

# User's Manual



## UTM Content Security Gateway

▶ CS-950



## **Copyright**

Copyright (C) 2017 PLANET Technology Corp. All rights reserved.

The products and programs described in this User's Manual are licensed products of PLANET Technology, This User's Manual contains proprietary information protected by copyright, and this User's Manual and all accompanying hardware, software, and documentation are copyrighted.

No part of this User's Manual may be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form by any means, electronic or mechanical including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, and without the prior express written permission of PLANET Technology.

## **Disclaimer**

PLANET Technology does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose.

PLANET has made every effort to ensure that this User's Manual is accurate; PLANET disclaims liability for any inaccuracies or omissions that may have occurred. Information in this User's Manual is subject to change without notice and does not represent a commitment on the part of PLANET. PLANET assumes no responsibility for any inaccuracies that may be contained in this User's Manual. PLANET makes no commitment to update or keep current the information in this User's Manual, and reserves the right to make improvements and/or changes to this User's Manual at any time without notice.

If you find information in this manual that is incorrect, misleading, or incomplete, we would appreciate your comments and suggestions.

## **FCC Compliance Statement**

This Equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can

be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

#### **CE mark Warning**



The is a class A device, In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

#### **WEEE**



To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

#### **Trademarks**

The PLANET logo is a trademark of PLANET Technology. This documentation may refer to numerous hardware and software products by their trade names. In most, if not all cases, these designations are claimed as trademarks or registered trademarks by their respective companies.

#### **Revision**

User's Manual of PLANET UTM Content Security Gateway

Model: CS-950

Rev.: 1.0 (Nov., 2017)

Part No. EM-CS-950\_v1.0

# Table of Contents

<b>Chapter 1. Product Introduction.....</b>	<b>9</b>
1.1 Package Contents.....	9
1.2 Overview .....	10
1.3 Features.....	14
1.4 Product Specifications .....	16
1.5 Hardware Interface .....	19
1.5.1 Diagrams:.....	19
1.5.2 LED:.....	19
1.5.3 Interfaces:.....	20
1.6 Topology .....	21
<b>Chapter 2. Hardware Installation.....</b>	<b>22</b>
2.1 Desktop Installation.....	22
2.2 Rack Mounting.....	23
<b>Chapter 3. Preparation .....</b>	<b>25</b>
3.1 Requirements.....	25
3.2 Setting TCP/IP on your PC .....	25
3.2.1 Windows XP .....	25
3.2.2 Windows 7 .....	27
3.2.3 Windows 10 .....	31
<b>Chapter 4. Login .....</b>	<b>34</b>
4.1 Logging in to the Security Gateway .....	34
4.2 Homepage .....	34
4.2.1 MENU .....	35
4.2.2 Language.....	36
4.2.3 Administrator Login.....	36
4.2.4 Interface.....	37
<b>Chapter 5. Configuration.....</b>	<b>38</b>
5.1 Date & Time .....	38
5.2 Administration .....	39
5.2.1 Administrator .....	39
5.2.2 System.....	41
5.2.3 IP Address .....	43
5.2.4 Clear Data .....	45
5.2.5 SMTP Server .....	46
5.3 System .....	47
5.3.1 System Backup.....	47

5.3.2	Firmware Message .....	47
5.3.3	Software Upgrade.....	48
5.4	Language .....	49
5.5	Notification .....	50
5.5.1	Notification .....	50
5.5.2	Notification Log.....	52
5.6	Report .....	53
5.6.1	Basic Setting.....	53
5.6.2	Recipient.....	55
5.7	Backup & Mount.....	56
5.7.1	Data Backup .....	56
5.7.2	Data Mount .....	57
5.8	Signature Update .....	58
5.9	CMS <del>.....</del> .....	59
5.9.1	CMS Setting (Client).....	59
5.9.2	CMS Setting (Server) .....	60
5.9.3	CMS Monitor.....	60
5.10	AP Management .....	61
5.10.1	AP Management Setting .....	61
5.10.2	AP Management .....	61
5.11	SSL Certificate .....	64
<b>Chapter 6.</b>	<b>Network.....</b>	<b>66</b>
6.1	Interface .....	66
6.1.1	LAN.....	66
6.1.2	WAN_1 .....	68
6.1.3	WAN_2 .....	70
6.1.4	DMZ.....	72
6.2	Interface (IPv6) .....	73
6.2.1	LAN (IPv6) .....	73
6.2.2	WAN_1 (IPv6).....	73
6.3	Routing.....	74
6.3.1	Routing Table .....	74
6.3.2	IPv6 Routing Table .....	74
<b>Chapter 7.</b>	<b>Policy .....</b>	<b>75</b>
7.1	LAN Policy, DMZ Policy, and WAN Policy.....	75
7.2	LAN to WAN (IPV6) .....	78
<b>Chapter 8.</b>	<b>Objects .....</b>	<b>80</b>
8.1	Address Table.....	80
8.1.1	LAN IP Address.....	80
8.1.2	LAN Group.....	81

8.1.3	DMZ IP Address .....	82
8.1.4	DMZ Group .....	83
8.1.5	WAN IP Address.....	83
8.1.6	WAN Group .....	84
8.2	Services .....	84
8.2.1	Basic Service .....	84
8.2.2	Service Group.....	85
8.3	Schedule .....	86
8.4	QoS .....	87
8.5	Application Control .....	89
8.6	URL Filter .....	90
8.6.1	List Settings .....	90
8.6.2	URL Settings .....	91
8.6.3	Other Settings.....	91
8.7	Virtual Server .....	92
8.7.1	Virtual Server.....	92
8.7.2	Mapped IP .....	94
8.8	Firewall Protection .....	98
8.8.1	Firewall Protection .....	98
8.8.2	Attack Log.....	99
8.9	Authentication .....	100
8.9.1	Auth Setting .....	100
8.9.2	Page Setting .....	102
8.9.3	Local User .....	103
8.9.4	POP3, RADIUS User.....	104
8.9.5	AD User .....	105
8.9.6	User Group .....	105
<b>Chapter 9.</b>	<b>Network Services .....</b>	<b>107</b>
9.1	DHCP .....	107
9.1.1	DHCP User List .....	107
9.1.2	DHCP Server .....	107
9.1.3	DHCP Static IP .....	108
9.2	DDNS .....	108
9.3	DNS Proxy .....	110
9.4	Web Services.....	111
9.5	FTP Services .....	111
9.6	High Availability.....	112
9.7	SNMP.....	114
9.8	Remote Syslog Server .....	114
<b>Chapter 10.</b>	<b>Advanced Protection .....</b>	<b>116</b>

10.1	Anomaly IP Analysis .....	116
10.1.1	Log Anomaly .....	116
10.1.2	Notify Anomaly .....	116
10.1.3	Notify Anomaly .....	118
10.1.4	Trusted IP .....	118
10.1.5	Anomaly Log .....	119
10.1.6	Block List .....	120
10.2	Switch .....	120
10.2.1	Switch Setup .....	120
10.2.2	Switch Status .....	122
10.2.3	Bind list .....	122
10.3	Intranet Protect .....	123
10.3.1	Spoofing Setup .....	124
10.3.2	ARP Spoofing Log .....	125
10.3.3	MAC Collision Log .....	125
10.3.4	IP Collision Log .....	125
10.3.5	Lock Status .....	126
<b>Chapter 11. Mail Security .....</b>		<b>127</b>
11.1	Filter & Log .....	127
11.1.1	Filter & Log .....	127
11.1.2	Valid Account Setting .....	129
11.1.3	Graylist and IP Resolved .....	132
11.1.4	Traffic Blocking .....	133
11.1.5	SMTP Blocking IP .....	134
11.2	Anti-Virus .....	134
11.3	Anti-Spam .....	135
11.3.1	Spam Setting .....	135
11.3.2	Auto Learning .....	137
11.3.3	Personal B & W .....	137
11.3.4	System B & W .....	139
11.4	Mail Log .....	140
11.4.1	Today Mail .....	140
11.4.2	Mail Search .....	141
11.4.3	Mail Search Result .....	142
11.5	SMTP Log .....	142
11.5.1	SMTP Log .....	143
11.5.2	SMTP Log Result .....	143
<b>Chapter 12. IDP .....</b>		<b>144</b>
12.1	Basic Setting .....	144
12.2	IDP Log .....	146

12.2.1	IDP Log .....	146
12.2.2	IDP Log Search.....	146
<b>Chapter 13.</b>	<b>SSL VPN.....</b>	<b>147</b>
13.1	SSL VPN Setting.....	147
13.1.1	SSL VPN Setup.....	147
13.1.2	SSL Client list.....	149
13.1.3	Software Download Page Setting .....	149
13.2	SSL Client On-Line Log .....	149
13.3	VPN Policy .....	149
13.3.1	VPN to Internal.....	150
13.3.2	Internal to VPN.....	151
<b>Chapter 14.</b>	<b>Content Record .....</b>	<b>154</b>
14.1	Web Virus Record .....	154
14.2	FTP Virus Record .....	154
<b>Chapter 15.</b>	<b>VPN.....</b>	<b>155</b>
15.1	IPSec Tunnel .....	155
15.1.1	IPSec Tunnel.....	155
15.1.2	Add IPSec Tunnel .....	156
15.2	PPTP Server .....	157
15.2.1	PPTP Account List .....	158
15.2.2	Add Account.....	158
15.2.3	PPTP Server .....	159
15.3	PPTP Client .....	159
15.3.1	PPTP Client.....	160
15.3.2	Add PPTP Client .....	160
15.4	VPN Policy .....	160
15.4.1	VPN to Internal.....	161
15.4.2	Internal to VPN.....	162

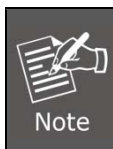


# Chapter 1. Product Introduction

## 1.1 Package Contents

The package should contain the following:

- CS-950 x 1
- Quick Installation Guide x 1
- Adapter x 1
- Power Cord x 1
- Console Cable x 1
- Ethernet Cable x 1
- Screw Package x 1
- Rack-mount Ear x 2
- Feet Pads x 4



If any of the above items are missing, please contact your dealer immediately.

## 1.2 Overview

### All-in-One Network Security Solution

The innovation of the Internet has created tremendous worldwide opportunities for e-business and information sharing. It has become essential for businesses to focus more on network security issues. The demand for information security has become the primary concern for the enterprises. To fulfill this demand, PLANET has launched the CS-950 UTM Content Security Gateway, an all-in-one appliance that carries several main categories across your network security deployments: firewall security protection, policy auditing (content filtering, VPN, and authentication), and easy management (CMS, wireless AP management and flow analysis). Furthermore, its VLAN, QoS and Outbound Load Balance features can improve the network efficiency while the web-based interface provides friendly and consistent user experience.



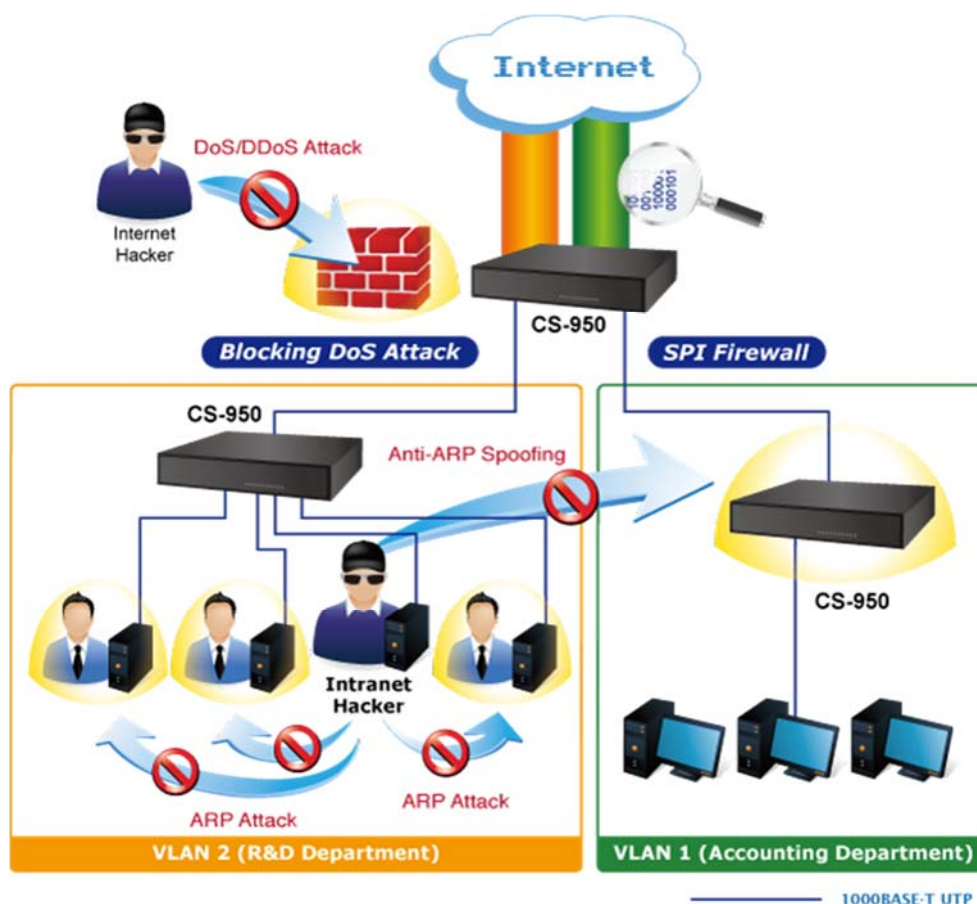
### Excellent Ability in Threat Defense

The CS-950 adopts Clam AV for virus scanning which detects over 800,000 kinds of viruses, worms, and Trojans. Once suspicious emails are detected, the CS-950 will modify the subject and record the mail. Besides, websites and FTP will be scanned once the function of antivirus is enabled in policy. It also employs multi-spam filters, auto learning, and personal Blacklist/Whitelist. It gives administrators the flexibility to enforce custom filtering. These help companies to create their own database by importing the latest spam update. Using the filter, the following action like forward or delete can be taken for any mail identified as a spam.

An advanced protection of UTM, the co-defense SNMP switch can be known on which computer and which switch port at the earliest possible time which prevents business network from failure, and monitor network-attached devices for conditions that warrant administrative attention.

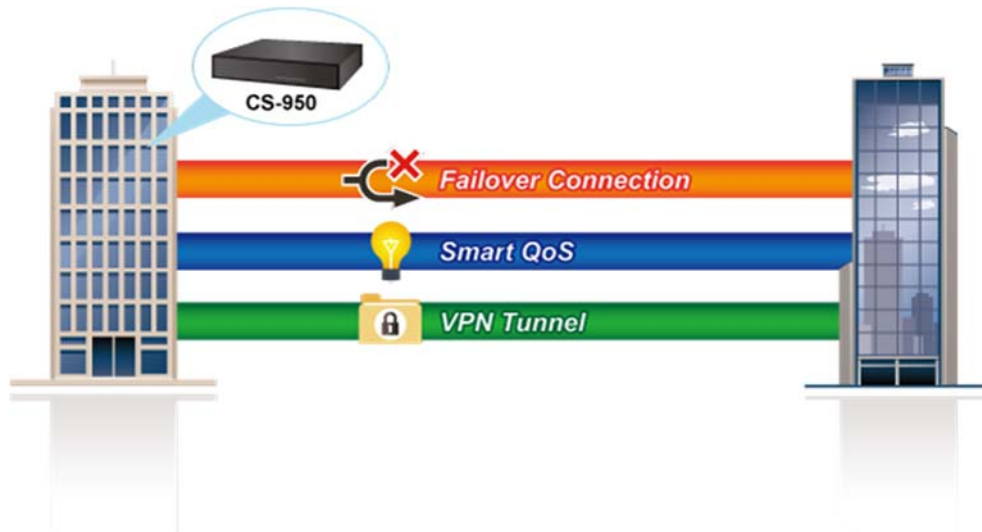
Moreover, its built-in SPI (Stateful Packet Inspection) firewall and IDP (Intrusion Detection

and Prevention) functions provide DoS detection and block concealed malicious code or worms delivered in TCP/IP protocols. As soon as an attack is suspected, the CS-950 will immediately notify the IT administrator and an extensive range of reports will be available for analysis.



### Cost-effective VPN Security Gateway Solution for SMBs

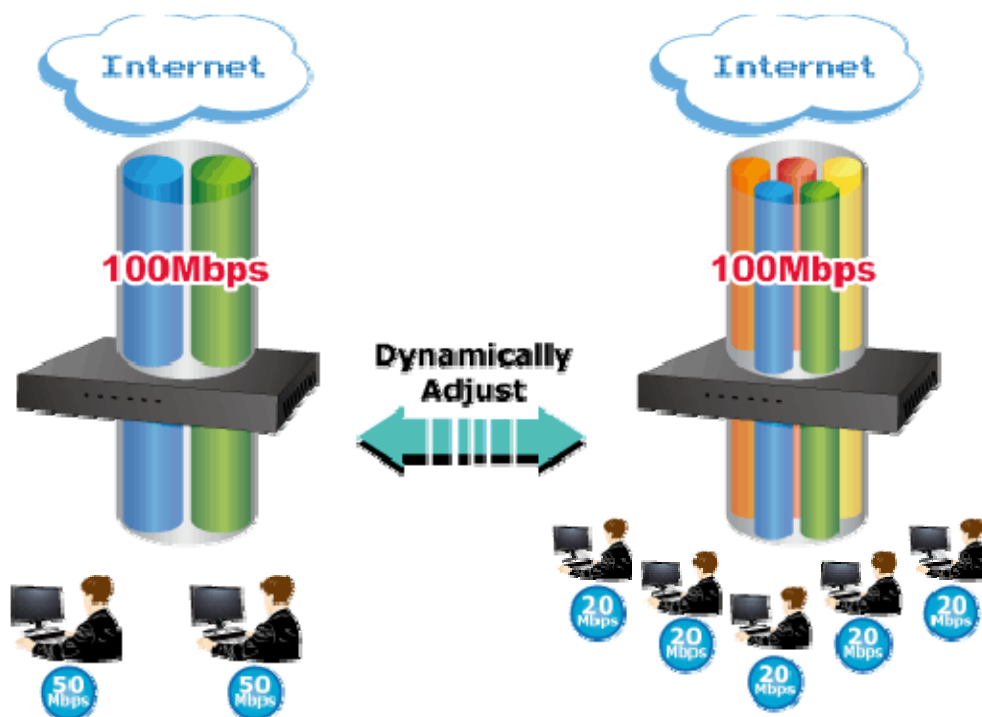
The CS-950 supports many popular security features including content blocking to block specific URL, authentication, IPSec, L2TP, SSL VPN, PPTP VPN server/client, outbound load-balancing, QoS, time schedule and more. Furthermore, it provides higher performance with all Gigabit Ethernet interfaces which offer faster speeds for your network applications. The Gigabit user-defined interfaces flexibly fulfill the network requirement nowadays, and the multiple WAN interfaces enable the CS-950 to support outbound load balancing and WAN fail-over features. The built-in multiple VPN tunnels (IPSec/PPTP/L2TP/SSL) enables businesses of any size to deliver secured connectivity for mobile employees, branch offices, and clients. As a result, the VPN functions not only provides high security level connection but also VPN fail-over features, a VPN redundant mechanism to always keep the VPN alive.



### Improving Network Efficiency

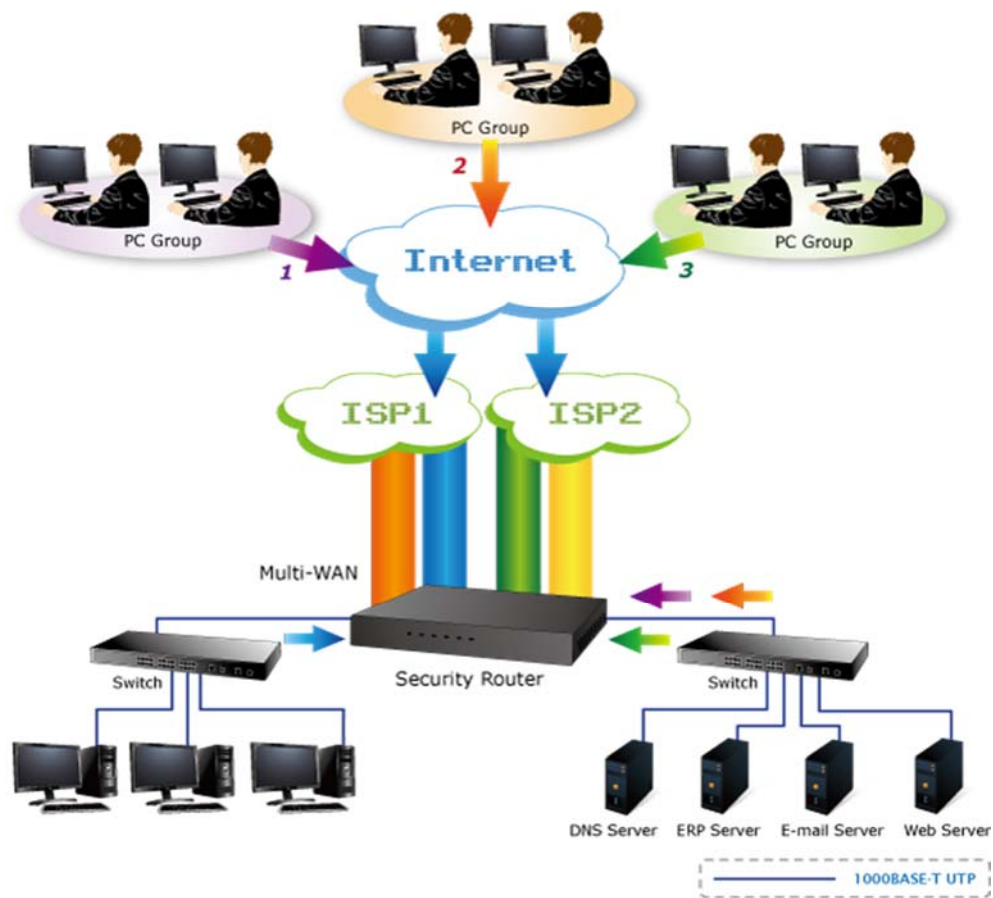
The CS-950 has link redundancy, application control and many more functions to make the entire network system better. It is applicable to the small-scale sector (from 40 to 50 people), using a 9-inch desktop design, with four Gigabit ports (WAN/LAN/DMZ). The CS-950's economical price with complete cable management features make it an inevitable choice for the next-generation office network load balancer.

The CS-950's built-in fully-qualified domain name (FQDN) feature can automatically resolve the IP address corresponding to all. Users' network can be easily managed by just typing the URL of the secure websites (HTTPS) like Facebook, YouTube and Yahoo.



The CS-950 can connect multiple WANs with up to three different ISPs. It creates a stable

and qualified VPN connection for many important applications such as VoIP, video conferencing and data transmission.



## 1.3 Features

### ➤ Physical Port

- 4 x 10/100/1000BASE-T RJ45
- 2 undefined Ethernet ports (WAN/LAN/DMZ)
- Multi-WAN function
- Outbound load balancing (Supported algorithms: Auto, Source IP, Destination IP or Manual)

### ➤ IP Routing Feature

- Static Route
- Dynamic Route (RIPv2)

### ➤ Firewall Security

- Stateful Packet Inspection (SPI) firewall
- Blocking DoS/DDOS attack
- Internal firewall
- IP address block
- Block website by URL, IP, Domain, FQDN
- Anti-ARP spoofing
- Application control

### ➤ Mail Security

- Antivirus base on auto-update antivirus engine
- Built-in multiple anti-spam algorithms, auto learning, and personal black/white list
- Mail log

### ➤ Advanced Security

- IDP (Intrusion Detection and Prevention)
- User Authentication
- Switch co-defense
- Anomalous IP traffic analysis

### ➤ VPN Features

- Max. Connection Tunnel Entries: 500 IPsec VPN tunnels, 200 PPTP VPN tunnels, 200 L2TP VPN tunnels or 50 SSL VPN tunnels
- Stateful packet inspection
- Encryption methods: DES, 3DES, AES, AES-128/192/256

- Authentication methods: MD5, SHA-1, SHA-256, SHA-512

### ➤ **Networking**

- Outbound load balance
- Failover for WAN
- PPPoE/Static IP/DHCP Client
- Protocols: TCP/IP, UDP, ARP, ICMP, FTP, IPv4, IPv6
- Virtual Server
- DDNS: DynDNS, 3322, No-IP, Planet DDNS & Planet Easy DDNS
- Transparent bridge/transparent routing

### ➤ **Others**

- Wireless AP Management
- CMS (Central Management System)
- HA (High Availability) mode
- Supported access by HTTP or HTTPS
- SNMP agent (SNMPv3-capable)
- Schedulable firmware upgrade through Web browser
- Comprehensive web-based management and policy setting
- Monitoring, logging, and alarms of system activities

## 1.4 Product Specifications

<b>Product</b>	UTM Content Security Gateway
<b>Model</b>	CS-950
<b>Hardware</b>	
<b>Ethernet</b>	4 10/100/1000BASE-T RJ45 Ethernet ports
<b>Console Port</b>	DB-9 console port (115200, 8, N, 1)
<b>USB Port</b>	2 USB 2.0 port for system configuration backup and recovery
<b>Reset Button</b>	Reset to factory default
<b>Thermal Fan</b>	1
<b>Software</b>	
<b>Management</b>	Web browser
<b>Operation Mode</b>	NAT, Transparent Bridging, Transparent Routing
<b>Routing Protocol</b>	Static Route, Dynamic Route (RIPv2)
<b>NAT Throughput</b>	Max. 1.8Gbps
<b>Max. Connections</b>	Max. 1.2 million
<b>Mail Scan/Day</b>	Max. 432000
<b>Firewall Security</b>	Stateful Packet Inspection (SPI) Internal firewall
<b>Multiple Subnet</b>	Supports max. 255 multiple subnets
<b>Outbound Load Balancing</b>	Supported algorithms: Auto, Source IP, Destination IP or Manual
<b>Protocol</b>	IPv4, IPv6, TCP, UDP, HTTP, HTTPS, SMTP, FTP, NTP, DNS, PLANET DDNS, PLANET Easy DDNS, DHCP, PPPoE, SNMP, QoS, IEEE 802.1q
<b>Content Filtering</b>	URL blocking IP blocking Domain blocking Black/White list
<b>Application Blocking</b>	P2P blocking (Bit Torrent, eDonkey, WinMX and more) IM blocking (WeChat, Yahoo Messenger, WhatsApp, QQ, Skype, Google Talk and more) Multimedia streaming (PPLive, PPStream, Tornado Broadcast and more) Web-based mail (Gmail, Yahoo, Hotmail and more) Online game (World of Warcraft, QQGame and more)

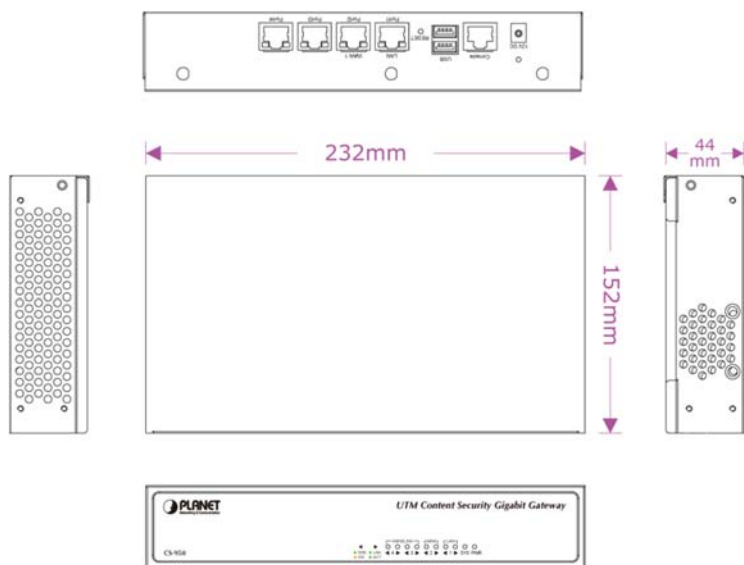


	<p>Remote controlling (TeamViewer, Remote Desktop and more)</p> <p>Web (YouTube, Facebook and more)</p> <p>VoIP (SIP, H.323 and more)</p>
<b>QoS</b>	<p>Smart QoS</p> <p>Guaranteed and maximum bandwidth configurable</p> <p>Priority levels</p> <p>Policy mode/Inside per source IP mode/Outside per source IP mode</p>
<b>User Authentication</b>	<p>Max. concurrent connections up to 256 entries</p> <p>Supports local database, RADIUS, POP3 and AD authentication</p>
<b>AP Management</b>	<p>Max. 50 APs</p>
<b>Logs</b>	<p>System Operation Log, Configuration Log, Network Log, Objects Log, Network Services Log, Advanced Protection Log, Mail Security Log, IDP Log and VPN Log</p>
<b>Reports</b>	<p>Show CPU/RAM system load, network flow and traffic ranking</p> <p>Mixed format reports: tabular and graphical</p> <p>Automated daily/weekly report</p> <p>Reports sent via email</p>
<b>Watch-Dog</b>	<p>Auto-reboot upon failure</p>
<b>Others</b>	<p>Outbound load balancing</p> <p>Failover for WAN</p> <p>CMS (Central Management System)</p> <p>HA (High Availability) mode</p> <p>FQDN</p> <p>Switch co-defense</p> <p>IDP (Intrusion Detection and Prevention)</p>
<b>Antivirus and Antispam</b>	
<b>Antivirus Engine</b>	<p>Clam AV</p>
<b>Antivirus Action</b>	<p>Modify the subject</p> <p>Record the suspicious mail information</p>
<b>Antispam Algorithms</b>	<p>Fingerprinting, bayesian filtering, auto learning, spam characteristics filtering and personal black/white list</p>
<b>Antispam Action</b>	<p>Modify the subject</p> <p>Delete the spam mail</p> <p>Record the suspicious mail information</p>
<b>VPN</b>	
<b>VPN Function</b>	<p>IPSec, PPTP server and client, L2TP, SSL</p>

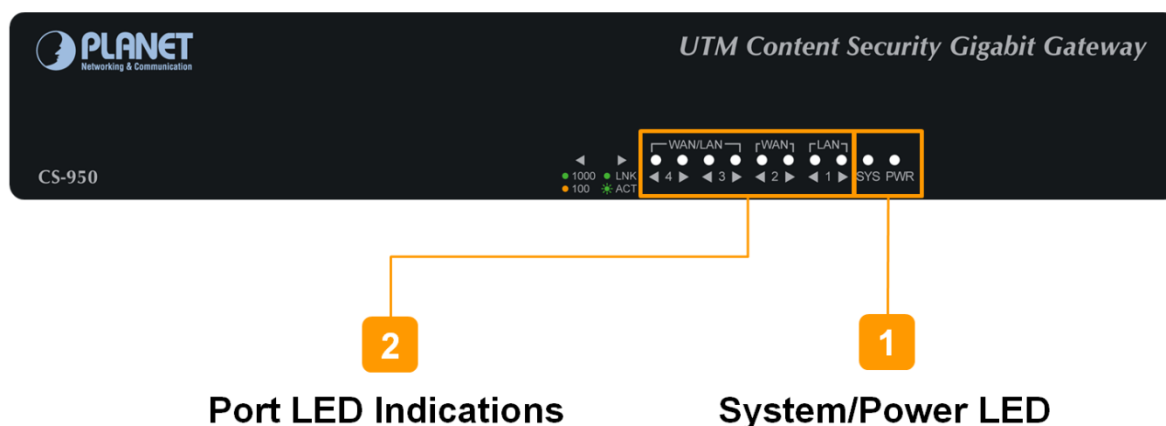
<b>IPSec VPN Tunnels</b>	Max. 500
<b>PPTP VPN Tunnels</b>	Max. 200
<b>L2TP VPN Tunnels</b>	Max. 200
<b>SSL VPN Tunnels</b>	Max. 50
<b>VPN Throughput</b>	Max. 90Mbps
<b>Encryption Methods</b>	DES, 3DES, AES or AES-128/192/256 encrypting
<b>Authentication Methods</b>	MD5/SHA-1/SHA-256/SHA-512 authentication algorithm
<b>General</b>	
<b>Power Requirements</b>	12V DC, 3.3A
<b>Power Consumption</b>	22W max.
<b>Weight</b>	0.96kg
<b>Dimensions (W x D x H)</b>	232 x 152 x 44 mm
<b>Regulatory Compliance</b>	CE, FCC
<b>Reliability</b>	MTBF > 63449hrs
<b>Standards Conformance</b>	
<b>Regulatory Compliance</b>	CE, FCC
<b>Environment Specifications</b>	
<b>Operating</b>	Temperature: 0 ~ 40 degrees C Relative Humidity: 5 ~ 95% (non-condensing)
<b>Storage</b>	Temperature: -20 ~ 75 degrees C Relative Humidity: 5 ~ 95% (non-condensing)
<b>Standard Accessories</b>	
<b>Packet Contents</b>	CS-950 x 1 Quick Installation Guide x 1 Adapter x 1 Power Cord x 1 Console Cable x 1 Ethernet Cable x 1 Screw Package x 1 Rack-mount Ear x 2 Feet Pads x 4

## 1.5 Hardware Interface

### 1.5.1 Diagrams:



### 1.5.2 LED:

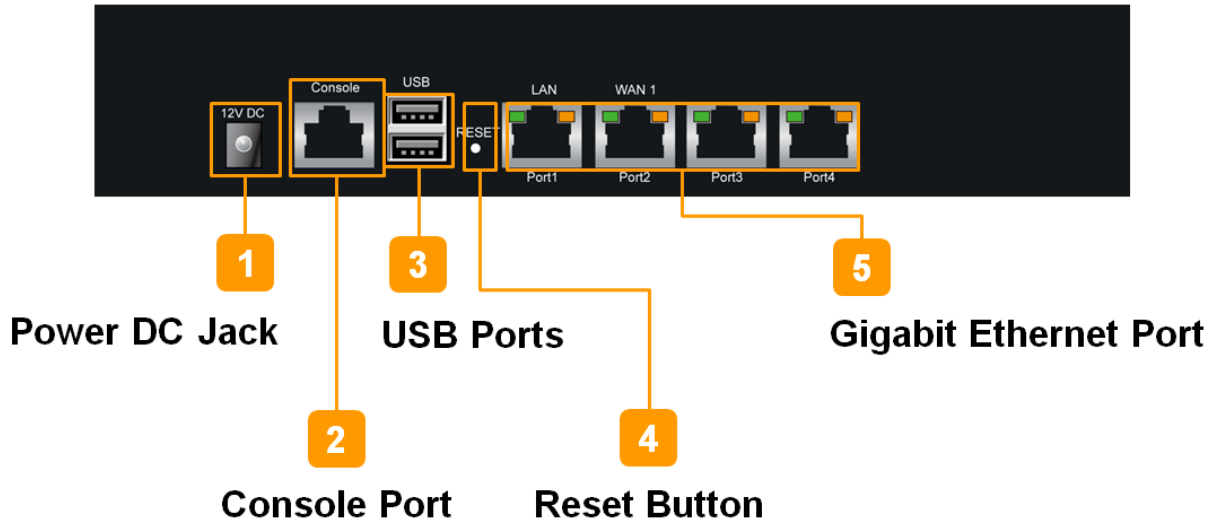


Port LED Indications

System/Power LED

LED		
PWR		Lights up when the power is on.
SYS		Blinks frequently when system is rebooting. When it starts to blink irregularly, the system boots successfully.
Port 1~4	LED1 (Right)	Green "Steady on" indicates the port is connected to other network device. "Blink" to indicate there is traffic on the port.
	LED2 (Left)	Green "Steady on" indicates the port is connected at 1000Mbps speed.
		Orange "Steady on" indicates the port is connected at 100Mbps speed.
	Off "Turn off" indicates the port is connected at 10Mbps speed.	

### 1.5.3 Interfaces:

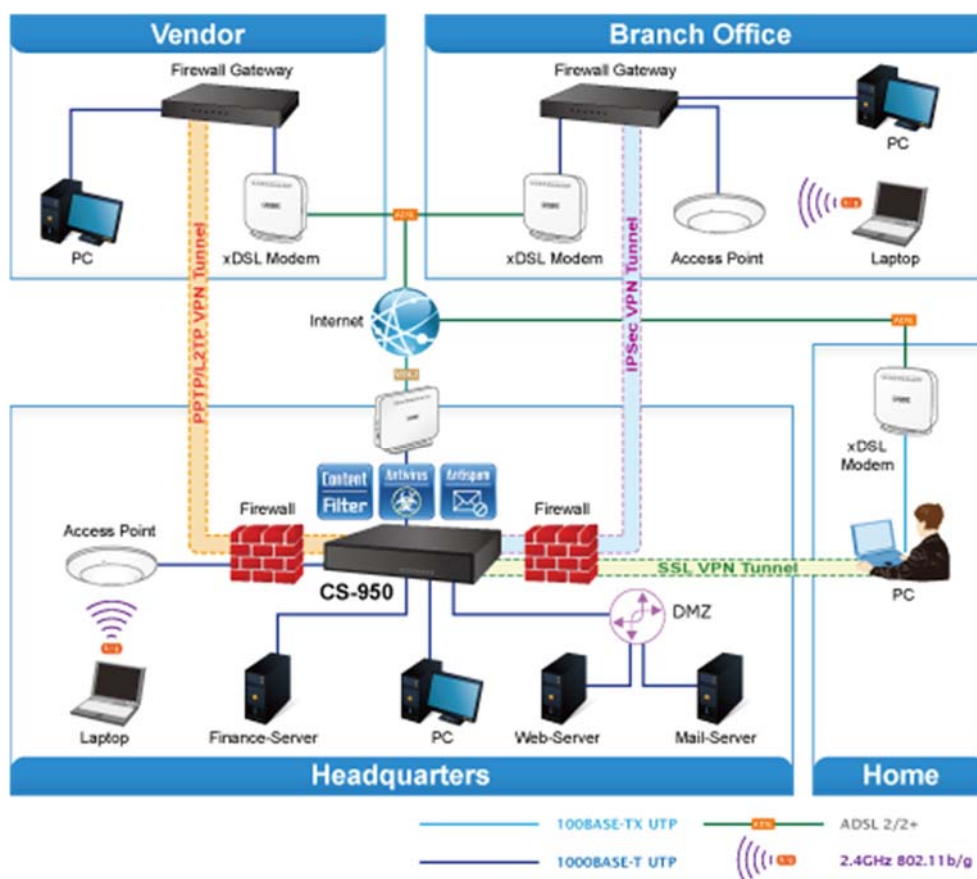


Ports		
DC in	12V, 3.3A DC power input.	
Console Port	A DB-9 console port (11520, 8, N, 1) to inspect internal network setting, or restore to its factory default.	
USB Port	USB 2.0 port for system configuration backup and recovery.	
Reset Button	Power on the device and press the reset button for five seconds to reboot it or twenty seconds to restore it to factory default settings.	
Port 1	It is a LAN port for connecting to a switch.	
Port 2	It is a WAN port for connecting to a perimeter router.	
Port 3	Default is off. It can be defined as LAN Port or WAN Port.	
Port 4	Default is off. It can be defined as WAN Port or DMZ Port. DMZ Port is for providing the public with services, such as email or Web, using a physically-separated network segment, while at the same time preventing any potential security threats.	
LED		
	D1 <b>Green</b>	Port is connected at 1Gbps.
	D1 <b>Orange</b>	Port is connected at 100Mbps.
	D1 Off	Port is connected at 10Mbps.
	D2 Flashing <b>Green</b>	Network Activity at the port.
	D2 <b>Green</b>	Correct cable is used and power is on.
	D2 Off	No link.

