

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

CONV	CONVENTIONS USED IN THIS BOOK			
CHAP	TER 0 : DESCRIPTION			
	0-1 Hardware Overview	7		
	O-2 FRONT PANEL			
	O-3 Rear Panel			
	O-4 System Setting			
	O-5 Setting internal and external network			
	0-6 Homepage Information			
CHAP	TER 1 : CONFIGURATION			
	1-1 Date & 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	59		
CHAP	TER 2 : NETWORK	80		
	2-1 INTERFACE			
	2-2 INTERFACE (IPv6)			
	2-3 Routing			
	2-4 802.1Q			



CHAPTER 3 : POLICY	105
3-1 WIFI POLICY	
3-2 LAN POLICY	
3-3 DMZ POLICY	
3-4 WAN POLICY	
CHAPTER 4 : OBJECTS	109
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	
CHAPTER 5 : NETWORK SERVICES	166
5-1 DHCP	
5-2 DDNS	
5-3 DNS Proxy	
5-4 SNMP	
5-5 Remote Syslog Server	
CHAPTER 6 : IDP	185
6-1 IDP Setting	
6-2 IDP Log	
CHAPTER 7 : SSL VPN	189
7-1 SSL VPN SETTING	
7-2 SSL VPN Log	



7-3 VPN POLICY	
7-4 SSL FROM YOUR ANDROID PHONE	199
CHAPTER 8 : VPN	209
8-1 IPSEC TUNNEL	
8-2 PPTP Server	
8-3 PPTP CLIENT	
8-4 VPN POLICY	
CHAPTER 9 : TOOLS	226
9-1 Connection Test	
9-2 PACKET CAPTURE	
CHAPTER 10 : LOGS	241
10-1 System Operation	
CHAPTER 11 : STATUS	245
11-1 Performance	
11-2 Connection Status	
11-3 FLOW ANALYSIS	



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

Administrator
 Backup & Upgrask
 Lanouage

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.



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.





0-2 Front Panel





Model Name : please see the Figure 0-2.1(Figure 0-2.1)
 Appliance LED Behavior

- F-F		
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.

\mathbf{Q} 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



Chapter 0 : Description



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)

stogot).	101					
E Session	Options controlling local serial lines					
 Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Connection Data Praxy Telnet Rlogin SSH Senal 	Select a serial line Serial line to connect to Configure the serial line Speed (baud) Data bits Stop bits Parity Flow control	COM1 115200 8 1 None None				

 $Figure \ 0\text{-}3. \ 4 \ \text{PuTTY} \ \text{Configuration}$



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

	• ×
** (通知後 CCOM NS LPF) *********************************	
· · · · · · · · · · · · · · · · · · ·	J

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"

8	PuTTY Configuration	×				
Category:						
	Basic options for your PuTTY session					
Logging	Specify the destination you want to co	nnect to				
Kevboard	Serial line	Speed				
Bell Features Window Appearance Behaviour Translation Selection	СОМЗ	115200				
	Connection type: Raw Telnet Rlogin	SSH 💿 Serial				
	Load, save or delete a stored session Saved Sessions					
Colours Connection Data Proxy Telnet Riogin SSH	Default Settings 115200 192.168.186.76 192.168.188.1 192.168.189.143 192.168.189.144 192.178.88.254	▲ Load Save Delete				
Senai	Close window on exit: Always Never Only of Onl	on clean exit				
About	Open	Cancel				

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.

P	COM3 - PuTTY	-	×
RV LAN IP IS 1 CONMAND: 1948; J wth3: port 2(w wth3: port 2(w 1948; ADORCONF	32.108.1.1 HEGRICHY(METREY_CHANGE): wissol: link becomes ready Land) shiered forwarding stats Land) entered forwarding stats (METREY_CHANNE): with: link becomes ready		~
T or help admin pu def admin ip def spachs port restart poweraff computed if is 13 1 computed	<pre>dimpley help) set shmin's phasmord to defailt? clear setting of stmin's source ip) show spaths http,https pot1 restart system! poweroff system! b2.165:3.1</pre>		

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 <u>http://192.168.1.1</u> 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.

→ C 192.168.1 Acres	1	<u></u>
	Authentication Required The server http://192.108.1.1.80 requires a username and pessword. The server rays: WELCOME-LOGIN User Name: admin Pessword	III sharetechtw@gmail.com -
		4

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



Login completed (Figure 0-4.3)

Share Tech									administration of the second s	1243
A Contraction								Language English	• 5 second • He	heshi
· Date & Time			System Lines					Server tota		
 Adversation Nation 	Server Date / Time		2016-06-13		09-44-46		Server Model		3G-100N	
= Parkage	Current Timezone			Asia/Tiapel			Server Version	£1.9		
 Language Nutficition 	Server Liptime 9 days. 16 hours. 12 min			hain 12 minut	tes.		Machine's Number			
 Backup & Mount Signature Update 	-		System Resource			Serve Service				
BBL Proof	Bystem Loading				0 15 0 09 0 06		DHCP Services	P Sevices		
 MyCloud Salting 	CPU Loading				0.8%		CERES Slanvican		0	
 Nertoph 	RAM (2.68)	(GB)			58%	IPSer VPN Service			0	
Princy	Flash (182 MB)				49%	SMART HEID overall health test		PASSED		
Objects	HDD (100 G)	22		1%		MyCloud		0		
Natural Services					2000 - 2000					
	Plant 1		Real 7		Unterfaces a Mo	ni -	Prest 2		10-4 F	
• (DP	POR		P.04 5		Profil at		+01.3 143.67		POR 4	
 SSLVPN 	interface sype		Lives		and 1		ath)		10112	
. VPN	Connell Status	_	0		0		0		0	-
	Live Status		2							
· 1000	iP Aibhess		192, 968 1 1		192, 168, 186, 187		CFF		OFF	_
Loge	4.04.00	7.0		0.1		4.258		.0		-P
e Status	Total Packata	Re		0		\$71,860	0			10
	The Play Barry Barry	Te		0		1.27M		â		0
ferman	(com have token)	340		0		11.87M		9		-11
	The second se	1190011								
Share Tech	Copyright @ 2010 Share Tex	:h Information	Co., LTD: All rights reserve	d))						



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 \square Save. (Figure 0-4.4)

۲	8 Language					
9	English	Traditional Chinese	Simplified Chinese			
	III Save					

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.

Paddelaer			
Paddees		Subnet mask	
	Add.	1.00	(Beine)
elauk galawake:			
Gateway		Hesc	
	Add.	10.	Ferrer
TCP/IP Addre		3 X X	and soldiers
IP address			
Subnet mask	6 I.		
23			

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.

and the second second		
	V HEALTH IN	iller -
	Contract (1984	- 147
100 100 10	and the second sec	the local sectors in the local
Villey Land	Energia de la companya	-Call Street
10040415		
See +	410	the .
(migs (1000, must) three is a rest		
		we" to complete th
n Walter Walter	a state of the second	
[115.7	
	- ALCONTON	
		Im Index 7(p) Im Index 7(p) Im Index

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.

Concern + marriere	2. Enter Port 2 (WAN)	Related info	
THE PART NEW YORK	Transition .		
Cont Conta	5a -	initial lat	
- management	-	towner fam.	Sec. 11
P-10mm	10.00.000		000404
Chief Colory	10.00.00	and index	DEADER
a loss in second	The second second	free front in . Without	in A said
Instantion from	tion F consister	100	1000000
and interest	fee	friend.	11791
	1992 Damas P	(1) Instanto P	100000
1. White Description		210/10/10/12	
Seedin Meter	THE POP THE DEL	lange - tops	10,00,001
In the second second	and size a state	and the second se	
1. Navi Printer	3. Setup Port 2 (WAN) Alive	Detection	
* General Service	A111	Referant -	100
100.04	and the second se	#7704.0xx	
2.7.7.		2.211	C. Street

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

Default is 255.255.255.0. Only in "Static" mode is required.
Static" mode is required.
Input new MAC address
Jser Define
an based on local ISP's MIRN speed

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)

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)





MENU

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

	2.MH
8	Configuration
	Network
	Policy
	Objects
8	Network Services
8	OP
	SSL VPN
	VPN
	Tools
	Logs
	Status

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/Ta	ipe .
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)	110	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.

5	erver Info	
Server Model	SIG-100N	
Server Version	6.1.9	
Machine's Number		
Ser	ver Service	
DHCR Services	0	
DDNS Services	0	
IPSec VPN Service	0	
SMART HDD overall-health test	PASSED	
MyClouet	0	



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. 3: It does not connect the Internet.
- Line Status: Whether the judgment network does connect
 - 1. 學: 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 s More		
Port		Part 1	Part 2	Pot 3	Port 4
Interface Type		LAN	WAND	WAN2	DMZ
Interface		eth0	ath 1	eth2	eth3
Connect Status		0	0	0	0
Line Status		4	¢		4.
IP Address		192 168 1 1	192.16B.10E.157	OFF	OFF
Total Darkate	Tx		240.887	0	0
T STAR T MUTURE	Re	10.799	3,391,926	0	a
Total Flow (bota)	Te	408	71.30M	0	0
Come is ideal for the	Rx	1.434	334.2714	0	0

Figure 0-6. 5 Interface



Click » More (Figure 0-6.6)

			Interfaces a More		
Port		Port 1	Port 2	Port 3	Port 4
Interface Type		LAN	WANT	WAN2	SMC
Intertace.		athG	ath1 192 165 186 157	eth2	ath3
Connect Status		0			0
Line Status		- R _1		2,	2
IP Address		192 168 1 1		OFF	OFF.
Total Decision	Ta	4	241,066	0	0
1048 P363000.	Ra	10,799	3,392,494	0	0
Total Elses Solari	Tκ	408	71.37W	0	a a
ione constratat	Rx	1.49M	334.364	0	0
Darket (secled/s)	T)	D	1	0	D
Fortige (Dorstena)	Rx	10	6	0	0
Finandative	Tx	0	444	0	Ð
LIOW (OWIE)	Ra	0	136	0	0
From Darket	Ta	0	0	a	0
CHO PACES	Rx	0	0	0	0

Figure 0-6. 6 Interface more detailed



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 (NTP¹). 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)

5 Timezone and Time			
Time Zone		Asia/Taipei	•
Tame		16 · 20 · 40 ·	
Date		66 • [May •] 2015 •]	
5 Sync with NTP Serve	R .		
Sync with NTP Server	Contraction		
Time Server	time atdtime.gov.tw	Time Log Refresh	
Belect Time Server	Тароі	•	
Define Time Server.	time stidtime gov tw		
			E Save

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)



 User Defined Men 					E Select Al / None
Configuration	Date & Time Diffication MyCloud Setting	C Administration E Backup & Mount	🗐 System 🗐 Signature Optime	🗊 Package 🗊 Ap Management	© Language ⊟ \$SL Proof
Network	101 Interface	😳 Interface (IPv6)	iii Routing	107 (H02, 110)	
Policy	E LAN Policy	C DMZ Policy	UWAN Policy		
Objects	III Address Table III URL Filter	≡ Services ≣ Virtual Server	Schedule Frewall Protection	III QoS III Authentication	Application Control Bulletin Board
Network Services	10 DHCP	S DONS	UNS Proxy	III SIMP	Remote Syslog Server
IDP	III IDP Setting	III IDP Log			
SSL VPN	E SSL VPN Setting	SSL VPN Log	III VPN Policy		
VPN	III IPSec Tunnel	PPTP Server	E PPTP Client	10 VPN Policy	
Tools	III Connection Test	III Packet Capture			
Logs	III System Operation				
Status	(3) Performance	Correction Status	E Flow Analysis		



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.



S. Mensin semul	
Login Message	WELCOME-LOGIN
Homepage Messaage	ShareTech
Browser Message	UTM
Upinad Logo	Chosse File No file chosen (Image size 150 x 90 pixel GIF.)
Memory Release	Every 30 minutes check mercory usage more than 50 %, release mercory
Pass-through Protocol	🛙 H-323 🗇 SIP.
Session timeout of established	800 Sec(500 - 86400)
WatchDug Timer	R (When the system is crashed, watchdog will mmediately restart the system,)

Figure 1-2. 2 System Setup

n 115	2.190.100.157		1	Ξ.	 -
	Authentication Required The server http://142.168.186.157.80 require LOGD User Name and password. The server available User Name admin. Password +++++ Log In	x LCOME: Cencel			

Figure 1-2. 3 Login Message

E UTM	-		1	
< → × ñ 🗋 19.	2.168.186.157	*	9	=
Share Tech	ShareTech			
Monte				
 Configuration 	1			
 Naterrik. 	Survey Finds / Time	System 1	ime	
Pálicy	Current Timezone	2010-00-12	Ania/Tapel	
Ottects	Server Uptime		days, 18 hours, 8 minu	ðes.
· Nationk Services		System Res	90100	
a IDP	System Loading			2.04 1.33 1
- 11.F	CPU Loading		14	4.0%
SSL VPN	RAM (2 GB)		A Property of the	18%
 VFN 	Flash (182 MB)			49%
Waiting to 192168 106 157.	00)		ALC: NO	1%

Figure 1-2. 4 Homepage Message



UTM	- No.		
< → × ň □ 19	2.168.186.157	÷ 9	=
Share Tech	ShareTech		
Configuration		Sustan Time	
 Naterrik 	Server Date / Time	2015-05-13	11
Pálcy	Current Timezone	Ania/7	apei
· Objects	Server Uptime	0 days, 18 hou	rs.8 minutes
· Nation Services		System Resource	
a IDP	System Loading		2.04 1.33 1
ineral sizes	CPU Loading	14	4.0%
336 (PR)	RAM (2 GB)	a function of a	18%
 VFN 	Flash (182 MB)	1. A CONTRACTOR OF	45%
Waiting for 192 168 186 157.	(0G)	8 PC	1%

Figure 1-2. 5 Browser Message

C UTM	*		haits as
← → × ň □ 19	2.168.186.157	÷ ¥	=
Share Tech	Share Tech		
Configuration		forter Terror	
 Nationk 	Berver Date / Time	2015-05-13	
Palicy	Current Timezone	â	sis/Taipe
Objects	Server Uptime	0 daya, 1	8 hours, 8 minutes
 Natwork Services 		System Resource	
a 10P	System Loading		2.04 1.53
	CPU Loading	22	4,0%
 SSL VPN 	RAM (2 GB)	2000	18%
 VPN 	Flatels (182 MB)	2210	49%
lating its 192 168 100 157.	0.03		1%

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)

& Login Failure Block Settings	
Temporarity block when login failed more than	5 (C means no limit)
IP blocking period	3 minute(s) (0 means permanent blocking)
Unblocked (P	No blocked IP



Were 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

Login Failure Block Settings		
Temporarily block when login failed more the	n 5	(0 means no limit)
IP blacking penad	3	minute(s) (0 mean
Unblocked IP	IP M	ocking list

Figure 1-2. 9 IP blocking list

IP blocking list		3/1 1 1 1 1	ttopart
Date +	IP e	Left Limited Time #	Unblock
2015-05-13 12:01:37	192 165 189 243	00.02.54	P





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.

8 ResetReboot Setting		
Reset to Default Setting	🙀 💷 Keep LAN and WAN Setting 🐵 Format Heed Disk 💷 Reset to My/Could Default Setting	
Reset to My Cloud Delault Setting	DK	
Reboot System	Dr.	

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 Confim 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!

🔬 Schedule Settings	Scheduling conditions are match, the system will reboot!
Wiekly Monday • 00:00 •	
G Monthly 1 • 00.00 •	
Define date and time 2015-05-08 00 00 00 *	
	@ Zara
10 Other heme	
Run Fack Hard Disk Immediately Confirm Run	





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) Administrator Management Interface LAN Fing # HTTP # HTTPS WAN Fing # HTTP # HTTPS W

DMZ	9	Ping R HTTP R HTTPS			
1 IP Address	Action	Allow all of the following *	Ching		170 (H) (H) (H) (H)
Mark.	Notes		Manager IP Addess and Netmask	Ping	Management Interface
			+ Add J Edat × D	*L	



the characteristic strand						
Name	Lan		Interface Type	LAN		
Interface Name	eth0		Enable	NAT	•	
IP Address	152.166.1.1		Netmask	255 255 25	6.0	
Up Speed	102400 (90)	pa)	Down Speed	102400	(Rups.)	
MAC Address	00 0D 48 31 1A 96					
Speed and Duplex Mode	Auto .		MTU	1500		
5 Administrator Management Administrator Management 😵 (Pang ₩HTTP ₩HTTP8					
			E Bava			
Multiple Submet ALL			E Fave			1/1 m a a m

Figure 1-2. 14 Port 1 Administrator Management



5 WAN 1 Setting			
Interface Name	0	Interface Type	WAN
Interface Name	withit	Connection Type	Static •
IP Address	192 168 186 157	Péétrussik.	255 255 255 0
Default Gateway	192 168 186 1	MAC Address	00.0D 48.31 AF 71
Up Speed(Max. 1000Mbps.)	100Mbps • Uner Define	Dearth Speed(Max 1000William)	VEMbps • Liter Define
Speed and Duplex Mode	Auto • 100Mb/Fuit	MTU	1500
Load Balance	@ Auto		1 .
	@ By Soutte IP	@ By Destination IP	
+ WAN Alive Detection			
Detection Method	DNS CIONP * NONE	Delected IP Address	0.0.0.0
Aðministrator Management	Ping MHTTP MHTTPS		
+ Firewall Protection			
Frewall Protection Items	SYN DIDNP SUDP	Port Scan [Leg]	
6 General Setting			
DNS Server 1	0.0.0.0	CNS Server 2	8.8.4.4
HTTP Port	80	HITPS Port	443
Wan Alive Detection Period	(1~60) Seconds	Idle Timeout	60 (5~60) Minutes
		3 .5x++	

Figure 1-2. 15 Port 2 Administrator

O 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)

5 Add Manager IP Address a	f Netmask
Action	ABow
Notes.	JT Department
IP and Netmask	TH2 168 TH9 0 246 255 255 0 (24) •
Administrator Management	R Ping M Management Interface
	+ A46

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





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)

3 Clear Data	
	R Select Al
Configuration	🕷 Time Update Log 🕷 Notify Log
Network.	98 WAN Alive Detection and POPOE Log
Policy	🕷 LAN Patrixy Packet 🕷 WAN Policy Packet
Objects	
Network Services	₩ DDN3 Update Log
IDP	₩ ICP Log
VPN	# IPSic Tunnel Log # PPTP Server Log # PPTP Client Log
Logs	# Loge
Status	# Traffic Analysis Log

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)

Data Storing Time		
Notify Log	12 • Month(s)	Chings
URL Log	12 • (Monthis)	Cheuge
Software Blocking Log	12 • Monthia)	Chinge
Feewalt Log	12 • Monthis)	Chirage 2
IDP Log	12 • Month(s)	Charge
System Log	12 • Month(s)	Change
Traffic Analysis Log	14 Day(6) (Range : 1 - 999)	Chauge

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.

1 Add SMTP Server	
Sender Alias	Customere TEST_TING
Siender Name	ting@sharetech.com.tw
Mail Server IP Address	where letch come tw
Account	ting
Password	
Authentication	×
TLS	0
Delivery Domain Name	



Sender Adda	Sender Nene	Mail Server IP Address	Account	Dallyary Domain Name Q	SMTP Test	Edit / Del
TEST_TING	ting@sharetisch.com.tw	sharefech com tw	ting	0	TEST	1 23
	TEST_TING	TEST_TING trig@sharetech.com.tw	TEST_TING trig@sharetisch.com.tw sharefech.com.tw	TEST_TING trig@sharelisch.com.tw sharelisch.com.tw Sing	TEST_TING trig@sharetech.com.tw sharetech.com.tw ling O	TEST_TING traggeharefects com tw sharefects com tw ling O

Figure 1-2. 21 SMTP Server List

• SMTE	² Server Setting							
4	Sender	Server	Account	Allo	er Spern List	Domain	SMTP Test Mail	Setting
1	ting@sharetech.com.tw	sharetech.com tw	ting		0	sharebech.com.tw	Test	123
							-	
				+ A4d	Explorer User Promp	*		
					Solpt Pongt Peace Vput Recover (Img@sharetech.cov	e Mai Address	OK Genos	
						Vessage from webpa		

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 \circ K.

System Backup	
System Backup	Backup
System Recovery	
System Recovery	Choose File No file chosen
	• 0K

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 ^{• oĸ}.

Method 2:

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



5 Schedule Backup			
Enable	×.		
Schedule Backup	Every Day(s) User Define		
	Honday E Tuesday E V	fednesday 🗐 Thursday 🕷 Friday 🗊 Saturday 🗟 Senday	
	O Every Hour(s) # User Define		
	III 00:00 III 01:00 III 02:00 I	01 01 00 0 04 00 0 05 00 0 06 00 0 07 00	
	ID 00:00 ID 09:00 ID 10:00 I	E 11:00 E 12:00 E 13:00 E 14:00 E 15:00	
	III 16:00 (III 17:00 (III 18:00)	□ 19:00	
Backup Copy	2		
Backup Now	Backup Now		
		• OE	
			174 回 回 臣 [
1	Backup Time	Firmware Version	Download / Restore / Delete / Log
20	15-05-08_20-00	5.1.9	Download Restore Delete Log (2)
20	16-05-08_18-03	6.1.9	Download Restore Delete Log (41)



	2 here 192.16	81161 900	an/Carliguetion	Auto_Backing_chy?fantilate=2011-01-02_00-0	unit in the	ddata+ E			
	Logs List			1/4	1	3 ALC: 1 ALC: 1			
	Time +	Account #	IP Address #	Function Path	Doing	Content			
	01-22 10:07:20	admin	192, 168, 1, 20	Configuration > Administrator > System Setup	Save	Loger Title			
	01-22-09-57.46	admin	192.168.1.111	Configuration > Administrator > System Setup	Save	Logis Title			
	01-22 09:48:53	admin	192 168 1 20	Configuration > Administrator > System Setup	Save	Login Title			
	01-22 09-47-57	admin	192 168 1 88	Configuration > Administrator > Permitted FFs	Daleta	P and Notmask			
	01-22 09-47-45	admin	192.168.1.111	Configuration > Administrator > Permitted \$7's	Add	P and Netmask			
	01-22 03:45:20	admin	192 168 1.23	Configuration > Administrator > Permitted FFs	Edit	E.and Stetmask			
	01-22-09-42-05	admin	192,160.1.23	Configuration > Administrator > Permitted IP's	Add	P and Netmask			
	01-22-09-18-26	adoun	192.168.1.111	Configuration > Administrator > System Setup	.San	Login Title			
	01-22-09-18-06	admin	192.108.1.111	Configuration > Administrator > System Setup	Save	Loger Title			
	01-22-09-11-55	admin	192.168 1.111	Configuration > Language > Language	.Sau	Language			
	01-21 12:30:38	admin	192.168.1.111	Policy > LAN Policy > LAN to WAN Policy	Delete	Source			
	01-21 13-28-12	adress	192 168 1 111	Policy > LAN Policy > LAN to WAN Policy	Esht	Policy Name			
	01-21 13:17:38	admin	192.168.1.111	Policy > LAN Policy > LAN to WAN Policy	Add	Policy Name			
	01-21 11 17 26	adress	192.588 1.26	VPN > IPSec Tunnel > VPN IPSec Tunnel List	Dolete	VPN Turnel Name			
	01-21 09:54:41	admin	192 168 1 26	VPN > IPSec Tunnel > VPN IPSec Tunnel List	Edit	Enabled			
	01-21 09:50:45	adress	192.165.1.111	Objects > Application Software	Add	Name			
						1			
				Market and American A			110		1.1
Backup rum	0.5		Hecord So	dimiti- Autoral		Downlo	Destain	a / Deteror / Log	
2011-01-22_10	01					Llowmoad	Testore	Dates Log 1	1
2011-01-22_10	29			1.13		Download	restore	Deleter Log 2	1

Figure 1-3. 3 Backup Logs



Backup Time	Record Software Version	Download / Restore / Delete / Log
2011-01-22_10-26	7.1.13	Download Restore Delete Log [1]
2011-01-22_10-25	7.1.13	Download Restore Delete Log (2)
2011-01-22_10-24	7.1.13	Download Restore Delete Log (52)
Do you want to op	ven or save <u>2011-01-22, 10-24-58-59004, 7, 1, 13-tgz (</u> 317	NE) how 192168.1.1617 Save Save and open

Figure 1-3. 4 Backup Download

Firmw	vare Message				
Firmware Message					
and time	2014-07-25 16:15:59 Update				
Apdate time	04 • 13 •				
pdate Server					
wtomatic Download	0				
			E Save		
Firmware File					
	Mandan	Time	Restart	Download progress	Firmware Upproale



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.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 Browce. 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 Browce. It find out the file where you have just download. Then, remember to click on wwww.sharetech.com. Upgrade information you had even done before.

 Firmware Upgrade 	
Server Model	SG-100N
Firmware Version	6.1.9
Firmware Upgrade	Choose File No file chosen
Upgrade Log	O Japanés





1-4 Package

Package

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

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

Please use the code t	to apply for package or click Trial button for trialFkYSfzEwYjdWmkcuShTRcNjCrqcajHy	
Package Name	Status	Note
WFT	Enable	Wireless
** Free trial is for 15 d	tays **	

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)

🖲 La	anguage		
® E	English	Traditional Chinese	Simplified Chinese
			12 Zave

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.

Sender Account		ling@sharetech.com.tw 🔹 🥥		
		Sender Address SMTP Server Account		
cumers 2	eurij	Imp@sharelecti.com.tw_sharelecti.com.tw_kmp		
Recipient		glnwwor=1004@gweil.co=		
Try to ser	id times	1 (1-5)		
Mark		Dam		ail Subject
10	1. WAN Disconnection		WAN disconnect	as poulers
	2 DONS Update Failed		DONS fail	
10	3 SLB Disconnetion		SLB disconnect	
	4 Freeal Protection (SYN, ICMP,	UDP, PortScarij	Firewall protection	
	5 IDP Attack Log		IDP Log	
	6. System Log		Admin log	
8	7. Administrator Login Failure Even	i	Admin login fail	
	IL SSL-VPN and Web Authenticatio	m Login Failure	Auth login fail	
- 10	9. Software Upgrade		Software upgrade	
-8	10. HDD Free Space Too Low, Usi	age over 90% or Bad Track	HOD State	
- 10	11. Schedule Backup Configuration		Auto Backup	
-	12. Collaborative defense		Cefense	
	13. Database Anomaly		Database Anomaly	
	54. AP Management (Ap managem	ent requests, Connect status abnormal)	AP Management	
- 10	15 IPSec Disconnection		IPSec discontect	

Figure 1-6. 1 Notification



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

1 20	from		Subject			Received	Site
12 . 12	rootigei	haretech.com.tw	经条款件按算法包			2010/00/19 13:88	14.73 KE
D A	居 ,展Ryy	49	NE: (基础课知) StateTech - 改築機関			2015/06/19 12:57	2.78 KB
2 会	TEST_T	inia.	+ 2015-05-19 12 45 + Admin kog			2015/05/19 12:45	2.40 kd
g Prom : TEST_TON	6+ m	ts : brg@shwetech	anulu •		1		
Subject:	= 2	2015-05-19 1	2:45 = Admin log				
			Admin Log				
Time	Admin	IP Address	Function Path	Action	Events Contant		
05-19 09.18:25	admin	192,108,188.1	Configuration > Ap Management > AP Management Setting	Save	Enable Ap Management		
	admin	792,168,168,1	VPN > IPSec Turnel > VPN IPSec Turnel List	Add	Enotied		
05-19 09:28:53							

Figure 1-6. 2 notification mail-1

din Xi	12	0		1.0		22		08 1 ±1+ 7	+ 188 21 . 4 . 5	4-
MB	= 20	15-05-18 12:45	= Admi	n log 😑 🏢	19E +					e 1
收件程(1) 已加星號	-	TEST_TING INTE FX.(+)			1220	27.121			12.45 (5 全49前) 〇	
鐵份		Time	Admin	IP Address	Agri	Function Path	Action	Events Coolent		
		05-18 09 56 27	admin	192,168,168,1	Network Services >	DHCP Services > LAN DHCP Server	Save	IP Bange 1		
		05-18 09:57:24	admin	192.168.188.1	Network Services >	DHOP Services > LAN DHCP Server	Save	IP Range 1		
		05-18.09.58.05	admin	192.168.188.1	Network Services >	DHCP Services > LAN DHCP Server	Save	P Range 1		
2		05-18 10 18:27	admin	192 168 185 1	Network Services >	DHCP Services > LAN DHCP Server	Save	IP Range 1		
		05-18 10 18:51	admin	192,168 186.1	Network Services >	DHCP Services > LAN DHCP Server	Save	IP Range t		
		05-18 10 30 54	-admitt	192.168,188.1	Network Services >	DHCP Services > LAN DHCP Server	Save	IP Range 1		
		05-18 10:31:39	admin	192.168 188.1	Network Services >	DHOP Services > LAN DHOP Server	Save	IP Range 1		
		05-18 10:32:25	admin	192.168.188.1	Objects	> Address > LAN IP Addr.	Add	Computer Name		
		05-18 10.32.47	admin	192.168 188.1	Network Services >	DHCP Services > LAN DHCP Server	Save	IP Range 1		
		05-18 10:33 18	admin	192 168 188 1	Network Services >	DHCP Services > LAN DHCP Server	Save	P Bange 1		

本信件可能包含·深坚何思想包有深公用 執密違則。 李指定之些计者。 路径复集,虚虚临刑用本信件不容, 过算研修此信件! 如为指定中作者, 置握要件提制件中本公用之室常得否思 個人切样。不得任意情能流得着。 世間在行機能本創件之則僅與凝重症之完全性。 已共同普重迫更充全叫 假道 性理教任。 Please be advised that this email message including any attachments) contains confidential indemails on sequely privileged. If you are not the intended recipient, please destroy this message and all attachments from your system and do not hother collect, process, or use them. If you are the intended recipient, please potent the confidential indep personal information contained in this email with due cass. Any unauthorad use, disclosure or distribution of the message in whole or in port is shortly prohibited. Also, please self-itspect attachments and hypefieles contained in this email to ensure the information security and to protect personal information.

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 [•] Starch, you will see the result below of the screen.

