User Manual for SANGFOR MIG

6.2.1

深信服智安全
SANGFOR SECURITY

September, 2019

Table of Contents

User Manual for SANGFOR MIG 6.2.1 1

Table of Contents 2

Declaration 1

Preface 2

About This Manual 2

Document Conventions 3

Format Conventions for Graphical Interface 3

Signs 4

Technical Support 4

Acknowledgement 5

1 Installation Guide 6

1.1. Environmental Requirements 6

1.2. Power Supply 6

1.3. Product Appearance 7

1.4. Configuration and Management 8

1.5. Wiring Method for Devices 9

1.6. Integration with BBC to Realize Easy-Deployment for Operation 11

1.6.1. BBC Configuration 11

1.6.2. Branch Deployment 14

2 Usage of Console 17

2.1. Log in to WebUI Configuration Interface 17

2.2. View Running Status 20

2.2.1. Device Running Status 20

2.2.2. VPN Running Status 20

2.2.3. User Traffic Ranking 22

2.2.4. View Online Users 24

2.2.5. DHCP Running Status 24

2.3. System Setup 24

2.3.1. Network Interface Setting 25

2.3.2. License Key 34

2.3.3. System Time Setting 35

2.3.4. Route Setting 36

2.3.5. Multi-line Settings 41

2.3.6. Local Subnet List 44

2.3.7. Console Settings........45

2.3.8. SYSLOG Settings 47

2.3.9. DHCP Settings 48

2.3.10. WLAN Settings (MIG-1110-W) 52

2.3.11. Generate Certificates 58

2.3.12. Settings for Joining to Central Management 59

2.4. Object Settings 63

2.4.1. View Algorithm 63

2.4.2. IP Group Settings 64

2.4.3. URL Group Settings 65

2.4.4. User Authentication Settings 66

2.4.5. Time Schedule Settings 70

2.4.6. Network Services Settings 71

2.5. VPN Info Settings 74

2.5.1. Basic Settings 75

2.5.2. Certificate Management 77

2.5.3. User Management 82

2.5.4. Connection Management 90

2.5.5. Virtual IP Pool 94

2.5.6. Inter-tunnel Route Setting 95

2.5.7. Third-party Connection 98

2.5.8. Advanced Settings 110

2.6. Access Control 117

2.6.1. IPMAC Authentication Settings 117

2.6.2. Authentication Options Settings 119

2.6.3. Access Policy Settings 120

2.7. Traffic Management 124

2.7.1. Line Bandwidth Configuration 125

2.7.2. Traffic Policy Settings 126

2.8. Firewall Settings 129

2.8.1. Filtering Rules Settings....130

2.8.2. NAT Settings....141

2.8.3. Anti-DOS attacks....153

2.8.4. ARP Spoofing Protection....155

2.9. System maintenance....157

2.9.1. Newbie Wizard....157

2.9.2. View Log....157

2.9.3. Policy Troubleshooting....159

2.9.4. Backup/Recovery Configuration....162

3 Case Set....164

3.1. Routing Mode Deployment Case....164

3.2. Deployment Case of One-arm Mode....169

3.3. SANGFOR VPN Interconnection Case....173

3.4. Case of IPSEC VPN Interconnection with CISCO PIX Standard....179

3.5. VPN LAN Permission Setting Case....188

3.6. VPN Multiple Lines Configuration Case....195

3.7. VPN Multi-subnet Configuration Case....200

3.8. Cases of Inter-branch Exchange Accesses Through Inter-tunnel Routing....202

3.9. Cases of Internet Access by Users via Destination Routing....203

3.10. SNAT Case of VPN Tunnel LAN Interface....206

4 Introduction of BBC's Management and Control of MIG....213

4.1. AutoVPN....213

4.1.1. Establishment of SANGFOR VPN 214

4.1.2. VPN Topology Reporting 216

4.1.3. VPN Status Visualization-Topology Large Screen 217

4.1.4. VPN Status Visualization-Device List 217

4.2. SD-WAN Intelligent Routing 218

Appendix: Use the RESET key to restore the default configuration and password. 222

Declaration

Unless otherwise agreed, this manual is intended as a user guide only, and all statements, information and recommendations in this manual do not constitute any warranty, express or implied.

The contents of this manual are subject to change without prior notice.

To obtain the latest manual, please contact the Customer Service Department of Sangfor Technologies Co., Ltd.

Sangfor Technologies Co., Ltd. (hereinafter referred to as Sangfor Technologies Inc. or SANGFOR).

Preface

About This Manual

Part 1 Product overview of MIG 6.2.0. This part mainly introduces the appearance, function features and performance parameters of MIG 6.2.0, as well as preparations and cautions before connection.

Part 2 Introduction to the usage and functions of MIG 6.2.0 console.

Part 3 Cases. This part specifies the functions and configuration steps of various modules through application cases.

Part 4 Introductions for joining BBC. This part provides instructions for how to configure the settings of device and BBC after the device joins BBC.

This manual takes SANGFOR MIG 1000-B500 as an example. Products of different models differs in both hardware and software specifications. Therefore, please confirm with SANGFOR for all the problems involving product specifications.

Document Conventions

Format Conventions for Graphical Interface

Text Description	Symbol	Example
Button	Border+Shadow+ Shading	The "OK" button can be simplified to OK
Menu item	『 』	The menu item "System Setup" can be simplified to 『System Setup』
Continuously select menu items and submenu items	→	Select 『System Setup』→『Interface Configuration』
Drop-down list, radio box, and check box options	[ ]	The check box option "Enable User" can be simplified to [Enable User]
Window name	【 】	For example, click to pop up the 【Add User】 window
Prompt message	""	The prompt box displays "Configuration saved successfully, the configuration has been modified. The DLAN service needs to be restarted to take effect. Restart now?"

Signs

Different signs are used in this document to indicate where special attention should be paid during the operation. The meanings of these signs are as follows:

⚠ Caution, Attention: alert users to the precautions during operation. Improper operation may result in the settings invalid, data loss or device damage.

⚠ Warning: the comments after the signs require special attention. Improper operation may cause personal injuries.

💡 Instructions, Tips, Tricks: provide necessary additions and explanations to the description of the operation.

Technical Support

User Support Email: tech.support@sangfor.com

Technical Support Hotline: +6012-711 7129 (available for both cell phones and telephones)

SANGFOR Community: community.sangfor.com

SANGFOR's service provider and service validity period inquiry:

http://community.sangfor.com/plugin.php?id=service:query

Official Website: www.sangfor.com

Acknowledgement

Thank you for using our products and user manual. If you have any comments or suggestions on our products or user manual, please feel free to give us feedback by phone, forum or email, we will be very grateful.

1 Installation Guide

This part mainly introduces the hardware installation of MIG series products. Only after proper installation can you configure and use the system.

1.1. Environmental Requirements

The MIG device requires the following environment:

- 🗁 Input voltage: 110V - 230V
- 🗁 Temperature: 0 - 45℃
- 🗁 Humidity: 5 - 90%

To ensure long-term and stable running of the system, please make sure that the power supply is well grounded, dustproof measures taken, working environment well ventilated and indoor temperature kept stable. This product complies with the design requirements on environment protection. The placement, usage, and discard of the product should comply with relevant national laws and regulations where it is applied.

1.2. Power Supply

MIG series products use the power supply of AC 110V -230V. Before the power is on, please make sure that the power supply is well grounded.

1.3. Product Appearance

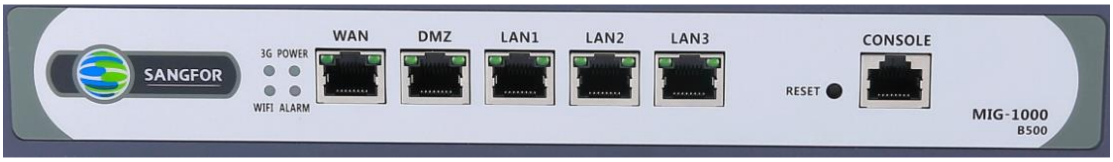


Fig. 1MIG1000-B500 Gateway Pannel

The interfaces and indicators from left to right are described respectively as follows:

3G indicator: the indicator will blink during 3G dialing; the indicator will be on when the 3G dialing is successful. The case applies to other device models supporting 4G (the indicator will be marked with "3G/4G" on top)

POWER: the power indicator of MIG device.

WIFI indicator: when the WIFI function is enabled, the indicator will be on; when the device is connecting to WIFI, the indicator will blink.

ALARM: Alarm indicator of MIG device (the indicator will keep on for 1-2 minutes when the device starts up).

WAN/WAN1: WAN1 interface of the device.

DMZ: DMZ interface of the device.

LAN1: LAN interface of the device.

LAN2: LAN interface of the device.

LAN3: LAN interface of the device.

RESET: to restore factory settings and restore default password. When MIG device is powered on, press the RESET button for 3 seconds then release, the ALARM indicator will blink red and then keep on. The indicator will turn off when the default settings are restored successfully. Short press the RESET button twice for restoring default password.

USB port: to connect with 3G Modem.

The picture above is for reference only. Please refer to the real product for different models.

The CONSOLE port is only for development, testing or debugging. For configuration, you need to connect the network interface to PC, then log in to the device through web browser.

1.4. Configuration and Management

Before configuring MIG gateway, you need to prepare a computer and make sure that the web browser is functional (Internet Explorer, Google Browser and Firefox are supported). Then connect the computer with MIG device within the same local area network, through which you can configure the device settings.

1.5. Wiring Method for Devices

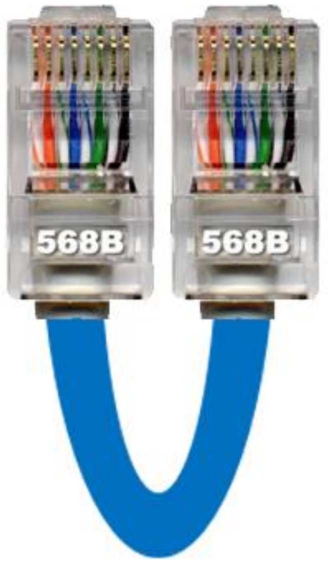
Plug the power cable into the rear panel of the device, and then turn on power supply. At this time, the Power indicator (in green) and Alarm indicator (in red) in the front panel will be on. Alarm indicator will go out in one or two minutes, indicating the gateway is working normally.

Use standard RJ-45 Ethernet cable to connect the LAN interface to the internal network (LAN) for further configuration on MIG.

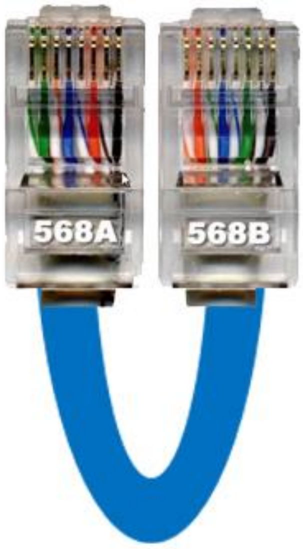
Use standard RJ-45 Ethernet cable to connect the WAN interface to the Internet access device, such as routers, optical fiber transceivers, or ADSL Modem, etc.

💡 **When the MIG device is working normally, the LINK indicators for both WAN interface and LAN interface as well as the POWER indicator will stay on. While the ACT indicator will blink constantly when there is data traffic. The ALARM indicator will keep red (for about one minute) only when the system is loading after a startup. The indicator will go out when the device is working normally. If the indicator stays on (in red) when the device is in normal working status, please switch off the power supply and reboot the device. If the red light still keeps on after reboot, please contact** us.

Use straight-through cable to connect the WAN interface to MODEM, while crossover cable should be used when connecting to router. Use straight-through cable to connect the LAN interface to the switch, while crossover cable should be used for direct connection to Ethernet interface of the computer. In case session cannot be established but the LED indicates normal working status, please check whether the cables are being used correctly. The difference between the straight-through Ethernet cable and the crossover Ethernet cable lies in the wire sequence at both ends of the cables as follows:



Straight Through Cable



Crossover Cable

1.6. Integration with BBC to Realize Easy-Deployment for Operation

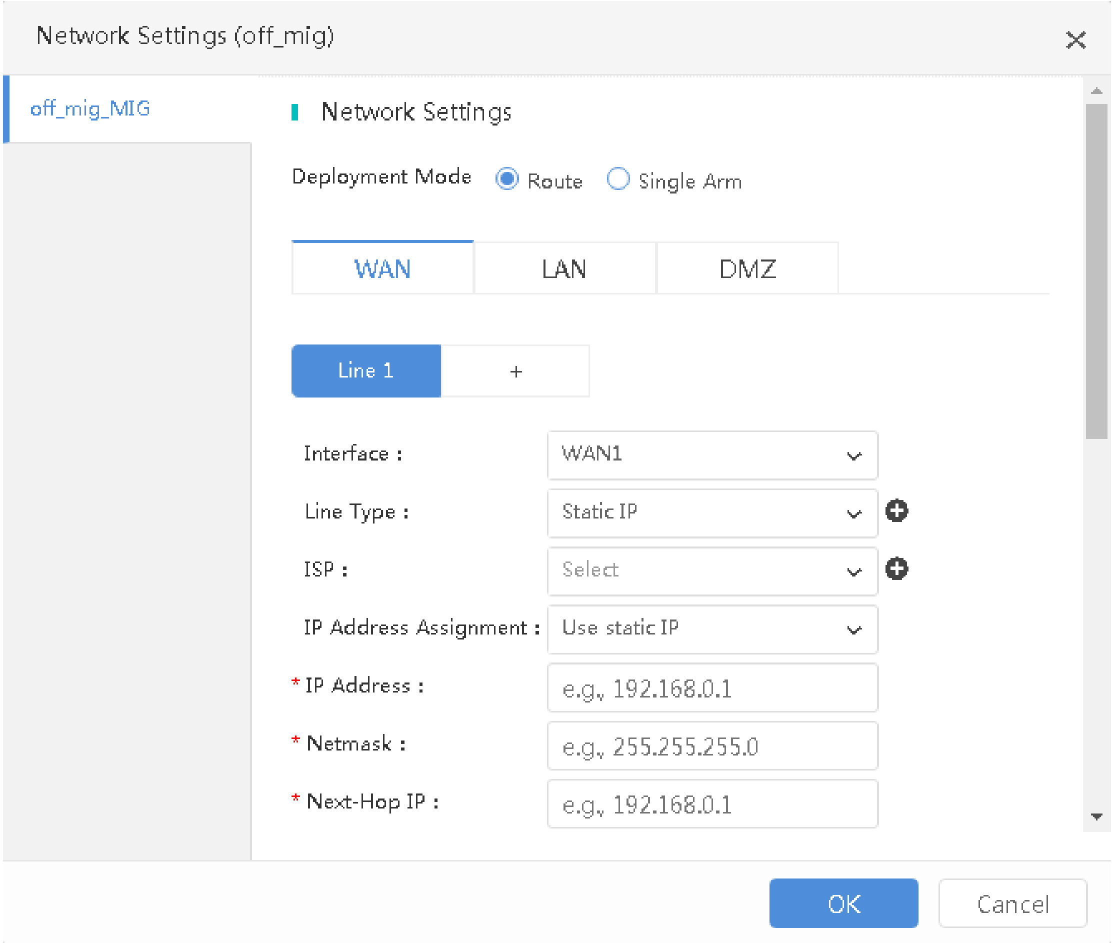
The BBC can uniformly send the configurations required for MIG to administrator by email. The administrator can check the email, then deploy the device network, access to BBC, and log in with password, thus to realize the easy-deployment.

⚠**Note：The Easy-deployment can be realized only to devices in the factory defaults. If there's any configuration changes to the device, the easy-deployment might fail unless the device is restored to factory settings. To access BBC correctly after the Easy-deployment, the BBC access address should be set before setting the Easy-deployment. The Easy-deployment email will be sent with the address. If configured incorrectly, the branches are unable to access the BBC.**

1.6.1. BBC Configuration

1.6.1.1. Create BBC Branch

Create a BBC branch, select branch device type and the like. On the page of Easy-configuration for branch device, click the 『Config』 option to configure necessary information such as branch network etc. As shown below:



Network Settings (off_mig)

Network Settings

Deployment Mode ● Route ○ Single Arm

Interface : WAN1

Line Type : Static IP

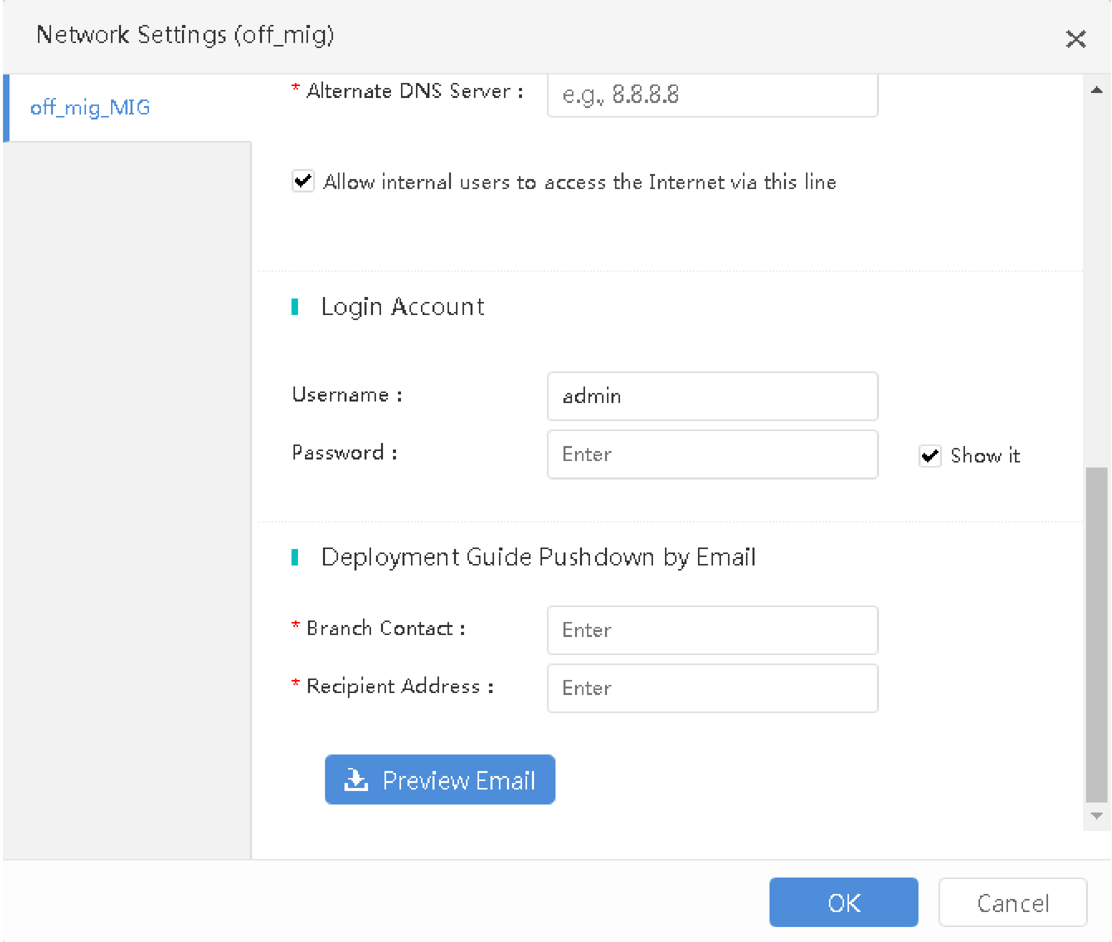
ISP : Select

IP Address Assignment : Use static IP

* IP Address : e.g., 192.168.0.1

* Netmask : e.g., 255.255.255.0

* Next-Hop IP : e.g., 192.168.0.1



Network Settings (off_mig)

off_mig_MIG

* Alternate DNS Server： e.g., 8.8.8.8

☑ Allow internal users to access the Internet via this line

Login Account

Username： admin

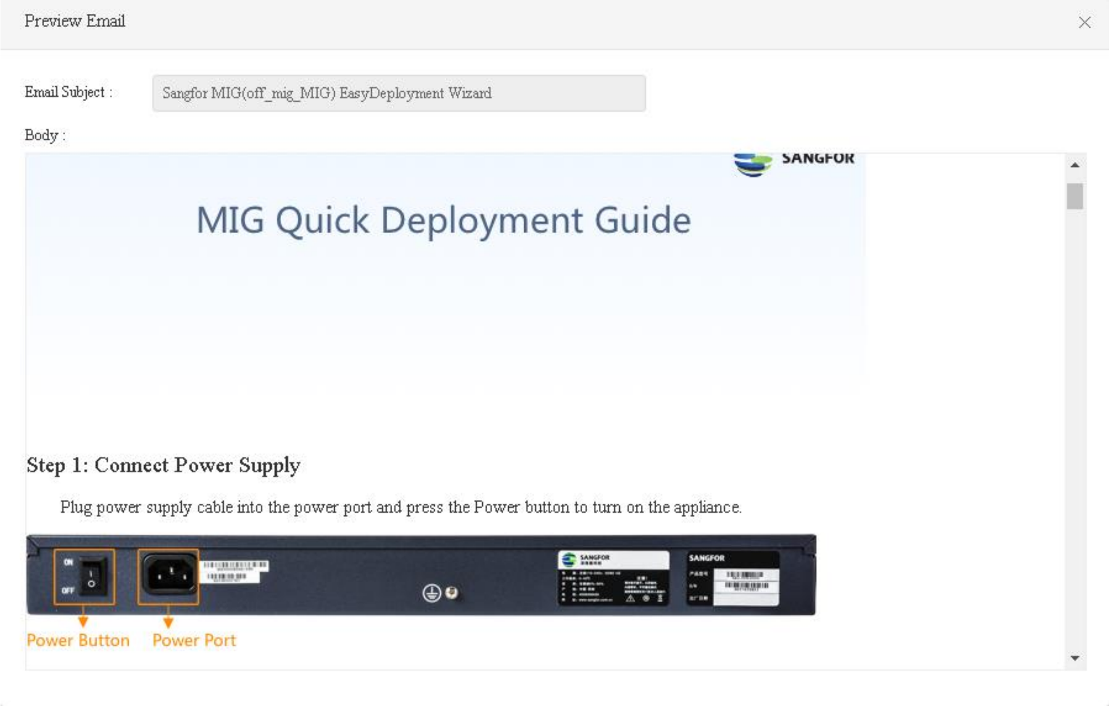
Password： Enter ☑ Show it

Deployment Guide Pushdown by Email

* Branch Contact： Enter

* Recipient Address： Enter

Click『Preview Email』to preview the email content, as follows:



Preview Email

Email Subject： Sangfor MIG(off_mig_MIG) EasyDeployment Wizard

Body：

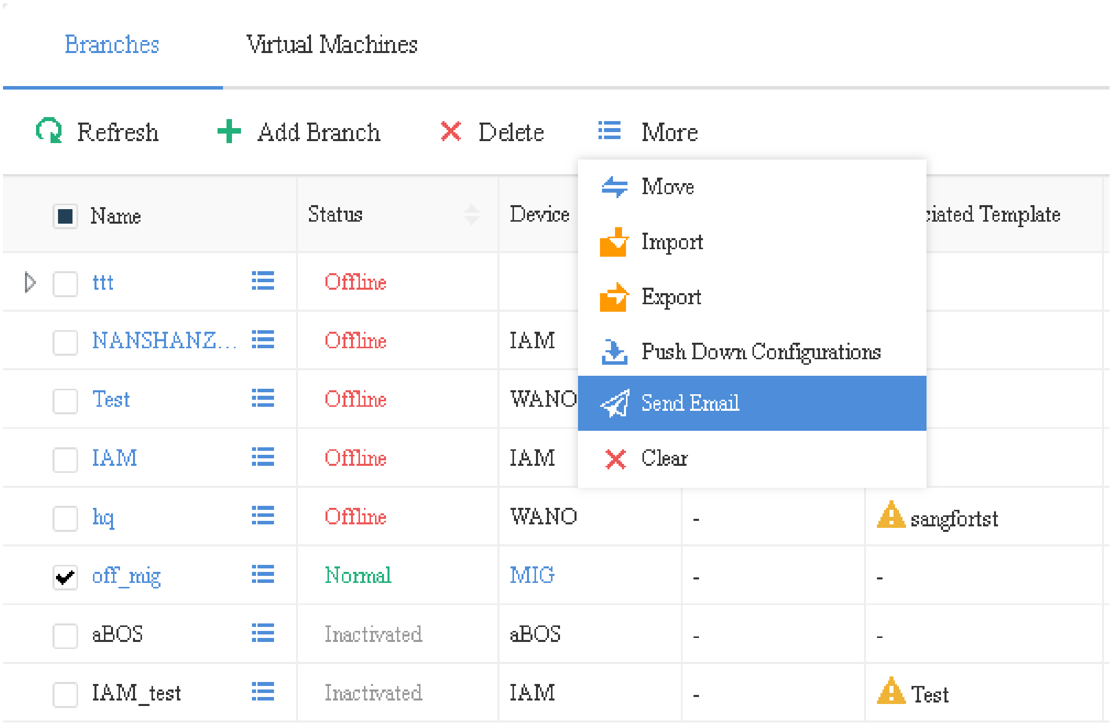
MIG Quick Deployment Guide

Step 1: Connect Power Supply

Plug power supply cable into the power port and press the Power button to turn on the appliance.

1.6.1.2. Send Deployment Emails

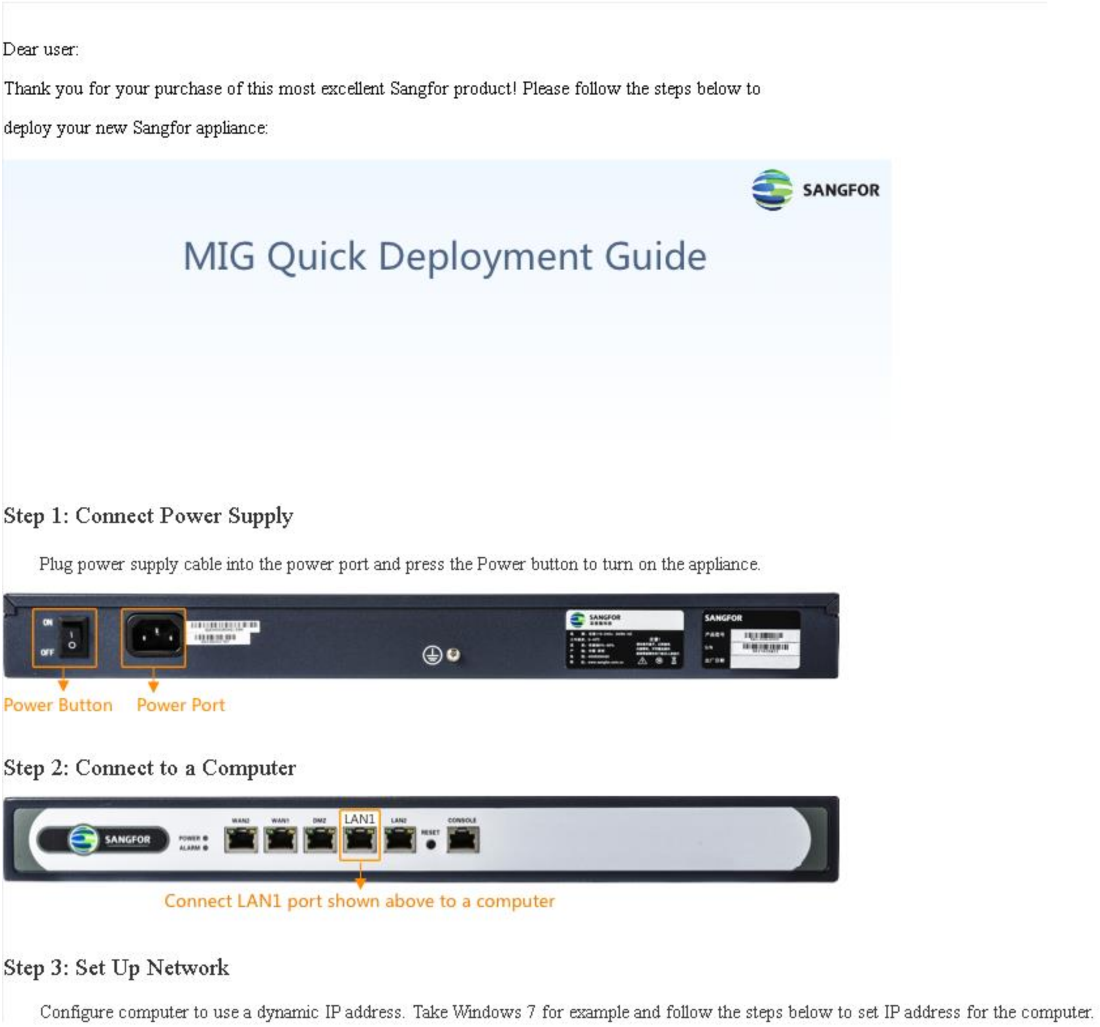
On the branch overview page, select the created branch, click 『More』 - 『Send Emails』 to send deployment emails to the mailboxes of the branch administrators.



Name	Status	Device		iated Template
ttt	Offline			
NANSHANZ...	Offline	IAM		
Test	Offline	WANO		
IAM	Offline	IAM		
hq	Offline	WANO	-	sangfortst
☑ off_mig	Normal	MIG	-	-
aBOS	Inactivated	aBOS	-	-
IAM_test	Inactivated	IAM	-	Test

1.6.2. Branch Deployment

At the branch end, the administrator should follow the instructions mentioned on the deployment mail to do configuration - turn on the device, connect network cables, and configure the IP address of the computer. Click the deployment link on the Easy-deployment mail to log in to the device (Only through the computers connected with the device can you jump to deploy). The email instruction is shown below:



Dear user:

Thank you for your purchase of this most excellent Sangfor product! Please follow the steps below to deploy your new Sangfor appliance:

MIG Quick Deployment Guide

Step 1: Connect Power Supply

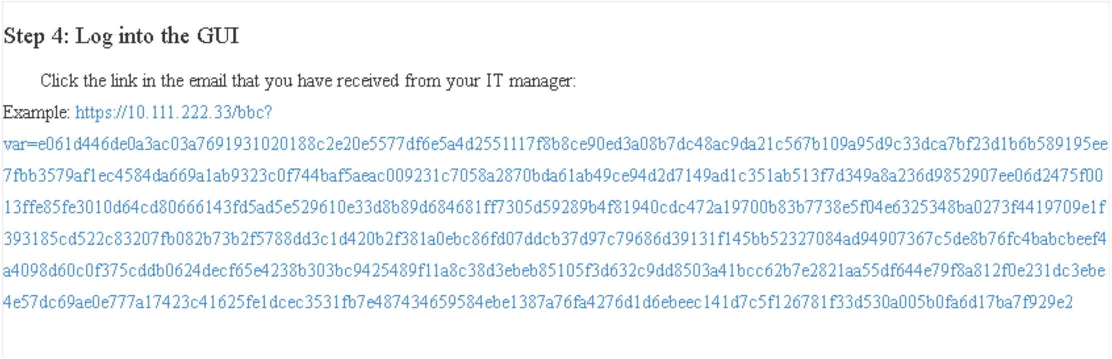
Plug power supply cable into the power port and press the Power button to turn on the appliance.

Step 2: Connect to a Computer

Connect LAN1 port shown above to a computer

Step 3: Set Up Network

Configure computer to use a dynamic IP address. Take Windows 7 for example and follow the steps below to set IP address for the computer.

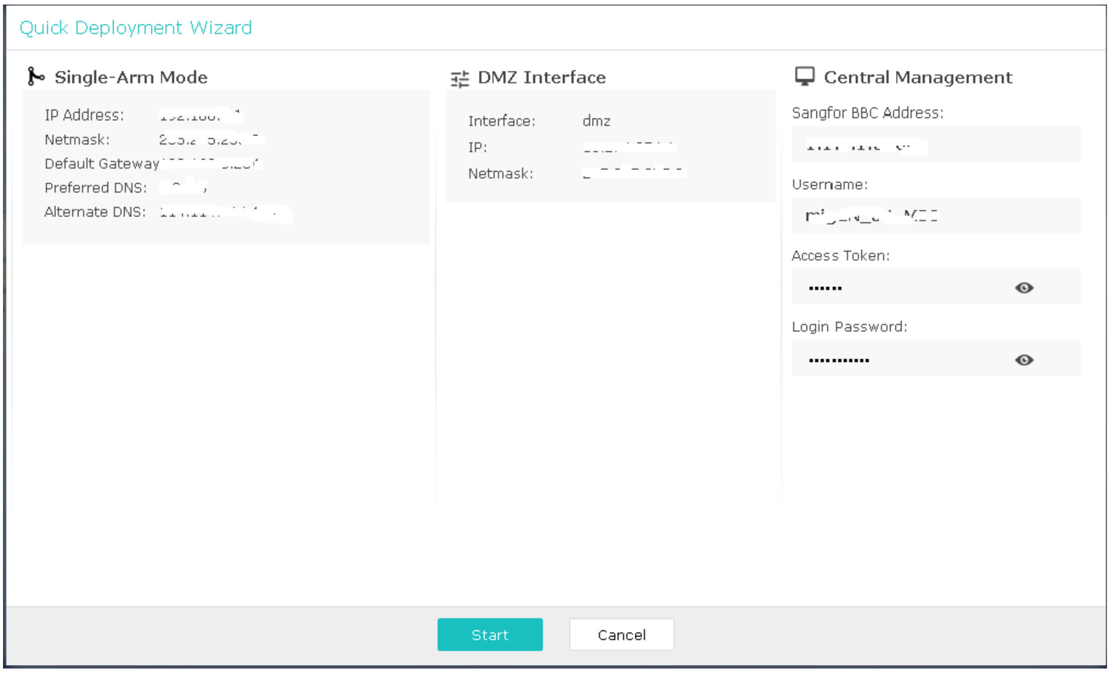


Step 4: Log into the GUI

Click the link in the email that you have received from your IT manager:

Example: https://10.111.222.33/bbc?var=e061d446de0a3ac03a7691931020188c2e20e5577df6e5a4d2551117f8b8ce90ed3a08b7dc48ac9da21c567b109a95d9c33dca7bf23d1b6b589195ee7fbb3579af1ec4584da669a1ab9323c0f744baf5aeac009231c7058a2870bda61ab49ce94d2d7149ad1c351ab513f7d349a8a236d9852907ee06d2475f0013ffe85fe3010d64cd80666143fd5ad5e529610e33d8b89d684681ff7305d59289b4f81940cdc472a19700b83b7738e5f04e6325348ba0273f4419709e1f393185cd522c83207fb082b73b2f5788dd3c1d420b2f381a0ebc86fd07ddcb37d97c79686d39131f145bb52327084ad94907367c5de8b76fc4babcbeef4a4098d60c0f375cddb0624decf65e4238b303bc9425489f11a8c38d3ebeb85105f3d632c9dd8503a41bcc62b7e2821aa55df644e79f8a812f0e231dc3ebe4e57dc69ae0e777a17423c41625fe1dcec3531fb7e487434659584ebe1387a76fa4276d1d6ebeec141d7c5f126781f33d530a005b0fa6d17ba7f929e2

After you click on the link, the browser will be opened and the device will be automatically logged on. The deployment information will appear after the successful log-on. After confirming the deployment information, click 『Start Deployment』. The configuration will be deployed successfully via emails in a few minutes. As shown below:



Quick Deployment Wizard

Single-Arm Mode

IP Address:

Netmask:

Default Gateway:

Preferred DNS:

Alternate DNS:

DMZ Interface

Interface: dmz

IP:

Netmask:

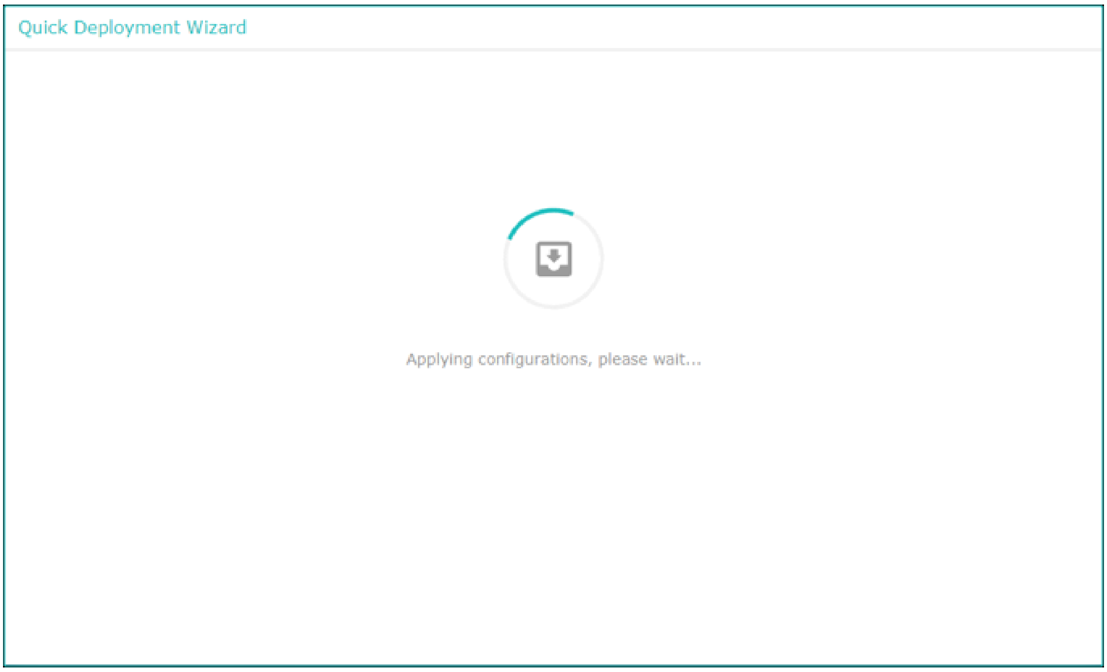
Central Management

Sangfor BBC Address:

Username:

Access Token: ••••••

Login Password: •••••••••••



Quick Deployment Wizard

Applying configurations, please wait...