## 1.6 Topology

PLANET CS-950 UTM Content Security Gateway has an SPI firewall with DoS detection. Through the FQDN function, it can easily block secure websites like Facebook, YouTube, Gmail, etc. With IPSec/PPTP/L2TP/SSL VPN solutions, the CS-950 provides secured data communication for branches, vendors, and mobile workers with a flexible way to connect back to the headquarters.

The CS-950 connects multiple WANs with up to three different ISPs. It creates a stable and qualified VPN connection for many important applications such as VoIP, video conferencing and data transmission.

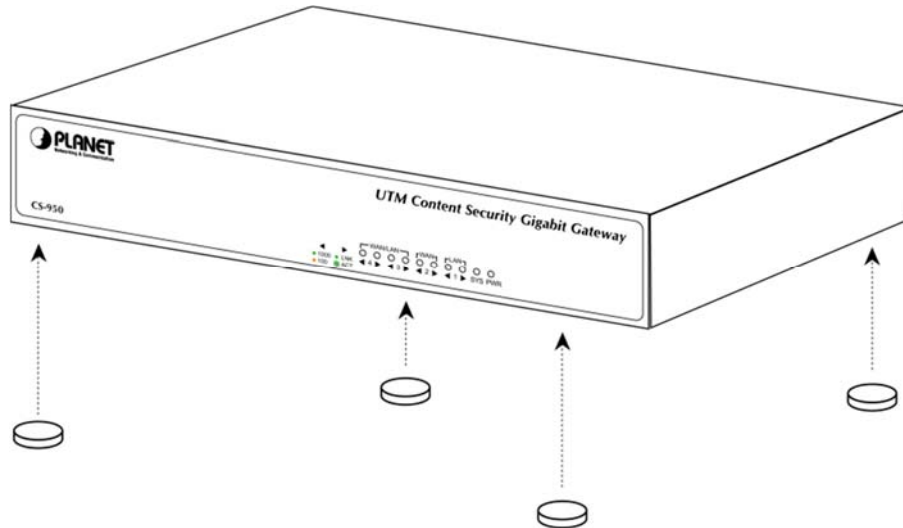


# Chapter 2. Hardware Installation

## 2.1 Desktop Installation

To install the CS-950 on desktop, simply follow the following steps:

**Step 1:** Attach the rubber feet to the bottom of the CS-950.



**Step 2:** Place the CS-950 on desktop.

**Step 3:** Keep enough ventilation space between the CS-950 and the surrounding objects.



When choosing a location, please keep in mind the environmental restrictions should be under the specifications of the CS-950.

**Step 4:** Connect your CS-950 to hub/switch.

- A. Connect one end of a standard network cable to the LAN port (port 1) on the rear panel of the CS-950.
- B. Connect the other end of the cable to the hub / switch.



The UTP Category 5, 5e, 6 network cabling with RJ45 tips is recommended.

**Step 5:** Connect your CS-950 to internet.

- A. Connect one end of a standard network cable to the WAN port (port 2) on the rear panel of the CS-950.
- B. Connect the other end of the cable to the ADSL router's LAN port or an upper layer port to outer network layer.



---

If there is only one line connected to the outer network in your network environment, it is suggested that you use WAN port (port 2).

---

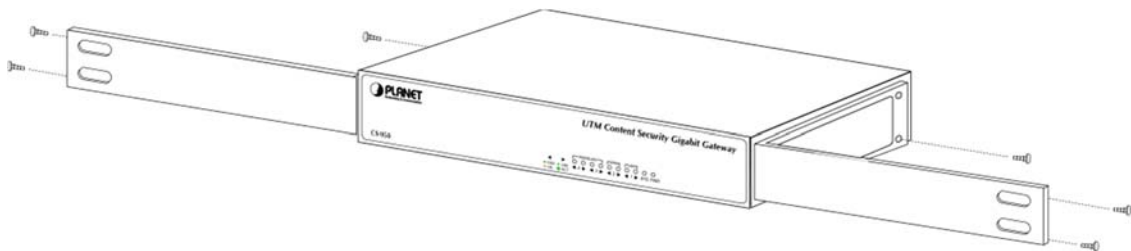
**Step 6:** Power on the CS-950 by the included 12V/3.3A DC adapter. When the CS-950 receives power, the Power LED should remain solid Green.

## 2.2 Rack Mounting

To install the CS-950 in a 19-inch standard rack, follow the instructions described below.

**Step 1:** Place your CS-950 on a hard flat surface, with the front panel positioned towards your front side.

**Step 2:** Attach a rack-mount bracket to each side of the CS-950 with supplied screws attached to the package. In the picture below, it shows how to attach brackets to one side of the CS-950.



---

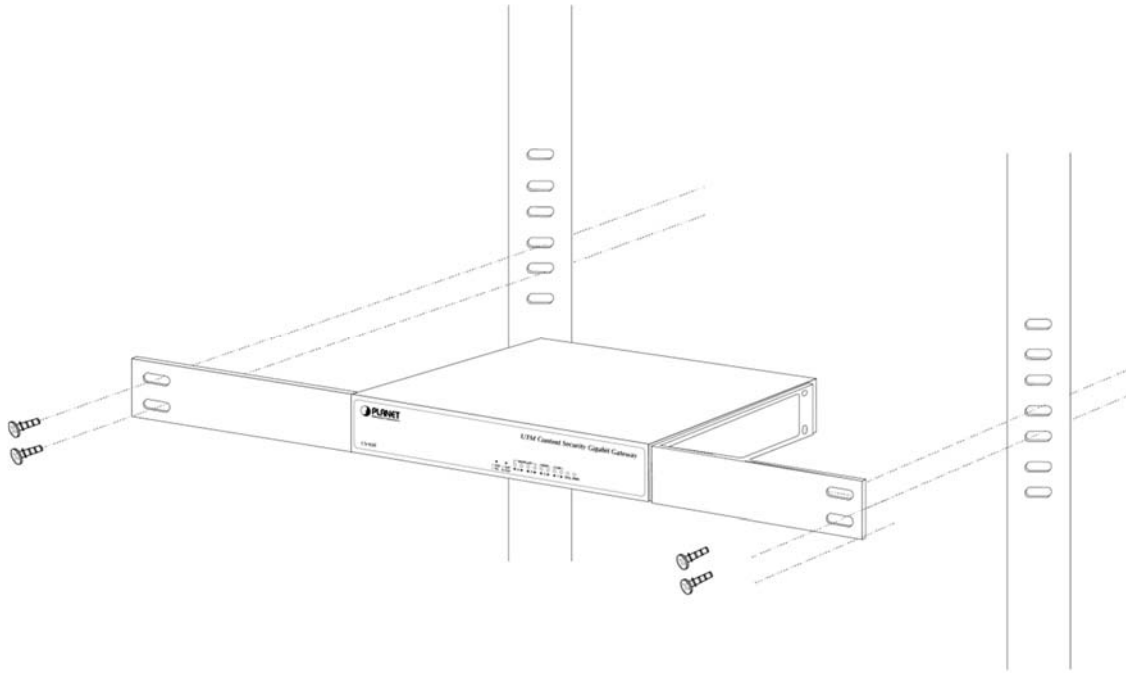
You must use the screws supplied with the mounting brackets. Damage caused to the parts by using incorrect screws would invalidate the warranty.

---

**Step 3:** Secure the brackets tightly.

**Step 4:** Follow the same steps to attach the second bracket to the opposite side.

**Step 5:** After the brackets are attached to the CS-950, use suitable screws to securely attach the brackets to the rack, as shown in the picture below.



The width of the rack should be at least 453 mm.

**Step 6:** Proceed with Steps 4, 5 and 6 of session 2.2.1 Desktop Installation to connect the network cabling and power on the CS-950.



# Chapter 3. Preparation

Before getting into the unit's web UI, user has to check the network setting and configure PC's IP address.

## 3.1 Requirements

User is able to confirm the following items before configuration:

1. Please confirm the network is working properly; it is strongly suggested to test your network connection by connecting your computer directly to ISP.
2. Suggested operating systems: Windows 7 / 8 / 10.
3. Recommended web browsers: IE / Firefox / Chrome.

## 3.2 Setting TCP/IP on your PC

The default IP address of the CS-950 is 192.168.1.1, and the DHCP Server is on.

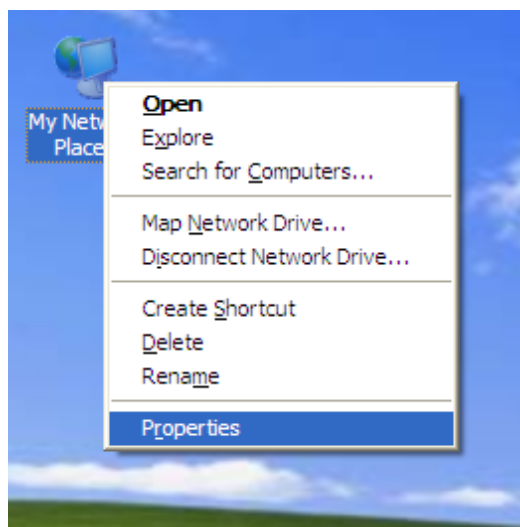
Please set the IP address of the connected PC as DHCP client, and the PC will get IP address automatically from the CS-950.

Please refer to the following to set the IP address of the connected PC.

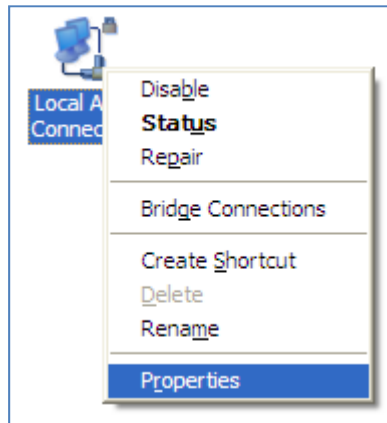
### 3.2.1 Windows XP

If you are using Windows XP, please refer to the steps below:

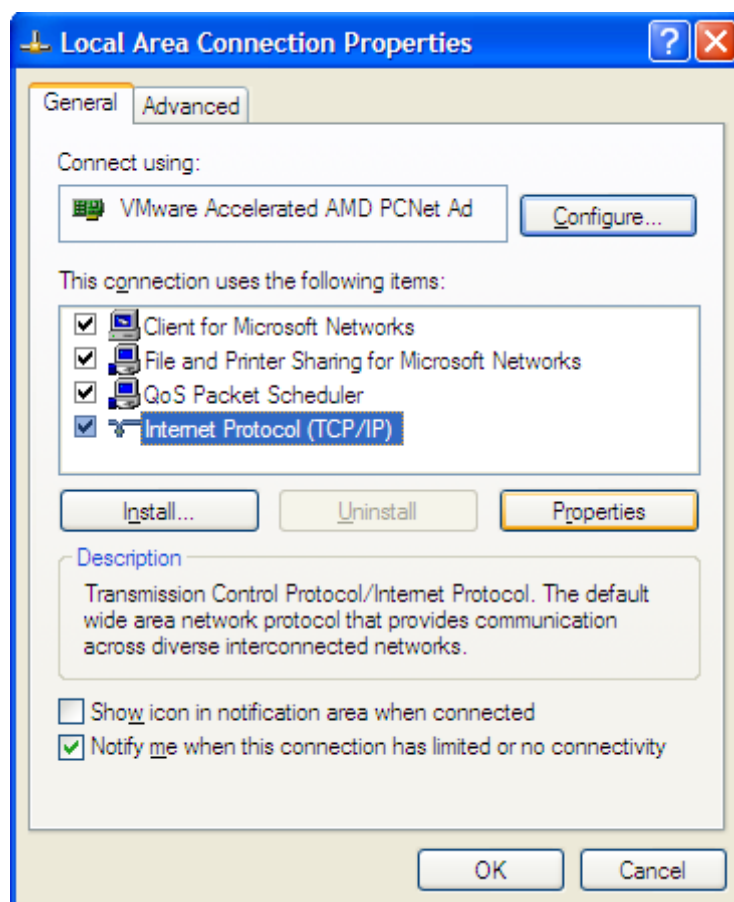
1. From the desktop, right-click My Network Places > Properties.



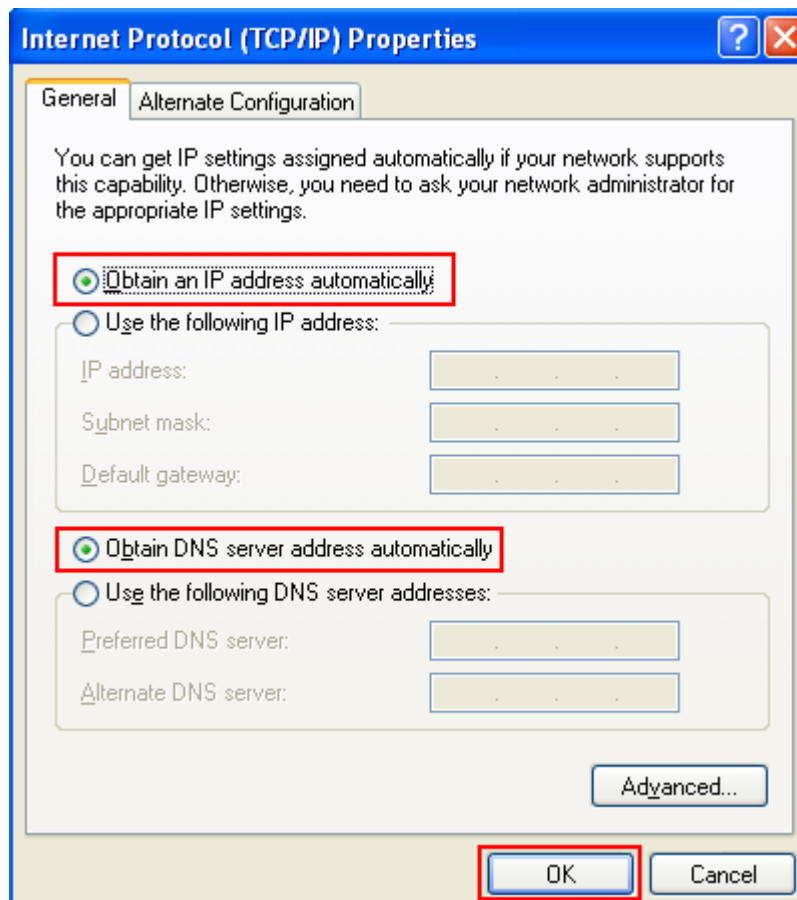
2. Right-click on the Local Area Connection and select Properties.



3. Select Internet Protocol (TCP/IP) and click Properties.



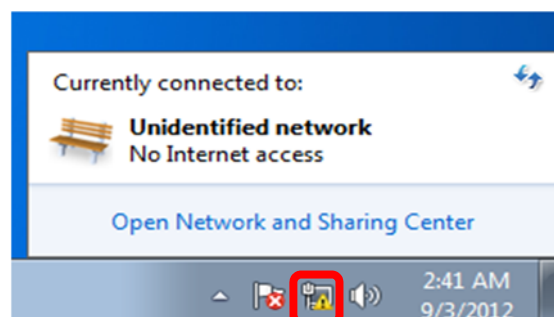
4. Select "Obtain an IP address automatically" and "Obtain DNS server address automatically", and then click the "OK" button.



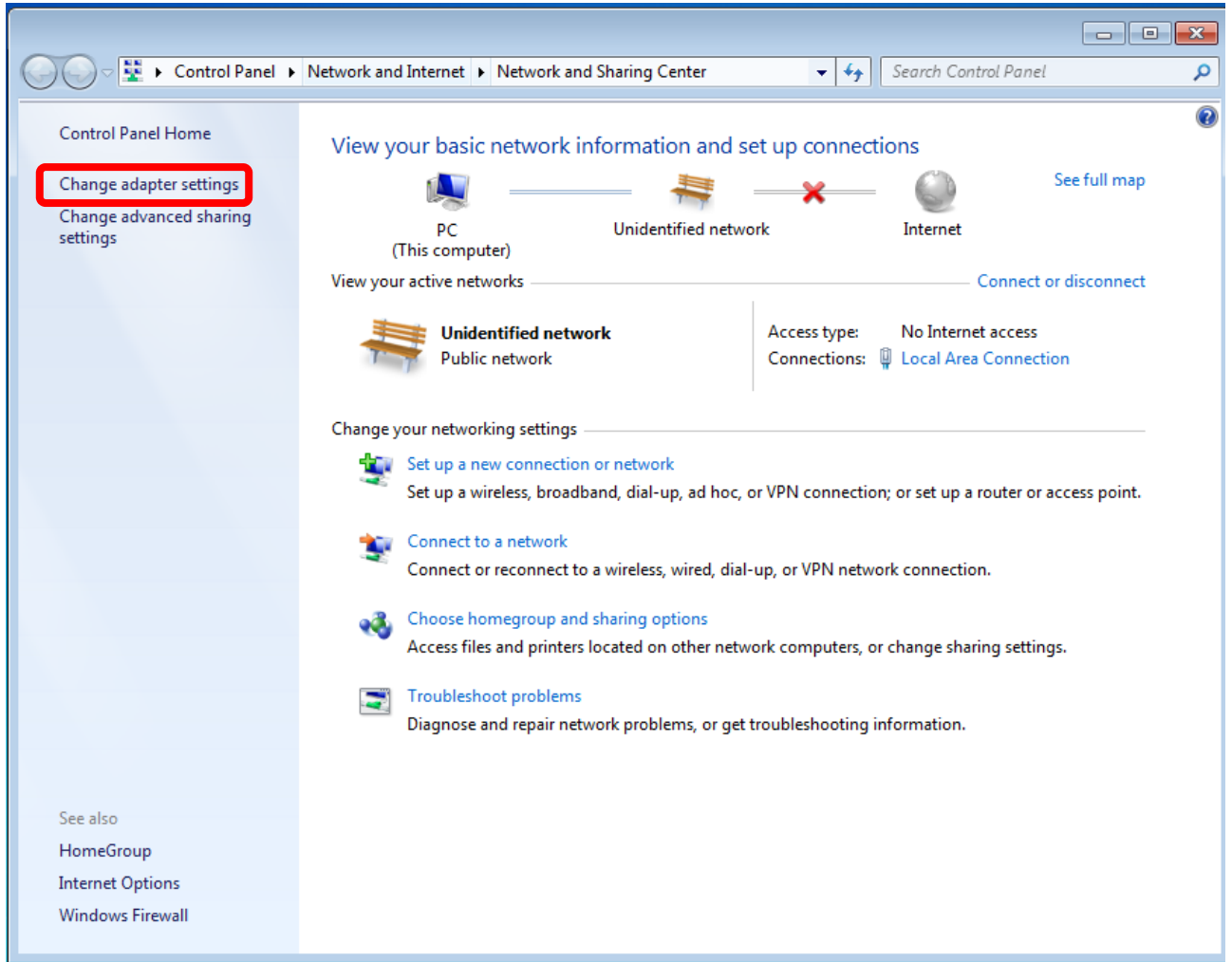
### 3.2.2 Windows 7

If you are using Windows 7, please refer to the following:

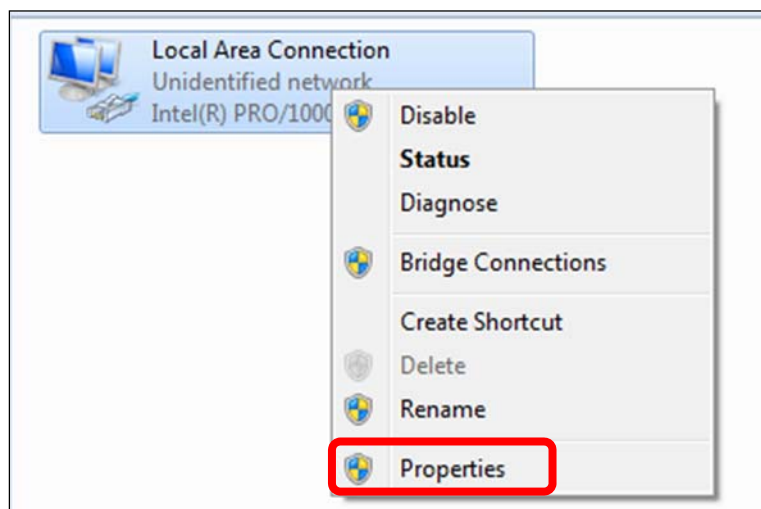
1. Click on the network icon from the right side of the taskbar and then click on "Open Network and Sharing Center".



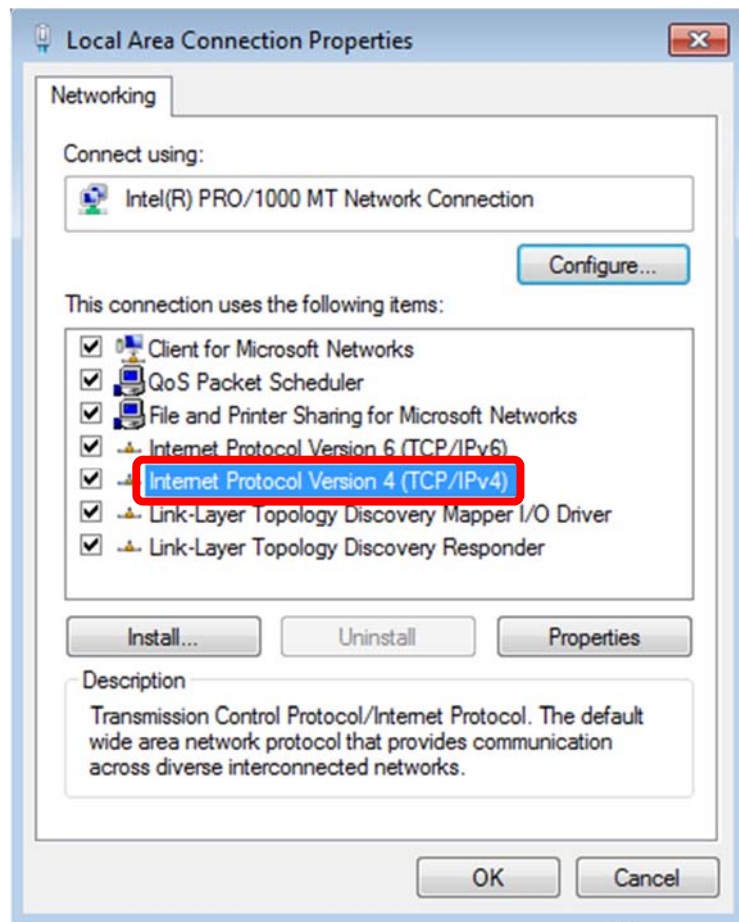
2. Click "Change adapter settings".



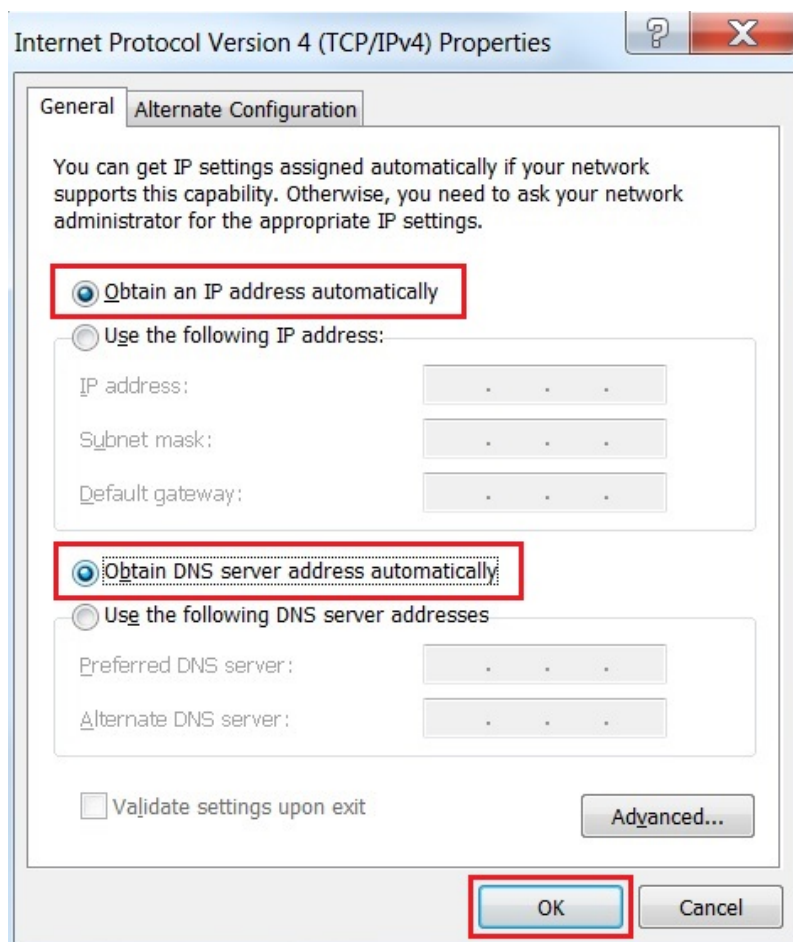
3. Right-click on the Local Area Connection and select Properties.



4. Select Internet Protocol Version 4 (TCP/IPv4) and click Properties or directly double-click on Internet Protocol Version 4 (TCP/IPv4).



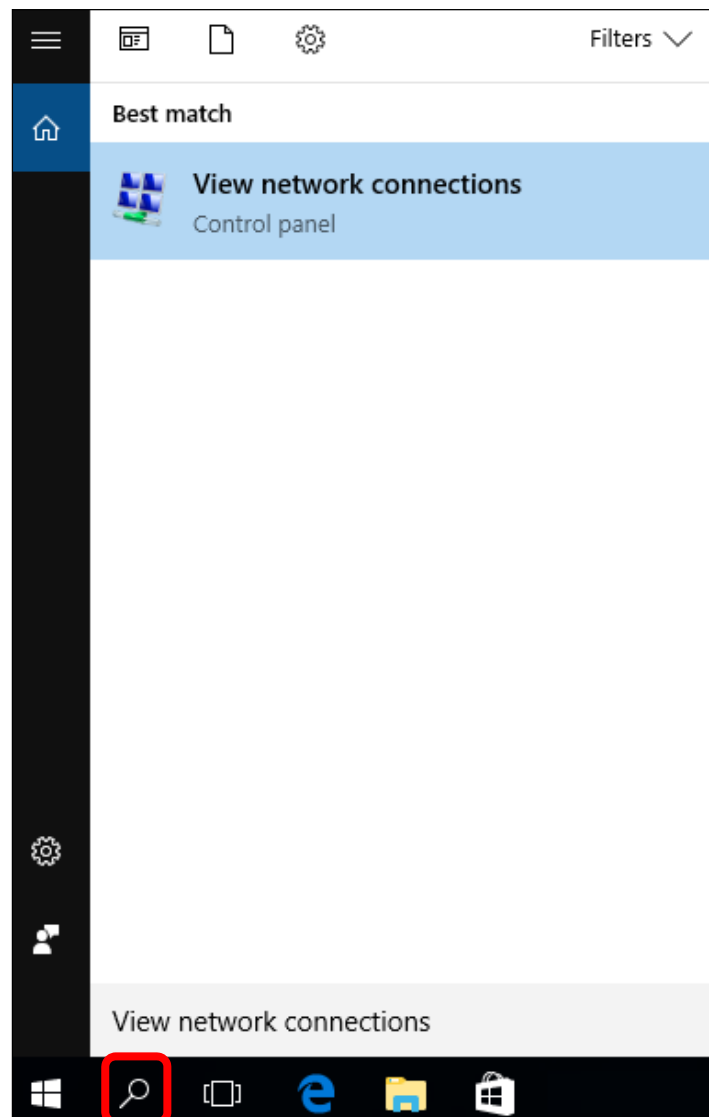
5. Select "Use the following IP address" and "Obtain DNS server address automatically", and then click the "OK" button.



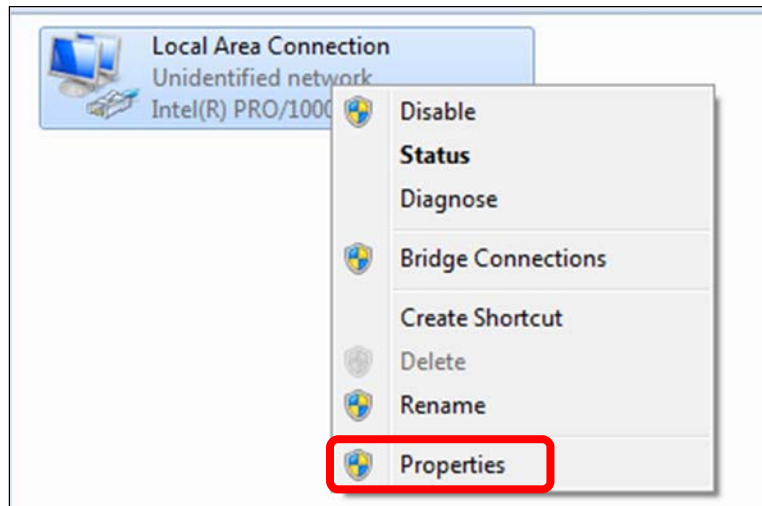
### 3.2.3 Windows 10

If you are using Windows 10, please refer to the following:

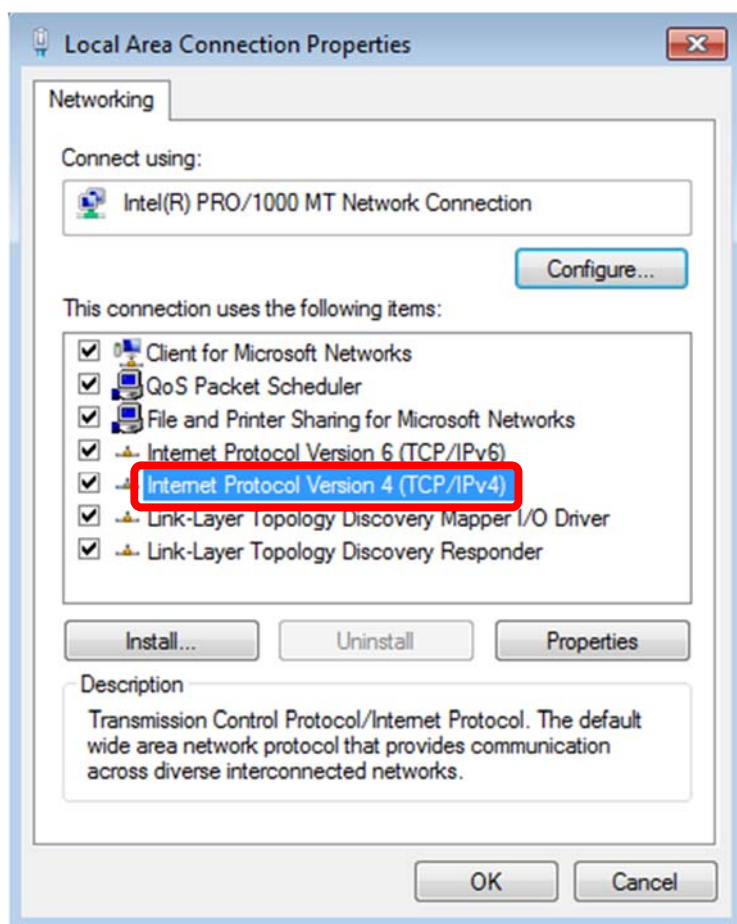
1. In the search box on the taskbar, type “View network connections”, and then select View network connections at the top of the list.



2. Right-click on the Local Area Connection and select Properties.

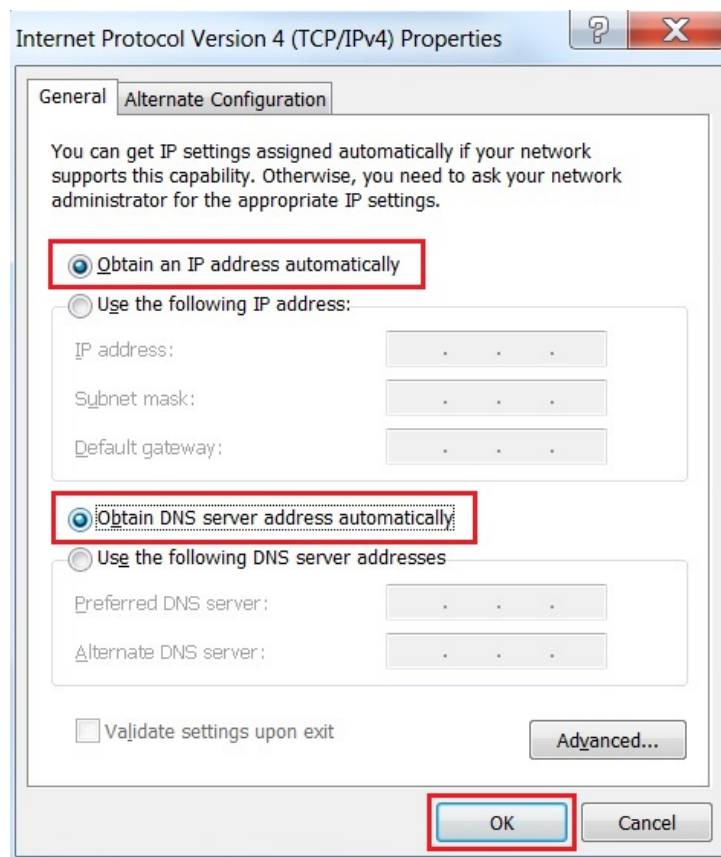


3. Select Internet Protocol Version 4 (TCP/IPv4) and click Properties or directly double-click on Internet Protocol Version 4 (TCP/IPv4).





4. Select "Use the following IP address" and "Obtain DNS server address automatically", and then click the "OK" button.

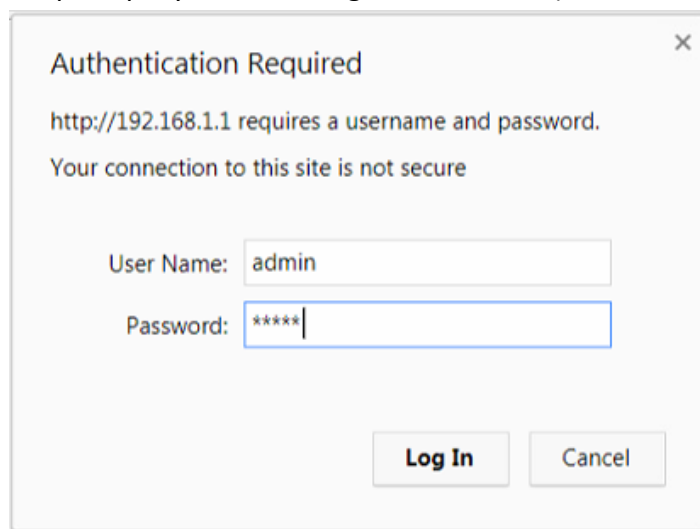


# Chapter 4. Login

## 4.1 Logging in to the Security Gateway

Refer to the steps to configure the CS-950:

- Step 1.** Connect the IT administrator’s PC and CS-950’s LAN port (port 1) to the same hub / switch, and then launch a browser to link the management interface address which is set to **http://192.168.1.1** by default. Therefore, the IP addresses of LAN PC 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.
- Step 2.** The browser prompts you for the login credentials. (Both are “**admin**” by default.)



Default IP Address: 192.168.1.1

Default User Name: **admin**

Default Password: **admin**



Administrators are strongly suggested to change the default admin and password to ensure system security. Please follow these steps: **Configuration > Administration > Administrator > Account and Privilege**. And then click on “**Save**” to complete setting.

## 4.2 Homepage

User is able to check the system information on this page. It shows System Time, firmware version, Server Service and Interfaces status. In addition, it displays the CPU, RAM, and Flash

simultaneously.

PLANET Networking & Communication

CS-950 UTM Content Security Gateway

Home Logout

admin 192.168.1.69 On Line : 1

Language English 5 second Refresh

**System Time**

Server Date / Time	2017-11-11	11:11:38
Current Timezone	Asia/Taipei	
Server Uptime	6 days,14 hours,32 minutes	

**System Resource**

System Loading	0.00 0.05 0.10
CPU Loading	0.5%
RAM ( 2 GB )	33%
Flash ( 195 MB)	16%
Online members	1
Total Session (Outgoing / Incoming)	67 / 0

**Server Info**

Server Model	CS-950
Server Version	2.2.1.1
Serial No.	

**Server Service**

DHCP Service	✘
DDNS Service	✘
Anti-virus Engine	✔
Web/FTP Anti-virus Service	✘
Mail Anti-virus Service	✔
Anti-Spam Service	✔
IPSec VPN Service	✘
HA	✘

**Interfaces » More**

Port	Port 1	Port 2	Port 3	Port 4
Interface Type	LAN	WAN1	WAN2	DMZ
Interface	eth0	eth1	eth2	eth3
Connect Status	✔	✘	✘	✘
Line Status	📶	📶	📶	📶
IP Address	192.168.1.1	OFF	OFF	OFF
Load Balance Ratio	--	0.00%	0.00%	--
Total Packets	Tx	102,721	0	0
	Rx	7,237,329	0	0
Total Flow (byte)	Tx	5.79M	0	0
	Rx	447.86M	0	0

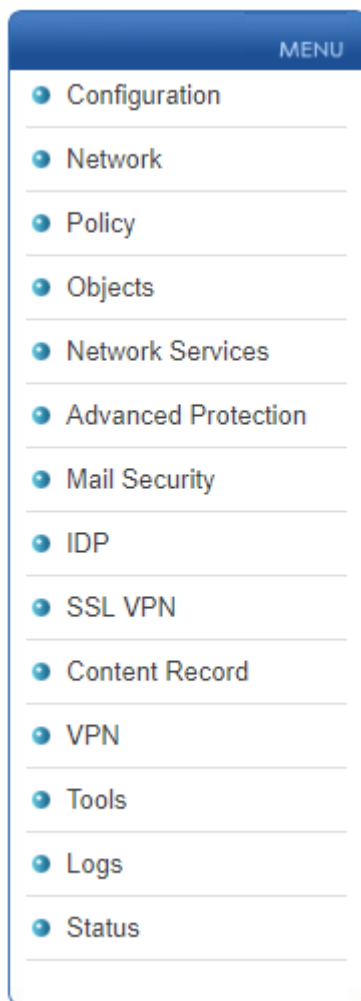
PLANET Networking & Communication

Copyright © PLANET Technology Corporation. All rights reserved.