Search Noti	ification Log			
)ata	2012-09-30 🔤 00:00	• - 2012-10-19 23-59 •		
vert	ALL.			
Recipient:				
Records / Page	10 -			
			(a	
			a sater	
Notification	Log		3/7 1) 💷 (e) (e) (e)
	Date +	Event. e	Recipient	Content
201	12-10-11 16:30 17	CMS (Client management requests, Connect status abnorms) Backup failed, Restore failed)	mandy@sharetech.com.tw	
201	12-10-11 14:33 64	CMB (Client management requests, Connect status almornal, Backup failed, Restore failed)	mandy@sharelech.com.tw	Ø
20	12-10-11 11 18:05	CMS (Client management requests, Contract status abnormal, Backup failed, Restore failed)	mandy@sharetech.com.tw	
20	12-10-11 11:00-26	CMS (Client management requests, Connect status abrormal: Backup failed, Rentore failed)	mandy@shawlech.com.tw	12
201	12-10-11 10 57 03	CMS (Client management requests, Contect status abnormal: Backup failed, Restore failed)	mandy@sharetech.com.bw	
201	12-10-11 08:12:06	CMS (Client management requests, Connect status abrormal, Backup failait, Restore failed)	mandy@sharehech.com.tw	0

Figure 1-6. 4 Notification Log

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

		CMS連線狀態異常通知		
時間	型鍵	名稱	Mac	IP
2012-10-11 16:26:02	HiGuard SOHO	higuard_146.164	00.12:0E BD 8D A0	192.168.195.146
2012-10-11 16:26:17	UR-500A	UR_1.164	00:0D:48:2C:32:AD	192.168.195.164
2012-10-11 16 26:03	HiGuard SOHO	higuard_26.164	00 12 OE BD 8D 98	192 168 195 166





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 <u>Connection Test</u> in order to check whether settings are right or not. (Figure 1-7.1)

Share Tech	ShareTech	ten OK I	OK D	2 4800 17 10 10 10 10 10 10 10 10
Configuration Date & Tree Configuration Configura	Configuration > Backup & Mov Pate Nacker Data Move & Backup Destination Backup Nethod IP Address Folder Nerre	Sarta 102 168 1.4 SHARE		
MyCloud Setting	Destary	lore		
 Netzezh 	Panawarti	jacente .		
· Policy	Californ Passworth		Connection Text.	
Organia	A. Backup Setting		50 C	
· Network Services	10 Schedulet Barton 0100 •			
· IDP	I Send Backup Fissult Notification			
· SSL VPN	Last Backup Terre			
. VPN	2000-00-20-00-30-27 > Sparrel Time - 2 ee	manah, Rende Avalable Space (32)499	MEDyten	
a Turis	Sathap New			
	The Backson Dame			
 Logi 	Sector Lookan			
@ Slither	The second second second			
	11		I Save	

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)

From	Subject	Received	Site:
TEST_TING	2015-05-20 Data Export Results	2015/05/20 09:35	1.45 KB
TEST_TING	2015-05-20 Data Export Results	2015/05/20 09:33	1.58 KB
vG + ∰r To : ting@alwret	hande •		
2015-05-20	ata Export Results		
	192.168.1.4		
	SHARE		
	574091 MBytes		
	148R02 MBytes		
	025490 MBytes		
	5 seconds		
Data Export Deatil			
2018-05-07 2018-05-08 2015-05-12 2018-05-13 2015-05-17 2015-05-18	015-06-09-2015-05-10-2015-05-11 015-05-14-2015-05-15-2016-05-18 015-05-19		
	From TEST_TING TEST_TING S • @ To iting@utweter 2015-05-20 D 2015-05-20 D 2015-05-10 D 2015-0	From Statest TEST_TING 2015-05-20 Data Export Results TEST_TINO 2015-05-20 Data Export Results 2015-05-20 Data Export Results	From State Receive TEST_TING 2015-05-20 Data Export Results 2015/05/20 09.13 TEST_TING 2015-05-20 Data Export Results 2015/05/20 09.13 St • Tring@dawsteth.com/se • 2015/05/20 09.13 2015/05/20 09.13 2015-05-20 Data Export Results 2015/05/20 09.13 2015/05/20 09.13 192.105.1.4 SHARE 2015/05/20 09.13 2015/20 09.13 192.105.10 SHARE 2015/20 09.13 2015/20 09.13 192.105.10 SHARE 2015/20 09.13 2015/20 09.13 2015/20 09.13 SHARE<



	Information as below. (Figure 1-7.4) (Figure 1-7.\53)
9 Backup Setting	
Scheduled Backup 01.00 •	
R Send Backup Result Notification	
Last Backup Time	
(Backup Mosc) 0 0 0 0 0 0 0 0 0	
	Figure 1-7. 3 Backup Now
9 Backup Setting	Figure 1-7. 3 Backup Now
Backup Satting	Figure 1-7. 3 Backup Now
 Backup Setting Scheduled Backup 01:00 • Send Stackup Result Notification 	Figure 1-7. 3 Backup Now
 Backup Setting Scheduled Backup (01:00 •) Send Backup Result Notification Last Backup Time 2015:05:20:00:13:19 = Spent Time : 5 seconds, Remote Available Space : 325439 MBgtes 	Figure 1-7. 3 Backup Now

Figure 1-7. 4 backup completed

Backup Item: Flow Analysis (Figure 1-7.6)

Backup Item
 Flow Analysis

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 cli	ick on Access to External Storage, you will see data items that you have ever backup
(Figure 1-7.7)	
Current Mount Item Item Flow Analysis	Year Month
Access to External Storage Unmount Remote Data	
Item Flow Analysis © 2015_05	Year-Month
	Mount Remote Data
	Figure 1-7. 6 Data Mount
Current Mount Item Item Flow Anthysis	Ver Month 2015-05
Access to External Storage Unmount Remote Dat	<u>à</u>
	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)	
Current Mount Item Item Flow Analysis	Year-Month
Access to External Storage Unmount Remote Da	na

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.

Name	Version	Last Check Time	Auto Update	Function
URL BlackList Cotabase Update	20	2015-01-23 16 13 51	8	Check Now
IDP Signature Update	1.0	2015-05-12 18 18 14	*	Check Now



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.

Name	Version	Last Check Time	Auto Update	Function
URL BlackList Cotabase Update	2.0	2015-01-23 16 13 51	0	Check Now
IDP Signature Update	1.0	2015-05-12 18 16 14		Check Now

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





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



CMS Setting	
Enable	2
Made	Ciert © Setas
6 Client Setting	
Server	111.252.72.198
Alian	848
Update Time	1 Nutes
Administrator account	admin . If you don't designated management account, the server-side will not be allowed to log into this device
	E 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

CMS Setting	
Enable	2
Mode	Clert © Seter
6 Client Setting	
Server	190. 168, 1. 163
Alian	bbb
Update Time	1 m Minutes
Administration account	admin • If you don't designated management account, the series side will not be allowed to log into this device
	III 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)

CMS Setting	
Enable	8
Mode	0 Client ® Server
 Client profile is automatically 	backed up to the machine
Enable	
	III Save.

Figure 1-9. 4 CMS server



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

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

nt request list					Bac
The last request time	Model	Mac	Alias	10	Action
2013-03-01 17 59 47	UR-838	00 60 E0 52 38 F5		220 132 217 122	Accept Delete

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

5. Set up group(Figure 1-9.7)

 CMS Setting 		Back
Model	UR-938	
MAC Address	00.60:E0:52:38:F5	
Alias	222	
Group	test1	
Auto Backup	Ø	
	E fave	





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



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

HiGuard	System %	Network	Log and Report	
a System	System / Overview	i.		Cogout
Overview	Mode Selection			
🔆 Firmware Upgrade	General Mode		₩AP Mode	
Restart Device			Apply	
	System Information			
Admin Password	Active Connection		18	
Web Access	Memory(Total/Used) Firmware Version		62080 KB F 48,8% 1,2:20130717	
🧕 Time Settings				
m Config Manager				

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

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

HiGuard	System New	Log and Rep	port				
a Network	Network / AP Manager	ment			Cogou		
Dverview	General Setup				-		
Configuration	Enable AP Management	iet AP					
AF Management	Manager IP	192.168 189.150					
Wireless	QOS Setting						
4. IPV6	Maximum Limit QO5	Up Speed D	Kbps	Download Speed	Kbps		
	VLAN ID Setting						
	Enable VLAN ID VLAN ID	(1-4094)					
	DHCP Relay				0		
	DHCP Relay DHCP Server Address	172.16.7.105					
		8	Apply				

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

Ping Watchdog		SNINP Agent	
Enable Firg Watchdog	0	Erable SHUF Agent	0
IF Address To Ping		SAUP Community	public
Prig Marcal	300 excords	Civiact	
Startup Delay	300 secords	Location	
Fallers Court To Reboot	3		
Web Server		SDI Server	
Use Secure Connection (#TTPS)		Enable SSH Server	
Secure Server Port	2442	Server Port	22
Server Port	00	Trutle Fast word Authoritzation	*
Seasion Treasul	tt minutes	Aufteriesd Keys	Tett.
Telket Server		INTP Client	
Esabe Teinet Server	0	Enable WTP Client	0
Server Port	25	NTP Server	
Dynamic DWS		System Log	
Enable Dynamic DVD	10	Evalue Log	0
most Name		Enable Remote Log	
Daemane		Remote Log IP Address	
Password	0 to	or Remaining Part	614
Denics Discovery		UTH Clant	
Exatle Discovery	×	Enable UTM Client	90 102 MIR 183 10

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)

Provide and the second s		A DECK WITH A DECK MANY	- BRANCE IN ALL COMPLEX
Physical Interface	etho	MAC Address	00.00.48.21.14.96
IP Address	152 168 189 153/24	Broatrast	152.168.189.255
DHCP Server Setting :			
Start Address of IP Range 1	192 168 189 1	End Address of IP Range 1	192 168 189 254
Start Address of II ² Range 2		End Address of IP Range 2	
Primary DNS	168.95.1.1	Secondary DNS	168 95 192 1
Primary WiNS		Secondary WINS	
Loose time(minutes)	3600	Max (dase time)minutes)	3600
Default Gateway	192.168.189.150	Enabled	8
Domain Name	internal example.org	100	





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

AP Management Requests

AP Bassagers	ent Setting Ap Blan	agentent								
Ap Managemen	User defined said s	1011								AP Management Requests G
Activity	Delivery Status	Allas	19	Channel	S-SID	Enable WiFi	Online Users	Flow	v (byte)	
Test 1										
HE HE WE SHE	OHO Delivery									
a ()	0	test1	192,168,189,174	1	Hgumd_Te	0	5	Up 432.12./s	Down	12.02 K /s
□ B:AF-200	Delivery									
	0	test2	192.168.196.69	Auto (11)	AP200 Test	0	0	12p : D /v	Down :	D /6



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)

AP I	lanagement S	Ap Managa	ment					
Ap Mana	gement							
	Activity	Delivery Status	Allas	IP.	Enable WIFI	Channel	Online Users	Flow (byte)
SSD Hg	used.							
Datio	iand							
	0	÷2	潮試中文	192 168 169 150	3	Auto (1)	1	Up: 3.73 K/s Down: 6.92 K/s
GD . sha	retech							
C gan	inetech							
	0		249	192 168 168 249	0	6	2	Up. 3.8 K/9 Down : 6,21 K/s
	0	0	248	192 168 186 248	0	1	11	Up 58K/s Down 779K/s

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)

68.388.1.9443 ···					S Aller-0192 168 188 1	0441/Yingnas/Configuration	ully_Um_Listy	N 12 1				
						😹 💓 7/192.168.188.1 644	OFregran/Configuration/Ap_Dis	e_Letalg/well363477079_04	2			
	ShareTech						1/2	1 00 44 4 10 10	ria			
ShareTech						1P	MAC	Login Time	SE 198 10			
							40/10/89 10:93 51	189 10 93 51 2013-05-13 09 44 29				
				-110		192.168.188.00	b4.07.19.cf.b2.85	2013-05-13 07.58 33				
	1000 121 2					192 168 188 263	74:10:63 79:68:10	2013-05-13 08 15:33	1.00			
Connigur	ation > A	p Management				192.168.188.58	84.46.65.92.05.17	2013-05-13-00 19:33				
in the second	WARDED-COM	Second In the second	and the second second			192.168.188.201	74 ft1 5d 79 2f bc	2013-05-13 08:45:29				
	even femen.	semal whereauside	mem			192.168.188.206	68.09.27.9b.ff.f6	2013-05-13 08:35:32				
Ap Mana	gement		1110 2001		-	192.168.188.211	f8.db 77.9f.b1.bd	2013-05-13 08:30:32				
the second second second	Activity	Delivery status	Anas	112	Enat	192 168 188 205	28 e0 2c.bc.02 77	2013-05-13 08 37:32				
	TAG					192 168 188 218	64.20.0c.6f.31.b2	2813-05-15 10:26:29				
L1 is Hig	uard		1. 14029-12-14-5			192 168 188 53	bll ee 45 a7 1e 61	2013-05-13 09 10:32				
		140	潮蚀中文	192 168 189 150					0/8			
SSID the	tritech .					A Online User grap	h					
□ (≘ Stu	webech.					Today Online User	graph O Search history	online user graph	2			
	0		249	192.168.108.249		8		1 10	/6			
		0	248	192,168,188,248		0	11	10p 5.8 K /s Down : 7.7	9 K /s			

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.





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)

· SSL Certification Impl	m
File server key	Choose File No file chosen
File server.crt	Choose File No file chasen
File Internediate Certificate	Choose File No file chosen

Import

Figure 1-11. 2 import SSL Proof

 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)

# SSL Proof Set	
Two-letter Country Codes	(ex: TW) Required
State Or Province	jex TAIWAN) Required
City	jax : TAIPEI) Required
Organization Name	(ex: TWCA) Required
Unit Name	(ox: IT + SYSTEM) Required
Domain Name	(ex., www.sample.com.tw) Required
Application Personnel Email	jex : sample@mail.com) Required

Downlode file server.csr+ server.key

Figure 1-11. 3 Enter SSL Proof

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

Acces			Contract the state		
	-	-			
	V.N	ail	rve	r	
	ÝN	ailsse	erve	r	
	ÝN	Administrator Lo	erve	r	
	Account	Administrator Lo	erve	r	





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"

10 MyCloud Setting			
Http: Port Setting	5000	Eruble Http:	
Imps Port Setting	8888	R Eruble Https	
 Restart MyCloud service 			III Sava
Restart MyCloud service	Restart		
· Reset MyCloud admin passw	ront		
Reset MyCloud admin password		0 OK	

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)

ne 🔿		9:	
All files	new 1		1 Personal
Shared with you	🕮 Name 🛦	Tire Istrabilies	42 Users
Shared with others	documents	Q.All Institution	E Admin
Shared by link	music	3.8 MB 20 days	ago
	photos	sto3 kill 20 thigh	ego
	1 Period	4.2 518	
0			
WebDAV			
https://192.168.180,157.8886/verbs			
Use this address to access your Res. In a WebDAV			





Personal

& Personal
🐇 Useri.
E Admin
() Logout

- 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)

You have used 4.2 MB of the available 432.8 GB Password Current parsword Full Name advar.	
Password Current password Full Name admin	
Current persword Press paceword (Change paceword)	
Full Name admin	
admini	
Language	
English •	

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)

Apps 🔿								9	===++
+ Add Group	Login Nemn	1	annene i	Groups	۰.	Create		Sect	Marta
Everyone (7)	Osename	Full Name	Password	- Groups		Grenat Admin	Quite		Left Legin
	admin	admin		admin	10	Group Admin	• Defau	n •	16 minutes ago
AGRIVITE (2)	lester	lester	++++++	Sales	*	Group Admin	Defini	n •	2 hours ago
text (2)	Iois :	lois		admin test		test +	Defeu	a •	2 hours ago
Engineering (1)	peter	peter		Groups	×.	Group Admin	Defau	n •	t hours ago
Others (1)	randy	randy		Engineering		Group Admin	• Defini	n •	19 minutes ago
Sales (1)	tiesti	1est1		test		Group Admin	5 GB	•	3 hours ago
	tripodworks	tripodwori		Others		Group Admin	Detau	in 🔸	12 hours ago
• Defast Quota Unitaritad •									





Add a New Group(Figure 1-12.8)

Username	Pull name							
		-Hanaword	Grinupi		Sing Admin	Quinta		Lastinger
admin	admin	******	admin	۰.	Greep Admin 🔹	Default	12	18 minutes ago
lester	løster	******	Sales		Group Admin 🔹	Detault		19 days ago
lois.	lois.		admin		Group Admin 🔹	Default		15 days ago.
randy	randy		Engineering		Group Admin 🔹	Default	34	15 days ago
tripodworks	tripodworks		Others		Group Admin +	Detault		19 days ago
	kester kois randy tripodworks	lester lester lois lois randy randy tripodworks tripodworks	lester lester lois lois randy randy tripodworks tripodworks	lester lester sommer Sales admin admin randy randy sommer Others Tripodworks sommer Others	lester lester	lester lester source Sales Croup Admin lois lois renup admin Croup Admin randy randy renup Engineering Group Admin tripodworks tripodworks seeson Others Sinoup Admin	lester lester senser Sales sensup Admin Default lois lois veenee Engineering Group Admin Default randy randy oeeee Engineering Group Admin Default tipodworks tripodworks seeeee Others Siroup Admin Default	lester lester sources Sales Group Admin Default • lois lois randy occess Engineering Group Admin Default • randy randy occess Engineering Group Admin Default • tripodworks tripodworks sources Others Group Admin Default •



No. 8 + Add Group ----• Grante Date: 1 1011 Tearch Streets sant Legin Quota Everyone (d) Admini (2) Engineering (1) Others (1) Sales (1) test -

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

+ Add Group	Cogin Norma	Per	BWDY II	Groups		Create			Starchil	Litera.
Evenue (7)	thername	Full Name	Painword	Groupe		Group Admin		Quita		Lastingin
	admin	admin		admin	*	Group Admin		Default	•	11 minutes ago
Admins (2)	lester	lester		Sales	2	Group Admin		Default		2 hours age
test (2)	lois	licis	******	admin. test		test •		Default		I hours ago
Engineering (1)	peter	peter		Groups	-	Group Admin		Default		\$6 minutes ago
Others (1)	randy	randy		Engineering		Group Admin	•	Defmitt	•	54 minutes ago
Sales (1)	text1	text 🖉		test	*	Group Admin	+	5 GB	·	3 hours ago 👘
	tripodworks	tripodworks		Others	÷	Group Admin	*	Default Unimited		12 hours ago
								5 GB 19 GB		
								Other	_	



Apps								٩	<u>9</u>	ann e
+ Add Group	Login Name	1	eroward.	Groups	•	Create			Teleficiti	Junes .
Everyone (f)	Quename	full Samè	Parrieded	009489		Group Admin		Quinta		Linit Light
and minutes of the	admin	admin		admin		Group Admin	$ \Psi $	Default		15 minutes ago
Address (2)	lester	letter		Sales	÷	Group Admin		Default	*	15 minutes ago
test (2)	fois	los /		test, admin		Group Admin		Default	*	15 days ago 🛛 🗑
Engineering (1)	randy	randy		😸 admin		Group Admin		Default	•	15 days ago
Others (1)	tests	test1		i test	_	Group Admin		5 68	•	17 minutes ago
Sales (1)	tripotivorks	tripodwork		Others	ing -	Group Admin	*	Default	٠	9 hours ago
				🖂 Sales						
				+ add group	£					
7/45										

■ 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.

Apps									
+ Add Group	Lopin Norte	Pa	itzworff.	Groups	*	Create		Search	29453
Everyone itil	Opername	Pull Name	Password	Gringer		Conicp Admin	Quinta		Last Light.
(Andrease of the	admin	admin		admin	\mathbf{t}	Group Admin +	Default		15 minutes ago
Admin. (2)	lester	lester	*******	Sales	*	Group Admin +	Default		15 minutes ago
14:52 (Z)	3015	lois 🖉		test, admin	\mathbb{R}^{n}	test -	Default		t5 days ago 🛛 🗑
Engineering (1)	randy	randy	*******	Engineering	- 4	Engineering	Default		15 days ago
Others (1)	test1	testi		test	10	Others	5 G8		17 minutes ago
Sales (1)	tripodworks	tripodwork	5	Others	*	i soies	Debuilt	•	9 hours ago



Admin



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

Depend on your	HDD usage. Default is 320G
----------------	----------------------------

HDD Usage

Figure 1-12. 13 HDD usage

File handling (Figure 1-12.14)

🕕 maximum Upload possible: 2 GB

Harmon uniout cmi 2/08	imus, nontible 7 GBI
------------------------	----------------------

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)

Apps			9.) poste
Upload Logo				
Login Lago	Select	(Recommended image sizes : 252 x 140 pixel)		
Logned Logn	Select	(Recommended image sizes : 62 x 34 pixel)		
Share Link Lego	Select	(Recommended image sizes : 150 x 34 poel)		
Page icon	Select	(Recommended image sizes : 32 = 32 pixel)		
Page Icono Pacl iPhon	ei Select	(Recommended image sizes : 128 = 128 prixel)		

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

🔿 Files		٩	
All flat	now 🚉		
Shared with you	- 62 - Norre 🔺	Size	Wodified
Shared with others	💋 documents 🖉 Second	:147.10	seconds ago
Shared by link	music Sharn with user or group .	30.00	21 days ago
User Litt	photos et Share lok	013.60	21 days ago
	Password protect Allow Public Option Set expiration date	. 4.4.172	

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

	Sharotuch		+ Dewnlead
#			
8	Marror A	51pe	Modéer
4	0429-770x2200acmer (r)	10730	seconds ago

Figure 1-12. 18 Share Link Logo



Page icon (Figure 1-12.19)

	*	TARRENAL PARTY	9 MI 80 80 1	
CABD	Hps://		\$	3
S Apps			٩	
Upload Logo				
Login Logo	Select	(Recommended image sizes : 252 x 140 pixel)		
Logined Loga	Select	(Recommended image sides : 02 x 34 pixel)		
Share Link Logo	Select	(Recommended image stees : 150 x 34 pool)		
Fage ILOO	Select	(Recommended image sizes : 32 a 32 pixel)		
Rape icon@Rad./Phone	Select	(Recommended image sizes : 128 n 128 pixel)		

Figure 1-12. 19 Page icon

■ Page icon(iPad, iPhone)

Background Color (Figure 1-12.20)

Background Color			
Lign BackGround	#SEDBEE	#17A48E	(Example: #31b5cit)
Logined Logo BackGmund	#itteco		(Examplie: #31b5cil)
Savo			

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)

Background Color	
Login Backdround #E9EE5E 🔤 #BE1717 💓 (Example: #3105cil)	
Logined Logn BackGround #4931CD	
Save	

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)

Upload User M	anual	
Upload User Manual	Select	(File extension: .pdf)
Uploaded User Manual	MyCloud User Manual pdf	Delete

Figure 1-12. 23 Uploaded 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

ine 🦳		Q.	
All files	L Group Extend		
Shared with you.	admin (2) Username Full Name		
Shared with others	admin admin Aces 104s		
Shared by Ink	Engineering (1) Username Full Name		
Uper List	a randy randy and the standard stand standard standard stand standard standard stan standard		
	Username Foll Name tripodworks		
	IF 🚜 Sales (1) Username Full Name		
	& lactor lester		
	Username Full Name		
	👗 testi testi		
0			

Figure 1-12. 25 User List

Sharing



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



🔿 ne			٩	
All files	new 1			
Shared with you	C Name A		310	Madified
Shared with others	documents	Preset.	2.40	last months (
Shared by link	music Branz with Loor or granip		3.8 M0	21 days ago
	photos Ø Share Ink		94340	21 dayi ago
	Property 102 368, 196, 157, 8000 geophic prophery Paceword protect Set expiration date	vice-files&t-a0fet	4216	
			21	
0				







inter 🔿 Res		9
All films	🖶 Now 主	
Shared with you	E Hama 🛦	Size Medified
Shared with others	documents.	it is int mooth
Shared by link	music place with tase or group .	2.4 MB 21 days ago
	photos	603 kB 21 days ago
		A2.60
0		




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

Default: Disable S Files 8 All files. 4 New 1 Shared with you 3104 Montified 13 Name A Shared with others 8 mars 248 last months documents Shared by link music 3.8 M0 21 days ago Share with user or group 943.44 21 days ago photos R Share Ink https://192.168.186.157.0086/pa Set expiration date 0



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





Figure 1-12. 32 Set default expiration date



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



Chapter 1 : Configuration

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)

🔿 Res				٩	
All flat	🕈 New 🛓				
Shared with you	B Name A			See	Wodified
Shared with others	documents		<	142.60	1 hour ago
Shared by Irw	music	place with user or group		3.0 Mit	23 days apo
Unjer Litt	photos	lois 🖉 can share 🥳 can edit 🔻	*	4014	21 days ago
	110eg	D Share Ink		4.4.115	
0					







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



Chapter 1 : Configuration

inter 🏠			٩	
All flat	🖷) New 土			
Shared with you	B Nome A		Sim	Modified
Shared with others.	documenta	< 2000	142.40	1 hour ago
Shared by Ink	bure with user or aroun .		23.0 MIC	23 days apo
User List	photos lester 🖉 can share 🗟 can edit *	¥	1443.44	21 days ago
	Share Ink		4.4.115	
	<u>.</u>			
0				

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



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



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)

in Files		(A)	
All films	New 1		
Shared with you	10 Nome A	Size Mudifier	
User Lin	📖 documents 🖌	Downcast 1111 15 days ago	×
	documents (2)	< 3.3 MD 15 days ago	
	music	3.6 MB 15 days ago	
	photos	nos kiu — 15 days ago	
	4 Surface	3.0.446	
A	deruttp/apps//lim/w		

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)

📥 ны			٩	
All files	🔹 New 🗶			
Shared with you	B Nove .		Stee	Modifier
Shared with others	documents	<	147.68	2 hours ago
Shared by lick	Lois shared documents	< Sum	001640	10 days ago
	iiii music		3.5 MB	16 days ago
	music (2)	< anti-	3.5 MII	23 dayi ago
	photos		663 68	16 days ago
0				

Figure 1-12. 39 All files

Shared with you (Figure 1-12.40)

🔨 Files		9.	
ul Man	• 2.		
Diared with you	hamir 🔺	Shar	n Terrar
hared with others	documents 🖌	÷ 20 m	inut Uniter
hared by link	music (2)	< 10100 1918	inutes ago



Chapter 1 : Configuration

Shared with others

🔿 Filis		(
All files	• >	
Shared with you.	Nami 🔺	Silvard Brite
Shared with others	Lois shared documents	< Dennel with carefy 10 days ago
anarea by sink		
0		



8

Shared by Link

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



Figure 1-12. 42 Shared by Link



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:



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.

Name	Lan	Interface Type	LAN
Interface Name	othe	Enable	NAT •
IP Address	192 168 189 150	Netrraniii	265.255.255.0
Up Speed	102400 (POps)	Down Speed	102400 (Hitspa)
MAC Address	00-0D-48-31-1A-96		
Speed and Duplex Mode	Auto 🔻	MTU	1500

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	Notes
	(Bytes)	
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	1492	
SNAP, PPPoE		
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)

ARP Spoofing Prevention
 Enable Every 30 Seconds(range 1-600), send 3 times in a row

Figure 2-1. 2 ARP Spoofing Prevention

What Is ARP Spoofing²?

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)

Administrator Management
 Administrator Management
 R Ping E HTTP # HTTPS

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."

Address.	192.168.1.1	Netmank	255 255 255 0		
erface	# LAN				
WAN Interfac	os IP / Operation Mode Setting				
WAN Interfac	IP / Operation Mode Setting	Operation 1	dože	* NAT © Routing	

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

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

1 Erlit Maltip	de Subnet					
Name	Marketing D	lepit.	Bind	8		
IP Address	192.168.2.1	0	Netropole	255 255 255 0		
Interface	O NONE	* LAN				
WAN Insert	lace IP / Operation Mode Settin 192.168.186.157	g	Operatio	on Modie	● NAT © Routing	
WAN_Z			Operation	on Mode	I NAT	
			W Save			

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



Completed

iple Subnet ALL *						579. mi in (b)
Name	Bind	Interface	IP Address	Normank	WAN Interface IP / Operation Mode	Edit / Del
Engineering Dept.	٥	-	192.158.1.1	266 266 266 0	WAN1: 152.168.165.167 (NAT) WAN2: (NAT)	/83
Marketing Dept.	0	CAN	192 168 2 1	286 265 256 0	WAN1 192.588.186.157 (NAT) WAN2 (NAT)	/8
Sales Dept	0	LAN	192 168 3.1	255 255 255 0	WAN1 192 168 186 157 (NAT) WAN2 (NAT)	18
Purchasing Dept	0	LAN	192,368 4 1	266 266 256 0	WAN1 192 168 186 157 (NAT) WAN2 (NAT)	/8
Accounting Dept	0	LAN:	192,160,5,1	255 255 256 0	WAN1 192 168 186 157 (NAT) WAN2 (NAT)	12



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



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 <u>Custom Define</u> 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.
 - 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 <u>Custom Define</u> 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}.



S WAR 3 Sutting			
Interface Name	0	Indeeflab er Typer	WAN
Interface Name	etrt .	Connection Type	Static •
IP Address	192.168.186.157	Netmask	255 255 255 0
Default Gateway	192.168.186.1	MAC Address	00 0D 48 31 AF 71
Up Speed (Max. 1000Wbps.)	100Mbps • User Defirm	Down Speed(Max. 1000Mbps)	100Mbps • User Define
Speed and Duplex Mode	Auto • 100Mb/Full	MTU	1500
Load Batarice	* Auto	Manual	1 (• •)
	@ By Source IP	© By Destination IP	



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.

5 WAN Alive Detection				
Detection Method	O DNS O ICMP # NONE LIKE	Detected IP Address	0.0 0 0	
Administrator Management	Mining Wintte Winttes			

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)

1748	2011-05-02	00 00 V	- 2015-05-21	23.68 *					
per	Port Scan	•							
ankes (P									
ctim IP									
tim IF		1				Bearch			1/1 (4) (4)
.tim IP	Time			Турн	Protocal	Bearch Port	Interface	Attacker 1P	1/1 at (a) Victim IP

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.

\rm 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

a sening	and a first second s		
DNS Server 1	8585	DNS Server 2	8.8.4.4
HTTP Port	80	HTTPS Pod	443
Wan Alive Detection Period	5 (1~66) Seconds	ide Timeout	60 (5~60) 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)



(b) Interface Config (The Interface you	want to change, you must first change its type	to OFF.)		
Port	Port 1	Port 2	Port 3	Port 4
Interface Type	LAN	WAN1	WAN2 *	DMZ +
Interface	949w	eth1	eth2	eth3
		III Jave		



15 WAN 2 Setting			
Interface Name	0	Interface Type	WAN2
Interface Name	+0n2	Convector Type	OFF .
IP Address		Netmask	266 266 266 0
Default Gateway		MAC Address	00 0D 48 31 AF 72
Up Speed(Max, 1000Mbps)		Down Speedt Max. 1000Whps.)	
Speed and Duplex Mode	Auto *	MTU	1500
Load Balance		C Manual	(1) ×
10 WAN Alive Detection			
Detection Method	O DNS WICMP ONONE	Detected IP Admiss	168.95.152.1
Administrator Management	R Ping HTTP R HTTPS		
Firewall Protection			
Firewall Protection Items	IS SYN I ICMP I USP I Put	t Scan Lea	
		E Save	



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 setting.