2 Usage of Console

2.1. Log in to WebUI Configuration Interface

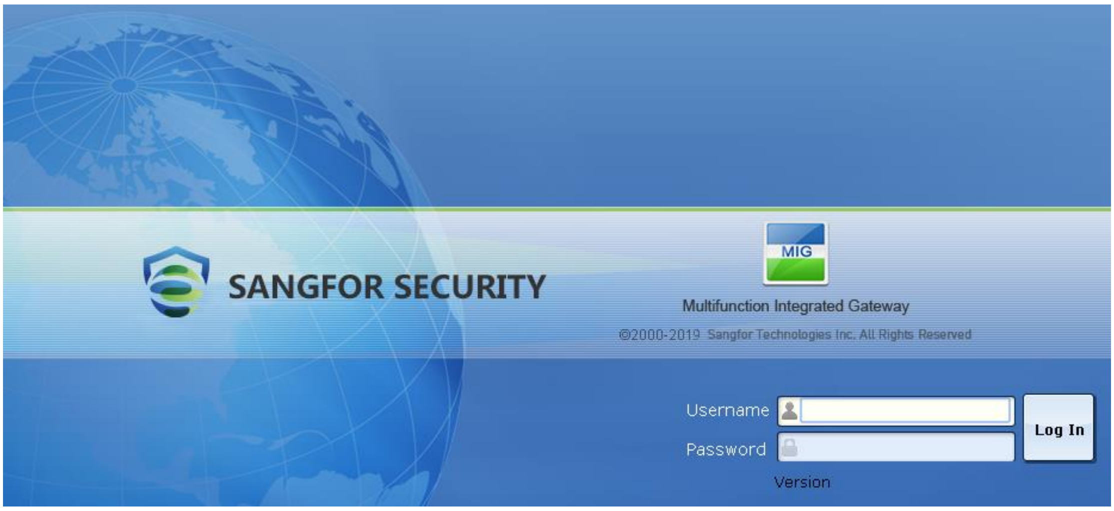
The factory default IP address of the device is shown in the table below:

Interface	IP address
LAN1, LAN2, and LAN3	10.254.254.253/24
DMZ	10.254.253.253/24

The MIG supports WEB administration. Log on via the port 443. If the initial address is used to log on the LAN, the URL address will be: https://10.254.254.253

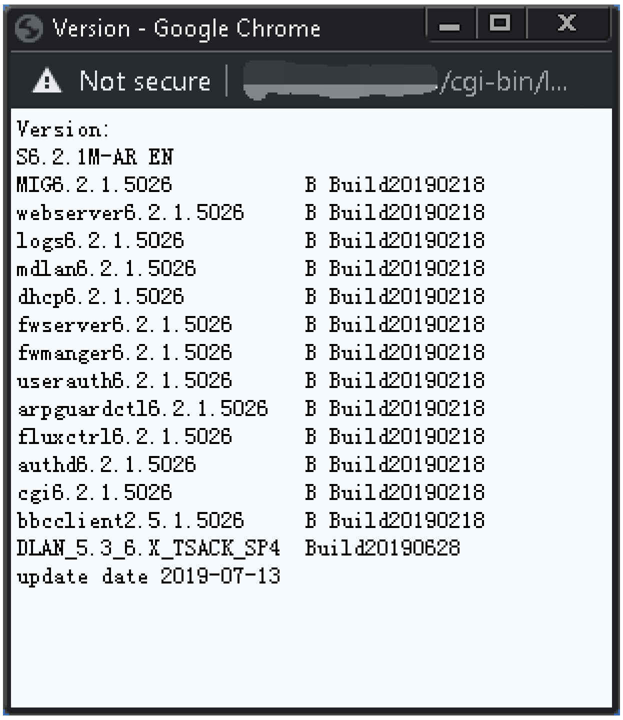
After wiring according to the method above, the MIG hardware gateway device can be configured through the Web interface. The method is described as follows:

First, configure an IP address that resides in the network segment 10.254.254.X for this machine (for example, 10.254.254.100), with subnet mask 255.255.255.0. Then enter the default IP address and port (https://10.254.254.253) of the gateway in the browser IE, Google Browser, or Firefox Browser. The page is shown as follows:


SANGFOR SECURITY
MIG
Multifunction Integrated Gateway
©2000-2019 Sangfor Technologies Inc. All Rights Reserved
Username
Password
Log In
Version

Enter username and password in the login box, and click Log In button to log in to the MIG gateway. The default username and password are: admin.

Click Version to view the version number of the current gateway. The version information of the current hardware will appear as follows:



```
Version:
S6.2.1M-AR EN
MIG6.2.1.5026           B Build20190218
webserver6.2.1.5026     B Build20190218
logs6.2.1.5026          B Build20190218
mdlan6.2.1.5026         B Build20190218
dhcp6.2.1.5026          B Build20190218
fwserver6.2.1.5026      B Build20190218
fwmanger6.2.1.5026      B Build20190218
userauth6.2.1.5026      B Build20190218
arpguardctl6.2.1.5026   B Build20190218
fluxctrl6.2.1.5026      B Build20190218
authd6.2.1.5026         B Build20190218
cgi6.2.1.5026           B Build20190218
bbcclient2.5.1.5026     B Build20190218
DLAN_5.3_6.X_TSACK_SP4  Build20190628
update date 2019-07-13
```

Log in to the WebUI Configuration Interface, and the configuration options in the left tree menu will appear as follows:

Running Status: status information such as device running status, VPN running Status, and user traffic ranking.

System Setup: settings of basic information for gateway device, such as network interface setting, route, etc.

Object Settings: settings for objects such as IP group, URL group, user group, application identification rules.

VPN Information Settings: settings for SANGFOR VPN or standard IPSEC VPN.

Access Control: settings for IPMAC authentication, authentication options, and access policy.

Traffic Management: settings for traffic policy, and line bandwidth.

Firewall Settings: settings for filtering rules, and NAT.

System Maintenance: newbie wizard, log review, policy debug, and back-up/restore settings.

⚠**Attention:**

1. Click OK or Complete button (if any) on the configuration page to save and activate

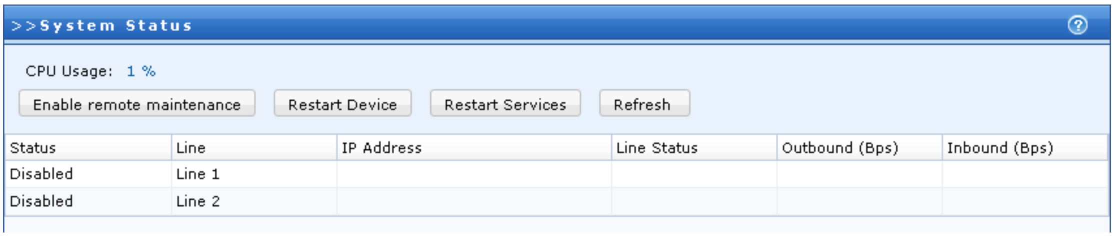
the settings. There won't be more description about this in the following content.

2. There's a Help button ? in the top right corner on every configuration page. Click the button to see the brief introduction of the current configuration items.

2.2. View Running Status

『Running Status』 allows users to view the running status of hardware gateway including『Device Running Status』, 『VPN Running Status』, 『User Traffic Ranking』, 『Application Traffic Ranking』, 『Online Behavior Record』, 『View Online Users』, and 『DHCP Running Status』.

2.2.1. Device Running Status


>>System Status

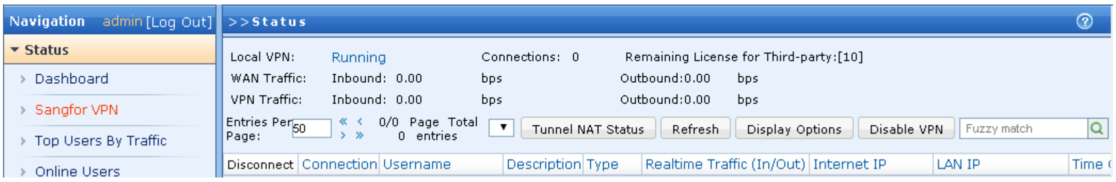
CPU Usage: 1 %

Status	Line	IP Address	Line Status	Outbound (Bps)	Inbound (Bps)
Disabled	Line 1				
Disabled	Line 2				

『Device Running Status』 allows users to view 『CPU Occupancy』 and overview of external network lines, and Restart Device or Restart Service. Activate [Allow Remote Connection] if needs to log in to gateway through external network for management.

2.2.2. VPN Running Status

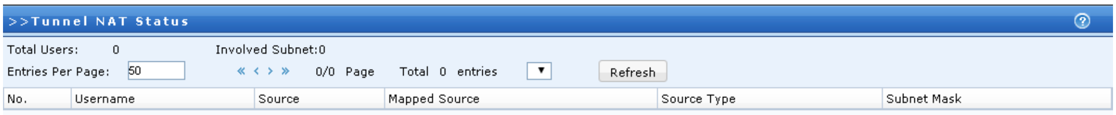
This page allows users to view the information about the current VPN connection and network traffic. The page is shown as follows:



Local VPN: Running Connections: 0 Remaining License for Third-party:[10]
WAN Traffic: Inbound: 0.00 bps Outbound:0.00 bps
VPN Traffic: Inbound: 0.00 bps Outbound:0.00 bps
Entries Per Page: 50 0/0 Page Total 0 entries

Disconnect	Connection	Username	Description	Type	Realtime Traffic (In/Out)	Internet IP	LAN IP	Time

Click Tunnel NAT Status to view the NAT status of the branches currently accessed, including username, initial subnet segment, proxy subnet segment, network types, and subnet mask. The page is available after VPN in-tunnel NAT is configured. The page is shown as follows:

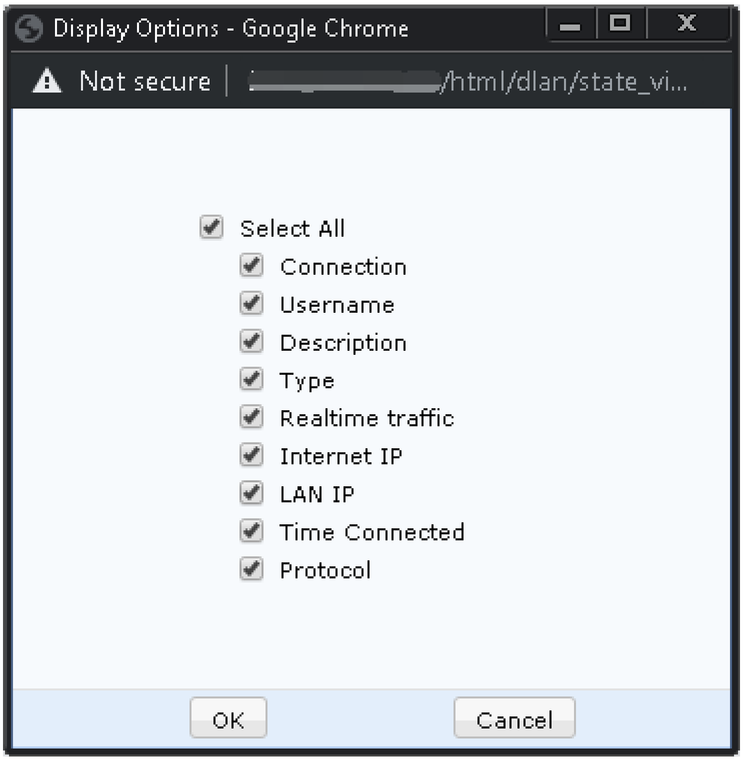


Total Users: 0 Involved Subnet:0
Entries Per Page: 50 0/0 Page Total 0 entries

No.	Username	Source	Mapped Source	Source Type	Subnet Mask

Click Refresh to view the current information about the VPN connection and network traffic.

Click Display Options to filter the list displayed. The page is shown as follows:



Display Options - Google Chrome

Not secure | [redacted]/html/dlan/state_vi...

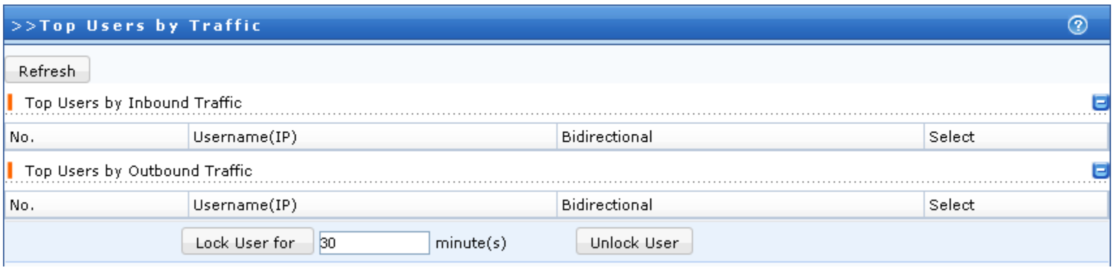
☑ Select All
- ☑ Connection
- ☑ Username
- ☑ Description
- ☑ Type
- ☑ Realtime traffic
- ☑ Internet IP
- ☑ LAN IP
- ☑ Time Connected
- ☑ Protocol

Click Disable VPN/Enable VPN to stop or start the VPN service.

Enter the username in the Fuzzy Match Search input box to rapidly view the connection status of the user. The fuzzy search function is available.

2.2.3. User Traffic Ranking

『User Traffic Ranking』 allows users to view the current network traffic information for Internet access from the Internal network (LAN) user. Able to block the selected user from accessing the Internet.



>>Top Users by Traffic

Top Users by Inbound Traffic

No.	Username(IP)	Bidirectional	Select

Top Users by Outbound Traffic

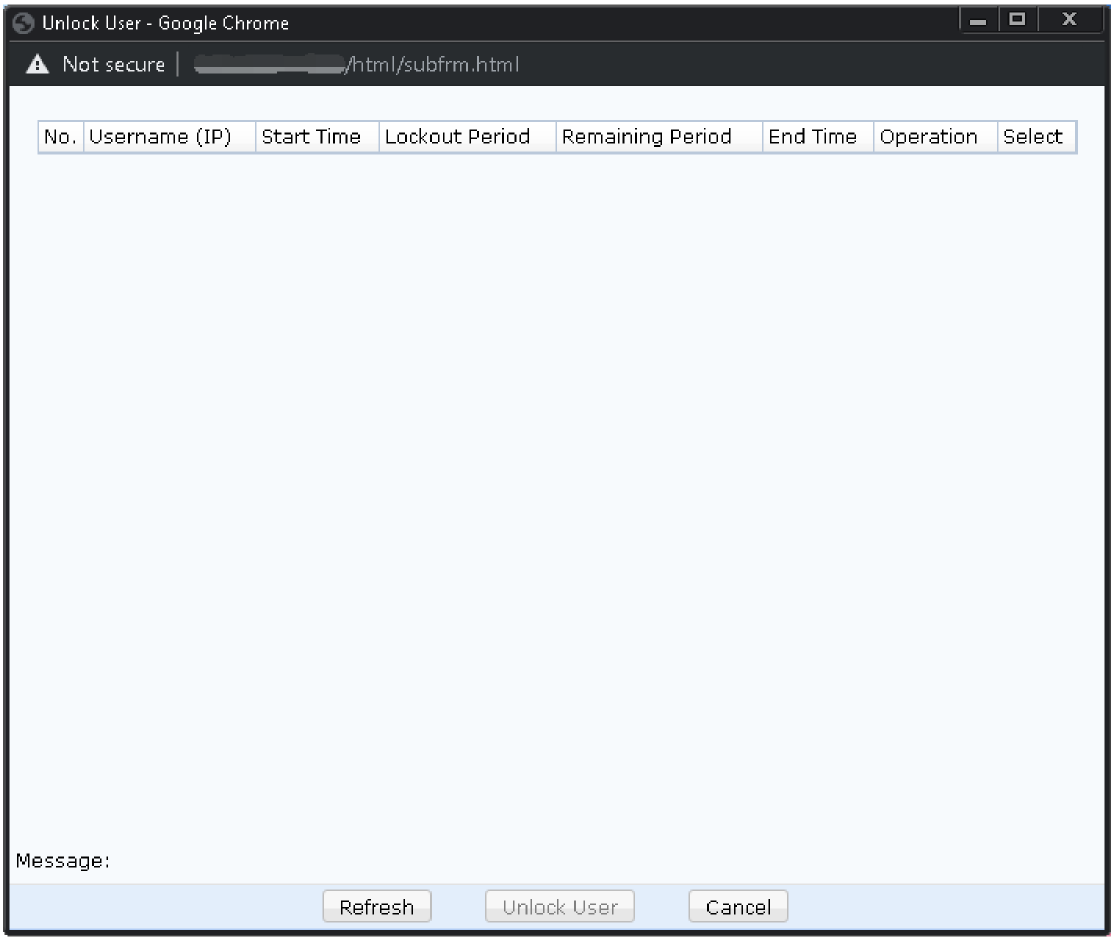
No.	Username(IP)	Bidirectional	Select

Lock User for 30 minute(s) Unlock User

Click Refresh to manually refresh the traffic ranking status on the page.

Select the user to be locked, set the locking period, and click Lock User for to ban the user from uploading data.

Click Refresh again and you can see that the corresponding IP has no uploading data (Currently, the IP can not access the Internet); Click Unlock User and you can see that the user is in the list of Unlock Users as follows:



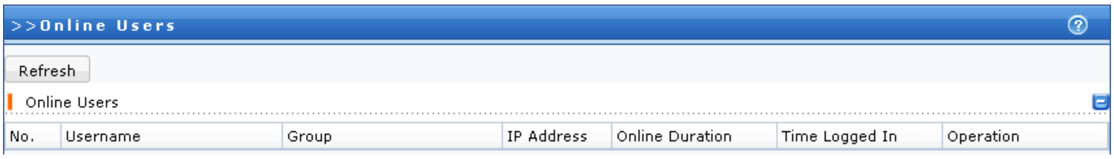
No.	Username (IP)	Start Time	Lockout Period	Remaining Period	End Time	Operation	Select

Message:

Click Unlock to unlock the users. Select all the users to be unblocked, and click Unlock User to unlock all the selected users.

2.2.4. View Online Users

『View Online Users』 allows to view the information of online users including the user name, the group, the IP address, and online time. See the following figure:



>>Online Users

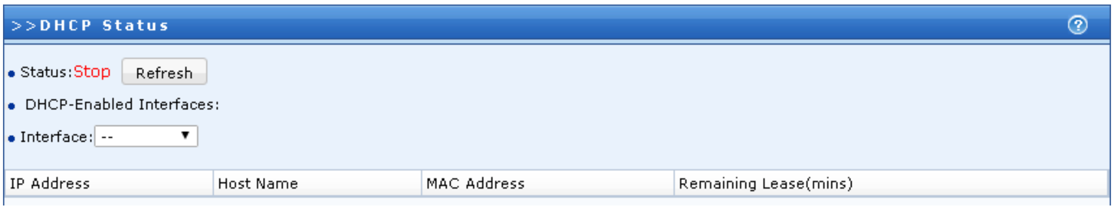
Refresh

Online Users

No.	Username	Group	IP Address	Online Duration	Time Logged In	Operation

2.2.5. DHCP Running Status

『DHCP Running Status』 allows users to view the running status of DHCP, and the IP allocation of other computers. See the following figure:



>>DHCP Status

- Status:Stop Refresh
- DHCP-Enabled Interfaces:
- Interface: --

IP Address	Host Name	MAC Address	Remaining Lease(mins)

Click Refresh to view the real-time DHCP running status.

『Allocated Network Interface』: choose to view the DHCP running status of different network interface.

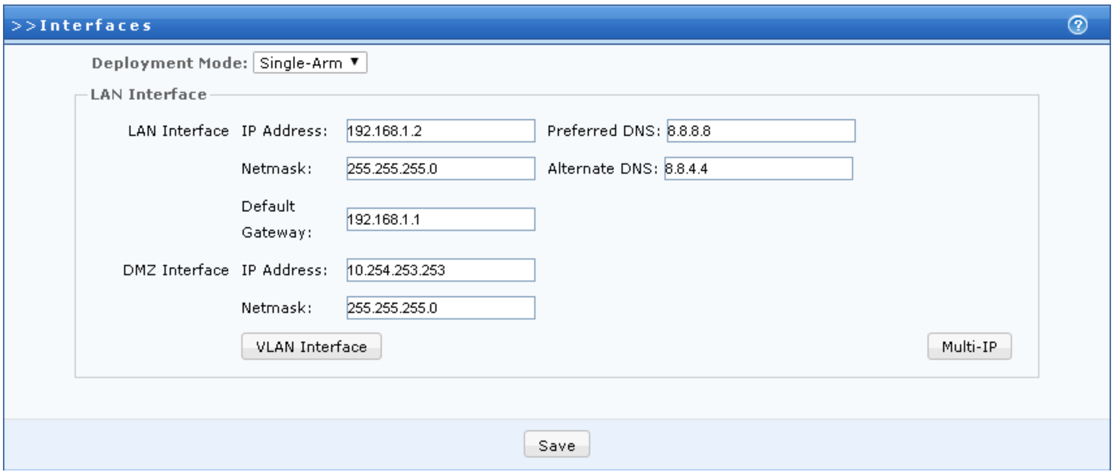
2.3. System Setup

Include modules of 『Network Interface Setting』, 『Serial No. Setting』,『System Time Setting』, 『Route Setting』, 『Mult-line Setting』, 『Local Subnet List』, 『Console Setting』, 『SYSLOG Setting』, 『DHCP Setting』, 『WLAN Setting』, 『Generate Certificates』，『Auto-upgrade Application Recognition Base』 and 『Setting for Joining to Unified Management』.

2.3.1. Network Interface Setting

For configuring the working modes for the device. Two working modes are available: the one-arm mode and the gateway mode.

When selecting the one-arm mode, you need to configure the IP address, subnet mask, and the default gateway of the LAN interface, configure the IP address of DMZ interface, and subnet mask, and configure DNS, and VLAN settings. The page is shown as follows:



>>Interfaces

Deployment Mode: Single-Arm

LAN Interface

LAN Interface IP Address: 192.168.1.2 Preferred DNS: 8.8.8.8

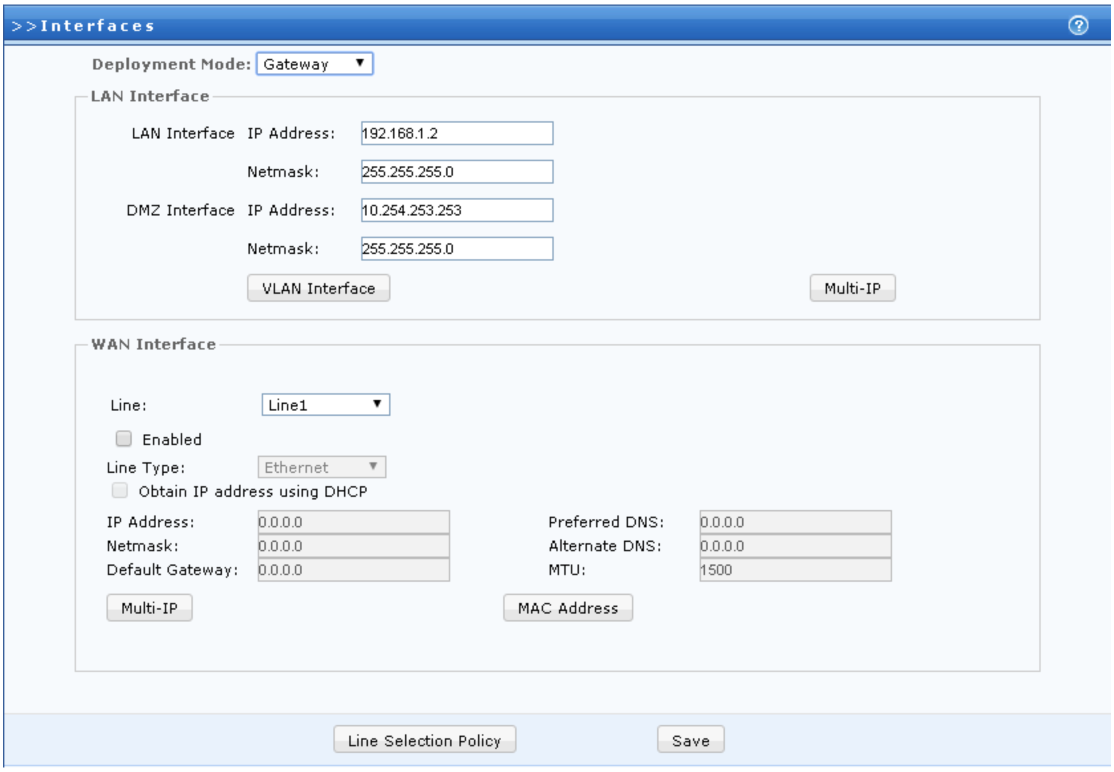
Netmask: 255.255.255.0 Alternate DNS: 8.8.4.4

Default Gateway: 192.168.1.1

DMZ Interface IP Address: 10.254.253.253

Netmask: 255.255.255.0

When selecting the gateway mode, you need not only to configure LAN interface, but also configure the corresponding external network lines. The configuration interface is shown as follows:



>>Interfaces

Deployment Mode: Gateway

LAN Interface

LAN Interface IP Address: 192.168.1.2

Netmask: 255.255.255.0

DMZ Interface IP Address: 10.254.253.253

Netmask: 255.255.255.0

WAN Interface

Line: Line1

□ Enabled

Line Type: Ethernet

□ Obtain IP address using DHCP

IP Address: 0.0.0.0

Netmask: 0.0.0.0

Default Gateway: 0.0.0.0

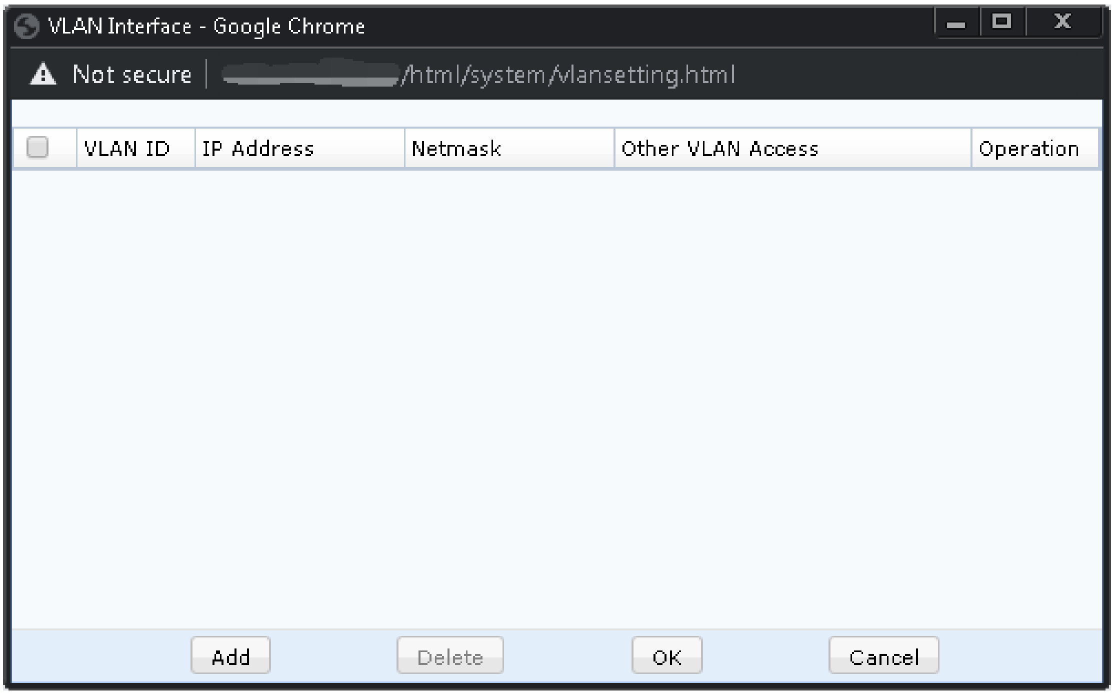
Preferred DNS: 0.0.0.0

Alternate DNS: 0.0.0.0

MTU: 1500

『LAN Interface』: set the corresponding IP address of the interface according to the actual situation;

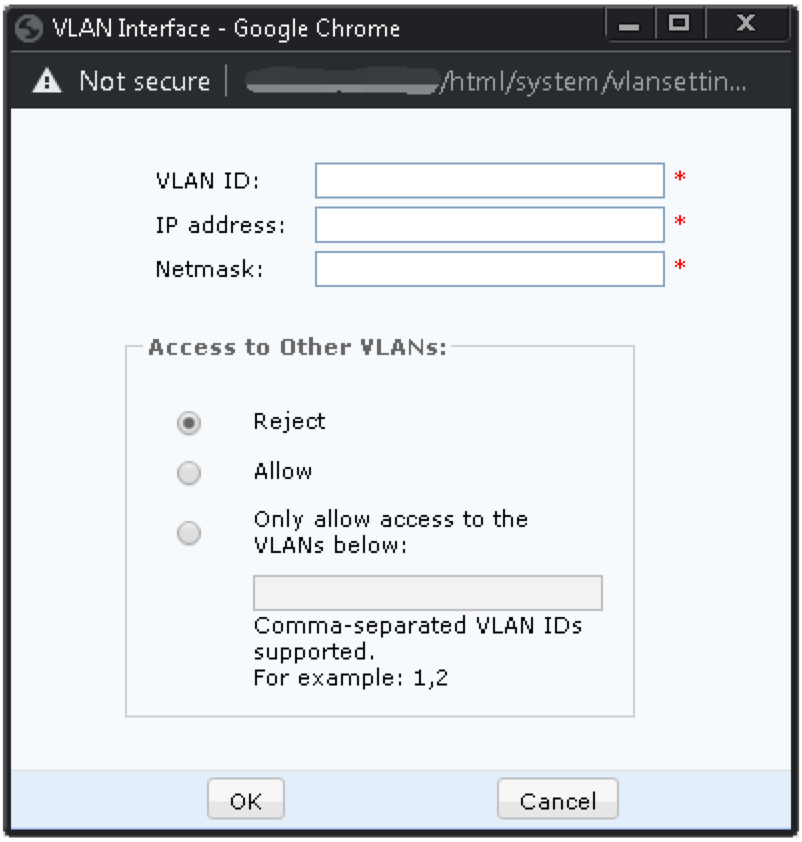
『VLAN Interface』: allows user to segment the LAN port into multiple VLANs to realize multi-segment isolation. The interface is shown as follows:



VLAN Interface - Google Chrome
Not secure | [redacted]/html/system/vlansetting.html

□	VLAN ID	IP Address	Netmask	Other VLAN Access	Operation

Click Add to create VLAN segments. The configuration interface is as follows:



VLAN Interface - Google Chrome
Not secure | [redacted]/html/system/vlansettin...

VLAN ID: ________ *

IP address: ________ *

Netmask: ________ *

Access to Other VLANs:

● Reject

○ Allow

○ Only allow access to the VLANs below:

____

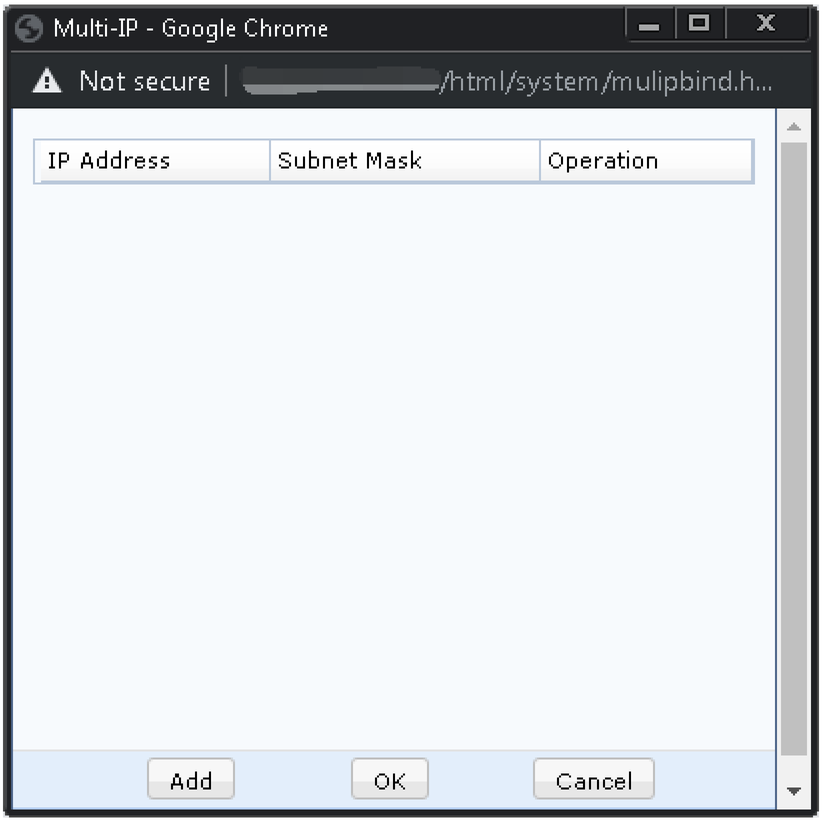
Comma-separated VLAN IDs supported.
For example: 1,2

“VLAN ID” is the VLAN identifier for the new VLAN label, with setting range of 1-4094.

"IP address and Subnet mask" is the address and the interface address of the VLAN for interconnection with other addresses.

"Permission to access other VLAN?" allows users to set the access permission among VLANs, including Allow, Reject, or only allow access for specific VLAN.