## 4.2.1 MENU

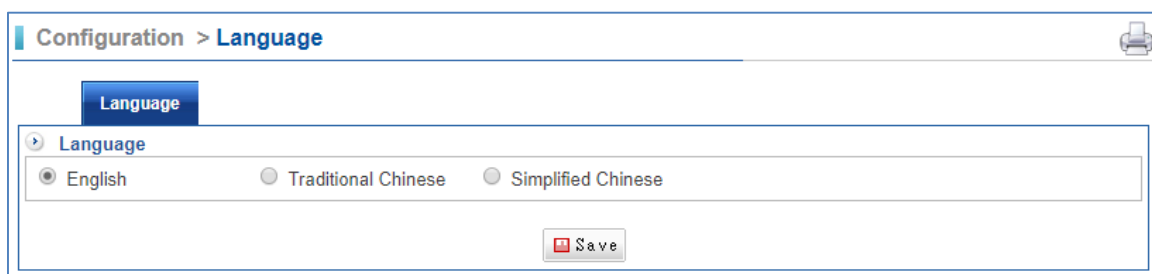
On the left side of the screen, check out the MENU, and you can see the function list. Click

on it to go to the configuration page.



## 4.2.2 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 the “Save” button.



## 4.2.3 Administrator Login

The administrator login name, IP address and the meantime show how many people are logged in, and also what your preferred duration is for renewing automatically the home page news. The durations that the system can automatically renew itself include every three

seconds, five seconds, 10 seconds, 20 seconds and 30 seconds.

Language

English
▼

5 second
▼

Refresh

## 4.2.4 Interface

The information of all Ethernet ports is shown here.

Interfaces » More				
Port	Port 1	Port 2	Port 3	Port 4
Interface Type	LAN	WAN1	WAN2	DMZ
Interface	eth0	eth1	eth2	eth3
Connect Status				
Line Status				
IP Address	192.168.1.1	OFF	OFF	OFF
Load Balance Ratio	--	0.00%	0.00%	--
Total Packets	Tx	102,721	0	0
	Rx	7,237,329	0	0
Total Flow (byte)	Tx	5.79M	0	0
	Rx	447.86M	0	0

Function	Description
<b>Interface Type</b>	LAN / WAN / DMZ.
<b>Interface</b>	From eth0 to eth3.
<b>Connect Status</b>	1. : The network connection is OK. 2. : The network connection failed.
<b>Line Status</b>	1. : The Ethernet cable is connecting. 2. : The Ethernet cable is not connecting.
<b>IP Address</b>	System binding IP address.
<b>Total Packets</b>	Each network interface transmission receives wrapped packets quantity. (bytes)
<b>Total Flow</b>	Each network interface transmission receives current capacity. (bytes)

# Chapter 5. Configuration

## 5.1 Date & Time

Select Configuration > Date & Time > Setting.

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 can be synchronized with time server hosts on the internet by using the network time protocol (NTP). 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 the CS-950 to access the internet. You can add a host in the User Defined Time Server field.

The screenshot shows a web interface for configuring the system's date and time. The breadcrumb trail is 'Configuration > Date & Time'. A 'Setting' tab is active. The 'Timezone and Time' section contains three rows of settings: 'Time Zone' is a dropdown menu set to 'Asia/Taipei'; 'Time' consists of three dropdown menus for hours (17), minutes (08), and seconds (48); 'Date' consists of three dropdown menus for year (2017), month (November), and day (23). The 'Sync with NTP Server' section has a checked checkbox labeled 'Enabled'. Below it, the 'Time Server' is 'time.stdtime.gov.tw' with 'Time Log' and 'Refresh' buttons. There are two radio buttons: 'Select Time Server' (selected) with a dropdown menu showing 'Taipei', and 'Define Time Server' with a text input field containing 'time.stdtime.gov.tw'. A 'Save' button is at the bottom right.

There are two parts you can use, “Timezone and Time” and “Sync with NTP Server”.

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 the “Save” button.

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

- Select Enabled in Sync with NTP Server.
- Time Zone: Select your country time zone.
- Click “Refresh”. Click on “Time Log” to check time log information, and it keeps within three days log information.

- Click on the "Save" button.

Method 3: This might be necessary if you are running a setup that does not allow the CS-950 to access the internet.

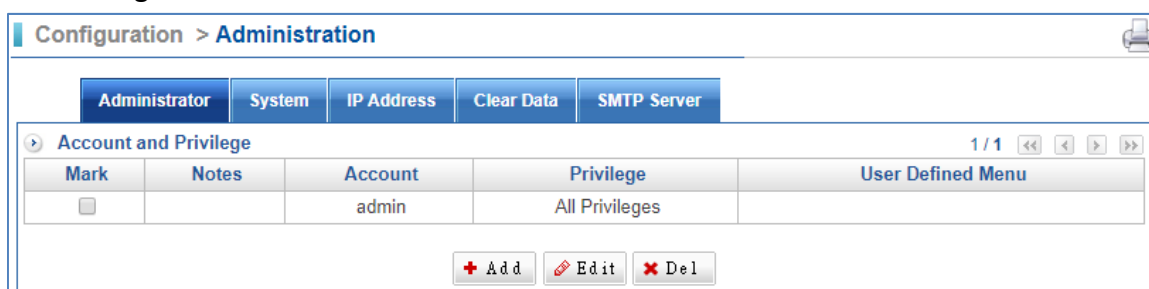
- Select Enabled in Sync with NTP Server.
- Define Time Server: Enter a time server manually.
- Click "Refresh". Click on "Time Log" to check time log information, and it keeps within three days log information.
- Click on the "Save" button.

## 5.2 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.

### 5.2.1 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) that are set "Read," it is "read-only" for that account that is not able to change any setting of the machine.

Configuration > Administration

Administrator System IP Address Clear Data SMTP Server

➤ Add New Administrator

Account

Password  ( Please input 3 to 32 characters, not the same with account )

Password Strength    ?

Confirm Password

Notes

Privilege

User Defined Menu

Function	Description
<b>Account</b>	Enter account name.
<b>Password</b>	The password for authentication.
<b>Password Strength</b>	If you want to make your password more secure, the following recommendations can be taken for more strength: <ol style="list-style-type: none"> <li>1. Use letters and digit.</li> <li>2. Use special characters, except “,” and “:”.</li> <li>3. Use capital and lowercase letters.</li> </ol>
<b>Confirm Password</b>	The confirmation of password
<b>Notes</b>	Easy to know who it is.
<b>Privilege</b>	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.
<b>User-defined Menu</b>	Administrator could customize MENU by selecting.

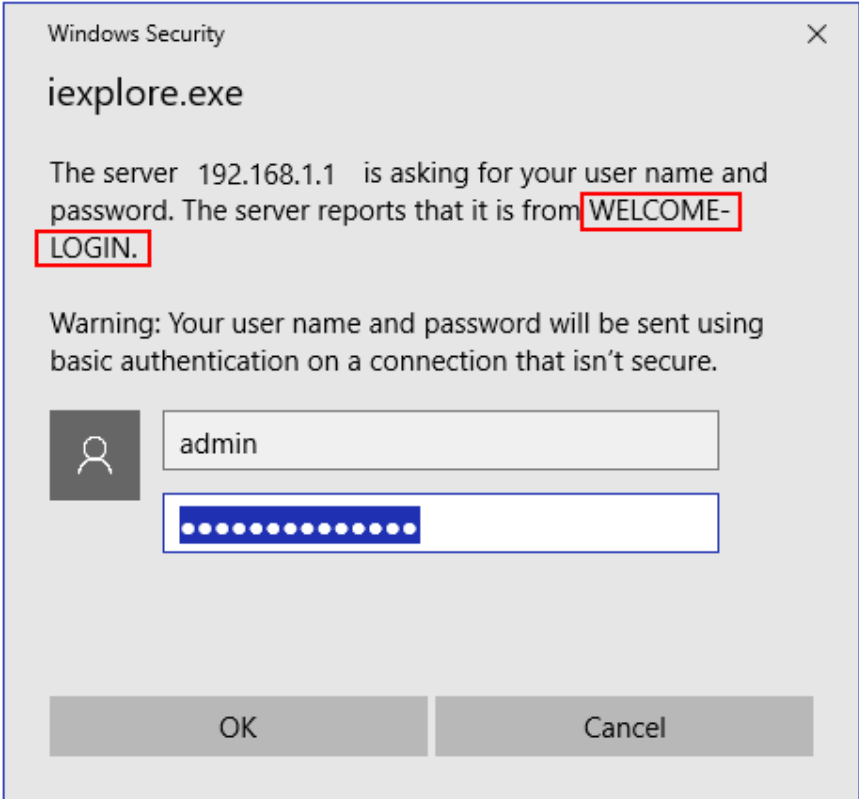

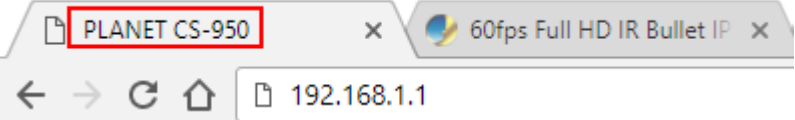



User Defined Menu <span style="float: right;"><input type="checkbox"/> Sel</span>	
Configuration	<input type="checkbox"/> Date & Time <input type="checkbox"/> Administration <input type="checkbox"/> System <input type="checkbox"/> Language <input type="checkbox"/> Notific <input type="checkbox"/> Report <input type="checkbox"/> Backup & Mount <input type="checkbox"/> Signature Update <input type="checkbox"/> CMS <input type="checkbox"/> AP Me <input type="checkbox"/> SSL Certificate <input type="checkbox"/> Data Items
Network	<input type="checkbox"/> Interface <input type="checkbox"/> Interface (IPv6) <input type="checkbox"/> Routing <input type="checkbox"/> 802.1Q
Policy	<input type="checkbox"/> LAN Policy <input type="checkbox"/> DMZ Policy <input type="checkbox"/> WAN Policy
Objects	<input type="checkbox"/> Address Table <input type="checkbox"/> Services Table <input type="checkbox"/> Schedule <input type="checkbox"/> QoS <input type="checkbox"/> Applic Control <input type="checkbox"/> URL Filter <input type="checkbox"/> Virtual Server <input type="checkbox"/> Firewall Protection <input type="checkbox"/> Authentication <input type="checkbox"/> Bulleti <input type="checkbox"/> WAN Group <input type="checkbox"/> RADIUS
Network Services	<input type="checkbox"/> DHCP <input type="checkbox"/> DDNS <input type="checkbox"/> DNS Proxy <input type="checkbox"/> WEB Service <input type="checkbox"/> FTP S <input type="checkbox"/> Anti-Virus Engine <input type="checkbox"/> High Availability <input type="checkbox"/> SNMP <input type="checkbox"/> Remote Syslog Server
Advanced Protection	<input type="checkbox"/> Anomaly IP Analysis <input type="checkbox"/> Switch <input type="checkbox"/> Intranet protect
Mail Security	<input type="checkbox"/> Filter & Log <input type="checkbox"/> Anti-Virus <input type="checkbox"/> Anti-Spam <input type="checkbox"/> Mail Log <input type="checkbox"/> SMTP
IDP	<input type="checkbox"/> IDP Setting <input type="checkbox"/> IDP Log
SSL VPN	<input type="checkbox"/> SSL VPN Setting <input type="checkbox"/> SSL VPN Log <input type="checkbox"/> VPN Policy
Content Record	<input type="checkbox"/> WEB Virus Record <input type="checkbox"/> FTP Virus Record
VPN	<input type="checkbox"/> IPSec Tunnel <input type="checkbox"/> PPTP Server <input type="checkbox"/> PPTP Client <input type="checkbox"/> L2TP <input type="checkbox"/> VPN F
Tools	<input type="checkbox"/> Connection Test
Logs	<input type="checkbox"/> System Operation <input type="checkbox"/> System Logs
Status	<input type="checkbox"/> Performance <input type="checkbox"/> Connection Status <input type="checkbox"/> Flow Analysis

## 5.2.2 System

Select Configuration > Administration > System.

Administrator	System	IP Address	Clear Data	SMTP Server
<p>General Setting</p> <p>Login Message: <input type="text" value="WELCOME- LOGIN"/></p> <p>Homepage Message: <input type="text"/></p> <p>Browser Message: <input type="text" value="PLANET CS-950"/></p> <p>Upload Logo: <input type="button" value="Choose File"/> No file chosen  <small>( Image size limit: 150 x 90 pixel ; optimal image size: 150 x 90 pixel GIF )</small></p> <p>Memory Release: Every <input type="text" value="30"/> minutes check memory usage more than <input type="text" value="90"/> %, release memory</p> <p>Pass-through Protocol: <input checked="" type="checkbox"/> H-323    <input checked="" type="checkbox"/> SIP</p> <p>Session timeout of established: <input type="text" value="600"/> Sec(600 ~ 86400)</p> <p>WatchDog Timer: <input checked="" type="checkbox"/> ( When the system is crashed, watchdog will immediately restart the system. )</p> <p>Outbound load balance of t-bridging: <input checked="" type="checkbox"/> ( Transparent LAN / DMZ WAN connection to the Internet via other WAN by NAT )</p>				
<p>Login Failure Block Settings</p> <p>Temporarily block when login failed more than: <input type="text" value="0"/> ( 0 means no limit)</p> <p>IP blocking period: <input type="text" value="0"/> minute(s) ( 0 means permanent blocking)</p> <p>Unblocked IP: No blocked IP</p> <p style="text-align: center;"><input type="button" value="Save"/></p>				
<p>Reset/Reboot Setting</p> <p>Reset to Default Setting: <input type="button" value="Reset to Default Setting"/> <input type="checkbox"/> Keep LAN,WAN and DMZ Setting</p> <p>Reboot System: <input type="button" value="Reboot System"/></p> <p>Poweroff System: <input type="button" value="Poweroff System"/></p>				

Function	Description
<b>Login Message</b>	<p>The message will be shown when user login is done.</p> 
<b>Homepage Message</b>	<p>The message will be showed next to the logo picture.</p> 
<b>Browser Message</b>	<p>The message will be shown on the top of browser.</p> 
<b>Upload Logo</b>	<p>Upload a resolution of 150x90 gif figure file. The image will automatically appear in the upper left corner of the screen.</p> 
<b>Memory Release</b>	<p>Memory is checked whenever memory usage reaches the one you set. System will release memory if the used memory is high. (Please see memory status in Homepage Information.)</p>
<b>Pass-through</b>	<p>System supports H-323 and SIP.</p>

Function	Description
<b>Protocol</b>	Please set it as enable when the VOIP phone does not work with CS-950.
<b>Session timeout of established</b>	Default value is 600 seconds.
<b>Watchdog Timer</b>	Enable it, watchdog will immediately restart the system when the system is crashed.
<b>Outbound load balance of t-bridging</b>	Transparent LAN / DMZ WAN connection to the Internet via other WAN by NAT.
<b>Temporarily block when login failed</b>	Default is 0 times. 0 means no limit.
<b>IP blocking period</b>	Default is 0 minute. 0 means permanent blocking.
<b>Reset to Default Setting</b>	If you want to keep LAN, WAN and DMZ IP settings, please select what you want. If you do not select, it will simply reset to the default setting.
<b>Reboot System</b>	Click on the "Reboot System" button to reboot system.
<b>Poweroff System</b>	Click on the "Poweroff System" button to power off system by software.

### 5.2.3 IP Address

Select Configuration > Administration > IP Address.

The screenshot shows the 'IP Address' configuration page. At the top, there are tabs for 'Administrator', 'System', 'IP Address', 'Clear Data', and 'SMTP Server'. Below the tabs, there is a breadcrumb trail: 'Administrator Management > Interface'. The main content area contains a table with the following data:

Interface	Ping	HTTP	HTTPS
LAN	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
WAN_1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
WAN_2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
WAN_3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
DMZ	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>


Below the table, there is an 'IP Address' section with an 'Action:' dropdown menu set to 'Allow all of the following' and a 'Change' button. To the right of this section, there is a '1 / 0' indicator and navigation arrows. At the bottom, there are buttons for '+ Add', 'Edit', and 'Del'.

Function	Description
<b>Ping</b>	Check it and then the IP address from the interface can ping this device.
<b>HTTP</b>	Check it and then the IP address from interface can visit this device via HTTP.
<b>HTTPS</b>	Check it and then the IP address from interface can visit this device via HTTPS.



User can't connect to the CS-950's web management from internet if all HTTP and HTTPS of WAN ports are disabled.

User is able to create a new management IP and Netmask. In order to effectively manage IP address, the IT administrator must cancel the ping, HTTP and HTTPS selections in WAN 1 Setup. Then, the management WAN interface will be inaccessible. Moreover, all systems are granted access with the correct password if no administrative IP addresses or networks are specified.

**Configuration > Administration** 

Administrator System **IP Address** Clear Data SMTP Server

**Add Manager IP Address and Netmask**

Action Allow

Notes

IP and Netmask  255.255.255.0 (/24) ▼

Administrator Management  Ping  Management Interface

Function	Description
<b>Note</b>	Input the name for recognition.
<b>IP and Netmask</b>	Input the IP and Netmask.
<b>Ping</b>	Check it and then the IP address can ping this device.
<b>Management Interface</b>	Check it and then the IP address can log in to this device.

## 5.2.4 Clear Data

Select Configuration > Administration > Clear Data.

Administrator
System
IP Address
Clear Data
SMTP Server

**Clear Data**

Select All

Configuration  Time Update Log  Data Storing Time Log  Notify Log  Report log

Network  WAN Alive Detection and PPPOE Log

Policy  LAN Policy Packet  DMZ Policy Packet  WAN Policy Packet

Objects  Firewall Log  Authentication Log  RADIUS

Network Services  DDNS Update Log  ClamAV Update Log  Anomaly Log

Mail Security  Anti-Spam Training Log  Mail Log

IDP  IDP Log

Content Record  WEB Virus Record  FTP Virus Record

VPN  IPSec Tunnel Log  PPTP Server Log  PPTP Client Log  L2TP Log

Logs  Logs

Status  Traffic Analysis Log

**Data Storing Time**  When the system capacity is insufficient, data storage time can be reduced automatically

Notify Log	12 ▼ Month(s)	<input type="button" value="Change"/>
Report log	12 ▼ Month(s)	<input type="button" value="Change"/>
Anomaly Flow Log	1 ▼ Month(s)	<input type="button" value="Change"/>
Firewall Log	12 ▼ Month(s)	<input type="button" value="Change"/>
RADIUS Log	12 ▼ Month(s)	<input type="button" value="Change"/>
IDP Log	12 ▼ Month(s)	<input type="button" value="Change"/>
Mail Log and Record	12 ▼ Month(s)	<input type="button" value="Change"/>
WEB Virus Record	12 ▼ Month(s)	<input type="button" value="Change"/>
FTP Virus Record	12 ▼ Month(s)	<input type="button" value="Change"/> ?
System Log	12 ▼ Month(s)	<input type="button" value="Change"/>
Traffic Analysis Log	14 <input type="text"/> Day(s) ( Range : 1 ~ 30 )	<input type="button" value="Change"/>

Function	Description
<b>Clear Data</b>	In order to make more space, clearing some data might be necessary.
<b>Data Storing Time</b>	You may select a number to decide how long you'd like to keep the data. Click Change signatures if you modify numbers.

## 5.2.5 SMTP Server

Select Configuration > Administration > SMTP Server.

Function	Description
<b>Sender Alias</b>	User is able to modify the sender alias.
<b>Sender Name</b>	Input the account to log in to the mail server, such as test@planet.com.tw.
<b>Mail Server IP Address</b>	Input SMTP server address, such as planet.com.tw or 211.22.22.1.
<b>Account</b>	Input the mail account, such as test or test@planet.com.tw.
<b>Password</b>	Input the password.
<b>Authentication</b>	Check it if the SMTP server requires it.
<b>TLS</b>	Check it if the SMTP server requires it.
<b>Bind specific Source IP</b>	The mail will send to the domain, such as planet.com.tw.

## 5.3 System

### 5.3.1 System Backup

Select Configuration > System > System Backup.

Function	Description
<b>System Backup to USB</b>	Insert a USB stick to the CS-950. Then click the “Backup” button to save the system configuration to the USB stick.
<b>System Backup</b>	Save the system configuration to the PC.
<b>System Recovery</b>	Click the “Choose File” button to select the system configuration file, and then click the “OK” button to upload configuration. Note that the system configuration file should be saved by the same firmware version as the current version.

### 5.3.2 Firmware Message

Select Configuration > System > Firmware Message.

The CS-950 supports downloading the latest firmware automatically.

Function	Description
<b>Update</b>	Click “Update” to connect the server and check the firmware version immediately.
<b>Update time</b>	User is able to set a suitable schedule for the CS-950 to update.
<b>Firmware File</b>	When there is a new firmware, it will be listed here.

### 5.3.3 Software Upgrade

Select Configuration > System > Software Upgrade.

System Backup
Firmware Message
Software Upgrade

▶
Software Upgrade

Server Model	CS-950
Software Version	2.2.1.1
Software Upgrade	<input type="button" value="Choose File"/> No file chosen

▶
Upgrade Log

```

2017-08-08 15:59:37 ==> 2.2.0.2 to 2.2.0.3
2017-08-08 16:01:02 ==> 2.2.0.3 to 2.2.0.4
2017-08-08 16:18:57 ==> 2.2.0.4 to 2.2.0.5
2017-08-08 16:28:59 ==> 2.2.0.5 to 2.2.0.6
2017-08-08 16:36:24 ==> 2.2.0.6 to 2.2.0.7
2017-08-08 17:10:27 ==> 2.2.0.7 to 2.2.1
2017-08-29 09:24:16 ==> 2.2.1 to 2.2.1.1
          
```

Function	Description
<b>Software Upgrade</b>	User is able to download the firmware from PLANET website first. Click the “Choose File” button to select the firmware and then click the “Upgrade” button to upgrade firmware.
<b>Upgrade Log</b>	The upgrade history will be listed here.



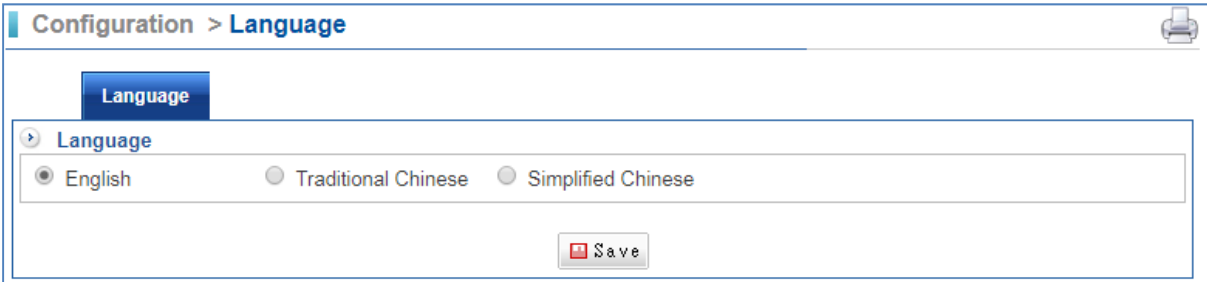
Please do not power off the device, disconnect network cable, close the browser or do anything when upgrading firmware.



## 5.4 Language

Select Configuration > Language > Language.

Please select a language and then click the “Save” button.



Configuration > Language

Language

Language

English     Traditional Chinese     Simplified Chinese

Save

## 5.5 Notification

### 5.5.1 Notification

Select Configuration > Notification > Notification.

This function is in order to remind administrator by mail when items are strange.

**Configuration > Notification**

**Notification** | **Log**

**Notification**

Sender Account:  ? ⚠ SMTP server doesn't set yet

Recipient:

Try to send times:  (1~5)

Mark	Item	Weight	Mail Subject
<input type="checkbox"/>	1. WAN Disconnection	<input type="text" value="1"/>	WAN disconnect
	⊕ Scheduling: every 03 min(s)		
<input type="checkbox"/>	2. DDNS Update Failed	<input type="text" value="1"/>	DDNS fail
	⊕ Scheduling: every 02 hour(s)		
<input type="checkbox"/>	3. SLB Disconnection	<input type="text" value="1"/>	SLB disconnect
	⊕ Scheduling: every 03 min(s)		
<input type="checkbox"/>	4. Master/Slave switch and data synchronization anomalies	<input type="text" value="1"/>	HA switch
	⊕ Scheduling: every 03 min(s)		
<input type="checkbox"/>	5. Firewall Protection (SYN, ICMP, UDP, PortScan)	<input type="text" value="1"/>	Firewall protection
	⊕ Scheduling: every 15 min(s)		
<input type="checkbox"/>	6. Anomaly IP (Outgoing/Incoming session, flow up, flow down)	<input type="text" value="1"/>	Anomaly IP
	⊕ Scheduling: every 15 min(s)		
<input type="checkbox"/>	7. IDP Attack Log	<input type="text" value="1"/>	IDP Log
	⊕ Scheduling: every 15 min(s)		
<input type="checkbox"/>	8. Virus Blocking (Web, mail...)	<input type="text" value="1"/>	Virus block
	⊕ Scheduling: every 15 min(s)		
<input type="checkbox"/>	9. System Log	<input type="text" value="1"/>	Admin log
	⊕ Scheduling: every 06 hour(s)		
<input type="checkbox"/>	10. Administrator Login Failure Event	<input type="text" value="1"/>	Admin login fail
	⊕ Scheduling: every 06 hour(s)		
<input type="checkbox"/>	11. SSL-VPN and Web Authentication Login Failure	<input type="text" value="1"/>	Auth login fail
	⊕ Scheduling: every 06 hour(s)		

<input type="checkbox"/>	12. Software Upgrade	1	Software upgrade
⊕ Scheduling: 00 : 57 every day			
<input type="checkbox"/>	13. Collaborative defense	1	Defense
⊕ Scheduling: every 30 min(s)			
<input type="checkbox"/>	14. CMS (Client management requests, Connect status abnormal, Backup failed, Restore failed)	1	CMS
⊕ Scheduling: every 03 min(s)			
<input type="checkbox"/>	15. Database Anomaly	1	Database Anomaly
⊕ Scheduling: every 15 min(s)			
<input type="checkbox"/>	16. AP Management (Connect status abnormal)	1	AP Management
⊕ Scheduling: every 03 min(s)			
<input type="checkbox"/>	17. Mail Traffic Blocking	1	Mail Traffic Blocking
⊕ Scheduling: every 03 min(s)			
<input type="checkbox"/>	18. IPSec Disconnection	1	IPSec disconnect
⊕ Scheduling: every 03 min(s)			
<input type="checkbox"/>	19. IPSec Switch Notification	1	IPSec Switch
⊕ Scheduling: every 03 min(s)			
<input type="checkbox"/>	20. Authentication Expiring notice	1	Auth Expiration
⊕ Scheduling: 01 : 45 every day			
<input type="checkbox"/>	21. Authentication Maturity delete notification	1	Auth Delete
⊕ Scheduling: 01 : 45 every day			
<input type="checkbox"/>	22. Data Export Results	1	Data Export Results
⊕ Scheduling: every 01 hour(s)			
<input type="checkbox"/>	23. Traffic quota exhausted notice	1	Traffic Quota Run Out
⊕ Scheduling: the 0th minute(s) of every hour			
<input type="checkbox"/>	24. Event of Generated Report	1	Event of Generated Report
⊕ Scheduling: 05 : 00 every day			
<input type="checkbox"/>	25. System capacity is too low (Usage over 95%)	1	System Capacity Anomaly
⊕ Scheduling: every 02 hour(s)			

Function	Description
<b>Sender Account</b>	<p>Select one SMTP server which you have ever set in Configuration &gt; Administration &gt; SMTP Server.</p> <p>Default selection is "Auto". It means CS-950 will detect the domain of receiver, and select the same domain to send mail. If there is no the same domain, CS-950 will send the mail by the first account which is inputted in SMTP Server function.</p> <p>If you did not set any SMTP server, the function will not send email.</p>
<b>Recipient</b>	<p>Input the receiver's mail address. If there is more than one mail address, please separate them by pressing "Enter" of keyboard.</p>

**Try to send times**

The function will try to send 1~5 times. The default value is 1.

## 5.5.2 Notification Log

Select Configuration > Notification > Log.

Configuration > Notification

Notification Log

Search Notification Log

Date: 2017-11-25 00:00 - 2017-11-25 23:59

Event: ALL

Recipient:

Search

Function	Description
<b>Date</b>	Set date and time.
<b>Event</b>	Set whatever information you want to search.
<b>Recipient</b>	Search by the mail receiver. You can use "*" to search, such as *@planet.com.tw.

## 5.6 Report

### 5.6.1 Basic Setting

Select Configuration > Reporter > Basic Setting.

Since the CS-950 is an all-in-one comprehensive gateway security machine, its reports may contain system status of CPU and RAM usage, firewall functions, inbound/outbound traffics, mail flow and type, source of spam mail, etc.

**Configuration > Report**

Basic Setting | Recipient | Report query interval | Log

**Auto-Generated Report**

On  Off    Delivery time: 00:00

SMTP Setting: Auto **SMTP server is not set yet**

Mail Subject: \$Y-\$m-\$d report    ex: \$Y-\$m-\$d 2017-11-25 report

**Default Setting**

Report type:  Daily report  Weekly report

Content include:  Text    Chart = Strip    Display top of 0

Ranking include Other:

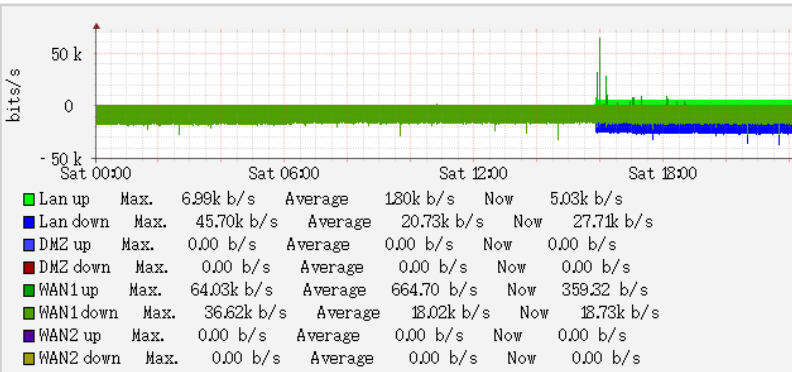
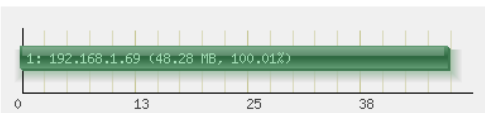
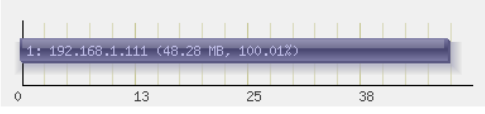
Pie angle degree(0-65): 55

**Report Content**

System report and safety factor	Text	By default	
Administrator configuration	Text	By default	
CPU / RAM status		No	
Device interface flow		On	
Outgoing traffic	Text	By default	Chart By default    Display top of 0
Outgoing traffic by destination	Text	By default	Chart By default    Display top of 0
Outgoing traffic by protocol	Text	By default	Chart By default    Display top of 0
Incoming traffic	Text	By default	Chart By default    Display top of 0
Mail flow	Text	By default	Chart By default    Display top of 0
Mail type	Text	By default	Chart By default
Source of spam mail	Text	By default	Chart By default    Display top of 0

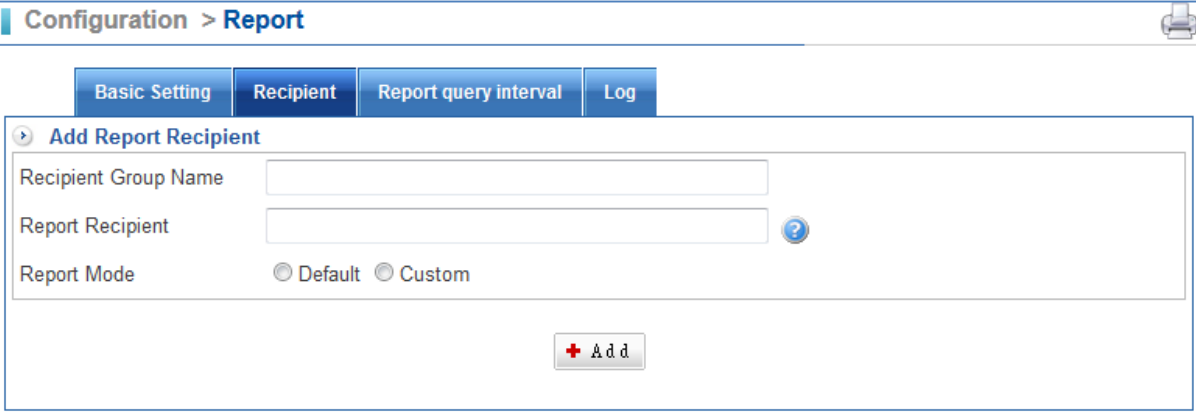
Save    Preview

Function	Description
<b>Delivery time</b>	The report will be delivered at scheduled time. The report will be sent 15 minutes later than the scheduled time.

<b>SMTP Setting</b>	Please go to Configuration > Administration > SMTP Server to create your SMTP first.																																				
<b>Report type</b>	There are three types: Daily report, Weekly report, or Both of them.																																				
<b>Ranking include Other</b>	Besides the top rankings, the rest are included and combined as the Other item.																																				
<b>Pie angle degree (0-65)</b>	<ol style="list-style-type: none"> <li>1. If angle degree is 0, it will be displayed as a floor plane chart;</li> <li>2. If angle degree is &gt; 0, it will be displayed as a block pie chart.</li> <li>3. The angle degree cannot be greater than 65.</li> </ol>																																				
<b>Report Content</b>	<ol style="list-style-type: none"> <li>1. By default means the option follows Default Setting;</li> <li>2. Otherwise, report displays the options you selected;</li> <li>3. If the ranking setting is blank, it will follow Default Setting as well.</li> </ol>																																				
<b>Preview</b>	<p>You are able to click the “Preview” button to see pie chart report, such as the following:</p> <p style="text-align: center;"><b>2017-11-25 Firewall DailyReport</b></p> <div style="border: 1px solid #ccc; padding: 5px;"> <p><b>Device interface flow</b></p>  <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Interface</th> <th>Max.</th> <th>Average</th> <th>Now</th> </tr> </thead> <tbody> <tr> <td>Lan up</td> <td>6.99k b/s</td> <td>180k b/s</td> <td>5.03k b/s</td> </tr> <tr> <td>Lan down</td> <td>45.70k b/s</td> <td>20.73k b/s</td> <td>27.71k b/s</td> </tr> <tr> <td>DMZ up</td> <td>0.00 b/s</td> <td>0.00 b/s</td> <td>0.00 b/s</td> </tr> <tr> <td>DMZ down</td> <td>0.00 b/s</td> <td>0.00 b/s</td> <td>0.00 b/s</td> </tr> <tr> <td>WAN1 up</td> <td>64.03k b/s</td> <td>664.70 b/s</td> <td>359.32 b/s</td> </tr> <tr> <td>WAN1 down</td> <td>36.62k b/s</td> <td>18.02k b/s</td> <td>18.73k b/s</td> </tr> <tr> <td>WAN2 up</td> <td>0.00 b/s</td> <td>0.00 b/s</td> <td>0.00 b/s</td> </tr> <tr> <td>WAN2 down</td> <td>0.00 b/s</td> <td>0.00 b/s</td> <td>0.00 b/s</td> </tr> </tbody> </table> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p><b>Outgoing traffic (All)</b></p>  </div> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p><b>Outgoing traffic ranking by destination</b></p>  </div>	Interface	Max.	Average	Now	Lan up	6.99k b/s	180k b/s	5.03k b/s	Lan down	45.70k b/s	20.73k b/s	27.71k b/s	DMZ up	0.00 b/s	0.00 b/s	0.00 b/s	DMZ down	0.00 b/s	0.00 b/s	0.00 b/s	WAN1 up	64.03k b/s	664.70 b/s	359.32 b/s	WAN1 down	36.62k b/s	18.02k b/s	18.73k b/s	WAN2 up	0.00 b/s	0.00 b/s	0.00 b/s	WAN2 down	0.00 b/s	0.00 b/s	0.00 b/s
Interface	Max.	Average	Now																																		
Lan up	6.99k b/s	180k b/s	5.03k b/s																																		
Lan down	45.70k b/s	20.73k b/s	27.71k b/s																																		
DMZ up	0.00 b/s	0.00 b/s	0.00 b/s																																		
DMZ down	0.00 b/s	0.00 b/s	0.00 b/s																																		
WAN1 up	64.03k b/s	664.70 b/s	359.32 b/s																																		
WAN1 down	36.62k b/s	18.02k b/s	18.73k b/s																																		
WAN2 up	0.00 b/s	0.00 b/s	0.00 b/s																																		
WAN2 down	0.00 b/s	0.00 b/s	0.00 b/s																																		

## 5.6.2 Recipient

Select Configuration > Reporter > Basic Setting.



The screenshot shows a web interface for configuring report recipients. At the top, there is a breadcrumb trail: Configuration > Report. Below this, there are four tabs: Basic Setting, Recipient (which is selected), Report query interval, and Log. The main content area is titled 'Add Report Recipient' and contains three input fields: 'Recipient Group Name', 'Report Recipient', and 'Report Mode'. The 'Report Recipient' field has a help icon (a question mark in a blue circle) to its right. The 'Report Mode' field has two radio buttons: 'Default' and 'Custom'. At the bottom center of the form is a button with a red plus sign and the text '+ Add'.

Function	Description
<b>Recipient Group Name</b>	Input the recipient group name.
<b>Report Recipient</b>	Input the receiver mail address. If there is more than one mail address, please separate them by comma.
<b>Report Mode</b>	Select use the default mode or custom a new one.

## 5.7 Backup & Mount

The CS-950 supports backing up the records of Flow Analysis and Mail Content into Samba.

### 5.7.1 Data Backup

Select Configuration > Backup & Mount > Data Backup.

Function	Description
<b>Backup Method</b>	Samba.
<b>IP address</b>	Input the Samba's IP address.
<b>Folder Name</b>	Input a folder name. If the OS of PC is Windows, user has to create this folder name in C.
<b>Username</b>	Input the account which can write data into Samba.
<b>Password</b>	Input the password which can write data into Samba.
<b>Confirm Password</b>	The confirmation of password.
<b>Scheduled Backup</b>	Set the schedule time.
<b>Backup Item</b>	There are two items -- flow analysis and mail content.



## 5.7.2 Data Mount

Select Configuration > Backup & Mount > Data Mount.

If user wants to see previous contents after reset or data clearance, users can use Backup & Mount application to back up contents to another server or computer. Then, you can mount these contents to search Content Record items.

Configuration > Backup & Mount

Data Backup Data Mount

Current Mount Item

Item	Year-Month
Flow Analysis	
Mail Content	

Access to External Storage Unmount Remote Data

Function	Description
<b>Access to External Storage</b>	Click the button, and you will see data items that you have backed up.
<b>Mount Remote Data</b>	Select the data which you want to mount, and then click the button.
<b>Unmount Remote Data</b>	Click the button if you do not need these contents for searching.

## 5.8 Signature Update

Select Configuration > Signature Update > Signature Update.