10 DM2 Setting							
Narras				Interface Type	DMC.		
Interface Name	eth3			Errabie	NAT	•	
IP Admiss	192 168 18	7.2		Netmask	255 255 256	5.0	
Up Speed	102400	(Khps)		Down Speed	102400	(OCbps)	
MAC Address	00.0D.48.3	1.AF.73					
Speed and Duplex Mode	Auto			-MTU	1500		
5 Administrator Management Administrator Management 8	é Ping & HTTP & H	1TTPS					
			Save				
Multiple Subset							171 (1) (1) (1) (1)
Name Bind	P Address	Netmank		WAN Interface IP / C	Operation Mode		Edit / Del
			+ 161				

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.



Transparent Routing

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)





Figure 2-1. 17 Transparent Bridge





Figure 2-1. 18 Transparent Routing / Transparent Bridge

Compare	Transparent Routing with Transpa	rent Bridge		
Transparent RoutingTransparent 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

Solut'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.

WiFi Setting	
Country	TW •
Network Mode	802.11 G/N mixed mode •
Frequency	Auto Channel
Enable WiFi SSID1	
Enable WiFi SSID2	
Enable WiFi SSID3	
Enable WiFi SSID4	
Enable WiFi SSID5	
Enable WiFi SSID6	
L	E Save

Figure 2-1. 20 WiFi



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

Please note systme will reboot after modify

Port	Port 1	Port 2	Port 3	Port 4
Interface Type	LAN	WAN1	WAN2 *	DMZ +
Interface	40%D	with 1	eth2	eth3

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

5 LAN IPV6 Setting		
Enable		
IPVE LAN (eth0) IP		(mr. 2001 288:1111-254-64)
IPV5 Auto Configuration	C Start # Stop	
1 Inside To Outside Conne	ction Type	
WAN_T	# Routing @ NAT	
WAN_Z	# Routing @ NAT	
WAN_3	# Routing @ NAT	
		III Easa

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

WAN1 IPV6 Setting		
IPV6 Model	OFF •	
	Static Tunnel PPPoE	E Save

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.

WAN2 IPV6 Setting			
IPV6 Model	OFF •		
	OFF		
	Static Tunnel PPPoE	Sava Sava	
	111100		



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.

DMZ IPV6 Setting			
Errable	. .		
IPVE DMZ (att3) (P		(ex. 2001 288 1111 25494)	
IPVII Auto Configuration	Start # Stop		
5 Inside To Outside Conne	ction Type		
WAN_1	# Routing @ NAT		
WAN_2	# Routing III NAT		
WAN_3	Routing ⊕ NAT		
		E Bave	

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

// DNS IPV6 Setting			
DNS Server 1	2001 4860 4860 8888	(ex: 2001:b000-1)	
DNS Server 2	2001 4860 4860 8844	(ex: 2001.b000.2)	
		Cla Ease	

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 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)

		()		
I	Interface	LAN T		
I	Gateway		(EX: 10.10.10.254)	
	Netmask		(EX: 255.255.255.0)	
	Destination IP		(EX:10.10.10.1)	
	Comment			
L	 Add Route 			

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 cancel list. (Figure 2-3.2)

Route List					1/1 (1) (1) (1) (1)
Mark	Comment	Destination IP	Netmask	Gateway	Interface
10		60.249.6.9	255 255 255 0	168.95.98.254	WANZ.
8	CK	192 168 30 07	265 255 255 255	192.168.10.163	CM/Z.
10	195	192.168.195.0	255,255,255,0	192 168 109 1	WAN1
			+ Add # Edit # Del		

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 or	ן 😐 Save	(Figure 2-3.3)
--	----------	----------------

Interface	i≇ LAN	K WANE III WANE III WANE III DAZ III LANT
Update Period	30	Seconds (Range: 30 - 3600)
Timeout	180	Saconti (Ranga: 30 ~ 3600)

Figure 2-3. 3 Dynamic routing Table

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

2-3.4)

IP Route
 default via 152, 158, 186, 1 dev eth1
 152, 168, 1.024 dev eth0 proto kernel scope link sit; 152, 168, 1, 1
 152, 168, 196, 0/24 dev eth1 proto kernel scope link sit; 192, 168, 186, 157

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)

 Route List 				1/1 44 4 10
Mark	Interface	Comment	IPV6 IP and Mask	IPV6 Gateway
			🕈 Add 🥔 Edit 🗰 Del	

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 to add VLAN ID.

Figure 2-4. 1 difference no VLAN between VLAN



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

3 192.168.1.144		0
	24G + 4 SFP Web Smart Switch	
Configuration System ViANS Appropriate System System Statustics Overview Databad Statustics Monitoring Statistics Overview Databad Statustics ACP System Statustics Overview Databad Statustics ACP System Statustics Monitoring Statustics Overview Databad Statustics Converview Statustics Status Statustics Status	Port Segmentation (VLAN) Configuration Add a VLAN VLAN ID Add VLAN Configuration List	



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

			- Accession (NAMES AND A STREET	
	24	G + 4	SFP	Web S	mart Switch	
Configuration	VLAN S	etup				
System Ports	-	Law of	and the second se			
VLANs Appregation	Constant of	VLAT	E DI A			
ISTP	Post	odember	Port 11	potember		
GMP Snooping	Port 1	1#1 3	Port 14			
Quality of Service	Don 1	100	Den 15			
Storm Control	Bog 4	140	Port 15			
Monitoring	Door 5	2	Port 17			
Entirties Duoties	Barth	100	Dort 18	-		
Detailed Statistics	Dort T	1	Dout 10	-		
RSTP Status	Port 8	197. 197	Port 20	TA INT		
Ping	Port 9		Borr 21			
Maintenance	Port 10		Pare 22	1		
Norm Dartan	Port 11		Port 23	(T)		
actory Default Software Upload	Port 12	10	Port 24			
Logout	Apple	Refeat				





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

1921681144						
	2	4G + 4 S	FP Web S	imart Switch		
onfiguration	VLAN	Per Port Co	nfiguration			
ortu LAJJa pgregation	Port	VLAN aware Enabled	Ingress Filtering Enabled	Packet Type	Pvid	
TP.	Port 1	10		All . Tagged Only	3 •	
MP Snooping	Port 2	1.		All . Tagged Only	3 •	
raity of Service	Port 3	1	1 2 2	All . Tagged Only	3 •	
orm Cantrol	Port 4	1		All = Tagged Only	2 *	
onitoring	Port 5	14	1	All . Tagged Only	3 •	
disting Openiew	Port 6	10	1 8 5	All = Tagged Only	3	
tailed Statistics CP Status	Port /	11		All * Tagged Only	Non	
TP Status	Port 8	101	1	All Tagged Only		
19	Port 9	10	1 H H	· All Tagged Only	1 •	
aintenance	Port 10	1.15	1. 20	All Tagged Only	1 *	
em Restart	Port 11			All Tagged Only	1 .	
ctory Default	Port 17	0	0 8	· All Tagged Only	1	
jout	Port 13	1		· All Tagged Only	1 +	
	Port 14			All Tagged Only	1	
	Port 15	0	1 9 7	All Tagged Only	1 •	
	Port 16	(Fi		· All Tagged Only	1 •	
	Port 17	10	1 13	All Tagged Only	1	
	Port 18	0	1 2 2	All Tagged Only	1 .	
	Port 19			All Tagged Only	1	
	Barr 30		1 H T	a dill manuficiale	1	

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.

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

Comment	Tagged VLAN ID	
Multiple Subret	Cookinday	
F Address	Outonize (10.1)	
Netmask	LAN 192.168.101 / 255.255.355.0 DNZ 172.163.161 / 255.255.355.0 565.265.0 1	
interface	LAN +	
VLAN D	t	
	+ 444	

Figure 2-4. 6 Add VLAN ID

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

Mark	Comment	IP Address	Netmask	Interface	VLAN ID
121	Tagged VLAN ID	192.168.23.161	255.255.255.0	LAN	3

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
- 3-2 LAN Policy
- 3-3 DMZ Policy
- 3-4 WAN Policy



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)

 WIFi to W/ 	W Policy : 🕢							1/1	1961 (4) (8) BAY
No.	Policy Name	Source	Destination	Services	Action	OwOff	Policy	Edit / Del	Log
				+ 444					



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. ICMP³
- 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



Chapter 3 : Policy

- 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. 2 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.



Chapter 3 : Policy

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



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)

a) DMZ to WAN Policy: Q							-00 (0) (m)		
No.	Policy Name	Source	Destination	5ervices	Action	On/Off	Policy	Edit / Del	Log
				* A.I.O					



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)

WAN to LAN	Policy						1/1 30 00 00 00				
No.	Policy Name	Source	Destination	5ervices	Action	06/0ff	Policy	Edit / Del	Log		
				* 444							

Figure 3-4. 1 WAN Policy


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.

Add Computer Ne	me and IP Address :					
Computer Name	Peter					
IP Address	192.168.186.60	Es 192.368.188.0				
IN COLUMN	1-10/00 AD 75 M	Es 102 00 00 00 00 00 00 00 00 00				
maio apolitios-	** Set physical address to ARP table					
Mode	IP and MAC Address	х.				
		(2017)				
		# A36				

Figure 4-1. 1 LAN IP Address



Setting LAN IP Address completed. In addition, select <u>Checkbox</u>, and click on <u>Add</u> to create a new sub-content, <u>Bddt</u> to modify contents, or <u>Store</u> to cancel list. (Figure 4-1.2) (Figure 4-1.3)

IP Address List :	Accest			X/1 (H) (A) (H)
0	Computer Name e	IP Address o	MAC Address #	Group Name
0	Peter	192.168.186.50	1 - 28.22 -38.0 ₀	Living the west

Figure 4-1. 2 LAN IP Address List

05	Static	Alias e	IP Address #	MAC Address +	Interface +	Status .	Last Update Time .
		192.168.106.253	152 168 186 253	00 05 1d 03 04 22	LAN	2.	2015-05-12.10:20:03
		192.168.186.245	192.168.186.245	00 90 fb: 2b: 2f.e7	LAN	2	2015-05-12 13:10:01
2	0	PETER-H56M-U02H	192 168 186 50	1c 61-65 28 9c dc	LAN		2015-05-12 t3 16.01
3		192,168,186,1	192 168 196 1	00 a8 fer 0f 15 81	LAN	2	2015-05-12 13.10.01
		192 168 1 5	15J.168.1.5	00 Df 38 6b 71 b2	LAN	2.	2015-05-12 15:00:03

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)



5 Add Member and Group :	
Group Name group A	
Select From LAN Address.	
Select From IP Range	
Select From IP/Mask	
Select From DHCP Users	
O User Define	
C Select MAC Address Group	
C Select From AP Users By SSID	Select IP and MAC address
Ruiar	
	.★ A44

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)

Start IP End IP IP-MAC Binding

Figure 4-1. 6 Select from IP Range



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

 IP and Netmask
 256 256 260 (24) *

 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)

 Stat Address of IP Range 1 102 100 109 1 = End Address of IP Range 1 102 100 109 254

 IFigure 4-1. 8 Select from DHCP Users

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

 IP MAC Brideg

 (Type the IP address, and the ENTER Range I Ing rooms in order to add multiple IP addresses (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)

	1 ex 00 60 E0 46 C8 (B
(Type the MAC address, a	nd press ENTER. Repeat this process in order to add multiple IP addresses.)



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)

3 Select JP Mod 5 Group Name a	a 1974 •	tor (all 2 all all
Mark	Group Name	Manther
(B)	group A	192.168.195.50,192.103.103.201
		+ 100 # Eest # Dol.

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 <u>DROP</u> or <u>Permit</u>, and then select Source to group A which you have just set in 4-1 Address. (Figure 4-1.12)

(1) Basic Setting	
Policy Name	
Source 🧿 🔹 group A 🔹 🖤 🖤 Address	MAC Address
Destination 🕢 * Peter 🕕 🖉 IP Address	
Action Per tochio	
8 Policy	
Protocol	ALL *
Service Port or Group 🕘	User Defined
Software Access Control	None •
Qo5	None *
Schedule	None •
URL Access Control	None •
Authentication	None •
Bulletin Board	None •
WAN	ALL •
Max. Concurrent Sessions for Each Source IP Address	0
ICP	0
Packat Tracing	0
Traffic Analysis	8
Max. Quota / Day	Up 0 KBytes / Down 0 KBytes (0 No Limit)
Max. Quota / Day(Per Scarce IP)	Up 0 KBytes / Down 0 KBytes (0 No Limit)
% Firewall Protection	
E SYN Attack E IDMP Attack E UDP Attack Port Scan	
	• 446

Figure 4-1. 12 Address Policy

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

No.	Policy Name	Source	Destination	Services	Action	On/Off	Policy	Edit / Del
1 .		Inside_Any	Outside_Any	ANY CHI	10)-		والصالي في الله الإلا علا هي ه	/ 🖾
2.*		group A	Outside Any	ABT	10			18

Figure 4-1. 13 Address Policy List



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



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 <u>Action</u> to <u>DROP or Permit</u>, and then select <u>Source</u> 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 and select <u>Action</u> to <u>DROP</u> or <u>Permit</u>, and then select <u>Source</u> 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 <u>Action</u> to <u>Drop</u>, and then select <u>Source</u> 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 <u>host</u> and <u>domain name</u>, including top-level domain.

For example, <u>www.higuard.com</u> is a fully qualified domain name in the Internet. <u>www</u> is the host, <u>higuard</u> is the second-level domain, and <u>com</u> 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)

Add Outside Network :
Group Name block youtube
Select From LAN Address
Salect From IP: Range
Galact From IP/Musk
O User Define IP
User Define Duman
google.com google.com facebook.com Zewtube.com (Type the domain, and then ENTER: Repeat this process in order to add multiple domain.)
★.A44

Figure 4-1. 15 WAN_User Define Domain



Select IP Mo Outside Netw	de IPV4 • ork :	
Mark:	Group Name	Momber
	hiotk youtube	74 125 204 100/32 74 125 204 101/32
-		◆ A4.8 4 PT4 4 Percentisti googew.deen(74.125.204.100; 74.125.204.101; 74.125.204.102; 74.125.204.113; 74.125.204.113; 74.125.204.138; 74.125.204.139) googew.dee.com(74.125.204.101; 74.125.204.104; 74.125.204.102; 74.125.204.106; 74.125.204.147; 74.125.204.39) face/stook.com(175.252; 120.8) youtube.com(74.125.204.138; 74.125.204.190; 74.125.204.91; 74.125.204.93)



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

(Fi	gure 4-1.18)					
5 Basic Setting Policy Name						
Source 🕢	Inside Any *	IP Addrese		MAC Address		
Destination 👩	block youtube *	P Address				
Action	Drop •					
Policy						
Protocol			ALL *			
Service Fort or Group 🥥			User Defined	Service Part		
Software Access Control			None *			
ReD			None 🔻			
Schedule			None •			
URL Access Control			None 💌			
Authentication			None 💌			
Bulletin Board			None •			
WAW			ALL *			
Max. Concurrent Sessions 1	tr Each South IP Address		0			
IDP			10			
Packet Tracing			0			
Traffic Analysis						
Max. Quota Day			Up 0	KBytes / Down Ø	KBytes (2 No Limit)	
Max, Guda / Day(Per Sout	(e IP)		Up 0	KBytes / Down 0	KBytes (0:No Limit)	
1) Firewall Protection						
SYN Attack U ICMP A	Itack UDP Attack UP of Scan					
			+ 444			



Chill do A	weight a much - 🕥							141 100 10	10. in/ in/
No.	Policy Name	Source	Destination	5ervices	Action	On/Off	Policy	Edit / Del	1.09
1.*		traide_Any	Outside Any	ANY DEL	- 40-			/83	
2.*		Inside Any	Diock youtube	ANY	0			/ 63	
			block your google com googlewder facebook co youtube cor	00 (74.125.204.100, 74.12 xcom(74.125.204.100, m(73.252.120.6) n(74.125.204.136, 74.1	9 304 101; 7 74 125 304 1 25 304 190;	4 125 204 102 74 04 74 125 204 10 74 125 204 91 74	125.204.113.74.125.204.136.74.125.204.130. 5.74.125.204.108.74.125.204.147.74.125.204.091 125.204.93i		

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)







•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** Service.
 - 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.



10 Basic Service and Port :			
ANY ANY (ANY)	TCP AFPoverTCP (541)	ACR. (5190)	BGP (179)
DIG ENG (53)	TEO FTP (21)	Finger (79)	GNUTwite (6346)
Score Gopher (70)	HTCCH H323 (NetMeeting) (1720)	NECON HITP (80)	I I SOL HTTPS (443)
ICQ (4000)	UNIT IKE (500)	TCP: IMAP over SSL (993)	1000 (MAP (143)
arene lawet (183)	L2TP (\$701)	LDAP Admin (3407)	LDAP over SSL (EDE)
LDAP (389)	TCP: MSN Messenger (1903)	TCH NNTP (119)	1000 NTP (123)
NTTP over SSL (563)	FOP2 (109)	COM POP3 over SSL (995)	POP3 (110)
FTCP: PPTP (1723)	FLIDE RP (520)	FERT RLOGIN (513)	Real Audio (7070)
SETT (115)	SMTP over SSL (465)	SMTP (26)	EUTOR SAMP (161)
SSH (22)	THUR SYSLOG (514)	TETTE TF TP (59)	Teinet (23)
Terminal (3389)	1008 UUCP (540)	TICK VNC (5900)	WAIS (210)
VICE WINFRAME (1494)	Viccell Yahoo (5050)		



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 **** to create a Service rule.
- Service Name: Enter some words for recognition.

Click on Assist to select services. (Figure 4-2.2)

0	APPowrtCPISAEL	0	ACUSTRDY	14	BGP(17P)	10	DNS(57)
101	TCP: FTP(21)	12	Fitpar(79)	10	GNUTela/8346	0	TCP Bophen(70)
į.	H323 (hwt/weitig) (1725)	10	NUCCE 1477191003		HTTPS(443)	1	100(4000)
0	1000 HCE(500)	10	MAP over SSL(993)	8	HIGH MAP(143)	10	Mediata)
間	LITPHT91	10	LDAP Admin(3407)	10	LDAP over SSL 836	-	LOAP(389)
ii)	MSN Messenger(1863)	10	FICE NUTPITION	8	Open NTP(123)	10	SSL(563)
0	POP2109	10	POP3 over	2	FOP3(110)	10	1000 PPTP(1723)
60	Ann. BP(520)	0	PLOGINSTAL	0	Tani Beal Audio(7070)	10	FOR SETF(155)
Ð.	SMTP over BBL(465)	1	SWITP(25)	2	SNMP(101)	10	ICP BSH(22)
-	SUITE SYSLOG(\$14)	0	HOLE TETPISA	-	Tetres 230	10	Terminal (2004)
E	UUCP(540)	18	NUC SIGN	10	ETCER WARS 2101	10	LLCO WINFRAME(1494)
10	Tere Yanos(\$0(0)	T.				T	and the second se

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)

5 Add Service Gro	sup : Group Name [test services]	Anis		+ More
	Protocol	Port	(Start : End)	
1	# TCP @ UDP	80	80	
2	# TCP @ UDP	443	443	
3	# TCP @ UDP	143	143	
4	# TCP O UDP	110	110	
5	TCP # UOP	161	161	
-6	# TCP @ UDP			
7	# TCP @ UDP	5		
8	# TCP @ UDP			
		• 84.4		

Figure 4-2. 3 Service group

Setting Service group completed. In addition, select <u>Checkbox</u>, and click on <u>Add</u> to create a new sub-content, <u>Set it</u> to modify contents, or <u>Set It</u> to cancel list. (Figure 4-2.4)

• Service Group Li	at :	Choose File No file chosen Ingent Q 1/1 a	0.10 07 00
Mark:	Group Name	Port (Start : End)	
0	test services	1021 80.443,143,110 1030 151	
		+ A44 = E4st * D+1	

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 <u>Action</u> to <u>DROP</u> or <u>Permit</u>, and then select <u>Service Port or Group</u> to <u>test service</u> which you have just set in 4-2 <u>Services</u>. (Figure 4-2.5)

a case second						
Policy Name						
Source 🕑	Innide_Any •	© IP Address		MAC Address	1	
Destination	Outside_Any •	@ IP Address				
Action	Drop •					
* Policy						
Protocol			ALL *			
Service Port or Group 🌒			test services	Service Port		
Software Access Control			POP3 PPTP			
QoS			RIP			
Schedule			Real Audio			
URL Access Control			SMTP over BS	L		
Authentication			SNMP			
Bulletin Board			SYSLOG			
WAN			Teinat			
Max. Concurrent Sessions	for Each Source IP Address		Terminal UUCP			
ICP			VNC WAIS			
Packel Tracing			WINFRAME			
Traffic Analysis			Inst nervices			
Male. Quinta / Dily			Up 0	KBytes / Down 0	KBytes (0:No Limit)	
Max. Quota / Day (Per Sou	ice IP)		Up (0	KBytek / Down 0	KBytes (0 No Limit)	
- Firewall Protection						
SYN Attack BIOMP	Attack III UDP Attack III Port Scan					
			2 Edit			

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)

AN to V	WAN Policy : 🕢							1/1	0, 00, Re.
No.	Policy Name	Source	Destination	Services	Action	OnIOff	Policy	Edit / Del	Log
1 .		Inside_Any	Outside Any	ANY D	n 📫	*	ہ کا کا تک ایک ایک ایک اس کا کا کا کا	/ 83	
2.*		Imside_Any	Outside_Any	MART 10			: ه: هر هر هر هر هر هر هر هر ه	123	
				+	Group Name Instaerytpes		Port (Mart : End) HTTP5(443.3MAP(140;POP2(110)) 2010 (2010)		

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)

5 Add Schedule :	
Schedule Name for working time	
Setting Mode - Mode 1 - Mode 2	
Sunday 🏶 Disable 🔍 All day 🔍 Start Time (00:00) - End Time (00:00)	
Monday 🔮 Disable 🔍 All day 🕷 Start Time 07.30 - End Time 22.00	
Tuesday 🔮 Disable 🐵 Al day 🌻 Start Time 02:00 - End Time 22:00	
Wednesday 0 Disable # All day 0 Start Time 00.00 - End Time 00:00	
Thursday 🔍 Disable 🔍 All day 🕷 Start Time 07.30 - End Time 22.00	
Friday	
Baturday @ Disable * All day @ Start Time 00.00 - End Time 00.00	
	* 846

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 <u>Checkbox</u>, and click on <u>Add</u> to create a new sub-content, <u>Set it</u> to modify contents, or <u>Set Del</u> to cancel list. (Figure 4-3.3)



5 Sched	da List :							1111 101-107-107
Mark:	Schedule Name	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
10	for working time	0	07:30 - 22:00	00.00 - 22.00	0	07:30 - 22:00	07 30 ~ 22 00	0
10	for part time			20	15-05-19-00:00 - 2015-05-3	9 23 00		
				+ A04 @ E4 (t	× D+1			



D 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 first.
- 2. Select <u>Action</u> to <u>DROP</u> or <u>Permit</u>, and then select <u>Schedule</u> to <u>for working time</u> which you have just set in 4-3 <u>Schedule List</u>. (Figure 4-3.4)

to timesc setting						
Policy Name						
Source 🕥	Inside_Any •	© IP Address		MAC Address		
Destination 🥥	Outside_Any	© IP Address				
Action	Permit *					
9 Policy						
Protocial			ALL .			
Service Port or Group 👔			User Define	d • Service Port		
Boftware Access Control			None.*			
Qo9			Nipne 🔻			
Bchadula			for working t	ime •		
URL Access Control			for working	irme .		
Authentication			for part time			
Bulletin Board			None *			
WAN			ALL .			
Max. Concurrent Sessions	for Each Source IP Address		D			
IDP			8			
Packet Tracing			65			
Traffic Analysis			0			
Max. Quota / Day			Up 0	KBytes / Down (0	KBytes (0 No Limit)	
Max. Quota / Day(Per Sour	ce (P)		Up D	KBytes / Down (b	KBytes (0 No Limit)	
+ Firewall Protection						
SYN Attack III ICMP	Attack 🗏 UDP Attack 🗏 Port Scan					
				8i4		
			gr. 11			

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)

		Poucy	On/Off	Action	5ervices	Destination	Source	Policy Name	No.
18				-	DHE DHE	Outside Any	Inside Any		1.
/ 23		3		-	ANY.	Outside_Any	Imide Any		2.*
	Wednesday Thur	Sanday Monday Teenday We	F Scheritule Name 1	•	ANY	Cutside, Any	imide_Any		2.*





•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 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.



5 Name	QOSPolicy					
ionly 🥥	1.		Select Bandwidth Mode		(For Policy •	
Interface	110	User Down Speed			User Up Speed	
T ON white	Min. 200	Kbps (1-102,400)	Min	200	Kbps (1~102,400)	
Data Month	Max 1000	Kbps (1-102,400)	Max	1000	Stbps (1-102,400)	
Tex7	Min O	Kbps (1-102,400)	Min	0	Khps (1-102,400)	
LINE MIL	Max 0	Khipa (1-302,400)	Мак	0	Khps (1-302,400)	
MARKED AND AND A	Man Ø	Klips (1-102,400)	Min	0	Khps (1-102,400)	
Anale Chil	Max, ID	Khipa (1-102,400)	Max	0	Khges (1-102,400)	
WANT .	Min. 0	Klopa	Min	Ű.	Khyu	
107012	Max. 0	Kbps	Max	0	Kips	
WANT	Min. 0	Klapa	Min.	Û	Kbps	
10-044	Max. 0	Kbps	Max	0	Whee	

Figure 4-4. 1 QoS Setup

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

lock	QoS Name	Priority	Bandwidth Mode	Interface	User Do	wn Speed	User U	p Speed	
		E provinción de		LAN	200(Khps)	1000(Kbps)	200(%bps)	1000(%bps)	
		К	1 None		DMZ				
12	QOSPolicy.			WAN					
					WAN2				
				WAND.					

