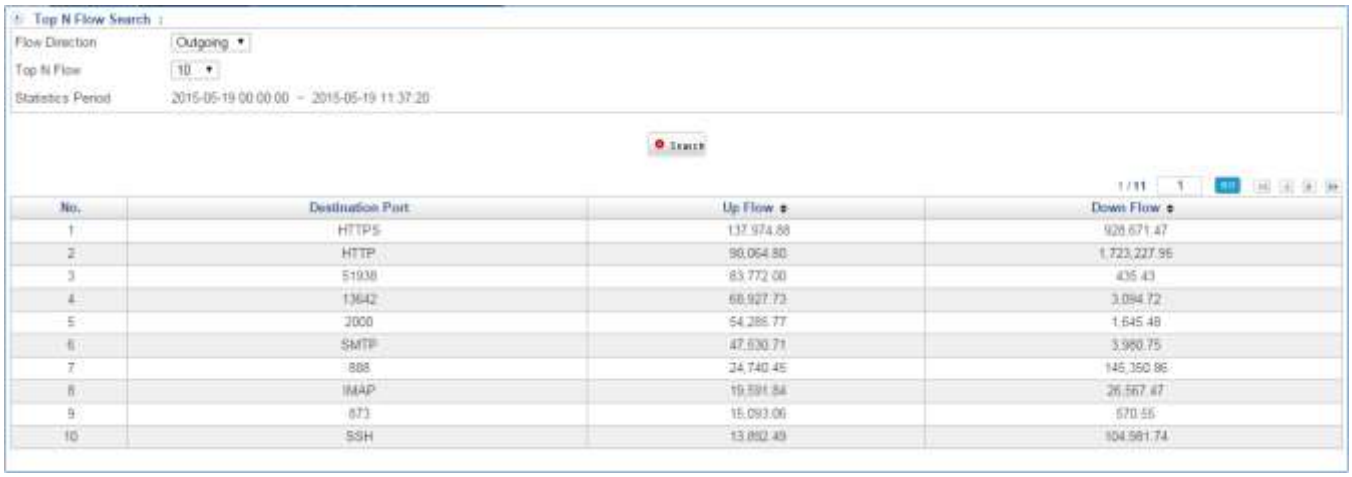


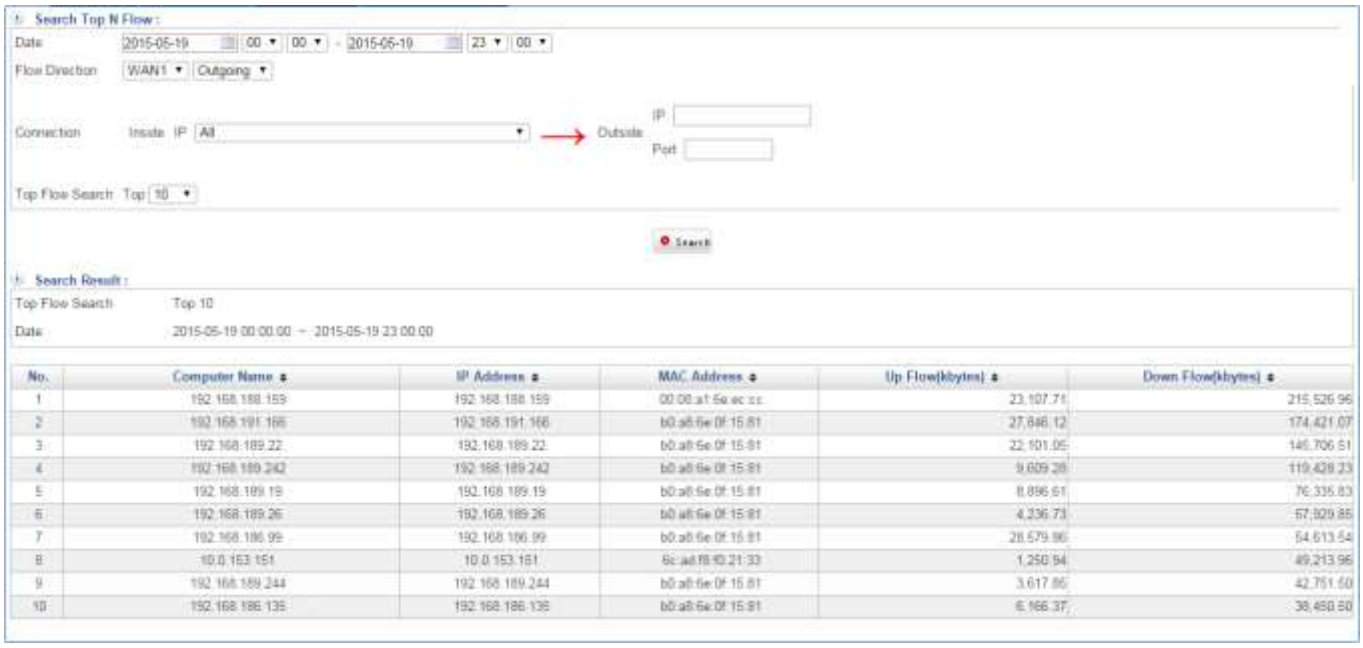
Figure 11-3. 4 Top N Port Flow

Top N Search

Select Status > Flow Analysis > Top N Search. (Figure 11-3.5)

- Date: Select date range.
- Flow Direction: There are two selections. Default setting is OutBound.
  1. Outgoing
  2. Incoming
- Connection: Select the computer IP Address.
- Top Flow Search: Select how many lists would be shown. Default setting is 10.

Click on Search you will see search result as below.



No.	Computer Name	IP Address	MAC Address	Up Flow(kbytes)	Down Flow(kbytes)
1	192.168.188.159	192.168.188.159	00:08:a1:6e:ec:cc	23,107.71	215,526.96
2	192.168.191.166	192.168.191.166	b0:a8:6e:0f:15:81	27,846.12	174,421.07
3	192.168.189.22	192.168.189.22	b0:a8:6e:0f:15:81	22,101.05	146,706.51
4	192.168.189.242	192.168.189.242	b0:a8:6e:0f:15:81	9,609.28	119,428.23
5	192.168.189.19	192.168.189.19	b0:a8:6e:0f:15:81	8,896.61	76,335.83
6	192.168.189.26	192.168.189.26	b0:a8:6e:0f:15:81	4,236.73	67,929.85
7	192.168.186.99	192.168.186.99	b0:a8:6e:0f:15:81	28,579.86	54,613.54
8	10.0.153.151	10.0.153.151	6c:ad:f8:f0:21:33	1,250.94	49,213.96
9	192.168.189.244	192.168.189.244	b0:a8:6e:0f:15:81	3,617.85	42,751.60
10	192.168.186.135	192.168.186.135	b0:a8:6e:0f:15:81	6,166.37	38,458.60

Figure 11-3. 5 Top Flow Search