Configuration > Signature Update

Signature Update

Name	Version	Last Check Time	Auto Update	Function
IDP Signature Update	2.0.1	2017-09-19 23:15:03	<input type="checkbox"/>	Check Now

Save

Function	Description
<b>Auto Update</b>	Please check the “Auto Update” box, and then system automatically updates the signature version.
<b>Manual Update</b>	Default is manual update. To manually update the signature version, you can click the “Check Now” button to detect signature version.

## 5.9 CMS

CMS is Central Management System. This application allows you to view each CS-950 over the network and Internet, but also allows you to back up each configure setting or update firmware from head office. For example, you can have 4 CS-950's in one building or different places, and be able to view each CS-950 interface from all of them on the same screen.

### 5.9.1 CMS Setting (Client)

Select Configuration > CMS > CMS Setting.

The screenshot shows a web interface for configuring CMS settings. The breadcrumb trail is 'Configuration > CMS'. A blue button labeled 'CMS Setting' is at the top. Below it, the 'CMS Setting' section contains an 'Enable' checkbox (unchecked) and a 'Mode' selector with 'Client' selected and 'Server' unselected. The 'Client Setting' section includes: 'Server' (text input), 'Alias' (text input), 'Update Time' (dropdown set to '1' with 'Minutes' label), and 'Administrator account' (dropdown set to 'admin' with a note: 'If you don't designated management account, the server-side will not be allowed to log into this device.'). A 'Save' button is centered at the bottom.

Function	Description
<b>Enable</b>	Check the box to set the function as enable.
<b>Mode</b>	Select the Client mode to make this device work as client. Select the Server mode to make this device work as server.
<b>Server</b>	Input the IP address of server device. If the client device connects to the server device via internet, please input the WAN IP of server device.
<b>Alias</b>	Input a name for recognition.
<b>Update Time</b>	Set the scheduled time to send information to server device.
<b>Administrator account</b>	Please set an administrator account.

## 5.9.2 CMS Setting (Server)

Select Configuration > CMS > CMS Setting.

Function	Description
<b>Enable</b>	Check the box to set the function as enable.
<b>Mode</b>	Select the Client mode to make this device work as client. Select the Server mode to make this device work as server.
<b>Enable</b>	Check the box to set the scheduled time to backup.  <div style="border: 1px solid #ccc; padding: 5px;"> <p><b>Client profile is automatically backed up to the machine</b></p> <p>Enable <input checked="" type="checkbox"/></p> <p>Automatic backup time</p> <p> <input type="radio"/> Every <input type="text"/> Days  <input checked="" type="radio"/> Custom <input type="checkbox"/> Monday <input type="checkbox"/> Tuesday <input checked="" type="checkbox"/> Wednesday <input type="checkbox"/> Thursday <input type="checkbox"/> Friday <input type="checkbox"/> Saturday <input type="checkbox"/> Sunday         </p> <p> <input checked="" type="radio"/> Every <input type="text" value="3"/> Hours  <input type="radio"/> Custom         </p> <p> <input type="checkbox"/> 00:00 <input type="checkbox"/> 01:00 <input type="checkbox"/> 02:00 <input type="checkbox"/> 03:00 <input type="checkbox"/> 04:00 <input type="checkbox"/> 05:00 <input type="checkbox"/> 06:00 <input type="checkbox"/> 07:00  <input type="checkbox"/> 08:00 <input type="checkbox"/> 09:00 <input type="checkbox"/> 10:00 <input type="checkbox"/> 11:00 <input type="checkbox"/> 12:00 <input type="checkbox"/> 13:00 <input type="checkbox"/> 14:00 <input type="checkbox"/> 15:00  <input type="checkbox"/> 16:00 <input type="checkbox"/> 17:00 <input type="checkbox"/> 18:00 <input type="checkbox"/> 19:00 <input type="checkbox"/> 20:00 <input type="checkbox"/> 21:00 <input type="checkbox"/> 22:00 <input type="checkbox"/> 23:00         </p> <p>The number of Backups to keep <input type="text" value="1"/> Numbers</p> </div>

## 5.9.3 CMS Monitor

Select Configuration > CMS > CMS Monitor.

The function only shows in the CS-950 which works as server.

Function	Description
<b>New client requests</b>	Click the button to accept the client device.

## 5.10 AP Management

### 5.10.1 AP Management Setting

Select Configuration > AP Management > AP Management Setting.

Function	Description
<b>AP Management</b>	By default, the AP Management is disabled. Select the “Start” button and click “Save” to apply change.

### 5.10.2 AP Management

Select Configuration > AP Management > AP Management.

Function	Description
<b>Add</b>	Click the button to add a new wireless network.
<b>Edit</b>	To modify the settings for an entry, check it and click the button.
<b>Del</b>	To delete an entry, check it and click the button.

After clicking “Add” button:



AP Management Setting
AP Management

>
Add AP

Alias

Model

WDAP-702AC
▼

IP

Group

User Define
▼

SNMP Read Community

Connection Test

SNMP Write Community

Connection Test

Save

Function	Description
<b>Alias</b>	Input a name for the AP.
<b>Model</b>	Select the PLANET AP from the list.
<b>IP</b>	Input the IP address of the AP.
<b>Group</b>	Choose a group from the drop-down list or choose User Define, and enter a new group name in the text box. The peer access points belonging to the group adopt the same policy.
<b>SNMP Read Community</b>	Input the password for Read permissions.
<b>SNMP Write Community</b>	Input the password for write permissions.

After adding AP:



AP Management Setting
AP Management

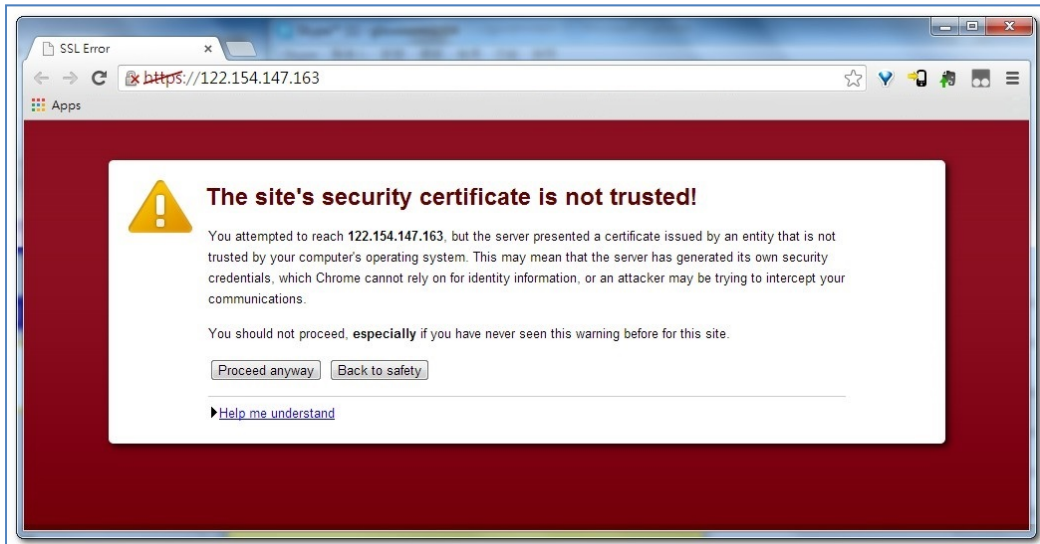
AP Management User defined ssid sort

Activity	Delivery Status	Alias	IP	Channel	SSID	Enable WiFi
Group1						
<input type="checkbox"/> <input type="checkbox"/> WDAP-702AC <span style="border: 1px solid red; padding: 2px;">Delivery</span>						
Delivery Items <input type="checkbox"/> AP Setting (2.4GHz) <input type="checkbox"/> AP Setting (5GHz) <input type="checkbox"/> LAN Setting <input type="checkbox"/> Management Interface Password						
<input type="button" value="Delivery all"/> <input type="button" value="Delivery"/>						
<input type="checkbox"/>			PLANET	192.168.1.252	Auto 2.4GHz 702AC_private Auto 2.4GHz PLANET_3-2.4GHz Auto 5GHz PLANET_1-5GHz	   
<a href="#">More</a>						
<input type="button" value="+ Add"/> <input type="button" value="✎ Edit"/> <input type="button" value="✖ Del"/>						

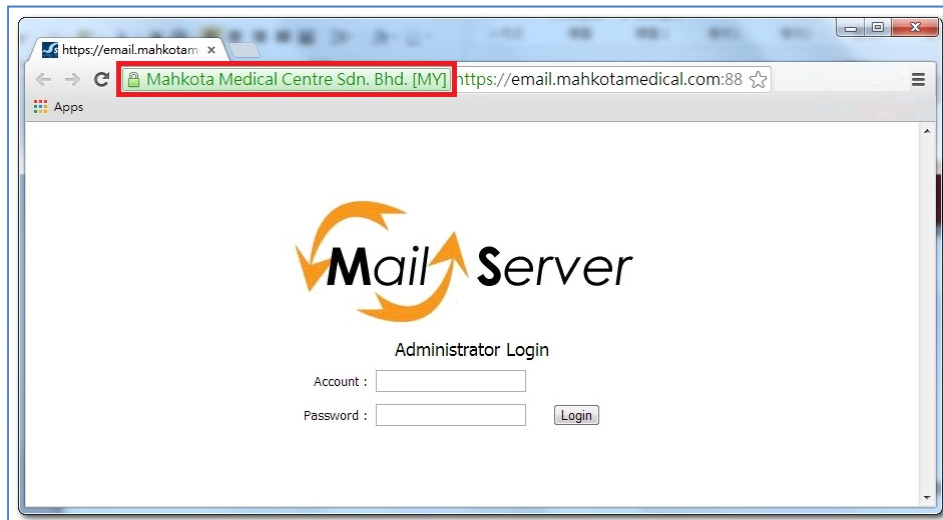
Function	Description
<b>User defined ssid sort</b>	Sort the SSID manually.
<b>Delivery</b>	Set the AP's settings.

## 5.11 SSL Certificate

If you don't like to show SSL notification on 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.



The information in the browser field will be green if SSL Certification is installed.



Select Configuration > SSL Proof.





SSL Proof Set

**SSL Proof Set**

Two-letter Country Codes  (ex : TW) Required

State Or Province  (ex : TAIWAN) Required

City  (ex : TAIPEI) Required

Organization Name  (ex : TWCA) Required

Unit Name  (ex : IT ` SYSTEM) Required

Domain Name  (ex : www.sample.com.tw) Required

Application Personnel Emal.  (ex : sample@mail.com) Required

**SSL Certification Import**

File server.key  No file chosen

File server.crt  No file chosen

File Intermediate Certificate  No file chosen

Function	Description
<b>SSL Proof Set</b>	Sometimes, organizations will ask for server.cst and server.key. Therefore, please enter information and download files. These two files are offered to SSL Certification organization.
<b>SSL Certification Import</b>	Please import three files (server.Key, server.crt, and intermediate certificate) which you apply for for your own SSL Certification from organizations.



PLANET doesn't suggest and guarantee any of the SSL Certification organizations.

# Chapter 6. Network

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

## 6.1 Interface

### 6.1.1 LAN

Select Networking > Interface > LAN.

The screenshot displays the 'LAN Interface Setting' configuration page. At the top, there are tabs for LAN, WAN\_1, WAN\_2, DMZ, and Interface Config. The LAN tab is selected. The configuration fields include: Name (Lan), Interface Name (eth0), IP Address (192.168.1.1), Netmask (255.255.255.0), Up Speed (1024000 Kbps), Down Speed (1024000 Kbps), MAC Address (A8:F7:E0:4C:0A:FD), and Speed and Duplex Mode (Auto). There are also sections for ARP Spoofing Prevention and Administrator Management (Ping, HTTP, HTTPS). A Save button is located at the bottom of the configuration area.

LAN Interface Setup:

Function	Description
<b>Name</b>	Input any word for recognition.
<b>IP Address</b>	Input an IP address.
<b>MAC Address</b>	Input a MAC Address. Note that if user uses the new MAC address instead of A8-F7-E0-xx-xx-xx, the PLANET DDNS and Easy DDNS function may not work properly.
<b>Netmask</b>	Input a Netmask.
<b>Up Speed</b>	Define a suitable Max. Upstream bandwidth for each of them so that

	the device may use it as a basis for operating.
<b>Down Speed</b>	Define a suitable Max. Downstream bandwidth for each of them so that the device may use it as a basis for operating.

Multiple Subnet Setup:

<b>Function</b>	<b>Description</b>
<b>Name</b>	Input any word for recognition.
<b>IP Address</b>	Input an IP address.
<b>Bind</b>	Select it to start multiple subnet function.
<b>Netmask</b>	Input a Netmask.
<b>WAN Interface IP Address</b>	The WAN IP addresses that the subnet corresponds to WAN.
<b>Forwarding Mode</b>	Allows the internal network to accommodate multiple subnets and enables Internet access through various external IP addresses. It displays modes of WAN interface IP. 1. NAT mode 2. Routing

## 6.1.2 WAN\_1

Select Networking > Interface > WAN\_1.

The screenshot shows the 'WAN\_1 Setting' configuration page. The interface includes tabs for LAN, WAN\_1, WAN\_2, DMZ, and Interface Config. The WAN\_1 Setting section contains fields for Name (empty), Interface Name (eth1), IP Address (empty), Default Gateway (empty), Up Speed (Auto), Speed and Duplex Mode (Auto), Load Balance (Auto), Interface Type (WAN), Connection Type (OFF), Netmask (255.255.255.0), MAC Address (A8:F7:E0:31:FF:1D), Down Speed (1500), MTU (1500), and Load Balance options (Manual selected). The WAN Alive Detection section includes Detection Method (ICMP selected), Detected IP Address (168.95.192.1), and Administrator Management (Ping, HTTPS selected). The Firewall Protection section has Firewall Protection Items (SYN, ICMP, UDP, Port Scan). The General Setting section includes DNS Server 1 (168.95.1.1), DNS Server 2 (168.95.192.1), HTTP Port (80), HTTPS Port (443), Wan Alive Detection Period (5 seconds), and Idle Timeout (60 minutes). A Save button is located at the bottom.

- Interface Name-eth1: Enter any word for recognition.
- IP Address: It depends on the connection type. DHCP and PPPoE mode do not need to set IP address. Only Static mode needs to set up IP address.
- Default Gateway: It depends on the connection type. DHCP and PPPoE mode do not need to set Default Gateway. Only Static mode needs to set up Default Gateway.
- Up Speed (Max. 1000Mbps): The IT administrator must define a proper bandwidth for each of them so that the device may use it as a basis for operating. The Kbps is a unit of Speed. You can click on User Define link to set your speed according to ISP's WAN Speed.
- Speed and Duplex Mode: Usually, it sets to Auto. You also can select another setting.
- Load Balancing: It offers four methods.
  1. Auto: Distributes the outward sessions by the usage status of each WAN port.
  2. By Source IP: For services that require using the same IP address throughout the process, such as online game and banking, CS-950 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 CS-950 and a specific host, the following sessions linking to that host will be automatically distributed to the same WAN port.
- **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 so that the device may use it as a basis for operating. The Kbps is a unit of Speed. You can click on User Define link to set your speed according to ISP's WAN Speed.
  - **Detection Method:** Using DNS, ICMP or NONE to check WAN is on or off. Both DNS and ICMP need to set up IP address for testing.
    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 optional modes, ping, HTTP, and HTTPS. In addition, you can click on [Log](#) to see more detailed recordings.
    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.
  - **Firewall Protect Items:** There are four choices, SYN, ICMP, UDP, and Port Scan. It offers currently available protection. In addition, you can click on [Log](#) to see more detailed recordings.
  - **DNS Server 1:** The IP address of the DNS server used for the bulk of DNS lookups. Default setting is 168.95.1.1
  - **HTTP Port:** HTTP port number for management. Default setting is 80.
  - **WAN Alive Detection Period:** System administrators can enter the system every interval of time to do much testing, unit calculated in seconds. Default setting is 3 seconds.
  - **DNS Server 2:** The IP address of the backup DNS server, used when the Primary DNS Server is unreachable. Default setting is 168.95.192.1

- HTTPS Port: HTTPS port number for management. Default setting is 443.
- Idle Timeout: The device may be configured to automatically disconnect when idle for a period of time upon using PPPoE connection. The minute is a unit of time. Default setting is 60 minutes.

### 6.1.3 WAN\_2

Select Networking > Interface > WAN\_2.

- Interface Name-eth1: Enter any word for recognition.
- IP Address: It depends on the connection type. DHCP and PPPoE mode do not need to set IP address. Only Static mode needs to set up IP address.
- Default Gateway: It depends on the connection type. DHCP and PPPoE mode do not need to set Default Gateway. Only Static mode needs to set up Default Gateway.
- Up Speed (Max. 1000Mbps): The IT administrator must define a proper bandwidth for each of them so that the device may use it as a basis for operating. The Kbps is a unit of Speed. You can click on User Define link to set your speed according to ISP's WAN Speed.
- Speed and Duplex Mode: Usually, it sets to Auto. You also can select another setting.
- Load Balancing: It offers four methods.
  1. Auto: Distributes the outward sessions by the usage status of each WAN port.
  2. By Source IP: For services that require using the same IP address throughout the process, such as online game and banking, CS-950 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 to administrator demand to share loading on the WAN.
4. By Destination IP: Once a session is created between the CS-950 and a specific host, the following sessions linking to that host will be automatically distributed to the same WAN port.

- **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 so that the device may use it as a basis for operating. The Kbps is a unit of Speed. You can click on User Define link to set your speed according to ISP's WAN Speed.
- **Detection Method:** Using DNS 、 ICMP or NONE to check WAN is on or off. Both DNS and ICMP need to set up IP address for test.
  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 optional modes, ping, HTTP, and HTTPS. In addition, you can click on [Log](#) to see more detailed recordings.
  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.
- **Firewall Protect Items:** There are four choices, SYN, ICMP, UDP, and Port Scan. It offers currently available protection. In addition, you can click on [Log](#) to see more detailed recordings.
- **DNS Server 1:** The IP address of the DNS server used for the bulk of DNS lookups. Default setting is 168.95.1.1
- **HTTP Port:** HTTP port number for management. Default setting is 80.
- **WAN Alive Detection Period:** System administrators can enter the system every interval of time to do much testing, unit calculated in seconds. Default setting is 3 seconds.
- **DNS Server 2:** The IP address of the backup DNS server, used when the Primary DNS Server is unreachable. Default setting is 168.95.192.1

- HTTPS Port: HTTPS port number for management. Default setting is 443.
- Idle Timeout: The device may be configured to automatically disconnect when idle for a period of time upon using PPPoE connection. The minute is a unit of time. Default setting is 60 minutes.

## 6.1.4 DMZ

Networking > Interfaces > DMZ.


The screenshot displays the configuration interface for a DMZ. At the top, there are navigation tabs: LAN, WAN\_1, WAN\_2, DMZ (selected), and Interface Config. Below the tabs, the 'DMZ Setting' section contains the following fields:

- Name: Dmz
- Interface Name: eth3
- IP Address: #
- Up Speed: 1024000 (Kbps)
- MAC Address: A8:F7:E0:31:FF:1F
- Speed and Duplex Mode: Auto
- Interface Type: DMZ
- Enable: OFF
- Netmask: 255.255.255.0
- Down Speed: 1024000 (Kbps)
- MTU: 1500

Below the DMZ Setting section, there are two other sections:

- ARP Spoofing Prevention:** Includes an 'Enable' checkbox and a text input field set to '30', with a note: 'Seconds(range:1~600), send 3 times in a row'.
- Administrator Management:** Includes a section for 'Administrator Management' with three checked checkboxes: Ping, HTTP, and HTTPS.

A 'Save' button is located at the bottom center of the configuration area.

- Name: Enter any word for recognition.
- IP address: Enter an IP address.
- Up Speed: The IT administrator must define a proper bandwidth for each of them so that the device may use it as a basis for operating. The Kbps is a unit of Speed.
- MAC Address: Enter a MAC address.
- 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. BRI: In this mode, the DMZ and the WAN interfaces are in the same domain. It is just for one WAN line when transparent Bridging.
- Netmask: Enter a Netmask.
- Down Speed: The IT administrator must define a proper bandwidth for each of them so that the device may use it as a basis for operating. The Kbps is a unit of Speed.
- Click on  after you finish setting.



## 6.2 Interface (IPv6)

### 6.2.1 LAN (IPv6)

Select Networking > Interface (IPv6) > LAN.

Network > Interface (IPv6)

LAN WAN\_1 WAN\_2 DMZ DNS Server

LAN IPv6 Setting

Enable

IPv6 LAN (eth0) IP  (ex: 2001:288:1111::254/64)

IPv6 Auto Configuration  Start  Stop

Inside To Outside Connection Type

WAN\_1  Routing  NAT

WAN\_2  Routing  NAT

WAN\_3  Routing  NAT

Save

- IPv6 LAN (eth0) IP: Enter IPv6 address.
- IPv6 Auto Configuration: Select Start to begin this function. On the other hand, select Stop to pause the function.
- Click on Save.

### 6.2.2 WAN\_1 (IPv6)

Select Networking > Interface (IPv6) > WAN\_1

Network > Interface (IPv6)

LAN WAN\_1 WAN\_2 DMZ DNS Server

WAN1 IPv6 Setting

IPv6 Model

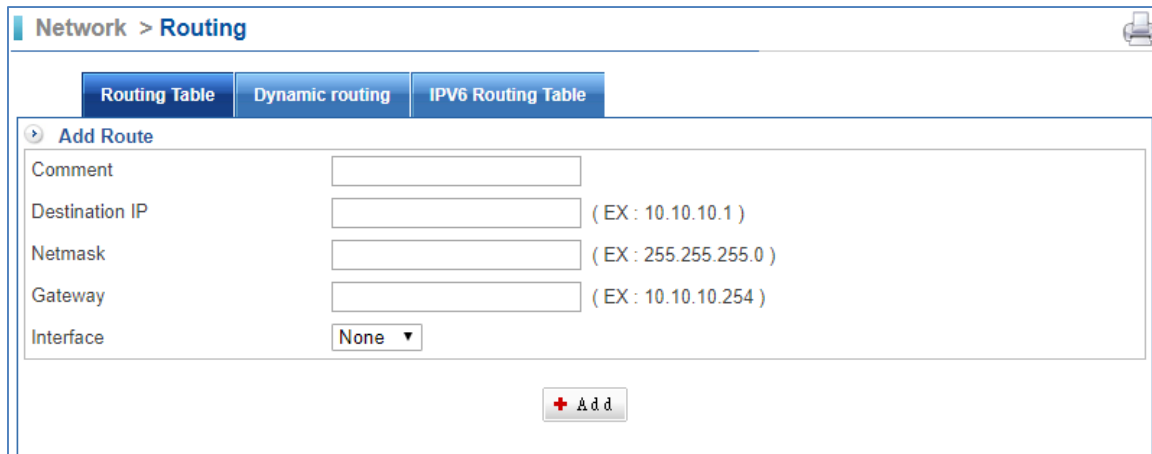
Save

- IPv6 Model: It offers two ways.
  1. Tunnel
  2. Routing
- WAN 1 IP: Enter your WAN IPv6 address.
- Local IPv6 IP: Enter your PC Local IPv6 address.
- ISP IP: Enter an IP address which from ISP.
- Click on Save.

## 6.3 Routing

### 6.3.1 Routing Table


Select Networking > Routing > Routing Table.



The screenshot shows the 'Add Route' form in the 'Routing Table' section. The form has a title bar 'Network > Routing' and a print icon. Below the title bar are three tabs: 'Routing Table', 'Dynamic routing', and 'IPv6 Routing Table'. The 'Add Route' form contains the following fields:

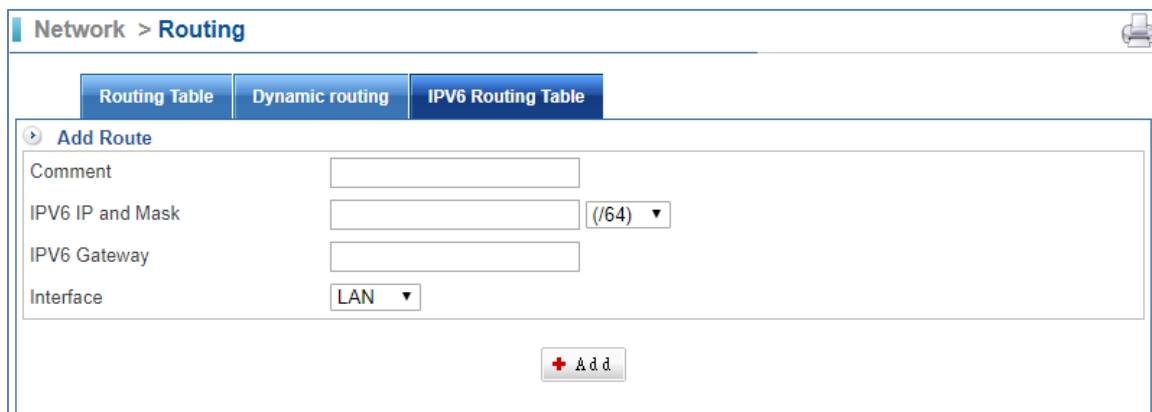
- Comment: Text input field.
- Destination IP: Text input field with an example '( EX : 10.10.10.1 )'.
- Netmask: Text input field with an example '( EX : 255.255.255.0 )'.
- Gateway: Text input field with an example '( EX : 10.10.10.254 )'.
- Interface: Dropdown menu with 'None' selected.

At the bottom of the form is a '+ Add' button.

- Click on  to create a new routing table.
- Comment: Enter any word for recognition.
- Destination IP: Enter an IP address.
- Netmask: Enter Netmask
- Gateway: Enter Gateway

### 6.3.2 IPv6 Routing Table


Select Networking > Routing > Routing Table.



The screenshot shows the 'Add Route' form in the 'IPv6 Routing Table' section. The form has a title bar 'Network > Routing' and a print icon. Below the title bar are three tabs: 'Routing Table', 'Dynamic routing', and 'IPv6 Routing Table'. The 'Add Route' form contains the following fields:

- Comment: Text input field.
- IPv6 IP and Mask: Text input field with a dropdown menu showing '( /64 )'.
- IPv6 Gateway: Text input field.
- Interface: Dropdown menu with 'LAN' selected.

At the bottom of the form is a '+ Add' button.

- Click on  to create a new routing table.
- Comment: Enter any word for recognition.
- IPv6 IP and Mask: Enter an IPv6 IP address and Netmask.
- IPv6 Gateway: Enter Gateway

# Chapter 7. Policy

The CS-950 UTM 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 include Policy Name, Source Address, Destination Address, Action, Protocol, Service Port or Group, Software Access Control, QoS, Schedule, URL Policy, Internet Auth, WAN selection, Maximum Concurrent Sessions per source IP Address, mail log and record, WEB/FTP Anti-virus, IDP, Packet tracing, Traffic Analysis, and mail quota. 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.

## 7.1 LAN Policy, DMZ Policy, and WAN Policy



- Click on first.

**Policy > LAN Policy**

LAN to WAN | LAN to DMZ | LAN to LAN | LAN to WAN (IPv6)

**Basic Setting**

Policy Name:

Source:  Inside\_Any  IP Address  MAC Address

Destination:  Outside\_Any  IP Address

Action:

**Policy**

Protocol:

Service Port or Group:  Service Port

Software Access Control:

QoS:

Schedule:

URL Access Control:

Authentication:

Bulletin Board:

WAN:

Max. Concurrent Sessions for Each Source IP Address:

Mail Log & Record:

WEB/FTP Anti-virus:

IDP:

Packet Tracing:

Traffic Analysis:



Max. Quota / Day: Up  KBytes / Down  KBytes (0:No Limit)
















Max. Quota / Day(Per Source IP): Up  KBytes / Down  KBytes (0:No Limit)


The quota is used up, web blocking message:

**Firewall Protection**

SYN Attack  ICMP Attack  UDP Attack  Port Scan

- 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 is Permit, the policy will be passed. On the other hand, it is Drop; the policy will be stopped.
  1.  Drop: Deny the Policy.
  2.  Permit: Allow the Policy.
- Protocol:
  1. ALL
  2. TCP
  3. UDP
  4. ICMP
- Service Port or Group: The services are regulated. Available options are the system default services and the services that are customized in the Services function.

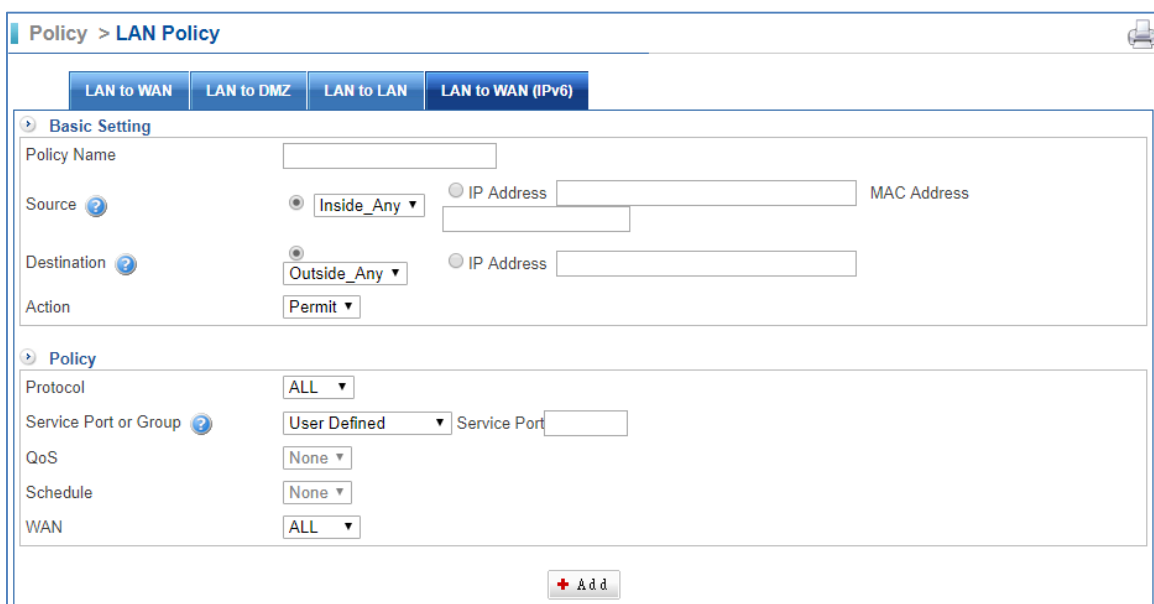
- Software Access Control: It can restrict the use of application software.
-  QoS: The guaranteed and maximum bandwidth settings (The bandwidth is distributed to users. Setting this in the QoS function)
-  Schedule: Activate as per the configured scheduled time. Set this function in the Schedule function.
-  URL Policy: It can restrict the access to any URL websites specified. Set this function in the URL List function.
-  Internet Auth: This requires users to be authenticated to create a connection. Set this function on the Internet Auth function.
- WAN: It determines over which WAN interface's packets are permitted to pass through.
  1. All: Packets are granted to pass through all interfaces once approved by the configured policy.
  2.  WAN 1: Policy approved packets may access WAN 1.
  3.  WAN 2: Policy approved packets may access WAN 2.
-  Maximum Concurrent Sessions per 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.
-  Drop Skype: It can restrict the use of Skype protocol.
-  WEB/FTP Anti-virus: It filters viruses contained within files transferred over WEB, FTP protocol.
-  IDP: It can identify intrusion packets and react to them in a timely manner.
-  Pause: Temporarily disable the policy.
-  Start: Start the Policy.
-  Delete: Delete the Policy.
-  Edit: Edit the Policy.
-  Traffic Analysis: Click on this button, and you can see the detailed illustration of traffic analysis.



-  Packet tracing: Record Logs of packet transmissions managed by the policy. You can click on the Log button to see packet logs.





## 7.2 LAN to WAN (IPV6)



- Click on  first.



- Policy Name: Enter any word for the description of the policy.
- Source Address: 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 Address: 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 is Permit, the policy will be pass. On the other hand, it is DROP, the policy will be stop.
  1.  DROP: Deny the Policy.
  2.  Permit: Allow the Policy.
- Protocol:
  1. ALL
  2. TCP
  3. UDP
  4. ICMP

- Service Port or Group: The services are regulated. Available options are the system default services and the services that are customized in the Services function.
-  QoS: The guaranteed and maximum bandwidth settings (The bandwidth is distributed to users. Setting this in the QoS function)
-  Schedule: Activate as per the configured scheduled time. Set this function in the Schedule function.
- WAN: It determines over which WAN interface's packets are permitted to pass through.
  1. All: Packets are granted to pass through all interfaces once approved by the configured policy.
  2.  WAN 1: Policy approved packets may access WAN 1.
  3.  WAN 2: Policy approved packets may access WAN 2.

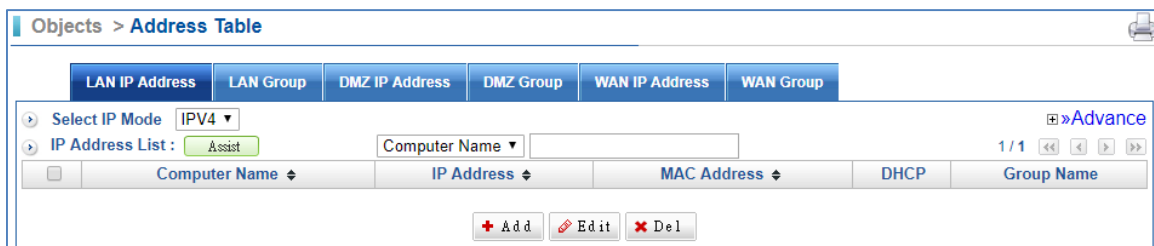
# Chapter 8. Objects

## 8.1 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.

### 8.1.1 LAN IP Address

Select Objects > Address Table > LAN IP Address.



- Select IP Mode:
  1. IPv4 Mode
  2. IP v6 Mode
- Computer Name, IP, and MAC 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.
- Click on **+ Add** to create one LAN IP Address first.



- Computer Name.
- Settings:



1. Only set the IP address
2. Set IP and MAC address
  - Get static IP address from DHCP Server.

## 8.1.2 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 the  button to create a LAN Group rule.
- Group Name: Enter any word for recognition.

- Select from IP Address Member: The left user lists which you add in LAN IP Address.
  - Select from IP Rang: Enter the range IP addresses which you want to restrict to.
  - Select from IP/Mask:
  - Select from DHCP Users: It shows a range of DHCP users, and these will be restricted. If you select IP-MAC Binding tick box, it will show list of IP MAC.
  - Users Define: Please enter an IP address or subnet.
  - Select MAC Address Group: Please enter an MAC address or subnet.
- There is an example of how LAN Group is used.
    1. Select Policy > LAN Policy > LAN to WAN or LAN to DMZ.

- Click on **+ Add**, and select Action to Drop, and then select Source to group A which you have just set in LAN IP Address function.

**Basic Setting**

Policy Name:

Source: **Inside\_Any** (selected)  
 Destination: **Inside\_Any** (selected)  
 Action: **Drop** (selected)  
 DR: Any, Ting, Tom, **group A** (selected)

**Policy**

Protocol: ALL  
 Service Port or Group: User defined  
 Service Port:   
 Software Access Control: None  
 QoS: None  
 Schedule: None  
 URL Policy: None  
 Internet Auth: None  
 Using Which WAN: ALL  
 Maximum Concurrent Sessions per IP Address: 0  
 Drop Skype:   
 WEB/FTP Anti-virus:   
 Packet tracing:   
 Traffic Analysis:

- Setting Address Policy completed.

No.	Policy Name	Source	Destination	Services	Action	On/Off	Policy	Edit / Del	Rec.
1		192.168.1.14	Outside_Any	ANY	Drop	On		[Edit] [Del]	Log
2		192.168.1.11	Outside_Any	ANY	Drop	On	?	[Edit] [Del]	Log
3		Inside_Any	Outside_Any	ANY	Drop	On		[Edit] [Del]	Log
4		group A	Outside_Any	ANY	Drop	On		[Edit] [Del]	Log

### 8.1.3 DMZ IP Address

Select Objects > Address Table > DMZ IP Address.

**Objects > Address Table**

LAN IP Address | LAN Group | **DMZ IP Address** | DMZ Group | WAN IP Address | WAN Group

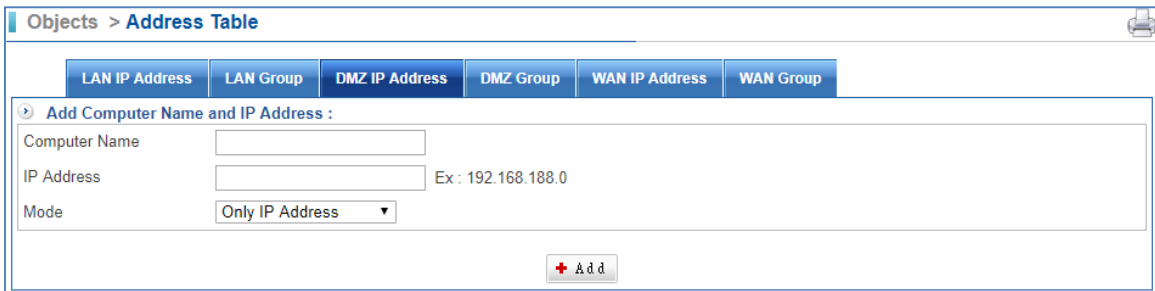
Select IP Mode: **IPv4** (selected) [Advance]

IP Address List: **Assist** (selected) Computer Name:

Computer Name	IP Address	MAC Address	DHCP	Group Name
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>

[+ Add] [Edit] [Del]

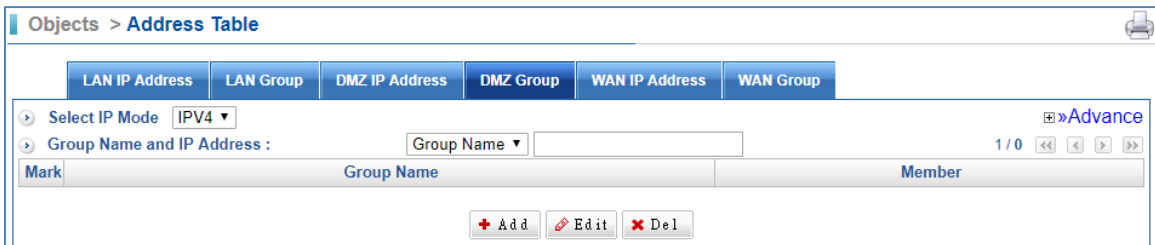
- Select IP Mode:
  - IPv4 Mode: IPv4 address.
  - IP v6 Mode: IPv6 address.
- Computer Name, IP, and MAC Address: It is recommended to configure some desirable address names within Address first so that they are ready to use for the Source Address or Destination Address setting of a policy. In addition, you may click on **Assist** to add to create an entry.
- Click on the **+ Add** button to create a DMZ IP Address first..



- Computer Name.
- Settings:
  1. Only set the IP address
  2. Set IP and MAC address
- Get static IP address from DHCP Server.