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 first.
- 2. Select <u>Action</u> to <u>Permit</u>, and then select <u>QoS</u> to <u>QOSPolicy(Per Souce IP)</u> which you have just set in 4-4 <u>QoS</u>. (Figure 4-4.3)



5 Basic Setting						
Policy Name						
fource 🕥	Inside_Any •	© IP Address		MAC Address		
Destination 🥥	Outside Any	IP Address				
Action	Permit •					
16 Policy						
Protoc al			ALL +			
Service Port or Group 🥥			User Defined	Berrice Part		
Software Access Control			None 🔻	_		
QoS .			QOSPolicy •			
Schedule			QOSPolicy			
URL Access Control			None +			
Authentication			None *			
Bulletin Board			None .*			
WAR			ALL +			
Max. Concurrent Sessions	for Each Source IP Address		Ô.			
IDP			8			
Packst Tracing			63			
Traffit: Analysis			10			
Max. Quoto / Day			Up 0	KBytes / Down 0	(KBytes (0 No Limit)	
Max. Quota / Day(Per Sou	te IP)		Up 0	KBytee / Down 0	(KBytes (0 No Lmit)	
+ Firewall Protection						
SYN Attack UI ICMP	Attack III UDP Attack III Port Scan					
			1.000			

Figure 4-4. 3 QoS Policy

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

E LAN to	WAN Policy Rule								1/1	98 B B B
No.	Policy Name	Source	Destination	Services	Action	0n/Off	Policy	Edite	Del	Rec.
1 -		Inside_Any	Ostaide_Any	ANY CHE	- sip.			1	×	Les. 23
2 -	-	Incide Any	Outside Any	ANY	-		8	1	×	
3 *		Inside_Any	Outside_Any	ANY	•		Ge5 Name Prix Source-Direction Interface	Dows Speed	tip	Speed
					• 113	n	COSPalicy 2 Outgoing Weith Weith	200(Kbps) 10000(lass) 2 (Klaps) (Klaps) ((Klaps) (Klaps) ((Klaps) (Klaps) ((Klaps) (Klaps) ((DO(KDµ) Khps) Khps) Khps)	(K3p5) (K3p5) (K3p5) (K3p5)

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)

Popular Software St Block Log			
File Sharing Application 😤 Select All			
R ares (Ares)	📽 billomett (Eit Torrant)	🕷 edankey (Edankey)	98 expeer (expeet)
R faxy (faxy)	🕷 gogobox (GoGoBo+)	🐼 slubbox (Childron)	60 aniesh (Mash).
M soulseek (P2P)	Winner (World)	🐼 stanlei (Thurder)	
Instant Messaging Client 🗷 Select Al			
🖉 am (CQ/AM)	🕷 geogletalk (Google Taik)	R mannessenger (MSN + MSNUte)	🕷 gg (00)
🕷 yahoo (Yafimi)	W wettern (WorktM)	Sine (UNE(for PC, Arstmid))	90 skype (Skype)
VDIP Application Block III Select All			
E jabber (An open instant messenger protocol)	III 16323 (H 323)	□ sip (SIP)	
WEB Application Block 🗍 Salact All			
E httpaudio (Audio over HTTP.)	http://deo.tvideo.tvideo.over.HTTP.)		
WEB Mail Block Select All			
webmail_163 (163/126/Yeah)	III webmail_gmail (Gmail.)	webmail_texet (Hinet)	E webmai_live (Hotmail)
III webmail_pchome (PChome)	💷 webmail_yahoo (Yahoo)	(QQ) pp_listndew III	<pre>iii webmal_seednet (Seednet)</pre>
💷 webmail_sohu (Sohu)			
Game 🗍 Select All			
D posteam (PPSbeam)	💷 cradio (Tornado Broadcaet.)	timedo (Hiredo Broadcast.)	🗐 ggive (QQLive)
ED furnition (Furnition Video)	III kunite (Kunite Video)	(D ppilve (PPLive)	baofeng (baofeng)
Others 💷 Select All			
🗊 ndp (Remote Desktop)	E vnc (VNC)	respan (NETPAS ACC)	phpraxy (HTTP proxy within in PHP.)
17 facebook (Facebook)	III teamviewer (TeamViewer)	💷 hamachi (Hamachi)	E torproject (TOR)
Intspot_shield (HutspotShield.)	vnn_chent (VNN_Client v4.v6.)	Itreegate (Freegate and Utlasuet)	

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)

E-Net Commonly David Software			
File Sharing Application 🖗 Select All			
80 100ban (100ban)	St Awaret (Anonymuus information retrieval.)	8 gruceostan (CAPForty P2P.)	🕷 gobbogy (Kanan P2P)
R hotine (An dd F2F.)	R sparit (A P2P filestrang protocol)	B poco (Chemina P2P.)	😹 heada (E2P)
🕷 sortiada (A Koway P2P.)	S grutella (F2P.)	B fastfräck (Fustfrack)	en geotalia (Grutalia)
🕷 mactella (grunello)	🕷 maie (bittomen, edooley)	🕅 vagas (PDP)	🕷 napater (P2P)
🕏 thacistle (P2P)	R Imewie (Limowie 7	R morphous (Morphous.)	🕷 mute (MUTE)
🛞 applejutoj (Applejutoj (96 directs privatel (DirectConnect.)	86 bearshare (BearShare)	😹 kazan (KaZan)
R audogalaxy (AutoGalaxy.)			
Instant Messaging Client III Select All			
aimwebcontent (AM web content)	💷 chikka (Chikka - SMS service)	El cirrid (SMSC protocol by Nokia)	≡ in: (Internet Relay Orat.)
B stun (Simple Traversal of UDP Through NAT)	III mon-Retransfer (MSN File Transfer)		
WEB File Extension Download Block III Select All		Custon Fée Ex	tomaionFile Extension ;
iii eve (Dourioud)	C flash (Download)	El g# (Download)	III html (Download)
greg (Downtoad.)	💷 mp3 (Download)	💷 ogg (Download)	piff (Dositioad)
ID pet (Deenload)	D prog (Download)	E postscript (Download)	💷 rar (Download)
(D) rpm (Download)	#f (Download)	(II tar (Download)	(D zip (Download)
WEB File Extension Upload Block C Select All			
💷 uexe (Upload)	💷 uffash (Upload)	i ugif (Upload)	💷 uhtml (Upload)
🗊 upreg (Upload)	imp3 (Upload)	🗐 uogg @pload)	iii updf (Upload)
III upert (Oploard)	III upng (Upload)	🕮 upostacipt (Upland)	i unar (Up(cad)
💷 upm (Upload.)	💷 urti (Upload)	💷 utar (Upitzed)	III ump (Uplead)
Video Software Block III Select All			
💷 live365 (An internet radio site)	Implayty-ivs (ReplayTV Internet Video Sharing)	shoutcast (streaming audio.)	
Garre C Select All			
E amagetron (Amagetron Advanced)	battletiekt/1942 (Battlefield 1942.)	Battlefield2 (Battlefield 2.)	10 battlefield2142 (Battlefield 2142)
🗊 counterstrike source (network game)	dayofdefeat eource (game Hat-Life2 mod.)	doorn3 (Doorn3-computer game)	Italfite2-deathmatch (Halt-Life 2.)
III Inveforspeed (A rating game)	mohaa (Medal of Honor Alked Assault)	quake-hattite (Hat-Life 1.)	💷 guaket (Quake)
D teerifortress2	i thereast to brief (World of Warcraft)	aboxive (Xbox Live)	💷 subspace (Subspace)
Virus, Worms, Spyware Block 🗍 Select All			
LL code_red	🗇 rumsta		
Stock Software Block III Select All			
Ⅲ westfutu (古家期前)	□ gen(廣州協長)	□ pote (博整大師)	III stockstar(: 編券之權)
印 gtja (國委君安)	章 duth (大智慧)	日 +ja (中投卓越)	回 gianlang (奴能)
D hean(和武宏書)	(2 white (文華財經)	□ siqn (大蔵共)	
Others 😳 Select All			
Ciscovpn (Disco VPN server.)	(ADI: xittl) xittli (nop (Novel: Core Protocol)	III pcanywhere (pcAnywhere)
III cadmin (Famatach Ramote Administrator.)	ssh (Secon SHell)	sucp (Unix to Unix Copy.)	III validsertssi
E http://www.cache.htl.)	E Http://www.cachemiss.com/	E http-dap (Download Accelerator Plus)	10 http-freshdownload (Fresh Download)-
EV Imp-itunes ()Tunes ()	http-rtsp (RTSP tunneled)	🗐 skypetoskype (Skype-to-Skype.)	III teamspeak (Teamspeak)
El ventrio (Ventrio)			

Figure 4-5. 2 Not Commonly Used Software



Setting Software Blocking List completed. In addition, select <u>Check box</u>, and click on <u>Add</u> to create a new sub-content, <u>Celit</u> to modify contents, or <u>Setting</u> to cancel list. (Figure 4-5.3)

ication Cont	DOT LINE!		777 (16) (6) (6)
Mark	Group Name	Regulatory Content	Block Log
0	test blocking	File Shanng Application , Instant Messaging Client	0
		◆ AdA → Edit ¥ D+1	

Figure 4-5. 3 Application Control List

There is an example of how Software Blocking is used.

- 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 <u>Action</u> to <u>DROP</u> or <u>Permit</u>, and then select <u>Software Access Control</u> to <u>test blocking</u> which you have just set in 4-5 Application Control. (Figure 4-5.8)

Policy Name						
Source 🕜	Inside_Any	IP Address		MAC Address		
Sestination @	Dutside Any •	O IP Address				
Action	Drop •	21 121 (2100-00-01				
Policy						
hotoc of			ALL +			
envice Port or Group 🥥			User Defined	 Service Port 		
oftware Access Control			test blocking			
8a			test bicking			
chestule			None			
RL Access Control			None •			
utbentication			Norm •			
utenn Board			Norse •			
AN .			ALL •			
tax. Concurrent Sessions	for Each Source IP Address		0			
19 C			-0			
acket Tracing			0			
affic Analysis			0			
lax Quota / Day			Up 0	KBytes / Down (0	(KBytes (0 No Lenit)	
Asis Quota I Day/Per Sour	te (P)		Up D	KBytes / Down D	KBytes (0 No Limit)	

SYN Attack III ICMP Attack III UDP Attack III Port Scan

+ 101

Figure 4-5. 4 Software Blocking Policy



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

(1) LAN to	WAN Policy : 🕡							17.1 THE GO. D. 187
No.	Policy Name	Source	Destination	5ervices	Action	On/Off	Policy	Edit / Del Log
t •		Inside_Any	Outside_Any	And Dell	10	×		183
2.*		Inside_Any	Outside_Any	ABY	0	- P -	i 🗖 Yan i shi ka ku ka ka ka ka ka ka ka ka	/8
				+ 14	d		Group Name Regulatory Content last biocump File Sharing Application Instant Mensaging Clent	



Block Log

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

erth Cr	ondition :							
1	2014-05-05	00:00 • - 0	23 23	59 *				
	ALL							
	ALL •							
e IP								
					e Seatth			
n List					C Swatch		1/1 (4) (4) (5) (6)	Beport Export All
ng List Tit	ima e	Name +	Action	Source IP •	• Search Date: IP #	Protocol	1/1 (e) (e) (e) (e)	Export All Date: Port #
ng Lint Tia D3-30	ime e 0 09 02 05	Name + thunder?	Action	Scenta IP +	© 3+exth Date: IP # 65 55 223 38	Protocol UDP	1/1 (4) (4) (4) (4) (4) Source Port # 64201	Export All Date: Port # 40005
ng List Tia 03-30 03-30	1mma e C 09 03:05 C 09 01:47	Name # thunder? edorskey	Action DROP DROP	Science IP • 192 (68,196,133 192 168 (96,133	Date: IP = 05.05.223.30 122.121.62.352	Protocol UDP TCP	171 en el la lee Source Port € 64705	Export All Dates. Port # 40005 8836
g List Ta 03-30 03-30 03-30	0004 6 0 09 03:05 0 09:01 47 0 09:01 32	Name # thunder? edictivey edictivey	Action DROP DROP DROP	Science IP • 192, 108, 106, 133 192, 168, 106, 133 134, 170, 136, 71	Date: IP # 66 56 223 38 122 121 82 552 152 168 186 133	Protocol UDP TCP TCP	1/1 (0) (0) (0) (0) Source Port ∉ 64705 60002	Export Al Date: Port + 40005 8836 54545
ng Line Ta 03-30 03-30 03-30 03-30	inna • 0 09 02 05 0 09 01 47 0 09 01 32 0 09 01 15	Name + munder7 edorikey edorikey edorikey	Action DROP DROP DROP DROP	Science IP • 192, 168, 106, 133 192, 168, 106, 133 1,54, 170, 136, 71 192, 168, 186, 133	Date: IP # 65 55 223 38 122 121 59 359 152 168 166 113 134 170 136 71	Protocol UDP TCP TCP TCP	1/1 (e) (e) (e) (e) Source Port # 64705 60000 64645	Espot 2 Expot Al Date: Port + 4005 8836 54645 5000

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.
- Sor 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.



1 Basic Setting	
Name	test_URL_2
List Mode	III Blacklist 😳 Whitehet
D Create Blacklist	
Match Mode	© Exact # Fuzzy
URL Blacklet	google youtube yebco
IP Blackfast	
b Default Black List	
	Aggressium(1) 💷 Auto-sides(2740) 📽 Disgs(11) 🛛 📽 Gambling(1534) 🕮 Hacking(223)
Default Blacklist	Pom(58300) Pmy(3281) E Redrector(25540) Servare(11691) Suspect(20)
	Wintercet2) Warezr553)
Other Setting	
Use Other Setting	No Other Setting
	II Zaxe

Figure 4-6. 1 List Settings

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

1 BW List Setti	ių.			1/1 3	N 10.01 M
Norte	List Mode	Match Mode	Default Blacklist	Other	Action
test_URL_2	•	Futty	0	8	123
			.12.5 10	+ 262	
				¥ 268	

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.

5 Setting	
Group Name	test123
Create block warning in	estape 8
Warning message	View
Warring Subject	Access Denied
Warring content	Access to the page has been - devied because the following " page is blacklisted
List Select	Inst_URL_2 ·
	* 644

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 to create a new sub-content, in modify contents, or is to cancel list. (Figure 4-6.5)

Contra Manual	1144	Transfer Pills of Misselson Revisions	
Geoup Name	1.101	Create clock warning wessage	ACTION
hist523	test URL 2	0	/ 53



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 <u>Permit</u>, and then select URL Access Control which you have just set in 4-6 URL Filter. (Figure 4-6.6)



D. Basic Setting						
Policy Name						
Source 🕤	* Inside_Any *	@ IP Address		MAC Address		
Destination @	Cutside_Any *	@ IP Address				
Action	Permit *					
Policy						
Pintocol			ALL +			
Service Port or Group 🌍	(3).		User Define	d 🔹 Service Port		
Software Access Control			None	•		
GoS			None	•		
Schedule			None			
URL Access Control			teet123 •			
Authentication			tests23			
Bulletin Board			None *			
WAN			ALL •			
Max. Concurrent Session	s for Each Source IP Address		0			
IDP			10			
Packet Tracing			13			
Traffic Analysis.			10			
Max. Quota / Day			Up 0	KBylas / Down Ø	Kityten (2 No Livet)	
Max. Quota / Day(Per So	ace IP)		Up 0	KBytes / Down 0	KBytes (0 No Limit)	
Eirewall Protection						
E SYN Attack E ICMP	Attack UDP Attack UP of Scan					
			+ A	1.6		

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)

								10.0	
No. Policy Name	Source	Destination	Services	Action	On/Off	Policy		Edit / Del	1.05
1.*	Inside_Any	Outside_Any	ARY DES	10				183	
2.4	Inside_Any	Outside Any	Abr	- 40				13	-
			+ 440	ũ		Group Name : List Mode March Mode : URL Blackfest P Blackfest Default Blackfest	Heat123 Blackind Futty Stoppe , youtube , yahoo		





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



Log

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

URL Log				
te	2014-04-27	(III 00:00 • - 2015-05-21 III 23:00 •		
ute IP				
р Туре	All	•)		
			. 3narth	1/1
0	ale a	Source IP +	Destination	Stop Type
2015-03	-30 09 10 23	192 168 186 133	http://youtube.com/	BLACKUST URL
2015-04	107 17:03 06	192 168 189 12	media.contextweb.com	BLACK Domain
2015-04	-07 17 02 28	192 168 189 12	103.245.222.65	BLACK Domain
2015-04	107 17:13:19	192 168 189 12	http://zzztube.com/	BLACKLIST URL
2015-04	1-07 17 13 22	112,168,189,12	http://www.zzztube.com/	BLACKLIST URL
2015-04	-07 17 53 11	152,168,189,12	http://www.zzztube.com/	BLACKUST URL
2015-04	107 17:58:53	192 168 189 12	http://play.txxii.com/	BLACKLIST URL
2015-04	-07 18:00 08	192, 168, 169, 12	216.17.109.145	BLACK IP
-herber all, where	07 17 06 41	193 166 195 13	http://wlautoit.com/	ELACKUST (EL

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) (Figure 4-7.2)
 - 1. WAN 1 Interface
 - 2. WAN 2 Interface

WAN	1	00 90 FEI 35 DRI DEI	Netmask	255 255 256 255
Using	IP Address	111.252.86.179	Broadcast	111.252.06 179
Start i	Candidata	NA	End Candidate	NIA
		• 0)E	

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)

Virtual Server List	1/1 (4 8 10
WAN IP	Edit / Del
WAN1 Interface(111252.88.179)	/ 🛛
► 434 ★	

Figure 4-7. 3 Virtual Server List

Click on it 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)

Second Contract of the second second second	
946,21,1/20	Inginisiona . 110,25,86,868
	• OK

Figure 4-7. 5 Select Service Group

WANTP	Victor 1	
Protocol	TCP +	
External Senice Port	22	Read
Vitual Server IP Address	192.168.9	9.117
Internal Senice Port	22	
Enable Seriel Load Balance	13	

Figure 4-7. 6 Enter single Port



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

S Virtual Server WAN IP WANT Inter	face			1/1. 廊画笛匾
Protocol	External Port	Virtual Server IP Address	Internal Port	Edit / Dol
Service Group	tingmo T020	192.168.99.250	tingms 1990	18
top	22	192 168 99 117	22	/ 🛛
	the second second	+ 114		
		(CONTRACTOR)		



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)

WAR IN LAW	WAR IN DWZ	
t/ Basic Setting		
Policy Name		
Source 🥹	Outside_Any *	© IP Address
Destination	Virtual Server(WAb11) +	Children de States
Action	Permit +	
Policy	Corop El Manifest I and	
Service Port or Group		ALL
QoS-		Pahrar +
Schedule		think +
Max. Concurrent Sessio	ns for Each Source IP Address	0
Enable incoming Mail Lo	d d	E1.

Figure 4-7. 8 WAN to LAN Policy

WAN to LAN	Policy							tit	出创 田 田
No.	Pulicy Name	Source	Destination	Services	Action	OeVOII	Policy	Edit / Del	Log
1 *		Outside_Any	VIP(WAN1)	ALL	-	*		/ 🔀	
			WAN Post Virtual Serv Ingens1000 19210 WAN Post Virtual Serv 22 19215	er IP Address Int 18.99.255 fin er IP Address Int 18.99.117	ernal Port pms1000 ornal Port 22				

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)

ShareTech	les en enc						-
	System Status						eng
Mail Server	Seconditiestocc					17	
Mai Record	1	System Time .			Server Info		
Rel Audit		Server Date / Time	2011-12-23	17:16:43	Server Nodel	M51000	
Arttl-Wrus		Sebup Time Zone	Time Zone	Asia/Taipei	Server Software Version	1.3.1	
Anto-Span		Server Start-up Time	6 days,1	houts,17 minutes	Contant Exercise		
khie Mgt.		Contraction of the local division of the loc			System Service	And a second	
Seatern Hyt.		Serie spann Konsurte	http://www.commune.com/action.com/actio			The second second	
Filme Statistica		CPU Model.	CPU Model. 2,506Hz			(manning)	
LORP Address Book.		CPU Utilization / System Average Loading	1000 0000		Service 3	Hamming	
Galleway			0.0%	0.54 0.11 0.00	WEBMAIL Service 1	Himmo	
PISP3 Proxy		Memory (All/Free) MB	256.3	53.5	POP3 Service :	Running	
SMTP Prose		Storage space (AI/Free)	0,656	6,402	IMAP Service :	Humming	
брарке		Ultra Manou (ABCas)			POP35 Service 1	Stopped	
Logad		MB	5,080.2	745.4	IMAPS Service :	Stopped	
		Domain / Account Count:	1	11	SQL Service :	Rumning	
		Network Flow Rate	1994	14.4	DNS Service T	Dunning	
		(Receive/Send) Kbps	-10.7	14.0	LDAP Service :	Ranning	
		Mail Flow Statistics		1.17	AD Senice :	Stopped	
		Total Mal Could			And the second se	A CONTRACTOR OF CONTRACTOR OFO	
		Coses Mod / Count (86)	7	20.000			
		time the (County N)	-	22.01			
		Curtain Andreas		8.076			
		(Time/State)	2011-	12-23 00:15:42			

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)

Compared and the second of the strength of the second seco	
Sharel	ShareTech 至質訊 Fech Webmail
田橋:	
#54-01001: 20	paperlove idv tw マ 在瑞祥電影上記世界的聖 入資料。
8	使用HTTP開始
8	M品版 [版入]
	2013年後期1000
	2

Figure 4-7. 11 WAN Virtual 888port



Because of the intranet is transferring the private IP by NAT⁴ 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:

WAILIP	192.168.188.252	Asset	
Map to Vitual IP	192.168.1.4		



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

Virtual Server Illapped IP		
Itapped IP List		1/1 44 4 30
WAN IP	Map to Virtual IP	Edit / Del
192.168.188.252	192.168.1.4	/ 🛛
	◆ Add	

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.

8 SYN Attack Detection Setting :	Attention! The packet flow rate is approximate
Allow maximum flow 10000 Packet / Second(s) (Range 1000-10000)	
Allow maximum flow for each source SP 100 Packet / Second(s) (Range 10-10000)	
Flow greater than maximum, block (60 Second(x) (Range 10-65536)	
5 1CMP Attack Detection. Setting 1	
Allow maximum flow 10000 Packet / Secondis) (Range 1000-10000)	
Allow maximum flow for each source IP 100 Paciliet / Second(s) (Range: 10-10000)	
Flow greater than maximum, block (0 Second(s) (Range 10-66536)	
UDP Attack Detection Setting :	
Allow maximum flow 10000 Packet / Second(s) (Range 1000-10000)	
Allow maximum flow for each source IP 100 Packet / Second(s) (Range 10-10000)	
Flow greater than maximum, block 60 Second(k) (Range 10-65536)	
Source IP address block 1	
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
d (ex. 192.168.0.1)	
Destination IP address block :	
111.111.111.111	
and Build Prints	
(ees. 192, 168,0,1)	

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.
 - 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 <u>Action</u> to <u>Permit</u>, and then choose protection on <u>Firewall Protection</u> (Figure 4-8.2) (Figure 4-8.3) (Figure 4-8.4)

10 Elwsin: Setting						
Policy Name	1					
Source 🕢	Inside_Any	IP Address		MAC Address		
Destination 🤤	* Outside_Any *	IP Address				
Action	Permit *					
(b) Palicy						
Protocol			ALL +			
Service Port or Group 🥥	8		User Defined	 Service Port 		
Software Access Control			None T			
QoS			None •			
Schende			None	•		
LFIL Access Control			None •			
Authentication			None •			
Bulletin Board			None 🔻			
VEAN			ALL •			
Max. Concurrent Sessions	for Each Source IP Address		0			
IDP			10			
Packet Tracing			0			
Traffic Analysis						
Max. Quota / Day			Up 0	KBytes / Down 0	(KBytes (0:No Limit)	
Max. Quota / Day/Per Sou	itte (P)		Up (0	KBytes / Cown 0	KBytes (0 No Limit)	
• Firewall Protection						
SYN Attack RICMP	Attack MUDP Attack M Port Scan					
			* A44			

Figure 4-8. 2 Firewall Protection on Policy

No.	Policy Name	Source	Destination	Services Action On/Off	Policy	Edit / Del Log
1.*		Inside Any	Outsida_Any	ANY DIS 📫		/ 🔛
2 .		Imide Any	Cutside Any	ANNU - ANN -		1 /8

Figure 4-8. 3 Completed Policy

Time :	2012-05-07 00.00 •	2015-05-21 23:59	•			
(pe	UDP Attack •					
tacker (P						
Yotana iP						
				(Search)		110 120 120 120
Time	Type	Protocol	Port	Interface	Attacket IP	Victim IP

Figure 4-8. 4 Firewall Protection Log


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

6 Other items ;		
Block IP Options	Block Land Attack	🗑 Block Smurf Attack
E Block Trace Route	H Block Fraggle (UDP treadcast)	HE Block Tear Drop Attack
C Block (CMP Fragment Attack	M Black Ping of Death Attack	III Block TCP Flags
Block SYN Fragment Packet	10 Detect unknown protocol packet	

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)

Time	2015-05-21 00:00 •	- 2015-05-21 23.59 •					
Турн	Ping of Death						
Attacker (P	1						
Victim IP							
				Bearch			1/16 1 0 0 0 0 0
	Time	Type.	Protocoli	Port	Interface	Attacker IP	Victim IP
	2015-05-21 16:42:39	Pirig of Death	ICMP	Ú	WAN2	218.75.109.18	125 227 221 222
	2015-05-21 1E 14 41	Ping of Death	ICMP	0	WAND.	45 232 206 146	125 227 221 218
	2015-05-21 16:14:41	Ping of Death	ICMP	0	WANZ .	37.29.13 E	120 227 221 210
	2015-05-21 16:14:41	Ping of Death	ICMP	-0	WANZ	37 29 0 146	125.227.221.218
	2015-05-21 16 13:54	Ping of Death	ICMP	0	WANZ	174.35 92,47	125 227 221 218
	2015-05-21 18:13:54	Ping of Death	ICMP	0	WAN2	37 29 0 130	125 227 221 218
	2015-05-21 16 13 54	Ping of Death	ICMP	0	WAN2	197.64.133.2	125 227 221 218
	2015-05-21 16:13:54	Ping of Death	ICMP	0	WAN2	151.249.88.86	125 227 221 218
	2015-05-21 16:13:54	Ping of Death	ICMP.	0	WANZ.	175,41.5.34	126 227 221 218
	2015-06-21 16 13:54	Ping of Death	ICMP	a	WAN2	190.54.183.70	125.227.221.218
	2015-05-21 16 13 54	Ping of Death	1CMP:	0	WAN2	119.31.252.44	125 227 221 218
	2015-05-21 16:13:54	Ping of Death	ICMP	0	WAN2	200 133 200 2	125.227.221.218
	2015-05-21 16:13:54	Ping of Death	ICMP.	- 17	WAND	37.29.13.963	125 227 221 218
	2015-05-21 18:13:54	Ping of Death	ICMP.	0	WAN2	37,29.0.146	125 227 221 218
	2015-05-21 16:13 54	Ping of Death	ICMP	12	WANZ	197.80 133 57	125 227 221 218
	2016-06-21 16 13 53	Ping of Death	ICMP	0	WANZ:	91 202 200 101	125 227 221 210



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)

	DALL AT ME	1000 C 000 000 C	all income		11 TO 12 TO 12 TO 12					
BITTHE .	2011-09-02	00.00	20154	05-21 ==	13.200					
pe	Port Scan		Ĩ.							
arke P										
tim IP										
ctim IP							Beann			
tim IP							Beanth			1/1 (20 (20)
ctim IP	Time			Type		Protocal	Bearch Port	Interface	Attacker IP	1/1 (a) (a) Victim IP

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 AD⁵ 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:
- ²range: 10 ~ 256
- Idle timeout: If an authenticated connection has been idle for a period of time, it will expire. Default is 60 minutes.
- ²²range: 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



O 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:

20 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

15 Authentication General Setting	
Authantization part	82 (tange 1 ~ 65535.0 means authentication disabled)
Authentication Connection Protocol	© HTTP * HTTPS
Max concurrent connections	296 (ranga: 10 ~ 256)
title timeout	(0) minute(s) (range: 1 - 1000)
Re-login after user has logged in for	24 hou(s) (range: 0 - 24.0 means no limit)
Allow change password	8
Deny multi-login	8
Temporarily block when logen failed more than	0 tane(s) (0 means no imit)
IP blocking period	G minute(s) (0 means permanent blocking)
Permanently block when login failed more than	0 time(s) (0 means no limit).
Unblocked IP	No blocked (P
Account expiration notification	Before 0 Days (0 represents the day)
Delete expired account	After 0 Days (0 means no limit - that is on-er deleted)
4 Authentication Mode Setting	
Select authentication mode LAP.R LAP.R LAP.R LAP.R LAP.R REBIN	s with commas)
	Ease.

Figure 4-9. 1 Authentication General Setting



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.

Delauit Setting					
Redirect successfully aut	hanticated users to serve sharetech com tw				
whether to have read page					
Client Login Message	e Login Preview				
Subject	Subject				
	Content				
Contwit					
and a start of the second					
Upload Logo	Choose File No file chosen				
Ellent Logined Mess	age Logined Preview				
	Melcose				
Logined Message					
		122770			
Annie Balletin Lawon	A	Hel Dava			1/0 (20 (20 10 10)
No.	Notes IP/Netmask	Bulletin Group	Subject	Content. Logo	Preview
		+ Add @ Edit # De	1		

Figure 4-9. 2 Page Default Setting

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

入家	ShareTech 至 資 時代	
	Subject	
	Content	
Account :	17.15.1542.1540-1.1.	
Padeword (
	login	

Figure 4-9. 3 Client Login Message

■ You are able to click <u>Login Preview</u> 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)

5 Add User Define Settings		Ba
Notes	PC	
IP Address	192.168.189.1	
Netmask	295.255.255.0 ((24) ·	
Apply bulletin	123 •	
Show Authentication Login Page	Subject Content Slopp	



Delauit	Setting							
Redirect su	ceastuly and	enticated users to	www.sharetech.com.tw					
whether to	have read page		8					
D. Client L	ogin Message	Login Preview						
Subject		Subject						
		Content						
Content								
Upload Log	0.	Choose #	File No file chosen	fage				
2.1.2.1								
5 Client L	ogined Messa	ge Logined Previ	ew.					
		ble1cowe						
Logined Me	u sada							
				Br				
+ Apply 8	ulletin Layout	t						1/1 (48.14) (6.14)
E	No.	Notes	IP/Netmask	Bulletin Group	Subject	Content	Logn	Proview
- 62	1.	PC	182 168 189 0/24	123	0		0	PC Version Mobile Version
- 時	2 .	mobile	10.0.153.0/24	mabile	0	0	0	PC Version Mobile Version
				+ Add # E	det 🗰 Dol			

Figure 4-9. 6 Apply Bulletin Layout

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

	engrated Security Solution for your Wind and Wireless Denset
A	Humple SSID (VLAN)
	the Best Security for
	Wiedless Network
-WF	-300 Best SME Decurty Solution Final at

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



add User Account				
name	Ting	(maximum 16 charactera)		
User Account	ting	(maximum 16 characters)		
Password		(case-senative, please use 3 to 16 characters, not with the same account number		
Password Detection	weak met strong	a		
Contim paseword				
D	require users to log on	when the next change password		
user account expiration date	1			
	# #	5 W		
	8 - 2 2 8	E 77 + 404		
	26 27 28 29 10	AL 2 2		
	1 1 4 1 4	2. A.		
	F 10 11 12 11	14 15		
	18 27 18 15 28	n 22		
	21 34 25 26 27	28 29		
	10 32 1 2 1	4 5		
	10 10 10 10 10 10 10 10 10 10 10 10 10 1	and the second se		

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)

L User list		Balware	- Import 😨	1/1.000 (0.00) (0.00)
name	liser Account	require users to log on when the next change password	user account expiration date	Edit / Del
Ting	ting	No		/8
Rambil	februer	No	2011-11-22	28
Jigan	jean	No	2020-01-23	/83
		* 260		



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)

Mail Server Network	Setting	
IP :	192.168.1.117	
MASK :	255.255.255.0	
GateWay :	192.168.1.161	
DNS :	168.95.1.1,168.95.192.1	
	OK Network Restart	Cacel





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

3 Add Server		
Domain Name	randoll.com.tw	ex: gnail com Domain can not be repeated
Server	192.168.1.117	6x: 74.125.53.109 or pop gmail.com
Login with domain	8	
Protocol	# POP3 0 IMAP	
Security	* Normal @ TLS @ SSL	
Port	110	
Certification	€ Ignore	
	Connection Test	
		122201010
		2 Save

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)

	Account	Fasaworth	Northe	Spice United	Used	Usgei	Days for Vold	Extend Date	WH	LDAP	Status	Publiking esoper	State
10	sharetech01@randol.com.t	1	sharetect	20 MB	1 MB	5%	FOREVER	9999-12-71	0	0	0	- 1	調
13	sharetech02@randol.com.t	1	sharetect	20 148	1.00	5%	FOREVER	9999-12-31	0	0	0		105
10	shanetech03@randol.com.t		sharetect	50 MI	3 NI	3%	FOREVER	9999-12-31	0	0	0		14
白	starstech04@candol.com.t	1	staretect	20 148	1.168	15%	FOREVER	9999-12-31	0	0	0	-	Elle
Ð	aharetech05@randol.com.t	1	wharetect	20 MB	1 MB	5.%	FOREVER	9999-12-31	0	0	0	-	54
25	sharetech06@randol.com.t	1.100	statement	20.98	1 MB	5.4.	FOREVER	9999.12.31	10	10	0		- Filt

Figure 4-9. 13 POP3 accounts



POP3 Server Lint						
Server	Protocol	Security	Port	Login with domain	Certification	Edit / Del
randoll.com.tw (192.168.1.117)	POP3	Normal	110	0	0	123
Radius Server List Server		* 443		Edit/Del		
		+ 44.0				



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

() Server 192.168	8.1.117 ember	🛫 Domain Name randolf.com.tw	Back
Туре	User •		
Account	sharetech01		
		Save.	