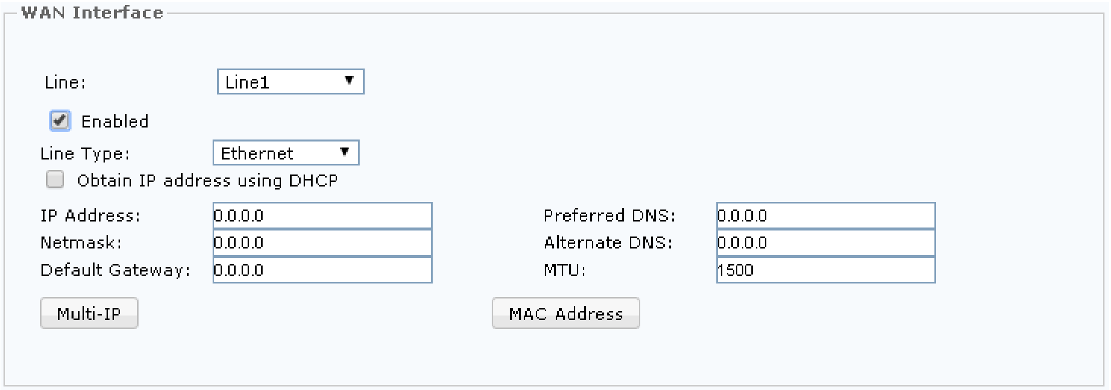
『Setting Multi IPs for LAN』 allows users to allocate IP in multiple segments for the LAN Interface. The interface after clicking is as follows:



IP Address	Subnet Mask	Operation

『External Network Interface Setting』 Choose "Line 1"or "Line 2-4G Line"

[Line 1 Setting]: click [Line 1] , check [Enable the Line] , then set [Line Type]. Two types are available - “Ethernet” and “ADSL”. The interface is shown as follows:



WAN Interface

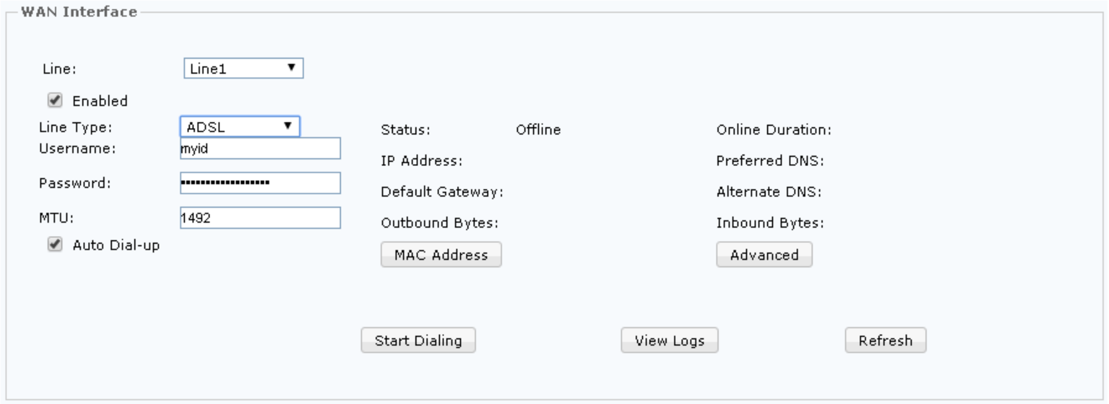
Line: Line1

☑ Enabled

Line Type: Ethernet

□ Obtain IP address using DHCP

IP Address:	0.0.0.0	Preferred DNS:	0.0.0.0
Netmask:	0.0.0.0	Alternate DNS:	0.0.0.0
Default Gateway:	0.0.0.0	MTU:	1500



WAN Interface

Line: Line1

☑ Enabled

Line Type: ADSL

Username: myid

Password: ••••••••••••••••••••

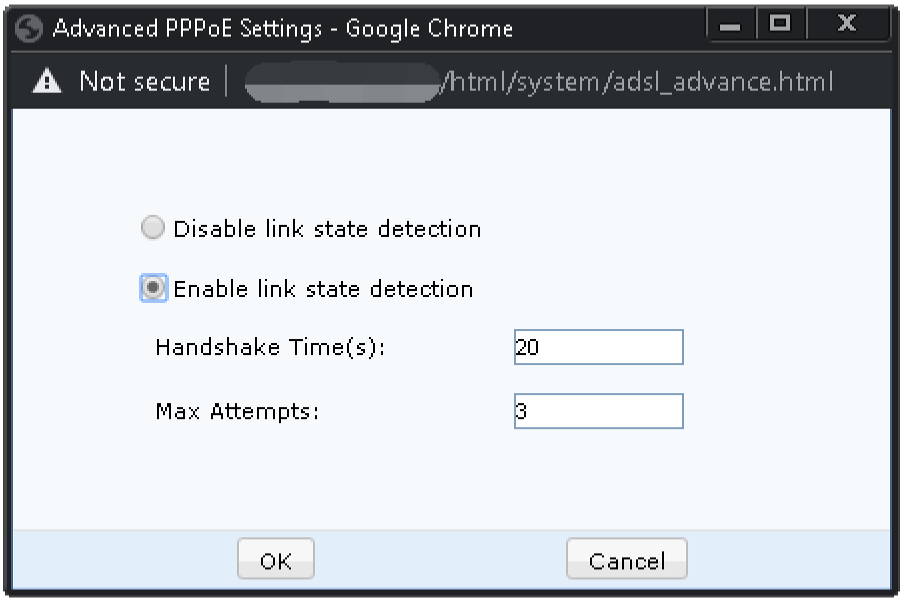
MTU: 1492

☑ Auto Dial-up

Status:	Offline	Online Duration:	
IP Address:		Preferred DNS:	
Default Gateway:		Alternate DNS:	
Outbound Bytes:		Inbound Bytes:	

When choosing line 1 for ADSL dialing, please check [Start Dialing] after enter the [User Name] and [Password]. Please click OK to save the setting after the configuration. The device will reboot all the services. Relog in and click Start Dialing, and the device will "Auto Dialing" after each disconnection. Click View Log to view the real-time dialing log.

Click Advanced Setting to set the Offline Detection Mechanism for ADSL dialing. You can choose [No Offline Detection] or [Conduct Offline Detection] in the following picture:


Advanced PPPoE Settings - Google Chrome
Not secure | [redacted]/html/system/adsl_advance.html
OK
Cancel

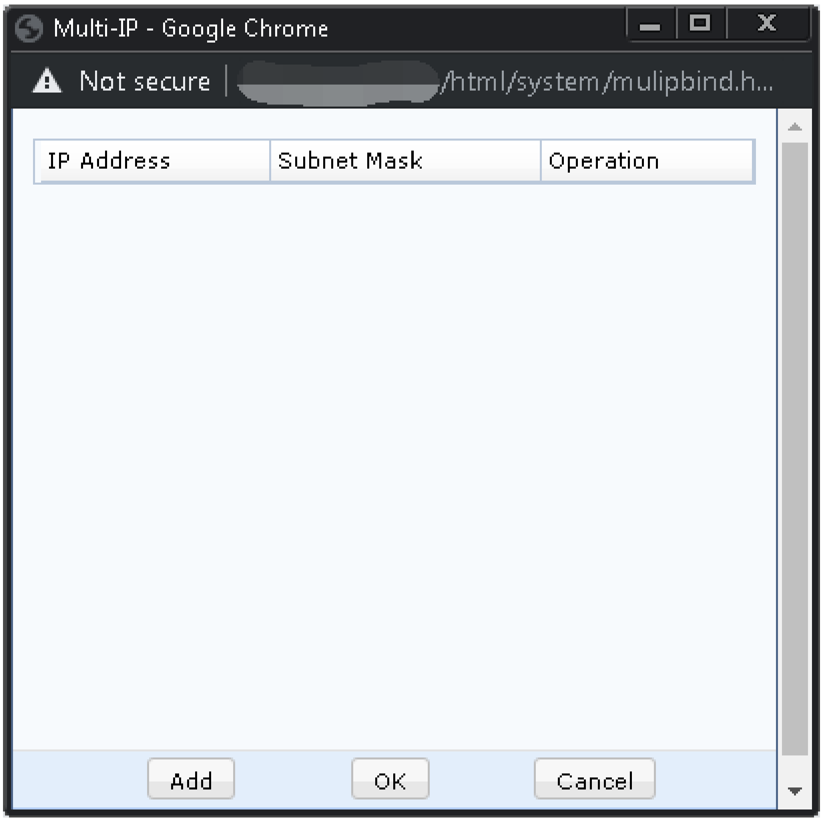
○ Disable link state detection

● Enable link state detection

Handshake Time(s): 20

Max Attempts: 3

[Multi-IP Binding]: available when the external network interface is under the Ethernet Mode. Multiple IP addresses can be obtained when setting the external network interface. The IP addresses are available only after mapping to internal network servers. Click Multi-IP Bind button, and the following dialog box will appear. Click New to bind multiple IP addresses for the WAN interface as follows:

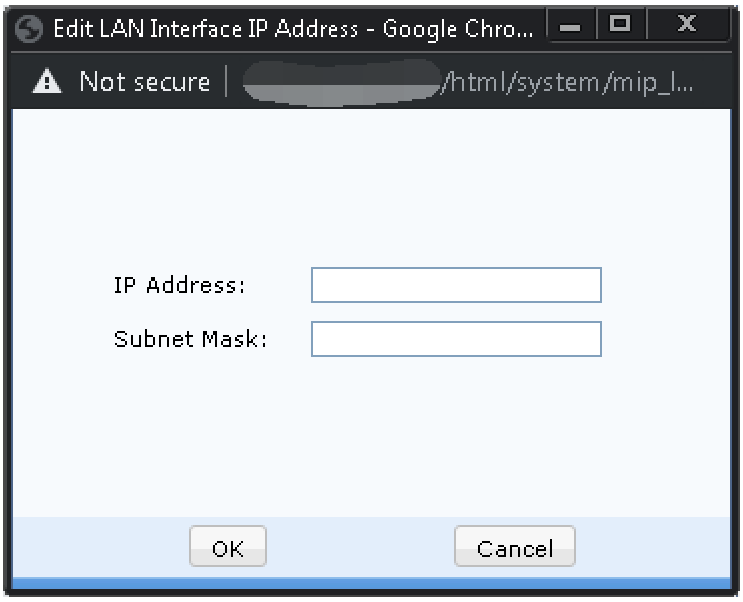


Multi-IP - Google Chrome

Not secure | [redacted]/html/system/mulipbind.h...

IP Address	Subnet Mask	Operation

Click Add to add VLAN segments. The configuration interface is as follows:



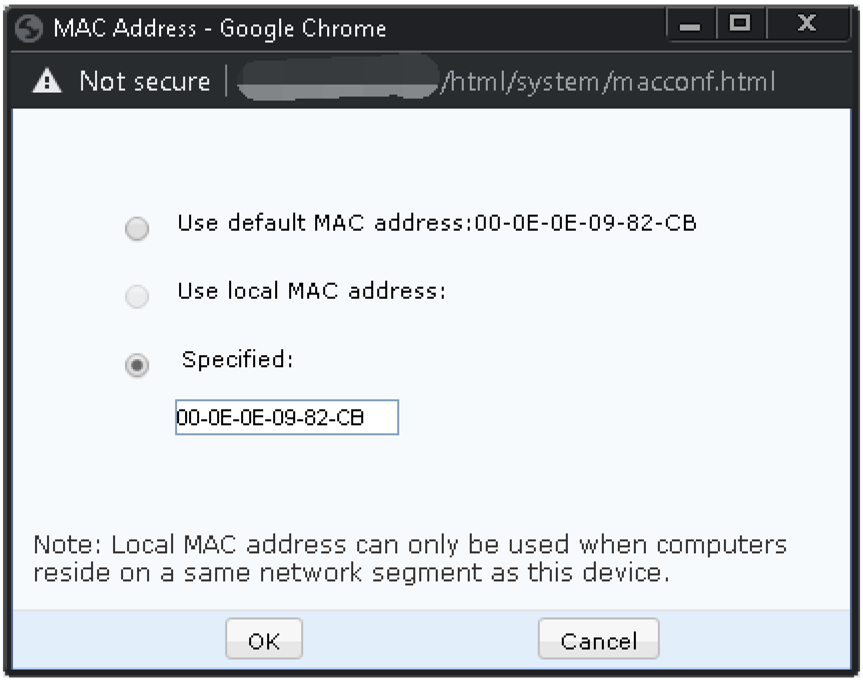
Edit LAN Interface IP Address - Google Chro...

Not secure | [redacted]/html/system/mip_l...

IP Address:

Subnet Mask:

[MAC Setting]: mainly for modifying the MAC address for the WAN port. Click "Use Local MAC" to use the MAC that is currently used when logging in to console from PC network interface. Click Mac Setting, the following dialog box will appear, which is for modifying the MAC address of the WAN interface.



MAC Address - Google Chrome

Not secure | [redacted]/html/system/macconf.html

○ Use default MAC address:00-0E-0E-09-82-CB

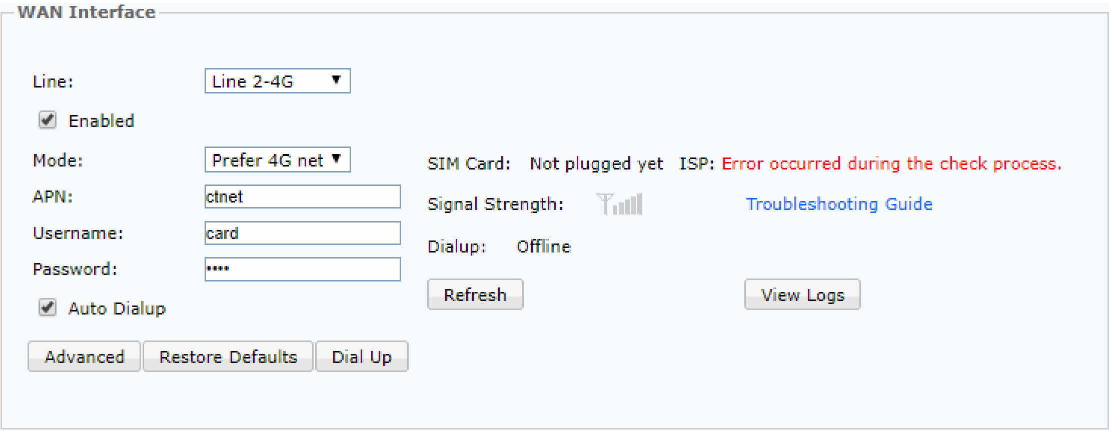
○ Use local MAC address:

● Specified:

00-0E-0E-09-82-CB

Note: Local MAC address can only be used when computers reside on a same network segment as this device.

[Line 2-4G Line Configuration]: MIG 1110 and MIG 1110-W devices support 4G dialing function. Select [Line 2-4G Line] when selecting Lines, and check [Enable the Line]. The configuration interface is as follows:



WAN Interface

Line: Line 2-4G

☑ Enabled

Mode: Prefer 4G net

APN: ctnet

Username: card

Password: ••••

☑ Auto Dialup

SIM Card: Not plugged yet ISP: Error occurred during the check process.

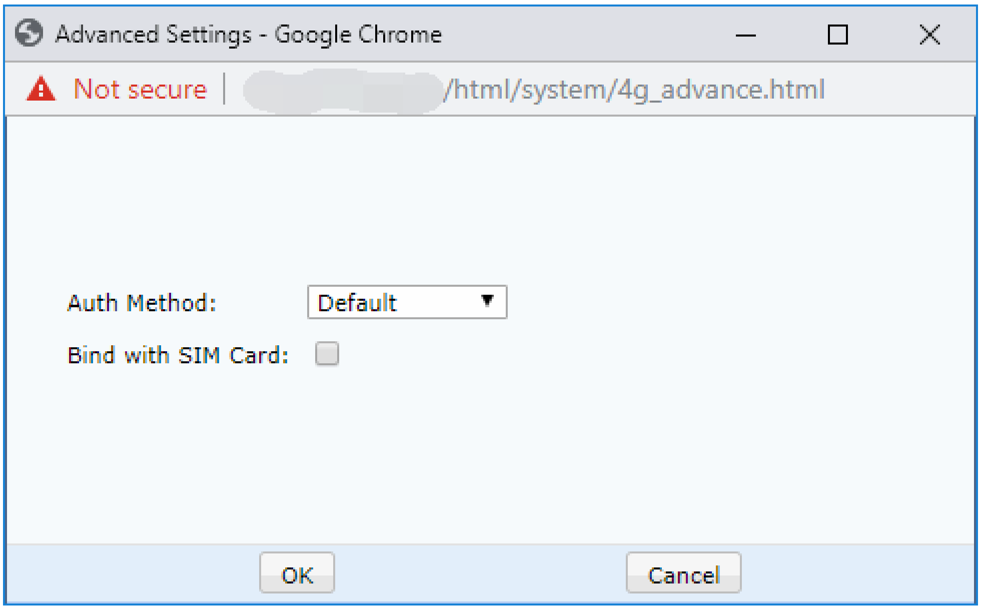
Signal Strength:

Troubleshooting Guide

Dialup: Offline

Select Mode, and you can choose 4G First, 3G First, or Only 4G

Click Advanced Setting to set the Authentication Method of 4G dialing and choose to Bind SIM Card. In Authentication Method, you can choose Default, PAP Authentication, or CHAP Authentication; When you check Bind SIM Card, you can only use the bound SIM card to dial. Others are not available. See the following figure:



Advanced Settings - Google Chrome

Not secure | [redacted]/html/system/4g_advance.html

Auth Method: Default ▼

Bind with SIM Card: □

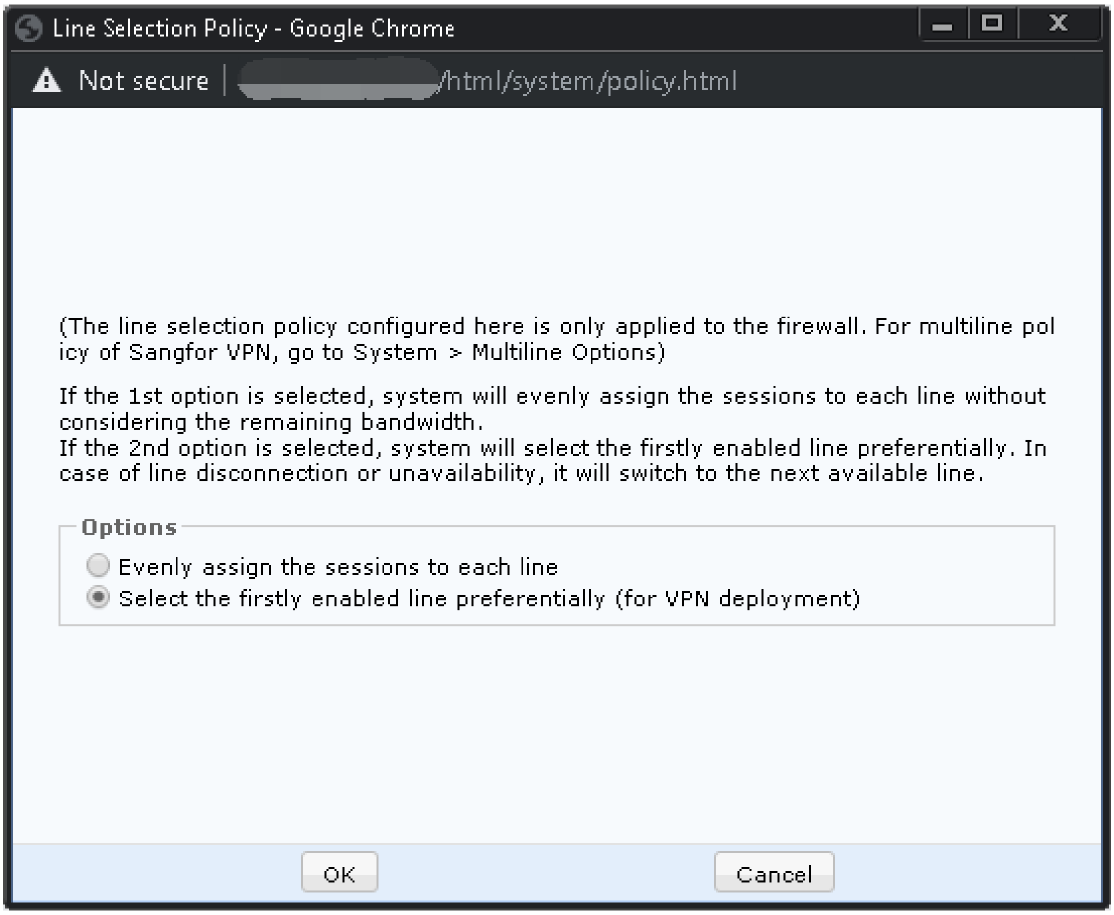
Click View Log to view the relevant log of the 4G dialing.

When you choose 4G Line, you only need to insert 4G card into the 4G card slot correctly. The APN code, dialing strings, the user name, and password will be automatically generated. No re-configuration is required. If necessary, edit in the text box directly.

Note: 4G Line supports China Telecom, China Mobile, and China Unicom, which can be automatically recognized through SIM card, and displayed in "Current Network" status.

[Distribution Policy]: allows users to set the selection policy of the MIG devices to external network lines. Refer to the Help on the top of the dialog box for further information.

Click "Line Selection Policy" button and the following dialog box will appear:


Line Selection Policy - Google Chrome
Not secure | [redacted]/html/system/policy.html

(The line selection policy configured here is only applied to the firewall. For multiline pol icy of Sangfor VPN, go to System > Multiline Options)

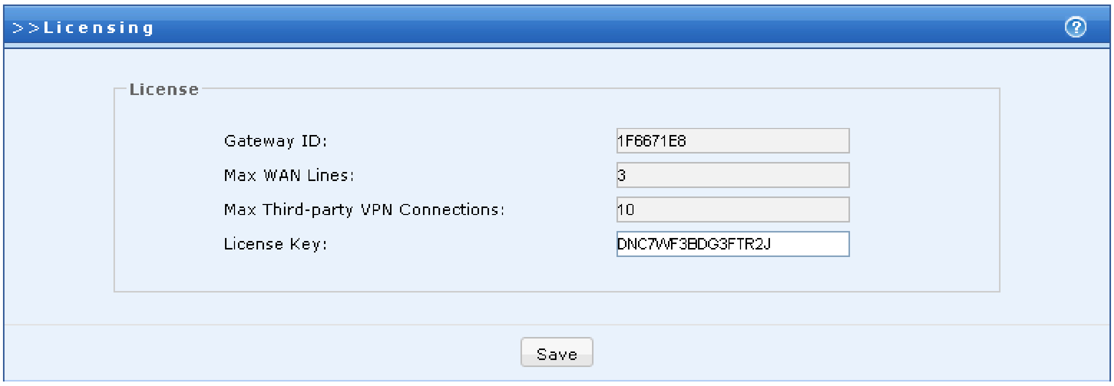
If the 1st option is selected, system will evenly assign the sessions to each line without considering the remaining bandwidth.
If the 2nd option is selected, system will select the firstly enabled line preferentially. In case of line disconnection or unavailability, it will switch to the next available line.

Options

○ Evenly assign the sessions to each line
● Select the firstly enabled line preferentially (for VPN deployment)

2.3.2. License Key

『License Key』 allows users to enter the License of the MIG hardware gateway. The licnese controls the quantity of lines of available external network, and the quantity of the third-party docking for IPSec. Different serial numbers have corresponding line quantity and access user quantity. After filling in the license key, the authentication quantity will be automatically generated. The Upgrade Licnese of Application Identification Base decides whether the MIG supports auto-upgrade for built-in application identification base. The configuration interface is as follows. Fill in the License, and Click Ok to save.



License

Gateway ID: 1F6671E8
Max WAN Lines: 3
Max Third-party VPN Connections: 10
License Key: DNC7WF3BDG3FTR2J

『Max WAN Lines』: the product has only one WAN interface, so the quantity is 3, which can not be modified.

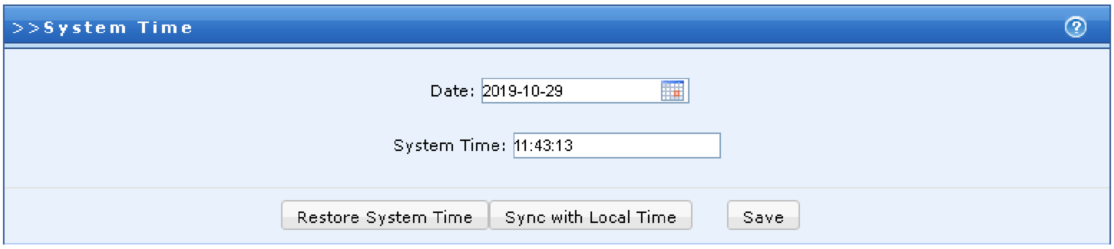
『Max Third-party VPN Connections』: define the quantity of third party device, which is automatically generated via『Licnese Key』and can not be modified.

『Gateway ID』: the hardware ID of the device, which is factory default and can not be modified.

『License Key』 : control the license of 『Max Third-party VPN Connections』. If you need more, you need to purchase new license.

2.3.3. System Time Setting

Set the system time of the MIG hardware gateway. Click Restore System Time to refresh the system time of the MIG hardware gateway. Click Sync with Local Time to modify the system time of the MIG hardware gateway into the computer time of the Web login. Click OK to save the setting. The page is shown as follows:

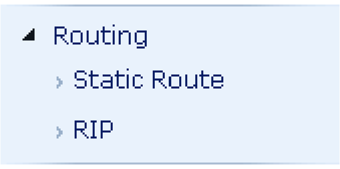


Date: 2019-10-29

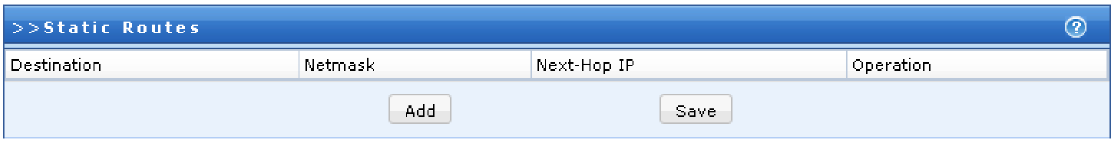
System Time: 11:43:13

2.3.4. Route Setting

Set the system route of the MIG device. Include the static ones and dynamic ones. The page is shown as follows:



2.3.4.1. Statis Route Setting



Destination	Netmask	Next-Hop IP	Operation

『Statis Route Setting』 mainly used to realize two functions:

1. Add default route when multiple segments access the Internet via the proxy.

2. Set the route when access to VPN internal multi-subnets is required.

1. Add "Static route" when multiple segments access the Internet via proxy

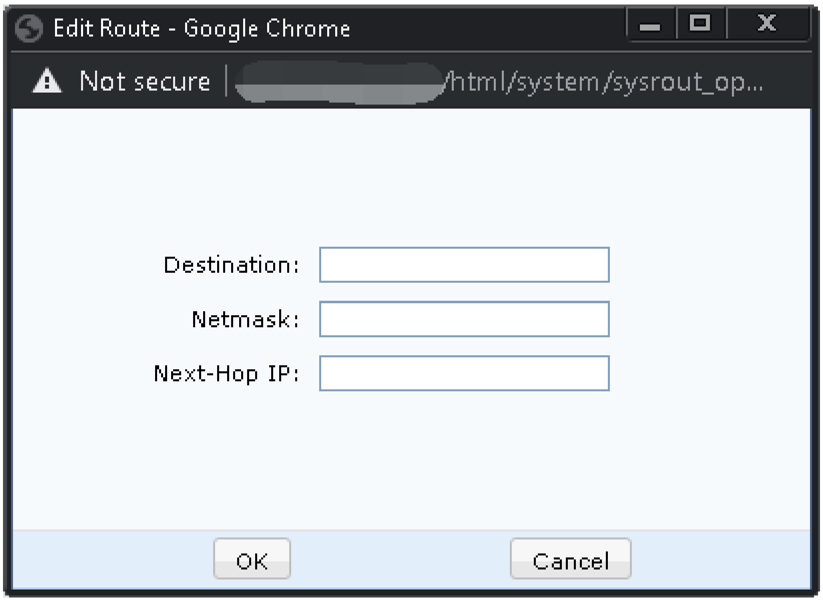
There're multiple network segments in the LAN of the enterprise. When the segments access the Internet via MIG gateway device, the static route need to be added so that MIG gateway device can backhaul the data package of different segments to layer-3 switch or routers correctly.

For example, the LAN of the company has two segments: 192.200.100.X and 192.200.200.X which are inter-connected through a layer-3 switch. The computer gateway of each segment is pointing to the gateway 192.200.X.254 of respective segment of the layer-3 switch. The IP of the LAN interface of the MIG device is 192.200.200.200, which is in the 192.200.200.X segment. WAN interface is configured to connect to the Internet. Now 192.200.100.X and 192.200.200.X segments are applied as public network export via MIG and share the internet.

Due to the fact that 192.200.100.X segment is not on the same segment as LAN interface (192.200.200.X) of MIG, MIG needs to be added with a system route to backhaul the data package of 192.200.100.X to 192.200.200.254 of the layer-3 switch of the LAN to export, and direct to the computer on the 192.200.100.X segment. The configuration is shown as follows:

A. Add multiple proxy segments: add 2 subnet segments to NAT configuration page of MIG, including 192.200.100.0/24 and 192.200.200.0/24 (for specific setting, see MIG User Manual**Error! Reference source not found.**2.9.2.1『Firewall Setting』→『NAT Setting』→『Proxy Access Setting』Section).

B. Add the static route: add a static route to the system route setting of MIG: 192.200.100.0/24-> 192.200.200.254 as shown below:


Edit Route - Google Chrome
Not secure | [redacted]/html/system/sysrout_op...
OK
Cancel

Destination:

Netmask:

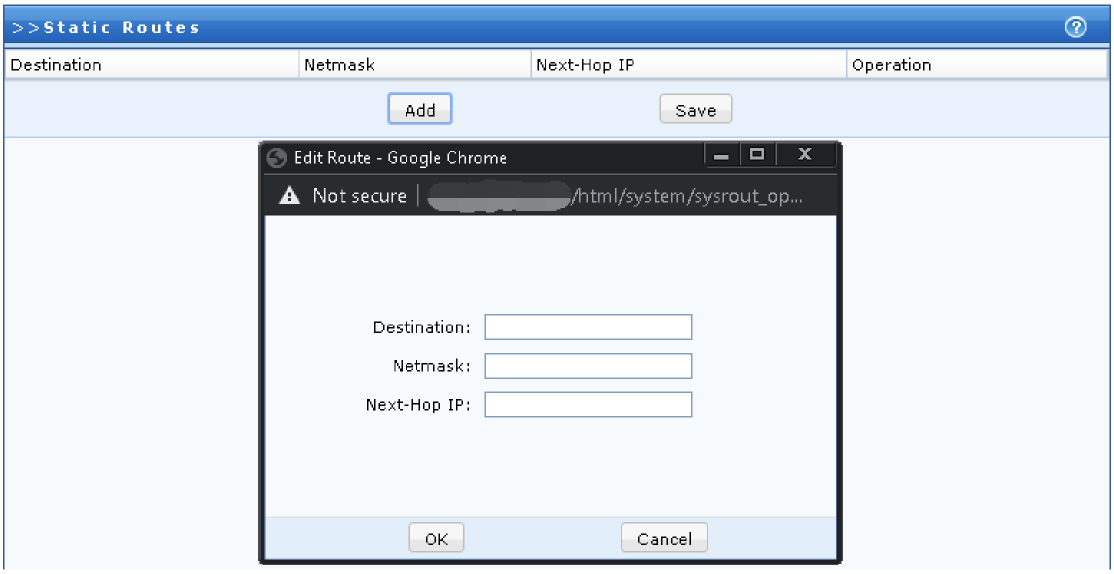
Next-Hop IP:

2. Set the route when access to VPN internal multi-subnets is required

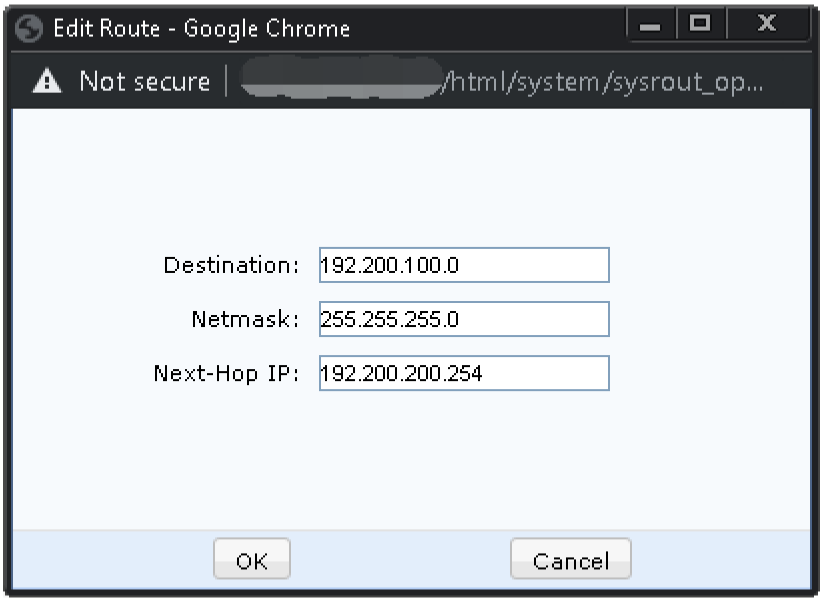
When the VPN network has multiple segment networks in the headquarters or the branch, we call it VPN multi-subnet. If the networks need to be added to the VPN network for inter-access of multiple segments in the branch or the headquarters of the VPN, the local subnet list and system route need to be added.

For example, the headquarters has two segments: 192.200.100.X and 192.200.200.X which are interconnected through a layer-3 switch. For the layer-3 switch, the IP address of the network interface connected with these two segments is respectively 192.200.100.254 and 192.200.200.254. The IP address of the LAN interface on the MIG device is 192.200.200.200, which is deployed in the 192.200.200.X segment.

First add a multi-subnet 192.200.100.X in the『Static Route』of MIG, as shown in the following page:



Then add a system route of 192.200.100.X in the『Static Route Setting』of MIG system route setting page, so as to direct the gateway to the network interface of the layer-3 switch 192.200.200.254 which is connected to 192.200.100.X as shown in the following figure:



Edit Route - Google Chrome

Not secure | [redacted]/html/system/sysrout_op...

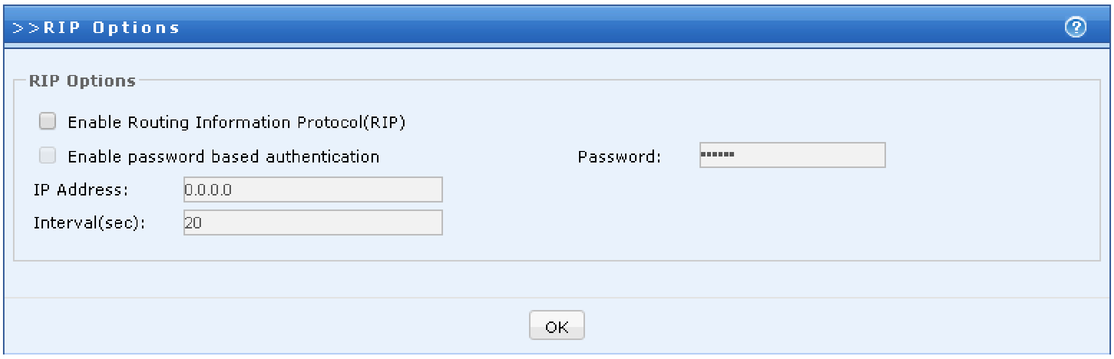
Destination: 192.200.100.0

Netmask: 255.255.255.0

Next-Hop IP: 192.200.200.254

2.3.4.2. RIP Settings

『RIP Settings』 allow users to set the MIG device to notify the route information to other route devices through RIP protocol to realize a dynamic update of the RIP route information of the route device of the LAN. The page is shown as follows:



>>RIP Options

RIP Options

□ Enable Routing Information Protocol(RIP)

□ Enable password based authentication

Password: ******

IP Address: 0.0.0.0

Interval(sec): 20

『Enable Route Selection Information Protocol』 : a switch for the update function of the whole dynamic route. After the function is enabled, MIG device will notify the information of P2P network with VPN access to the home terminal to the route device of the internal network (update the route list of other devices, and add to the route which is the opposite terminal of the VPN to point to MIG. Once the VPN is disconnected, the route device will be notified to delete the route).