### 8.1.4 DMZ Group

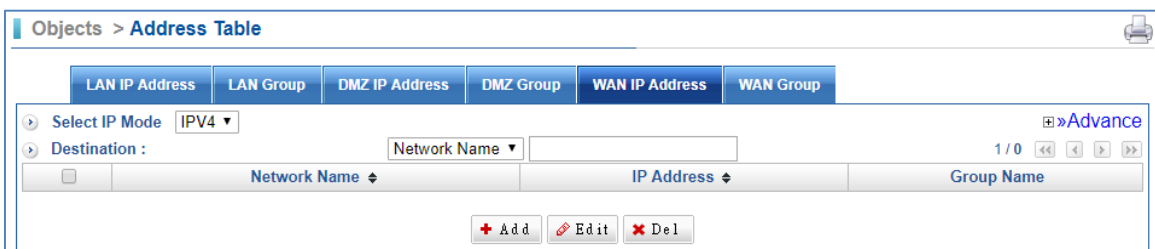
Select Objects > Address Table > DMZ Group.



DMZ Group setting way is the same as LAN Group. When you want to use DMZ Group, just select Policy > DMZ Policy> DMZ to WAN or DMZ to LAN. Click on **Add**, and select Action to Drop, and then select Source to which you have just set in Address Table.

### 8.1.5 WAN IP Address

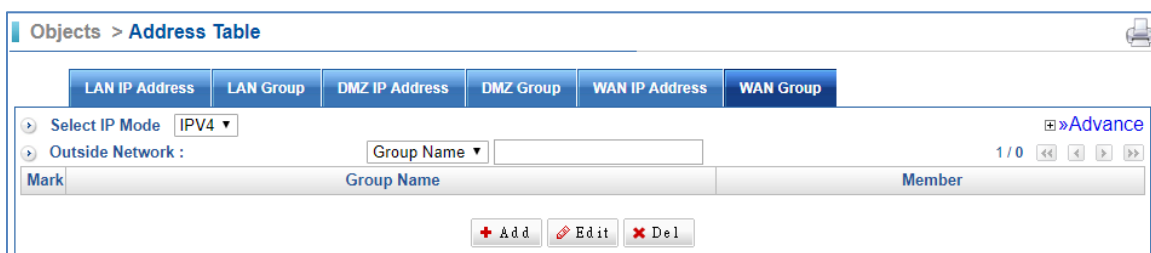
Select Objects > Address Table > WAN IP Address.



WAN IP Address setting way is the same as LAN IP Address.

## 8.1.6 WAN Group

Select Objects > Address Table > WAN Group.



WAN Group setting way is the same as LAN Group. When you want to use WAN Group, just select Policy > WAN Policy> WAN to LAN or WAN to DMZ. Click on **+ Add**, and select Action to Drop, and then select Source to which you have just set in Address Table.

## 8.2 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.

### 8.2.1 Basic Service

Select Objects > Services > Basic Service.

Objects > Services Table

Basic Service | Service Group

Basic Service and Port :

ANY ANY (ANY)	TCP AFPoverTCP (548)	TCP AOL (5190)	TCP BGP (179)
UDP DNS (53)	TCP FTP (21)	TCP Finger (79)	TCP GNUTella (6346)
TCP Gopher (70)	TCP H323 (NetMeeting) (1720)	TCP HTTP (80)	TCP HTTPS (443)
TCP ICQ (4000)	UDP IKE (500)	TCP IMAP over SSL (993)	TCP IMAP (143)
TCP Ident (113)	TCP L2TP (1701)	TCP LDAP Admin (3407)	TCP LDAP over SSL (636)
TCP LDAP (389)	TCP MSN Messenger (1863)	TCP NNTP (119)	UDP NTP (123)
TCP NTTP over SSL (563)	TCP POP2 (109)	TCP POP3 over SSL (995)	TCP POP3 (110)
TCP PPTP (1723)	UDP RIP (520)	TCP RLOGIN (513)	TCP Real Audio (7070)
TCP SFTP (115)	TCP SMTP over SSL (465)	TCP SMTP (25)	UDP SNMP (161)
TCP SSH (22)	UDP SYSLOG (514)	UDP TFTP (69)	TCP Telnet (23)
TCP Terminal (3389)	UDP UUCP (540)	TCP VNC (5900)	TCP WAIS (210)
TCP WINFRAME (1494)	TCP Yahoo (5050)		

## 8.2.2 Service Group

Select Objects > Services > Service Group.

Objects > Services Table

Basic Service | Service Group

Service Group List : Choose File No file chosen Import Export 1 / 1

Mark	Group Name	Port (Start : End)

+ Add Edit Del

- Click on **+ Add** to create a 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).



Basic Service
Service Group

▶ Add Service Group :

Assist
» More

	Protocol	Port (Start : End)
1	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> ICMP	<input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/>
2	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> ICMP	<input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/>
3	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> ICMP	<input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/>
4	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> ICMP	<input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/>
5	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> ICMP	<input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/>
6	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> ICMP	<input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/>
7	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> ICMP	<input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/>
8	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> ICMP	<input style="width: 40px;" type="text"/> : <input style="width: 40px;" type="text"/>

+ Add

- Group Name: Enter some words for recognition.
- Click on Assist to select services.
- After selected. If you make the wrong selection, you will want to remove one port. Please blank out the port.

### 8.3 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.

Select Objects > Schedule > Schedule List.

Objects > Schedule

Schedule List

▶ Schedule List :
1 / 0

◀◀ ◀ ▶ ▶▶

Mark	Schedule Name	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday

+ Add
✎ Edit
✖ Del

- Click on + Add to create a new Schedule rule first.



**Schedule List**

▶ Add Schedule :

Schedule Name

Setting Mode  Mode 1  Mode 2

---

Sunday  Disable  All day  Start Time  -- End Time

Monday  Disable  All day  Start Time  -- End Time

Tuesday  Disable  All day  Start Time  -- End Time

Wednesday  Disable  All day  Start Time  -- End Time

Thursday  Disable  All day  Start Time  -- End Time

Friday  Disable  All day  Start Time  -- End Time

Saturday  Disable  All day  Start Time  -- End Time

- Schedule Name: Enter some words for recognition.
- Setting your time schedule.

## 8.4 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.

Select Objects > QoS > QoS Setting.

**Objects > QoS**

**QoS Setting**

▶ Bandwidth Can Be Allocated :  %

▶ QoS List : 1 / 0 << < > >>

Mark	QoS Name	Priority	Bandwidth Mode	Interface	User Down Speed	User Up Speed
<input type="button" value="+ Add"/> <input type="button" value="Edit"/> <input type="button" value="Del"/>						

- Click on  to create a new QoS rule first.

Objects > QoS 🖨️

**QoS Setting**

➤ Add QoS Rule :

QoS Name

Priority  Select Bandwidth Mode

Interface	User Down Speed		User Up Speed	
LAN eth0	Min. <input type="text" value="0"/>	Kbps (1~1,024,000)	Min. <input type="text" value="0"/>	Kbps (1~1,024,000)
	Max. <input type="text" value="0"/>	Kbps (1~1,024,000)	Max. <input type="text" value="0"/>	Kbps (1~1,024,000)
DMZ eth3	Min. <input type="text" value="0"/>	Kbps (1~1,024,000)	Min. <input type="text" value="0"/>	Kbps (1~1,024,000)
	Max. <input type="text" value="0"/>	Kbps (1~1,024,000)	Max. <input type="text" value="0"/>	Kbps (1~1,024,000)
WAN1	Min. <input type="text" value="0"/>	Kbps	Min. <input type="text" value="0"/>	Kbps
	Max. <input type="text" value="0"/>	Kbps	Max. <input type="text" value="0"/>	Kbps
WAN2	Min. <input type="text" value="0"/>	Kbps	Min. <input type="text" value="0"/>	Kbps
	Max. <input type="text" value="0"/>	Kbps	Max. <input type="text" value="0"/>	Kbps
WAN3	Min. <input type="text" value="0"/>	Kbps	Min. <input type="text" value="0"/>	Kbps
	Max. <input type="text" value="0"/>	Kbps	Max. <input type="text" value="0"/>	Kbps
Tunnel1	Min. <input type="text" value="0"/>	Kbps	Min. <input type="text" value="0"/>	Kbps
	Max. <input type="text" value="0"/>	Kbps	Max. <input type="text" value="0"/>	Kbps
Tunnel2	Min. <input type="text" value="0"/>	Kbps	Min. <input type="text" value="0"/>	Kbps
	Max. <input type="text" value="0"/>	Kbps	Max. <input type="text" value="0"/>	Kbps
Tunnel3	Min. <input type="text" value="0"/>	Kbps	Min. <input type="text" value="0"/>	Kbps
	Max. <input type="text" value="0"/>	Kbps	Max. <input type="text" value="0"/>	Kbps

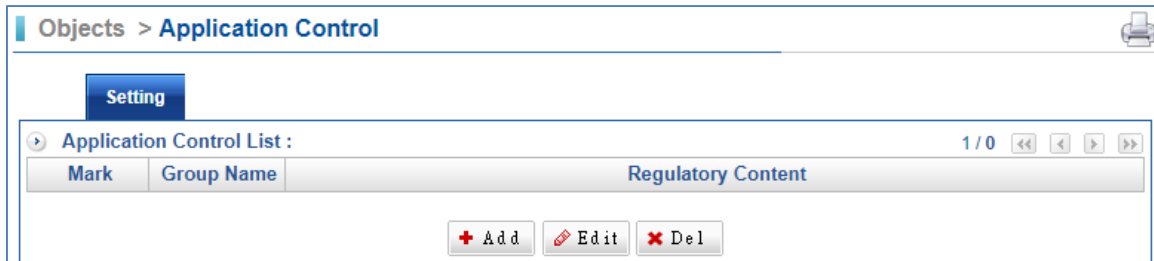
- QoS Name: Enter any word for recognition.
- Priority: To configure the priority of distributing Upstream/Downstream and unused bandwidth
- Select Bandwidth Mode: It offers three ways.
  1. By Policy Based.
  2. Per Outgoing IP Based (It includes Smart QoS application).
  3. Per Incoming IP Based.
- Interface: Display LAN, DMZ, WAN and Tunnel.
- 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.
- Min. (Guaranteed Bandwidth): Specifies the minimum (guaranteed) amount of bandwidth.
- Max. (Maximum Bandwidth): Specifies the maximum amount of bandwidth.



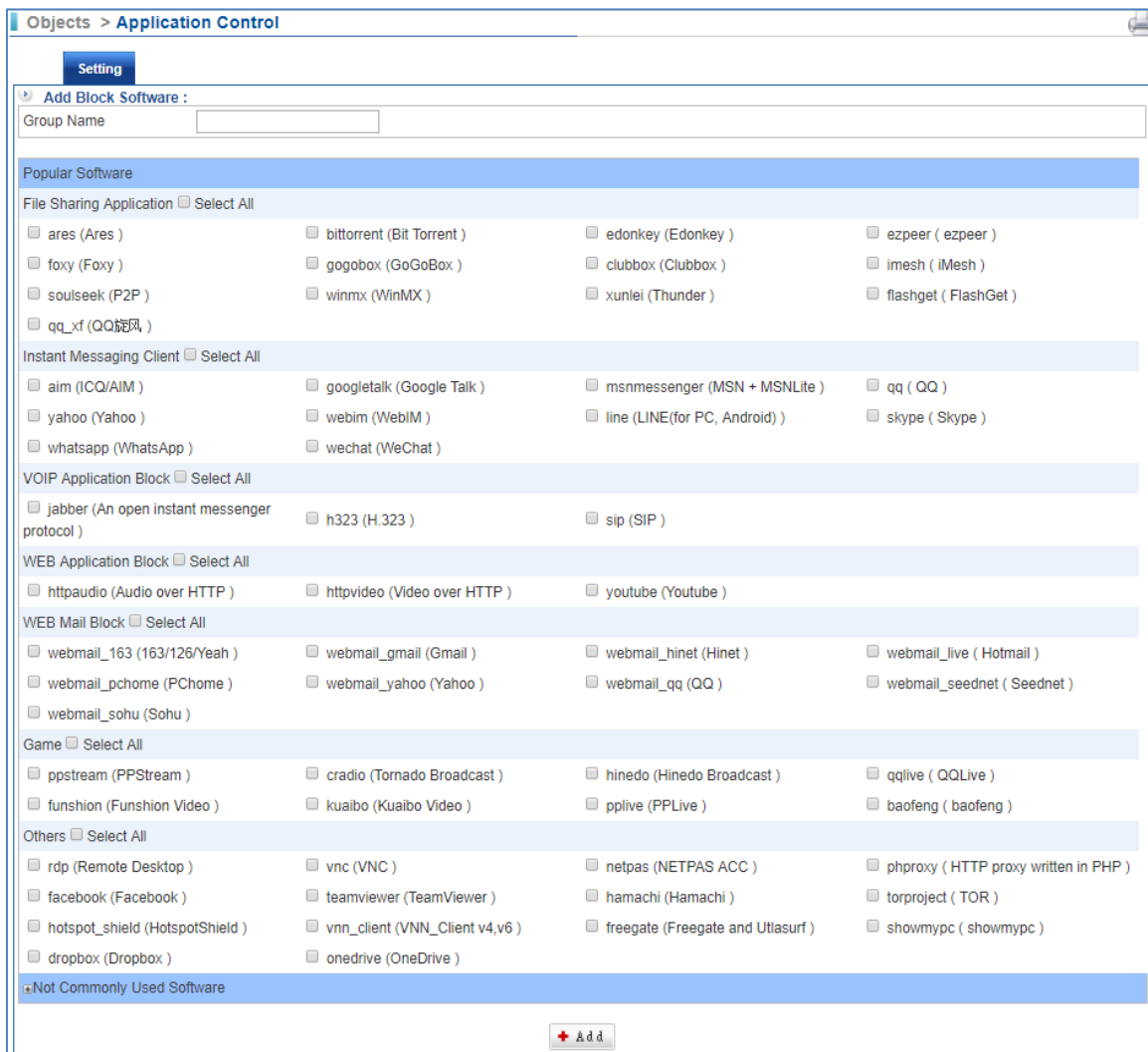
## 8.5 Application Control

It offers several kinds of software blocking, such as File Sharing Application, Instant Messaging Client, Web Application, VoIP Application Block, Web Mail, Game and Other Applications.

Select Objects > Application Control > Setting.



■ Click on  first.



■ Group Name: Enter any word for recognition.

■ Popular Software/ Not Commonly Used Software: Select the software which you want to block.

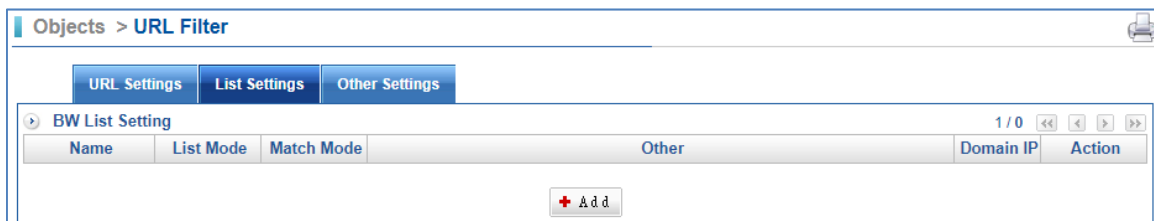
## 8.6 URL Filtering

URL Filtering is widely used for parental control, compliance and productivity. In schools, for instance, URL Filtering is used to help deter exposure to inappropriate websites, such as pornography, nudity, aggressive sites, etc. In offices, URL Filtering is especially an indispensable 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.

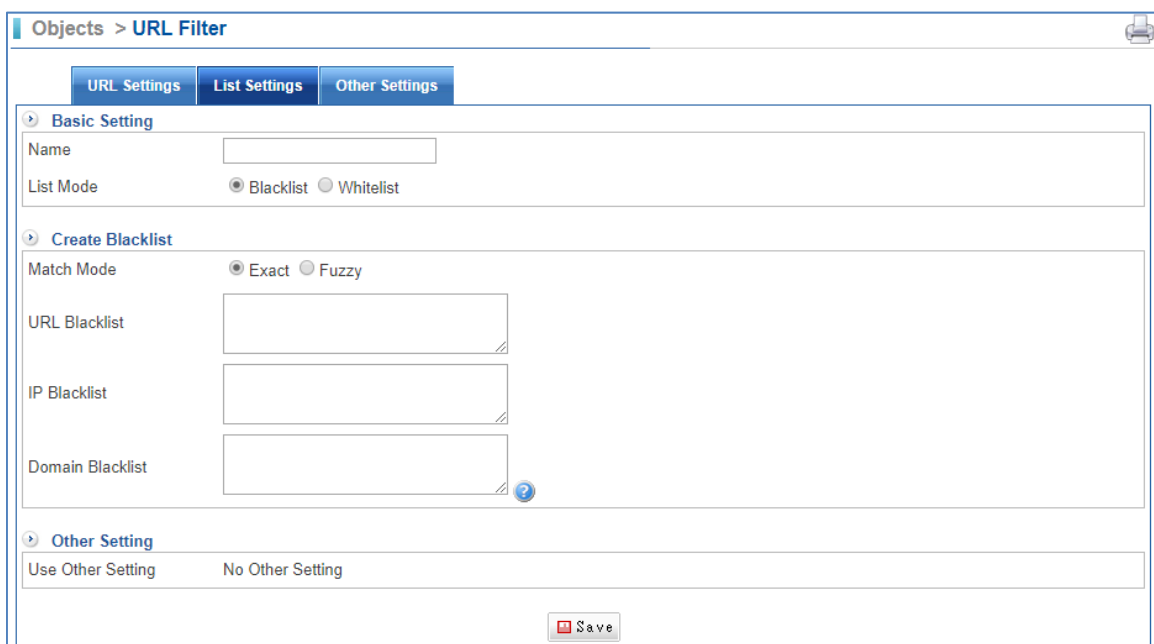
### 8.6.1 List Settings

Select Objects > URL Filter > List Settings.



The screenshot shows the 'List Settings' tab for a URL Filter. At the top, there are three tabs: 'URL Settings', 'List Settings' (selected), and 'Other Settings'. Below the tabs is a sub-section titled 'BW List Setting' with a '1 / 0' indicator and navigation arrows. A table with the following columns is displayed: 'Name', 'List Mode', 'Match Mode', 'Other', 'Domain IP', and 'Action'. Below the table, there is a '+ Add' button.

- Click on  first.



The screenshot shows the 'Basic Setting' section of the 'List Settings' tab. It includes a 'Name' text input field. Below it, 'List Mode' has two radio buttons: 'Blacklist' (selected) and 'Whitelist'. The 'Create Blacklist' section contains a 'Match Mode' with 'Exact' (selected) and 'Fuzzy' radio buttons, and three text input fields for 'URL Blacklist', 'IP Blacklist', and 'Domain Blacklist'. At the bottom, there is an 'Other Setting' section with a 'Use Other Setting' checkbox and a 'No Other Setting' text input. A 'Save' button is located at the bottom center.

- Name: Enter any words for recognition.
- List Mode: Select for Black list or White list.

- Match Mode: There are two ways, Exact and Fuzzy.
- URL Black list: Enter the complete domain name or key word of the website. It is restricted specific website whether user surfs Internet or not; however, it depends on what you select in List Mode. For example, "www.kcg.gov.tw" "kh.google.com" "gov" or "\*google\*".
- IP Black list: Enter the complete IP address. It is restricted specific website whether user surfs Internet or not; however, it depends on what you select in List Mode.

## 8.6.2 URL Settings

Select Objects > URL Filter > URL Settings.

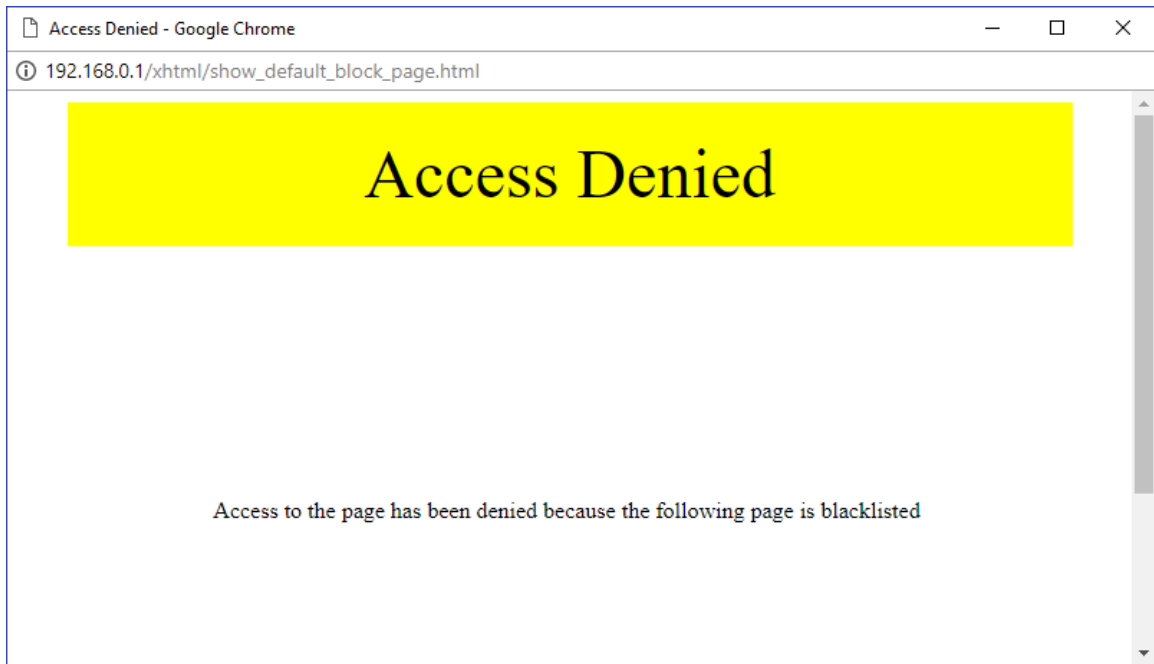
- Click on  first.

- Group Name: Enter any words for recognition.
- Create block warning message: User can create block warning message their own if selected.
- List Select: Select one that you have ever added in List settings.

## 8.6.3 Other Settings

Select Objects > URL Filter > Other Settings.

- Warning message: Click “[View](#)” to preview the warning message page; the page is shown below:

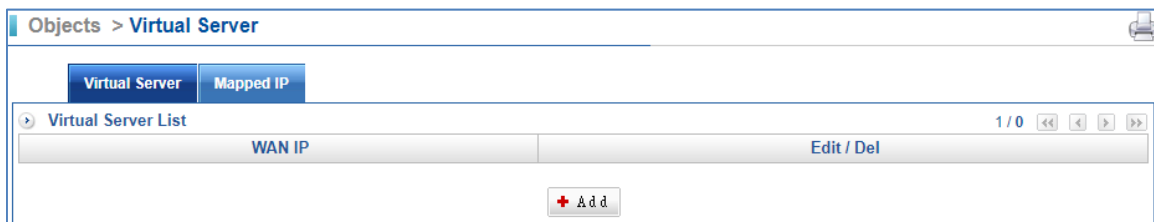


- Warning Subject: Input the subject.
- Warning content: Input the content.

## 8.7 Virtual Server

### 8.7.1 Virtual Server

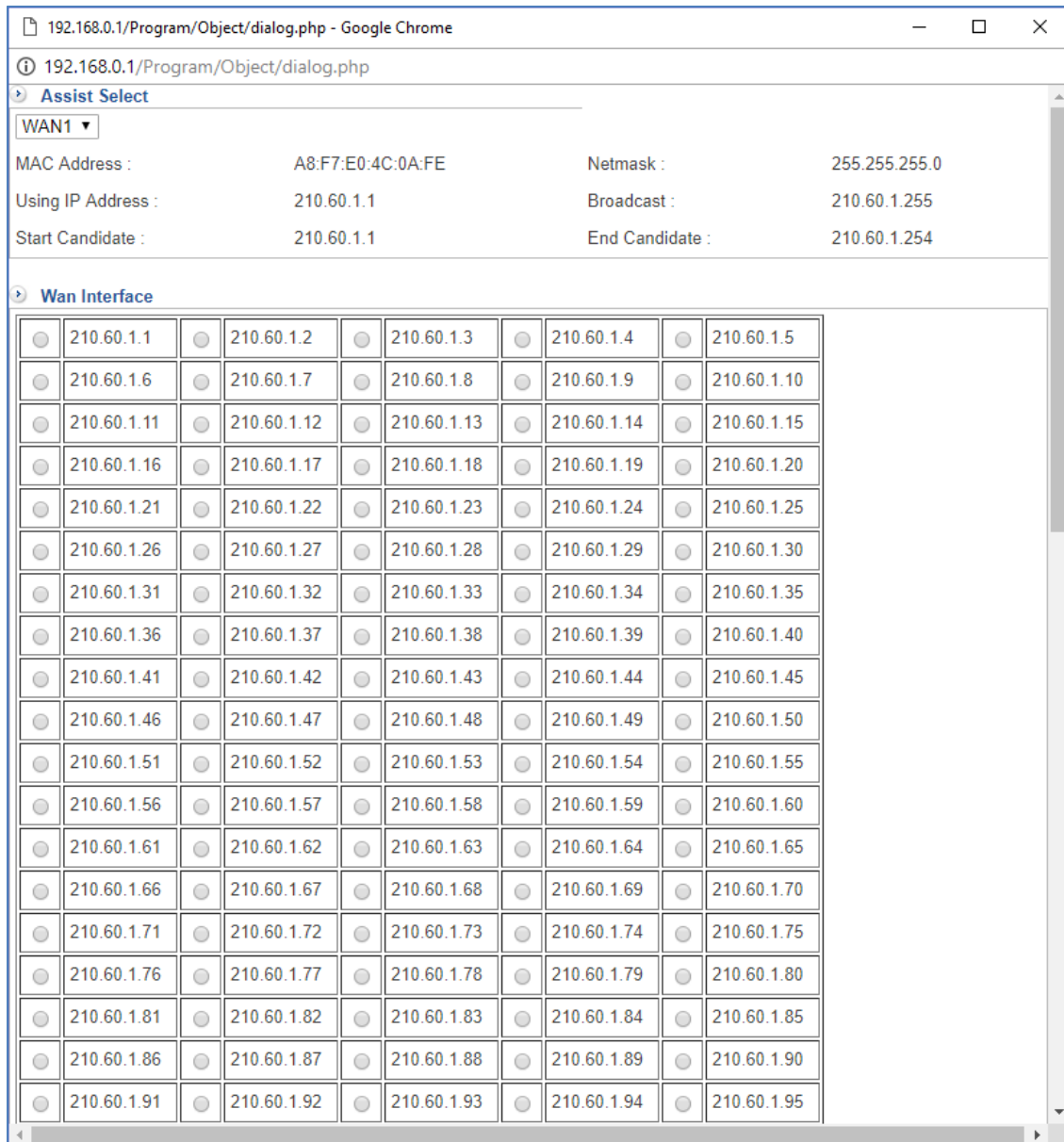
Select Objects > Virtual Server > Virtual Server.



- Click on  first.



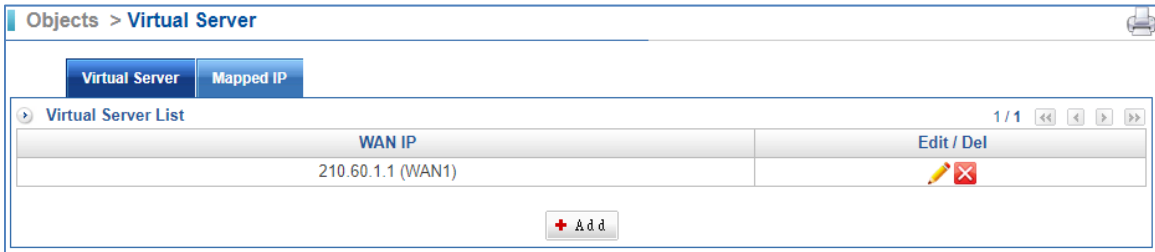
- Click on  to select IP address. Here, we suggest using “static IP”.



- It offers two options:
  1. WAN 1 interface.
  2. WAN 2 interface.



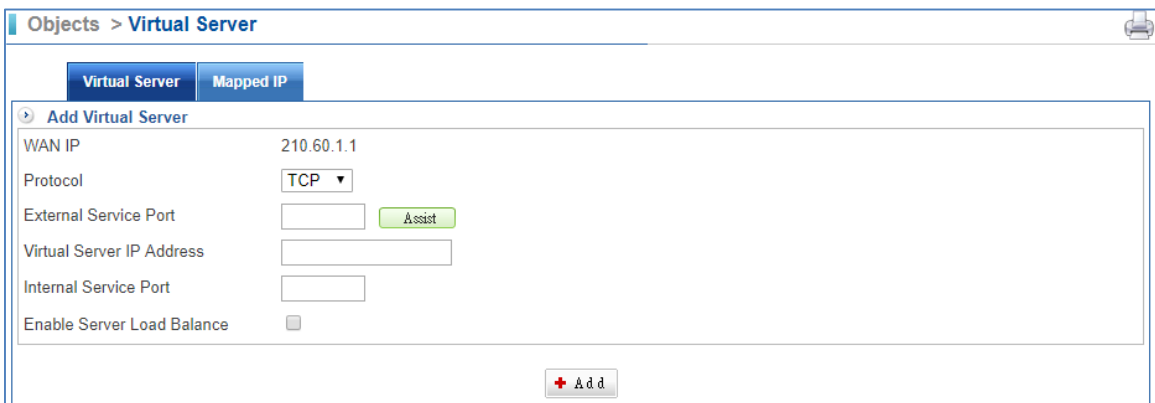
- After selected Virtual WAN IP.



- Setting Virtual Server WAN IP completed.
- Click on to edit content



- Click on , enter Virtual Server IP Address.



- User can click on to select External Service Port easily, (Figure 4-7.5) or 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.

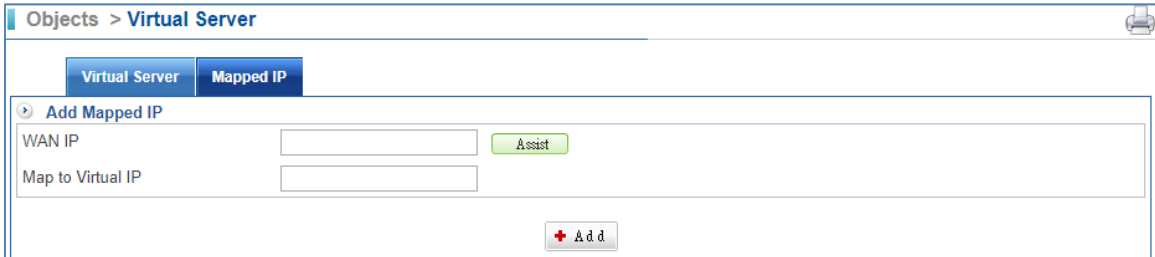
## 8.7.2 Mapped IP

Because of the intranet is transferring the private IP by NAT 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  first.



- Click on the Assist button to select WAN IP address. Here, we suggest using "static IP".

## Assist Select

WAN1 ▾

MAC Address : A8:F7:E0:4C:0A:FE      Netmask : 255.255.255.0  
 Using IP Address : 210.60.1.1      Broadcast : 210.60.1.255  
 Start Candidate : 210.60.1.1      End Candidate : 210.60.1.254

## Wan Interface

<input type="radio"/>	210.60.1.1	<input type="radio"/>	210.60.1.2	<input type="radio"/>	210.60.1.3	<input type="radio"/>	210.60.1.4	<input type="radio"/>	210.60.1.5
<input type="radio"/>	210.60.1.6	<input type="radio"/>	210.60.1.7	<input type="radio"/>	210.60.1.8	<input type="radio"/>	210.60.1.9	<input type="radio"/>	210.60.1.10
<input type="radio"/>	210.60.1.11	<input type="radio"/>	210.60.1.12	<input type="radio"/>	210.60.1.13	<input type="radio"/>	210.60.1.14	<input type="radio"/>	210.60.1.15
<input type="radio"/>	210.60.1.16	<input type="radio"/>	210.60.1.17	<input type="radio"/>	210.60.1.18	<input type="radio"/>	210.60.1.19	<input type="radio"/>	210.60.1.20
<input type="radio"/>	210.60.1.21	<input type="radio"/>	210.60.1.22	<input type="radio"/>	210.60.1.23	<input type="radio"/>	210.60.1.24	<input type="radio"/>	210.60.1.25
<input type="radio"/>	210.60.1.26	<input type="radio"/>	210.60.1.27	<input type="radio"/>	210.60.1.28	<input type="radio"/>	210.60.1.29	<input type="radio"/>	210.60.1.30
<input type="radio"/>	210.60.1.31	<input type="radio"/>	210.60.1.32	<input type="radio"/>	210.60.1.33	<input type="radio"/>	210.60.1.34	<input type="radio"/>	210.60.1.35
<input type="radio"/>	210.60.1.36	<input type="radio"/>	210.60.1.37	<input type="radio"/>	210.60.1.38	<input type="radio"/>	210.60.1.39	<input type="radio"/>	210.60.1.40
<input type="radio"/>	210.60.1.41	<input type="radio"/>	210.60.1.42	<input type="radio"/>	210.60.1.43	<input type="radio"/>	210.60.1.44	<input type="radio"/>	210.60.1.45
<input type="radio"/>	210.60.1.46	<input type="radio"/>	210.60.1.47	<input type="radio"/>	210.60.1.48	<input type="radio"/>	210.60.1.49	<input type="radio"/>	210.60.1.50
<input type="radio"/>	210.60.1.51	<input type="radio"/>	210.60.1.52	<input type="radio"/>	210.60.1.53	<input type="radio"/>	210.60.1.54	<input type="radio"/>	210.60.1.55
<input type="radio"/>	210.60.1.56	<input type="radio"/>	210.60.1.57	<input type="radio"/>	210.60.1.58	<input type="radio"/>	210.60.1.59	<input type="radio"/>	210.60.1.60
<input type="radio"/>	210.60.1.61	<input type="radio"/>	210.60.1.62	<input type="radio"/>	210.60.1.63	<input type="radio"/>	210.60.1.64	<input type="radio"/>	210.60.1.65
<input type="radio"/>	210.60.1.66	<input type="radio"/>	210.60.1.67	<input type="radio"/>	210.60.1.68	<input type="radio"/>	210.60.1.69	<input type="radio"/>	210.60.1.70
<input type="radio"/>	210.60.1.71	<input type="radio"/>	210.60.1.72	<input type="radio"/>	210.60.1.73	<input type="radio"/>	210.60.1.74	<input type="radio"/>	210.60.1.75
<input type="radio"/>	210.60.1.76	<input type="radio"/>	210.60.1.77	<input type="radio"/>	210.60.1.78	<input type="radio"/>	210.60.1.79	<input type="radio"/>	210.60.1.80
<input type="radio"/>	210.60.1.81	<input type="radio"/>	210.60.1.82	<input type="radio"/>	210.60.1.83	<input type="radio"/>	210.60.1.84	<input type="radio"/>	210.60.1.85
<input type="radio"/>	210.60.1.86	<input type="radio"/>	210.60.1.87	<input type="radio"/>	210.60.1.88	<input type="radio"/>	210.60.1.89	<input type="radio"/>	210.60.1.90
<input type="radio"/>	210.60.1.91	<input type="radio"/>	210.60.1.92	<input type="radio"/>	210.60.1.93	<input type="radio"/>	210.60.1.94	<input type="radio"/>	210.60.1.95

■ It offers two options:

1. WAN 1 interface.
2. WAN 2 interface.





Virtual Server Mapped IP

➤ Add Mapped IP



WAN IP	<input type="text" value="210.60.1.1"/>	<input type="button" value="Assist"/>
Map to Virtual IP	<input type="text" value="192.168.0.30"/>	

- After selecting WAN IP, please input the Map to Virtual IP.



Virtual Server Mapped IP

➤ Mapped IP List 1 / 1 << < > >>

WAN IP	Map to Virtual IP	Edit / Del
210.60.1.1 (WAN1)	192.168.0.30	 

- Setting Mapped IP completed.

## 8.8 Firewall Protection

### 8.8.1 Firewall Protection

Select Objects > Firewall Protection > Firewall Protection.

**Objects > Firewall Protection**

**Firewall Protection** | **Attack Log**

**SYN Attack Detection Setting :** Attention! The packet flow rate is approximate

Allow maximum flow  Packet / Second(s) (Range:1000~10000)  
Allow maximum flow for each source IP  Packet / Second(s) (Range:10~10000)  
Flow greater than maximum, block  Second(s) (Range:10~65536)

**ICMP Attack Detection Setting :**

Allow maximum flow  Packet / Second(s) (Range:1000~10000)  
Allow maximum flow for each source IP  Packet / Second(s) (Range:10~10000)  
Flow greater than maximum, block  Second(s) (Range:10~65536)

**UDP Attack Detection Setting :**

Allow maximum flow  Packet / Second(s) (Range:1000~10000)  
Allow maximum flow for each source IP  Packet / Second(s) (Range:10~10000)  
Flow greater than maximum, block  Second(s) (Range:10~65536)

**IP address block :**

Source IP address   
Destination IP address   
(ex. 192.168.0.1 or 192.168.0.1/24) (ex. 192.168.0.1 or 192.168.0.1/24)

**IP address exception :**

Source IP address   
Destination IP address   
(ex. 192.168.0.1 or 192.168.0.1/24) (ex. 192.168.0.1 or 192.168.0.1/24)

**Other items :**

<input type="checkbox"/> Block IP Options	<input type="checkbox"/> Block Land Attack	<input type="checkbox"/> Block Smurf Attack
<input type="checkbox"/> Block Trace Route	<input type="checkbox"/> Block Fraggles (UDP broadcast)	<input type="checkbox"/> Block Tear Drop Attack
<input type="checkbox"/> Block ICMP Fragment Attack	<input type="checkbox"/> Block Ping of Death Attack	<input type="checkbox"/> Block TCP Flags
<input type="checkbox"/> Block SYN Fragment Packet	<input type="checkbox"/> Detect unknown protocol packet	

- SYN attack detection: SYN Flood is a popular attack way. DoS and DDoS are TCP protocols. Hackers like using this method to make a counterfeit of connection, and the CPU and memory, and so on.
- ICMP attack detection: ICMP is kind of a pack of TCP/IP; its important function is to 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.

## 8.8.2 Attack Log

Select Objects > Firewall Protection > Attack Log.

**Objects > Firewall Protection**

**Firewall Protection** **Attack Log**

**Search Condition :**

Time: 2018-01-03 00:00 - 2018-01-03 23:59

Type: All

Attacker IP:

Victim IP:

Search

1 / 0 << < > >> Export Export All

Time	Type	Protocol	Port	Interface	Attacker IP	Victim IP
------	------	----------	------	-----------	-------------	-----------

## 8.9 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 Internet. In this section, it offers some authentication modes, Local Users, User Group, External Auth Settings which include AD 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 they have done.

### 8.9.1 Auth Setting

Select Objects > Authentication > Auth Setting.