Figure 4-9. 15 Enter POP3 Account



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

E Server Setting				Back
Domáin Name	randull.com.tw			
Server	192.168.1.117	ex: 74.125.53.100 or pop-gmail.com		
Login with domain	2			
Protocol	# POP3 @ IMAP			
Security	* Normal @ TLS @ SSL			
Port	110			
Certification	🖬 Ignore			
	Connection Test			
			III Face	
6 Server Member Se	nting	Choose File No file shosen	Leepont 🕖	1/1 GE (E 15 G
Type		Name	Account	Edit J Dal
User		sharetech01	stureech01	8
			+ A44	
			(woxcaseda)	

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)

5 Add Domain	
Domain name	randoli com tw (ixx: yourdomain.com)
Domain address	Custom • 192 168 1 117
Server name	dhs randoll com tw Custom
Server address	Custom • 192 168 1 117
Administrator's email	sharetech01@randoll.com.tw/ (It is not allowed dot() in account nam
Refeash	10830 seconda
Retry	3600 seconda
Expire	604800 seconds
Minimum	38400 seconds
Treate reverse DNS domain	
	+ Add

Figure 4-9. 17 DNS Server

Setting DNS Server completed. (Figure 4-9.18)

Master Domain	
Domain	Status
randoll.com.tw	/ 🛛
◆ Add	

Figure 4-9. 18 Setting DNS Server completed



Domain name : rastolLcos.tw Neverse DNS domain address Add Resource Record SOA						
Mantur xorvec	Administrator's small	Refresh	Retty	Expire	Minimum	Status
dre randoll.com tw.	sharetech01@randoll.com.tw	10000	3600	664800	38400	1
 Add resource record : MI NS CNAME (A) NS 						
Domain name	Time to the		16	ame anyone .		Edit
randell.com.tw	30430		drs.	with the state of		1
A A	his who					-
Rame	Time to live.		IP Au	idress		EdR
randoll com tw	36400		192,168	1.117(any)-		123
dra randoll.com tw	36420		192 168	1.117(Juny)		123





Select Objects > Authentication > AD User

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

10 AD Setting		
AD Address	Committee Las	
Domain Name		
Account	(maximum 16 characters)	
Password	(maximum MS characters)	
Ignore the AD Group	Commain Computers Domain Controllars Schess Admins Enterprise Admins	
ignore the AD User	Administrator Guest	
	E fave.	

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)

	C use a shared set Auth Settings
When asked how long the idle re-registration	min (range: 1 - 1000)
How long after the user logs requested a re-registration	time (range: 0 - 24,0 representatives of non-limit)
Select Authentication Mode	LAP FEIL (L. Lecal A: AD, P. POP3 Passe follow the custom order by a comm.

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)

Group Name TeamA	
Auth Setting 🕷 General 🗇 User dat Select üser type – Lo	betting Inved setting Call •
	cooldia jason ting
, Alta	1

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)

Groep Name	Member	Auth Setting	Edit / Del
teemA	cooldia jason	General setting	183



2. POP3 (Figure 4-9.13)

group nan	una testgrup
Auth Settings	use a shared ket O Use outlow settings
choose to edit the	r user type POP3 ·
 	anaenechol (POP3 Used)
_	Berger

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)

(6) group list		1/1 田 田 田 田 田
group name	Group members	Edit / Del
bestgroup	sharetech01[POP3 User]	/ 🗃
	* 648.	

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 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)

(f) Basic Setting						
Policy Name	testtest					
Source 🥥	Inside_Any •	P Adde	192.16	al 1.111	MAC Address	
Destination 🕢	Outside_Any •	© P Adde	193			
Action	ACCEPT .					
· Policy						
Protocol			ALL +			
Service Port or Group 👔			User defr	ed · Senice Port		
Software Access Control			None	(1. C.		
QoS			filme +			
Scherlule			time +			
URL Policy			Ninix +	(HTTP port to use with)		
Internet Auth			teamA •			
Using Which WAN			None			
Maximum Concurrent Seas	ens per IP Address		0			
Drop Skype			15			
WEB/FTP Anti-wut			10			
IOP .			8			
Packet tracing			8			
Traffic Analysis			8			
leased-line Set/day			UP 0	KBytes / DOWN 0	KBytes (2 unimited)	
(6) Content Recorder	Select All					
WEB Recorder		FTP Recorder			Outgoing Mail 🔲	
M Recorder 🥥 🛅		MSN Recorder 🔟				
				* 844		

Figure 4-9. 26 Internet Auth Policy



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

No.	Policy Name	Source	Dustination	Services	Action	MOnOff	P	olicy	Edit / Del	Rec
1 -	DNS	Insida Any	Outside_Any	ANY Des	4				/ 88	
2 -	Insliest	192 168 1 111	Outside_Any	ANT	-			0	/8	
3 •	Drop All	Inside_Any	Outside_Any	ANT	0				- / 83	



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

~	ShareTech
5	Subject
rontent Your P	* 192 105 1 111
Over Account :	ing
User Password :	******
	[Tanks]



O 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)



(b) Basic Setting				· · · · · · · · · · · · · · · · · · ·
Policy Name	tinglest			
Source 😧	Inside_Any *	P Addres	192 158 1 118	MAC Address
Destination	· Outside_Any ·	© P Addres	14	
Action	ACCEPT -			
· Policy				
Protocol			ALL .	
Service Port or Group 👔			User defined Sentce Port	
Software Access Control			None •	
QoS		[flume .+	
Scherlule			firms +	
URL Policy			himse + (HTTP port to use with)	
Internet Auth			None •	
Using Which WAN			None	
Maximum Concurrent Seas	ions per IP Address		0	
Drop Skype				
WEB/FTP Anti-wut			8	
IOP .			8	
Packet tracing			8	
Traffic Analysis			0	
leased-line Set/day			UP 0 KBytes / DOWN 0	KBytes (8 unlimited)
· Content Recorder	Select All			
WEB Recorder		FTP Recorder		Outgoing Mail
M Recorder 🥥 🛅		MSN Recorder III		
			+ 444	

Figure 4-9. 29 Internet Auth policy

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

LAND	Batter Nate	Patrice 1	Hardwiner	Palation		0.0	Pier Pierre	C 414 C 71+2	The second second
HQ.	Poncy Name	SUINCH	Destination	Services	Action	Union	Poncy	Entriper	ISEC.
1 •	ONS	Insida Any	Outside_Any	ANY DIS-	-	P		/ 🛛	
2	Tingtast	192.168.1.118	Outside_Any	ANT.	-		8	/ 28	Lag II
3	Drop All	Inside_Any	Outside_Any	ANT	0	*		/88	



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

5	ubject
content	
Your IP	a 192.166.1.118
Unier Account 1	sharetech01
User Password :	

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)

Internet Auth Record	Search Com	lition			
lima .ogin IP Addressea	2011-01-22	00.00 • 2011-01-22 23.59 •			
User Account		(user account belongs to the keyword query)			
State	ALL.				
Auth Successful Method	ALL +				
 Search Result Time 		User Account	Login IP Addresses	State	1/1 H R E
2011-01-22 16	19-13	sharetech01	192 168 1.118	login Success	POP3
2011-01-22 15	20:04	sharetech01	192, 168, 1, 118	idel logout	
2911-01-22 14:	18:24	sharetech01	192 160.1.118	login Success	POP3
2011-01-22 14	15:16	sharetech01@randel.com.tw	192.168.1.118	Jogin Fail	
2011-01-22 14	14:44	sharetech01@rande8.com.tw	192.168.1.118	login Fail	
2011.01.22.54	14:26	abaoatach01	192 168 1 118	Jooin Fail	



Status

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

s	Subject
content	
Your IP	a 192-166-1-118
Over Account 1	sharetech01
And the second sec	5-

Figure 4-9. 33 login interface

User list				
group name	User Account	IP	Kick	Group Kick
testgroup	sharetech01	192.168.1.118	Kick	Kick

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.

Solution Solution Read and Authentication cannot be used together.

Bulletin setting

Select Objects > Bulletin Board > Bulletin setting. Click on 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)

15 Add Group :		
Group Name	mobile	
How long to alert bulletin	24 11	
Before read bulletin, deny all outgoing	8	
After mad bulletin, urt redeect	www.google.com	
*. A 4 4		

Figure 4-10. 1 add new bulletin board

Select.	Group Name	How long to alert bulletin	Before read bulletin, steny all outgoing	After read bulletin, un redirect	Layout
8	123	24H	0	www.google.com	Layout
	mobile	24H	0	www.google.com	Lavout

Figure 4-10. 2 add bulleting completed





1 Layout : Space available (Us	age / All) : 376K/100M			Batk
Group Name mobile				
Select Template 🕷 Basic	c Template 🔍 Image Template 🔍 Image-best	Template 🔍 Path Links		
e Template Setting PC Ver	sion Mulsie Version			
Title of bulleti	Title of bulletin	Welcom		
S. 1. 1. 11. 3	Batton Text	í Have Read	🐵 User Define	
Consense of Doce	Content of bulletin	E dourse B / U Hello Welcom to veit here hope you have a great d	E E 또 표 패 표 Sere · Ar· A· III	
I Have Read	Backgroup Color	Meeco (ex. TIROO	88)	
		E Iare Pr	den farenze	

Figure 4-10. 3 edit mobile authentication content

Click on Preview (Figure 4-10.4)

	Welcom	
Hello	to the last	
probe how	have a great day?	
	I Have Read	

Figure 4-10. 4 Mobile version Bulletin Board Preview



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

Layout : Space available (Usage / All) :	376K/100M		Back
Group Name 123			
Select Template Di Basic Template 1	🖲 Image Template 🔍 Image-text T	emplate 🔍 Path Links	
• Template Setting PC Mesion Mobil	e Version		
Title of hulletin	Title of bulletin	WF series launched	
The of Lineon	Picture Display	1.0	
	Picture Transform	30 Seconda	
	Picture size	Default (800 x 600 pixel) User Define 709 x 296 pixel	
	Select Mode	All Random ⁽ⁱ⁾ User Define (After Saved, Please go to ⁽¹ Picture Management) doing setting)	
100 C	Uplnad Picture	Choose Files No file chosen	
PictureT	Picture Management	Picture Management (Uploaded pictures: 2	
	Hide button	III 🥥	
	Button Text	ll Have Read 🛛 🖶 User Define	
	Backgroup Color	/mm (ex: RIVGGBE)	
I Have Read			
- Lincoln and a start of the			
		E Preciew	

Figure 4-10. 5 edit PC authentication content



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 to add new policy. (Figure 4-10.7)

9 Basic Setting Policy Name . Source 🥥 Inside_Any ❀ IP Address 192.168.1.111 MAC Address Destination () * Outside_Any * ◎ IP Address Pennit + Action · Policy ALL + Protocol Service Pot Service Port or Group 👔 User Defined None • Software Access Control QoS None ٠ None • Schedula URL Access Control None * Authentication None T 123 • Bulletin Board NOT WAN 123 mobile Max. Concurrent Sessions for Each Source IP Address 8 Mail Log & Record WEB/FTP Ami-imm G (DP 6 Botnet None • Packet Tracing 63 Traffic Analysis 6 Max. Quota / Day Up 0 KBytes / Down 0 KBytes (0 No Limit) Max. Quota / Day(Per Source IP) Up 0 KBytes / Down 0 (Ebytes (0 No Limit)

Figure 4-10. 7 add policy

LAN to	WAN Policy : 🌒								174 (1)	i ce li	1.97
No.	Policy Name	Source	Destination	Services	Action	On/Off		Policy	Edit / Del	Log	
1 .		192, 168 1, 111	Outside_Any	ANY	-	P.			123		æ
					6	144		Bulletin 123			

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 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 <u>Kick</u> out.

Group Name	IP Address	Computer Name	When to read the bulletia	Nick	Kick the group
Tent Bulletin	192 168 1 111	TING-PC	2012-08-23 14 51 37	Rick	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 DHCP⁶service 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 (Figure 5-1.1)

⁶ Dynamic Host Configuration Protocol



Chapter 5 : Network Services

Physical Interface	ethO	MAC Address	00.0d.48.31.1a.96
IP Address	182 168 189 150/24	Broadcast	152.168.189.255
OHCP Server Setting :			
Start Address of IP Range 1	192 168 189 1	End Address of IP Range 1	192 168 189 254
Start Address of IP Range 2		End Address of IP Range 2	
Primary DNS	168.95 1.1	Secondary DNS	168 95 192 1
Primary WitNS		Secondary WINS	
Loose fime(minutes)	3600	Max (dase time)minutes)	3600
Default Gateway	192.168.189.150	Enabled	8
Domain Name	internal example.org		



LAN User List

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





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 (Figure 5-1.3)

hysical Interface	ath3	MAC Address	08.0d.48.31 af 73
P Addreas	192 16H 187 2/24	Broadrast	192 168 187 255
DHCP Server Setting :			
Start Address of IP Rarge 1		End Address of IF Range 1	
Start Address of IP Rarge 2		End Address of IP Range 2	
himary DNS	168.95.1.1	Secontary DNS	168.95.192.1
Primary WINS		Secondary WilkIS	
wase Sine(minutes)	10	Max lease time(minutes)	36
Jefault Gateway	192 168 187.2	Enabled	0
Domain Name	internal example org		

Figure 5-1. 3 DMZ DHCP Server



Chapter 5 : Network Services

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.

+ DMZ User List :				7212	170 101 101 101 101
IP Address a	MAC Address +	Start Time	End Time	Hostname ¢	Status +

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)

DHCP Static IP List : ALL	×		1/1 46 6 10
Interface	Computer Name	IP Address	MAC Address

Figure 5-1. 5 DHCP Static IP



• 5-2 DDNS

DDNS⁷, 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" <u>http://www.noip.com/support/knowledgebase/getting-started-with-no-ip-com/</u>
- 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



Chapter 5 : Network Services

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

5 Add Host ;				
Service Provider	3322.org *			
Acetoane	share/27028ech	3322 org	User Define	
Nam	WAN1 .			
Account	share			
assword				
iomment	test DDNS Server			
Enabled	0			



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)

DONS	List : Los Refre	the l					1/1 10 00 00
lark	Updated	Service Provider	Hostname	Account	Wan	Enabled	Comment
3	0	dyndna org	maximax10 dyndris org	maxmax10	WAN2	0	kai test
1	0	3322 arg	share2702tech 3322.org	stars	WAN1	0	for test

Figure 5-2. 2 DDNS Server List



5-3 DNS⁸ 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)



General Setting

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

۲	Allow recursive queries from :							
Γ	ex: 192.168.1.0/24 192.168.6.50/32							
	E Save							



⁸ DNS = Domain Name Servers



Allow recursive queries from :
 192.168.188.186
 ox. 192.168.1.0/24
 192.168.6.50/32

🔲 Salve

Figure 5-3. 3 Allow recursive quires



Chapter 5 : Network Services



•5-4 SNMP

SNMP⁹ 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

10 SNMP Agent							
SNMP Agent	(iii Enable						
Javice Name	Frewall						
Device Location	Taipei, Taiwan						
Community	public						
Contact Parson	help@common.com						
Comment.	Firewall						
5NMP+3	Erable						
Gecurity Level	AuthPriv +						
User Name	public						
Auth Protocol	MD5 Y						
Auth Password							
Privacy Protocol	DES .						
Privacy Password							
La Gave							

Figure 5-4. 1 SNMP

⁹ SNMP = Simple Network Management Protocol



Chapter 5 : Network Services

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)

15 SNMP Agent	
SNMP Agent	🗷 Enable
Device Name	Firewall
Device Location	Taipei, Taiwan
Community	public
Contact Parson	help@common.com
Comment.	Firewall
SNMP+3	Erable Erable
Security Level	AuthPriv +
User Name	public
Auth Protocol	MD5 Y
Auth Password	
Privacy Protocol	DES .
Privacy Password	





MRTG Index Page

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.

Remote Connect Setup							
Enable 🕑							
Server IP 192.168.189.243							
Server Port [514 (UDP 514)							
Log Item							
Packet Tracing Log							
Application Control Log							
IDP Log							
🖬 Sava							

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=7015000000Es8J



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)

E KW 1900 Server 52	O Installer		
solarwinds	Service Install Optio Drose the account th service.	na ot pay would like to use	to install the Kivi
percentary notice if y then you MUST use an ac- Instal the Service using	nu are not using the Local ount that is a member of t	System account to insta the local Administrators	l the service grive.
1. # The LacatDyster A	counts		
C An Admin Account:			
1.00			
Carfeel passend			
		CBack Next's	Canal

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

Onn'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


Chapter 5 : Network Services

13. Please select Policy.

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

b Basic Setting						
Policy Name						
Source 🕢	Image_Any •	III Address		MAC Address		
Destination 🥥	Outside_Any *	© IP Address				
Action	Perrit •					
Policy						
Protocil			ALL *			
Service Port or Group 🥥			User Defined	 Service Port 		
Software Access Control			None •			
RoD			None •			
5c herbole			Norse 🔻			
URL Access Control			None •			
Authentication			None 💌			
Bulletin Board			None •			
ALA.PA			ALL •			
Max. Concument Sessions	for Each Source IP Address		0			
DP			0			
Packet Tracing			8			
Itallic Analysis			0			
Max. Quota / Day			Up 0	KBytes / Down 0	(K8ytes (0;No Limit)	
Max. Quota / DayiPer Sou	ite (P)		Up (D	KBytes / Cown 0	KBytes (0 No Limit)	
Firewall Protection						
SYN Attack III IGMP	Attack 🗄 UDP Attack 🗏 Port Scan					
			+ na.			

Figure 5-5. 10 Select "Packet Tracing"

AN to	WAN Policy : 🕜							1/1 1	10.00
No.	Policy Name	Source	Destination	Services	Action	On/Off	Policy	Edit / Del	Log
1.*		inaida_Any	Outside_Any	ANT D	d 📫	*		123	
2.4		Imside_Any	Cutside_Any	ABT	(14)	4		/23	Lag
Contract (inside_Any	COURSE ANY	BALLE				/23	-
					104 +				





- 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)

Kiwi Sysic	g Service h	hanager (Vers	6×93	
File Edit	View Ma	nage Help		Update mailabi
# 2 m	1 20	Display 00	(Default) +	? Canage feature of the free and control working and the here
Date	Time 13.31.01	Priority Cocorr meto	Hostname Factory Francisco	Message Mig to 1, 2011 111 051-118, 167 76,64 LEN-128 T05-00 PREC-Md0 T1L-128 (D-0132 07 PR0T0-40P SPT-30129 0PT-33251
08-28-2012	13:31:05	Local1.Info	192.168.1.161	Aug 28 13:31:10 (7)w degd[13256]; 1345057503.15 (N=eth0.001* MAC=00.04.48.0e; 26.f2:40:61:06:66.fc;81:08:00 SRC=192.168.1.111.051=192.168.26.164.LEN=52.105=00.PREC=0:00.011.=128.10=0108.0F.PR0110=TCP.SPT=49780.0PT=5000
08-28-2012	13:31:03	Locall Info	192.168.1.161	Aug 28 13:31:07 I7tw dogd[13266] 1346057503 15 IN-eth0 001+ MAC-00:04 48:0e:25 12:40:51:85:56:1c #10:00 SRC-192 368 1.111 DST-118:167.76 64 LEN-130 TOS-00 PREC-0x00 TTL-128 ID-0183 PR0T0-000P SPT-30129 DPT-33351
08-28-2012	13:31:01	Local).Info	192.168.1.161	Aug 28 13 31:05 I/Tw diopd[13266]: 1346057503 15 IN= 0UT-eth0 MAC= SRC=157.55.130.143 DST=192.168.1.111 LEN=141 T0S=00 PRIC=0x00 TTL=50 ID=0 DF PR0T0=UDP SPT=40013 DPT=30135 LEN=121
08-28-2012	13:31:01	Local1.lefo	192.168.1.161	Aug 28 13 31 05 (7hv slogd(13265): 1346057503 15 (N=eth0 001= MAC=00.04 48 0e:25 (2:40:51:05:65:1c (0:40:00 SIIC=192 168 1.111 DST=157 55:130.143 LEN=39 TOS=00 PRIC=0x00 TTL=128 (D=RII2 PR0T0=00P SPT=30129 DPT=40013
08 28 2012	13:31:01	Local1.lefo	192.168.1.161	Aug 28 13:31:05 (7hv vlogd) 3266) 1346057503 (5 IN= OUT=eth0 MAC= SRC=157.55.130 143 DST=192 168.1.111 LEN=136 TOS=00 PREC=1x80 TTL=50 (D=0 DF PR0T0=UDP SP1=40013 DPT=30129 LEN=116
08-28-2012	13:31:01	Local1.lefo	192.168.1.161	Aug 28 13 31:05 (7hv vligdt) 3266); 1346057503 15 (N=eth0 001= NAC=00:04 48:0e:26 (2:40:61:86:66:1e:01:00:00 SRC=192 168:1,111 DST=110:167 76:64 LEN=130 TOS=00 PREC=0x00 TTL=120 (D=0101 PR0T0=00P SPT=30129 DPT=33251
08-28-2012	13:31:01	Local1.Info	152 168 1.161	Aug 28 13:31:05 f7tw ologi@132661_1346057503.15 IN= OUT=eth0 MAC= SRC=157.55.235.161 DST=192.168.1.111 LEN=460 TOS=00 PREC=0x00 TTL=48.00=0 DF PR010=UDP SP1=40028 DPT=30139 LEN=440
08-28-2012	13:31:01	Local1 Info	192.168.1.161	Aug 28 13:31:05 17tw ulogd[13266] 1346057503 15 IN -eth0 0UT - MAC-00:04 48 0e 26 02 40:61:06:06 1e @ 08:00 SRC-192 168 1.111 051-157 55 130 143 UEN-172 T0S-00 PREC-0x00 TTL-120 80-8100 PR0T0-00P SPT-30139 DPT-40013
08-28-2012	13:31:01	Locall Info	192.168.1.161	Aug 28 13:31:05 I7te ulogd[13266] 1346057503 15 IN- OUT-eth0 MAC- SRC-157.55.130.143 DST-192.168.1.111 LEN-39 T0S-00 PREC-0x00 TTL-50 ID-0 DF PR0T0-UDP SPT-40013 DPT-30139 LEN-19
08-28-2012	13:31:01	Local1 Info	192.168.1.161	Aug 28 13 31:05 I/Tw ologd(13266): 1346057503 15 IN-eth0 0UT- MAC-00.04 48 0e:26 (2:40:61:86:56 ie:#:00:00 SRC-192 168 1.111 D5T-157 55 235 161 LEN-59 T05-00 PREC-0x00 TTL-128 ID-0179 PR0T0-00P SPT-30139 0PT-40028
08-28-2012	13:31:01	Locall Info	192.168.1.161	Aug 28 13 31:05 17tw ologo[13266] 1346057503 15 IN -eth0 0UT - MAC-00:04 48 0e:26 (2:40:61-86:66:1c:8:08:00 SRC-132 168 1, 111 051-157 55, 120:143 LEN-167 T05-00 PREC-0x00 TTL-128 ID-8178 PROT0-00P SPT-30139 DP1-40013
08-28-2012	13.30.43	Local Jefu	192.168.1.161	Aug 28 13 30 47 I/Tw ulspft132661 1346057503 15 IN-eth0 0UT- MAC-00.04 48 0e 26 (2:40:61:86:56:1c:8:00:90 SRC-192 108 1.111 05T-111 254 100.144 UEN-144 T05-00 PREC-0x40 TTL-120 ID-0T72 DF PR0T0-00P SPT-30129 DPT-34524
08-28-2012	13:30:40	Local1.Info	192.168.1.161	Aug 28 13:30:44 I7tv-ulogd[13266] 1346057503:15 IN= OUT=ethD MAC= SRC=85:55:223:29:05T=192:168:1.111 LEN=40:T05=08 PREC=0x00:T11=46 ID=28260 DF PR010=TCP: SPT=40020:DPT=45349:5EQ=2474514379:ACK=3770563196:WINDUW=02:ACK
08-28-2012	13:30:39	Local1 Islo	192.168.1.161	Aug 28 13:38:43 I7fw ulogd[13266] 1346057503 15 IN=eth0 0UT= MAC=00:04:48:0e:26 (2:40:61:86:86:ie:#:08:00 SRC=132:168 1.111 DST=65:55 222:29 LEN=44 105=00 PREC=0x00 TTL=128 ID=0171 DF PR010=1CP SP1=49343 DPT=40020
08-28-2012	13:30:39	Local1.Info	192.168.1.161	Aug 28 13:38:43 (7hv ulogd[13268]: 1346057503:15 IN= 0UT=eth0 MAC= SRC=65:55:223:29 DST=132:168:1.111 LEN=50 T05=00 PREC=0x00 T11=46 ID=20790 DF PROT0=TCP SPT=40020 DPT=43049 SEQ=2474514369 ACX=3770965132 WIND/W=ID ACX PSH
08-28-2012	13:30:39	Local1.Info	192.168.1.161	Aug 28 13:36:43 (7)w ologo[13268]; 1346057503:15 (N=eth0 0UT= MAC=00:04:48:0e:26:62:40:61:86:86:ic:#:00:00 5RC=192:168:1:111 DST=111:254:100:144 LEN=144 TOS=00 PREC=0x00 TTL=128 (D=8120 DF PROTO=0DF SPT=30128 DPT=34524
				1003; 100 MPH 13.44 00-20-2012



opra enerox.							Section of the
192.168.1.161/Program Time	sinc IP	pbp?in=1346057 DST IP	WAN	Protocol	Packet Size	SRC Part	DST Pot
2012-00-28 13:48:21	192 168 1 111	65.55 223 29	2	TCP	427	49349	40020
2012-08-28 13 48:21	68.55.223.29	192 168 1 111	Ð	TCP	40	40020	41349
2012-06-28 13 48 21	192 168 1 111	36.226.38.217		TCP	40	49950	6523
2012-86-28 13 48 21	64.4.44.51	192 568 1.111	Ð	TCP	310	.443	49355
2012-06-28 13 48:21	192,168.1.111	65 55 223 29	B	TCP	42	49349	40020
2012-08-28 13 48:21	36.226.36.217	192 168 1 111	D	TCP	67	6623	49950
2012-08-28 13 48-21	192,168,1,111	66.220.151.99	Ð	TCP	40	49361	6222
2012-08-28 13 48:21	64.4.44.51	192 168 1 111	8	TCP	40	443	48356
2012-68-28 13 48:21	66.220.151.99	192 168 1 111	Ð	TCP	402	6222	49351
012-06-28 13:48:21	86.220.151.99	192, 168, 1, 111		TCP	40	6222	49351
012-06-26 13:48:21	192.168 1.111	64.4.44.51	Ð	TCP	40	49356	443
2012-08-28 13 48 20	192.168.1.111	06.220.151.99	8	TCP	253	49351	5222
012-06-28 13:48:20	64.4.44.61	192 168 1 111	8	TCP	309	443	49356
2012-00-28 13 48:20	114.37.114.12	192.160.1.111	B	TCP.	ab	19460	49949
2012-08-28 13:48:20	192 168 1 111	64.4.44.51	Ð	TCP	310	49356	443
012-68-28 13:48:20	64.4.44.51	192 168 1 111	2	TOP	306	443	49356
2012-08-28 13 48 20	192.168.1.111	65 55 223 29	E	TCP	40	49349	40620
2012-06-26 13:48:20	192.168.1.111	54.4.44.51	Ð	TCP.	311	49355	443
2012-06-28 13:48:20	65.55.223.29	192.568.1.111	E	TCP	44	40020	49349
2012-08-28 13 48 20	65 55 223 29	192.168 1 111	2	TCP	40	40029	49349
2012-68-28 13 48 20	192 16B 1.111	64.4.44.51	Ð	TCP	40	49366	443
2012-08-28 13 48 20	64.4.44.51	192 168 1 111	2	TCP	80	443	45356
2012-08-28 13 48 20	64.4.44.51	192 168 1 111	Ð	TCP	495	443	49356

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)

K. wit Typele	ing Service I	Lalager (Versid	192		
Tile Edg	View Ma	rage Help			
Setup		1111111	Cbl+P	1	7 Consume homeans of the form and Revenue sections
Send b	ett message	e to localhort	Chi+T	-	Manage PE#Web#Svalon T
Purge		-		4.254	kernet: '000780184501 ACCEPT LOG ' SRC-192 168 254 253 DST-61 220 8 48 PROTO-UDP SPT-63 DPT-6150 LEN-119 WAN-1 DIR-out MARK-1019248736563 (Thu- Jun 38 12-00 60 2011)
Export	settings to	ern (Dist nice 3NE film		4.254	kernet '000700104601 ACCEPT LOG ' SRC-61.220.0.40 DS1-192 168.254 253 PROTO-UDP SP1-6150 DP1-53 LEN-73 WAN-1 DIR-in MARK-10192407305e5 (Thu Jun 30 12:00 to 2011)
Create	Tech-Supp	ort File (Zip)		4,254	kennel: 1091210164006 ACCEPT LOG : SRC-192 160 254.30 DST-213 146 109 205 PR0T0-TCP SPT-1161 DPT-12250 LEN-40 WAN-1 DIR-out NARK-101914626666
Estt				4.254	kennel: 1012/10164006.4CCEPT LOB 15RC-213.146.103.205 D5T-152.168.254.30 PROTO-TCP SPT-12350 DPT-1161 LEN-40 WAM-1 DIR-in NARK-101914b2b606
95-30-2011	11:58:57	Kenel Notice	192.168.2	54.254	kennel: 101218164086 ACCEPT LOB 1 SRC-213.146.183.205 DST-192.168.254.30 PR0T0-TCP SPT-12350 DPT-1161 LEN-45 WAM-1 DIR-in NARK-101914k2b608
05-30-2011	11:58:57	Kernel Notice	192.168.2	54.254	kennel: '080708184601 ACCEPT LOG ' SRC-66.249.68.1 DST-192.168.254.253 PROT0-TCP SPT-45345 DPT-80 LEN-52 WAN-1 DIR-in MARK-1019248736549 [Thu
05-38-2011	11:58:57	Kemel Notice	192.168.2	54.254	kensel 1/20070184601 ACCEPT LDG 1 SRC-66.249.68.1 DST=192.168.254.253 PROT0=TCP SPT=45345 DPT=80 LEN=52 WAN=1 DIR-in MARK=101924873b5e9 [Thu
05-30-2011	11:58:57	Kernel Notice	192,168.2	54.254	kernel: 1000700184601 ACCEPT LOG * SRC-66.245.68.1 DST-192.168.254.253 PROT0-TCP SPT-45345 DPT-80 LEN-52 WAN-1 DIR-in MARK-10192487305e9 [Thu
05-30-2011	11:58:57	Kernel Notico	192,168,2	54,254	kemet: 1000/08184691 ACCEPT LOG ' SRC-66.245.68.1 DST-192.168.254.253 PROT0-TCP SPT-45345 DPT-80 LEN-52 WAN-1 DIR-in MARK-103924873b5e9 [Thu
05-30-2011	11:50:56	Komel Notice	192 168.2	54,254	kanet 191210164006 ACCEPT LOG * SRC-192 160 254.30 DST-213 146 109 205 PRDT0-TCP SPT-1161 DPT-12250 LEN-45 WAN-1 DIR-out NARK-101914b2bb066 The law 01 1 55 59 2011
05-30-2011	11:58:56	Kamel Notice	192,168,2	54.254	kmisk 100700104001 ACCEPT LOG 1 SRC-66.245.08.1 DST-192.168.254.253 PR0T0-TCP SPT-45345 DPT-00 LEN-52 WAN-1 DIR-is WARK-1019240236543 [Thu and a 11-154-59 2011]
05-30-2011	11:58:56	Kennel Notice	192.168.2	54.254	kennel: 1000/0018468/1 ACCEPT LOG * SRC-66.249.68.1 DST=192.168.254.253 PROT0=1CP SPT=45345 DPT=80 LEN=52 WAN=1 DIR-in WARK=10192482365e3 [Thu Line 20 Line 20 Directory 20 Di
05-30-2011	11:58:56	Kernel Notice	192 168 2	54.254	kemel: 100708184681 ACCEPT LOG ' SRC-66.249.68.1 DST-192.168.254.253 PROT0-TCP SPT-45345 DPT-80 LEN-52 WAN-1 DIR-in MARK-10192482365e9 [Thu
05-38-2011	11:58:56	KamalNotice	192,168,2	54.254	kenet: '000708184601 ACCEPT LOG ' SRC-66.249.68.1 DST=192.168.254.253 PROT0=TCP SPT=45345 DPT=80 LEN=52 WAN=1 DIR-in MARK=1019248736549 [Thu
05-30-2011	11:58:56	KenelNotice	192,168.2	54.254	kernel: '0807/08184601 ACCEPT LOG ' SRC-66.249.68.1 DST-192.168.254.253 PROT0=TCP SPT-45345 DPT-80 LEN=52 WAN=1 DIR-in MARK=10192487365e9 [Thu
05-30-2011	11:58:56	Keinel Notico	192,168.2	54,254	keinet: '080708184661 ACCEPT LOG ' SRC-66.249.68.1 DST=192.168.254.253 PROTO=TCP SPT=45345 DPT=80 LEN=52 WAN=1 DIR-in MARK=103924873b5e9 (Thu Jun 30 11:59:59.2011)
06-30-2011	11:58:56	Kernel Notice	192,168.2	54,254	kernet: 1002/00104601 ACCEPT LOG / SRC-66.243 68.1 DST-192.168.254.253 PROT0=TCP SPT-45345 DPT-80 LEN-52 WAN-1 DIR-in MARK-101924823b5e3 (Thu Jun 30.11-59.59.2011)
05-30-2011	11:58:55	Kamal Notice	192,148.2	54.254	Kernel: 100700104021 ACCEPT LOG ' SRC-66.249.08.1 DST-192.168.254.253 PROT0=TCP SPT-45345 DPT-80 LEN-52 WAN-1 DIR-in WARK-1019248236549 [Thu June 20.11:54:553.2011]
05-30-2011	11:58:55	Kernel Notice	192,168,2	54.254	kernet: 1002/0104021 ACCEPT LOG 1 SRC-66.249.68.1 DST-192.168.254.253 PR010-1CP SPT-45345 DPT-80 LEN-52 WAN-1 DIR-in WARK-1019248/365ir9 [Thu Jun 30 11:59:59 2011]