『Enable Password based authentication』: set the password for verification when exchanging RIP information, and can set accordingly.

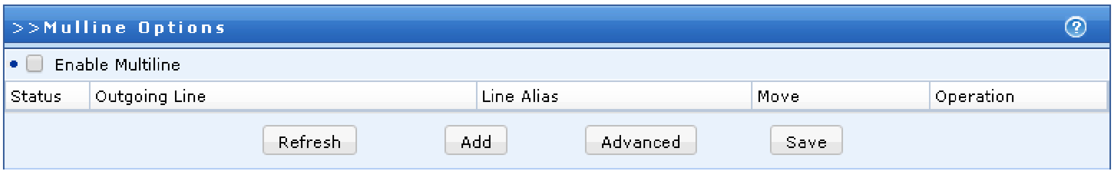
『IP Address』 and 『Port』: set to actively publish updated route information to a certain IP (route device IP).

[Update Cycle] If any change to the route information, MIG will trigger the process of route information update. At this time, the parameter of Update Cycle for RIP will be invalid.

In the end, click OK to save the configuration.

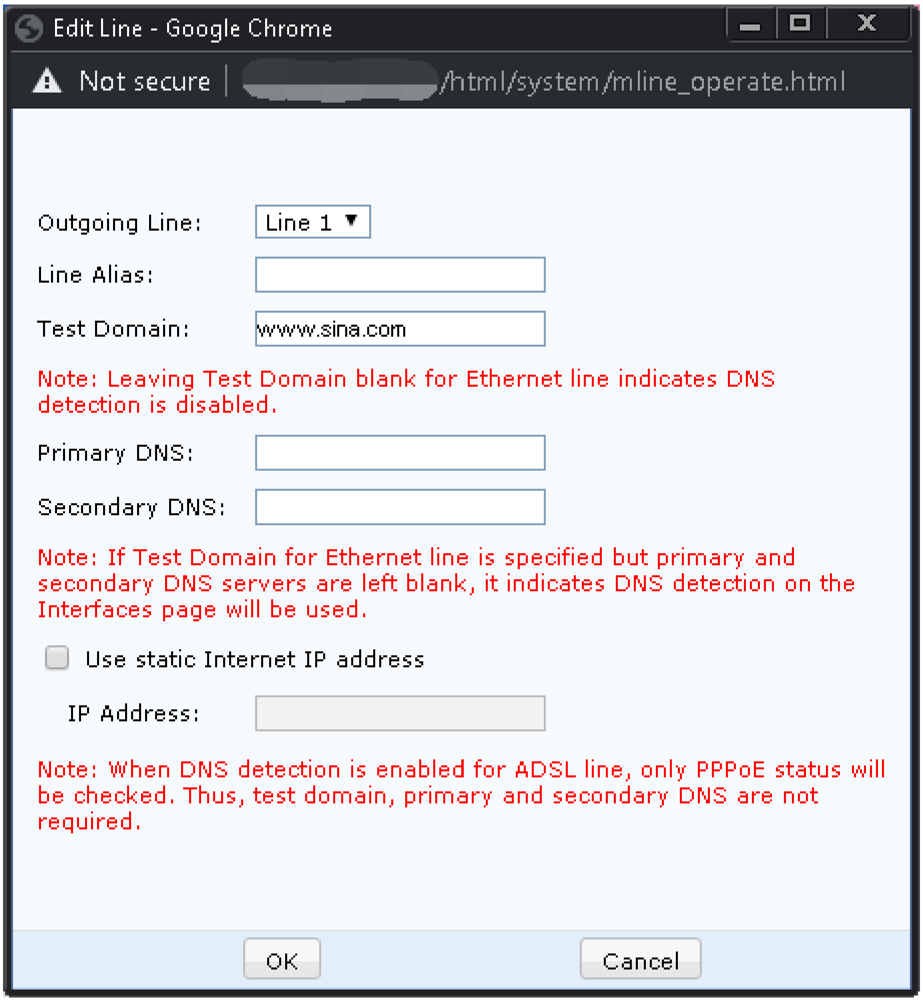
2.3.5. Multi-line Settings

When the device is available for multi-line authorization, 『Multi-line settings』 is required to detect the health status of the two lines. At the same time, to realize the auto selection function for MIG multi-line, the option must be set. As shown below:



[Refresh]: refresh the current line status

[Add]: for adding new lines. Here, both lines are to be added. Click "Add" button, the following interface will appear:



[redacted]/html/system/mline_operate.html

Outgoing Line: Line 1

Line Alias:

Test Domain: www.sina.com

Note: Leaving Test Domain blank for Ethernet line indicates DNS detection is disabled.

Primary DNS:

Secondary DNS:

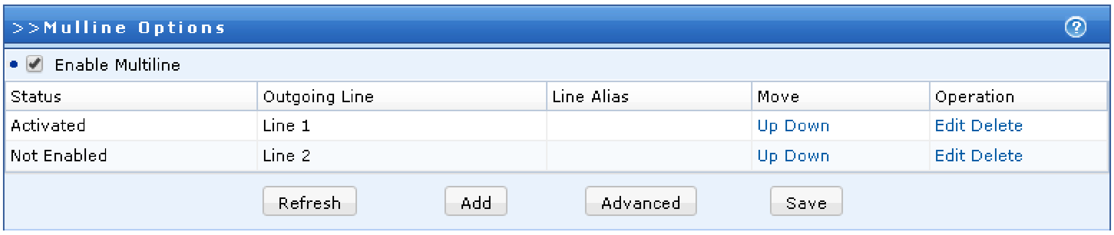
Note: If Test Domain for Ethernet line is specified but primary and secondary DNS servers are left blank, it indicates DNS detection on the Interfaces page will be used.

□ Use static Internet IP address

IP Address:

Note: When DNS detection is enabled for ADSL line, only PPPoE status will be checked. Thus, test domain, primary and secondary DNS are not required.

Line alias can be customized, such as “China Telecom" and "China Unicom". Usually, enter a domain name that can be analyzed normally through the line to the Test Domain. The device will analyze the domain regularly through the line. If the domain can be analyzed, the line is normal. DNS detection need to be enabled in [Advanced]. See the blue font part for other settings. The following interface will appear after setting the two lines:

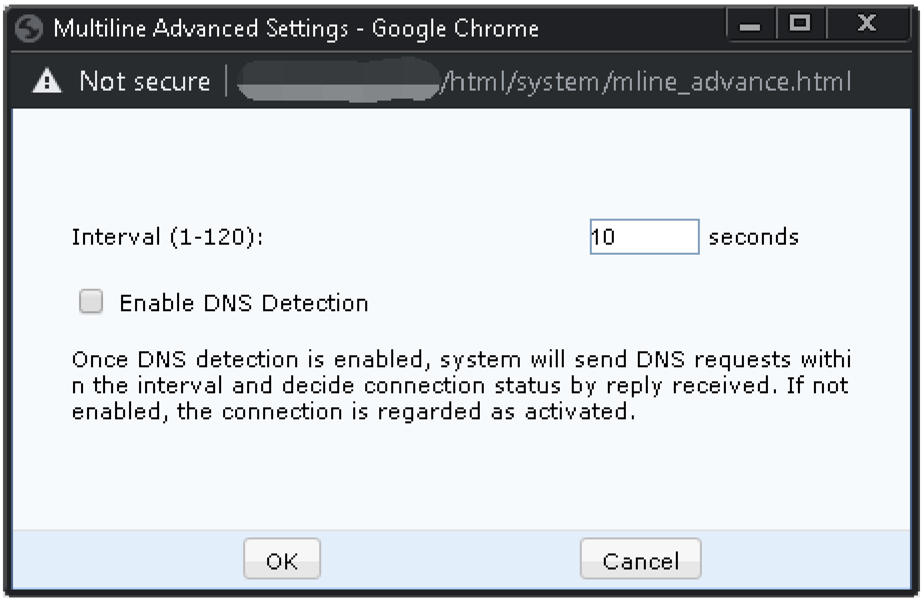


>>Mulline Options

☑ Enable Multiline

Status	Outgoing Line	Line Alias	Move	Operation
Activated	Line 1		Up Down	Edit Delete
Not Enabled	Line 2		Up Down	Edit Delete

[Advanced]: for setting Enable DNS Detection, set detection cycle for line status, and Disable or Enable DNS Detection. Click Advanced and the following interface will appear:



Multiline Advanced Settings - Google Chrome

Not secure | [redacted]/html/system/mline_advance.html

Interval (1-120): 10 seconds

□ Enable DNS Detection

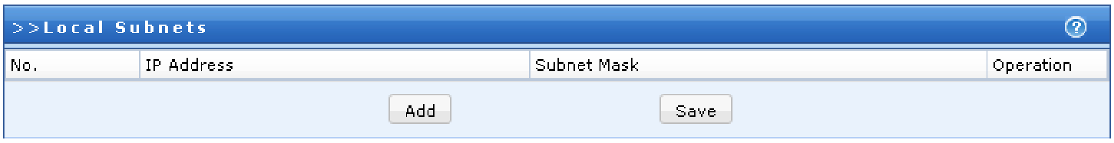
Once DNS detection is enabled, system will send DNS requests within the interval and decide connection status by reply received. If not enabled, the connection is regarded as activated.

Move
Up Down
Up Down

Under the dual-line scenario, through the adjustment to the line order, the default route pointing of the device and the default DNS order can be modified. For example, on the picture above, the default route of the device is pointed to China Telecom line. When the device and the proxy LAN analyze the domains, the DNS of China Telecom line will be used in priority. (When detecting, DNS specified when adding lines in the『Multi-line Setting』is used)

2.3.6. Local Subnet List

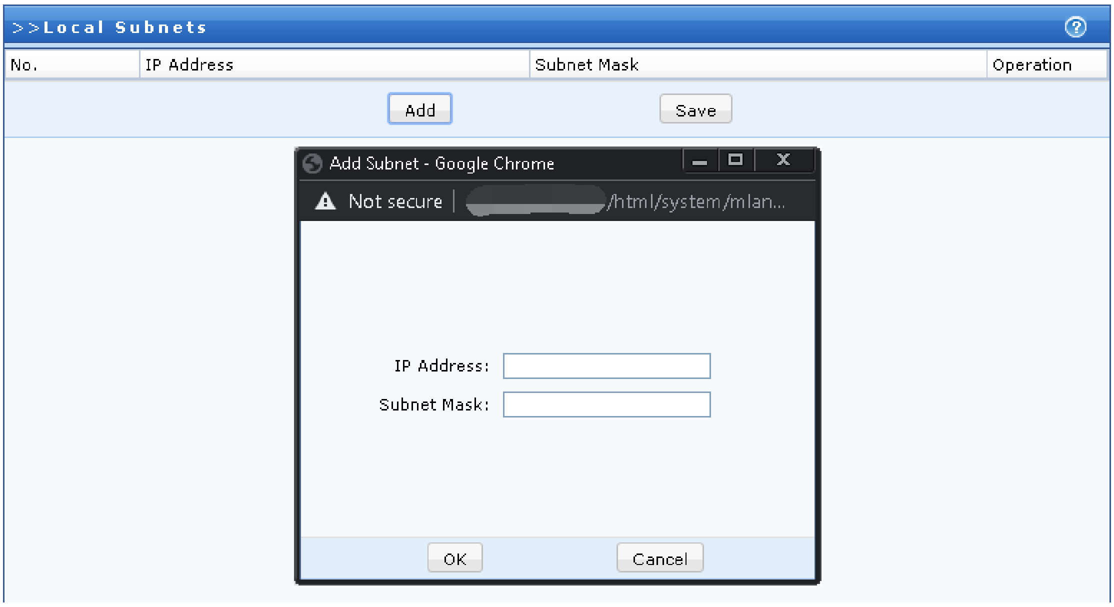
When the LAN connected with the device has a layer-3 switch or a router, and is segmented into multiple segments, information of all of the segments except the segment where the LAN interface of the device resides need to be added to the list.



>>Local Subnets

No.	IP Address	Subnet Mask	Operation

Click Add, fill in other segment addresses of local end to the local subnet list. The page is shown as follows:



>>Local Subnets

No.	IP Address	Subnet Mask	Operation

Add Subnet - Google Chrome

Not secure | [redacted]/html/system/mlan...

IP Address:

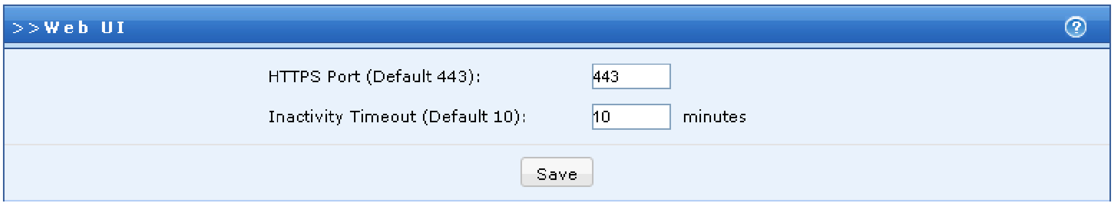
Subnet Mask:

⚠ **Note: For the segments where the LAN interface and DMZ interface of the device reside, you don't need to add them to the Local Subnet List. Only when the local LAN has multiple segments, it's necessary to add other segments to the local subnet list.**

2.3.7. Console Settings

2.3.7.1. WEBUI Settings

It's used to set the http service port of the gateway console (default port 443) and the timeout for user to log in to the device console. If the service port is modified, it's required to log in to the gateway console via the port modified. See the page below for details.



>>Web UI

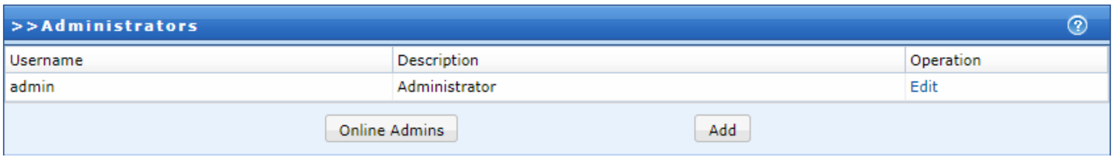
HTTPS Port (Default 443): 443

Inactivity Timeout (Default 10): 10 minutes

2.3.7.2. Administrator Settings

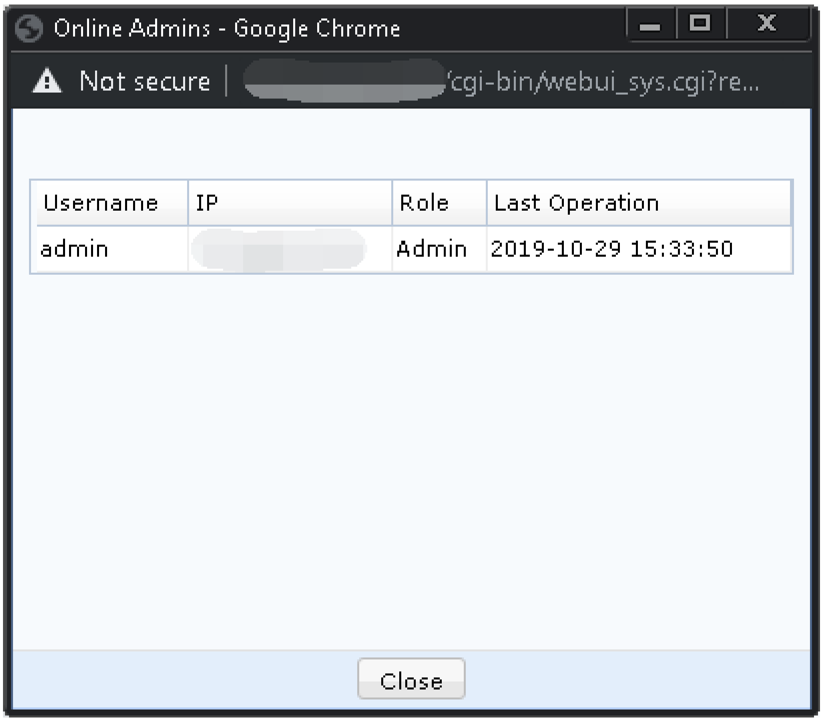
『Administrator Settings』 is used to set the administration account to log in to the gateway console.

Click Online Admins, you can see the administrator access to this hardware device as shown in the figure below:



>>Administrators

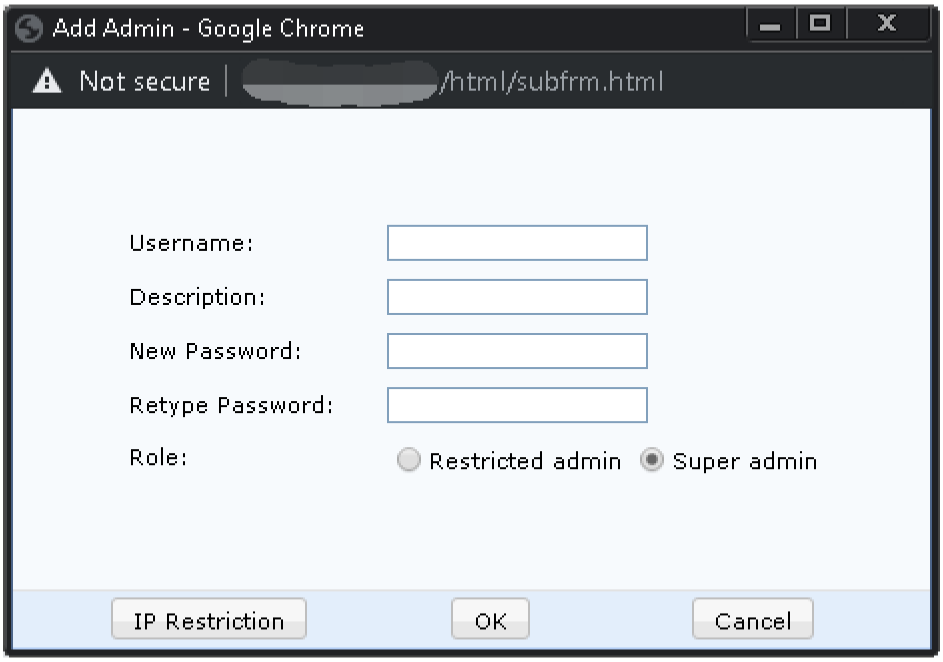
Username	Description	Operation
admin	Administrator	Edit



[redacted]/cgi-bin/webui_sys.cgi?re...

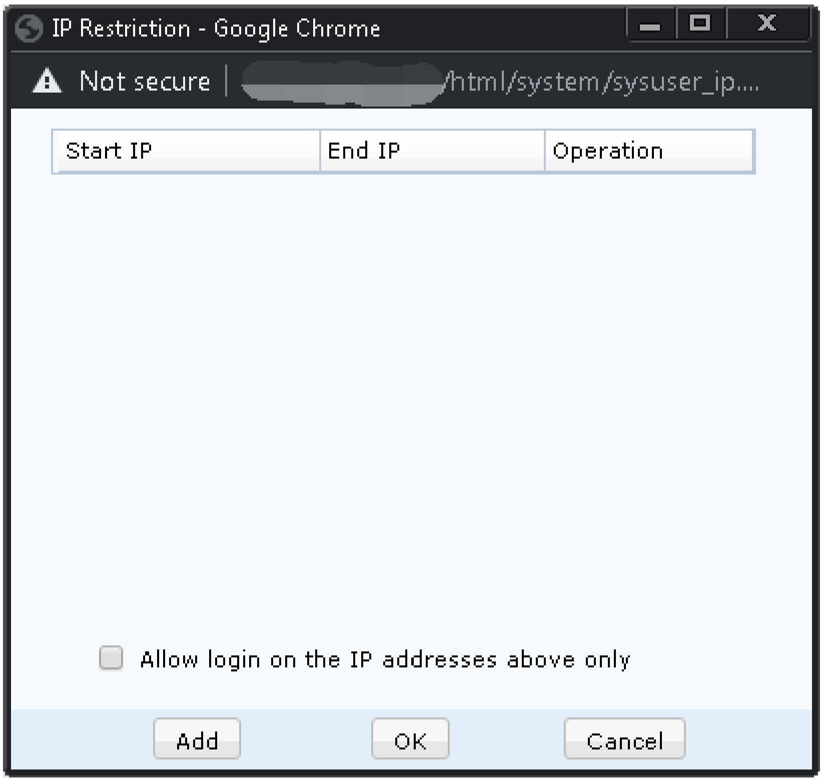
Username	IP	Role	Last Operation
admin	[redacted]	Admin	2019-10-29 15:33:50

Click Add to pop up a dialog box for adding users, then set『Username』, 『Password』,『Role』 and 『IP Restrictions』. The page is shown as follows:



[redacted]/html/subfrm.html

Username:	
Description:	
New Password:	
Retype Password:	
Role:	○ Restricted admin ● Super admin



IP Restriction - Google Chrome

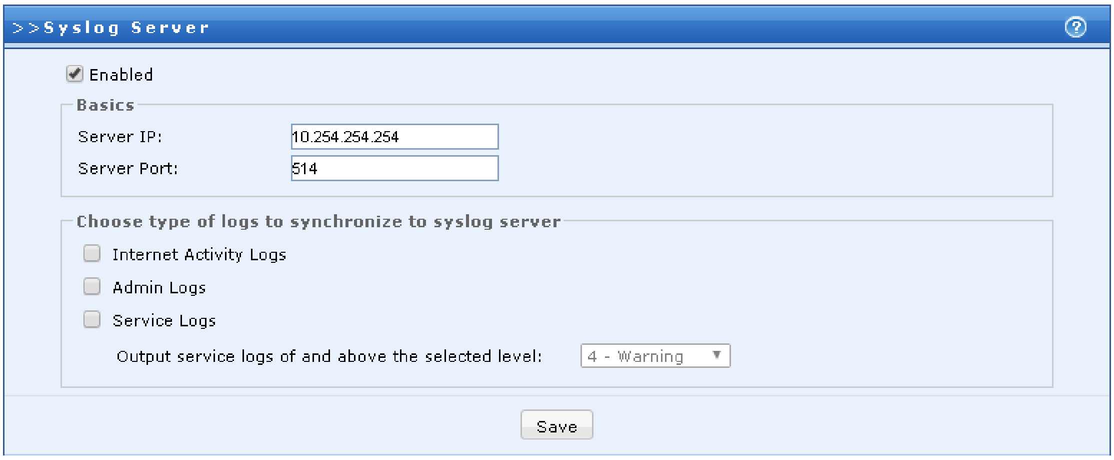
Not secure | [redacted]/html/system/sysuser_ip....

Start IP	End IP	Operation

□ Allow login on the IP addresses above only

2.3.8. SYSLOG Settings

『SYSLOG Settings』 is used to set the IP address and port No. of the syslog server, and helps send the Internet access behavior logs, administrator logs and system logs generated at the MIG device to other third-party syslog servers. The page is shown as follows:



>>Syslog Server

☑ Enabled

Basics

Server IP: 10.254.254.254

Server Port: 514

Choose type of logs to synchronize to syslog server

□ Internet Activity Logs

□ Admin Logs

□ Service Logs

Output service logs of and above the selected level: 4 - Warning

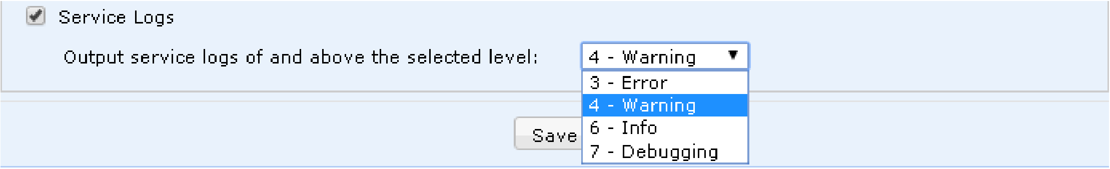
『Enable SYSLOG Server』: Enable the functions to access the syslog server.

『Server IP』: IP address of syslog server.

『Server Port』: Sync ports enabled by the syslog server.

『Output the Following Logs to SYSLOG Server』: Select online behavior logs, management logs and service logs.

『Service Log』 The service logs for devices. Users can select the level of output logs as shown in the figure below:

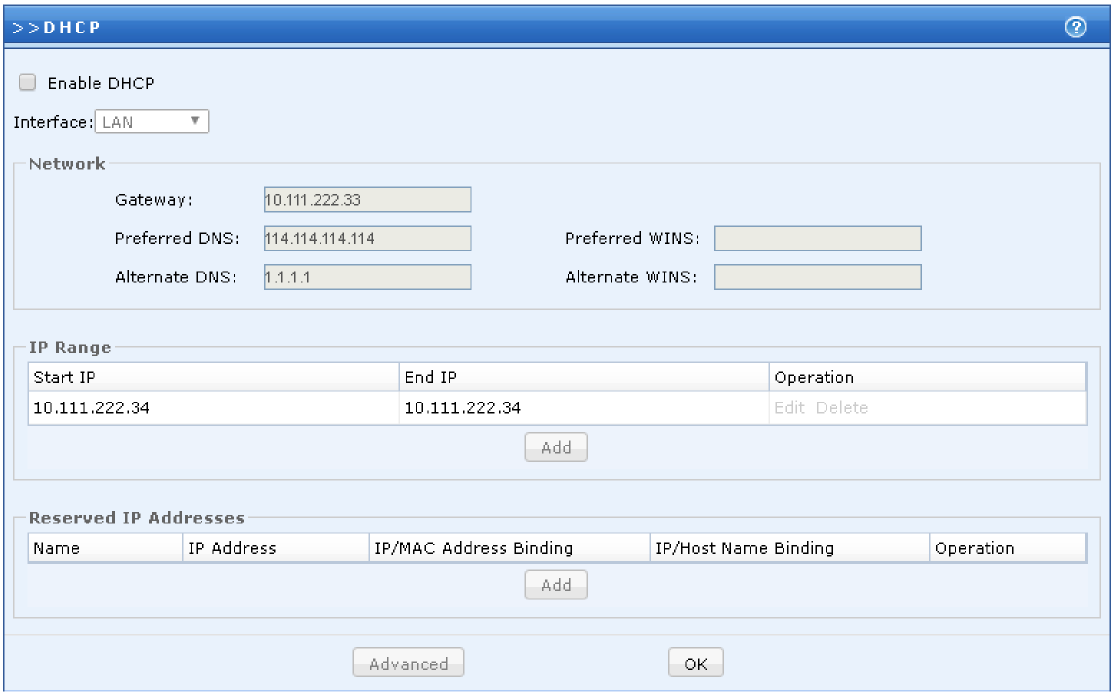


☑ Service Logs

Output service logs of and above the selected level: 4 - Warning

2.3.9. DHCP Settings

It is mainly used to set some parameters for DHCP services. The page is shown as follows:



>>DHCP

□ Enable DHCP

Interface: LAN

Network

Gateway: 10.111.222.33

Preferred DNS: 114.114.114.114 Preferred WINS:

Alternate DNS: 1.1.1.1 Alternate WINS:

IP Range

Start IP	End IP	Operation
10.111.222.34	10.111.222.34	Edit Delete

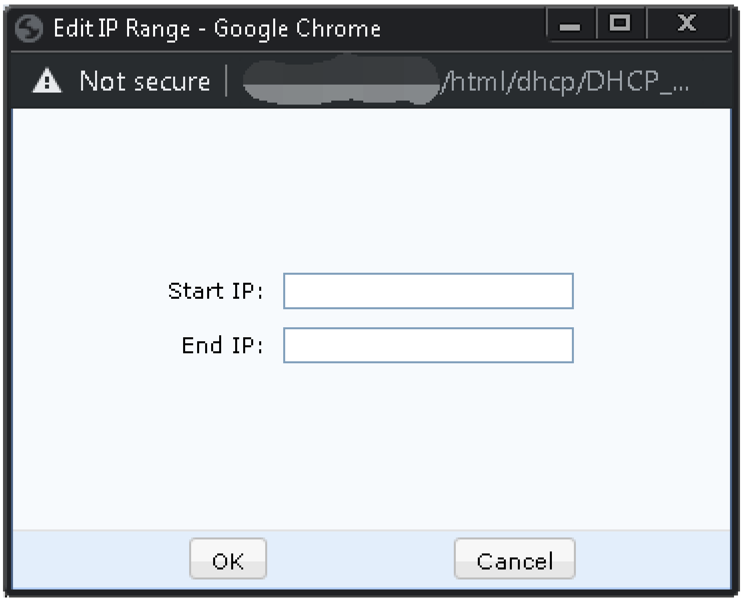
Reserved IP Addresses

Name	IP Address	IP/MAC Address Binding	IP/Host Name Binding	Operation

[Assigned Network Interface] can be LAN/WLAN interface or DMZ/WLAN interface.

At [DHCP Network Configuration], set appropriate gateway IP and valid DNS server IP. Generally, at [Gateway], fill in “LAN IP” or “DMZ Port IP” for VPN1110/1110-W/1200 devices; At [DNS], fill in DNS server IP offered by local ISP. [WINS] may be filled in or not according to the specific application.

Click Add under [DHCP IP Address Range] to pop up a dialog box below:

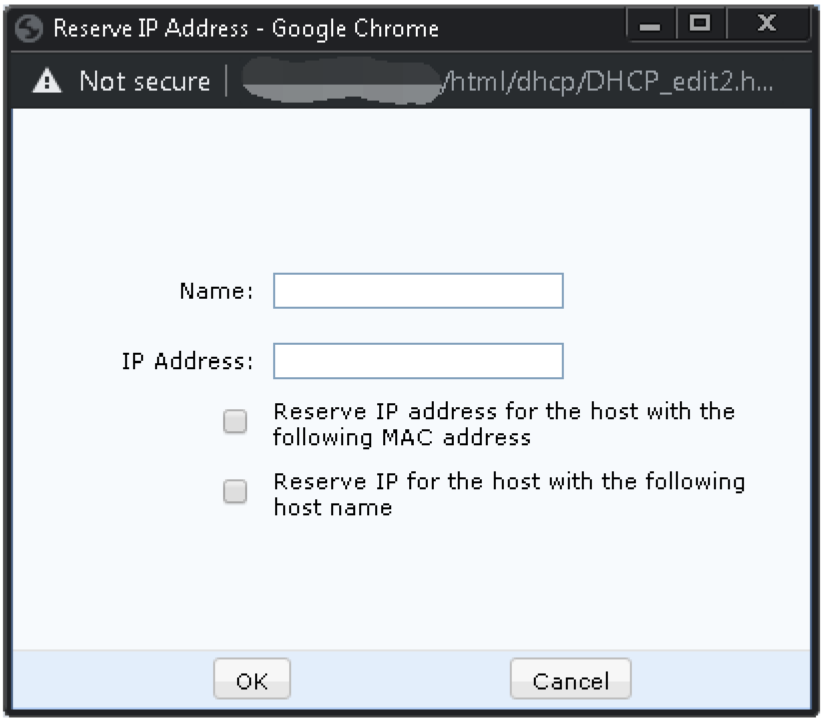

Edit IP Range - Google Chrome
Not secure | [redacted] /html/dhcp/DHCP_...
Start IP:
End IP:
OK
Cancel

Here the IP address range is assigned by DHCP. Fill in the start IP and end IP to determine the range.

Note: 1. Some computers access to the LAN are offered with a fixed private IP. Here the IP address range shall not include the used IP to avoid IP conflicts with randomly assigned IP.

2. In general, the IP addresses ending in 0 and 255 shall not be added, as the two are network address and broadcast address IN this segment.

[DHCP Reserve IP Settings] is used to set the IP retained to some computers. Click Add below, the dialog box [Edit DHCP Retained IP] would pop up as follows:



Reserve IP Address - Google Chrome

Not secure | [redacted]/html/dhcp/DHCP_edit2.h...

Name:

IP Address:

□ Reserve IP address for the host with the following MAC address

□ Reserve IP for the host with the following host name

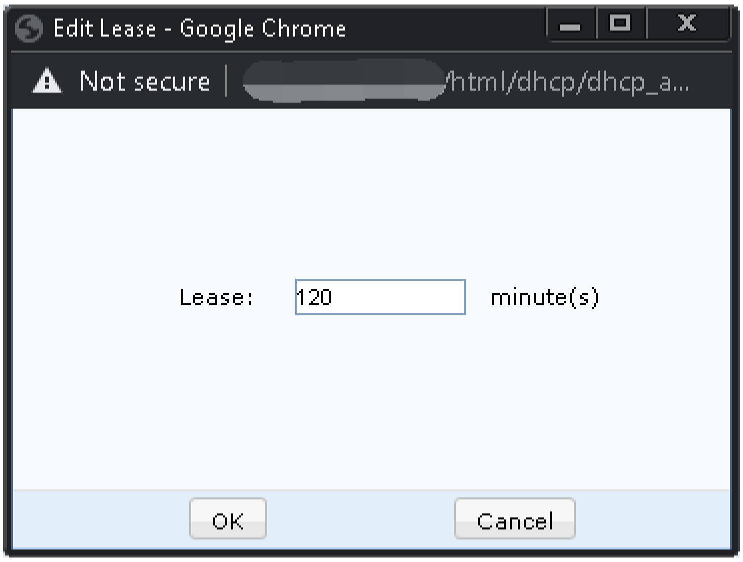
[Name] is defined by the user. You can fill in any name easy to remember and understand.

[IP] address shall be the specific LAN IP retained to this user.

The conditions retained by DHCP can be bound according to "MAC Address" or "Machine Name" of user's computer.

Check the appropriate options, and then fill in the corresponding "MAC Address" and "Machine Name". You can also click Acquire by IP to acquire corresponding parameters, then click OK to save.

[Advanced] is used to set the lease time of DHCP. The time can be modified to (1-7,200 minutes) and its default is 120 minutes. As shown below:

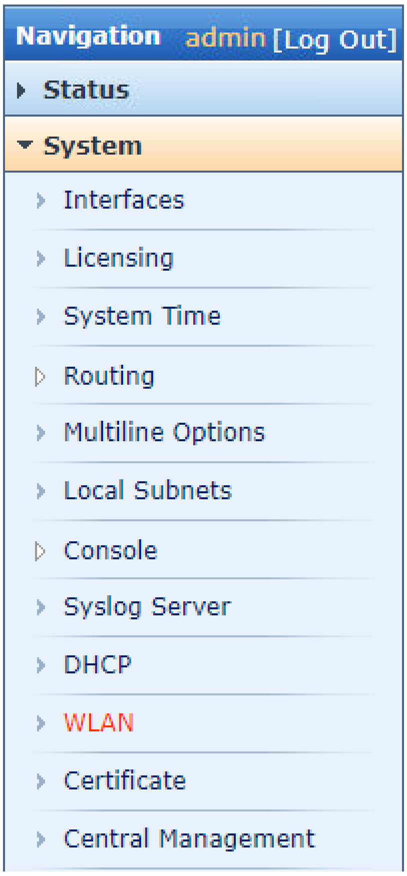


Lease: 120 minute(s)

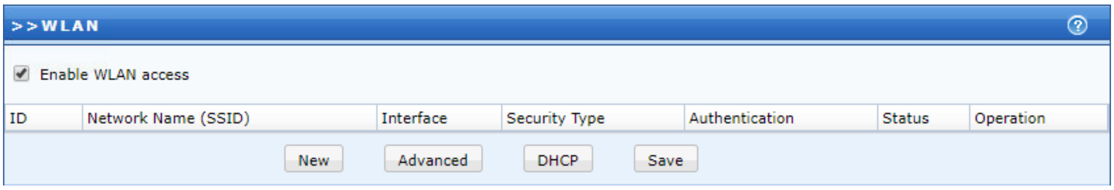
Finally, check [Enable DHCP Service], and then activate the DHCP functions.