If you would like to know which service is the IP address connects to, select the rectangular from. You will see a figure as below. (Figure 11-3.6)

Service	Up Flow(kbytes)	Percentage	Down Flow(kbytes)	Percentage	Record
HTTPS	17,911.04	74%	210,976.31	92%	Log
other	6,191.24	26%	18,091.14	8%	Log

Figure 11-3. 6 Top N Search Detail

You are able to click on Log to see more detailed. (Figure 11-3.7)

Date	Protocol	Src IP	Dst IP	Port	WAN	Up Flow(kbytes)	Down Flow(kbytes)	Policy
2015-05-19 00:00:32	tcp	192.168.188.159	23.100.42.232	59327 -> 443	1	0.84	1.92	LAN to WAN [19] 2014-02-12 客戶端國際用PORT
2015-05-19 00:01:02	tcp	192.168.188.159	23.100.42.232	59336 -> 443	1	1.26	2.88	LAN to WAN [19] 2014-02-12 客戶端國際用PORT
2015-05-19 00:01:33	tcp	192.168.188.159	104.45.86.116	56088 -> 443	1	0.84	1.92	LAN to WAN [19] 2014-02-12 客戶端國際用PORT
2015-05-19 00:02:33	tcp	192.168.188.159	104.45.86.116	56103 -> 443	1	1.26	2.88	LAN to WAN [19] 2014-02-12 客戶端國際用PORT
2015-05-19 00:03:34	tcp	192.168.188.159	23.100.42.232	59376 -> 443	1	0.84	1.92	LAN to WAN [19] 2014-02-12 客戶端國際用PORT
2015-05-19 00:04:04	tcp	192.168.188.159	23.100.42.232	59386 -> 443	1	1.68	3.84	LAN to WAN [19] 2014-02-12 客戶端國際用PORT
2015-05-19 00:04:34	tcp	192.168.188.159	23.100.42.232	59395 -> 443	1	1.26	2.88	LAN to WAN [19] 2014-02-12 客戶端國際用PORT
2015-05-19 00:06:05	tcp	192.168.188.159	23.100.42.232	59418 -> 443	1	1.26	2.88	LAN to WAN [19] 2014-02-12 客戶端國際用PORT