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"



Chapter 5 : Network Services

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

Construction Description Description <thdescription< th=""> <thdescription< th=""></thdescription<></thdescription<>
2012-08-28 12:18:29,Locall.ixto, 192,168,1.161,Aug 28 12:18:34 17fw ulogd 13266 : 1346057503.15 N=07D=010 MAC=SRC=174,120.252, 2012-08-28 12:18:29,Locall.ixto, 192,168,1.161,Aug 28 12:18:34 17fw ulogd 13266 : 1346057503.15 N=07D=010 MAC=SRC=174,120.252, 2012-08-28 12:18:29,Locall.ixto, 192,168,1.161,Aug 28 12:18:34 17fw ulogd 13266 : 1346057503.15 N=07D=010 MAC=SRC=174,120.252, 2012-08-28 12:18:29,Locall.ixto, 192,168,1.161,Aug 28 12:18:34 17fw ulogd 13266 : 1346057503.15 N=07D=010 MAC=SRC=174,120.252, 2012-08-28 12:18:30,Locall.ixto, 192,168,1.161,Aug 28 12:18:34 17fw ulogd 13266 : 1346057503.15 N=07D=010 MAC=SRC=174,120.252, 2012-08-28 12:18:30,Locall.ixto, 192,168,1.161,Aug 28 12:18:34 17fw ulogd 13266 : 1346057503.15 N=07D=010 MAC=SRC=174,120.252, 2012-08-28 12:18:30,Locall.ixto, 192,168,1.161,Aug 28 12:18:34 17fw ulogd 13266 : 1346057503.15 N=07D=010 MAC=SRC=174,120.252, 2012-08-28 12:18:30,Locall.ixto, 192,168,1.161,Aug 28 12:18:34 17fw ulogd 13266 : 1346057503.15 N=07D=010 MAC=SRC=174,120.252, 2012-08-28 12:18:30,Locall.ixto, 192,168,1.161,Aug 28 12:18:34 17fw ulogd 13266 : 1346057503.15 N=07D=010 MAC=SRC=174,120.252, 2012-08-28 12:18:30,Locall.ixto, 192,168,1.161,Aug 28 12:18:34 17fw ulogd 13266 : 1346057503.15 N=07D=010 MAC=SRC=174,120.252, 2012-08-28 12:18:30,Locall.ixto, 192,168,1.161,Aug 28 12:18:34 17fw ulogd 13266 : 1346057503.15 N=07D=010 MAC=SRC=174,120.252, 2012-08-28 12:18:30,Locall.ixto, 192,168,1.161,Aug 28 12:18:34 17fw ulogd 13266 : 1346057503.15 N=07D=010 MAC=SRC=174,120,252, 2012-08-28 12:18:30,Locall.ixto, 192,168,1.161,Aug 28 12:18:34 17fw ulogd 13266 : 1346057503.15 N=07D=010 MAC=SRC=174,120,252, 2012-08-28 12:18:30,Locall.ixto, 192,168,1.161,Aug 28 12:18:34 17fw ulogd 13266 : 1346057503.15 N=07D=010 MAC=SRC=174,120,252, 2012-08-28 12:18:30,Locall.ixto, 192,168,1.161,Aug 28 12:18:34 17fw ulogd 13266 : 1346057503.15 N=07D=010 MAC=SRC=174,120,252,

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 IDP¹⁰ (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.

- 6-1 IDP Setting
- 6-2 IDP Log

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 IDS¹¹ and IPS¹² 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			
Basic Setting IDP Advanced Setting	. Click save after completing setting.		
	Risk Level	Action	Log
	High Thick (333)		•
	Medium Risk (503)	6 C C C C C C C C C C C C C C C C C C C	0

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 <u>IDP Advanced Settings</u> link, you will see a view as below figure. On the other hand, click on <u>IDP Basic Setting</u> to get back previous step. Setting your IDP function, and then do not forget to click on <u>Save</u>. 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



Chapter 6 : IDP

Advanced Setting IDP Basic Setting (22:0)		🐁 Click save after completing setting. 🔲 2×++.			
	Group Name			Action	Log
	ATTACK-RESPONSES (u) /		40	0
	BACKDOOR (214)	Group Name	Risk Loval		0
	BLACKLIST (8)	ATTACK-RESPONSEB command completed		40	0
	BOTHET-CNC (16)	ATTACK RESPONSET successful onlytics and emited CORR F	- Q		0
	CHAT (24)	ATTACK-RESPONSES successful poblies sub sightluniame	î	4	0
	DDOS (6)	ATTACK-RESPONSES successful kadmind buffer overflow attempt	M.		0
	DELETED (202)	ATTACK-RESPONSES successful ladmind buffer overflow attempt	M	4	0
	DNS (13)	ATTACK RESPONSES successful cross site scruting furced downlined attempt	÷ 1	аф. (0
	005 (8)	ATTACK-RESPONDES command enter	1	140-	0
	EXPLOIT (37)	ATTACK RESPONSES Invalid URL	1	- 1	0
	FINGER (12)	ATTACK-REBPONSEB directory Testing	1	10	0
	FTP (16)		- MUN	si i	0
	ICMP (62)			40	0
	ICMPv6 (2)			аф. (0
	INEQ. (4).			10	0

Figure 6-1. 2 IDP Advanced Setting



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

Figure 6-1. 3 Risk Group Name

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

10 Basic Setting		
Policy Name		
Source 🕥	Outside_Any	© IP Address
Destination		
Action	Permit •	
* Policy		
Protocal	ALL .	
Service Port or Group	User defined Service Pod	
GoS	None •	
Schedule	Nons •	
Max. Concurrent Sessions for Each Source IP Address	0	
IDP	2	
Packet Tracing	0	
Traffic Analysie	-	
NAT	0	
5 Finewall Protection		
SYN Attack III ICMP Attack	BUDP Attack Port Scan	
		+ 434

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)



Search Results

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

6 Search Results							1/5	1 🖂 🕫	a a a Espor
Date +	Event .	Group Name +	Risk Level +	Interface +	Source IP Address #	Destination IP Address +	Protocol .	Source Port +	Destination Part
2011-11-08 06 35 27	P2P Skype client start up get latest version attempt	P2P	Med	LAN	182 168 99 117	204.9 163 158	TOP	43909	80
2011-10-24 11:09:44	WEB-PHP vestopic 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 vewtopic php access	WEB-PHP	Mert	LAN	192.168.99.120	202 39 234 30	TCP	609/17	80
2011-10-24 11:09:43	WEB-PHP vestopic php access	WEBPHP	Med	LAN	192.168.99.126	202.39.234.38	TCP	60817	80
2011-10-24 11:05:43	WEB PHP viewtopic php access.	WEB-PHP	Meit	LAN	192.168.99.120	118.215 191.139	TCP	60521	80
2011-10-24 11:09:43	WEB-PHP vestopic php access	WEB-PHP	Meit	LAN	192 168 99 126	202 39 234 36	TCP	60915	80
2011-10-24 11 03 43	WEB PHP viewtopic php access.	WEB-PHP	Med	LAN	192 168 99 126	202 39 234 38	TCP	6091E	60
2011-10-34 11 08 43	WEB-PHP vewtopic php access	WEB-PHP	Mad	LAN	192.168.99.126	202 39 234 38	TCP	60916	80
2011-10-24 11:09:07	WEB-PHP viewtopic php accesa	WEB-PHP	Mad	LAN	192 168 99 126	74.125 71.155	TCP	60889	86
2011-10-34 11 09 07	WEB-PHP vewtopic php access	WEB-PHP	Mad	LAN	192.168.99.126	202 39 234 36	TCP	60880	80
2011-10-24 11:05:06	WEB-PHP vewtopic php access	WEB-PHP	Med	LAN	192,168.99.126	202 39 234 38	TCP	60876	86
2011-10-24 11 09:06	WEB-PHP wewtopic php access	WEB-PHP	Med	LAN	192 168 99 124	202.39.234.38	TCP	08808	80
2011-10-24 11.06.27	WEB-PHP viewtopic php access	WEB-PHP	Met	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	102 168 99 126	202 39 234 38	TCP	SOME	80
2011-10-24 11:00:25	WEB-PHP viewtopic php access	WEB-PHP	Meit	LAN	192.165.99.126	74.125.71.155	TCP	60811	80
2011-10-24 11 08:26	WEB FHP wewtopic php access	WEB-PHP	Mad	LAN	192 168 99 126	202 39 234 38	TOP	60867	80

Figure 6-2. 2 IDP Log Search Results



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
- 7-2 SSL VPN Log
- 7-3 VPN Policy
- 7-4 SSL From your Android Phone



•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 <u>Modify the Server Setting</u> 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.



Salaria Semila	Start @ Stop Note	· h will take a fi	ex seconds to sta	rt, please be patient.		
Local Interface	Want - Deine					
Local Port	367					
Max concurrent connections	20 (Range 20 -	256)				
Client IP Range	10 8 0 0	/ 255	255 255	0 (Client IP sample need different with	LAN DMZ interface (
DRS Sener 1	168.95.1.1					
DNS Server 2	168.95.192.1					
WINS Server 1						
WINS Senior 2						
WINS Server 2						
WINS Server 2 5 Certificate Setting CA's Name	LTFW_SSLVPN_CA			Country	TW	0
WHIS Server 2 © Certificate Setting CA's Name Province of State	LTFW_SSLVPN_CA			Country City	TW Taipei	0
WHIS Server 2 © Certificate Setting CA's Name Province of State Organization	LTFW_SSLVPN_CA TC Common Inc.	3		Country City Unit	TW Taipei L7FW Team	0
WHIS Server 2 Certificate Setting CA's Name Province of State Organization Certificate Name	LTPW_SSLVPN_CA TC Common Inc L7FWSSLVPNCA			Country City Chrit Centificate E-mail	TW Taipei L7FW Team help@common.com	
WHIS Server 2 Certificate Setting CA's Name Province as State Organization Certificate Name Server Name	LTFW_SSLVPN_CA TC Common Inc. L7FWSSLVPNCA L7FW_SSLVPN_SERVE			Country City Link Centificate E-mail	TW Taipei L7FW Team help@commos.com	



SSL Client List

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

add User Account			
name	Ting	(maximum 16 characters)	
User Account	ting	(maximum 16 charactera)	
Password		(case-senaltive, please use 3 to 16 characters, not with the same account	t number
Password Detection	weak much stran	9	
Contim password			
0	require users to log	n when the next change password	
user account expiration date	[B		
	** * 一月 20	**	
	8 - 2 =	± π + Δ04	
	26 27 28 29	H F	
	1 1 4 1	경망	
	9 H H H H	14 15	
	18 17 18 10	n 2.	
	20 34 25 26	A 2)	
	10 32 1 2		
	e :#2 -	- ALC	

Figure 7-1. 2 Create Authentication account

👍 User list		Baiwse	- Import 🕑	1/1 100 100 100
name	User Account	require users to log on when the next change password	user account expiration date	Edit / Del
Ting	ting	No		/8
Rambal	febres	No	2011-11-22	/8
Jean	jean	340	2020-01-23	/83
source and a		* 864		Pro 200

Figure 7-1. 3 Authentication User List



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

Edit Group Nembers	
Group Name IsamA	
Auth Setting Diserdet Select üser type Lp	setting ned satting cal 🕶
	cooldia jason ing
a lidat.	

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)

Groep Name	Member	Auth Setting	Edit / Del
teamA	cooldia jason	General setting	18

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 to create a new certification SSL VPN Group. (Figure 7-1.6) (Figure 7-1.7)

2umment	sshipn
Authentication Group	(Complete Group' setting in 'Objects > Authentication > User Group' before adding SSI, VPN authentication group.)

Figure 7-1. 6 New Certification Group



SOL CHRITTLIST HQ:	develace Celoncare		OR 180 187 8
Comment	Authentication Group	User Management	Delete
asiype	teamA	Group Member Number 3	
	scool data	* 144	
	They can		
	ting		

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

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

Group Man	aber List					111.00 0.00 0
User Account	Cancel Certificate	Re-generate Certificate	Download	Set the user a static IP address	Suspended	Set Static MAC Address
cookda	Cancel Certificate	Beigenerate Certificate		# Adit	Not Disabled 🥒 Ed it	d Hatat
jason	Gancel Certificate	Re-generate Certificate	(🖋 Ed it	Not Divotted @ Ed.it	de Edit
terg	Gancel Certificate	Be-generate Certilicate	1901	a Rdat	Not Disabled 🧈 8d it	🥔 E.d. it.

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)

Interface Name affet		Connection Tune	PPPoE . Deal Decompet
IP Addama	1444 052 TO 274	Natranik	The buy buy buy
D.L.a.Colonia	HOR OF BRIDE	1140 54555	45 40 19 50 40 FF
Depart Galeway	156.09, 08.254	MAC ADDRESS	00/00/48/32/60/EE
Account	88792199@fimet.net	Passwird	
Up Speed Max, 1000Mbps (3Mbps • Mass.Defina	Down Speed(Max. 1000Maps.)	tMbpsUxer.Dyline
Speed and Duplex Mode	Auto • 100Mb/Full	MIL	1500
Load Balance	() Auto	· Manual	1 -
	C By Source IP	© By Destination IP	
WAN Alive Detection			
Detection Method	O DNS # KMP O NONE	Detected IP Address	168.95.1.1
Administrator Management	図 Pag 目HTTP 図 HTTPS		
Firewall Protection			
Filewall Protection Items	R SYN R IOMP R UDF	Pon Scan	
S General Setting			
DNS Server 1	168 35.1,1	DNS Server 2	168 95 192 1
HTTP Port	80	HTTPS Part	443
	and the second s		

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

Enter <u>https://111.252.70.234:443/sslvpn.php</u> 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.

191	92	末の	
bin	爆震道共共		
corfig	保険波利用		
diver	植五黄科丰		
log	福倉営共工		
shpn-qui-103-en	用用電気		110)

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)

Refuse Connection Log						
Refuse Connection Log	O Start 🗣 Stop 🌘	Les				
User List					17	1.00.00.00
Account a	Status 4	Source IP Address	Local IP Address	Last Connection	Kick	Log
cooldia	8.				Kickcooldia	Log
Binnet C			-		Kiciding	(Test)





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. OFF 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 t	to Internal		
& Basic Setting :			
Policy Name			
Source	VPN_Any •	IP Addess	MAC Address
Destination	* Inside_Any •	IP Address	
Action	DROP •		
9 Policy 1			
Protoc #	ALL •		
Senice Port or Group	User custom		
GoS	bionu .*		
Schedule	Norm •		
Packet Tracing	8		
Traffic Analysis	13		
NAT	60		
		+ A.I.G	

Figure 7-3. 1 VPN to Internal

Internal to VPN 6 Elwsin: Setting : Policy Name MAC Address * [inside_Any *] Source O P Abbess * VPN_Any * Destination (FIP.Addwsii) DROF . Action 1 Policy (ALL . Protoc.pl Senice Port or Group Service Part User custom Q6S None .* Schedule Norm V Packet Tracing 12 Traffic Analysis 13 + 214

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

	é
er POPS, RACIUS User AD User User Group Log Status	
HTING (maximum 16 characters)	
ting (maximum 16 characters) 🥥	
reserved (Please input 3 to 56 characters, nut the same with account	ant)
West Far Strong	
Require Password Change at Next Login	
(III)	
	Image: status AD ther Meet Status 3-TTNG (maximum 16 characters) freg (maximum 16 characters) freg (maximum 16 characters) freg (maximum 16 characters) freg (maximum 16 characters) maximum 16 characters) Image: status free Storng Image: status maximum Storng maximum Image: status Require Passesend Charge at Next Login

Figure 7-4. 1 Add an authentication account

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

Auth Setting	Local Unit	POPS, RADIUS USA	All Movers	UserGroup Log Status			
User List	Accourt	e 💌)	植成杨紫 未没得有末	Import () 212	2	100.00.00
Name		Account	Nequire Pasa	word Change at Next Login	Account Expiration Date	1	Edit / Del
1 TING		Ting		Tip			183

Figure 7-4. 2 User List



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

Objects > Authentication > User Group

Auto Setting	odar User POIDS, RADRUST	User All Oser User Group	Log Status	
Add Group Humber)		Provide and and and and	
		Group Name android	1_SSL	
		Auth Setting 🖶 Generat D User d Select user type 🛛 Lo	al setting ednad setting scall =	
	rando8 jaan kinn syncs jinsen Lin_JC kud gary 智耀 CK coatt KAQA coatt3 venpeds easen 發表會專購		LTVIG	

Figure 7-4. 3 add Group Member

Auth Setting LocalUser POPP	RADIUS User ADTUSET User Group La	g Value	
Group List			2/2 2 00 11 11 11
Group Name	Member	Auth Setting	Edit / Del
android_SSL	LTING	General setting	/ 23

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

SSL VPN Setup SSL C	ent List	
New Certification Group		
Comment	sharetech_ting	
Authentication Group	nsitechSSH •	
Address of information message	www.google.com.tw	

Figure 7-4. 5 Add a New Certification Group

SSL VPN > SSL VPN Setting > SSL Client List

	SSE VITH Selip SSE Che	and Liest		
	w] : ptttPS Port) /witypn.php	111 (10 (0) (0) (0)		
	Comment	Authentication Group	User Management	Delete
	shareforth find	android SSL	Genus Member Number 1	123

Figure 7-4. 6 SSL Client List



5. Start SSL VPN

SSL VPN > SSL VPN Setting > SSL VPN Setup

SSL VEW Serup SSL	Clean List			
Server Setting Modify the and download again.	e Server Setting Note : System w	vill cancel all certificates after modification	on (except service status). Ple	ase Re-generate certificate
Service Status	🕷 Start 🛈 Stop: Note It ei	ill faixe a few seconds to start, piessa be pat	ient.	
ocal interface	peterms dyndms biz	Asseit		
	wan1 : 60.249 6 194.60.249.6 10 wan2 : 220.132.217 122	85,60,249,6,186,60,249,6,214		
.ocal Port	443 - 450			
Nax concurrent connections	50 (Range 20 - 60)			
Jiert IP Range	10.8.0.0	55 255 0 0 Client I	P cange need different with LAN.	(IMZ interface.)
WS Server 1	192.168.188.1			
WS Server 2	168.95 192 1			
MNS Server 1				
MNS Server 1 MNS Server 2				
MNS Server 1 MNS Server 2				
WHS Server 1 WNS Server 2 Centificate Setting			- 90.0	
WHS Server 1 WHS Server 2 • Certificate Setting A's Name	L7FW_SSLVPN_CA	Country	TW	0
WHS Server 1 WHS Server 2 Cartificate Setting Ws Name Vroince or State	L7FW_SSLVPN_CA	Cruntry City	(TW (Taipei	0
WHS Server 1 WHS Server 2 Contificate Setting Wis Name Province or State Organization	L7FIV_SSLVPN_CA TC Common Inc.	Crurbý City Uni	TW Taipei L7FW Team	•
MHS Server 1 MHS Server 2 Contificate Sotting 24's Name hownce or State Joganization Jordificate Name	L7FW_SSLVPN_CA TC Common Inc L7FWSSLVPNCA	Crumbry City Uni Certificate E-mail	TW Taipei L7FW Team help@common.com	•

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

Interface Name-eth1	0	Connection Type	Static .	
IP Addess	60.249.6.184	Netmaali	256 256 255	5.0
Default Gateway	60 249 6 764	MAC Address	08 00 48 32	C9.90
Up Speed Max. 1000Mops)	10Mbps 💽 User Define	Down Speed(Max. 1000Mbps)	51200	(tope) Define by System
Speed and Duplex Mode	Auto	MTU	1500	
Load Balance	🗣 Auto	© Manual	1 +	
	(D By Source (P	() By Destination IP		
U WAN Alive Detection				
Detection Method	DIENS . ICMP O NONE	Les Delected IP A	ddress (60 249 6 254
Administrator Management	Reag IDATE MATES			
Firewall Protection				
Firewall Protection Items	WISYN WICHP	EUDP Port Scan		
9 General Setting				
DNS Server 1	168 95.1.1	DHS Saver 2	168.95	192.1
	6088	HTTPS Part	8443	
HTTP:Poet				

8. Enter Server Information





9. Connection establish and Authorizing



10. Address of information message

SSL VPN > SSL VPN Set	ting		4
SSL VPH Setup	Bent List		
New Certification Group			
Comment	sharetech_ting		
Authentication Group	nsitechSSH .		
Address of information message	www.google.com.tw		
		+ A66	
	/		

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







12. SSL VPN Log

SSL VPN >	SSL VPN Log	2								
SSI Chi	at On Law Log									
Refuse Con	nection Log									
Raflusa Connect	ian Log	Start © Stop	(Lag)							
E User List	. On fine	t Account			2/2	2		1.00		81
Account #	Status a	Source IP Addres	a Local IP Address	Last Connection	Local Interface		Kick		1	og
ting	16	116 55 243 182-606	3E 10 8 0 34	2013 05-08 12 21 27			Kiciting		1	14

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?

10-1 SSLVPN

oadlar

Local IP.

Route Information



16. Setting







17. SSL Version



18. SSL VPN Connection Logs





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

IPSec¹³ 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 IKE¹⁴. 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 **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. Solution Sector 2018 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. Subnet in CIDR notation.

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.
- ISAKMP¹⁵: It provides the way to create the SA¹⁶ 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. AES¹⁷: All using a 128-bit, 192-bit and 256-bit key. AES is a commonly seen and adopted nowadays.
 - 2. 3DES¹⁸: Triple DES is a block cipher formed from the DES¹⁹ cipher by using it three times. It can achieve an algorithm up to 168 bits.
 - 3. SHA1: The SHA1 is a revision of SHA²⁰. It has improved the shortcomings of SHA. By producing summary hash values, it can achieve an algorithm up to 160 bits.
 - MD5²¹ 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.

- ¹⁶ SA = Security Association
- ¹⁷ AES = Advanced Encryption Standard
- ¹⁸ 3DES = Triple-DES

¹⁵ ISAKMP = Internet Security Association Key Management Protocol

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

* Add New Connection :			
Enabled	8		
IPSec Turnel Name	connect to A		
Interface	© WAN1 ♥ WAN2 ◎ :	WAND	
Remote IP Address	# IP Address or Doman	211 20 227 193	Dynamic IP Aldress
Local Subnet	192.168.99.0	255 255 255 0 (/24)	
Remote Subnet	192 168 168 0	255 255 255 0 (/24)	
IKE Setting (Phase1)			
Connection Type	@ Main @ Aggressive		
Presihare Key	123456	1	
ISAKMP	aos • shat • DH G	Broup 2 🔹 🖬 Auto Matr	thing
Local ID	# WAN IP Domain N	tame (g)	
Remote ID	* WAN IP Domain N	kernel (0	
IKE SA Lifetime	3 • Hour(a)		
IPSec Setting (Phase 2)			
IPSec	aes 🔻 shat 🔹 🕷 A	uto Matching	
Perfect Forward Secrecy (PFS)	🖲 No 🗇 Yes		
IPSec 5A Lifetime	(3 • Hourss)		
Tead Peer Detection	restart • Delay 10	Seconds Time out	60 Seconds
Chop SMB Protocol			

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)

IPSec Tunnel Name	Interface	Local Subset ¢	Status	Romote IP Address +	Remote Subnet #	phase 1	phase 2	Operation time	Enabled	Edit / Del	Log
Econoect to A	•	192,168,99,0/24		211.20,227,193	192, 168, 168, 0/24	area-shat	aes-stat	-		183	Lag

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. **III**: Stand for suspension

- 4. 4.
 Stand for edit the VPN setting
- 5. Log 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	4	30 Seconds · Befresh export clear	174 188 183 181 194
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 stentify ourselves with either end of this connection	
2016-05-19 09-32:02		deleting connection	
2015-05-19 09:32 01		We cannot dentify curselves with either and of this connection.	
2016-05-19-09-34-02		deleting connection	
2015-05-19 09 34 02		We cannot identify surselves with either end of this connection	
2015-05-19-09:30.02		deleting connection	
2015-05-15 09 36 03		We cannot identify ourselves with either end of this connection:	
2016-05-19-09:38:02		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)

1P-SOC Turninal and Sta	Inis 1 Show Poor	10 10	pitter	I San San San T	and a first statement of the		1			Concernance and	and the second	111 10	AL 18. 1
Tunnel Name	Interface 4	Loca	I Subnet a	Status	Remote IP +	Remote Subnet a	phase 1	phose 2	Operation time	Enabled	Switch	Edit / Del	Log
	0	192.1	188 184 0/21	9	116.231.248.225	152.158.21.0/24	des-mit5	des-md5	00:31:58	P	· · ·	123	Ling
	83	192.1	168.184.0(21	4	122 117 136 68	192.168.200.0/24	dep-md5	des-md5	15.13.26	10			Leg
	1	192.7	168.168.0/24	4	60.250.106.211	152,168,100,0/24	3des-md5	3des-md5	00.36.01	*	- A1	12	Leg
		192.1	168.195.0/24	4	60.250.106.211	192,168,100,0/24	3tes mit5	3det-mff	00.34.33	- P.		123	Ling
	63	192.1	168.188.0/24	40	220.130.209.67	192.168.1.0/24	des mid5	des-md5	00.11.18			123	Leg
	0	192.1	稿 189 0.24	ø	60.250.106.211	152 168 100 0/24	3des-md5	30es-mit5	00.28.57	¥ .	+ .	18	Linx
		192.1	168.191.0/24	1	60.258.106.211	192 168 100 0/24	3det-md5	3des-md5	15.11.68	1	- A.C.	183	Les
	0	192.1	158 185 0/24	0	115.231.248.225	192.168.21.0/24	dis-miti	des-mit5	00 31:59			12	Les
	13	112.1	168.189.0/24	1	116,231,248,225	192.168.21.0/24	dee md5	des-md5	00.31.68	1		12	Lag
		192.7	168.186.0.24	4	123/205.117.19	152 168 202 5/24	ais-stat	aus-sha1	00.42.55			12	Ling
		192.1	168.186.0/24	100	210 202 56 31	192 168 196 0/24	ant-shaf	ues-sha1	06 65:22			10	Les
	10	192.1	168 106 0/24	4	122.117.136.58	192 165 200 0/24	des mitti	des-md5	00:34:31		4	12	(L+=
		152.1	168 186 0/24	4	60.250.106.211	192 168 100 0/24	3dea-mi5	3dea-mit5	00.33.13		±4	18	Leg
		192.1	198 188 0/24	4	Dynamic (P	172.16.10.0/24	des-end5	deo-md5	-	1		183	Leg
		1931	168 188 0/24	4	123 205 117 19	192 168 202 0/24	aws-shat	awa-ahat	00.05.29	*	-	18	Les

Figure 8-1. 5 Multiple IPSec VPN

omment :	Peter2.2	中 30 Seconds * Retrest clear		export	Export	t All						
			36/38	36	1812	84		E) (8				
TIME	NUMBER	EVENT										
2015-05-19 09:30:36	#5672	keeping refnim=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	#9672	TATE_QUIOX_R1: sent QR1, inbound iPsec SA installed, expecting QI2										
2015-05-19 09-30-36	\$5672	Dead Peer Detection (RPC 3706) enabled										
2015-05-19 09-30-36	#5672	banation from state STATE_QUICK_R1 to state STATE_QUICK	JR2									
2015-05-19 09:30:36	\$5672	STATE_QUICK_R2_IPsec_SA established turnel mode (ESP=>) HMAC_SHA1 NATOA=nane NATD=none DPD=enabled)	0x29:62563 <0	k90e2ec1	93 afim	=AE8	12	18.				

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.


PPTP Server :		
Enabled	8	
Compression & Encryption	H1	
Internet Access over PPTP	61	
Client IP Address (Starl End)	10 10 10 50	- 60
The First DNS Server	168.95.1.1	
The Second DNS Server	139.175.10.20	
The First WINS Server		
The Second WINS Server		=10



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..

Add Account :	
Enabled	8
Account	ting
Passworth	++++
Client IP Address	Assign by PPTP Server .
	User Define IP Address





How do users create VPN connection in their computer?