2.3.10. WLAN Settings (MIG-1110-W)

MIG-1110-W device can also support the local area network users to access via wireless WIFI. You can see WIFI-related config options on the configuration interface of MIG-1110-W device as shown below:



『WLAN Settings』 configuration interface is as follows:

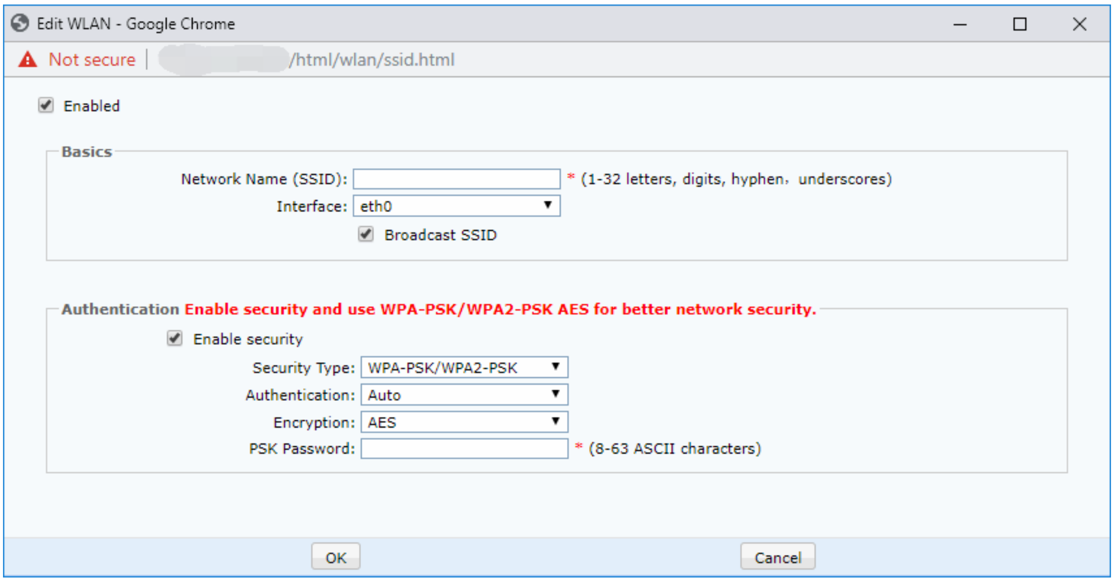


☑ Enable WLAN access

ID	Network Name (SSID)	Interface	Security Type	Authentication	Status	Operation

Check [Enable WLAN] to enable WIFI functions on the device.

WLAN Settings supports dual SSID. Allow dual SSID and SSID enabled and disabled, binding network ports, SSID broadcast, security certification and other independent configuration. The page is shown as follows:


Edit WLAN - Google Chrome
Not secure | [redacted]/html/wlan/ssid.html
OK
Cancel

☑ Enabled

Basics

Network Name (SSID): ______ * (1-32 letters, digits, hyphen，underscores)

Interface: eth0

☑ Broadcast SSID

Authentication Enable security and use WPA-PSK/WPA2-PSK AES for better network security.

☑ Enable security

Security Type: WPA-PSK/WPA2-PSK

Authentication: Auto

Encryption: AES

PSK Password: ______ * (8-63 ASCII characters)

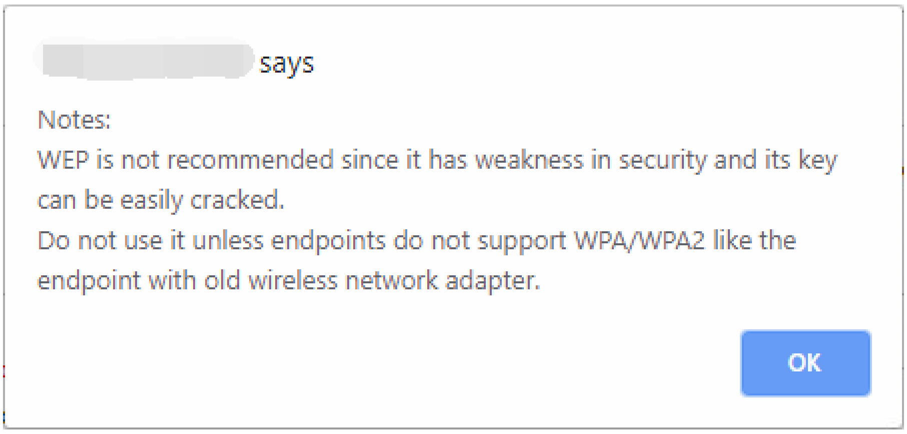
『SSID』 is used to set the name of WIFI, and WIFI wireless client will display the SSID name accordingly.

『Bind Network Interface』 can select eth0 or eth1 interface.

[Enable SSID Broadcast] is used to set whether to broadcast SSID. If yes, all wireless devices within the range of the wireless signal device can find this WIFI network. This option is enabled by default, but if you need high security, do not check this function.

By checking [Enable Security Settings], users can encrypt the WIFI network to avoid unauthorized wireless users to access the WIFI network.

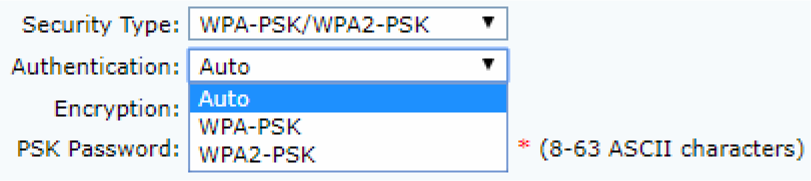
『Security Type』 is used to select the encryption protocol for WIFI network, including WPA-PSK/WPA2-PSK and WEP. The default is WPA-PSK/WPA2-PSK. As WEP encryption protocol is vulnerable to be cracked, the WEP is not recommended to use unless the wireless devices do not support WPA-PSK/WPA2-PSK. When switching to WEP mode, the device will give a prompt as shown below:



[redacted] says

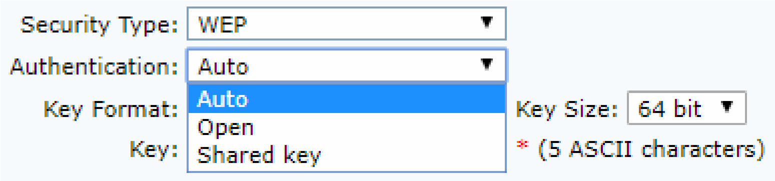
Notes:
WEP is not recommended since it has weakness in security and its key can be easily cracked.
Do not use it unless endpoints do not support WPA/WPA2 like the endpoint with old wireless network adapter.

『Security Options』 are used to select the specific encryption protocol. If WPA-PSK/WPA2-PSK is selected, the『Security Options』include auto select, WPA-PSK and WPA2-PSK as shown below:



Security Type: WPA-PSK/WPA2-PSK
Authentication: Auto
Encryption:
PSK Password: * (8-63 ASCII characters)

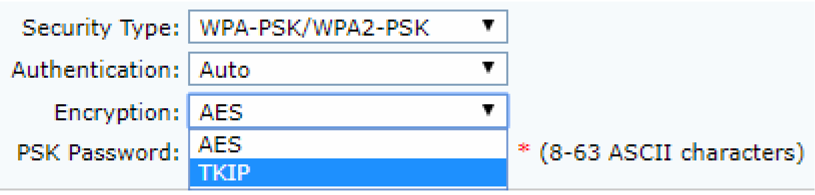
If the WEP mode is selected in 『Security Type』, the 『Security Options』 include auto select, open system and shared key as shown below:



Security Type: WEP
Authentication: Auto
Key Format:
Key Size: 64 bit
Key: * (5 ASCII characters)

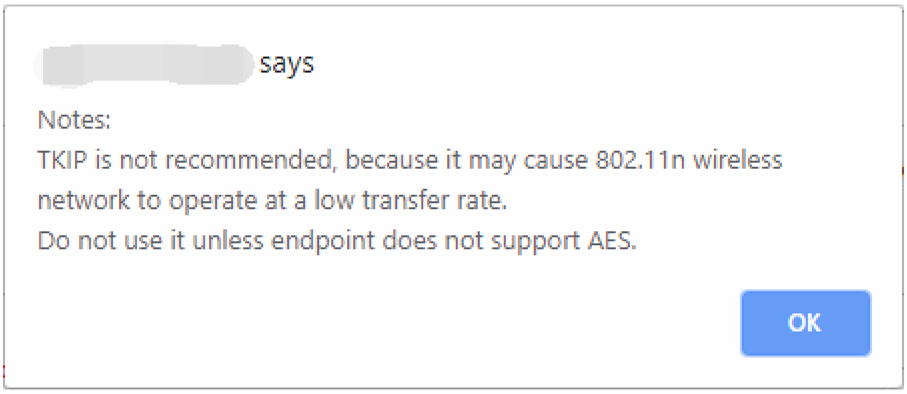
Open System means no authentication needed, so any wireless clients can access the WIFI network. For shared key, the wireless clients are required to enter the shared key consistent with the device to access the WIFI network.

『Encryption』 are used to select corresponding encryption algorithms, including AES and TKIP as below:



Security Type: WPA-PSK/WPA2-PSK ▼
Authentication: Auto ▼
Encryption: AES ▼
AES
TKIP
PSK Password: * (8-63 ASCII characters)

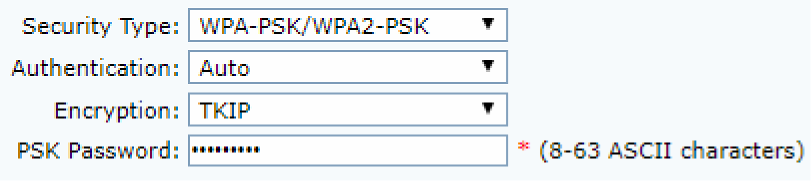
The default is AES algorithm. TKIP encryption algorithm would get WIFI 802.11n working under lower transmission rate. Therefore, it's recommended to adopt the default AES algorithm, unless the wireless terminal does not support AES algorithm. In case that the algorithm is switched to TKIP algorithm, the device will give corresponding tips as shown below:



[redacted] says

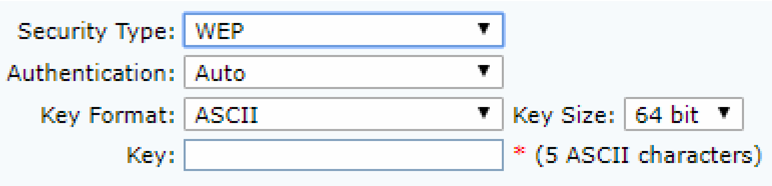
Notes:
TKIP is not recommended, because it may cause 802.11n wireless network to operate at a low transfer rate.
Do not use it unless endpoint does not support AES.

『PSK Password』 is used to set the WIFI network password with 8-63 ASCII characters. Users need to enter correct password for wireless terminals to access WIFI network as shown below:



Security Type: WPA-PSK/WPA2-PSK ▼
Authentication: Auto ▼
Encryption: TKIP ▼
PSK Password: ••••••••• * (8-63 ASCII characters)

If the WEP mode is selected in Security Type, no options for encryption algorithm or PSK password settings exist. There are options for key format, key length and key as shown below:



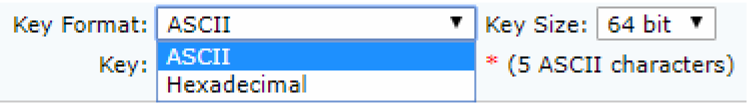
Security Type: WEP

Authentication: Auto

Key Format: ASCII Key Size: 64 bit

Key: * (5 ASCII characters)

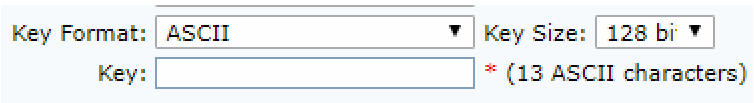
『Key Format』 is used to set the key format for WEP encryption, including ASCII Code and hexadecimal system. The key has a length of 64 bits and 128 bits as shown below:



Key Format: ASCII Key Size: 64 bit

Key: * (5 ASCII characters)

『Key』 is used to set the key for WEP. Under ASCII Code, the Key has 5-13 characters or has 10-26 hexadecimal characters under the hexadecimal system as shown below:



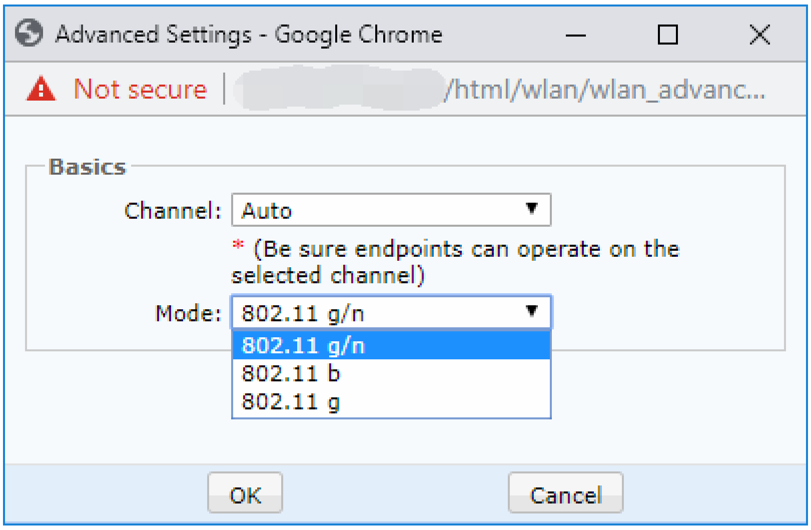
Key Format: ASCII Key Size: 128 bi

Key: * (13 ASCII characters)

Click OK to save the WIFI settings.

The 『Channel』 in the Advanced Settings is used to set the WIFI wireless channel. It supports Channel 1 to Channel 13, or the device can auto select the channel. It's recommended to auto select the channels to avoid the decrease of transmission rate due to wireless channel conflicts.

『Mode』 in the Advance Settings is used to set the working mode supported by WIFI and the default is 802.11 b/g/n mixed mode. As follows:



Advanced Settings - Google Chrome

Not secure | [redacted]/html/wlan/wlan_advanc...

Basics

Channel: Auto

* (Be sure endpoints can operate on the selected channel)

Mode: 802.11 g/n

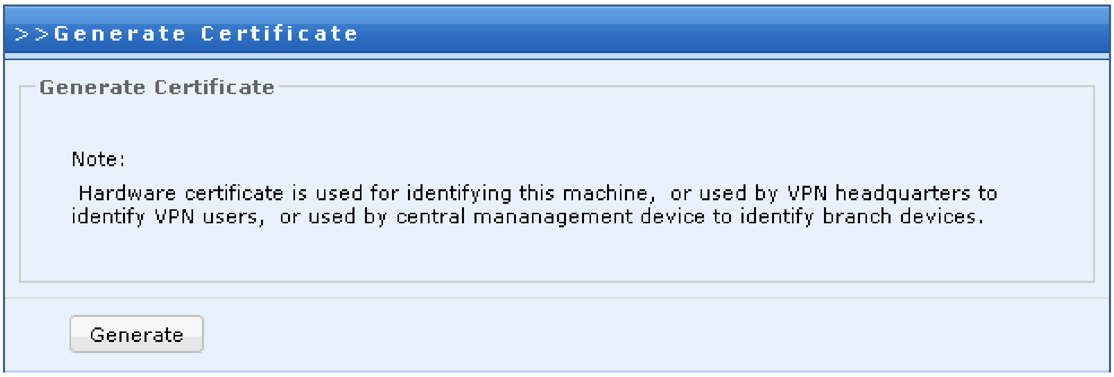
Click DHCP Settings to jump to the DHCP settings page, and you can also configure a DHCP address pool for WIFI users. See Section 2.3.9 for the configuration methods.

Click OK to save the WLAN (WIFI) settings.

2.3.11. Generate Certificates

The certificate authentication system based on hardware characteristics is one of the patented invention by SANGFOR. MIG device also adopts this technology for identify authentication between different VPN nodes. This certificate has extracted some hardware characteristics of the MIG device to generate an encrypted authentication certificate. Due to unique hardware characteristics, this certificate is unique and unforgeable. By verifying the hardware features, it guarantees that only the specified hardware device is authorized to access the network, avoiding security risks.

Click Generate Certificates and select the save path to generate a hardware certificate and save it on your local computer. The page is shown as follows:



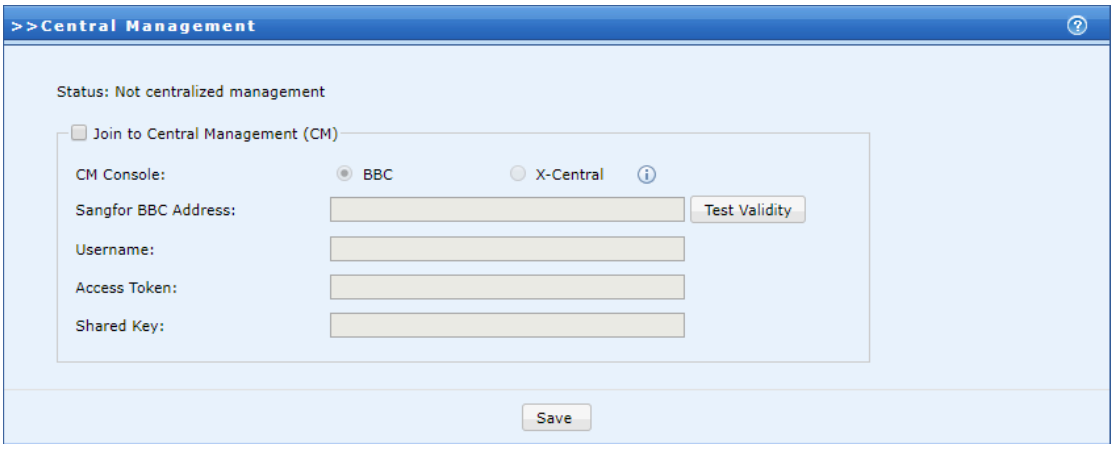
Note:

Hardware certificate is used for identifying this machine, or used by VPN headquarters to identify VPN users, or used by central mananagement device to identify branch devices.

The generated certificate is sent to the headquarters administrator, who selects hardware authentication when creating a VPN user account and binds the user with the corresponding hardware certificate.

2.3.12. Settings for Joining to Central Management

『Settings for Joining to Central Management』can be configured to access BBC so that the branch services can be controlled by the BBC center. After access to BBC, 『Basic Settings』, 『User Management』 and『Connection Management』at『VPN Information Settings』cannot be configured at MIG end, as these modules are controlled by the BBC. The page is shown as follows:


>>Central Management

Status: Not centralized management

□ Join to Central Management (CM)

CM Console: ● BBC ○ X-Central

Sangfor BBC Address: Test Validity

Username:

Access Token:

Shared Key:

Save

The configuration interface is shown as follows:

『Central Management Address』: Fill in BBC's IP and port.

『Username』: Fill in the username _MIG configured on BBC

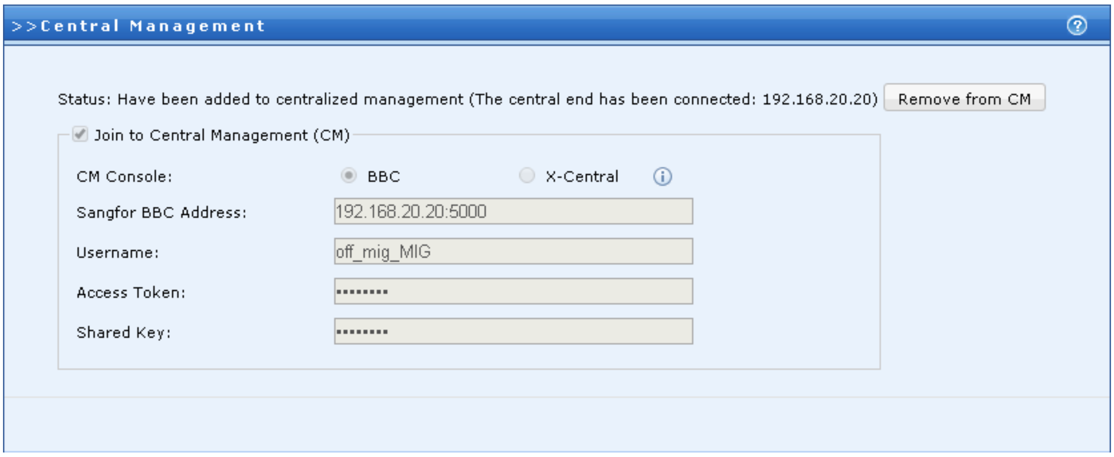
『Access Token』: Fill in the access password configured on BBC

『Shared Key』: Fill in the shared key configured on BBC. If the BBC is not configured with the shared key, no configuration of 『Test Validity』 at MIG end is required: Click to test whether the format of access address to BBC center is correct or not.

Click OK to save the configuration.

Note: After joining BBC central management, some configurations on the device would be issued uniformly from BBC center. The device will not be able to configure these functions. Joining BBC will reboot all MIG services. Please operate during an idle period to avoid adverse impacts.

The interface after joining BBC is shown as follows:



Status: Have been added to centralized management (The central end has been connected: 192.168.20.20) Remove from CM

☑ Join to Central Management (CM)

CM Console: ● BBC ○ X-Central

Sangfor BBC Address: 192.168.20.20:5000

Username: off_mig_MIG

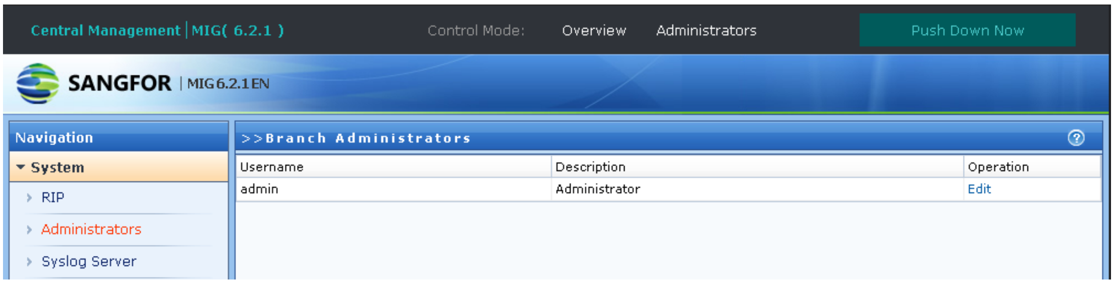
Access Token: ••••••••

Shared Key: ••••••••

『Disable Central Management』: Click to exit management with a password configured at the headquarters BBC.

2.3.12.1. BBC Config Delivery

After MIG branches access the BBC, the policy templates can be configured uniformly at the BBC center and delivered to MIG controlled end in batches. BBC can deliver 『System Setup』-『Console Settings』-『Administrator Settings』 and 『Firewall Settings』-『Filtering Rules Settings』 - 『Local Rules』. The interface for BBC to deliver configurations to MIG is shown as below:



Username	Description	Operation
admin	Administrator	Edit

2.3.12.2. BBC Views the Device Status and Status Alarming

After MIG accesses BBC, the device status and status alarming can be viewed at BBC center. It supports:

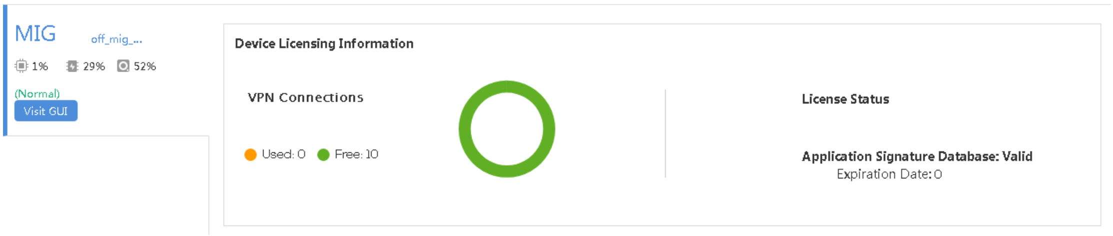
1. CPU, memory, disk to set alarming threshold. Once exceeding the threshold, an alarm is generated.

2. Alarming in case of offline VPN and inefficient VPN authorization.

3. Alarming in the case of offline MIG.

2.3.12.3. Report System Status to BBC

After MIG joins BBC, the MIG controlled end can be viewed for its CPU, memory and disk usage at the BBC branch details. In addition, users can view the flow rate in last hour as shown below:



MIG off_mig_...

1% 29% 52%

(Normal)

Device Licensing Information

VPN Connections

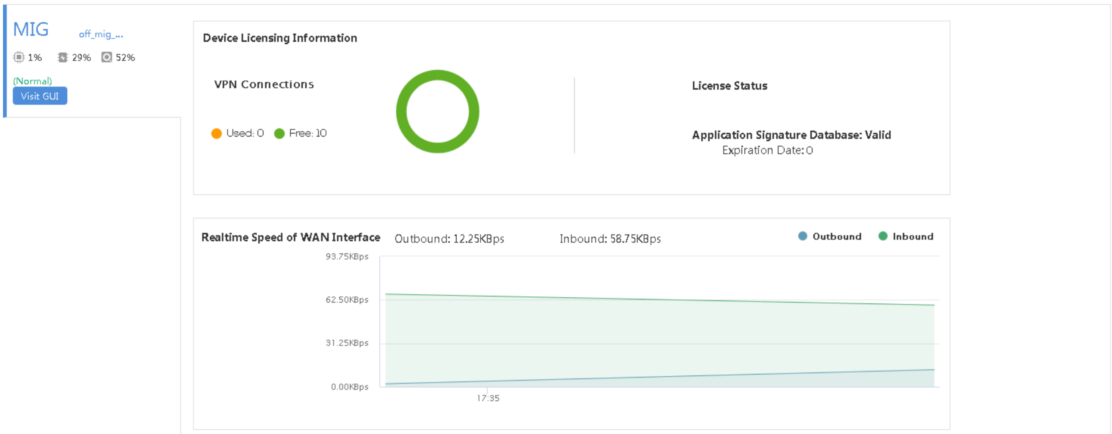
● Used: 0 ● Free: 10

License Status

Application Signature Database: Valid
Expiration Date: 0

2.3.12.4. Single Sign-on of BBC to MIG

Single sign on to MIG devices via『Branch Details』without password or network device name at the branch overview. Select MIG branch on『Branch』page of BBC, and click『Remote Access』 in 『Details』 to achieve the single sign-on to the device. As shown in the figure.

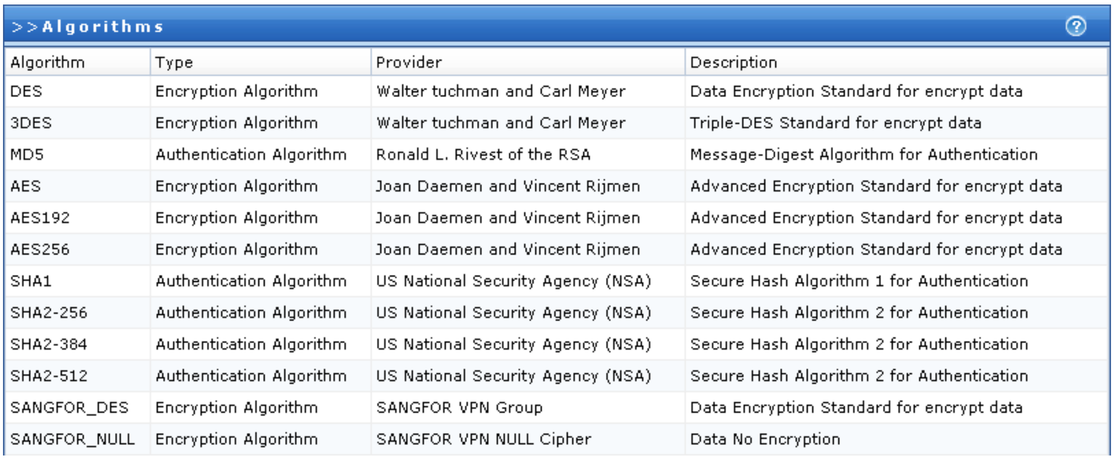


2.4. Object Settings

2.4.1. View Algorithm

It's used to view the encryption and authentication algorithms for VPN connection.

The page is shown as follows:

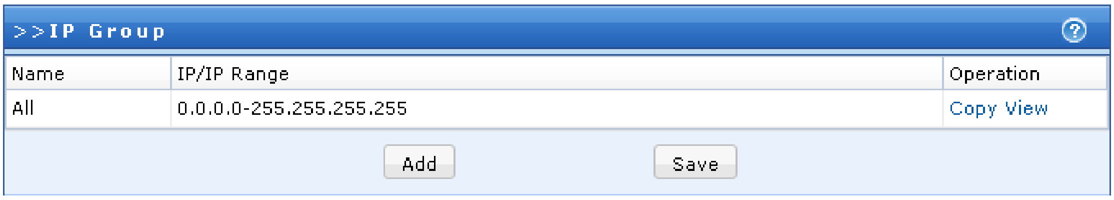


>>Algorithms

Algorithm	Type	Provider	Description
DES	Encryption Algorithm	Walter tuchman and Carl Meyer	Data Encryption Standard for encrypt data
3DES	Encryption Algorithm	Walter tuchman and Carl Meyer	Triple-DES Standard for encrypt data
MD5	Authentication Algorithm	Ronald L. Rivest of the RSA	Message-Digest Algorithm for Authentication
AES	Encryption Algorithm	Joan Daemen and Vincent Rijmen	Advanced Encryption Standard for encrypt data
AES192	Encryption Algorithm	Joan Daemen and Vincent Rijmen	Advanced Encryption Standard for encrypt data
AES256	Encryption Algorithm	Joan Daemen and Vincent Rijmen	Advanced Encryption Standard for encrypt data
SHA1	Authentication Algorithm	US National Security Agency (NSA)	Secure Hash Algorithm 1 for Authentication
SHA2-256	Authentication Algorithm	US National Security Agency (NSA)	Secure Hash Algorithm 2 for Authentication
SHA2-384	Authentication Algorithm	US National Security Agency (NSA)	Secure Hash Algorithm 2 for Authentication
SHA2-512	Authentication Algorithm	US National Security Agency (NSA)	Secure Hash Algorithm 2 for Authentication
SANGFOR_DES	Encryption Algorithm	SANGFOR VPN Group	Data Encryption Standard for encrypt data
SANGFOR_NULL	Encryption Algorithm	SANGFOR VPN NULL Cipher	Data No Encryption

2.4.2. IP Group Settings

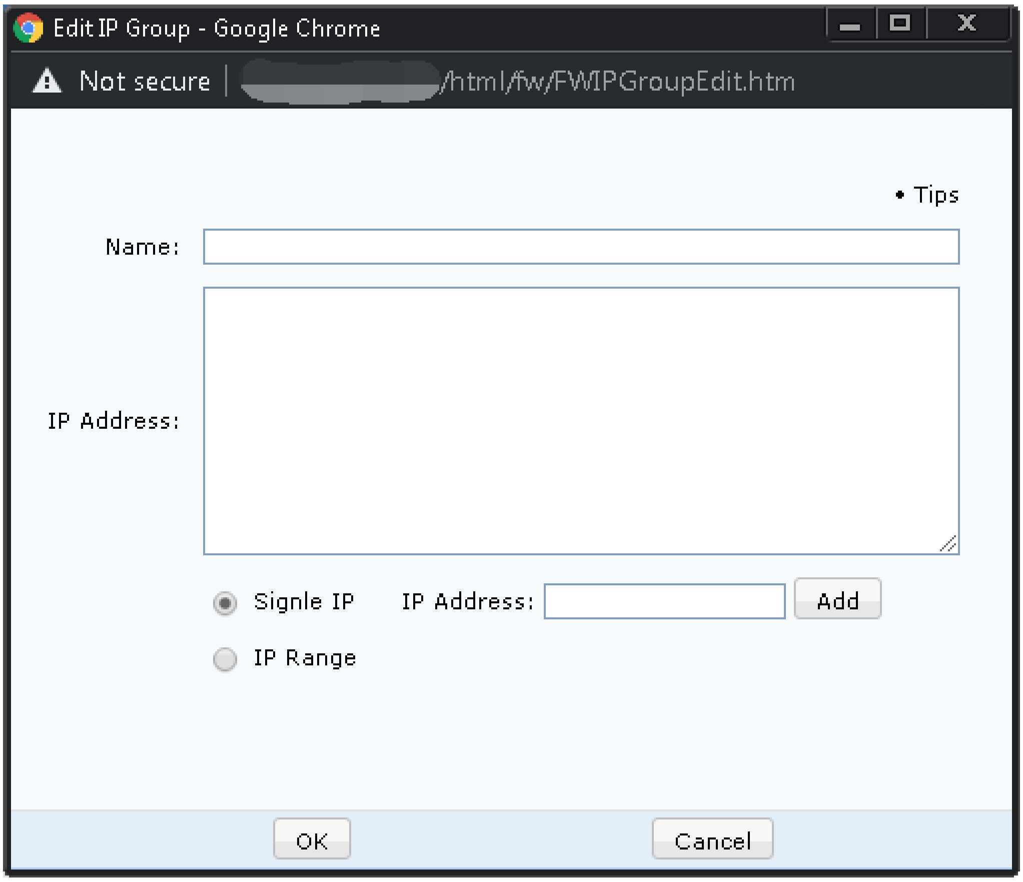
If the LAN has different IP segments or the vlan has different access rights, IP groups can be defined according to IP address as shown below:



>>IP Group

Name	IP/IP Range	Operation
All	0.0.0.0-255.255.255.255	Copy View

For example, the client LAN has two address segments - 192.168.1.0/24 and 192.168.1.0/24, here the IP group can be defined. You can define a single IP or a segment of IP. Click "Add" to pop up 【IP Group Edit】page:



Edit IP Group - Google Chrome

Not secure | [redacted]/html/fw/FWIPGroupEdit.htm

• Tips

Name:

IP Address:

● Signle IP IP Address:

○ IP Range

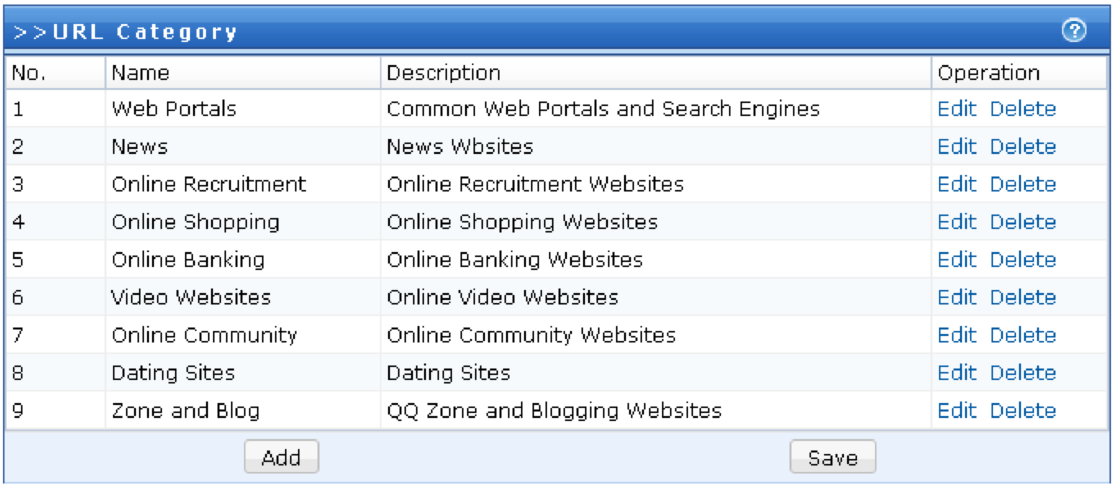
『IP Group Name』: Name the IP or IP segment to be defined at will.

『IP Address』: You can select a single IP or the IP range, and fill in them. Click Add to add to the IP group definition box; Click OK to add to the IP group definition list.