**Objects > Authentication**

Auth Setting | Page Settings | Local User | POP3, RADIUS User | AD User | User Group | Log

Status

**Authentication General Setting**

Authentication port: 82 (range: 1 ~ 65535, 0 means authentication disabled)

Authentication Page: [https://\[LAN or DMZ IP Address\]:82](https://[LAN or DMZ IP Address]:82), [http://\[LAN or DMZ IP Address\]:83](http://[LAN or DMZ IP Address]:83)

Authentication Connection Protocol:  HTTP  HTTPS

Max concurrent connections: 256 (range: 10 ~ 256)

Idle timeout: 60 minute(s) (range: 1 ~ 1000)

Re-login after user has logged in for: 24 hour(s) (range: 0 ~ 24, 0 means no limit)

Allow change password:

Deny multi-login:

Temporarily block when login failed more than: 0 time(s) (0 means no limit)

IP blocking period: 0 minute(s) (0 means permanent blocking)

Permanently block when login failed more than: 0 time(s) (0 means no limit)

Unblocked IP: No blocked IP

Account expiration notification: Before 0 Days (0 represents the day)

Delete expired account: After 0 Days (0 means no limit, that is never deleted)

**Authentication Mode Setting**

Select authentication mode: L,A,P,R   
( L : Local , A : AD , P : POP3 , R : RADIUS Separate items with commas )

- Authentication port: The port number that authentication requires. Default port is 82.
- Max. concurrent connections: Input the max. concurrent connections

- Idle timeout: If an authenticated connection has been idle for a period of time, it will expire. The default is 60 minutes.
- Re-login after user has logged in for: Determines the valid time of an authentication. Authentication expires on the due time.
- 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: Input a number from 0 to 99.
- IP blocking period: Input a number from 0 to 99.
- Permanently block when login failed more than: Input a number from 0 to 99.
- Select Authentication Mode: Click on the Edit button to enter mode. These modes are separated by using comma.
  1. L: Local
  2. A: AD
  3. P: POP3
  4. R: RADIUS

## 8.9.2 Page Setting

Select Objects > Authentication > Page Setting.

**Objects > Authentication**

**Auth Setting** **Page Settings** Local User POP3, RADIUS User AD User User Group Log Status

**Default Setting**

Redirect successfully authenticated users to

whether to have read page

**Page Color Setting**

Content Block Background:  Word:

Foreground Block Background:  Word:

Background Block Background:

**Client Login Message** [Login Preview](#)

Subject

Content

Upload Logo  No file chosen

**Client Logged Message** [Logged Preview](#)

Logged Message

**Apply Bulletin Layout** 1/0

No.	Notes	IP/Netmask	Bulletin Group	Subject	Content	Logo	Preview
-----	-------	------------	----------------	---------	---------	------	---------

- 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 in website subject.
- Content: Enter some messages shown in the login screen. Leaving it blank will result in no message.
- Upload logo: This picture will show when users use Internet via the Internet authentication way. The Login screen shows before a user accesses a website.

## 8.9.3 Local User

Select Objects > Authentication > Local User.


Objects > Authentication

Auth Setting Page Settings Local User POP3, RADIUS User AD User User Group Log Status

User List Expired Log Account Choose File No file chosen Import 1 / 1 Export

Name	Account	Require Password Change at Next Login	Account Expiration Date
------	---------	---------------------------------------	-------------------------

+ Add Edit Del

- User List: If you have many accounts, you can click on “Choose File” to bring in accounts. After selecting, click on “Import”. Then, you do not have to enter account step by step.
- Click on  first.

Objects > Authentication

Auth Setting Page Settings Local User POP3, RADIUS User AD User User Group Log Status

Add User Account

Name (maximum 16 characters)

Account (maximum 16 characters)

Password (Please input 3 to 16 characters, not the same with account)

Password Strength Weak Fair Strong

Confirm Password

Require Password Change at Next Login

Account Expiration Date

+ Add

- Name: The user name for authentication.
- Account: The account for authentication.
- Password: The password for authentication.
- Confirm Password: The confirmation of password.
- Require Password Change at Next Login: If selected, the local authentication accounts can be forced to change their passwords at their next login attempt.
- Account Expiration Date: Sets the period of validity for a user's account.

## 8.9.4 POP3, RADIUS User

Select Objects > Authentication > POP3, RADIUS User.

Objects > Authentication

Auth Setting Page Settings Local User **POP3, RADIUS User** AD User User Group Log Status

POP3 Server List

Server	Protocol	Security	Port	Login with domain	Certification	Edit / Del
--------	----------	----------	------	-------------------	---------------	------------

+ Add

Radius Server List

Server	Edit / Del
--------	------------

+ Add

Please click "Add" to add POP3 or RADIUS server.

POP3 server:

Objects > Authentication

Auth Setting Page Settings Local User **POP3, RADIUS User** AD User User Group Log Status

Add Server

Domain Name  ex: gmail.com **Domain can not be repeated**

Server  ex: 74.125.53.109 or pop.gmail.com

Login with domain

Protocol  POP3  IMAP

Security  Normal  TLS  SSL

Port

Certification  Ignore

Connection Test

Save

RADIUS server:

Objects > Authentication

Auth Setting Page Settings Local User **POP3, RADIUS User** AD User User Group Log Status

Add RADIUS Setting

RADIUS Name  ex: my\_radius **RADIUS can not be repeated, use english chars without empty**

Server  ex: 12.34.56.78 或 your.radius.com

Port  ( Range: 1025 - 65535 )

Shared Secret

Interface

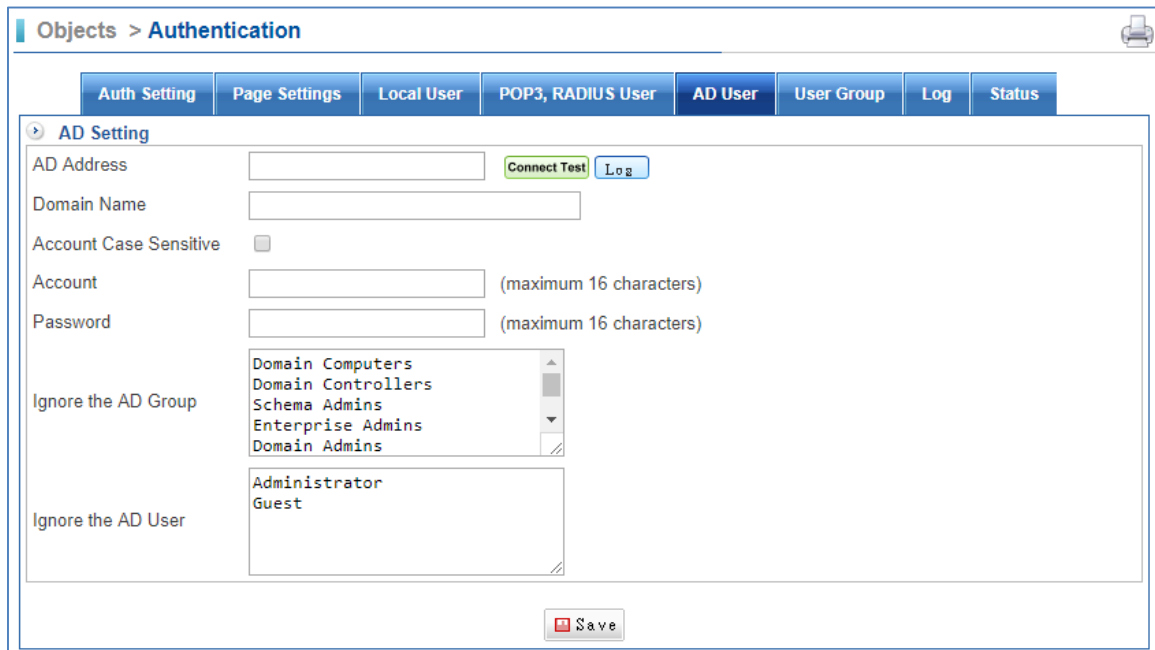
Connection Test

Save



## 8.9.5 AD User

Select Objects > Authentication > AD User.



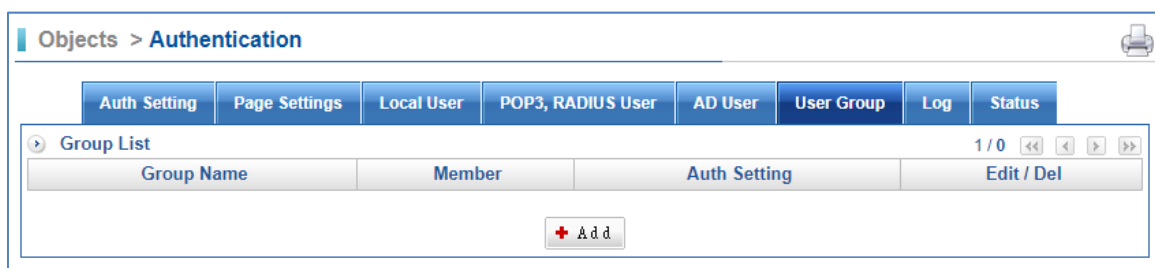
The screenshot shows the 'Objects > Authentication' page with the 'AD User' tab selected. The 'AD Setting' section contains the following fields and controls:

- AD Address: Text input field with 'Connect Test' and 'Log' buttons.
- Domain Name: Text input field.
- Account Case Sensitive: Checkmark.
- Account: Text input field with '(maximum 16 characters)'.
- Password: Text input field with '(maximum 16 characters)'.
- Ignore the AD Group: List box containing 'Domain Computers', 'Domain Controllers', 'Schema Admins', 'Enterprise Admins', and 'Domain Admins'.
- Ignore the AD User: List box containing 'Administrator' and 'Guest'.
- Save: Button at the bottom.

- AD Address: The IP address of the AD server.
- Domain Name: The domain name of the AD server, such as ad.com.tw.
- Account: The account for authentication.
- Password: The password for authentication.
- Ignore the AD Group/User: Input the AD group/user which is not used. Leave it blank, all group/user will be used.

## 8.9.6 User Group

Select Objects > Authentication > User Group.



The screenshot shows the 'Objects > Authentication' page with the 'User Group' tab selected. The 'Group List' section contains the following elements:

- Group List: Table with columns 'Group Name', 'Member', 'Auth Setting', and 'Edit / Del'.
- 1/0: Page indicator.
- Navigation buttons: '<<', '<', '>', '>>'.
- Add: Button with a red plus sign.

- Click on  first.



Auth Setting
Page Settings
Local User
POP3, RADIUS User
AD User
User Group
Log
Status

➤ Add Group Member

Group Name

Auth Setting  General setting  
 User defined setting

Select user type

Search

=====all users=====

Search

=====selected users=====

- Group name: Enter some words for recognition.
- Auth Settings:
  1. General setting: Using Auth Settings.
  2. Use defined settings: User is able to define the User Group by himself.
- Select the user type: L means Local, A means AD, P means POP3, R means RADIUS.

# Chapter 9. Network Services

## 9.1 DHCP

### 9.1.1 DHCP User List

Select Network Services > DHCP > DHCP User List.

Network Services > DHCP

Interface: LAN

The number of unleased IP address : 244

IP Address	MAC Address	Start Time	End Time	Hostname	Status
192.168.0.109	48:4B:AA:88:F0:4D	2018-01-11 08:47:05	2018-01-13 20:47:05	lee	
192.168.0.117	0C:38:3E:1E:C8:52	2018-01-11 09:14:32	2018-01-13 21:14:32		
192.168.0.116	A8:F7:E0:12:AB:00	2018-01-11 15:26:44	2018-01-14 03:26:44		
192.168.0.114	38:D5:47:32:9A:9C	2018-01-11 15:39:04	2018-01-14 03:39:04	android-8517d3c1708a9c8	
192.168.0.108	00:30:4F:A6:92:AE	2018-01-11 18:05:02	2018-01-14 06:05:02	ICA-4210P	
192.168.0.2	00:30:4F:27:60:EF	2018-01-11 20:32:04	2018-01-14 08:32:04	ENM-ESTHER	
192.168.0.110	08:D8:33:CE:84:05	2018-01-12 03:50:12	2018-01-14 15:50:12	android-e53eae6fafeddec4	
192.168.0.106	00:EE:BD:B4:13:6D	2018-01-12 08:49:48	2018-01-14 20:49:48	android-7bed67ccf1e404e5	
192.168.0.113	00:F7:6F:E5:B4:21	2018-01-12 09:48:53	2018-01-14 21:48:53	Yien-Weng	

### 9.1.2 DHCP Server

Select Network Services > DHCP > DHCP Server.

Network Services > DHCP

Interface: LAN

Interface Info:

Physical Interface	eth0	MAC Address	A8:F7:E0:4C:0A:FD
IP Address	192.168.0.1/24	Broadcast	192.168.0.255

DHCP Server Setting:

Start Address of IP Range 1	192.168.0.1	End Address of IP Range 1	192.168.0.254
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 WINS		Secondary WINS	
Lease time(minutes)	3600	Max lease time(minutes)	3600
Default Gateway	192.168.1.254	Enabled	<input checked="" type="checkbox"/>
Domain Name	internal.example.org		

Save

- 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.

- 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.
- 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.
- Max lease time (mins): In order to avoid using the same IP, how long can we also establish the same IP max lease time.
- Enabled: Check the box to enable the DHCP server.

### 9.1.3 DHCP Static IP

Select Network Services > DHCP > DHCP Static IP.



## 9.2 DDNS

Select Network Services > DDNS > DDNS Server.



- Click on  first.

Network Services > DDNS

DDNS Server

Add Host :

Service Provider: planetddns.com  Easy mode

Hostname:  planetddns.com

Wan: WAN1 IP: 192.168.1.111, MAC: A8:F7:E0:4C:0A:FE

Account:

Password:

Comment:

Enabled:

+ Add

- Service Provider: Choose the DDNS provider.

planetddns.com ▼

planetddns.com

dhs.org

dyndns.org

dyns.cx

hn.org

no-ip.org

zonedit.com

easydns.com

ods.org

3322.org

ezip.net

tzo.com

justlinux.com

88ip.net

changeip.org

- Hostname: The hostname and domain as registered with your DDNS provider.
- WAN: Select the WAN interface.
- 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. If enabled, it will automatically connect to the dynamic DNS provider and tell it the new IP address after every address change.

Network Services > DDNS

DDNS Server

DDNS List : Log Refresh 1 / 1

Mark	Update Status	Service Provider	Hostname	Account	Wan	Enabled	Comment
<input type="checkbox"/>	✓	planetddns.com	88888.planetddns.com	keithy	WAN1	✓	

+ Add Edit Del

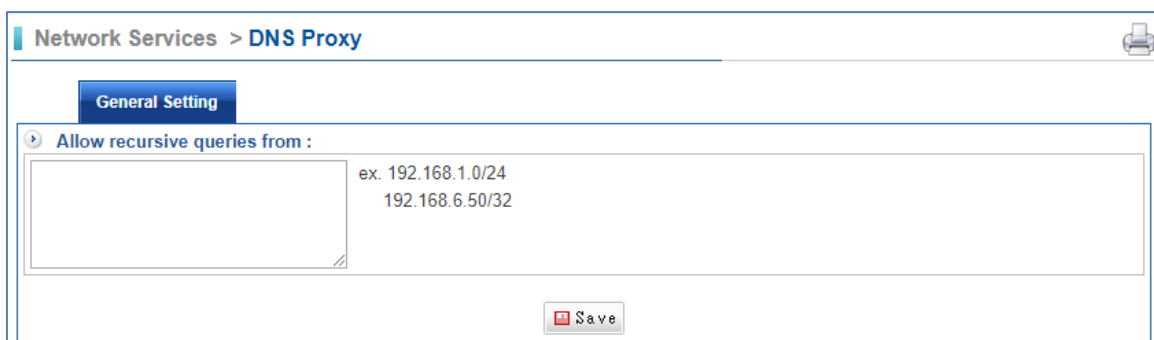
## 9.3 DNS Proxy

Short for Domain Name System (or Service or Server), an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address.

For example, the domain names translate to IP address. Therefore, "www.planet.com.tw" might translate to "59.125.xxx.xxx"

The DNS system is, in fact, its own network. If one DNS server doesn't know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

Select Network Services > DNS Proxy > General Setting.



- Click on  to allow recursive queries from these IP addresses.

## 9.4 Web Services

Select Network Services > WEB Services> WEB.

Network Services > WEB Service

WEB Non-standard HTTP Log Non-standard HTTP Exclude

WEB Anti-Virus Setting :

Max. Concurrent Sessions  (Range: 10 ~ 400)

Timeout  (Range : 20 ~ 600 Seconds)

Max. Scan File Size( kb )  (Range: 1 ~ 1024)

Listen Port  (Range: 1 ~ 65535) ?

Virus Engine  ClamAV

Warning Setting [Preview](#)

Warning Subject

Warning Message

- Max. Concurrent Sessions: Limit the max. concurrent sessions.
- Timeout: Set the timeout range. Default is 300 seconds.
- Max. Scan File (KB): Limit the max. scan file size.
- Listen Port: Default is 80.
- Virus Engine: The virus engine is ClamAV.
- Warning Setting: Click on Preview link, another pop-up window will demonstrate the warning subject.
- Warning Subject: Enter some words to warn users.
- Warning Message: Enter some messages to warn users.

## 9.5 FTP Services

Select Network Services > FTP Services > FTP.

Network Services > FTP Service

FTP

FTP Anti-Virus Setting :

Max. size of scanned files ( KB )  Kbytes

Listen Port  (Range: 1 ~ 65535) ?

Support active FTP connection mode

Virus Engine  ClamAV

Extension file whitelist

- Max. size of scanned files (KB): It determines of which size an email is to be not scanned for viruses and spam.
- Listen Port: Default is 80.
- Support active FTP connection mode: Check the box to support active FTP mode.
- Virus Engine: The virus engine is ClamAV.
- Extension file whitelist : The extension file will not be inspected.

## 9.6 High Availability

The CS-950 can be easily run in HA (High Availability) mode. At least two CS-950 machines with the same firmware version are required for HA mode: one assumes the role of the active (Master) device while the others are standby (Backup) devices. If the Master device fails, an election between the Backup will take place and one of them will be promoted to the new Master, providing for transparent failover.

Select Network Services > High Availability > High Availability.

- To set up such a HA configuration, first set up the CS-950 that is going to be the Master: At this point the Backup mode cannot be reached anymore via its old IP address (factory default or previous LAN address).

The screenshot shows the configuration interface for High Availability. At the top, there are tabs for 'High Availability' and 'Sync Log'. Below the tabs is a 'Setup' section with a 'Refresh Every 30 seconds' indicator and a 'Refresh' button. The 'Setup' section contains the following fields:

- Enable:** A checkbox that is currently unchecked.
- Mode:** A dropdown menu with 'Master' selected.
- Manage IP:** An empty text input field.
- Remote IP:** An empty text input field.

At the bottom of the 'Setup' section is a 'Save' button.

1. Select Enable tick box to start function, and set mode to Master.
  2. The Manage IP is used to log in to the Master device whether the active device is Master or Backup. The Manage IP of Master device and Backup device should be the same.
  3. The Remote IP is the Backup device's IP.
  4. Finally, click on "Save" to activate the settings.
- Set up the CS-950 that is going to be the backup: At this point an extra panel appears where the Backup-specific settings can be configured.



Network Services > High Availability

High Availability Sync Log

Setup : Refresh Every 30 seconds Refresh

Enable

Mode Backup ▾

Manage IP

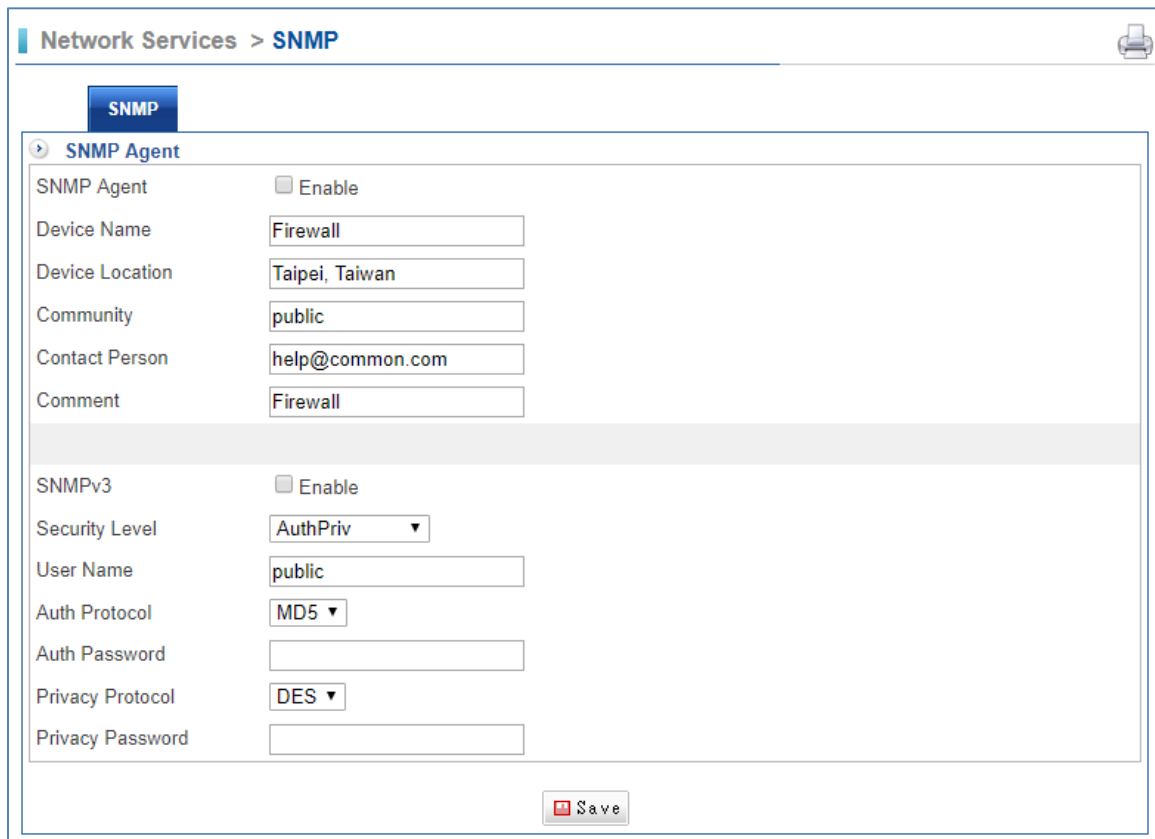
Remote IP

Save

1. Select Enable tick box to start function, and set mode to Backup.
  2. The Manage IP is used to login the Master device whether the active device is Master or Backup. The Manage IP of Master device and Backup device should be the same.
  3. The Remote IP is the Master device's IP.
  4. Finally, click on "Save" to activate the settings.
- In conclusion, the Backup mode cannot be reached anymore via its old IP address (factory default or previous LAN address) since it is in standby mode. It is connected to the Master mode only through the management network.

## 9.7 SNMP

Select Network Services > SNMP > SNMP.



The screenshot shows a web-based configuration interface for SNMP. The breadcrumb navigation at the top reads "Network Services > SNMP". A blue button labeled "SNMP" is visible. Below it, the "SNMP Agent" section is expanded, showing a list of configuration fields. The "SNMPv3" section is also visible below a horizontal separator.

Section	Field	Value
SNMP Agent	Enable	<input type="checkbox"/>
	Device Name	Firewall
	Device Location	Taipei, Taiwan
	Community	public
	Contact Person	help@common.com
	Comment	Firewall
SNMPv3	Enable	<input type="checkbox"/>
	Security Level	AuthPriv
	User Name	public
	Auth Protocol	MD5
	Auth Password	
	Privacy Protocol	DES
	Privacy Password	

At the bottom right of the configuration area, there is a "Save" button with a red icon.

## 9.8 Remote Syslog Server

UTM 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.

Select Network Services > Remote Syslog Server > Remote Connect Setup.

The screenshot shows a web-based configuration interface. At the top, there is a breadcrumb trail: "Network Services > Remote Syslog Server". A blue button labeled "Remote Connect Setup" is visible. Below this, there is a section titled "Remote Connect Setup" with a dropdown arrow. It contains three fields: "Enable" with an unchecked checkbox, "Server IP" with an empty text box, and "Server Port" with an empty text box and "(UDP 514)" to its right. Below this section is another section titled "Log Item" with a dropdown arrow, containing two unchecked checkboxes: "Packet Tracing Log" and "IDP Log". At the bottom center of the form is a "Save" button with a red icon.

- Enable: Check the box to enable the function.
- Server IP: Enter Server IP address.
- Server Port: Enter Server Port.

# Chapter 10. Advanced Protection

## 10.1 Anomaly IP Analysis

### 10.1.1 Log Anomaly

Select Advanced Protection > Anomaly IP Analysis > Log Anomaly.

Advanced Protection > Anomaly IP Analysis

Log Anomaly | Notify Anomaly | Block Anomaly | Trusted IP | Anomaly Log | Block List

Inside to Outside Anomaly (Range : 1 ~ [Notify Anomaly >> Inside to Outside Anomaly])

- Connection Session exceeds 100 and continues 120 seconds
- Upload flow exceeds 512 Kbps and continues 120 seconds
- Download flow exceeds 1024 Kbps and continues 120 seconds

Outside to Inside Anomaly (Range : 1 ~ [Notify Anomaly >> Outside to Inside Anomaly])

- Connection Session exceeds 100 and continues 120 seconds
- Upload flow exceeds 512 Kbps and continues 120 seconds
- Download flow exceeds 1024 Kbps and continues 120 seconds


Save


- Inside to Outside Anomaly/Outside to Inside Anomaly: Input the suitable value and check the box to enable the rule.

### 10.1.2 Notify Anomaly


It is recommended to set SMTP Server (Configuration > Administration > SMTP Server) and Notification (Configuration > Notification > Notification) functions as enable first.

Select Advanced Protection > Anomaly IP Analysis > Notify Anomaly.

**Advanced Protection > Anomaly IP Analysis** 

**Inside to Outside Anomaly**  (Range : [Log Anomaly > Inside to Outside Anomaly] ~ [Block Anomaly > Inside to Outside Anomaly] )

Connection Session exceeds  and continues  seconds  
 Upload flow exceeds  Kbps and continues  seconds  
 Download flow exceeds  Kbps and continues  seconds

**Outside to Inside Anomaly**  (Range : [Log Anomaly > Outside to Inside Anomaly] ~ [Block Anomaly > Outside to Inside Anomaly] )

Connection Session exceeds  and continues  seconds  
 Upload flow exceeds  Kbps and continues  seconds  
 Download flow exceeds  Kbps and continues  seconds

- Inside to Outside Anomaly/Outside to Inside Anomaly: Input the suitable value and check the box to enable the rule.

## 10.1.3 Notify Anomaly

Select Advanced Protection > Anomaly IP Analysis > Block Anomaly.

**Advanced Protection > Anomaly IP Analysis**

Log Anomaly | **Notify Anomaly** | **Block Anomaly** | Trusted IP | Anomaly Log | Block List

**Inside to Outside Anomaly** (Range : [Notify Anomaly >> Inside to Outside Anomaly] ~ 100000 )

- Connection Session exceeds 300 and continues 120 seconds
- Upload flow exceeds 512 Kbps and continues 120 seconds
- Download flow exceeds 1024 Kbps and continues 120 seconds

**Outside to Inside Anomaly** (Range : [Notify Anomaly >> Outside to Inside Anomaly] ~ 100000 )

- Connection Session exceeds 300 and continues 120 seconds
- Upload flow exceeds 512 Kbps and continues 120 seconds
- Download flow exceeds 1024 Kbps and continues 120 seconds

**Action**

- Block 0 minute(s)
- Block all day
- Block until administrator to unlock
- Bandwidth Limited 0 minute(s)
- Bandwidth Limited all day
- Bandwidth Limited until administrator to unlimit

**Advanced Setup**

Bandwidth Limited Upload 64 Kbps, Download 128 Kbps

Block Message: Your IP is currently blocked, please contact the system administrator

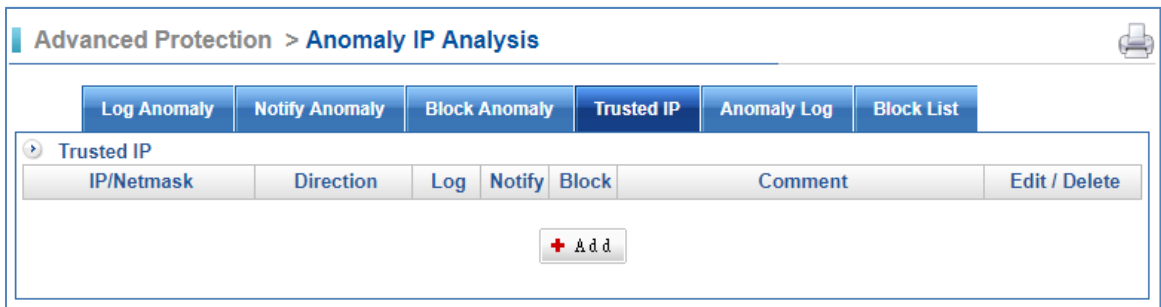
Save

- Inside to Outside Anomaly/Outside to Inside Anomaly: Input the suitable value and check the box to enable the rule.
- Action: select an action for blocking the IP.
- Advanced Setup: Set the max. bandwidth and the block message.

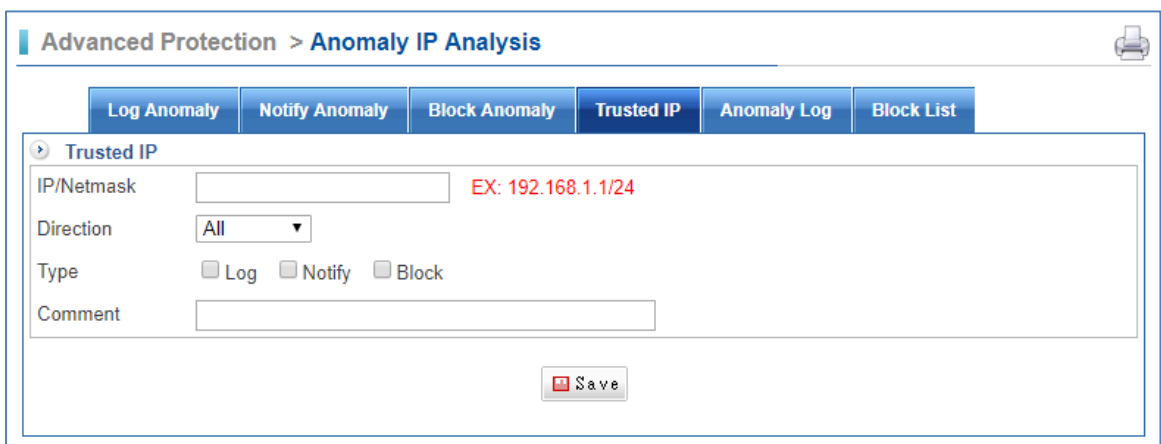
## 10.1.4 Trusted IP

If user has some IP addresses which do not want to be restricted by this function, user could enter the IP ranges. After that those IPs you entered would not be detected anomaly analysis.

Select Advanced Protection > Anomaly IP Analysis > Trusted IP.

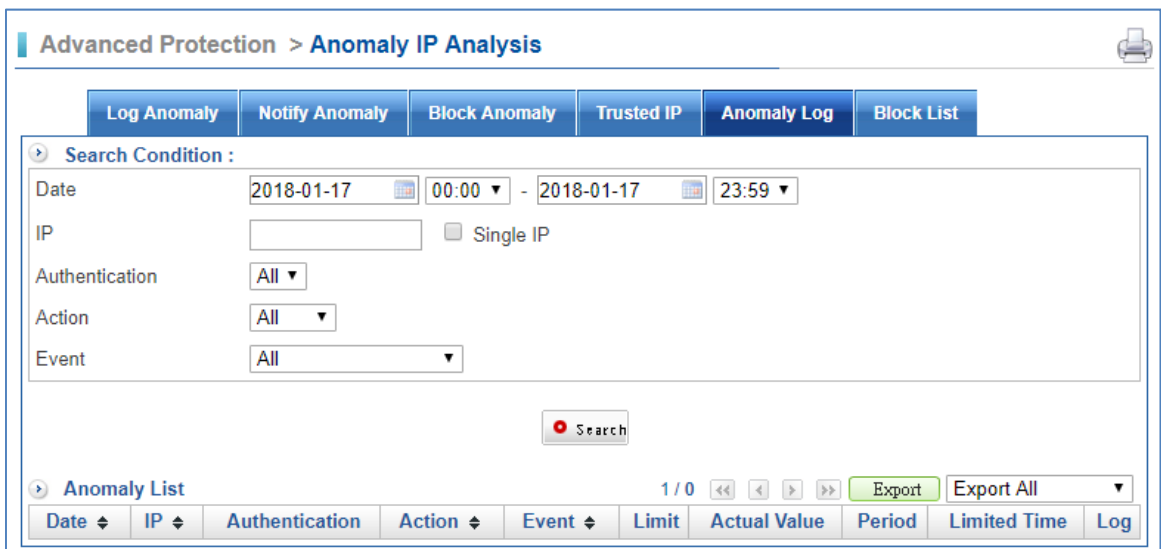


■ Click on  first.



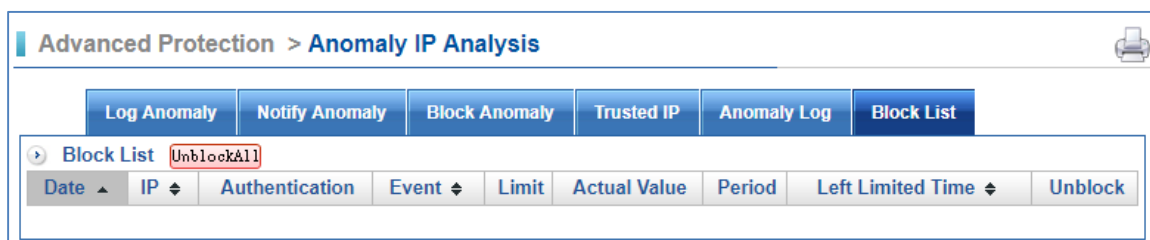
### 10.1.5 Anomaly Log

Select Advanced Protection > Anomaly IP Analysis > Anomaly Log.



## 10.1.6 Block List

Select Advanced Protection > Anomaly IP Analysis > Block List.



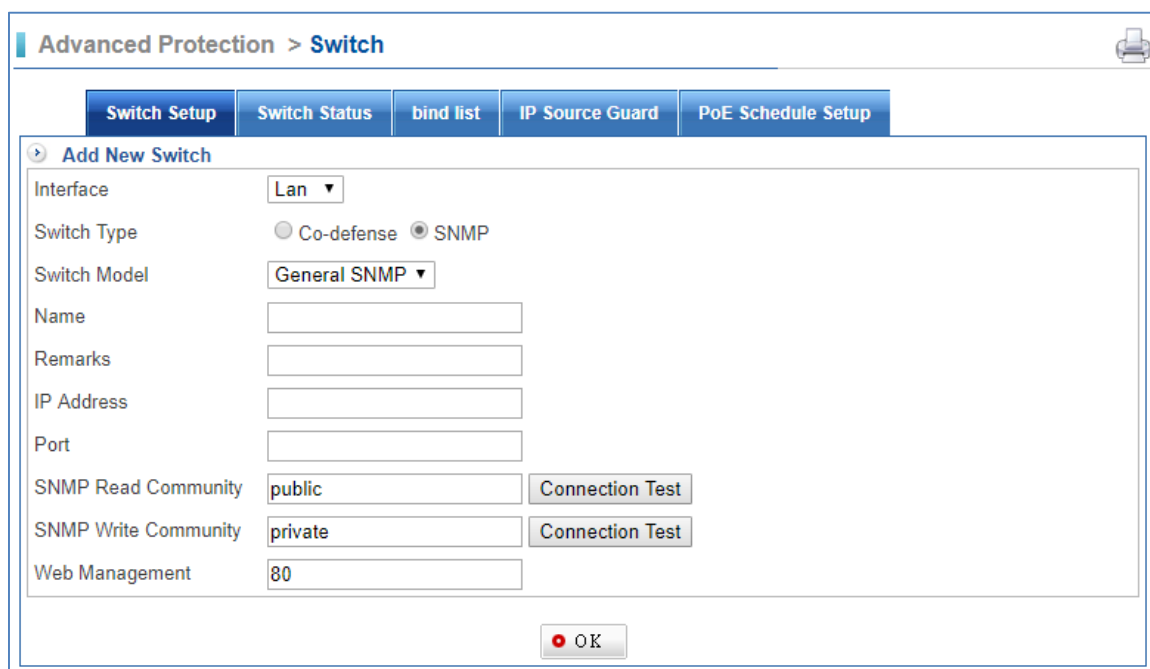
## 10.2 Switch

### 10.2.1 Switch Setup

Select Advanced Protection > Switch > Switch Setup.



- Click on  first.



- Interface: Choose your switch at which UTM interface.
  1. Lan.
  2. DMZ.
- Switch Type: Choose the kind of function you need.



## 1. Co-defense.



Switch Setup | Switch Status | bind list | IP Source Guard | PoE Schedule Setup

➤ Add New Switch

Interface	Lan ▾
Switch Type	<input checked="" type="radio"/> Co-defense <input type="radio"/> SNMP
Switch Model	Cisco3560e ▾
Name	<input type="text"/>
Remarks	<input type="text"/>
IP Address	<input type="text"/>
Advanced Command	<input checked="" type="radio"/> Telnet <input type="radio"/> SSH
Command Port	23
Login Account	<input type="text"/>
Login Password	<input type="text"/>
Enable Password	<input type="text"/> <input type="button" value="Connection Test"/>
Bind mode	<input checked="" type="radio"/> IP + MAC + PORT <input type="radio"/> MAC + PORT
Port	<input type="text"/>
SNMP Read Community	public <input type="button" value="Connection Test"/>
SNMP Write Community	private <input type="button" value="Connection Test"/>
Web Management	80

## 2. SNMP.

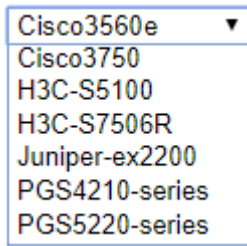


Switch Setup | Switch Status | bind list | IP Source Guard | PoE Schedule Setup

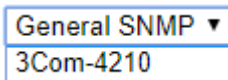
➤ Add New Switch

Interface	Lan ▾
Switch Type	<input type="radio"/> Co-defense <input checked="" type="radio"/> SNMP
Switch Model	General SNMP ▾
Name	<input type="text"/>
Remarks	<input type="text"/>
IP Address	<input type="text"/>
Port	<input type="text"/>
SNMP Read Community	public <input type="button" value="Connection Test"/>
SNMP Write Community	private <input type="button" value="Connection Test"/>
Web Management	80

- Switch Model: select one, depending on what you choose on switch Type
  1. Co-defense: The current CS-950 supports PLANET GS-4210 series, GS-5220 series and other brands.