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

●● ● ● ● ● ● ●	R版和模築構築 ・ 機能和共用中心		* 6 7 3	建烧毛油	
문화소문제	機視思基本的網路資訊並設定連線				
WENERBER	A &		0	体测完整绝效量	
examines.	TING-PC 多重成 (語形電腦)	8	派派政策		
	植港作用中的研算			傳播或中斷連環	
		存改調型 連续	机型机器 章 医单连带		
	任论所国的简整 公开编辑	주말해입 생각	■構想存取 ■ VirtuelBox I ■ VirtuelBox I ■ VMware Ne VMmet1 ■ VMware Ne VMmet8	lost-Only Network twork Adapter	
	展開構新設定				
	至5年前通道市政器 股市用:直接:和快、期间操作或VS	州 總徵 或延定算击	1年存取起·		
	第四款通知 通信或重新通信到供信·预信·指则或 VPN 研究通信。				
a a fa HomeGroup	····································	- 成變更共用設定。			
Windows 防火費		e0.			

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)

輸入要連線的網際	早期蹲位社	
生的病院多校會議員可	以進供禮儀包起・	
通常規算位なの	111.252.70.234	
育的地表稱(I);	VPN connection testing	
ご 使用解解卡(5)		
● □北計其他人使用 定要項可歸任何	E位軍連線(A) E線券式電腦存取權的人使用式連線。	
四字第2日命统;	元記立行・武林後耳達信(D)	

Figure 8-2. 5 Enter WAN IP address

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

使用者名稱(1):	ing	
岩硯(F)	******	
	回 載示于元(1) [1] 紀住遺儀液確(n)	
病或(編復生)(D):		

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)

<pre>indows IP Configuration ithermet adapter 國境運搬: Connection-specific DMS Suffix .: IP Address</pre>	::\>ip	config	
ithermet adapter 區境連線: Commection-specific DMS Suffix .: IP Address: 192.168.161.117 Submet Mask: 255.255.255.0 Default Gateway: 192.168.161.254 PP adapter ShareTech: Commection-specific DMS Suffix .: IP Address: 10.10.10.50 Submet Mask: 255.255.255 Default Gateway: 10.10.10.50	lindov	= IP Configuration	
Connection-specific DMS Suffix .: IP Médress	therm	et adapter 區域連接:	
IP ##dress		Connection-specific DNS Suffix . :	
Salmet Mask		IP #ddress	
Default Gateway : 192.168.161.254 PP adapter ShareTech: Connection-specific DMS Suffix . : IP Medress : 10.10.10.50 Subnet Mask : 255.255.255 Default Gateway : 10.10.10.50		Submet Mask	
<pre>PP adapter ShareTech:</pre>		Default Gateway : 192.168.161.254	
Connection-spectric UMS suffix .: IP #ddress: 18,18,18,50 Submet Mask: 255,255,255 Default Gateway: 18,18,18,50	PPP add	apter ShareTech:	
Tr monress		Gennection-specific DMS Suffix . :	
Default Gateway		Coheat Harly	
betwart Outerway 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		Default Ostening	
		Derwite University 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	





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. 上: 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.

Account	Statum	Enabled	Edit / Dol	Log
ting	- 4 .		/ 🔤	Lee
			/ SO	1 1.00

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.

Add New Connection :		-		
Naryus	test	Enabled	*	
Account	Test	Password	www.	
PPTP Server IP or Domain	192.168.186.53	Compression & Encryption	×	
Remote IP Range ex 192 168 1 0/24	0.0.0/24			
		★ A4.6		





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

PPTP LI	ist						1/1 3	en 140 (A) a
Name	Account	PPTP Server IP or Domain	Remote IP Range	Compression & Encryption	Statue	Enabled	Edit / Del	Log
Inst	- test	192 168 186 53	6660/24	0	æ.,	*	/ 🖾	Les
			+ A4	14				





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.
 - 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. OFF 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

(b) Basic Setting :			
Policy Name	[]		
Source	* [VPN_Any •]	IP Addess	MAC Address
Destination	Inside_Any •	IP Address	
Action	DROP •		
9 Policy 1			
Protoc pl	ALL •		
Service Port or Group	User custom Service Port		
Gos	Biorus .		
fichedule	Norm V		
Packet Tracing	8		
Traffic Analysis	10		
NAT	400		
		+ AA.5	

Figure 8-4. 1 VPN to Internal



Internal to VPN

6 Busic Setting :			
Policy Name	[]		
Source	Inside_Any •	© IP Address	MAC Address
Destination	* VPN_Ary *	G IP Addees	
Action	DROP .		
9 Policy I			
Protoc al	ALL .		
Service Port or Group	User custom Service Port		
QuS	bionu		
Schedule	Norm ·		
Packet Trazing	0		
Traffic Analysis	10		
		+ 224	

Figure 8-4. 2 Internal to VPN



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 \circ K. 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.





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 \circ \circ κ . 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.

S Traceroute Setting	-							
Target IP or Domain	Target IP or Domain 88.8.8 (Max: 30 characters)							
Package Size	fackaga 52a do Bytes (Range : 40 - 9999)							
Max. Next Hop.	has Next Hisp 30 Nodas (Ranga 1+255)							
Watt Time (2 Security (Range (2-9999))								
Tracing Methods ICMP .*								
Source Interface	une interface WAN1 •							
<pre>troceroute to 8.6.8. 1 302.108.188.045 2 190.168.188.045 3 190.168.188.1 11 3 192.108.188.1 11 4 60.240-6.254,100 5 * * * 6 * schn-3502.himt 7 tchn-302.himt 8 tchr-302.himt 1 0 72.14.233.254 (7) 11 72.14.233.256 (7) 11 72.14.233.261 (11 2 216.243.254.3 (3) 2 216.259.43.181 14 * * * 5 gongle-public.ds</pre>	<pre>8 (8.0.8.0), 90 800 (02,108,108,245) (02,108,108,11 5.3) 22.188,108,11 5.3) 27.27 Alnet.net (01 27.27 Alnet.net (01 27.27 Alnet.net (01 27.27 Alnet.net (01 27.27 Alnet.net (01 27.27 Alnet.net (01 27.28 Alnet.net (01 27.28</pre>	5 mov, 40 byte packets 0.370 m 0.231 ms 0.423 ms 1 ms 4.103 ms 5.111 ms 1 ms 5.121 ms 3.514 ms .040.5.246 .4.255 ms 4.5 081) 3.045 ms 3.559 ms 3.125 ms 6.425 ms 15.25 ms 3.125 ms 6.425 ms 15.25 ms 3.126 ms 5.127 ms 3.121 ms 5 ms 5.060 ms 5.273 ms 5.231 ms 5 ms 5.060 ms 2.050 ms .631 ms 14.816 ms 14.640 ms .631 ms 14.816 ms 14.640 ms .631 ms 14.816 ms 14.73 ms 13.562 ms						

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 \circ K. 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.

(b) DNS Query Setting		
Using DNS Server	User Define • 168.95.1.1	(Max. 50 characters)
Domain or IP to Query	www.sharetech.com.tw (Max. 60	characters)
Quely Type	ANY •	
10 ONS Query Result		• OK
entersturatech.com.tv.	19010 IN # 60.249.0.105	
11 Query time: 7 mint 11 SERVEN: 108-95-1-1 11 WHEN: More Nay 11 1 11 PDB SIZErcvd: 54	#55(188.95.1.1) (4)29(58-2015	

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.

2 Port Scan Setting				
Domain or IP	to Scan (scan sharetech com tw) (Max 50, characters)			
• Port Sca	n Result	O OK.		
14:33:30	FTP====>> FAIL			
14:33:21	SSHITTERS CK			
14:33:31	TELNET ####>> FAIL			
14:33:31	SMTP====>> OK			
14:33:31	HTTP====> OK			
14:33:31	POP3namoo OK			
14:33:31	SAMBA===>> FAIL			
14:33:31	IMAP CK			
14:33:21	SNMP++++>> FAIL			
14.33.32	PROXY=====> FAIL			
14:33:32	MySQL====>> FAIL			
14:33:32	SMTPS====>> FAIL			
14.33.32	POP35====> OK			
14:33:32	IMAPS****>> OK			



+ Port Sca	m Setting	
Domain or IP	P to Scan (www.google.com.tw (Max 50, characters.)	
· Port Sca	m Rissult	• OK
14,34,04	FTP===>> FAIL	
14:34:05	SSEmmers> FAIL	
14:34:07	TELAETETEN> FAIL	
14:34:07	SMTP====>+ OK	
14:34:07	HTTP=====> OK	
14.34:07	POPJananoo OK	
14:34:06	SAMBA====> FAIL	
14.34.09	IMAD ****>> FAIL	
14:34:10	SNMP++++>> FAIL	
143411	PROXYEEEE>> FAIL	
14:34:12	MySGL====>> FAIL	
14:34:12	SMTPS====>> FAIL	
14:54:14	POP3S====> FAIL	
14:34:15	IMAPS****>> FAIL	





IP Route

IP Route shows router status in order to know router information; it also shows multiple subnet

status. (Figure 9-1.6)

bP Route
 default via 152 158 185 1 dev eth1
 152 168 1 0/24 dev eth2 proto kernel scope link arc 152 168 1 1
 152 168 186 0/24 dev eth1 proto kernel actpe link arc 192 168 186 157

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)

6 Interface Information Query		
Interface LAN •		
	O OK	
t leterlace Information		
5. eth0: mtu 1500 qdioz bitb state DOWN iden 1000		
Snk/ether 00 0d 48 31 1a 95 lad If If If If If If If		
inet 192,168 1 1/24 brd 192,168 1 255 scope global eth0		
valid_ft forever preferred_ft forever		

Figure 9-1. 7 LAN Information

B Interface Information Query		
Interface LAN •		
	• OR	
6 Interface Information		
5. eth0: mtu 1500 gdioz btb state DOWN gien 1000		
Snk/ether 00 0d 48 31 1a 96 Led II II II II II II II		
inet 192 168 1 1/24 brd 192 168 1 255 scope global eth0		
valid_ift forever preferred_ift forever		

Figure 9-1. 8 DMZ Information



10 Interface Infor	mation Query	
Interface	WAN1 *	
		80 B
to beterface Infor	mation	
4: off)1: mtu 150 Srikilether 00:0d / met 152:168:186 valid_th forever p inet5:1e80:20d / valid_th forever p	1 gdias, hdb state UP glen 1000 I0 31 af 71 bri ####### 157/24 brd 1921 fi8t 106 265 scope global eth1 aefemal_th forever 8H fis311 af71/64, scope link wefwrest_th forever	
192 168 1 30	ether 20 cf 30 33 6f bl C eth 1	
192, 168, 186, 1	ether b0.a8;6e:0f.16:81 C ath1	
192, 168, 18E 50	ather to 60.65-28.9c dz. C with1	
192.168.1.2	ether 29.cf.30/33.0f.bf C eth1	
192.168.186.246	either 00.90 fb 2b 2f e7 C eth1	
192.168,186.32	ether 00.90 e0.5d 26.76 C eth1	

Figure 9-1. 9 WAN1 Information

6 Interface Information Query		
Interface WAN2 *		
	O DE	
9 Interface Information		
3 eth2: mtu 1500 qdisc roop state DOWN glen 1000		
Ind/lether 00.0d 48 31 at 72 brd ff ff ff ff ff ff ff		

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)

		1/1 (e) (e) (e)
Computer Name +	IP Address +	MAC Address e
192.168.186.253	192.168.106.253	00.06 1#03.04.22
192 168 166 245	192 168 186 245	00 90 fb 2b 2f e7
PETER-H56M-UD2H	192.168.186.50	1c 6! 65 29.9c ds
192 168 106 1	192.108.196.1	b0:a0:6e.01:15:01
PETER-HESM-UD0H	192 168.1 5	00 0f 18 6b 7f 62
	Computer Name	Computer Name IP Address 192 168 166 253 192 168 166 253 192 168 166 246 192 168 166 246 PETER-H53A-UD2H 192 168 166 50 192 168 106 1 192 168 106 1 PETER-H53A-UD2H 192 168 106 1 PETER-H53A-UD2H 192 168 16 1

Select

Figure 9-1. 11 wake up

Wake Up	
Using Interface & IP	LAN • Amint
MAC Address	1c: 6f: 65: 28: 9c: de
	O OF







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

N Plug Setting	
Target IP 2001 4860 4860 4888	
	0.0E
time not Line tot Line tot Line tot	
tr Reade	
Av00, 100 deur attil prote karrel reakte 200	
* Address Table	
NeO 2534 9600 2543 9655 dwv with liautili dit dit 64 11 14 14 STALE NeO 2110 2webchd0 aweb die webb liautili 20 th all that all that 27 STALE NeO 2004 967 967 967 2011 1400 14 767 65 02 01 16 STALE NeO 2004 976 968 968 969 969 141 1400 14 767 65 02 01 16 STALE NeO 2004 976 968 969 1469 1469 147 1400 14 767 95 14 95 469 157 ALE NeO 2004 976 976 968 969 1491 1400 14 767 95 14 95 469 157 ALE NeO 2004 976 976 968 969 1491 1400 15 767 95 14 95 14 95 14 95 14 1400 2004 976 1411 1400 9774 05 1400 100 15 77 140 1200 9774 15 NeO 2004 97740 9784 969 961 11 1400 100 100 767 140 100 00 974 15 NeO 2004 97740 9784 969 961 11 1400 100 100 974 140 100 00 974 15 1400 1401 1400 1700 9774 969 961 11 1400 100 100 974 15 1400 1401 1400 1400 9774 11 1400 100 100 974 1400 100 140 974 15 1400 1401 11 1400 1400 1400 1400 1400 1	

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)

Explan	The second second second	
old	Esplan	Example
su 36 12 1.17 12	search switch total port counts	140 3.6 1.2 1 17 1.2.0 = INTEGER 24
so 3 6 1 2 1 2 2 1 10	search port at flow	iso 3.6.1.2.1.2.2.1.10.515 = Counter32. 3692512
903612122116	search port out flow	iso, 3, 6, 1, 2, 1, 2, 2, 1, 16, 515 = Counter32, 11238968
an 3.6.1.2.1.4.72.1.2	asarch ip mac Conseponding	iso 3.6.1.2.1.4.22.1.2.38.120.0.0.1 = Hex-STRING: 00.08 CA FE 00.00
ao361419946131121	search Vian ID	150.3.0.1.4.1.9.9.46.1.3.1.1.2.1.10 = INTEGER: 1
no36121171412	search port Corresponding Illindee	100 3 6 1 2 1 17 1 4 1 2 515 = INTEGER 500
9535121311111	search port entity address	iso.3.6.1.2.1.21.1.1.1.1.515 = STRING "ge-0/0/6"
so 3.6.1.2.1.17.4.3.1.2	search mat port Corresponding	iteo 3 6.1.2 f. 17.4 3 f.2 fl 13 72 50 168 248 = INTEGER: 522
so 3 6 1 2 1 4 20 1 2	nearch Vian id	itio 3 6 1 2 1 4 20 1 2 128 0.0 1 = INTEGER 38
su 3612111	search switch name	isu 3.6.1.2.1.1.1.0 = STRING: '24G + 4 SFP Web Smart Switch - 2.03
0361212217	search port lock	iso 3.6.1.2.1.2.2.1.7.515 = INTEGER 1
su 3.6 1 2 1 2 2 1 8	search port Plug	150.3.6.1.2.1.2.2.1.8.515 = INTEGER 2
iso 3 6 1 2 1 17 1 4 1 1	search vian port	ino 3.6.1.2.1.17.1.4.1.1.515 = INTEGER .515
0036141922111	search port interface	iso 3.6.1.4.1.9.2.2.1.1.1.10101 = STRENG: "Gigabit Ethemat"
00361212212	neurch mac port Corresponding	190.36.1.2.1.2.2.1.2.515 = STRING "ge-606"
6036121177122122	search port entity address	IN6 3.6 1.2 1 17 7 1 2 2 1 2 2 0 28 240 40 57 191 = INTEGER 21





Stor instance, select Tools > Connection Test > SNMP, and enter your switch IP, Read

permissions, and OID. It shows switch SNMP result. (Figure 9-1.15)

S SNMP				
Switch IP	192 168 186 253	Ex. 192 168 1 t		
Read permissions	public	Ex. public		
DID	100.3.6 1.2.1.2.2.1	Ex. no.36121221		
Ytan ID		Ex. 10		
80361212211 80361212211 80361212211 80361212211 80361212211 80361212211 80361212211 8036121221 8036121221 8036121221 80361212211 80361212211 80361212211 80361212211	11 = INTEGER: 1 12 = INTEGER: 2 13 = INTEGER: 3 14 = INTEGER: 4 15 = INTEGER: 4 15 = INTEGER: 6 17 = INTEGER: 7 18 = INTEGER: 8 10 = INTEGER: 8 10 = INTEGER: 10 111 = INTEGER: 11 112 = INTEGER: 11 112 = INTEGER: 13 114 = INTEGER: 14			

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.

Schedule List

Select Tool > Packet Capture > Schedule List. Click + Add 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 <u>http://www.wireshark.org/docs/wsug_html_chunked/</u>
- 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

Туре	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



Urransfer Direction: <u>src</u>, <u>dst</u>, <u>src or dst</u>, <u>dst and src</u>

C-like	Туре	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	İ	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)

us 前专信用平元 - ping 1921681161 +	COLOR MAN
opyright (c) 2009 Microsoft Corporation. All rights reserved.	2
: Weero'ting)ping 192.160.1.161 -t	2
the state of the s	
'ing 192,168,1,161 (使用 32 位元跑的酒种):	
回题目 192.168.1.161: 区汇组=32 time(int TTL=64	
回题岩 192.168.1.161: 位元祖=32 time(ins TTL=64	
回题目 192.168.1.161: 位元泪=32 time(ins TTL=64	
回题图 192.168.1.161: 位元组=32 time(ins TTL=64	
回题目 192.160.1.161: 位元组-32 time(in: TTL-64	
回题目 192.168.1.161: 位元纪-32 time(ins TTL-64	
回题自 192.168.1.161: 位元组-32 time(ine TTL-64	
回题目 192.168.1.161: 位元祖-32 time(ins TTL-64	
回题前 192.168.1.161: 位光矾-32 time(ins TTL-64	
回题目 192.168.1.161: 位元组-32 time(in: TTL-64	
回题目 192.168.1.161: 位元组-32 time(ins TTL-64	
回题目 192.168.1.161: 位元组-32 time(ine TTL-64	
回题图 192.168.1.161: 位元组-32 time(ine TTL-64	
回题目 192.168.1.161: 位元纪-32 time(ine TTL-64	
回题目 192.168.1.161: 位元组-32 time(ine TTL-64	
回题目 192.168.1.161+ 位元组-32 time(ine TTL-64	
回题自 192.168.1.161: 位元组-32 time(ing TTL-64	
回题目 192.168.1.1611 位元组-32 time(Ins TTL-64	
回题自 192.168.1.1611 位元组-32 time(1mz TTL-64	
回覆白 192.168.1.161+ 位元纪-32 time(inz TTL-64	

Figure 9-2. 1 ping LAN



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

Enabled	2
Time Range	2012-11-30 1 16 • 45 • - 2012-11-30 1 17 • 30 •
briterface	LAN -
Fratocol	KOMP +
Filter Condition	hurt190.168.1.111
pcap File Size (MB)	5 (1-10)
pcap File Num	10 (1-100)
Post the link-level header	

Figure 9-2. 2 Add listen Schedule

Schedule List							11. ()))))))))))))))))))))))))))))))))))	116
Time Range	Interface	Protocol	Filter Condition	pcap File Size	pcap Filé Num	Enabled	Edit / Del	Log
11/30 16 14 - 11/30 23:59	WANI	AND!	host 192 168 1 111	5	10	*	183	Leg
11/30 15:45 - 11/30 17:30	LAN	ICMP	host 192.168 1.111	5	10	2	183	Leg



Completed List

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

Completes List					1/1	1460 (46) (8	11.18
Time Range	Interface	Protocol	Filter Condition	pcap File Size	pcag File Num	Log	De
10/30 12:04 - 10/30 13:30	LAN	ANY.	mut 192 168 1 0/24	5	10	Leg	E
10/38 17:04 - 10/30 17:29	LAN	ANY	Book 192 168 7 111	6	10	Leg	E
10/30 14:04 - 10/30 15:50	LAN	ANY.	met 192 168 t 0/24	5	10	Lea	E
11/30 18:45 - 11/30 17:30	LAN	ICMP	Boot 1107 168 7 111	5	10	Lyg	12



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

	PCAP File Download	
Please use wresterk to (Confirm to Download File ?	tit a a ta
	87. R.A.	

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)

13542052220 [Wireshark 1.8.3 (5VH Rev 45256 from /trunk-1.8]]		
Ele Edit Wew Go Capture Analyte Statistics Telephony Tools	Jitemak Help	
使免疫免疫 印图关键印 卢卡卡格树	🛓 🅅 🕼 q q q 🗉 🖬 🖉 😹 📓	
Fiber	· Expression Ower Apply Law	
Ne. Time Source Destination 0 2.026277 192.166.1.101 192.108.1.101 7 2.026277 192.166.1.101 192.108.1.101 8 7.22344 197.166.1.101 192.108.1.101 9 7.27344 197.166.1.101 192.108.1.101 9 7.27344 197.166.1.101 192.108.1.101 10 7.27344 197.166.1.101 192.108.1.101 10 7.27344 197.166.1.101 192.108.1.101 10 7.27344 197.166.1.101 192.108.1.101 10 7.27344 197.166.1.101 192.108.1.101 11 7.303006 197.166.1.101 192.108.1.101 12 3.045102 197.166.1.101 192.168.1.101 13 3.045002 197.166.1.101 197.168.1.101 14 5.046574 197.166.1.101 197.168.1.101 15 5.046574 197.166.1.161 197.168.1.161 14 4.52262 197.166.1.161 197.168.1.161 15	Pressed Length Min IOMP 74 Echo (ping) request id=0x0001, seq=56/14336, IOMP 74 Echo (ping) reply id=0x0001, seq=56/14336, IOMP 590 DEStination unreachable (Fragmentation needed IOMP 74 Echo (ping) request (d=0x0001, seq=57/14592, IOMP 74 Echo (ping) request (d=0x0001, seq=57/14592, IOMP 74 Echo (ping) request (d=0x0001, seq=57/14592, IOMP 74 Echo (ping) reply (d=0x0001, seq=58/14888, IOMP 74 Echo (ping) reply (d=0x0001, seq=59/15104, IOMP 74 Echo (ping) reply (d=0x0001, seq=59/15104, IOMP 74 Echo (ping) reply (d=0x0001, seq=59/15106, IOMP 74 Echo (ping) reply (d=0x0001, seq=69/15306, IOMP 74 Echo (ping) reply	ttl=128 ttl=64)(Hacket size limited during capture))(Jacket size limited during capture) ttl=128 ttl=64 ttl=128 ttl=64 ttl=128 ttl=64 ttl=128 ttl=64
0000 00 0d 48 0e 26 f2 40 61 88 66 fc ff 08 00 45 0 0010 00 3c 2c 88 00 00 80 01 80 48 c0 a8 01 6f c0 a 0020 01 41 08 00 42 50 00 10 00 36 61 62 63 64 65 6 0020 67 68 69 6a 60 65 66 66 6f 70 71 72 73 74 75 7	00H.&.Ga FE. 18Gabcdef 16 ghtTkTan oggracuv gabridefn bydracuv	
🔵 🛒 File: "C'lliters(ting)(Downloads(13542652 Packets: 1241 Deploye	ed: 1241 Narked: 0 Load time: 0:00,549	Profile: Default

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 (<u>http://www.wireshark.org/docs/wsug_html_chunked/</u>)
 Here are some things Wireshark does not provide:

- 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)

Catthew	1	Herford	1964	nation de la constanción	e Daren Morde	Search		NUMBER OF STREET	Cather	dat 1
Ø.	Reading PC to Gr which for a company company of the company of the company company of the company of the company company o	n Landy Controller Distri Distriction (Controller Distriction (Controller)	- Giler	E)	entited	:445				
۵.	VMware Virtual 980-3ca795cto8c 102388.001	Ethernet Adapter: \ : Sale	Ethen	ret :	enabled	dela	suit	1		
=	VMware Virtual WR051118585355 1921882061	Ethernet Adapter: \ PRest	Ether	rat	anabled	defe	ut	1		
10	TAP-Win12 Add fe80 5546480 206 000.0	pter WE\Device\NP e211	Ethen	net	evabled	defa	ut	1		
* laste										- 10
Capit	ture on all interla ture all in gromiu	ces wous made	-			-			Manage) + Dräerfaces
Capital Capita	ture on all interfa ture all in groniu File(s)	oes wous made		a.				Deplay Opt	Manage	i Interlaces
Capt (2) Capt Capture F File:	ture on all interfa ture all in gromiu File(s)	ces wous made		t.		Brown		Dealey Oat	Manage Jons e list of packets	in real time
Capit (2) Capit Capture F Fle:	ture on all interfa ture all in promis File(s) guiltiple files	ces wous mode		th. In the p	caping toma	Brown	1	Display Out	Manage sons e list of peckets	in real time
Capit Capture F File: Use g	ture on all interfa ture all in gromiu FR(s) guilogie files file many	ues suitus mode		The part of the pa	caping linna	Brown		Display Opt	Manage tans e list of packets arts sciolling in	in real time
Capi Capi Capture F File: Use t filant	ture on all interfa ture all in promis Re(s) Multiple files Multiple files Multiple files	eei saatua mode		R. E Use p Insignity Printers	caping forma	Brown f	(H) (E)	Display Opt 12 Updan 13 Autom 13 Hide o	Manage tons e list of peckets into: uscalling in apture info dial	in real time
Capi Capi Capi Capture F Fie: Use : Trans Trans	ture on all interfa ture all in promisi Re(s) Subjecties The every Suffer each Suffer each	oei saaus mode	100 mile 428	the p	caping forma	Brown (Display Opt @ Updato @ Autom @ Hide o	Manage lons e list of peckets atte smolking in apture info dial	in real Sm live captur
Capture F File: Use y File: Fi	ture on all interfa ture all in promis FR(s) multiple files file every fully every fully every fully every fully every	001 Subus mode	10. 10. 10. 10.	f Use p megaler megaler fess files	ceping forme ar(1)	(Brown	13 11	Display Opt	Manage tons e his of peckets afte scoolling in apture info chai kution	in real time
Copy	ture on all interfa ture all in gromiu Flo(s) multiple files file every fully every fully every fully every fully every	ces useus made 1 2 1	100 million (100 m	Terepaire Interpaire Internation Teres	cep-ng forme or(0)	8-cm		Depty Opt 12 Lipday 12 Autom 12 Hide o Name Roso 12 Snable	Manage lons e los of peckets ato: usoilling in apture info diai lution : <u>M</u> AC name re	in real tim in real tim live captur log
Capture F File: Use t Use t Us	ture on all interfa ture all in growing Flo(s) The servery flore servery Suffer solth construct after fore ter	2003 mode	211-111-115-116-11-11-11-11-11-11-11-11-11-11-11-11	Terepairy Interpairy Interpairy Teres Teres International International	saping tuma ar(i)	Brown f		Display Opt 12 Jupidas 12 Jupidas 12 Jupidas 12 Jupidas 12 Stable 12 Stable	Manage tons e has of peckets actor scrolling in apture info dial kution <u>MAC</u> name re- patasorik name	in real tim in real tim live captur og colution readution
Copy Copy Capture F Fle: Use y flue	ture on all interfa ture all in promisi file(s) multiple files file every stuffer each contras after ture ture ture	2015 Subus mode 1 2 1 1 1 1 1 1 1 1	1010 Holes	(K) Use p (magaloy (magaloy (magaloy (magaloy (magaloy)	saping time s()) tr[]	Brown		Display Opt 12 Jupidas 12 Jupidas 12 Judeo 14 June Reso 12 Enable 13 Enable 14 Enable	Manage sons e lat of peckets artic smolling in apture info dial apture info dial futtori fulfAC name rec getwork name	in real tim in real tim live captur log colution resolution

Figure 9-2. 8 select network card



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

#2	Usen	name:	Pasawo	ntr	Port:	Quickconnect -
計算程程 MOTH UT 21 <u>3-2012</u>	893年医興移線 科多功能防火調 1002162254	t ∎_SOHO.pdf				
Site M	eneger	· ····································				-
Select	t Entry:		General Ad	anced Transfer S	Sattings Charse	10
eter:	ly Stes		Hosti	download.sharet	ech.com.tar	Parts
	A CONTRACTOR		Protocol	FTP - File Transfe	er Protocal	
			Encryption:	lise plan FTP		
EM			10000000	far a		
			Logon Type	Normal		
826.ep			User:	canay		
268			Account:			
326 ml			Dermache			
W-560 N	lew Sta	New Folder				1
az a Nev	Bookmark	Rename				
8/214	Dolete	Copy				
		1	12 12 14	1955	10	
		1	Connect	OK Ca	ncel	

Figure 9-2. 9 connect FTP server

Bet	Stop the ru	ring live capture		Expression	Ower Apply Seve
i Tir	w Sourc		Destination	Protocol La	ngth lefa
221 7.	87642200 192.	168.189.31	192.168.189.120	5948	146 Trans2 Response-unknown>
222 7.	87664800192.	168.189.31	192.168.189.120	5948	258 Trans2 Response-unknown>
223 7.	87682900192.	168.189.31	192.168.189.120	5948	138 Trans2 Response unknown>
224.7.	87968800192.	168.189.31	192.168.189.120	5918	898 Trans2 Response-unknowno
225 7.	88004000 192.	168.189.31	192.168.189.120	5948	105 Trans2 Response-cunknown, Error: STATUS_OBJECT
226 7.	88064400 192.	168.189.11	192.168.189.120	\$940	173 NT Create Andx Response, FID: 0x0004
227 7.	88093300192.	168.189.11	192.168.189.120	\$46	138 Trans2 Response-cunknowns
328 74	88117300197.	165.189.11	192.168.189.120	\$46	105 Close Response
229.6	88170800 192.	168.189.11	192.168.189.120	240	105 Delete Response
210.0	\$9209100 192.	168.189.11	192.168.189.120	540	258 Trans2 Response cunk nowns
100	91695500 197.	168.189.11	192.168.189.120	540	150 Trans2 Responsecurik nowns
112 0	96814900 197.	168.189.11	192.168.189.120	540	105 Tree Disconnect Response
- 22.0	95515300 292.	100.109.31	192.168.189.120	1990	10% Lugor r Anux Response
234.8.	08023800 192.	100.1.130	192.108.1.200	NDNS	92 NAME QUELY NO MEGA-ORGY.COM-0005
	110010001990	100,109,11	196-100-109-170	192P	The mitraspicane a press fear, well perfectat were
-	227	10000			
	TI, SPC: A	cloetec_SLice erston 4, sro	:5f (00:60:e0:51:ce:) : 111.221.77.148 (11)	5f), DST: 1 1.221.77.1- 1), DST PO	Hicro-St_66:fc:ff (40:61:86:66:fc:ff) 48), Dut: 192.168.188.111 (192.168.188.111) 1: 49247 (49247), Seq: 1, Ack: 1, Len: 0
Etherne Interne Transei	t Pratacal v ssian contro	Protocol, s			