Then click OK on the page to save the configuration.

2.4.3. URL Group Settings

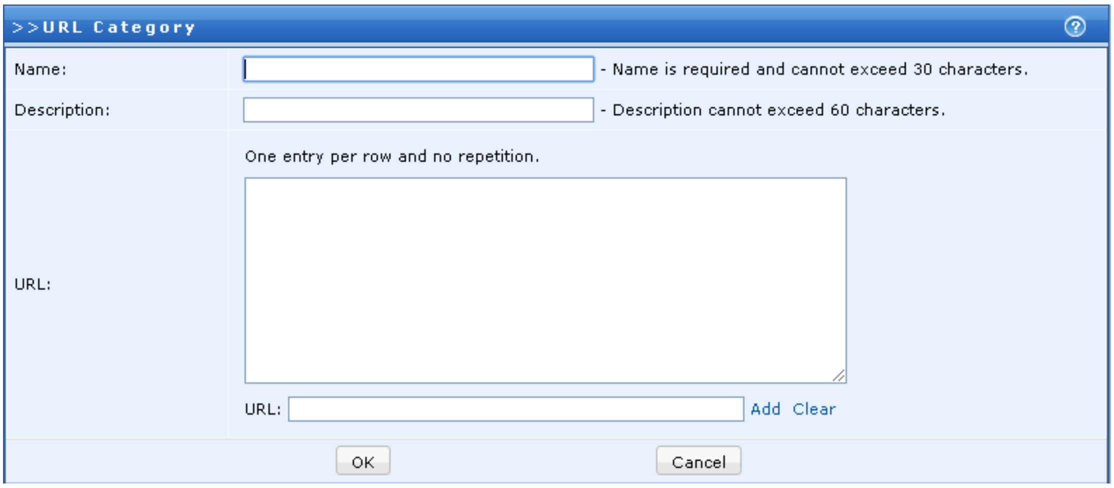
It's used to define the URL group. These URL groups can be used in 『Access Policy Settings』 as shown below:



>>URL Category

No.	Name	Description	Operation
1	Web Portals	Common Web Portals and Search Engines	Edit Delete
2	News	News Wbsites	Edit Delete
3	Online Recruitment	Online Recruitment Websites	Edit Delete
4	Online Shopping	Online Shopping Websites	Edit Delete
5	Online Banking	Online Banking Websites	Edit Delete
6	Video Websites	Online Video Websites	Edit Delete
7	Online Community	Online Community Websites	Edit Delete
8	Dating Sites	Dating Sites	Edit Delete
9	Zone and Blog	QQ Zone and Blogging Websites	Edit Delete

Click Add to pop up the dialog box - 【URL Group Settings】 as shown below:



Name: - Name is required and cannot exceed 30 characters.

Description: - Description cannot exceed 60 characters.

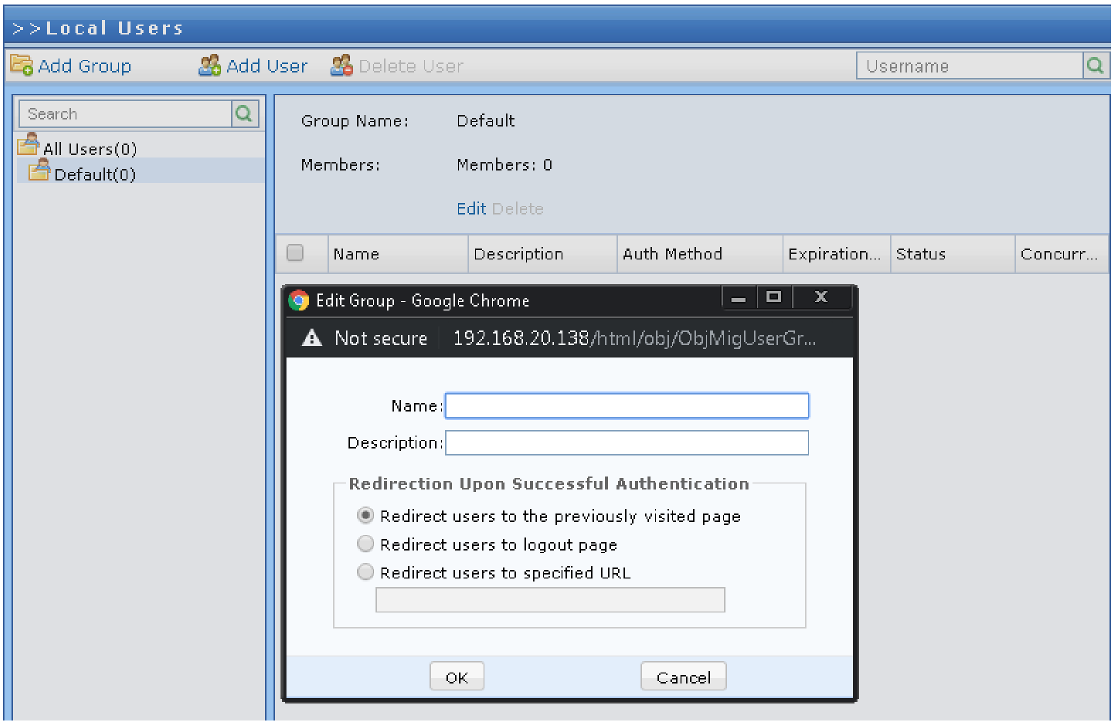
URL: One entry per row and no repetition.

URL:

Here you can edit a new URL group including multiple URLs. After addition, click OK to complete the definition of a URL group.

2.4.4. User Authentication Settings

It's used to define the user authentication group. After the successful authentication of different user authentication groups, it will jump to different pages. The page is shown as follows:



Group Name: Default

Members: Members: 0

192.168.20.138/html/obj/ObjMigUserGr...

Name:

Description:

Redirection Upon Successful Authentication

● Redirect users to the previously visited page

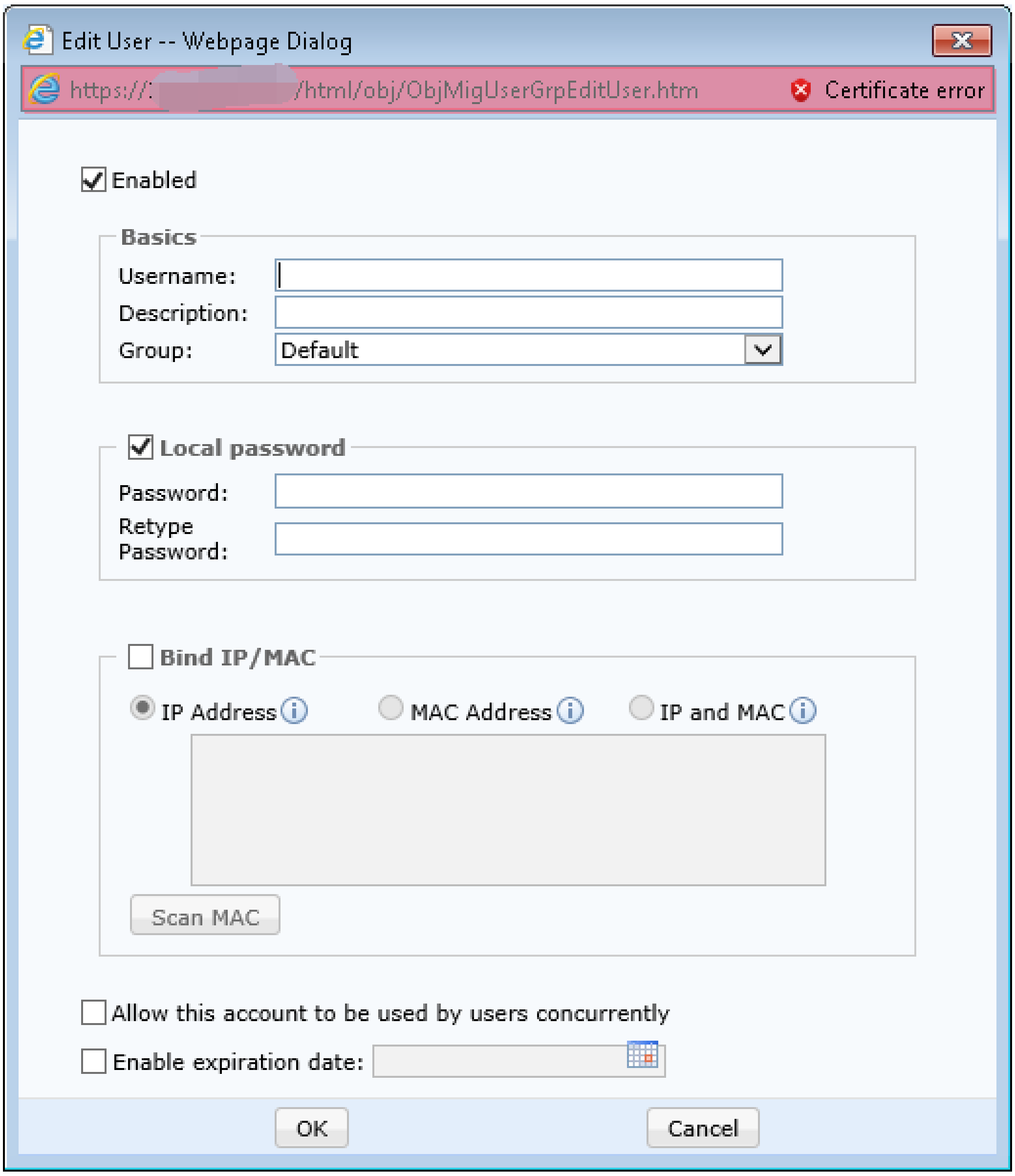
○ Redirect users to logout page

○ Redirect users to specified URL

『Name』: Name the user group. The name cannot be blank or exceed 30 characters.

『Description』: Describe the user group.

New user, username, description, group, password, ip/mac binding and other information. As shown in the figure.



Edit User -- Webpage Dialog

https://[redacted]/html/obj/ObjMigUserGrpEditUser.htm   Certificate error

☑ Enabled

Basics

Username:

Description:

Group: Default

☑ Local password

Password:

Retype Password:

☐ Bind IP/MAC

● IP Address ○ MAC Address ○ IP and MAC

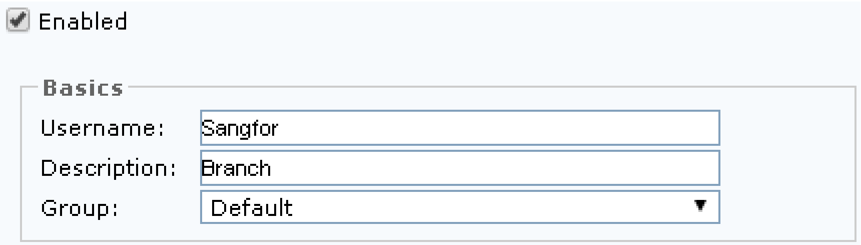
Scan MAC

☐ Allow this account to be used by users concurrently

☐ Enable expiration date:

OK   Cancel

【Add User】: Check [Enable this User], and fill in [Username], [Description] and [Current Group].



☑ Enabled

Basics

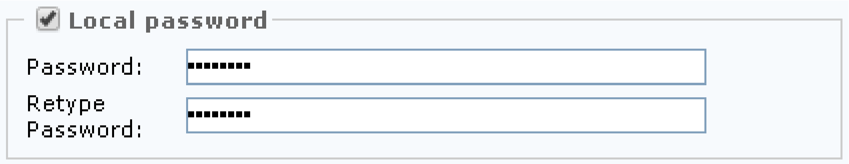
Username: Sangfor

Description: Branch

Group: Default

Check [Local Password] and enter the user login authentication password in the

[Password] input box.



☑ Local password

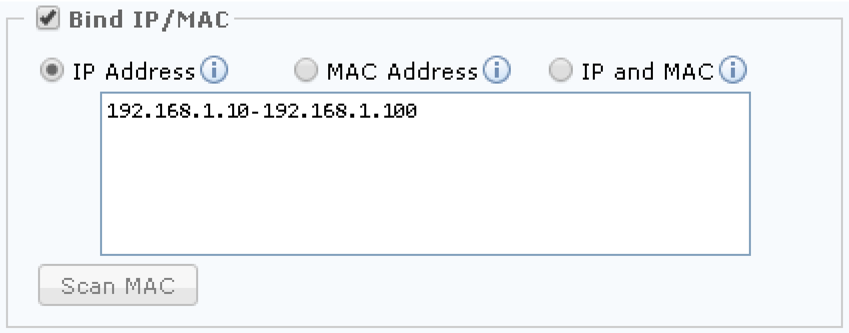
Password: •••••••••

Retype Password: •••••••••

Check [Bind IP/MAC Address] to bind the user to IP/MAC address. It requires in this example that the one-way binding IP range (i.e. to limit the scope of login IP) is 192.168.1.2-192.168.1.100.

Click [Binding Mode], and select the [One-way Binding User and Address] on the pop-up page

Check [Bind IP] to fill in 192.168.1.2-192.168.1.100 in the input box.

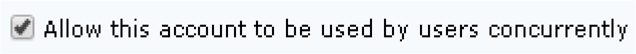


☑ Bind IP/MAC

● IP Address ○ MAC Address ○ IP and MAC

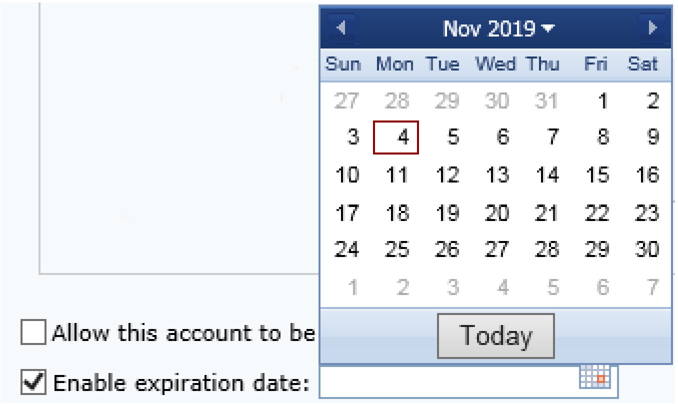
192.168.1.10-192.168.1.100

[Allow Multiple Users to Use the Account to Log in] is used to set whether the user with username and password authentication to allow multiple users to use this account to log in simultaneously. Check this option to allow multiple users to log in at the same time. In this example, the user allows multiple users to log in at the same time, so check this option.



☑ Allow this account to be used by users concurrently

[Expiration Time] is used to set the expiration time of the user.



Nov 2019

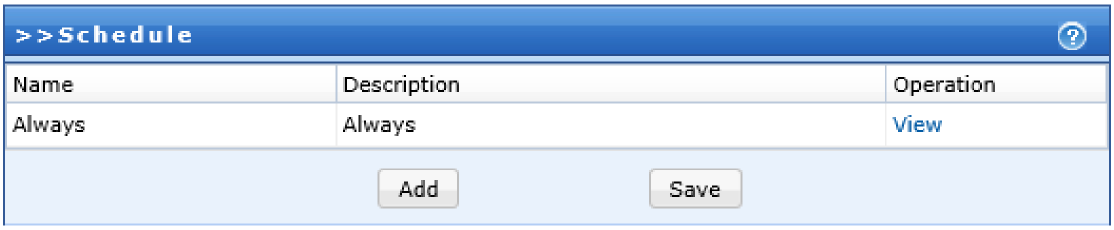
Sun	Mon	Tue	Wed	Thu	Fri	Sat
27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
1	2	3	4	5	6	7

□ Allow this account to be

☑ Enable expiration date:

2.4.5. Time Schedule Settings

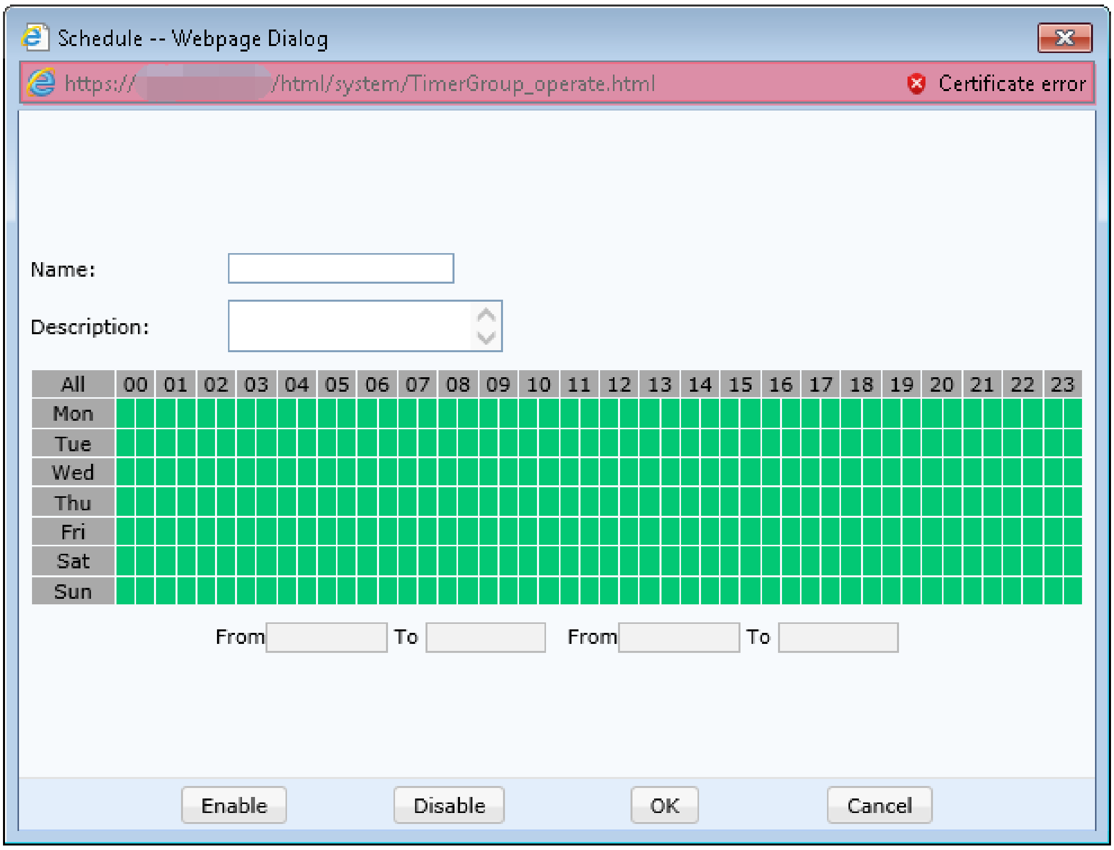
It's used to define the common time combination, which can be used in the modules such as『Access Control』,『Traffic Management』and『Firewall』to set corresponding effective / expiration time of rules. The time on the device shall prevail as shown below:



>>Schedule

Name	Description	Operation
Always	Always	View

Click "Add" to pop up the dialog box - 【Edit Time Schedule】as shown below:



https://[redacted]/html/system/TimerGroup_operate.html

Name:

Description:

All	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Mon	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩
Tue	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩
Wed	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩
Thu	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩
Fri	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩
Sat	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩
Sun	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩

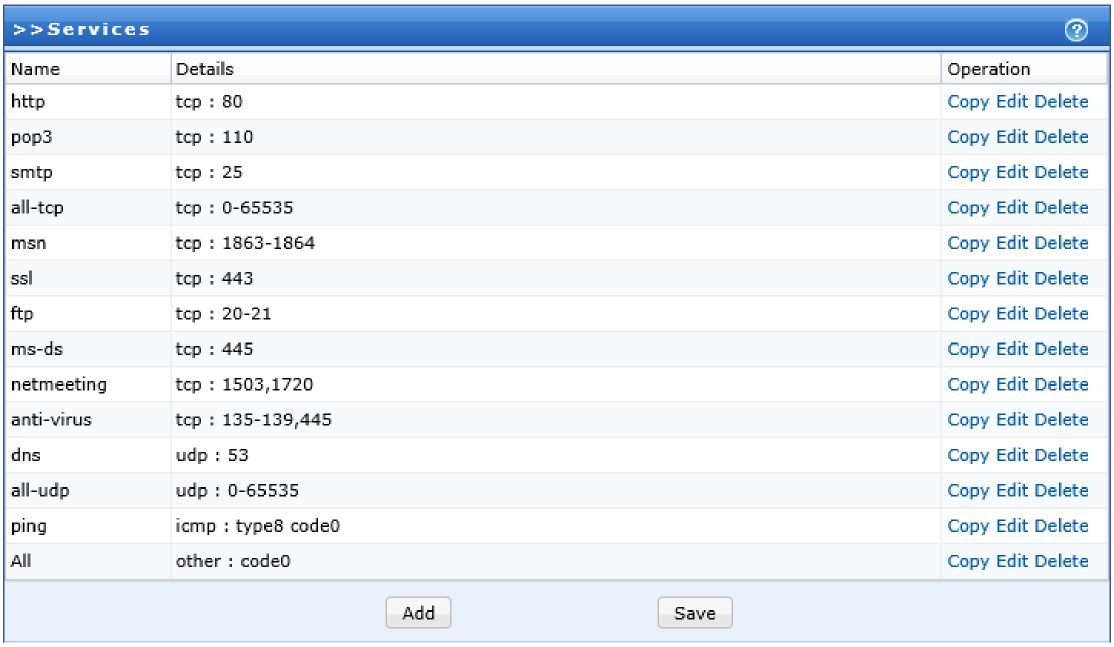
From To From To

Here a time segment named "Working Time" is defined with different combinations of time segments. The green refers to the effective time segment, while the gray is for the failure segment. Click OK to complete the definition of a time group.

Drag the mouse to select the time range, then set the selected segment via the Enable Rules or Disable Rules button on the page, and finally click OK to save this time schedule.

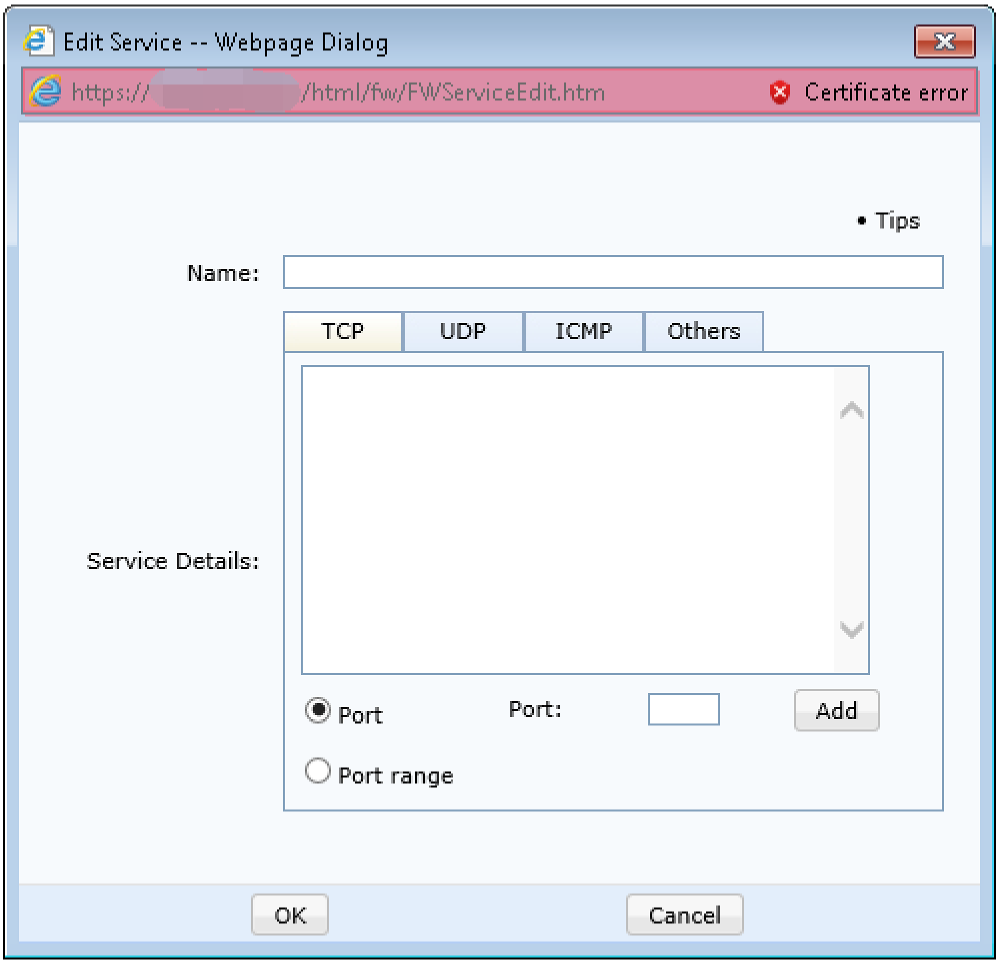
2.4.6. Network Services Settings

The software and communication program running via the Internet adopt different transmission protocols and ports. Before setting the firewall rules for these data, it's required to define their transmission protocols and ports as shown below:


>>Services

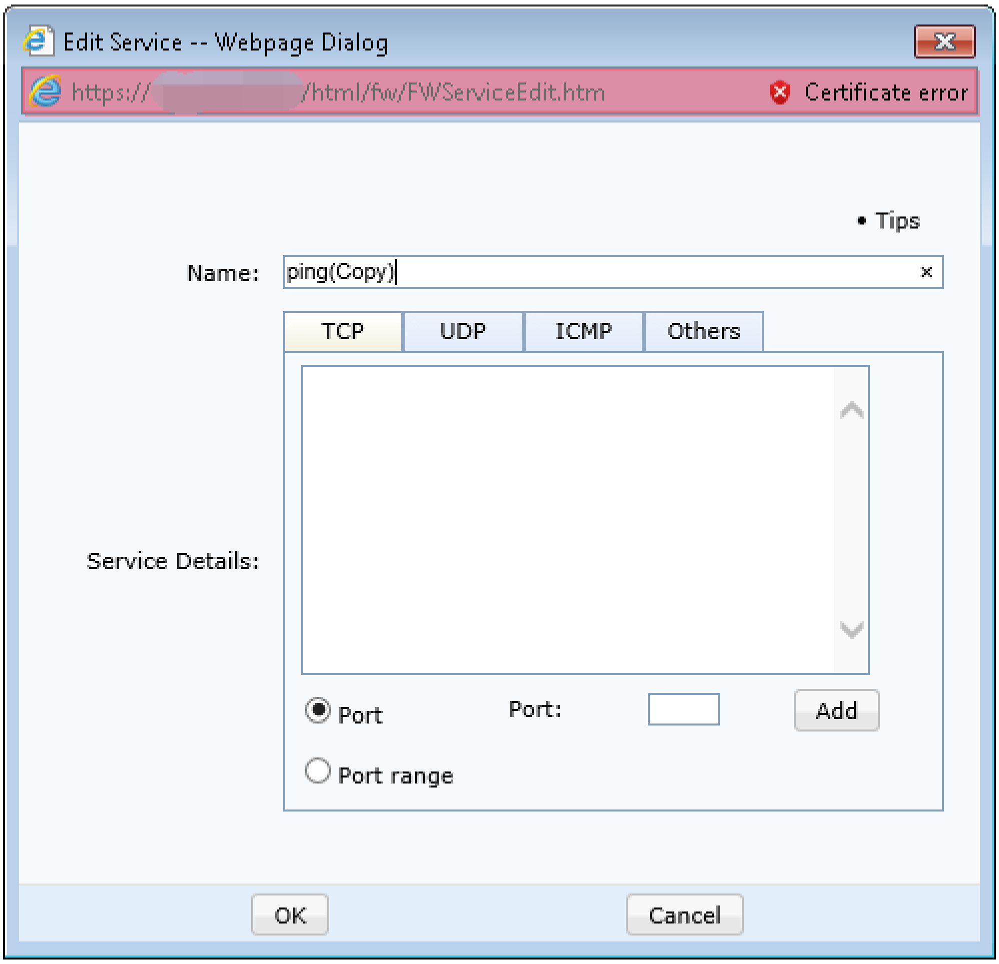
Name	Details	Operation
http	tcp : 80	Copy Edit Delete
pop3	tcp : 110	Copy Edit Delete
smtp	tcp : 25	Copy Edit Delete
all-tcp	tcp : 0-65535	Copy Edit Delete
msn	tcp : 1863-1864	Copy Edit Delete
ssl	tcp : 443	Copy Edit Delete
ftp	tcp : 20-21	Copy Edit Delete
ms-ds	tcp : 445	Copy Edit Delete
netmeeting	tcp : 1503,1720	Copy Edit Delete
anti-virus	tcp : 135-139,445	Copy Edit Delete
dns	udp : 53	Copy Edit Delete
all-udp	udp : 0-65535	Copy Edit Delete
ping	icmp : type8 code0	Copy Edit Delete
All	other : code0	Copy Edit Delete

For example: it's required to set transmission rules for SQL SERVER service data on the MIG hardware gateway. Firstly, define the protocols and ports used by SDL SERVER, then click Add to pop up a dialog box - 【Edit Firewall Information】 as shown below:



『Service Name』 can be customized (in this case set as SQL). For『Protocol』, select TCP and for『Port No.』, select 1433, then click Add to add to the box - service definition, click OK to add this service to the definition list of network service settings, and click OK to save the definition for SQL SERVER services.

Add a replication feature here, and you can copy the service rules directly. Click Replicate, the following page pops up:



Name: ping(Copy)

● Port

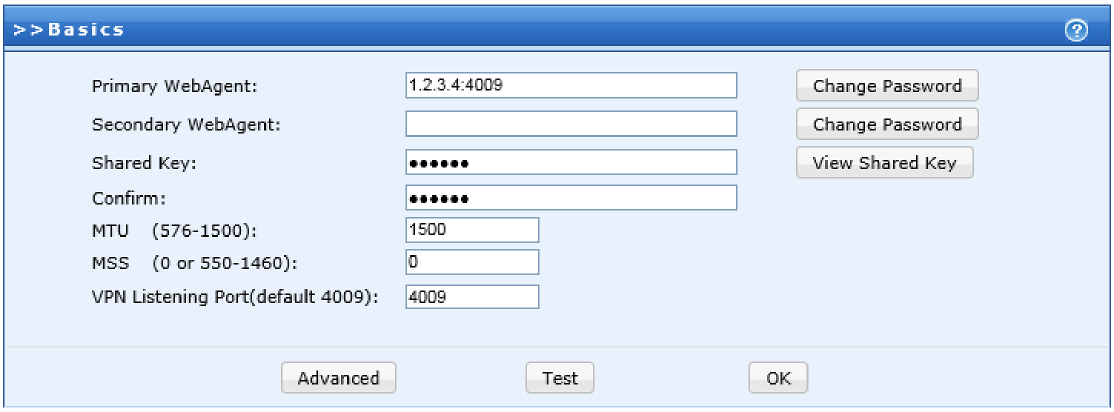
『Service Name』can be modified with the ports added in the same way as above. If the customer has an ERP system which needs to use SQL service ports and port 80, add them to this list. In the case of enabling rules, you only need to enable these rules for one service.

2.5. VPN Info Settings

It includes such modules as 『Basic Settings』, 『Certificate Management』, 『User Management』, 『Connection Management』, 『Virtual IP Pool』, 『Inter-tunnel Route Settings』, 『Third-party Connection』 and 『Advanced Settings』.

2.5.1. Basic Settings

It's used to set some basic VPN parameters. The page is shown as follows:



Primary WebAgent: 1.2.3.4:4009

Secondary WebAgent:

Shared Key: ●●●●●●

Confirm: ●●●●●●

MTU (576-1500): 1500

MSS (0 or 550-1460): 0

VPN Listening Port(default 4009): 4009

『Basic Settings』: include 『Primary, Secondary WEBAGENGT』, 『Shared Key』, 『View Shared Key』, 『MTU Value』, 『MSS Value』 and 『VPN Listening Port』.

『WEBAGENT』: refer to the address of the dynamic addressing file in WEB server, including the address for active Webagent and standby Webagent.

If it is "Dynamic Addressing (non-static IP at headquarters)", enter "WebAgent Web Address" (usually ended in .PHP). After WebAgent is entered, you can click Test to see if it can be connected. If the headquarters is of "Static IP", enter the address in the format of "IP Address: Port", such as 202.96.134.133:4009. Click Modify Password to set the WebAgent password, thus to prevent illegal users from embezzling the WebAgent to update the fake IP address, which works only for WEB address. Click Shared Key to set the shared key to prevent illegal device access. Click View Shared Key to enter login password, then view the shared key.

⚠**Note: If 『Webagent Password』 is set, it cannot be recovered once lost, and you have to contact the customer service center of SANGFOR to regenerate a file excluding the Webagent password and replace the original file. If『Shared Key』is set, all VPN sites cannot be interconnected with each other until they set the same 『Shared Key』. In the case of multiple lines and static IPs, WebAgent can be filled in the format of "IP1 # IP2: Port".**

『View Shared Key』: used to view the shared key, and the password of the system administrator admin to be entered.

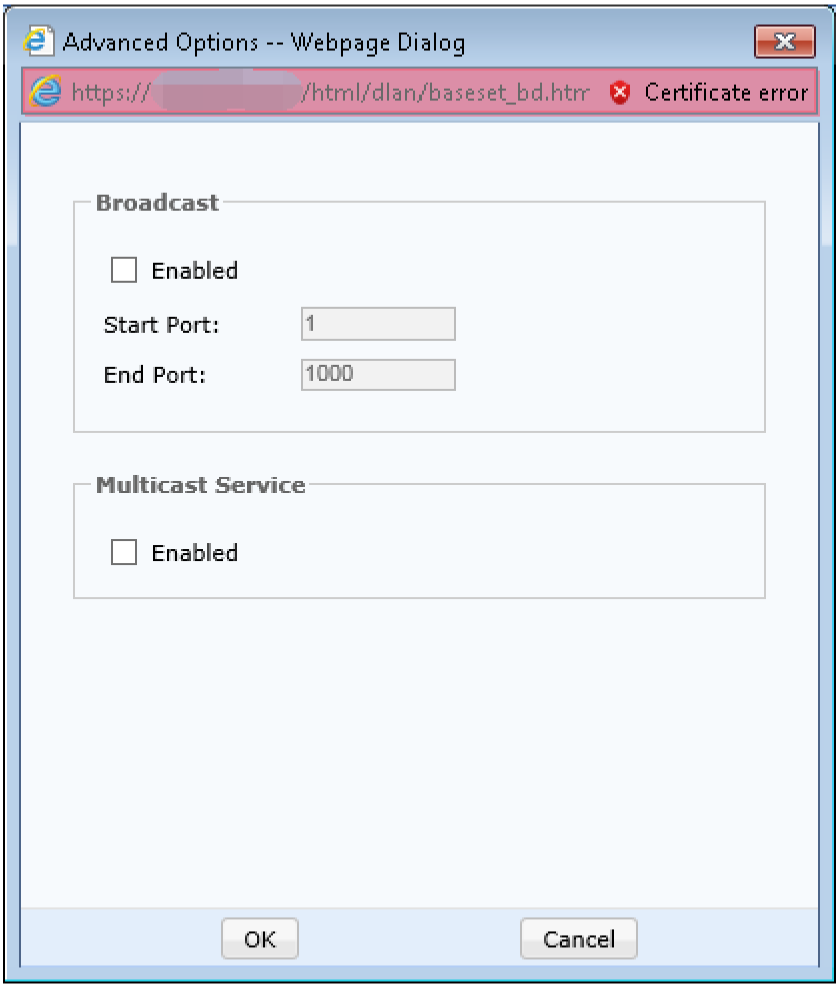
『MTU Value』: used to set the maximum MTU value of VPN value and being 1500 by default.

『VPN Listening Port』: used to set the listening port for VPN services. It is 4009 by default and can be set on demands.

『MSS Value』: used to set the maximum segment of VPN data under the UDP transmission mode.