Figure 11-3. 7 logs

Search Quota History

If you have ever set up Quota on Policy, you are able to search history log here. (Figure 11-3.8) (Figure 11-3.9)

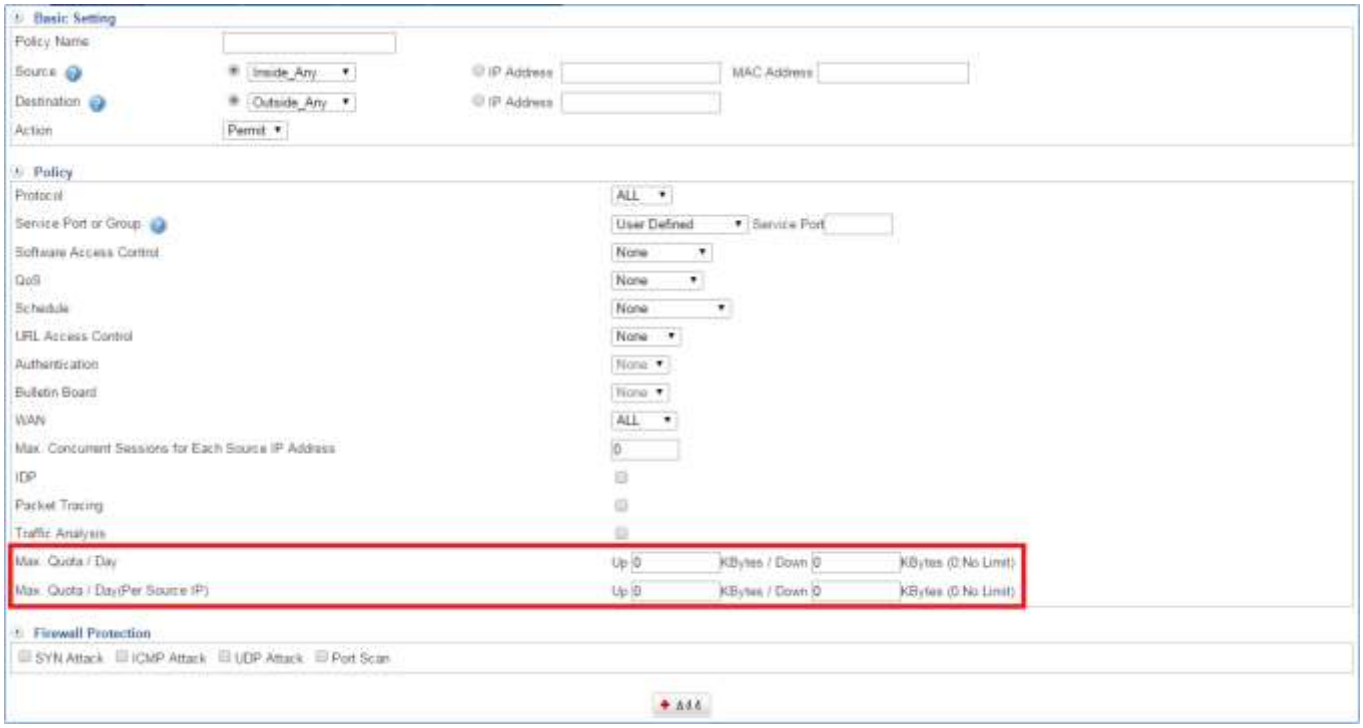


Figure 11-3. 8 Quota / Day

Figure 11-3. 9 Search Quota History