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)

weil	· Laurente, Chie Aure	fave	
The Source Destruction 10 data 244 AGA (244 AGA) - 244 - 245 10 data 244 AGA (244 AGA) - 244 - 245 Weinhardt Filter Eigenscher Findler Defaut Field name IF FIGTIAL - File Replication Service DEF E IF TOWN - IEO 00512 FFMM FILE DATA - FILE DATA IF DE TATA br>IF DE TATA - FILE DATA IF DE TATA IF DE TATA - FILE DATA IF DE TATA IF DE	Promot Lange Mid A 148-111 212 A Become Relation Rela	49581 [1.7 CCV_DOCK PO data 1.00851 print 3856 get_fml 1.00851 print 3856 get_fml 1.00851 print 3856 get_fml 1.00851 print 3856 get_fml 1.00855 get_fml	
10 40 61 60 Fc Ff 00 60 81 cs 15 10 10 46 5c 10 00 17 16 </td <td>00 00 45 00 84.5. 0. 5. 06 09 00 88 7. 46.7. 1. 71 75 71 50 8. 8. 1</td> <td></td> <td></td>	00 00 45 00 84.5. 0. 5. 06 09 00 88 7. 46.7. 1. 71 75 71 50 8. 8. 1		

Figure 9-2. 11 Wireshark Expression

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

	tutzo Telephony Icele \$	nternih (jelp	Concerning and the second
教教教教教 计司状链型	几中中华等点	BB dddD	(編約幣容 品)
Riber da		Equipages, Class (10) 1	ave
42. Tene Source 1255 47.1280080 60,249.6.185	Outination 192-166, 168-111	Protoint Langth Info #TP 64 Response	1 500 cors:
1338 47,1281160 60,249.6,163 1259 47,1261160 60,249.6,193 1366 50,8366550 60,249.6,185	142.168.188.111 192.168.188.111 192.168.188.111	FTII 00 Response FTII 62 Response FTII 72 Response	: 100 cors: priv_sock.get_ted : 220 (vstred 2.2.2)
1369 30, 6317220 60, 249, 6, 163 1369 30, 6317220 60, 249, 6, 163	192.168,188,111 192.168,188,111	FTP 58 Response FTP 58 Response	: 331 Flease specify the password.
1171 30.871080 60.264.6.183 1174 8.08544400 67012 840144 1373 50.8723120 60.248.6.183	192.168.188.111 192.168.188.111	TTT 80 Atsports	1 JUD LOGIN HOLEMELTAL. COTTA UNIT CO 1 200 Always in UTES 8000,
1376 50.8779490 60.249.6.185	192.165.188.111	FTP 63 Sepportie	
and the second se			
Frame 1257: 64 bytes on wire (6) Ethermet II, Src: AddedTes_Dico Different Frotobol version 4, Src Tranemitsion Control Protocol, s File Transfer Protocol (TTP)	3 bits), 84 bytes cm 195 (00:00:00:51:ee; 5 90:340 A185 (00:5 ec #ort: ftg (23), p	stured (871 Stes) on in SF), Dat: Micro-St.00.7 90.8.183), Ost: 130.168 st Port: 19989 (19989),	terface 0 Liff (40:42:38:48:fi:ff) 1984 III (19) 148.188.111) 984 III, ACK: 7, Len: 30
Frame 1257: 84 bytes on sire (6 Cohernet II, Src: ActorReg II: co Uniforms routool version 4, Sr Transmission Control Protocol, 1 File Transfer Protocol (FTP) 005 40 61 85 66 fc ff 00 60 e0 010 60 45 fc 5c 40 00 5f 06 be 0250 6c 6f 00 13 46 01 41 47 fd 0250 6c 6f 00 13 46 01 41 47 fd 0250 6c 6f 00 13 46 01 41 47 fd	2 bft3), 84 bytes co 15 (20-05-05 sizes) 2 00,340 5 100 (00,3 2 00,340 5 100 (00,3 2 00,340 5 100 (00,3), 10 51 cm 37 06 39 c0 48 51 cm 37 06 30 cm 38 c0 48 c0 48 c0 48 c	<pre>But 6012 bits) on in 57). Out: Micro-50.001 60 ± 183). Oct: 102 166 51 #0011 102166 51 #0011 109180 (19065). 0.0011 1090</pre>	terfac 0 1:ff (40:81:88:86:f1:ff) 1:88.111 (192:158.183.111) 90(11, 408: 7, (en. 30

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.

ps List				171	- 1 - -
Time 4	Account ¢	IP Address a	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	liester	192, 168, 186, 1	Login OK	Login	Login False
05-11 11:42:38	inster	192,168,188,1	Logn OK	Login	Login Exten
05-11 11 42 33	leater	192 168 188 T	Login OK	Login	Login False
05-11 11 42-34	Tenter	192 168 188.1	Logn OK.	Login	Login Ealare
05-11 11:42:15	Jester	192.168.188.1	Logout	Logout	Lopout Successful
05-11 11 42:07	admin	192,168,186,1	Logout	Logait	Logout Successful
05-11 11:07:07	admin	192 168 188 1	Login OK-	Login	Login Successful
05-09-14-51-57	naredy	154 73 53 30	Logn OK	Login	Login Successful
05-08 18:06:10	admin	192 168 188 1	Configuration > Backup & Upgrade > Auto Backup	Download	Data
05-08 18:03 11	admin	152 168 188 1	Configuration > Backup & Upgrade > Auto Backup	Save	Etad
06-08 17:37 19	admin	192 168 168 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	192,168,586,50	Networking > Interfaces > Interface Corrlig	Save	Interface Config
05-08 17 29 44	admin	192.168.196.50	Login OK	Looin	Looin Successful

Figure 10-1. 1 Logs

Chapter 10 : Logs



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.

1 Search Condition						
Account	(and) .*					
Computer Name	• IAI • IAI					
IP Address	() Al +					
Salect All	8					
Login Logout	🕷 System Logn 🕷 Logout					
Configuration	🕷 Date & Time 🕷 Administration 🕷 System 🕷 Language 🕷 Signature Update 🕷 Ap Management					
Network	₩ interface ₩ Routing ₩ 802.10					
Pošcy	AN Policy & DMZ Policy & WAN Policy					
Chiects	🕷 Address. 🕷 Services 🕷 GoS: 🕷 Schedule 🕷 Application Software 🕷 UPL					
Network Services	R DHCP R DDNS Remote Systog Server					
VEN	₩ VPN Turnel & PPTP Server & PPTP Client					
	O Search					

Figure 10-1. 2 Logs Search



Chapter 10 : Logs

Logs Search Result

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

Time +	Account +	IP Address e	Function Path	Action	Description
06-09 14-51 57	randy	164 73 53 30	Login OK	Login	Login Successful
04/29/00/24:54	raridy	192,16B,188.1	Login OK	Login	Login Successful
04-29 00 20 06	randy	192 168 188 1	Login QK	Login	Login Successful
04-29-00-19:00	randy	192.168.185.1	Login CK	Login	Logn False
04-29 00 18 54	randy	192 168 188 1	Light OK	Login	Login Ealas
04-29 00 18 31	randy	192,168,185,1	Logout	Engout	Logist Successful
64-29 00 18 21	candy	192.168.188.1	Engout	Logout	Longot 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 . 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



Chapter 11 : Status



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)

		-				ob hull of th	eren i eren eren eren eren eren eren ere	2. or r .
0.0 00000 0200 0400 0600 0800 1000	bita/s	10 0.8 0.6 0.4 0.2						
Average up out by a warage down out by s	A 9	0,0 + 00:00 erage up 0,0	02:00 10 b/s Avers	04:00 ige down 0.00	06:00 b/s	08:00	1000	

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



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



Chapter 11 : Status



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

History Status

Select Status > Performance > History Status. Set information, and click on • Sume. 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 <u>Refresh</u>. You are also able to enter <u>Excluding IP</u> 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.

10107	05.	Shitie	Alian	ID Address A	MAC Address +	Interface +	Shiftin a	Last Undata Time .
	10.00	and the second		Concentration			and the second se	and a product the set
2	_		192 168 106 253	192.108.186.253	00.05 18.03.04.22	LAN	4	
a			192,168,186,245	192.168.586.245	00 90 fb 2b 2f e7	LAN		
		0	Peter	192.168.186.50	1c 6F.65 28 9c dc	LAN	۹.,	2016-05-14 14 28:02
8			152 168 196.1	192 168 106 1	10 all 6x 0f 15 81	LAN	2	
			152 168 1 5	192,168,1.5	00:0f.38.6b.77.b2	LAN	8.	2015-05-12 15:00:03

Figure 11-2. 1 Computer List



Total on	too: T		Batanh Start OS	Detect				1/2 1 00 (4) (1) (1)
Select	05	Static	Computer Name +	IP Address .	MAC Address +	basertace +	Status +	State Update Time +
13	122		192.168.1.20	192,168 1.26	00:0c:6e:b5:8:m5	LAN	5	2010-10-19 10:00:53
13	2		EX07SP1	192_168 1.91	00 0c 29 e3 60 ec	LAN	5	2010-10-18 10:00:53
0	19		VM_TEST	192.168 1.68	00.01:29:34:15:58	LAN	5	2010-10-15 10 00 53
D	0		MWE.PC	152.168.1.111	48:61:05:66.左非	LAN	5	2010-10-19 10:00 53
0	20 5	OS: Microsof	N Windows Viste	192.168 1.24	00/22/cf.25/1e/12	LAN	\$	2010-10-19-10-00-53
13	1	PORT Protoco	Mile Anacha Miner 7.7.0 (0040-72) Public 7.4	92.168.1.86	00.0c.29-99.06 au	LAN	5	2010-10-15 10:00:53
10	R	135 top	margine Microsoft Windows RPC	192.168.1.23	45:61:96:02;0c:3a	LAN	5	2010-10-19 10:00:53
8	1	43 top	stype2 flype	92.168.1.127	00 Oc 25 59 36 au	LAN	2	2010-10-13 10:44.01
8	20	start the	http:// Microsoft HTTFXP1 Word 2.0 (SSDPR)PoP	192.160.1.92	00:0c:29:23:37:a0	LAN	4	2010-10-14 05 08 02
21	11		ROOKES_WU_2	192 168 1 93	00.0c 29.23 37 a0	LAN		2010-10-14 03-16-01
10	27		192-168.1.155	192.168.1.165	6c:10:49:68:a9:5f	LAN	8.	2010-10-15 09:28:02
10	0		KRN-PC	192.168.1.158	44.07.tc.43.95.60	LAN		2010-10-15 00 36 02
13	21		PC.	192.168.155.23	00.08 02 d9 du 20	DM2	a.	2018-10-18 22 40 02
0	1		192.168.156.1	192.168.156.1	00 0d 48 De 21 ed	DMZ		2010-10-14 11 26 02
101	itei	1	pinatolicate a	ADD ACD & MILL	00-04-30-30-44-5E	1.000		TRAD 42 44 44 42 D1



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)

1	On lin	e: 0	Re	te-iti	Client OS Detection Excludio	ng IP			AL . 1/1
		05	Static	Alim +	IP Address	MAC Address +	Interface +	Stime +	Last Update Time +
						🗶 D+i			



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)

() On line	1	Retruch				1/1 30 00 00 00
0	AP Allas +	55ID +	IP Address .	MAC Address +	Status	Last Update Time .
0	AP-200	AP-200	192 168 1 2	M-H 5a 89 water	8	2016-65-19 16 44 02
				× Del		



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)



Chapter 11 : Status

- 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 / To	tal Session : 904 / 1434	ALL T	Outgoing • 30 Seconds • #	atrosh 1/4 1	
Computer Name	IP Address	Semion +	Up Speed bits .	Down Speed bits .	Log
192.168.188.23	192 168 189 23	815	28.55K	13.58K	Lin
192, 168, 189, 12	192.168.189.12	110	40.24K	38.190	Lag
192.168.188.31	192 168 168 31	56	6.68K	13.470	(Leg)
192, 168, 189, 19	192.168.189.19	81	£ 76K	0.62%	Les
192 168 189 21	192 166 169 21	70	0	0	Leg
152, 168, 186, 50	152,168,186,60	62	1.386	1.5K	Leg
192 168 169 242	192.168.189.242	61	0	0	Les
192 168 189 243	192,168,189,243	44	0	0	Lts
192.168.188.159	192,968,188,359	42	9K	6.0K	Leg
192 168 186 99	192 168 186 99	42	0	0	Leg
192 168 189 244	192,168,189,244	-40	432	0	Leg
192 168 186 38	192 168 186 38	33	0	D	Lea
192 968 186 201	192.168.186.201	- 31	0	0	Leg
192.168.189.7	192.168 189.7	28	260	880	(Les
192 168 188 103	192.168.188.103	28	520	0	Les
152 168 189 20	192 198 189 20	27	0	0	Les

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	2		search kiear	0 Seconds	• insteach inte	arat
Protocol	Source IP	Destination IP	Port	WAN	Up Packets	Down Packets	t/10 Up bytes	1 Down bytes	Police
utto	192 168 189 20	168 95 1.1	54597 -> 53	8	1	1	576	1.07K	LAN to WAN [11]
udp	152 168 169 23	168.95.1.1	65140 -> 53		2	2	1.050	1.65K	LAN to WAN [11]
tep	192.168.169.23	23.13.167,122	59047 -> 90	8	20	9	11.68K	32.2K	LAN to WAN [70] 2014-02-12-再借重WAN2
tep	192 168 188 23	64 233 189 132	58931 -> 80	8	13	13	18.12K	71.43K	LAN to WAN (70) 2014-02-13-制倍忠WAN2
tep	192 168 189 23	74 126 23 191	58907 -> 110	8		7.	6.84K	9.316	LAN to WAN [70] 2014-02-12-常相主WAN2
ttp	102 168 189 23	47.22.13.43	59064 -> 48054	8	21	17	18.06K	17.24K	LAN to WAN [31] CK 30140503
top	192.168.189.23	23 13 197 122	59011 ~ 80	E	15	15	9.48K	116.9K	LAN to WAN [70] 2014-02-12 其相志WAN2
tepi	102 168 180 23	74.125.23.94	68880 -> 443	10	10	10	6.42K	12.2K	LAN to WAN [20] 2014-02-12 容卢维据常用PORT
tep-	192.168.189.23	23.13.184.216	58967 -> 80	E	-13	13	21.34K	75.27K	LAN 10 WAN [70] 2014-02-12 其他主WAN2
trp	192,168,189,23	74 125 204 99	60062 > 443	0	11	12	29.45K	25.32K	LAN to WAN [20] 2014-02-12 資产修繕常用PORT
udp	152 168 189 23	168.95 1.1	53897 -> 53		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.

to Top N Fla	ree Search :					
Flow Direction	All • Outgoing •	All Outgoing *				
Top N Flow	10 +					
Statistics Pe	riod 2015-05-19-00-00-00 - 21	2015-05-19-00-00-00 - 2015-05-19-11-33-27				
			• Start			
Marc	Computer Name A	ID Address A	MAC Address 4	Un Elmathistical +	1/11 1 Dear Dear Dear Dear Dear Dear Dear Dear	
1	192 168 189 19	152 168 189 19	NO 28 50 07 15 81	op Provincipanta +	604 445 09	
2	192 168 188 159	192 168 188 169	00.00 at Selecist	34 325 29	358,732,43	
3	152 168 191 166	192 168 191 168	60 a8 5e 0f 15 81	57,712.89	353.128.88	
4	192,168,189,22	192 168 189 22	1/0 s8 6e 07 15 81	22,918,27	151,665,37	
5	192 168 189 242	192 168 189 242	60 a8 6e 0f 15 81	15.669.12	140,721,42	
6	192 168 186 50	192 168 186 50	60 a8 5e 01 15 81	87.714.77	110.908.37	
9	192, 168, 196, 61	192.168.195.51	00 ±0 ±0 51 ±1.18	19 643 33	109,758.62	
	192 168 189 12	152 168 189 12	50 a5 5e 0f 15 81	17.299.93	84,528,54	
9	192 108 189 241	192 168 189 241	60 a8 Se 0f 15:81	6.935.38	75.563.47	
10	192 158 189 20	192 168 185 20	50 x8 5e 0f 15 81	5 301 56	65,688,63	

Figure 11-3. 1 Top N Flow


Chapter 11 : Status

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)

4 IP : 192.168.189.20	Type : Out	tgoing			
Service	Up Firm(kbytes)	Percentage	Down Flow(hbytes)	Percentage	Record
DNS	56.70	176	128.45	< 174	Leg
HITP	3,600,89	.39%	27.562 Hi	41%	Line
other	718.30	8%	13,409.91	20%	5.04
IMAP	13.21	< 1%	766.21	1%	Les.
HTTPS	4.914.02	63%	24,826-23	37%	Leg

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		(6)	Type : Outgoing		10	Service : HTTP	EI Be	werse Dat IP	Back
						1244	1 (1)	Export Al	E
Date	Pintocol	Sie IP	Dat 1P	Port	WAN	Up Flow(khytes)	Down Flow(khytes)	Policy	
2015-05-19-08:33:59	tεp	192.168.189.20	74.204.71.137	49208 -> 80	8	1.23	2.77	LAN to WAN [70] 2014-02-12-34	他主WAN2
2015-05-19 08:34:29	ttp	192,168,189-20	111.221.29.13	49227 → 80		0.96	1.15	LAN to WAN [70] 2014-02-12-34	他走WAN2
2015-05-19 08:34:59	tτp	192.168.189.20	170.255.83.1	49199 -> 80		1.43	3.18	LAN to WAN [70] 2014-02-12-18	他主WAN2
2015-85-15 88 34 59	ttp	102 168 189 20	103.23.106.224	49277 -= 80	E	11.08	15.31	LAN to WAN [70] 2014-02-12-M	他走WAN2
2015-05-19-08-34 59	tzp	192.168.189.20	202.39.236.195	49275 ~ 80	2	0.96	5.91	LAN to WAN (70) 2014-02-12-14	他主WANZ
2015-05-19 08:34:59	tep	192 168 199 20	178.255.83.2	45206 -> 80	2	1.70	63.47	LAN to WAN [70] 2014-02-12-#	他主WAN2
2015-05-19 08 36 30	tep	192 168 189 20	2012.66.2113.185	49313 -> 80	E	1.01	7.72	LAN to WAN (70) 2014-02-12-14	相老WANZ
2015-05-19 08 36:00	top	162,168,189,20	192 229 145 200	49221 → 80	8	0.55	1.06	LAN to WAN [70] 2014-02-12-14	地本WAN2
2015-05-15 08:37 00	htp	192.168.189.20	103.23.108.119	45318 -> 80	2	1.66	5.54	LAN IS WAN [70] 2014-02-12-86	他走WANZ
2015-05-19-08:37:00	tτp	192.168.189.20	54,65.184.229	#9379 -+ 80	E	5.20	14.90	LAN to WAN [70] 2014-02-12-14	他主WAN2
2015-05-15 08 37 00	tcp	192.168.185.20	68.232.44.121	45328 -> 80		5.21	33 33	LAN to WAN [70] 2014-02-12-34	他主WAN2
2015-05-19-08:37-00	trp	192.168.189.20	203.66.213.165	49312 80	0	3.43	40.47	LAN to WAN [70] 2014-02-12-18	他主WAN2
2015-85-15 08 37 00	tip -	102 168 189 20	118 163 170 12	49294 -> 80	E	1.88	22.97	LAN to WAN [70] 2014-02-12-M	他主WAN2
2015-06-19-00:37-00	tzp	192.168.189.20	103 23 108 224	49289 -> 80	8	27.50	76.58	LAN to WAN (70) 2014-02-12 #	他主WAN2
2015-05-19-08:37:00	tep	102.168.189.20	103,23,108,184	45316 -> 80	2	0.80	1.16	LAN to WAN [70] 2014-02-12-M	他主以从12
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) 2014-02-12-14	相差WAND

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.

ow Direction	Outgoing *		
A RI Flow	10 -		
p in r tom			
atistics Period	2016-05-19 00 00 00 - 2015-05-19 11 37:20		
		• Irach	
			1/11 1 💷 🗷 🗃 🔅
No.	Destination Part	Up Flow a	Down Flow +
+	HTTPS	137.974.88	928,671,47
2	HITP	99,054.80	1,723,227.96
3	51938	83 772 00	435.43
4	13642	68,927 72	3.094 72
5	2000	54.285.77	1,645,48
-61	SMTP	47.630.71	3.960.75
Z .	808	34 740 45	145,350.85
8	IMAP	10.824.84	26.567.47
n -	673	15.093.06	570.55
		and the second se	

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 • starth you will see search result as below.



1 Search Top	N Flow :				
Date	2015-05-10 00 • 00 • 201	5-05-19 23 * 00 *			
Flow Direction	WAN1 . Outgoing .				
Connection	Inside IP [Al	•) → •	Dutside Post		
Top Flow Search	h Top[10]•				
			· Search		
+ Search Res	dt :				
Top Flow Search	11 Top 10				
Date	2015-05-19 00:00 00 + 2015-05-	9 23 00 00			
	7.			1942 32 37 77	
No.	Computer Name #	IP Address a	MAC Address a	Up Flow(kbytes) #	Down Flow(kbytes) #
1	192 168 169	192 168 168 169	00 00 at 5e ec st	Up Flow(kbytes) # 23.107.71	Down Flow(kbytes) # 215,526.96
No. 1 2	192 168 198 193 192 168 198 195	192 168 186 156 192 168 191 166	MAX, Address a 00.00 at 5e ec zc 60.a6.5e 0F 15.81	Up Flow(bbytes) # 23,107.71 27,646,12	Down Flow(kbytes) # 215,526.96 174,421.07
No. 1 2 3	Computer Name # 192 158 159 192 158 191 158 192 158 191 158	192 168 159 192 168 159 192 168 191 166 192 168 191 166	MAC, Address + 02.00.at 5e.ec.st b0.a6.6e.0f 15.81 b0.a0.6e.0f 15.81	Up Flow(kkytm) + 23, 107 71 27, 846 12 22, 101.05	Down Flow(kbytes) = 215,526.96 174,421.07 146,706.51
No. 1 2 3 4	Computer Name # 192 168 188 153 192 168 191 168 192 168 192 22 192 168 199 242	87 Address a 192 568 188 159 192 168 191 166 192 168 189 22 192 168 189 242	MAX, Autoress a 00:00:a1:5x:ec.zr. 50:a8:5e.01:15:81 50:a8:5e.01:15:81 50:a8:5e.01:15:81	Up How(klytin) # 23,107.71 27,646.12 22,101.05 9,009.28	Down Filow(khytes) # 215,526 96 174,421 07 145,706 51 119,428 23
No. 1 2 3 4 5	Computer Name # 192 168 188 155 192 168 191 166 192 168 199 22 100 168 169 242 192 168 199 19	HP Address # 192,168,158,159 192,168,151,165 192,168,161,222 192,168,189,242 192,168,189,19	MAX: Address = 00.00 at 5e or sc 00.05 5e 0F 15.81 00.05 5e 0F 15.81 b0.06 5e 0F 15.81 b0.06 5e 0F 15.81	Up How(kbytm) # 23,107.71 27,646.12 22,501.05 9,609.20 8,896.61	Down Filow(khytes) # 215,526.96 174,421.07 145,706.51 119,428.23 76,335.83
No. 1 2 3 4 5 6	Computer Name + 192 168 189 155 192 168 197 169 192 168 197 22 192 168 199 22 192 168 199 19 192 168 199 26	HP Address a 192 198 188 189 192 188 191 188 192 188 191 22 193 188 189 22 193 188 189 242 193 188 189 19 193 168 189 19	MAX, Audiness + 00.00 at 5e c st. 00 at 5e 01 5 81 00 at 5e 01 5 81 00 at 5e 01 15 81 00 at 5e 01 15 81 00 at 5e 01 15 81	Up How(kbytm) + 23,107.71 27,646.12 22,101.05 3,609.20 8,896.61 4,236.73	Down Flow(khytes) 4 215, 526 96 174, 421 07 146, 706 51 119, 429 23 76, 335 63 57, 409 85
No. 1 3 4 5 6 7	Computer Name + 192 168 189 155 192 168 197 168 192 168 197 168 192 168 199 22 192 168 199 19 192 168 199 19 192 168 199 26 192 168 195 26	HP Address a 192 198 188 189 192 188 191 186 192 188 191 22 193 188 189 24 192 188 189 242 192 188 189 242 192 188 189 29 192 168 189 39	MAX, Autoress 4 00.00 at 5e cr.s. 50 a6 5e 01 5 81 50 a6 5e 01 55 81 50 a6 5e 01 581 50 a6 5e 01 15 81 50 a6 5e 01 15 81 50 a6 5e 01 15 81	Up How(kbytm) + 23,107.71 27,648.12 22,101.05 3,609.28 8,896.61 4,236.73 28,673.05	Down Flow(khytes) 4 215 526 96 174 421 67 146 706 51 119 428 23 76 335 83 57 409 88 54 613 54
No. 1 2 3 4 5 6 7 8	Computer Name # 162 168 169 169 192 168 199 169 192 168 199 22 192 168 199 242 192 168 199 242 192 168 199 26 192 168 199 26 192 168 195 26 192 168 195 151	UP Address a 192 198 198 199 192 198 191 198 192 198 191 198 192 198 199 24 193 198 199 242 192 198 199 19 192 198 198 29 192 193 199 19 193 193 193 191	MAC, Address 4 00 00 at 5e et st 00 at 5e 01 5 51 00 at 5e 01 55 11 00 at 5e 01 51 51	Up How(kbytm) # 23,107.71 27,848.12 22,101.05 9,609.28 8,896.61 4,336.73 28,679.95 1,256.54	Down Flow(shytes) # 215,526.96 174,421.07 146,706.51 119,428.23 76,336.83 57,509.85 54,613,54 46,213,96
No. 1 2 3 4 5 6 7 7 8 9	Computer Name # 162 168 169 169 192 168 199 169 192 168 169 22 192 168 169 242 192 168 169 26 192 168 169 26 192 168 169 26 192 168 169 24	HP Address a 192 592 188 159 192 188 191 186 192 188 191 186 192 188 189 242 192 188 189 242 192 168 189 19 192 168 186 39 192 168 196 39 192 168 199 244	MAC, Address 4 00 00 at 56 et 11 00 at 56 0f 15 81 00 at 56 0f 15 81	Up Flow(blytm) # 23,107.71 27,846.12 22,501.05 38,609.28 8,896.67 4,236.73 28,673.86 1,250.54 3,617.86	Down Flow(shytes) # 215,526 96 174,421 07 146,706 51 119,428 23 76,336 83 67,509 88 54,613 54 48,213 56 44,613 54 48,213 56 44,213 56

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)

IP : 192.168.188.159	Type : Outgoing				
Service	Up Flow(kbytes)	Percentage	Down Flow(kbytes)	Percentage	Record
HTTPS	17,911.04	74%	210,976.31	92%	Leg
other	6.191.24	26%	18,091.14	35	Los

Figure 11-3. 6 Top N Search Detail

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

IP : 192.168.188.1	59		Type : Outgoin	9) Service : HTTP	· 5	B Revene Dst IP	Back
							1/116 1 🔤	Henry Carles and Export All	٠
Chate	Protocol	Stc.IP	Dat #P	Pott	WAN	Up Flow(kbytee)	Down Firm(kbytes)	Policy	
2015-05-19 00:00:32	ttp	192,168,108,159	23 100 42 232	59327 -> 443	10	0.84	1.92	LAN to WAN [19] 2014-02-12 客戶催擾常用PI	ORT
2015-05-19-00-01-02	tep	192,368,188,169	23 105 42 232	60336 -> 443	13	1.26	2.88	LAN to WAN [19] 2014-02-12 晋戶總選求帝P6	ORT
2015-05-15 00:01:33	htp	192.168.188.159	104.45.86.116	56088 -> 443		0.84	1.92	LAN to WAN [15] 2014-02-12 客戶條證來用Pr	ORT
2015-05-19 00:02:33	tep	192.168.168.169	104.45.86.116	56103 -> 443	0	1.26	2.88	LAN to WAN [19] 2014-02-12 容戶總羅常用PI	ORT
2015-05-19 00:03:34	ttp .	192, 168, 188, 159	23.100.42.232	69376 > #43	10	0.84	1.92	LAN IN WAN [19] 2014-02-12 客戶催還常用PI	ORT
2015-05-19 00 04 04	tcp	192 168 108 159	23 100 42 232	69386 -> 443	10	1.66	3.84	LAN to WAN [19] 2014-02-12 省戶建議常用户	ORT
2015-06-15 00:04:34	tep -	192 168 188 155	23.100.42.232	68395 -> 443	0	1.26	2.88	LAN to WAN [19] 2014-02-12 容戶建議常用PI	OFT
2015-05-19-00-06-05	ttp	192.168.188.159	23 103 42 232	69418 -> 443		1.26	2.88	LAN to WAN [19] 2014-02-12 客戶確接意用Pt	ORT





Chapter 11 : Status

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)

& Basic Setting						
Policy Name						
Source 🕢	Inside_Any •	© IP Addrese		MAC Address		
Destination 🜍	Outside_Any •	IP Address		1		
Action	Perrut •					
10 Policy						
Protocol			ALL +			
Service Port or Group			User Defined	 Service Port 		
Software Access Control			None			
QoS			None •			
Schedule			None			
UFIL Access Control			None •			
Authantication			None •			
Bulletin Board			Nione 🔻			
W0A74			ALL •			
Max. Concurrent Sessions for E	ach Source IP Address		0			
IDP			10			
Packet Tracing			65			
Traffic Analysis			0			
Max. Quota / Day			Up 0	KBytes / Down 0	K8ytes (0:No Limit)	
Max. Quota / Day/Per Source R	Þj		Up 0	KBytes / Cown 0	KBytes (0 No Limit)	
5 Firewall Protection						
SYN Attack III ICMP Attac	k ⊟ UDP Attack .					
			+ 644			

Figure 11-3. 8 Quota / Day

U Dawry 1				
Dana (2015-46-21	III - (2015-05-21 III)			
Se P				
		O Jaarn		
5 Search Neselt 1				
	Woland Backets .	Desering Parkets	the Floratkinstern +	Driver Finnelkinstent +

Figure 11-3. 9 Search Quota History