⚠**Note: 『MTU Value』and『MSS Value』are generally kept at their default values, and only revised under the guidance of SANGFOR technical support engineers.**

Click Advanced to set VPN performance, broadcast and multicast settings, as shown in the following figure:



Advanced Options -- Webpage Dialog

https://[redacted]/html/dlan/baseset_bd.htm Certificate error

Broadcast

□ Enabled

Start Port: 1

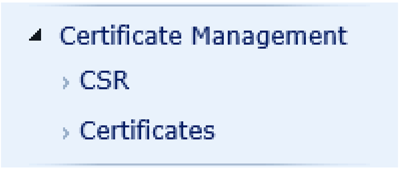
End Port: 1000

Multicast Service

□ Enabled

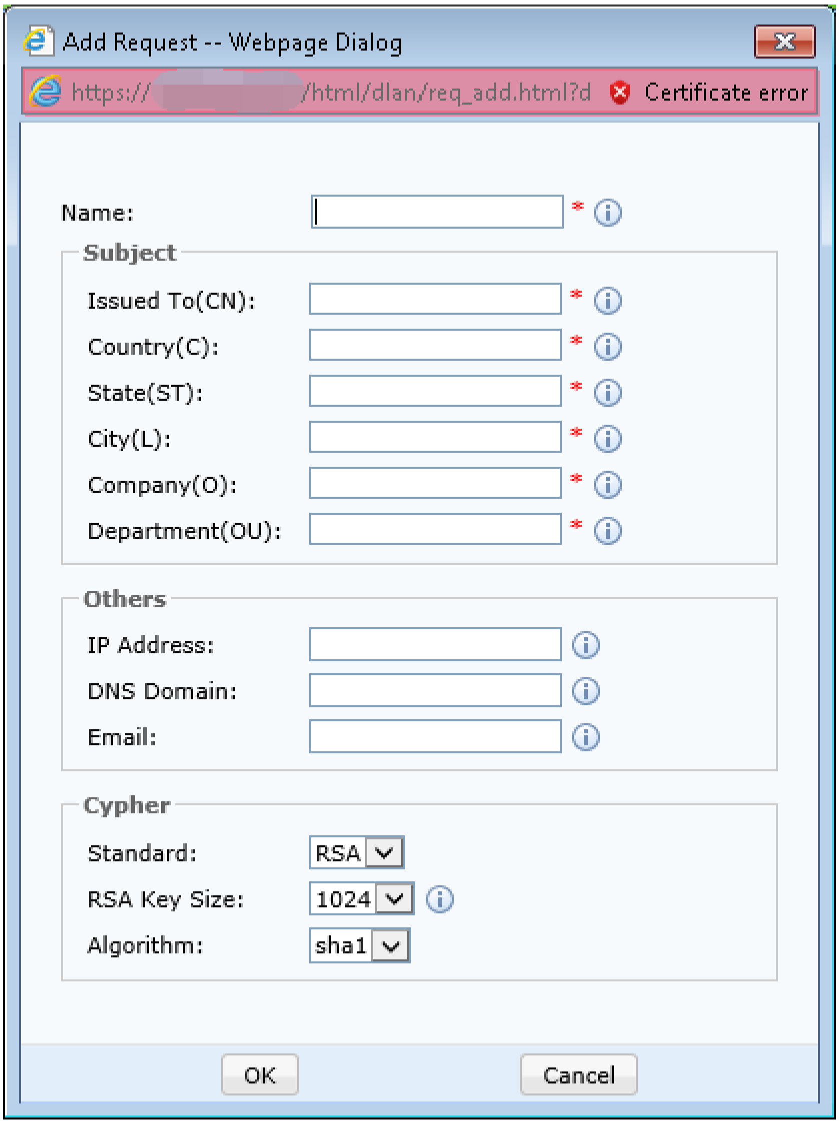
2.5.2. Certificate Management

『Certificate Management』 involves 『Certificate Request』 and 『Certificate List』, and is used to generate and import the RSA-signed certificate.



2.5.2.1. Certificate Request

Click "Add" to add a certificate request as shown in the figure below:



Add Request -- Webpage Dialog

https://[redacted]/html/dlan/req_add.html?d Certificate error

Name: *

Subject

Issued To(CN): *

Country(C): *

State(ST): *

City(L): *

Company(O): *

Department(OU): *

Others

IP Address:

DNS Domain:

Email:

Cypher

Standard: RSA

RSA Key Size: 1024

Algorithm: sha1

For 『Name』, 『Subject』 and 『Extension Identification Info』 modules, please enter real information.

[Cypher Settings]: Select the required password standard, RSA password length, and digest algorithms.

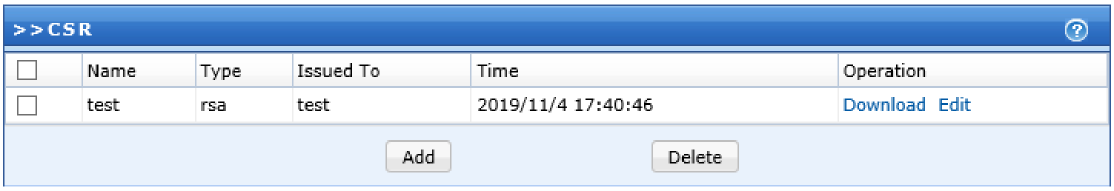
『Cypher Standard』: Choose international business key standard (RSA).

『RSA Key Size』: Choose 512, 1024 or 2048.

『Algorithm』: Choose sha1 or sha2.

After adding requests, a certificate application file and a key file will be generated.

Click "Download" to download the application file. Only offline certificate requests are supported. The figure is shown as below:

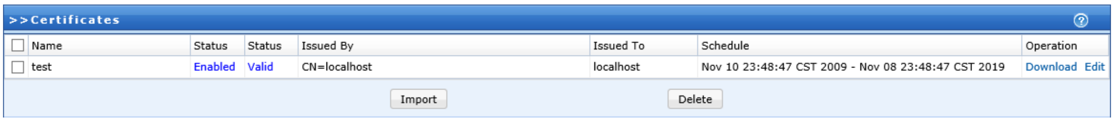


>>CSR

□	Name	Type	Issued To	Time	Operation
□	test	rsa	test	2019/11/4 17:40:46	Download Edit

2.5.2.2. Certificate List

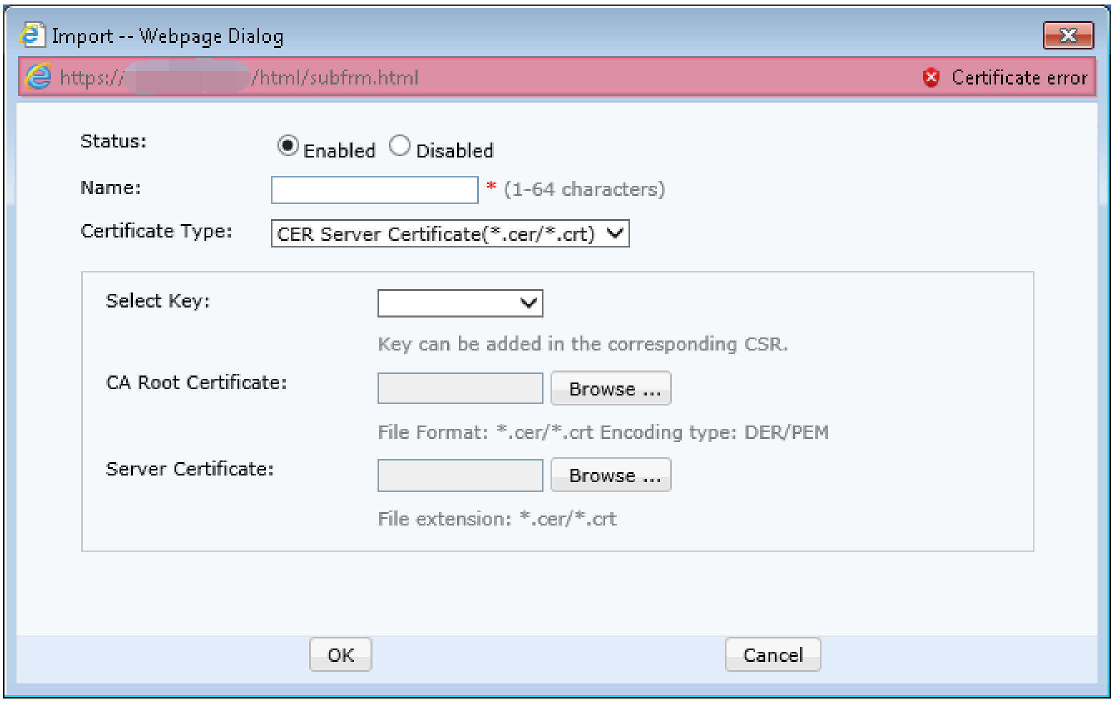
The certificate list page is shown as follows:



>>Certificates

□	Name	Status	Status	Issued By	Issued To	Schedule	Operation
□	test	Enabled	Valid	CN=localhost	localhost	Nov 10 23:48:47 CST 2009 - Nov 08 23:48:47 CST 2019	Download Edit

Click Import to import the offline application certificates into the certificate list. The page is shown as follows:



Import -- Webpage Dialog

https://[redacted]/html/subfrm.html

Certificate error

Status: ● Enabled ○ Disabled

Name: * (1-64 characters)

Certificate Type: CER Server Certificate(*.cer/*.crt)

Select Key:

Key can be added in the corresponding CSR.

CA Root Certificate: Browse ...

File Format: *.cer/*.crt Encoding type: DER/PEM

Server Certificate: Browse ...

File extension: *.cer/*.crt

『Status』: Used to enable or disable this certificate.

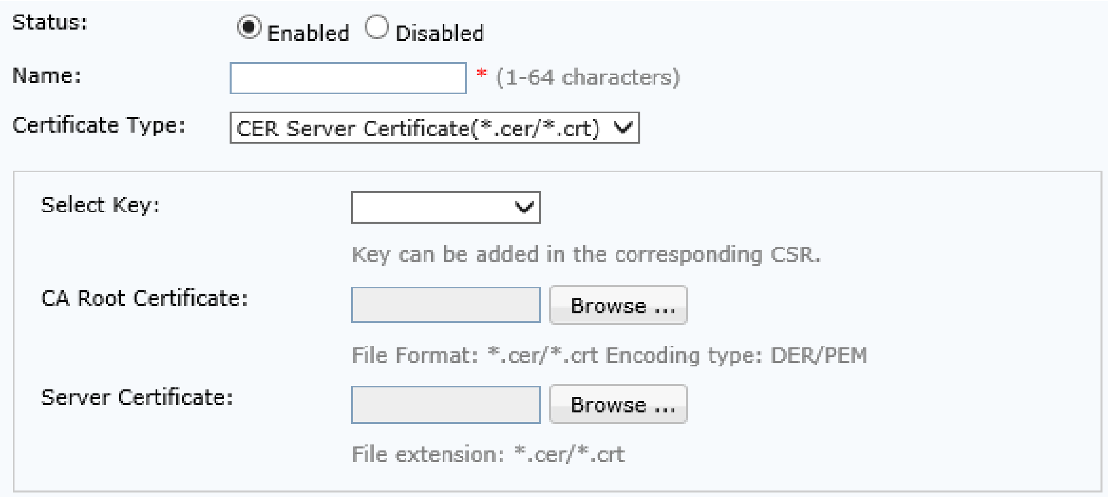
『Name』: Customize the name as the case may be.

『Certificate Type』: Select the local CER certificate (*.cer/*crt), CER root certificate

(*.cer/*crt),

PKCS#12 certificate (*.pfx/*.p12) or PKCS#7 certificate (*.p7b).

『Certificate Type』: Select the local CER certificate to import, with the verification key from the application information list, i.e. select the application information corresponding to the certificate to be imported. The page is shown as follows:



Status: ● Enabled ○ Disabled

Name: * (1-64 characters)

Certificate Type: CER Server Certificate(*.cer/*.crt)

Select Key:

Key can be added in the corresponding CSR.

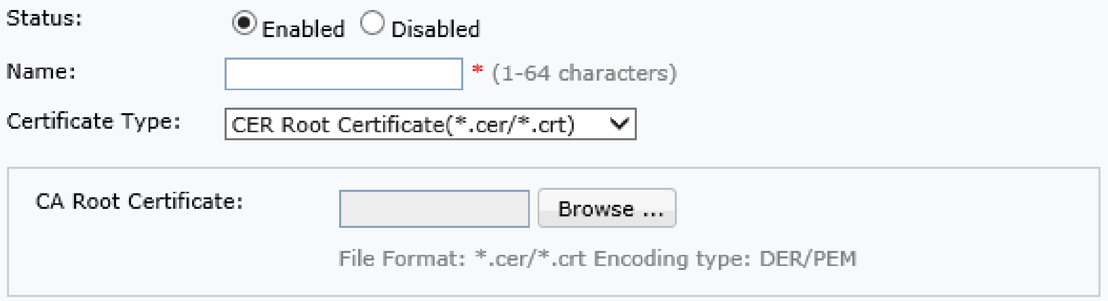
CA Root Certificate: Browse ...

File Format: *.cer/*.crt Encoding type: DER/PEM

Server Certificate: Browse ...

File extension: *.cer/*.crt

『Certificate Type』: Select the CER root certificate to import. The page is shown as follows:



Status: ● Enabled ○ Disabled

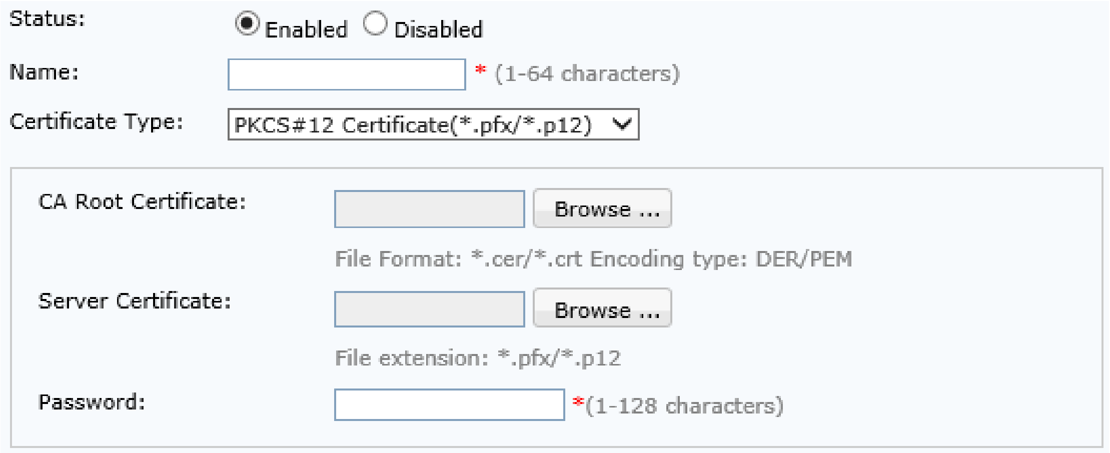
Name: * (1-64 characters)

Certificate Type: CER Root Certificate(*.cer/*.crt)

CA Root Certificate: Browse ...

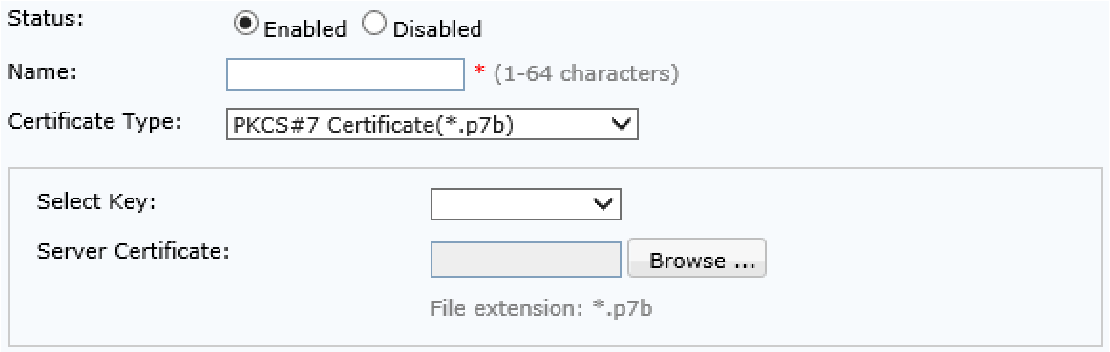
File Format: *.cer/*.crt Encoding type: DER/PEM

『Certificate Type』: Select PKCS#12 certificate to import. The protection password is filled in when the certificate is imported or generated. The certificate can be imported successfully only when the root certificate and protection password are correct. The page is shown as follows:



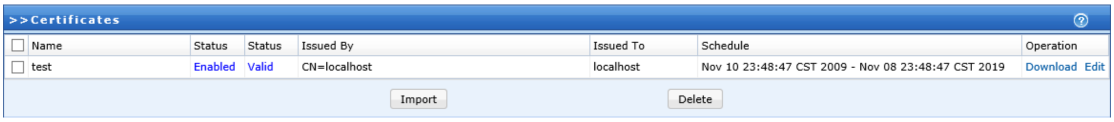
Status:	● Enabled ○ Disabled
Name:	* (1-64 characters)
Certificate Type:	PKCS#12 Certificate(*.pfx/*.p12)
CA Root Certificate:	Browse ... File Format: *.cer/*.crt Encoding type: DER/PEM
Server Certificate:	Browse ... File extension: *.pfx/*.p12
Password:	*(1-128 characters)

『Certificate Type』: Select PKCS#7 certificate to import. The verification key comes from the application information list. Namely, select the application information corresponding to the certificate to be imported. The figure is shown as below:



Status:	● Enabled ○ Disabled
Name:	* (1-64 characters)
Certificate Type:	PKCS#7 Certificate(*.p7b)
Select Key:	
Server Certificate:	Browse ... File extension: *.p7b

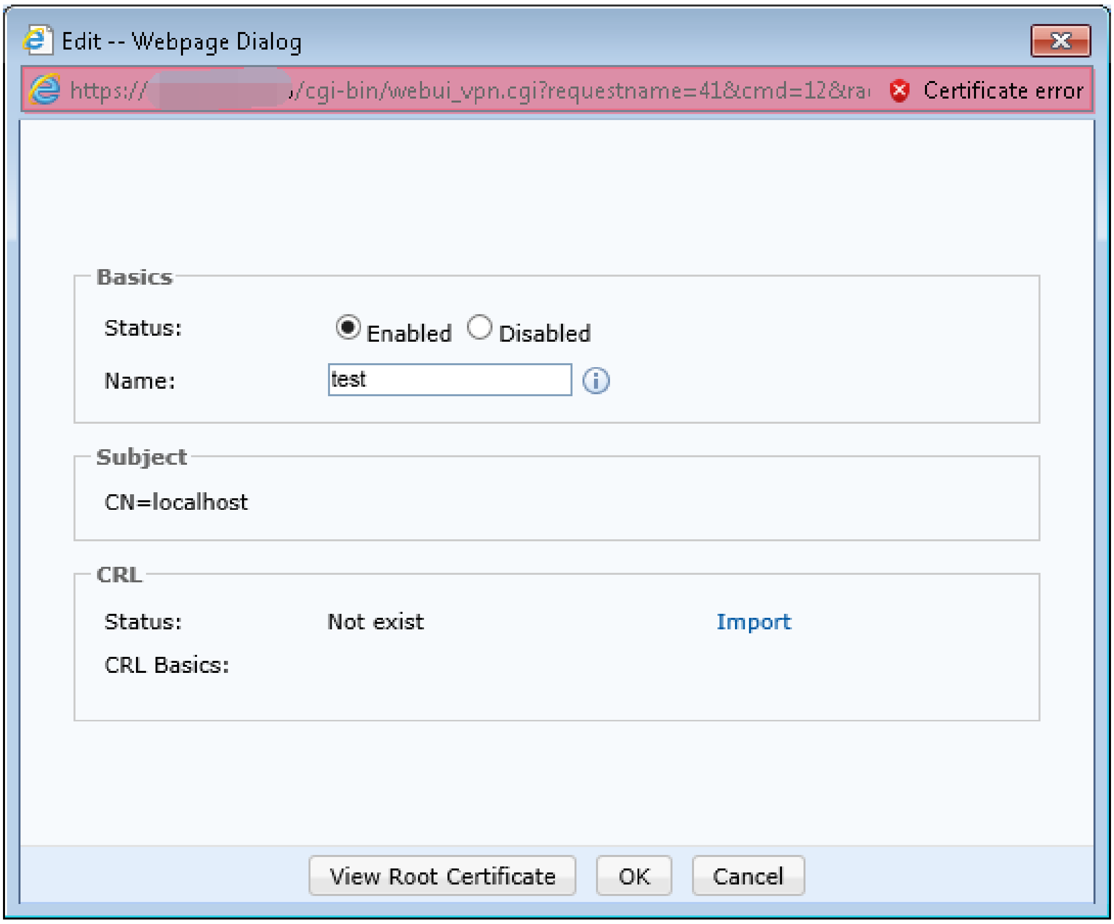
After the certificate is imported, you can view the certificate information in the certificate list, and you can edit and download them. The figure is shown as below:



>>Certificates

□ Name	Status	Status	Issued By	Issued To	Schedule	Operation
□ test	Enabled	Valid	CN=localhost	localhost	Nov 10 23:48:47 CST 2009 - Nov 08 23:48:47 CST 2019	Download Edit

Click Edit to view the certificate details. The page is shown as follows:



Edit -- Webpage Dialog

https://[redacted]/cgi-bin/webui_vpn.cgi?requestname=41&cmd=12&ra Certificate error

Basics

Status: ● Enabled ○ Disabled

Name: test

Subject

CN=localhost

CRL

Status: Not exist Import

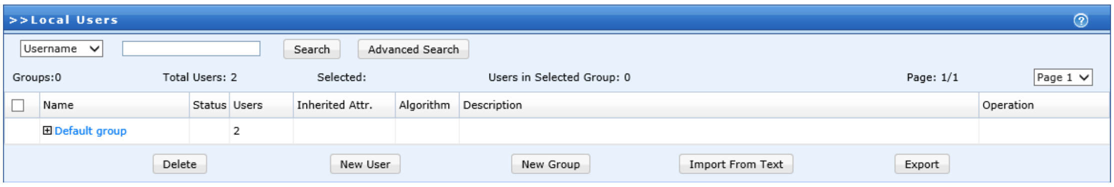
CRL Basics:

Click Download to download the certificate.

When the certificate is a root certificate, it supports to download the CA root certificate. If not, it supports to download the CA root certificate or PRCS#12 certificate (*.pfx/*.p12).

2.5.3. User Management

『User Management』 is used to manage the VPN access account information, set the user account and password for access to VPN, the algorithms for the account, and user type, group the users and set the common attributes of group users, whether to enable the hardware bundle authentication, the account valid period, the LAN permissions of the account, the multicast settings, NAT settings within tunnels, and other user policies. The figure is shown as below:

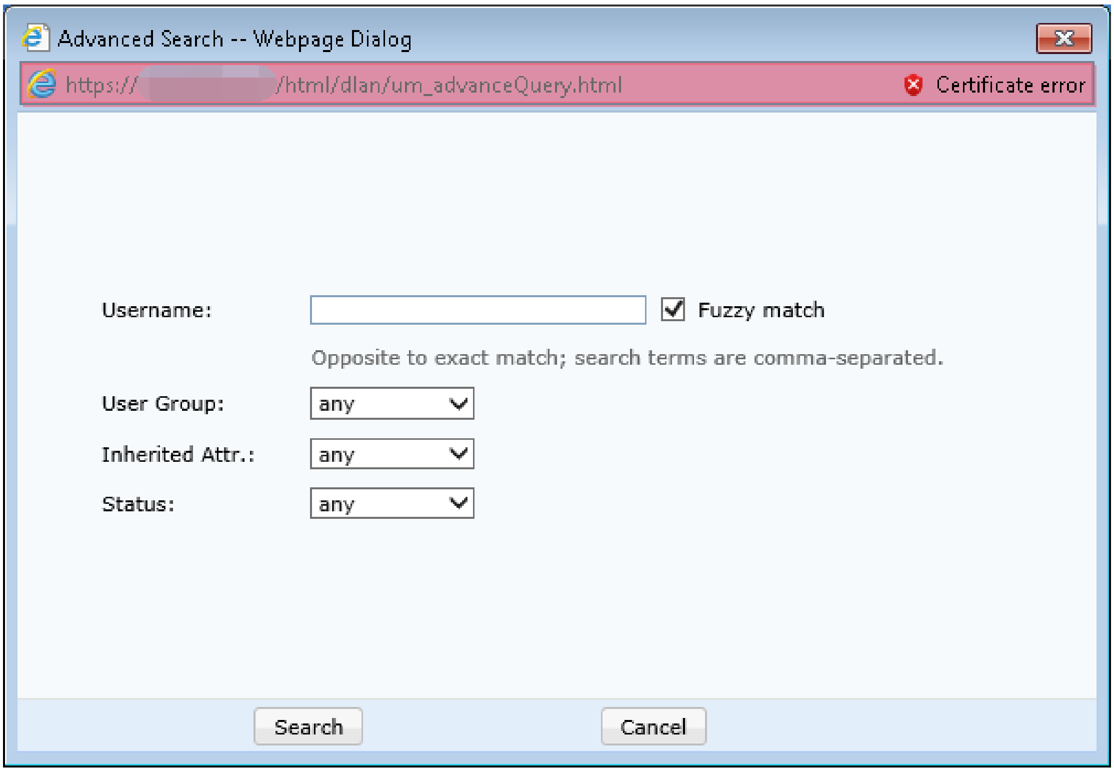


Groups:0 Total Users: 2 Selected: Users in Selected Group: 0 Page: 1/1 Page 1

□	Name	Status	Users	Inherited Attr.	Algorithm	Description	Operation
	⊞Default group		2				

Click Search to search for the username entered so as to edit the user found out.

Click Advanced Search to add filtering conditions for the found users to search for. As shown below:



https://[redacted]/html/dlan/um_advanceQuery.html

Username: ☑ Fuzzy match

Opposite to exact match; search terms are comma-separated.

User Group: any

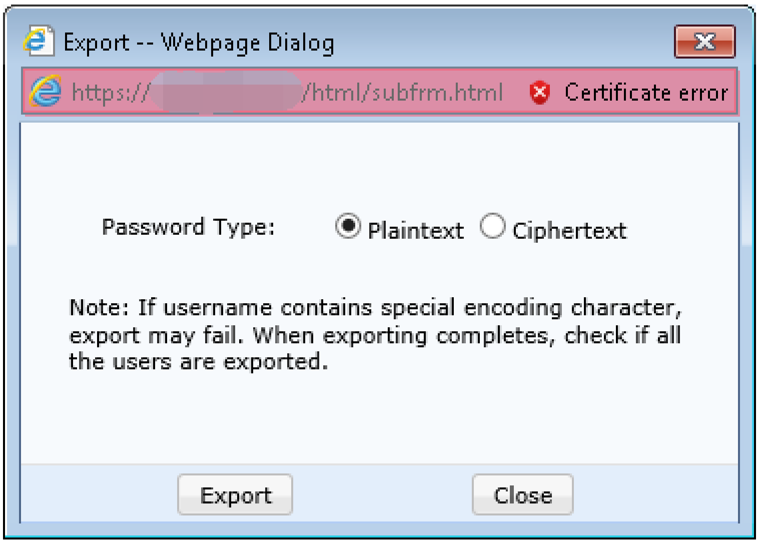
Inherited Attr.: any

Status: any

Click Delete to delete the users selected.

Click Import from Text to import user information from TXT or CSV files.

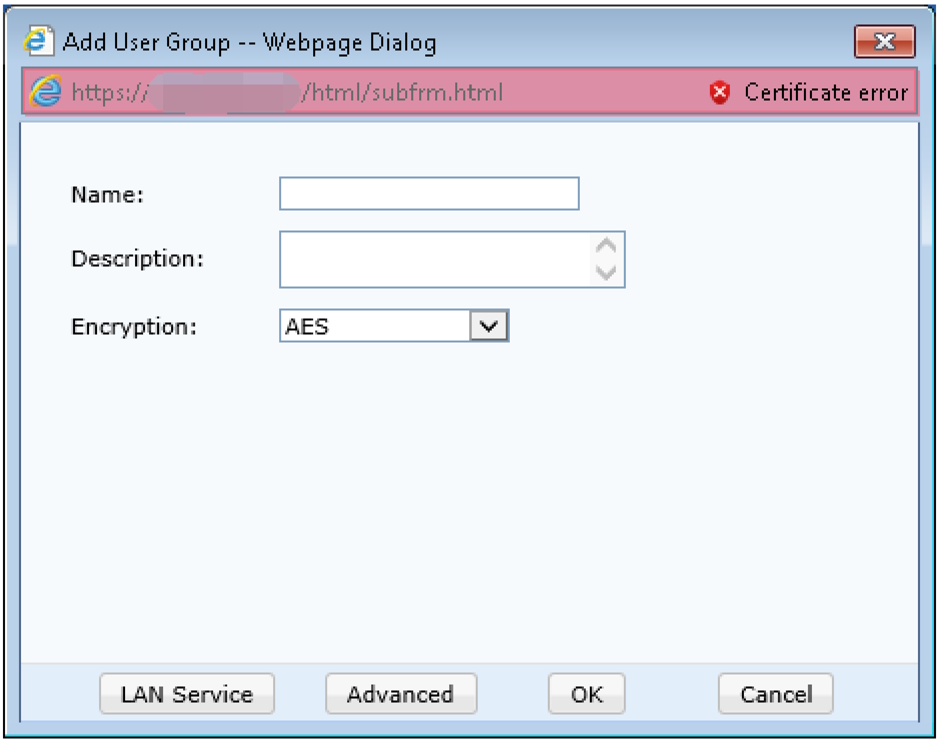
Click Export User to export the user from the device to the local for saving. You can choose whether the exported user password is encrypted or not. The page is shown as follows:



Password Type: ● Plaintext ○ Ciphertext

Note: If username contains special encoding character, export may fail. When exporting completes, check if all the users are exported.

『User Group』: Used to set the user group『Name』,『Description』and the common attributes (including『Encryption Algorithm』,『Enable Network Neighborhood』,『LAN Permissions』and『Advance』as shown below:



Add User Group -- Webpage Dialog

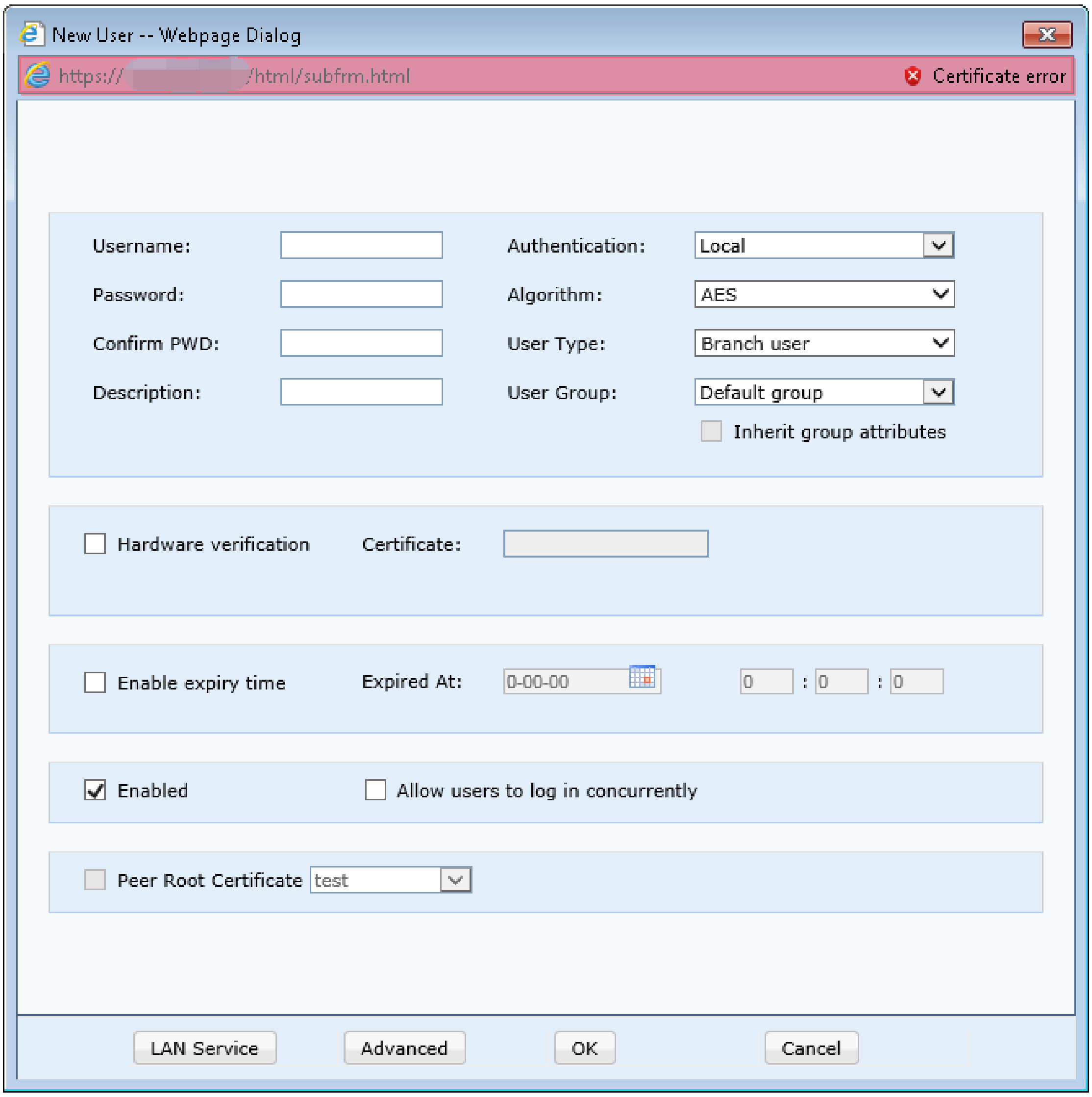
https://[redacted]/html/subfrm.html Certificate error

Name:

Description:

Encryption: AES

『Add User』: Used to set『Username』, 『Password』, 『Description』 and 『Others』 in order for the account accessed as shown below:



New User -- Webpage Dialog

https://[redacted]/html/subfrm.html

Certificate error

Username:

Password:

Confirm PWD:

Description:

Authentication: Local

Algorithm: AES

User Type: Branch user

User Group: Default group

□ Inherit group attributes

□ Hardware verification   Certificate:

□ Enable expiry time   Expired At: 0-00-00   0 : 0 : 0

☑ Enabled   □ Allow users to log in concurrently

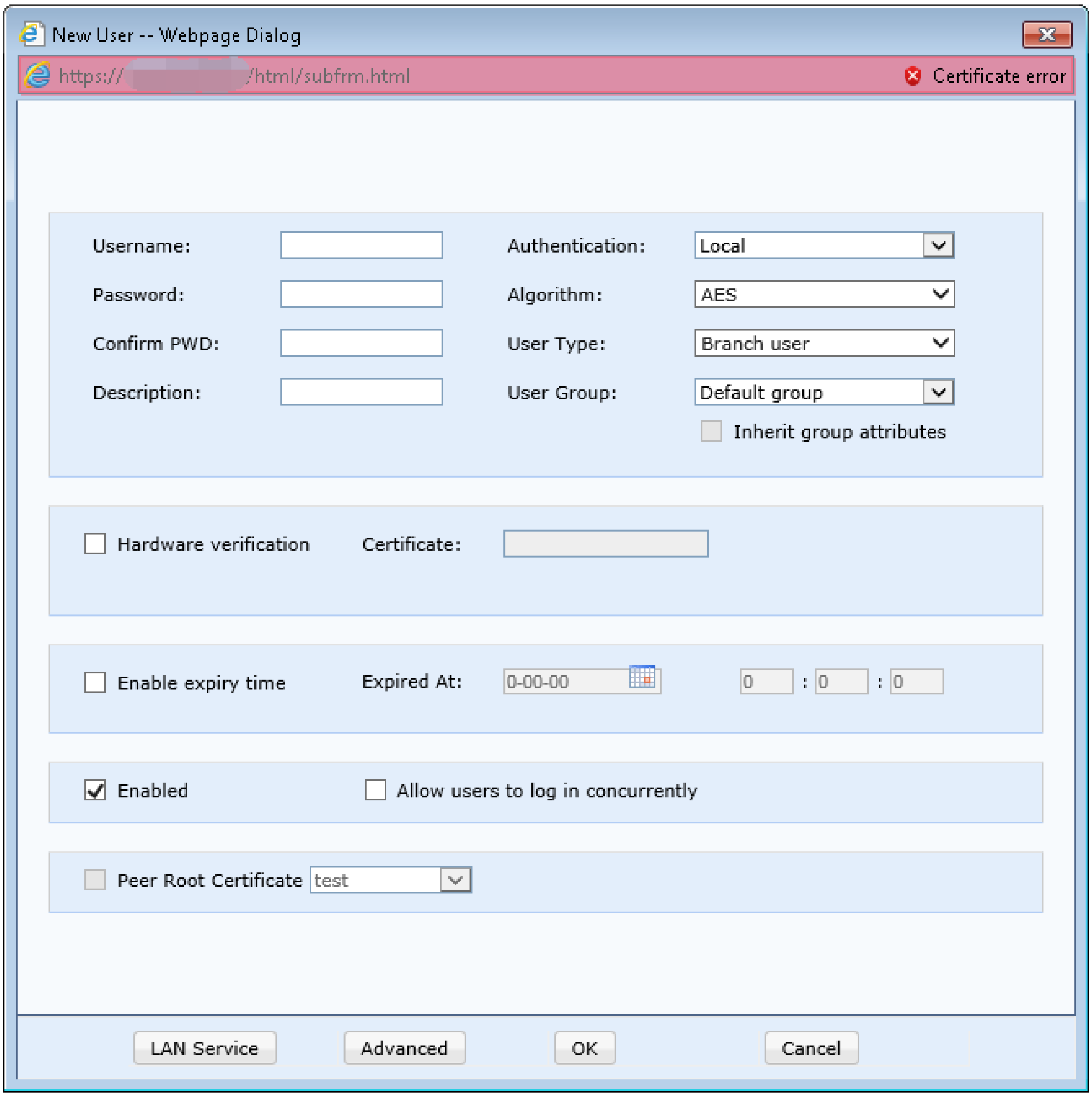
□ Peer Root Certificate test

『Authentication Method』 is used to set the user authentication type, including local authentication (i.e. Username password authentication) and certificate authentication.