2. SNMP: The CS-950 supports these types: General SNMP and other brands.



- Name: Enter Switch model name.
- Remarks: Enter any words for recognition.
- IP Address: Enter switch IP address.
- Port: Total switch port.
- SNMP Read Community: Default read community is "public". Administrator could click on  to check connection.
- SNMP Write Community: Default write community is "private". Administrator could click on  to check connection.
- Web Management: Enter switch web management port. Default port is 80.

## 10.2.2 Switch Status

Select Advanced Protection > Switch > Switch Status.



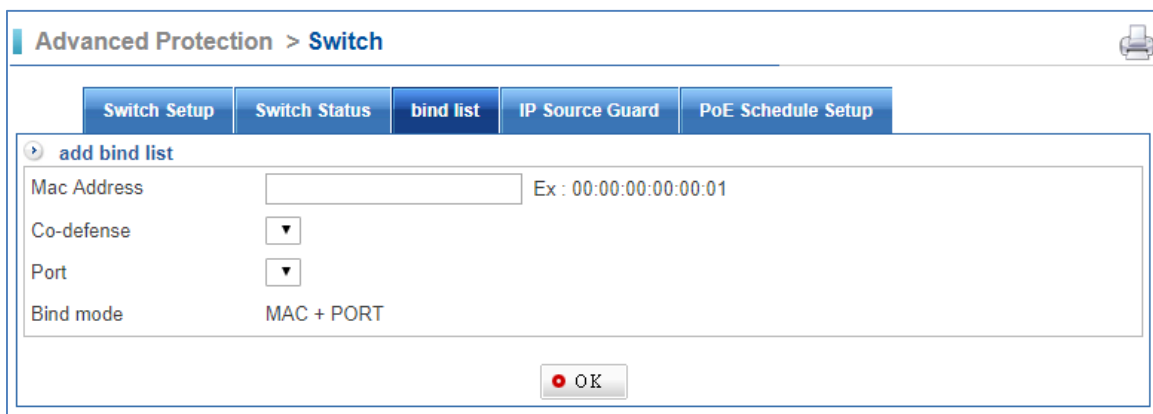
## 10.2.3 Bind list

Some switches have IP/MAC binding function. It offers much safer and easier network management systems to monitor network-attached devices for conditions that warrant administrative attention.

Select Advanced Protection > Switch > Bind list.



■ Click on  first.



■ Add bind list: Input the switch information.



Internal user will not be allowed to surf Internet if internal user changes device IP, MAC, or switch port.

## 10.3 Intranet Protect

It has been the most difficult for UTM Gateway to detect broadcast package sent out on the local network such as ARP spoofing and private DHCP server because of congenital defects of communication protocols.

The CS-950 can effectively detect the man-in-the-middle attack. With a Co-defense switch, physical IP destination can be marked.

## 10.3.1 Spoofing Setup

Select Advanced Protection > Intranet Protect > Spoofing Setup.

The screenshot shows the 'Advanced Protection > Intranet protect' configuration page. It features a navigation bar with tabs for 'Spoofing Setup', 'ARP Spoofing Log', 'MAC Collision Log', 'IP Collision Log', and 'Lock Status'. The main content is organized into several sections:

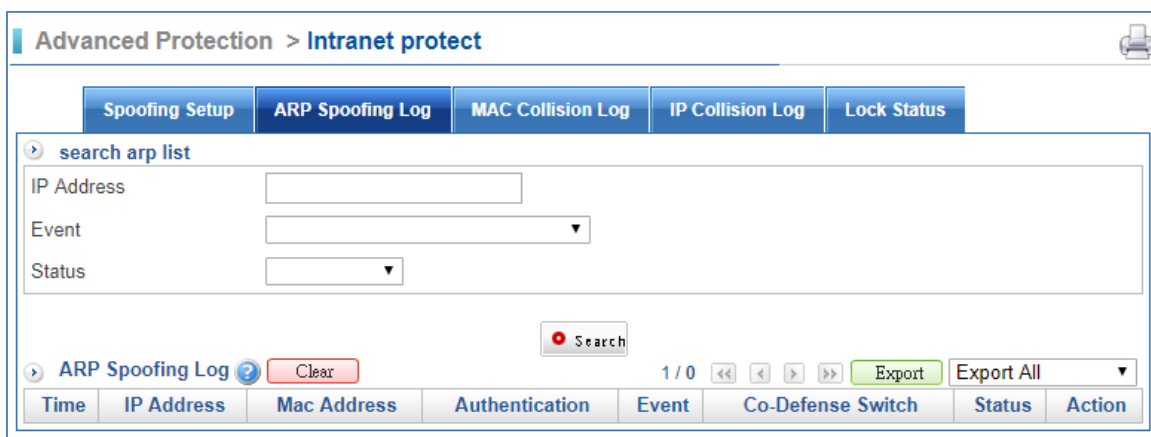
- Detection Interface:** Includes checkboxes for 'Lan' and 'Dmz'.
- ARP Spoofing Alert Value:** A text input field is set to '100' with a note '(Minimum value is 50)'. Below it is an 'Automatically Block by Switch' checkbox and a port selection dropdown set to 'Advanced Management Switch Port'.
- True Address:** A large empty text area for specifying true addresses.
- Collision Detection : IP:** Similar to the ARP section, with an 'IP Address Collision Detection' checkbox and an 'Automatically Block by Switch' checkbox.
- Collision Detection : MAC:** Includes a 'MAC Address Collision Detection' checkbox with a value of '3' and the text 'times / hour. Block it by switch', along with an 'Automatically Block by Switch' checkbox.
- Co-defense:** Features a 'Linked abnormal IP block list Port Close' checkbox.
- Notify Item:** A list of checkboxes for 'Linked abnormal IP block', 'Arp Protection', 'IP collision', and 'MAC collision'.

A 'Save' button is located at the bottom right of the configuration area.

- Detection Interface: Select LAN or DMZ. The interface should be NAT.
- ARP Spoofing Alert Value: If the source IP address exceeds the amount of ARP packets, more than the value, the function will be triggered.
- Collision Detection IP/MAC: Check the box to enable the detection.
- Notify Item: If the Linked abnormal IP block/Arp Protection/IP collision/MAC collision is detected, it will be shown in the log.

### 10.3.2 ARP Spoofing Log

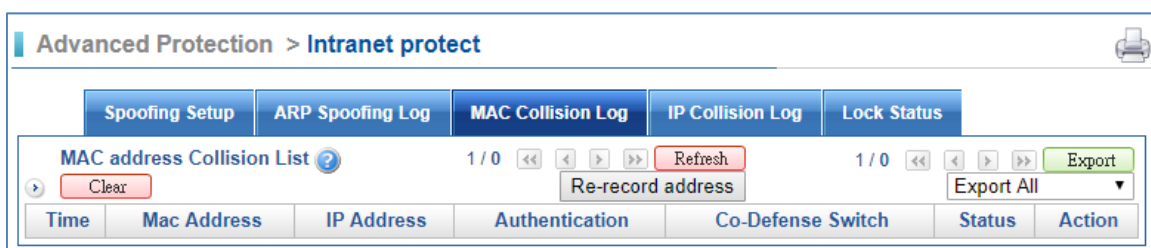
Select Advanced Protection > Intranet Protect > ARP Spoofing Log.



- Search ARP list: User is able to search ARP list by IP address/Event/Status.
- ARP Spoofing Log: The ARP spoofing log will be shown here.

### 10.3.3 MAC Collision Log

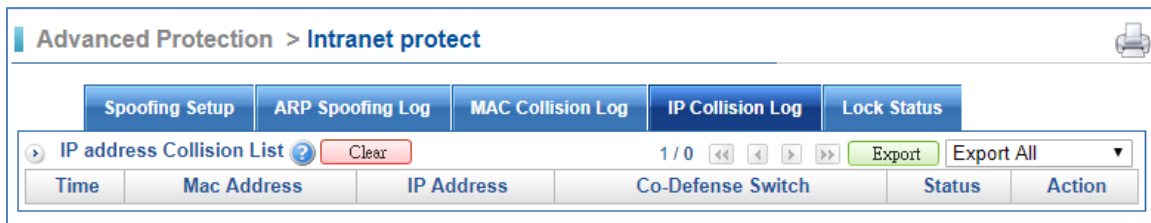
Select Advanced Protection > Intranet Protect > MAC Collision Log.



- MAC Collision Log: The MAC collision log will be shown here.

### 10.3.4 IP Collision Log

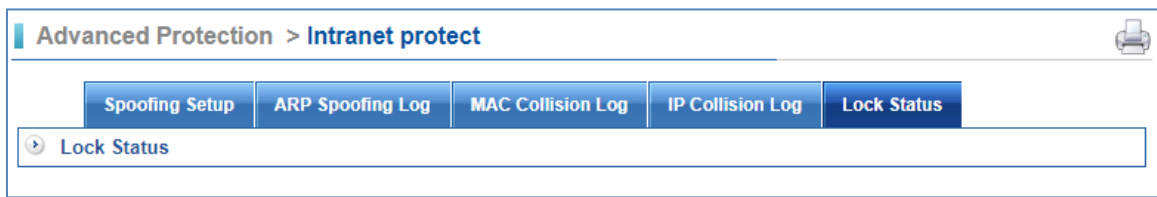
Select Advanced Protection > Intranet Protect > IP Collision Log.



- IP Collision Log: The IP collision log will be shown here.

## 10.3.5 Lock Status

Select Advanced Protection > Intranet Protect > Lock Status.



- Lock Status: The Lock status will be shown here.

# Chapter 11. Mail Security

## 11.1 Filter & Log

### 11.1.1 Filter & Log

Select Mail Security > Filter & Log > Filter & Log.

Mail Security > Filter & Log

Filter & Log | Valid Account Setting | Graylist and IP Resolved | Traffic Blocking | SMTP Blocking IP

Incoming Mail Anti-Virus and Anti-Spam

Function Select All  Anti-Virus  Anti-Spam

LAN and DMZ Outgoing Mail Anti-Virus and Anti-Spam

Send Mail Anti-Virus

Retrieve Mail Select All  Anti-Virus  Anti-Spam

SMTP Log Setting

Incoming  Disable  Accept  All

Outgoing  Disable  Fail  All

Log Type  Simple

Mail Record Setting

LAN and DMZ Retrieve Mail Mail file larger than  KB do not scan Anti-Virus and Anti-Spam, only check black and whitelist

Source IP replaced by WAN IP

LAN,DMZ Incoming Mail(Send)  Enable  Disable

LAN,DMZ Outgoing Mail(Send)  Enable  Disable

Release to carry the subject

Join Subject  Enable  Disable

Subject  ex: \$Y-\$m-\$d \$H:\$i:\$s

Save

- Incoming Mail Anti-Virus and Anti-Spam: All incoming mails from WAN to LAN or WAN to DMZ will be filtered for malicious mails.



If user needs to check the Mail log, please set the Policy of WAN to LAN or WAN to DMZ as enabled.

Path: Policy > WAN Policy > WAN to LAN or WAN to DMZ.

Policy

Protocol: ALL

Destination Service Port or Group: User defined Service Port

QoS: None

Schedule: None

Max. Concurrent Sessions for Each Source IP Address: 0

Mail Log & Record

IDP

Packet Tracing

Traffic Analysis

NAT

- LAN and DMZ Outgoing Mail Anti-Virus and Anti-Spam: All outgoing mails from LAN to WAN or DMZ to WAN have to go through the Anti-Virus and Anti-Spam check.

If user needs to check the Mail log, please set the Policy of LAN to WAN or DMZ to WAN as enabled.

Path 1: Policy > LAN Policy > LAN to WAN.

Path 2: Policy > DMZ Policy > DMZ to WAN.



Policy

Protocol: ALL

Source Service Port or Group: User Defined Edit

Destination Service Port or Group: User Defined Edit

Software Access Control: None

QoS: None

Schedule: None

URL Access Control: None

Authentication: None

Bulletin Board: None

WAN: ALL

Max. Concurrent Sessions for Each Source IP Address: 0

Mail Log & Record

WEB/FTP Anti-virus

IDP



- SMTP Log Setting:
  1. Incoming: There are three selections, Disable, Accept, or All.
  2. Outgoing: There are three selections, Disable, Fail, or All.
  3. Log Type: The type is simple.
- Mail Record Setting: If email files are higher than the number in KB which you enter, email files will be not scanned by the Anti-Virus and Anti-Spam check.
- Source IP replaced by WAN IP:
  1. LAN, DMZ Incoming Mail (Send): Sender IP will be replaced by the CS-950's WAN IP, so internal users get to see the CS-950's WAN IP when getting emails, not from the outside IP.
  2. LAN, DMZ Outgoing Mail (Send): Sender IP will be replaced by the CS-950's WAN IP, so outside receivers get to see the CS-950's WAN IP when getting emails.
- Release to carry the subject: User is able to join subject.

## 11.1.2 Valid Account Setting

Maybe there are Exchange Servers or mail servers in you internal network, and you want to make mail routes of sending become faster. Valid Account Setting feature makes internal mail server or Exchange Servers' performance better.

Select Mail Security > Filter & Log > Valid Account Setting.

- Valid Account Setting (Authentication): When incoming mails go through by the CS-950, system will check internal mail server whether those mail accounts exist or not. It makes mail server safer, meaning less spam mails because of the CS-950 filter valid account.

Valid Account Setting ( Authentication )

Enable  Enable  Disable

Study Enable  Enable  Disable

Domain List  ?

Mail Account  ?

Import  No file chosen   ?

1. Enable: "Enable" means the function is working; otherwise, "Disable" means the function is stopped.
2. Study: Set it as enable to study mail accounts.
3. Domain List: Enter domains; each line is for one domain like "planet.com.tw".
4. Mail Account: Enter e-mail addresses; each line is for one e-mail address like "sales@planet.com.tw".
5. Import: Click on "Choose File" to select a file that contains imported account emails.

- Valid Account Setting (Non-Authentication): It's like trusted domain. The domains and accounts you enter will not be filtered. Those accounts are trusted forever and thus, they will always go through here.

Valid Account Setting ( Non-Authentication )

Enable  Enable  Disable

Domain List  ?

Mail Account  ?

Import  No file chosen   ?

1. Enable: "Enable" means the function is working; otherwise, "Disable" means the function is stopped.
2. Domain List: Enter domains; each line is for one domain like "planet.com.tw".
3. Mail Account: Enter e-mail addresses; each line is for one e-mail address like "sales@planet.com.tw".
4. Import: Click on "Choose File" to select a file that contains imported account emails.

■ Valid Account Setting (Exchange Server):

Valid Account Setting ( Exchange Server )

Enable  Enable  Disable

Synchronization Enable  Enable  Disable

Domain List  ?

Mail Account  ?

Import  No file chosen   ?

1. Enable: "Enable" means the function is working; otherwise, "Disable" means the function is stopped.
2. Synchronous: Set it as enable to start synchronous Exchange Server. Click on  to enter your Exchange Server IP address, domain name, and so on.

Exchange Server setting

Exchange Server address

Exchange Server Domain Name

Exchange Server Login ID

Exchange Server Login Password

Ignore the Ms Exchange group

- Domain Computers
- Domain Controllers
- Schema Admins
- Enterprise Admins
- Domain Admins

Ignore the Ms Exchange user

- Administrator
- Guest

3. Domain List: Enter domains; each line is for one domain like "planet.com.tw".
4. Mail Account: Enter e-mail addresses; each line is for one e-mail address like "sales@planet.com.tw".
5. Import: Click on "Choose File" to select a file that contains imported account emails.

■ Invalid Account Setting:

1. Allow invalid domain pass: If user wants to allow invalid domain to be passed, please set it as enabled.
2. Block Log: Click on  to see whether the Invalid Mails are allowed to pass through.

### 11.1.3 Graylist and IP Resolved

Select Mail Security > Filter & Log > Graylist and IP Resolved.

Mail Security > Filter & Log

Filter & Log | Valid Account Setting | **Graylist and IP Resolved** | Traffic Blocking | SMTP Blocking IP

**Graylist**

Graylist  Enable  Disable

Receiver Delay Time  Sec ( 1 ~ 1000 Sec )

Block Log  ( Note : The content will be automatically cleared if this record files is larger than 100K. )

**IP Inverse solution**

IP Inverse solution Authentication  Enable  Disable

Did not pass validation approach  Delete  Increase the spam score  ( 1 ~ 20 )

**Generic Settings**

Trust IP List  
input IP address,  
one line for each IP, ex :  
10.0.0.1  
192.168.0.0/16

Import  No file chosen

Trust Domain List  
input sender domain,  
one line for each domain, ex:  
my.domain

Import  No file chosen

- **Graylist:** Graylisting is a method of defending e-mail users against spam. A mail transfer agent (MTA) using graylisting will "temporarily reject" any email from a sender it does not recognize. If the mail is legitimate, the originating server will, after a delay, try again and, if sufficient time has elapsed, the email will be accepted.
- **Block Log:** Click on  to see blocking logs.
- **IP Inverse solution:**
  1. **Trust IP list:** Input IP address or a range will be graylisting; one line for each IP. For instance, input 12.34.56.78 or 12.34.56.78/24.
  2. **Import:** Click on "Choose File" to select a file that contains imported IPs. One line for each IP, and should be a .txt file.

## 11.1.4 Traffic Blocking

Sometimes some accounts' passwords are so easy to be hacked, or a company got virus. Then, the hackers will use their computer to send spam emails. IT administrator may find out many spam emails are either coming from "Internal IP" or "External IP." The function is helpful to resolve the situation.

Select Mail Security > Filter & Log > Traffic Blocking.

Mail Security > Filter & Log

Filter & Log Valid Account Setting Graylist and IP Resolved **Traffic Blocking** SMTP Blocking IP

**Auth Unusual**

User Authentication abnormal situation  Start  Stop

Auth Unusual SetRule  seconds the same source IP login failures  times

**Traffic Blocking**

Block by Sender  Start  Stop

Check this IP Range Only  
input IP address,  
one line for each IP, ex :  
10.0.0.1  
192.168.0.0/16

Trusted Sender  
input sender address,  
one line for each address, ex:  
trustname@my.domain

Trusted Sender Domain  
input sender domain,  
one line for each domain, ex:  
my.domain

Block by IP  Start  Stop

Sender and IP Rules  seconds limit of letter number

**Generic Settings**

block each time  Sec

Trusted IP list  
input IP address,  
one line for each IP, ex :  
10.0.0.1  
192.168.0.0/16

Import  No file chosen

Blocking Log

- Block by Sender: Select "Start" to block mail traffic, or select "Stop" to disable it. Default is Stop.
- Check this IP Range Only: Input IP address or a range should be checked, one line for each IP. For instance, input 10.0.0.1 or 192.168.0.0/16.
- Trusted Sender: Input sender address will be unblocked forever, one line for each IP. For instance, input trustname@my.domain.
- Block by IP: Select Start to block mail traffic, or select Stop to disable it. Default is Stop.

- Sender and IP Rules: Input the time for blocking, and input the letter number.
- Trusted IP List: Input IP address will unblock forever, one line for each IP. For instance, input 10.0.0.1 or 192.168.0.0/16.
- Blocking Log: IT administrator could click on the [Log](#) button to see traffic mail block logs.

## 11.1.5 SMTP Blocking IP

Select Mail Security > Filter & Log > SMTP Blocking IP.

The screenshot shows the 'SMTP Blocking IP' configuration page. At the top, there are tabs for 'Filter & Log', 'Valid Account Setting', 'Graylist and IP Resolved', 'Traffic Blocking', and 'SMTP Blocking IP'. The 'SMTP Blocking IP' tab is active. Below the tabs, there is a section for 'SMTP Blocking IP' with a red note: 'Note : It will blocking ip which is unable to connect with SMTP by this function'. There are radio buttons for 'Enable' (selected) and 'Disable'. A 'Save' button is located below this section. Below that is a 'Blocking IP' section with an 'UnblockAll' button. There is a search bar for 'Search IP' and a table with columns for 'Blocking IP', 'Timeleft of Blocking', and 'Unblock'. A table with one row is visible. Below the table is an 'Unblock' button.

- Enable: Set the function as enable to block IP which is unable to connect with SMTP.

## 11.2 Anti-Virus

Select Mail Security > Anti-Virus > Anti-Virus setting.

The screenshot shows the 'Anti-Virus Setting' page. At the top, there are tabs for 'Anti-Virus Setting' and 'Anti-Virus'. The 'Anti-Virus Setting' tab is active. Below the tabs, there is a section for 'Basic Setting'. It includes radio buttons for 'Anti-Virus' (Start selected, Stop unselected), a dropdown for 'Virus Engine' (ClamAV selected), a text input for 'Don't Scan File' (jpg, jpeg, gif), and a text input for 'Max. Scan Size (KB)' (640) with a 'Suggest' button. Below this is a section for 'Action for Infected Mail'. It includes a text input for 'Add file extension to infected mail' (virus) and a text input for 'Subject of Infected Mail' (This mail is virus). A 'Save' button is located at the bottom.

- Anti-Virus: Set it as start to be effective. Default is start.
- Virus Engine: Available virus-scanning engine is ClamAV, the default and free of charge virus-scanning engine.
- Don't Scan File: You can enter the kind of file that does not need to be scanned for example, Jpg, jpeg, gif and so on.

- Max. Scan Size (KB): Once the mail exceeds the set value, the mail will be viewed as infected mail.
- Add file extension to infected mail: User is able to define it. Default is virus.
- Subject of Infected Mail: It will add some words in those virus emails subject title. Scan incoming and outgoing emails for viruses. Affected emails will be marked as "This mail is virus-affected" in its subject field, whereas clean emails remain the same original subject.

## 11.3 Anti-Spam

### 11.3.1 Spam Setting

Select Mail Security > Anti-Spam > Spam Setting.

Mail Security > Anti-Spam

Spam Setting

Auto Learning

Personal B & W

System B & W

**Anti-Spam Setting**

Status Running...

Spam Mail Filter  Start  Stop

Spam After SMTP Authentication  Start  Stop

Max. Scan Size (KB)  [Suggest](#)

**Anti-Spam Engine Setting**

IP Rating  Start  Stop

Bayesian Filter  Start  Stop

Bayesian Filter and Auto Learning  Start  Stop

Auto-Whitelist ( AWL )  Start  Stop

Spam Characteristics Filter Start ( Default is Start.)

Finger Printing Start ( Default is Start.)

**Action for Spam Mail**

Change Subject and Forward  Start  Stop

Score Greater than  ▼

Tag Spam Mail's Subject



Delete Spam Mail  Start  Stop


Score Greater than  ▼

- Spam Mail Filter: Set is as start, and the Status will show "Running".

- **Anti-Spam Engine Setting:** As you can see in screen, there are some engines, IP Rating, Bayesian Filtering, Bayesian Filter and Auto Learning, Auto-Whitelist (AWL), Spam Characteristics Filter, and Finger Printing.
- **Bayesian filtering:** It is a normal engine; you can search this information on the Internet. In addition, you also can set Bayesian filtering auto learning to start if you have set to Bayesian filtering.
- **Action for Spam Mail:** According to Anti-Spam method, add points when engine gauges that mail is a spam from patterns. For example, there is only “one link” in a mail and it has no other words anymore, moreover, spam engine would think it is a spam mail, therefore, add 0.1 point in this mail. After this mail through engines which you set to start, this mail would have a score which is convenient for us to know whether it is a spam or not. Therefore, you can set what score you judge spam in this part, and what to do if that score more than your setting. There are three parts:
  1. Change Subject and Forward: Set the function to start or stop.
  2. Score Greater than: Setting score to be spam.
  3. Tag Spam Mail's Subject: Add words to mail subject, and then the mail would be send to recipient account. Add to Subject could be [Spam-Mail] or some words which easy to remind recipient account.
  4. Delete Spam Mail: Set score to be deleted. Select on Deleted to see mails deleted.

Deleted MailSearch Condition

Date	2018-01-18 	00:00 ▼	-	2018-01-18 	23:59 ▼
Sender IP	<input type="text"/>				
Sender Address	<input type="text"/> @ <input type="text"/>				
Size Range	<input type="text"/> - <input type="text"/>				
Recipient Address	<input type="text"/> @ <input type="text"/>				
Score Range	<input type="text"/> - <input type="text"/>				
Virus	All ▼				
Subject	<input type="text"/>				
Each page shows	20 ▼ Records				

 Search



## 11.3.2 Auto Learning

Select Mail Security > Anti-Spam > Auto Learning.

The screenshot shows the 'Mail Security > Anti-Spam' configuration page. It has four tabs: 'Spam Setting', 'Auto Learning', 'Personal B & W', and 'System B & W'. The 'Auto Learning' tab is active. Under 'Anti-Spam Learning Setting', there are options for 'Auto Learning' (radio buttons for 'Start' and 'Stop'), 'Learning Every' (a dropdown set to '12' and a 'Learning' button), 'Blacklist Learning' (a 'Choose Files' button, 'No file chosen' text, and 'Import' and 'Record' buttons), 'Whitelist Learning' (a 'Choose Files' button, 'No file chosen' text, and 'Import' and 'Record' buttons), and 'Clear Learning Database' (a 'Clear' button with a note: '( Make sure you have backup data before clearing. )'). Below this is the 'Learning Database Import and Export' section with a 'Choose File' button, 'No file chosen' text, and 'Import' and 'Export' buttons. A 'Save' button is at the bottom.

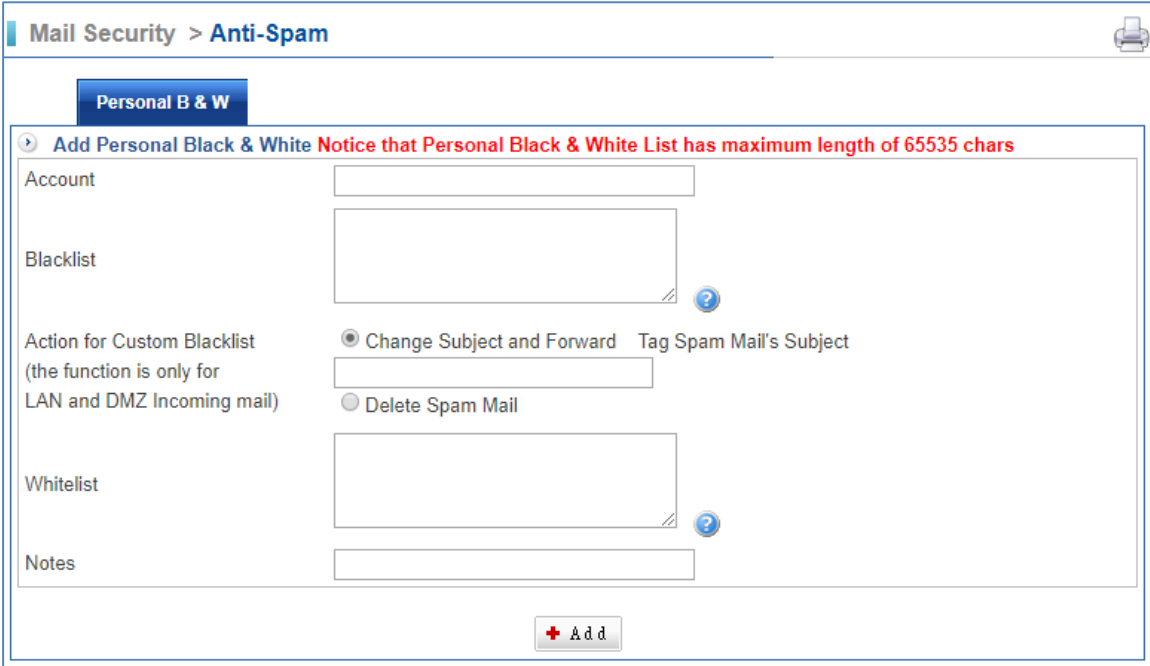
- Auto Learning: Set it as start, the function will work. Default is stop.
- Learning Every: Select the time user want, and click on **Learning**.
- Blacklist Learning: Click on “Choose File” to find blacklist file, and then click on **Import** to bring blacklist into the server. The system would learn these blacklist emails automatically. User also can click on **Record** to see learning status.
- Whitelist Learning: Click on “Choose File” to find whitelist file, and then click on **Import** to bring whitelist into the server. The system would learn these whitelist emails automatically. User also can click on **Record** to see learning status.
- Clear Learning Database: User can click on **Clear** if user wants to clear Learning database.
- Learning Database: Click on “Choose File” to find user’s original learning database file, and then click on **Import** to import original learning data file here. Besides, user can click on **Export** to export the learning database.

## 11.3.3 Personal B & W

Select Mail Security > Anti-Spam > Personal B & W.

The screenshot shows the 'Mail Security > Anti-Spam' configuration page with the 'Personal B & W' tab active. It features a 'Personal Black & White Import and Export' section with a 'Choose File' button, 'No file chosen' text, and 'Import' and 'Export' buttons. Below this is a 'Personal Black & White List' section with a notice: 'Notice that Personal Black & White List has maximum length of 65535 chars' and a '1 / 0' indicator. A table below the notice has columns: 'Notes', 'Account', 'Blacklist', 'Whitelist', 'Action for Custom Blacklist', and 'Edit / Del'. An 'Add' button is at the bottom.

- Click on  first.



- Account: Internal mail account.
- Blacklist: Specifies prohibited email addresses.
- Action for Custom Blacklist: The function is only for LAN and DMZ Incoming mail. There are two ways you can choose if the mail is from Blacklist.
  1. Change Subject and Forward: It is kind of a notification. You can add words to mail subject, and then the mail would be send to recipient account. Add to Subject could be [It is a spam] or some words which easy to remind recipient account.
  2. Delete Spam Mail: If users select "Delete Spam Mail", system will delete that email which was sent from Blacklist. Then, the recipient (account) will not receive that mail.
- Whitelist: Specifies permitted email addresses.

## 11.3.4 System B & W

Select Mail Security > Anti-Spam > System B & W.

Mail Security > Anti-Spam

Spam Setting Auto Learning Personal B & W System B & W

System Blacklist & Whitelist Setting (Sender Address)

Blacklist  Export

Import Blacklist Choose File No file chosen Import ?

Action for Blacklist  Change Subject and Forward Tag Spam Mail's Subject [Spam-Mail]   
 Delete Spam Mail

Whitelist  Export

Import Whitelist Choose File No file chosen Import ?

Trusted IP Address  ?

Spam Exception Setting (Recipient Address)

Trusted Domain  Export

Import Domain Choose File No file chosen Import ?

Trusted Address  Export

Import Email Address Choose File No file chosen Import ?

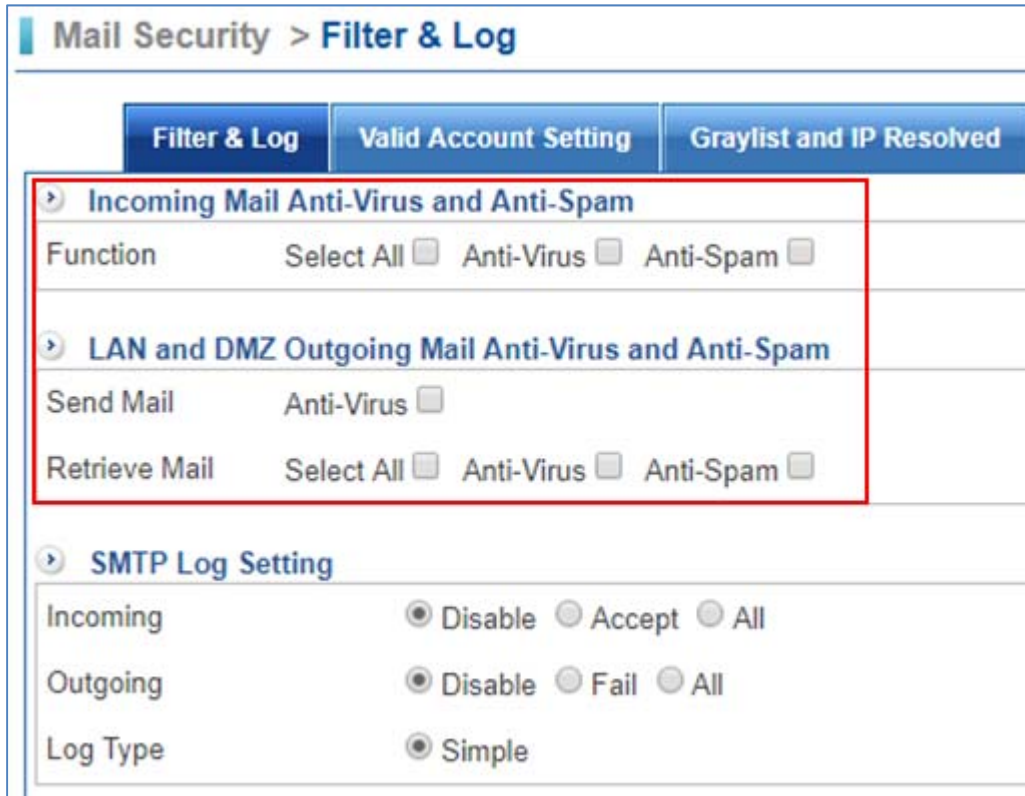
Save

- Blacklist: Used as a reference for classifying an email as a spam. On the other hand, you also can click on  to export system blacklist from the server.
- Import Blacklist: Click on "Choose File" to find which file you want to import, and then click on  to bring blacklist into server.
- Action for Blacklist: There are two ways you can choose if the mail is from Blacklist.
- Change Subject and Forward: It is kind of a notification. You can add words to mail subject, and then the mail would be send to recipient account. Add to Subject could be [Spam-Mail] or some words which easy to remind recipient account.
- Delete Spam Mail: Selected this, recipient account will not receive that mail.
- Whitelist: Used as a reference for classifying an email as a ham. On the other hand, you also can click on  to export system whitelist from the server.

- Import Whitelist: Click on “Choose File” to find which file you want to import, and then click on  to bring whitelist into server.

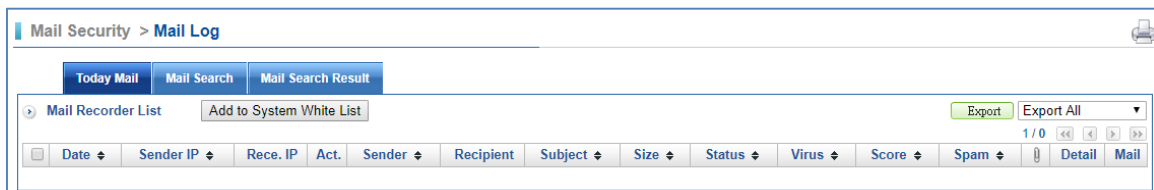
## 11.4 Mail Log

The feature accords with 11.1 Filter & Log section. You should select Mail Security > Filter & Log > Filter & Log, and enable Anti-Spam.



### 11.4.1 Today Mail

Select Mail Security > Mail Log > Today Mail.



- Date: It shows date and time.
- Sender IP: The sender IP addresses.
- Rece. IP: Resource IP.
- Act.: It offers three ways.
  1. 📧 : Incoming mail.
  2. 📤 : LAN 、 DMZ Outgoing mail (Send).
  3. 📥 : LAN 、 DMZ Outgoing mail (Receive).
- Sender: The sender accounts.

- Recipient: The receiver accounts.
- Subject: The title of mail.
- Size: The size of mail.
- Status: Current status.
- Virus: It is related to the section of 11.2 Anti-virus. User has to set Anti-Virus function as enable.
- Score: It is related to the section of 11.3 Anti-Spam. User has to set Anti-Spam function as enable.
- Spam: Add words to mail subject. It is related to the section of 11.2 Anti-virus and 11.3 Anti-Spam. User has to set Action of Infected Mail and Action for Spam Mail.
- Detail: Click on Detail link to see mail status details.

## 11.4.2 Mail Search

Select Mail Security > Mail Log > Mail Search.

Mail Security > Mail Log
Print

Today Mail
Mail Search
Mail Search Result

Search Condition

Date	2018-01-22 <span style="font-size: x-small;">📅</span>	00:00 <span style="font-size: x-small;">▼</span>	-	2018-01-22 <span style="font-size: x-small;">📅</span>	23:59 <span style="font-size: x-small;">▼</span>
Source	Local Data <span style="font-size: x-small;">▼</span>				
Sender IP Address	<input style="width: 95%;" type="text"/>				
Recipient IP Address	<input style="width: 95%;" type="text"/>				
Action	All <span style="font-size: x-small;">▼</span>				
Sender Account	<input style="width: 80%;" type="text"/>	@	<input style="width: 80%;" type="text"/>		
Mail size( KB )	<input style="width: 80%;" type="text"/>	-	<input style="width: 80%;" type="text"/>		
Recipient Account	<input style="width: 80%;" type="text"/>	@	<input style="width: 80%;" type="text"/>		
Spam Type	All <span style="font-size: x-small;">▼</span>				
Spam Score	<input style="width: 80%;" type="text"/>	-	<input style="width: 80%;" type="text"/>		
Virus Mail	All <span style="font-size: x-small;">▼</span>				
Status	All <span style="font-size: x-small;">▼</span>				
Subject	<input style="width: 95%;" type="text"/>				

Search

## 11.4.3 Mail Search Result

Select Mail Security > Mail Log > Mail Search Result.

Mail Search Result											
Date	Sender IP	Act.	Sender	Receiver	Subject	Size	Virus	Score	Spam	Details	Send
08-19 16:14:33	168.95.4.113		rosa	rookieswu	[Spam-Mail]This is a SMTP Test IV	607 B	-	6.2	Subject	<a href="#">Detail</a>	
08-19 13:04:36	211.22.160.30		kirin	rookieswu	[Spam-Mail]f	3.0 KB	-	6.3	Subject	<a href="#">Detail</a>	
08-19 13:03:32	211.22.160.30		kirin	rookieswu	[Spam-Mail]ds	3.0 KB	-	6.3	Subject	<a href="#">Detail</a>	
08-19 13:03:09	211.22.160.30		kirin	rookieswu	[Spam-Mail]jd	3.0 KB	-	6.3	Subject	<a href="#">Detail</a>	
08-19 13:01:52	211.22.160.30		kirin	rookieswu	[Spam-Mail]jd	3.0 KB	-	6.3	Subject	<a href="#">Detail</a>	
08-19 13:00:32	211.22.160.30		kirin	rookieswu	[Spam-Mail]sd	3.0 KB	-	6.3	Subject	<a href="#">Detail</a>	
08-19 13:00:09	211.22.160.30		kirin	rookieswu	[Spam-Mail]d	3.0 KB	-	6.3	Subject	<a href="#">Detail</a>	
08-19 12:59:55	211.22.160.30		kirin	rookieswu	[Spam-Mail]j	3.0 KB	-	6.3	Subject	<a href="#">Detail</a>	
08-19 12:57:12	211.22.160.30		kann	rookieswu	[Spam-Mail]sd	3.4 KB	-	6.3	Subject	<a href="#">Detail</a>	
08-19 12:52:52	211.22.160.30		kann	rookieswu	[Spam-Mail]jd	3.4 KB	-	6.3	Subject	<a href="#">Detail</a>	
08-19 12:49:54	211.22.160.30		kann	rookieswu	[Spam-Mail]jdf	3.4 KB	-	6.3	Subject	<a href="#">Detail</a>	
08-19 12:48:53	211.22.160.30		kann	rookieswu	[Spam-Mail]jdf	3.0 KB	-	6.3	Subject	<a href="#">Detail</a>	
08-19 12:20:15	211.22.160.30		kann	rookieswu	[Spam-Mail]jdf	3.4 KB	-	6.3	Subject	<a href="#">Detail</a>	
08-19 12:08:43	211.22.160.30		kann	rookieswu	[Spam-Mail]jdf	3.4 KB	-	6.3	Subject	<a href="#">Detail</a>	
08-19 12:07:34	211.22.160.30		kann	rookieswu	[Spam-Mail]jd	3.4 KB	-	6.3	Subject	<a href="#">Detail</a>	
08-19 11:59:25	211.22.160.30		kann	rookieswu	[Spam-Mail]jdf	3.4 KB	-	6.3	Subject	<a href="#">Detail</a>	

## 11.5 SMTP Log

User needs to select SMTP Log Setting first if user wants to have SMTP Log.

**Mail Security > Filter & Log**

**Incoming Mail Anti-Virus and Anti-Spam**

Function       Select All    Anti-Virus    Anti-Spam

---

**LAN and DMZ Outgoing Mail Anti-Virus and Anti-Spam**

Send Mail       Anti-Virus

Retrieve Mail    Select All    Anti-Virus    Anti-Spam

---

**SMTP Log Setting**

Incoming       Disable    Accept    All

Outgoing       Disable    Fail    All

Log Type       Simple

## 11.5.1 SMTP Log

Select Mail Security > SMTP Log > SMTP Log Search.

**Mail Security > SMTP Log**

SMTP Log Search

SMTP Log Search Result

**Search condition**

Date   -

Sender Account  @

Mail Size( KB )  -

Recipient Account  @

Status

## 11.5.2 SMTP Log Result

Select Mail Security > SMTP Log > SMTP Log Search Result.

Date	Sender	Receiver	Size	Status	Message	Deta.
01-20 11:06:12	rookieswu	rookieswu	492 B	Accept	250 Ok: queued as 0D4A872F14	<a href="#">?</a>
01-20 11:06:06	rookieswu	rookieswu	492 B	Accept	250 Ok: queued as 914FE72F0B	<a href="#">?</a>
01-20 11:05:49	rookieswu	rookieswu	492 B	Accept	250 Ok: queued as 2ACAA72F02	<a href="#">?</a>
01-20 11:05:19	rookieswu	rookieswu	492 B	Accept	250 Ok: queued as 20E5772EF9	<a href="#">?</a>
01-20 11:05:07	rookieswu	rookieswu	492 B	Accept	250 Ok: queued as A1E2072EE8	<a href="#">?</a>
01-20 11:05:07	rookieswu	rookieswu	492 B	Accept	250 Ok: queued as 380B272EE7	<a href="#">?</a>
01-20 11:04:59	rookieswu	rookieswu	492 B	Accept	250 Ok: queued as 63C2472ED8	<a href="#">?</a>
01-20 11:04:53	rookieswu	rookieswu	492 B	Accept	250 Ok: queued as E971572ECF	<a href="#">?</a>
01-20 11:04:48	rookieswu	rookieswu	492 B	Accept	250 Ok: queued as 5C9CB72EC6	<a href="#">?</a>
01-20 11:04:45	rookieswu	rookieswu	492 B	Accept	250 Ok: queued as CC56272EBD	<a href="#">?</a>
01-20 11:04:40	rookieswu	rookieswu	492 B	Accept	250 Ok: queued as 4AE6B72EB4	<a href="#">?</a>
01-20 11:04:38	rookieswu	rookieswu	492 B	Accept	250 Ok: queued as D98C172EAB	<a href="#">?</a>
01-20 11:04:35	rookieswu	rookieswu	492 B	Accept	250 Ok: queued as 5B91E72EA2	<a href="#">?</a>
01-20 11:04:29	rookieswu	rookieswu	492 B	Accept	250 Ok: queued as CB5BA72E91	<a href="#">?</a>
01-20 11:04:28	rookieswu	rookieswu	492 B	Accept	250 Ok: queued as 3AEFE72E88	<a href="#">?</a>
01-20 11:04:26	rookieswu	rookieswu	492 B	Accept	250 Ok: queued as B570F72E87	<a href="#">?</a>

# Chapter 12. 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.

CS-950 built-in IDP (Intrusion Detection System + Intrusion Prevention System) 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, CS-950 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. CS-950 built-in IDP with huge database can inspect all the packets from WEB, P2P, IM, NetBIOS etc.

## 12.1 Basic 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. CS-950 includes the well-known IDS (Intrusion Detection System) and IPS (Intrusion Prevention System) Snort. It is directly built into the IP-firewall (Snort inline). At this time no rules can be added through the web interface.

Select IDP > IDP Setting > 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. : On.
  - 2. : Off.
- Save: After completed this model setting, please click on .
- Click on IDP Advanced Settings link to see the page below. On the other hand, click on IDP Basic Setting to get back to the previous step.

IDP > IDP Setting

Advanced Setting

Advanced Setting IDP Basic Setting (2397) Click save after completing setting. 

Group Name	Action	Log
ATTACK-RESPONSES (13)		
BACKDOOR (214)		
BLACKLIST (21)		
BOTNET-CNC (16)		
CHAT (24)		
DDOS (8)		
DELETED (262)		
DNS (13)		
DOS (8)		
EXPLOIT (37)		
EXPLOIT-KIT (6)		
FINGER (12)		
FTP (15)		
ICMP (62)		
ICMPv6 (2)		
INFO (4)		
MALWARE-BACKDOOR (2)		
MALWARE-CNC (121)		
MALWARE-OTHER (8)		
MISC (25)		
MYSQL (4)		
NETBIOS (6)		
ORACLE (15)		
OTHER-IDS (3)		
P2P (17)		
PECIFIC-THREATS (1)		
PHISHING-SPAM (1)		
POLICY (49)		
POP3 (5)		
PUA-ADWARE (1)		
RPC (38)		
RSERVICES (13)		
SCAN (5)		
SERVER-WEBAPP (4)		
SHELLCODE (8)		
SMTP (14)		
SNMP (2)		
SPECIFIC (1)		
SPECIFIC-THREATS (99)		
SPYWARE-PUT (280)		
SQL (73)		
TELNET (15)		
WEB-CGI (295)		
WEB-CLIENT (38)		
WEB-COLDFUSION (44)		
WEB-FRONTPAGE (35)		
WEB-IIS (81)		
WEB-MISC (255)		
WEB-PHP (122)		
X11 (2)		

To set your IDP function, do not forget to click on . In addition, click rectangular form if you want to see the list of class names.

## 12.2 IDP Log

### 12.2.1 IDP Log

Select IDP > IDP Log > IDP Log.

The screenshot shows the 'IDP > IDP Log' page. At the top, there are two tabs: 'IDP Log' (selected) and 'IDP Log Search'. Below the tabs is a table header with the following columns: Date, Event, Group Name, Risk Level, Interface, Source IP Address, Destination IP Address, Protocol, Source Port, and Destination Port. To the right of the table header, there are navigation controls showing '1 / 0' and buttons for '<<', '<', '>', and '>>'. There are also two buttons: 'Export' and 'Export All'.

### 12.2.2 IDP Log Search

Select IDP > IDP Log > IDP Log Search.

The screenshot shows the 'IDP > IDP Log' page with the 'IDP Log Search' tab selected. The search criteria are as follows:

- Date: 2018-01-22 00:00 - 2018-01-22 23:59
- Event: [Empty text box]
- Group Name: [Empty text box]
- Risk Level: All
- Interface: All
- Source IP Address: [Empty text box]
- Destination IP Address: [Empty text box]
- Protocol: All
- Source Port: [Empty text box]
- Destination Port: [Empty text box]

A 'Search' button is located at the bottom center of the search form.

# Chapter 13. SSL VPN

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

## 13.1 SSL VPN Setting

### 13.1.1 SSL VPN Setup

Select SSL VPN > SSL VPN Setting > SSL VPN Setup.

SSL VPN > SSL VPN Setting

SSL VPN Setup | SSL Client List | Software Download Page Setting

Server Setting [Modify the Server Setting](#) Note : System will cancel all certificates after modification (except service status). Please Re-generate certificate and download again.

Service Status  Start  Stop Note : It will take a few seconds to start, please be patient.

Local Interface

Local Port  -

Max concurrent connections  (Range: 20 ~ 50)

Client IP Range  /  .  .  .  ( Client IP range need different with LAN,DMZ interface.)

DNS Server 1

DNS Server 2

WINS Server 1

WINS Server 2

Certificate Setting

CA's Name  Country

Province or State  City

Organization  Unit

Certificate Name  Certificate E-mail

Server Name

- Service Status: You have to click on “Modify the Server Setting” link to modify SSL VPN settings.  
Then please set it as start to be effective. Default setting is Stop.



SSL VPN Setup    SSL Client List    Software Download Page Setting

Server Setting [Modify the Server Setting](#) **Note : System will cancel all certificates after modification (except service status). Please Re-generate certificate and download again.**

Service Status     Start     Stop    Note : It will take a few seconds to start, please be patient.

Local Interface       

Local Port     -

Max concurrent connections     (Range: 20 ~ 50)

Client IP Range     /  .  .  .  ( Client IP range need different with LAN,DMZ interface.)

DNS Server 1   

DNS Server 2   

WINS Server 1   

WINS Server 2   

**Certificate Setting**

CA's Name	<input type="text" value="L7FW_SSLVPN_CA"/>	Country	<input type="text" value="TW"/>
Province or State	<input type="text" value="TC"/>	City	<input type="text" value="Taipei"/>
Organization	<input type="text" value="Common Inc."/>	Unit	<input type="text" value="L7FW Team"/>
Certificate Name	<input type="text" value="L7FWSSLVPNCA"/>	Certificate E-mail	<input type="text" value="help@common.com"/>
Server Name	<input type="text" value="L7FW_SSLVPN_SERVER"/>		

- Local interface:
  1. WAN 1
  2. WAN 2
- Local port: Set a using port. Default setting is 387.
- Max. concurrent connections: Set the max. concurrent connections. Default setting is 20.
- Client IP range: Set IP range.
- 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 click on  to start SSL VPN.

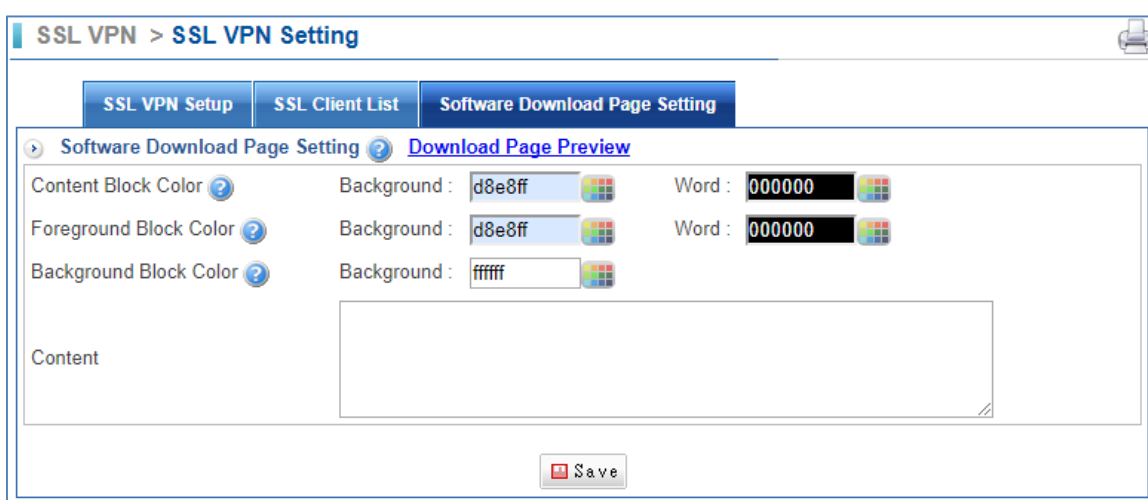
### 13.1.2 SSL Client list

Select SSL VPN > SSL VPN Setting > SSL Client list.



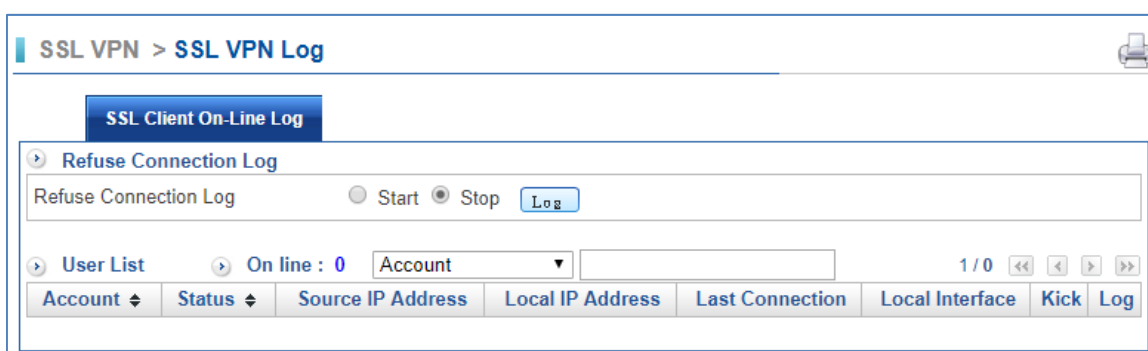
### 13.1.3 Software Download Page Setting

Select SSL VPN > SSL VPN Setting > Software Download Page Setting.



### 13.2 SSL Client On-Line Log

Select SSL VPN > SSL VPN Log > SSL Client On-Line Log.



### 13.3 VPN Policy

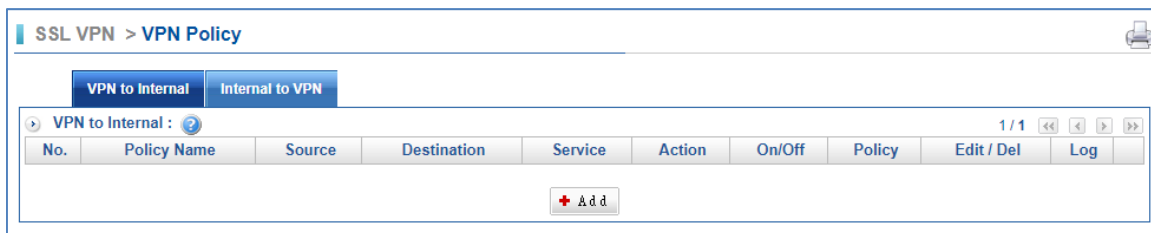
SSL VPN on internal control and external control through the SSL VPN connection points is

connected to internal network, the Protocol, Service group port, QoS bandwidth and Schedule, Packet tracing, and Traffic Analysis.

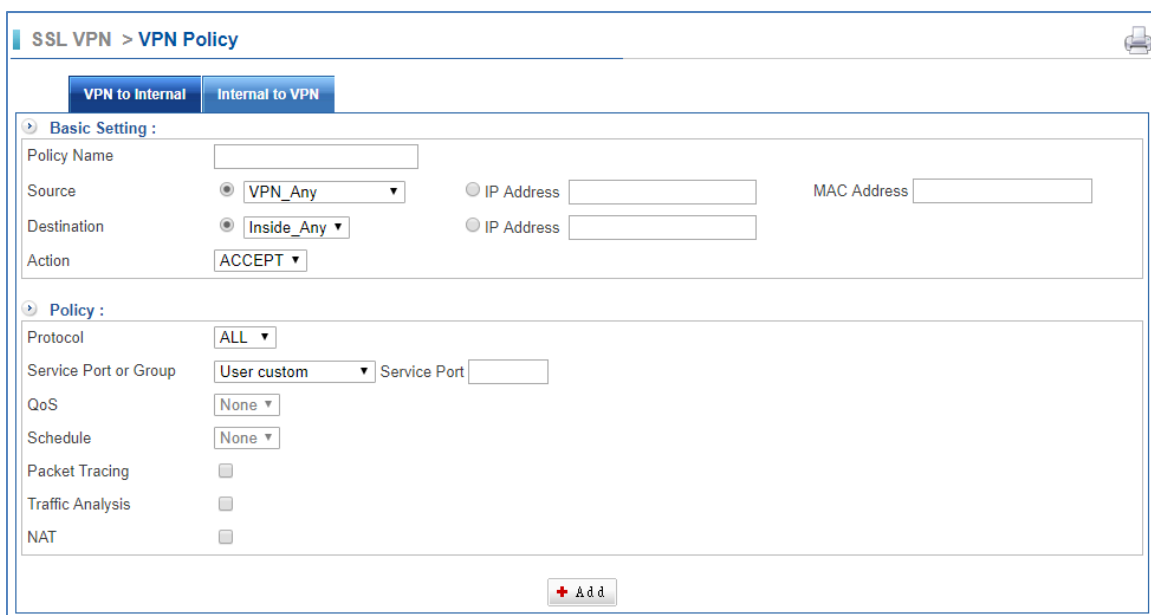
VPN's policy is as follows: policies started from the priority1 will be the implementation of eligible project. If you want to ban non-control information from the internal network, you will need to list a total of all the packets prohibited.

### 13.3.1 VPN to Internal

Select SSL VPN > VPN Policy > VPN to Internal.



- Click on  first.



- 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 be the 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 be the 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 from incoming VPN controls.

- Action: It offers two movements.
  1. ACCEPT means the Policy of the packet will be released.
  2. DROP means discarded.
- Protocol: The protocol is used for communication between two devices. TCP and UDP are the two most frequently seen protocols among others.
- Service group Port or Group: With service groups, the administrator in setting policy can simplify many processes.  
For example, there are ten different IP addresses on the server that can access five different services, such as HTTP, FTP, SMTP, POP3, and TELNET. If you do not use the service group functions, you will need to develop a total of  $10 \times 5 = 50$  policies. But use the service group name applied to the service option on, you only need a policy that can achieve the function of 50.
- QoS: Select Objects > QoS. Then, the VPN policy set the maximum 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.

### 13.3.2 Internal to VPN

Select SSL VPN > VPN Policy > Internal to VPN.



- Click on  first.

- 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 be the 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 be the 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 the Policy of the packet will be released.
  2. DROP means discarded.
- Protocol: The protocol used for communication between two devices. TCP and UDP are the two most frequently seen protocols among others.
- Service group Port or Group: With service groups, the administrator in setting policy can simplify many processes.



For example, there are ten different IP addresses on the server that can access five different services, such as HTTP, FTP, SMTP, POP3, and TELNET. If you do not use the service group functions, you will need to develop a total of  $10 \times 5 = 50$  policies. But use the service group name applied to the service option, and you only need a policy that can achieve the function of 50.

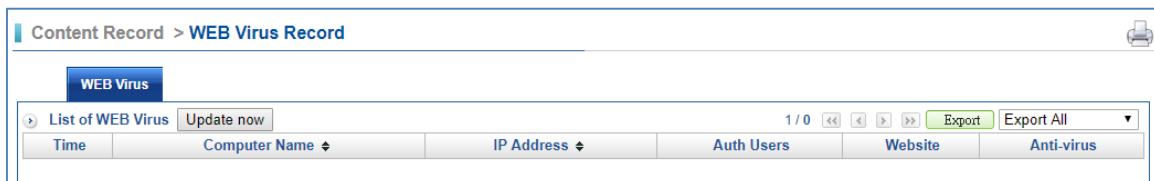
- QoS: Select Objects > QoS. Then, the VPN policy set the maximum bandwidth and rate bandwidth (Bandwidth is consistent with the policy of the user to share).
- Schedule: Select Objects > Schedule. Then, set your schedule time.
- Packet Tracing: Select Packet tracing tick box to start function; all records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

# Chapter 14. Content Record

## 14.1 Web Virus Record

This function records Web anti-virus logs. You have to select Policy > LAN Policy, DMZ Policy, or WAN Policy. Then, select functions you need on the right side. In the screen below, select WEB/FTP Anti-virus function.

Select Content Record > WEB Virus Record > WEB Virus.



## 14.2 FTP Virus Record

This function records FTP anti-virus logs. You have to select Policy > LAN Policy, DMZ Policy, or WAN Policy. Then, select functions you need on the right side. In the screen below, select WEB/FTP Anti-virus function.

Select Content Record > FTP Virus Record > FTP Virus.



# Chapter 15. VPN

To obtain a private and secure network link, the CS-950 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.

## 15.1 IPSec Tunnel

IPSec (IP Security) is a generic standardized VPN solution. IPSec must be implemented in the IP stack which is part of the kernel. Since IPSec is a standardized protocol it is compatible to most vendors that implement IPSec. It allows users to have an encrypted network session by standard IKE (Internet Key Exchange). 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.

### 15.1.1 IPSec Tunnel

Select VPN > IPSec Tunnel > IPSec Tunnel.



- Interface: At present IPSec VPN use entity interface.
  1. : Represent WAN 1.
  2. : Represent WAN 2.
- Status:
  1. : The VPN is not work.
  2. : The VPN is on work.
- Enabled: Control IPSec VPN start and suspension button.
  1. : Stand for start.
  2. : Stand for suspension.
- Edit/Del: Click on to edit the VPN setting; click on to delete it..
- Log: This VPN communication record, IPSec VPN channel; if it has the communication record with opposite party, select "Log" to open the new Windows; the data will be in accordance with time sorting and most recent news on the last page.

## 15.1.2 Add IPsec Tunnel

Select VPN > IPsec Tunnel > Add IPsec Tunnel.

VPN > IPsec Tunnel

IPsec Tunnel Add IPsec Tunnel

Add New Connection :

Enabled

Tunnel Name

Interface  WAN1  WAN2  WAN3

Remote IP  IP Address or Domain   Dynamic IP Address

Enable Redundant

Multiple Tunnel Mode

Local Subnet  255.255.255.0 (/24)

Remote Subnet  255.255.255.0 (/24)

IKE Setting (Phase1)

IKE  v1  v2

Connection Type  Main  Aggressive

Preshare Key

ISAKMP  des  md5  DH Group  1  Auto Matching

Local ID  WAN IP  Domain Name @

Remote ID  WAN IP  Domain Name @

IKE SA Lifetime  3  Hour(s)

IPsec Setting (Phase 2)

IPsec  des  md5  Auto Matching

Perfect Forward Secrecy (PFS)  No  Yes

IPsec SA Lifetime  3  Hour(s)

Dead Peer Detection  hold  Delay 10  Seconds  Time out 60  Seconds

Drop SMB Protocol

- Enabled: Select it to start the connection.
- 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.
  3. WAN 3.
- Remote IP Address: The IP or fully qualified domain name of the remote host.
  1. IP Address or Domain: Enter an IP Address or Domain.
  2. Dynamic: Follow Dynamic IP address.
- Local Subnet: The local subnet in CIDR notation. For instance, "192.168.15.0/24".
- Remote Subnet: This is only available for net-to-net connections and specifies the remote subnet in CIDR notation. For instance, "192.168.16.0/24".
- IKE: Select the IKE (Internet Key Exchange) version.
- Connection Type:

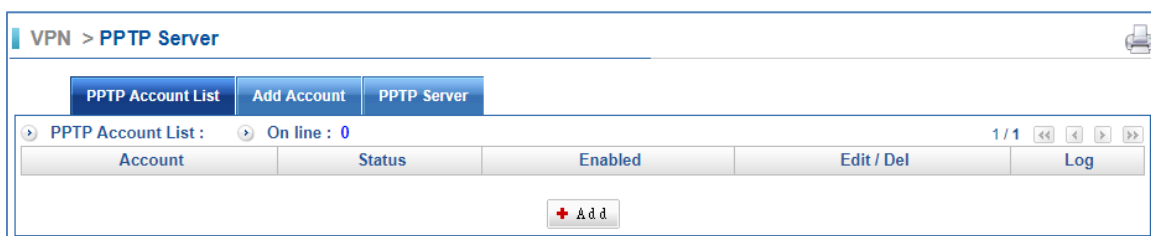
1. Main.
  2. Aggressive.
- Preshare Key: Enter a pass phrase to be used to authenticate the other side of the tunnel.
  - ISAKMP: It provides the way to create the SA between two PCs. The SA can access the encoding between two PCs, and the IT administrator can assign of which key size or Preshare Key and algorithm to use. The SA comes in many connection ways.
    1. AES: 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.
    5. DH Group: When the encryption technique is AES, it can be choice 2, 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.







## 15.2 PPTP Server

Use the IP address and the scope option needs to match the far-end the PPTP server; its goal is to use the PPTP channel technology, and establish Site to Site VPN where the channel can have equally good results from different methods with IPsec.

## 15.2.1 PPTP Account List

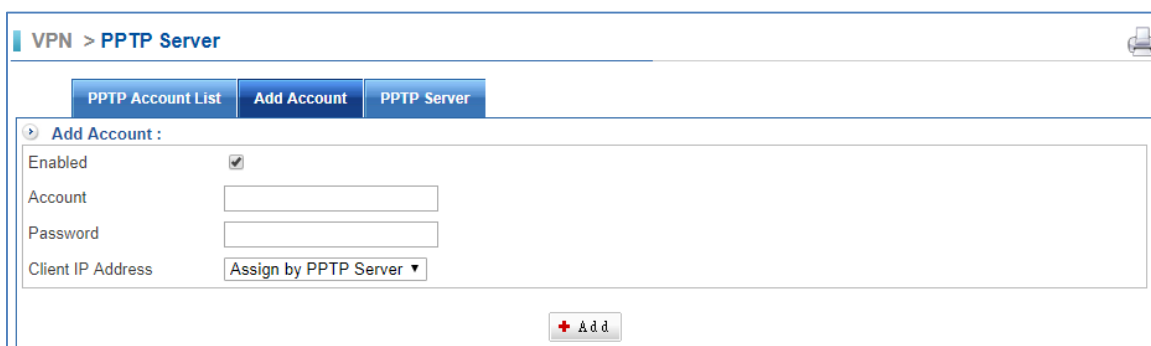
Select VPN > PPTP Server > PPTP Account List.



- Account: Available VPN-PPTP account
- Status: The symbol and its description used in the VPN connection status.
  1.  : It is connecting.
  2.  : Disconnected
- Enabled: Click signature again will change to disable.
  1.  : Enable
  2.  : Disable
- Edit/Del: Click on  to modify PPTP account; click on  to delete it.
- Log: It shows the PPTP account connection logs.

## 15.2.2 Add Account

Select VPN > PPTP Server > Add Account.



- Enabled: Select Enabled to start this account.
- Account: Enter an account.
- Password: Enter a password.
- Client IP Address:
  1. Assign by PPTP Server: The CS-950 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.

## 15.2.3 PPTP Server

Select VPN > PPTP Server > PPTP Server.

VPN > PPTP Server

PPTP Account List Add Account PPTP Server

PPTP Server :

Enabled

Compression & Encryption

Internet Access over PPTP

Client IP Address (Start-End) 192.168.100.1 - 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

Source IP limit  
(ex. 192.168.0.1 or 192.168.0.1/24)

Save

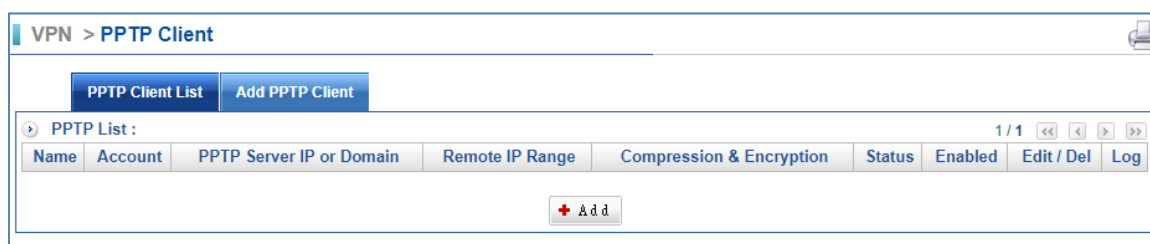
- Enabled: Check the box to enable the function.
- Compression & Encryption: Check the box to enable the function.
- Internet Access over PPTP: Check the box to allow user who pass through Internet by VPN-PPTP.
- Client IP Address: The range of IP address for clients using PPTP connection
- The First 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  to start PPTP Server.

## 15.3 PPTP Client

Use the IP address and the scope option needs to match the far-end the PPTP server; its goal is to use the PPTP channel technology, and establish Site to Site VPN where the channel can have equally good results from different methods with IPsec.

## 15.3.1 PPTP Client

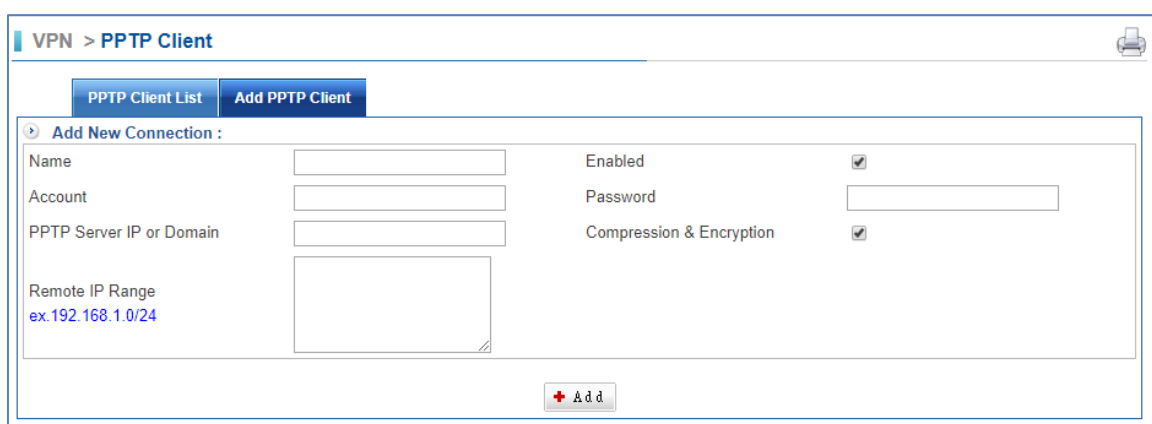
Select VPN > PPTP Server > PPTP Client List.



The screenshot shows a web interface for managing PPTP clients. At the top, there is a breadcrumb trail 'VPN > PPTP Client' and a printer icon. Below this, there are two buttons: 'PPTP Client List' and 'Add PPTP Client'. The main content area is titled 'PPTP List :'. It features a table with the following columns: Name, Account, PPTP Server IP or Domain, Remote IP Range, Compression & Encryption, Status, Enabled, Edit / Del, and Log. The table is currently empty. Below the table, there is an 'Add' button with a red plus sign.

## 15.3.2 Add PPTP Client

Select VPN > PPTP Server > Add PPTP Client.



The screenshot shows the 'Add PPTP Client' form. At the top, there is a breadcrumb trail 'VPN > PPTP Client' and a printer icon. Below this, there are two buttons: 'PPTP Client List' and 'Add PPTP Client'. The main content area is titled 'Add New Connection :'. It contains several input fields and checkboxes: 'Name' (text input), 'Account' (text input), 'PPTP Server IP or Domain' (text input), 'Remote IP Range' (text input with a hint 'ex. 192.168.1.0/24'), 'Enabled' (checkbox, checked), 'Password' (text input), and 'Compression & Encryption' (checkbox, checked). Below the form, there is an 'Add' button with a red plus sign.

- Name: The description for PPTP Client.
- Account: It displays the name of clients using PPTP to log in to PPTP server.
- PPTP Server IP or Domain: Enter a server IP address or domain.
- Remote IP Range: PPTP Client enters the IP address of PPTP Server.
- Enabled: Check the box to enable the PPTP Client account.
- Password: It displays the password of clients using PPTP to log in to PPTP server.

## 15.4 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.

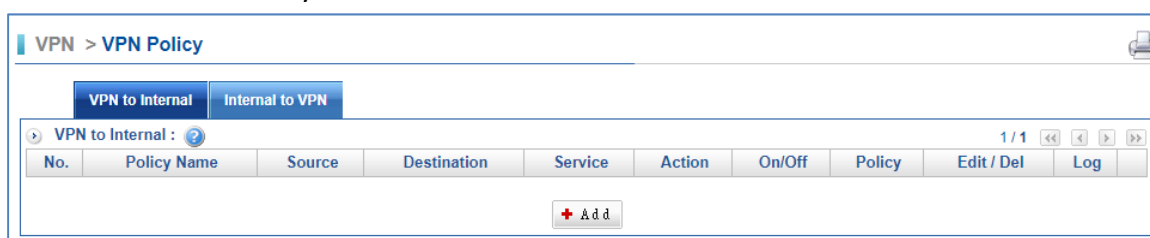
The default of VPN Policy does not grant pre-control as long as the VPN is established successfully, and two-way computer can communicate, if only the control of the target was expected through the proposed regulations in the last one against all connections.



## 15.4.1 VPN to Internal

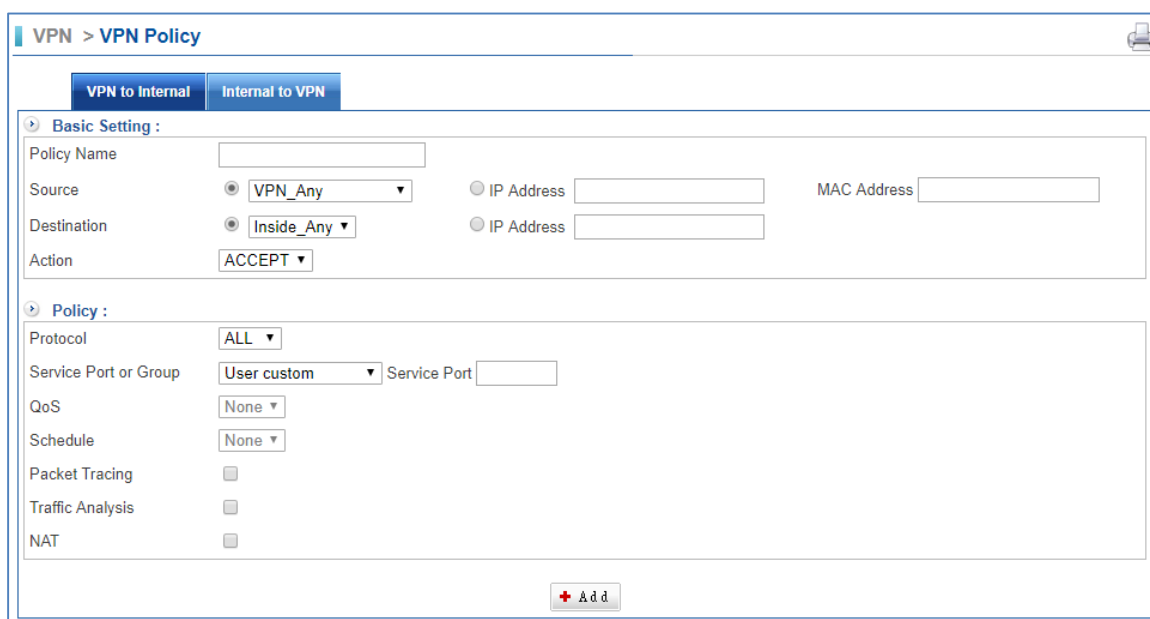
The control of the VPN in the past, most were carried out from the policies or is unable to monitor, but CS-950's VPN is directly controlled from the VPN.VPN on internal control and external control through the VPN connection points connected to internal network, the Protocol, Service port, QoS bandwidth and Schedule, Packet tracing, and Traffic Analysis. VPN's policy is as follows: policies started from the priority1 will be the implementation of eligible project. If you want to ban non-control information from the internal network, you will need to list a total of all the packets prohibited.

Select VPN > VPN Policy> VPN to Internal



The screenshot shows the 'VPN > VPN Policy' configuration page. The 'VPN to Internal' tab is selected. Below the tabs, there is a breadcrumb 'VPN to Internal' and a table with 10 columns: No., Policy Name, Source, Destination, Service, Action, On/Off, Policy, Edit / Del, and Log. The table is currently empty. Below the table, there is an 'Add' button with a red plus sign.

- Click on  first.



The screenshot shows the 'VPN > VPN Policy' configuration page with the 'VPN to Internal' tab selected. The 'Basic Setting' section includes: Policy Name (text input), Source (radio button selected for 'VPN\_Any'), Destination (radio button selected for 'Inside\_Any'), and Action (dropdown menu set to 'ACCEPT'). There are also radio buttons for 'IP Address' and 'MAC Address' with corresponding text input fields. The 'Policy' section includes: Protocol (dropdown menu set to 'ALL'), Service Port or Group (dropdown menu set to 'User custom' with a 'Service Port' text input field), QoS (dropdown menu set to 'None'), Schedule (dropdown menu set to 'None'), Packet Tracing (checkbox), Traffic Analysis (checkbox), and NAT (checkbox). An 'Add' button is visible at the bottom.

- Policy Name: Enter any word for recognition.
- Source 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 be the 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

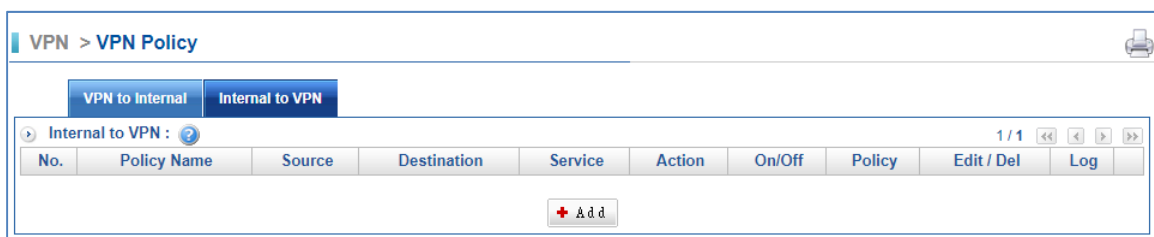
with the conditions. The default IP address of the PPTP server will also be included in the default source IP address.

2. The destination IP Address: Inside\_Any will be the 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 the Policy of the packet will be released.
  2. DROP means discarded.
- Protocol: The protocol is used for communication between two devices. TCP and UDP are the two most frequently seen protocols among others.
- Service Port or Group: With service groups, the administrator in setting policy can simplify many processes. For example, there are ten different IP addresses on the server that can access five different services, such as HTTP、FTP、SMTP、POP3 and TELNET. If you do not use the service group functions, you will need to develop a total of  $10 \times 5 = 50$  policies. But use the service group name applied to the service option on, and you only need a policy that can achieve the function of 50.
- QoS: Select Objects > QoS. Then, the VPN policy set the maximum 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.

## 15.4.2 Internal to VPN

Select VPN > VPN Policy> Internal to VPN.



- Click on  first.

- Policy Name: Enter any word for recognition.
- Source 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 be the 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 be the 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 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 Port or Group: With service groups, the administrator in setting policy can simplify many processes. For example, there are ten different IP addresses

on the server that can access five different services, such as HTTP、FTP、SMTP、POP3 and TELNET. If you do not use the service group functions, you will need to develop a total of  $10 \times 5 = 50$  policies. But use the service group name applied to the service option, and you only need a policy that can achieve the function of 50.

- QoS: Select Objects > QoS. Then, the VPN policy set the maximum 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.