For the certificate authentication, only after the username is subject to certificate authentication along with the field "Issued to" in the branch certificate, you can select corresponding certificates. When the certificate used by the branch end is not issued by the same CA authority as the certificate of the local end, import the CA root certificate of the peer end into the certificate list first, and then select the corresponding CA certificate

in the designated root certificate of the peer end.

In case of multiple users using certificate authentication, there is no need to add these users one by one. Just enable the default user and select the certificate authentication, then set corresponding rules, finally import these users meeting certificate authentication. In addition, these rules can be used to determine whether the user is allowed or not. See the figure below:



New User -- Webpage Dialog

https://[redacted]/html/subfrm.html

Certificate error

Username:

Password:

Confirm PWD:

Description:

Authentication: Local

Algorithm: AES

User Type: Branch user

User Group: Default group

□ Inherit group attributes

□ Hardware verification   Certificate:

□ Enable expiry time   Expired At: 0-00-00   0 : 0 : 0

☑ Enabled   □ Allow users to log in concurrently

□ Peer Root Certificate test

『Authentication Method』: When the user type is selected as "Branch" , you can select local authentication or certificate authentication. The certificate for authentication can be selected from the new ones in "Certificate List".

『User Type』: Branch

『Use Group』: Used to group the users. Check [Use Group Attributes], you can activate the settings for『User Group』and add the user to a certain user group and apply the common attributes of this group.

Before setting "Use Group Attributes", add user groups. After a user joins a user group, its『Algorithms』,『Permissions』and 『Advance』cannot be set alone.

『Enable Hardware Verification』: Used to set the certificate authentication based on hardware features. Once enabled, please select the certificate file (*.id) corresponding to the user.

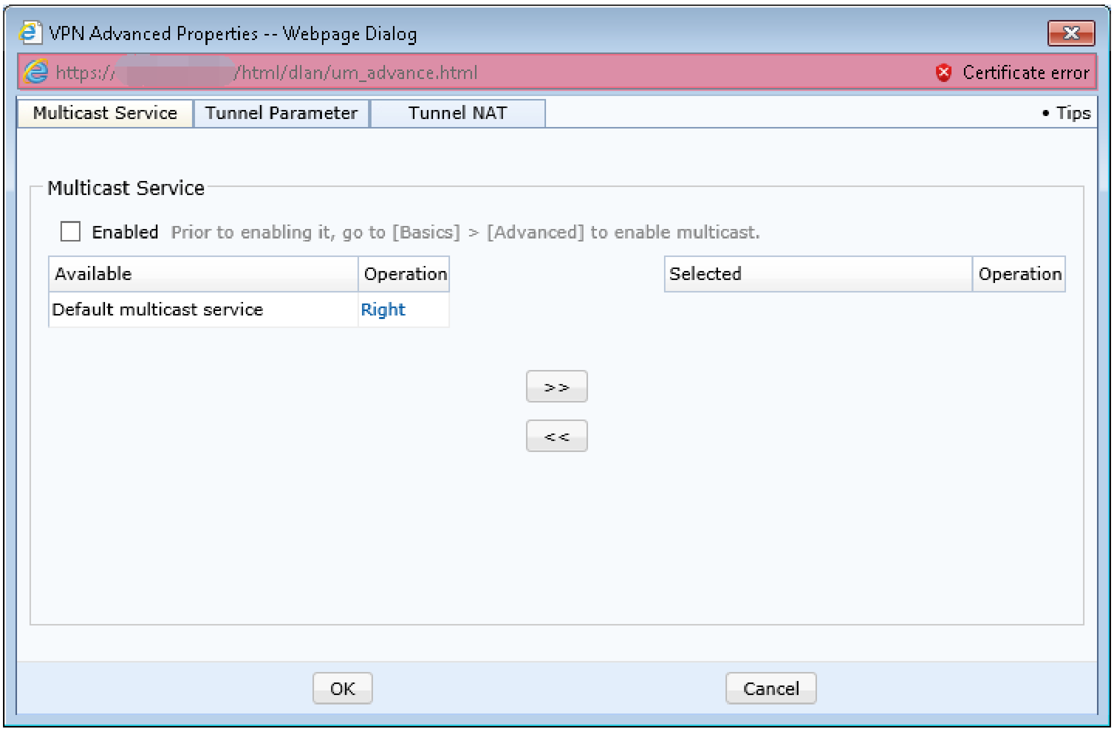
『Enable Expiration Time』: Used to set the valid time and expiration time for "Account Accessed".

『Enable Multi-user Login』: Used to set whether to allow multiple users to share the account to log in to VPN.

『LAN Service』: Used to set the access permissions after the user's access to VPN, i.e. allowing the user to access some services only. In general, no limit is set by default.

Before enabling 『LAN Permissions』, please add required services in 『VPN Settings』 → 『Advanced Settings』 → 『LAN Service Settings』.

『Advanced』: Used to set some advanced attributes for users after accessing VPN, including multicast service settings and tunnel parameters settings. Multicast services are mainly to meet the needs of applications requiring multicast support such as videos between headquarters and branches. The setup page is shown as below:


VPN Advanced Properties -- Webpage Dialog
https:// [redacted] /html/dlan/um_advance.html
Certificate error
Multicast Service
Tunnel Parameter
Tunnel NAT
• Tips

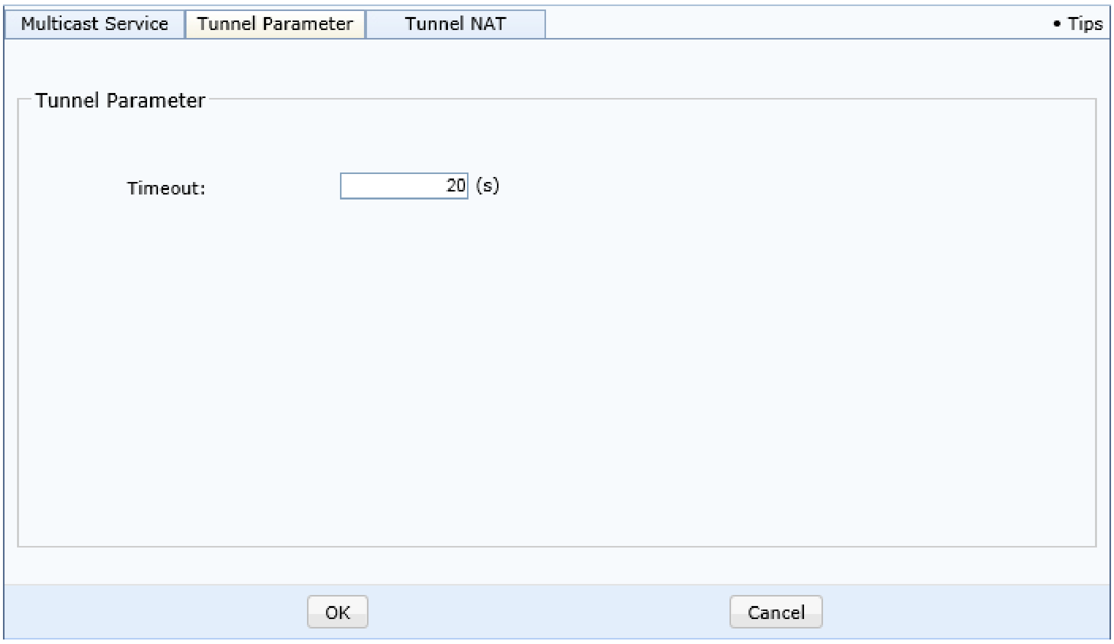
Multicast Service

☐ Enabled Prior to enabling it, go to [Basics] > [Advanced] to enable multicast.

Available	Operation
Default multicast service	Right

Selected	Operation

『Tunnel Parameters Settings』: Used to set the VPN tunnel timeout.



Tunnel Parameter

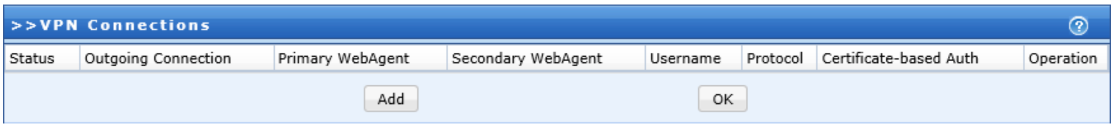
Timeout: 20 (s)

『VPN Tunnel Timeout』: In the case of a large network delay and a high rate for packet loss, SANGFOR VPN can set specific timeout for these networks. The timeout for each tunnel shall be subject to the configuration by the headquarters, and should be 20s by default. But in a poor network, the timeout can be extended.

2.5.4. Connection Management

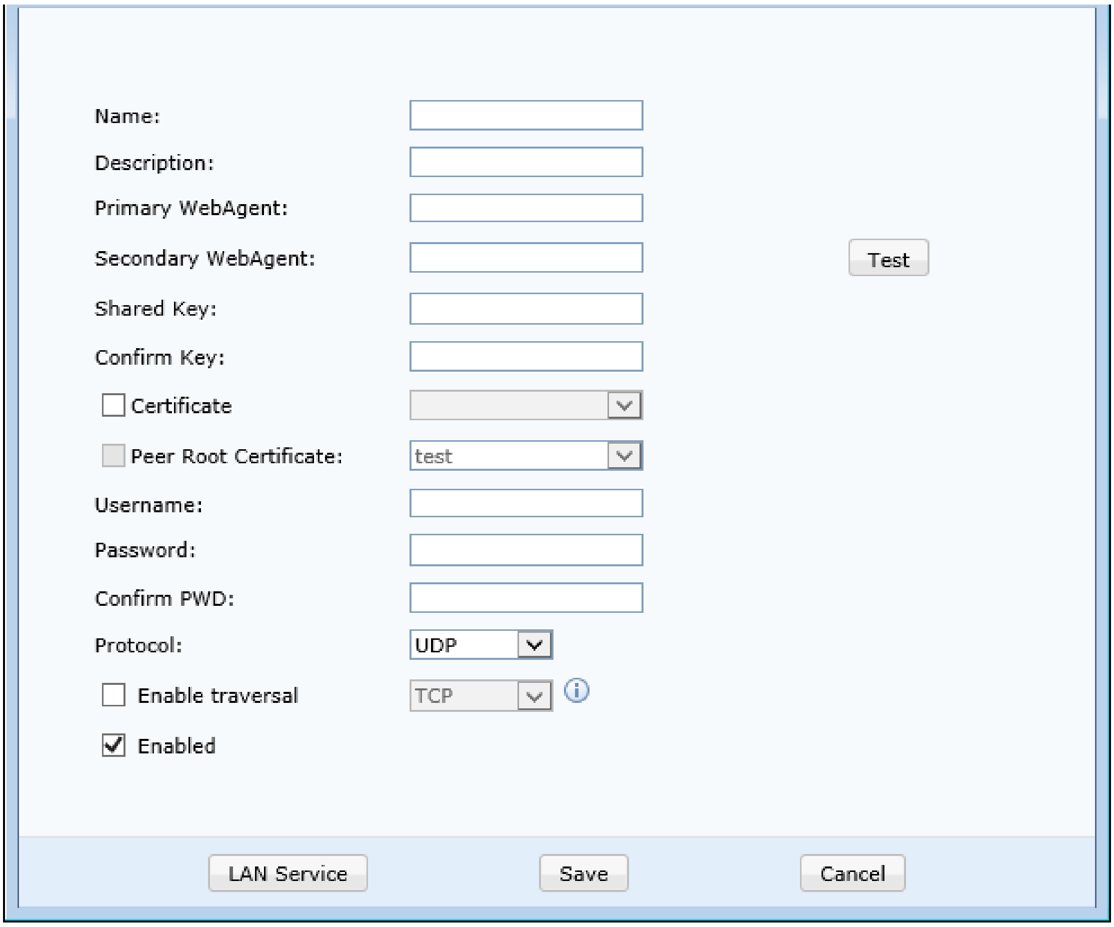
VPN hardware gateway can provide self-management and setting functions for interconnection of multiple network nodes (forming "mesh" network). You can make relevant settings in『Connection Management』. The page is shown as follows:

⚠**Note: Only the device is used as a branch to connect other MIG devices, can the connection management be enabled. If at the local end is the VPN headquarters device, there is no need to enable the connection management.**



Status	Outgoing Connection	Primary WebAgent	Secondary WebAgent	Username	Protocol	Certificate-based Auth	Operation

『Add』: Used to add a connection to other VPN headquarters. The page is shown as follows:



Name:

Description:

Primary WebAgent:

Secondary WebAgent:

Shared Key:

Confirm Key:

□ Certificate

□ Peer Root Certificate: test

Username:

Password:

Confirm PWD:

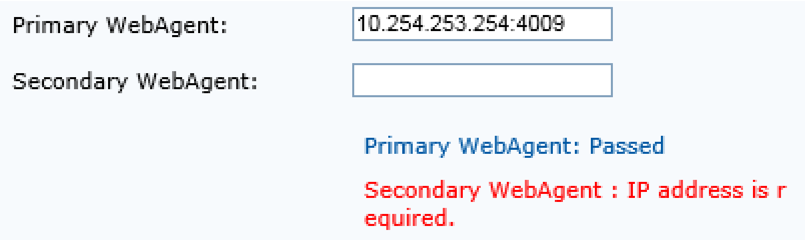
Protocol: UDP

□ Enable traversal TCP

☑ Enabled

『Headquarters Name』 and 『Description』 are used to indicate the connection name and can be filled in at will.

『Primary/Secondary Webagent』 is used to fill in the Webagent corresponding to the headquarters to be connected. Click "Test" to check whether the Webagent works normally or not. See the figure below for the results:



Primary WebAgent: 10.254.253.254:4009

Secondary WebAgent:

Primary WebAgent: Passed

Secondary WebAgent : IP address is r equired.

Test requests are initiated from the machine rather than the device. If the webagent is in domain name format, successful test indicates that the web exists, otherwise it does not exist. If the webagent adopts static IP mode, successful test indicates that the IP:PORT filled in is of correct format, but it does not mean that the VPN connection succeeds.

『Protocol』 includes [TCP] and [UDP], and is used to determine the encapsulation type for transmission of VPN packet. The default is [UDP] transmission mode.

『Shared Key』,『Username』 and 『Password』 shall be filled in according to the access account information provided by the headquarters.

『Enable Traversal』 The tunnels established with UDP protocol may be blocked, so it's necessary to enable the blocking penetration.

TCP's encapsulation penetration is added to its header in UDP message, making the packet look like a TCP packet in appearance, thus to penetrate the encapsulation. However, TCP penetration does not achieve the TCP three-way handshake, so there is still the possibility of being blocked by operators.

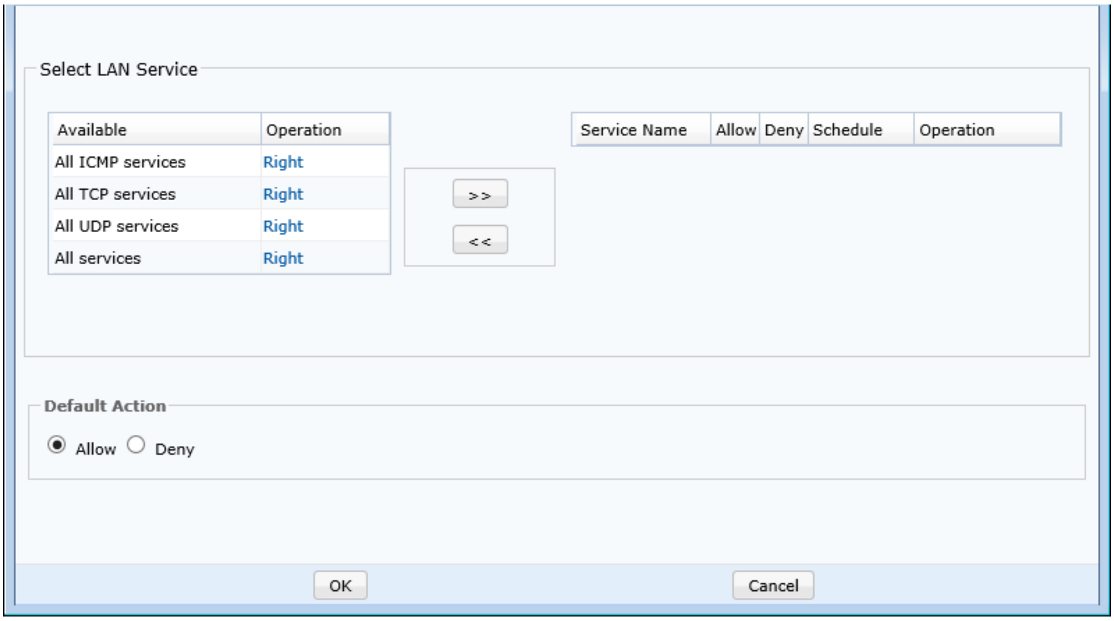
ESP's encapsulation penetration is added to its header in UDP message, making the packet look like an ESP packet in appearance, thus to penetrate the encapsulation. This kind of penetration can also be recognized by the operators, leading to penetration failure.

『Certificate Authentication』 is used to select corresponding certificates for authentication.

『Specify Peer Root Certificate』: Check and select it when the certificate used by the headquarters is not issued by the same CA as the local one.

⚠Note: If the certificate authentication is applied, there is no need to fill in the username, as the field "Issued to" on the certificate will be automatically acquired.

Click LAN Service to set the permissions for VPN peer, that is, to specify which services of local end the VPN peer can access, as shown in the figure below:



Select LAN Service

Available	Operation
All ICMP services	Right
All TCP services	Right
All UDP services	Right
All services	Right

Service Name	Allow	Deny	Schedule	Operation

Default Action

● Allow ○ Deny

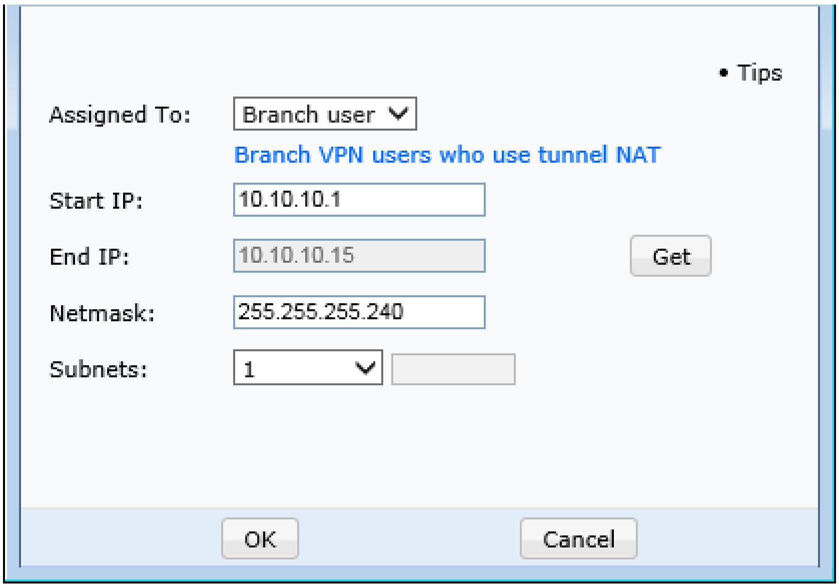
After setting the above information, check [Enable] to activate this connection. Finally, click OK to save the settings.

⚠ **1. As for setting LAN services for network points enabling NAT functions within tunnels, if the LAN permissions are set at the headquarters, the source IP is the segment before NAT; If the LAN permissions are set in the branches, the source IP would be the segment after NAT.**

2.Once VPN's LAN permissions established, not only VPN peer's access to the local would be affected, but also the local's access to VPN peer affected by the LAN permissions. Since IP and ports of the packets are subject to the LAN permissions, the packets in line with rules conditions would face the same restrictions, regardless of whether the VPN peer initiates a packet or the local initiates a packet while the VPN peer responds accordingly.

2.5.5. Virtual IP Pool

It's used to create a branch virtual IP pool. In the branch virtual IP pool, the virtual IP segment for the branch's access to the headquarters would replace the original segment at the branch to a segment in the virtual IP pool, solving the LAN IP conflicts when two branches for the same segment access the headquarters. While setting, firstly set the start IP, mask of virtual IP, and the number of segments for branches, then click "Calculate" to auto calculate the qualified end IP. The page is shown as follows:



Assigned To: Branch user

Branch VPN users who use tunnel NAT

Start IP: 10.10.10.1

End IP: 10.10.10.15

Netmask: 255.255.255.240

Subnets: 1

『Start IP』 : The first IP address of the branch virtual IP segment.

『End IP』 : The last IP address of the branch virtual IP segment.

『Get』 : Auto calculate the last IP address of the virtual IP segment.

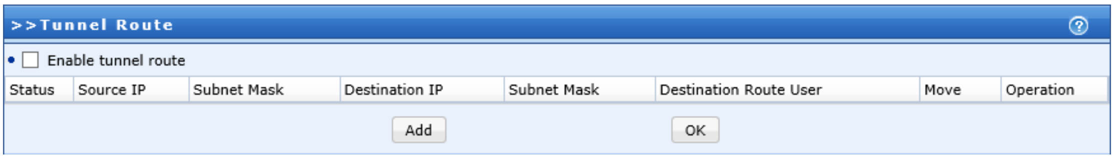
『Netmask』 : The number of virtual IP segments needed.

『Subnets』 : The subnet mask of the virtual IP segment. It shall be consistent with the subnet mask at the branch.

After setting the branch virtual IP segment, create a new user in『VPN Information Settings』→『User Management』, select 『Branch』 for user type, and then configure the branch segments to be switched in 『Advance』 → 『NAT Settings in Tunnels』 .

2.5.6. Inter-tunnel Route Setting

The MIG hardware gateway provides a powerful VPN inter-tunnel routing function, which can easily achieve the interconnection between multiple VPNs (software/hardware), the real "mesh" VPN network.

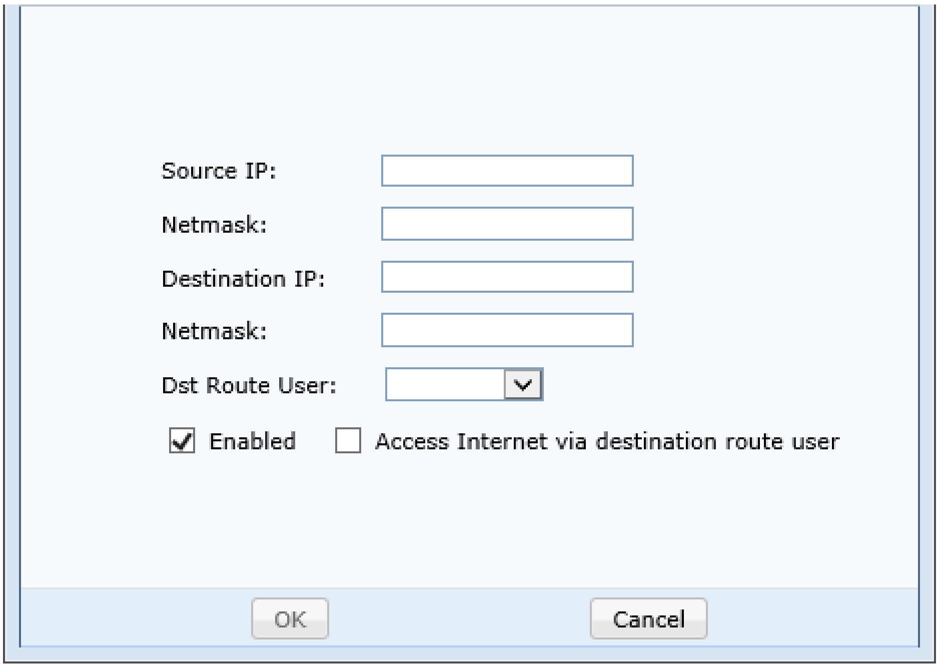


>>Tunnel Route

□ Enable tunnel route

Status	Source IP	Subnet Mask	Destination IP	Subnet Mask	Destination Route User	Move	Operation

Click Add to add an inter-tunnel routing as shown below:



Source IP:

Netmask:

Destination IP:

Netmask:

Dst Route User:

☑ Enabled □ Access Internet via destination route user

『Source IP』: Used to set the source IP address for inter-tunnel routing.

『Subnet Mask (Source)』: Used to set the source subnet segment for inter-tunnel routing.

『Destination IP』: Used to set the destination IP address for inter-tunnel routing.

『Subnet Mask (Destination)』: Used to set the destination subnet segment for inter-tunnel routing.

『Destination Route User』: Used to select the destination users for inter-tunnel routing items (for example, a VPN connection is established between A and B, and User A uses this connection. Now A wants to visit C via B, then for Device A, the destination routing user would be "A").

Check [Enable] to enable this inter-tunnel routing.

By checking [Online via Destination Route User], the Internet traffics through this device would be sent to the destination routing user by the inter-tunnel routing, which would forward the traffics to the Internet.

⚠ 1. In the case of enabling [Online via Destination Route User], the device at the VPN remote access end must be deployed as gateway mode, and the local device can be in gateway or one-arm mode.

2. Before creating a new inter-tunnel routing, confirm that a user is created via 『VPN Information Settings』-> 『User Management』or the connection management is configured in the Connection Management, otherwise no inter-tunnel routing is created.

3. The destination routing users include the user not enabling multi-user login in user management and the user configured in connection management (excluding the users of the same names or disabled users).

Check [Enable Routing] to enable the inter-tunnel routing.

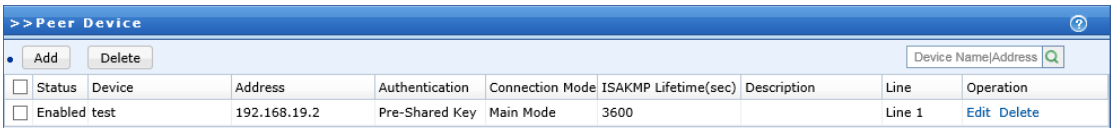
2.5.7. Third-party Connection

The MIG hardware devices provide the interconnection with the third-party MIG devices and can establish standard IPSec VPN connection with the third-party MIG devices.

Third-party connection requires SANGFOR devices to be authorized by the branchs to work normally, and one third-party VPN connection takes up one branch authorization.

2.5.7.1. Phase 1

『Phase 1』 is used to set the peer MIG devices in need of establishing standard IPSec connection with MIG hardware gateway. This is the first phase of the standard IPSec protocol negotiation. The page is shown as follows:

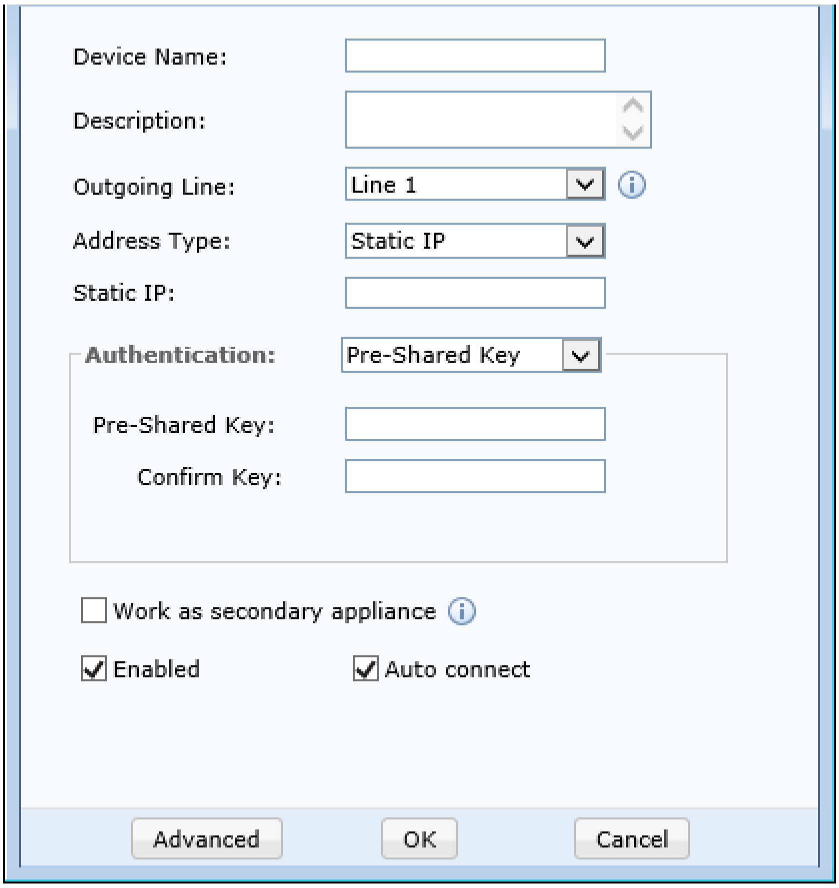


□	Status	Device	Address	Authentication	Connection Mode	ISAKMP Lifetime(sec)	Description	Line	Operation
□	Enabled	test	192.168.19.2	Pre-Shared Key	Main Mode	3600		Line 1	Edit Delete

When a device in the device list has been used in inbound and outbound policies, the device cannot be deleted or renamed.

The device name and device address can be searched in the input box i n the upper right corner.

Click Add to pop up a page as follows:



Device Name:

Description:

Outgoing Line: Line 1

Address Type: Static IP

Static IP:

Authentication: Pre-Shared Key

Pre-Shared Key:

Confirm Key:

□ Work as secondary appliance

☑ Enabled ☑ Auto connect

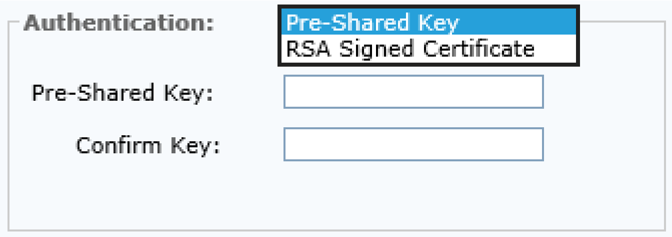
『Device Name』: Customization.

『Description』 : Customization.

『Outgoing Line』: Select the line egress for IPSEC VPN tunnel. It's used to customize different line egress selected in Phase 1, achieving the backup of standard IPSECVPN lines.

『Address Type』: Include three types: the peer can adopt fixed IP, dynamic IP and fixed domain name. Select as the case may be. Select the static IP, then fill in the IP address of the peer; Select the dynamic domain name, then fill in the domain name bound to external network.

『Authentication Method』 includes PSK and RSA-signed certificate. The figure is shown as below:

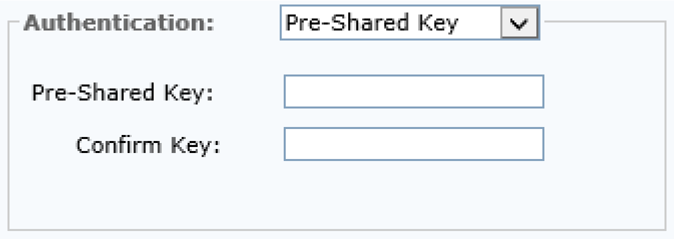


Authentication: Pre-Shared Key
RSA Signed Certificate

Pre-Shared Key:

Confirm Key:

『PSK』 and 『Confirm Key』: Fill in correct PSK and ensure both sides of the connection use the same PSK. The page is shown as follows:

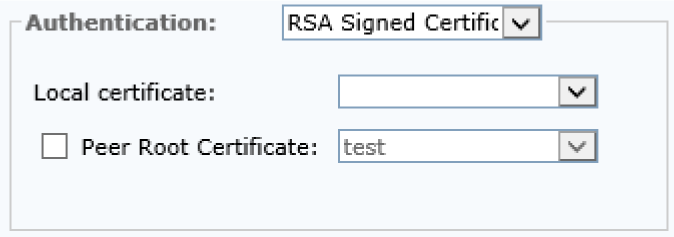


Authentication: Pre-Shared Key

Pre-Shared Key:

Confirm Key:

『RSA-signed Certificate』: Select a correct certificate. When the peer certificate is not issued by the same CA as the local one, check this option and select the peer root certificate. The page is shown as follows:

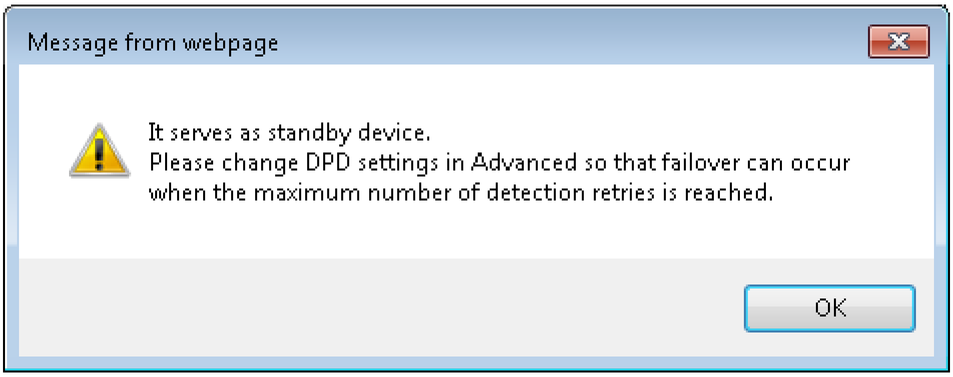


Authentication: RSA Signed Certific

Local certificate:

□ Peer Root Certificate: test

『As Backup Device』: In establishing the active and standby tunnels, when the main tunnel is disconnected, it will be used as a backup tunnel to send data to the peer end for configuring the backup function of standard IPSEC line, marking one of the first phases as backup device. Once enabled, the following tips would appear:



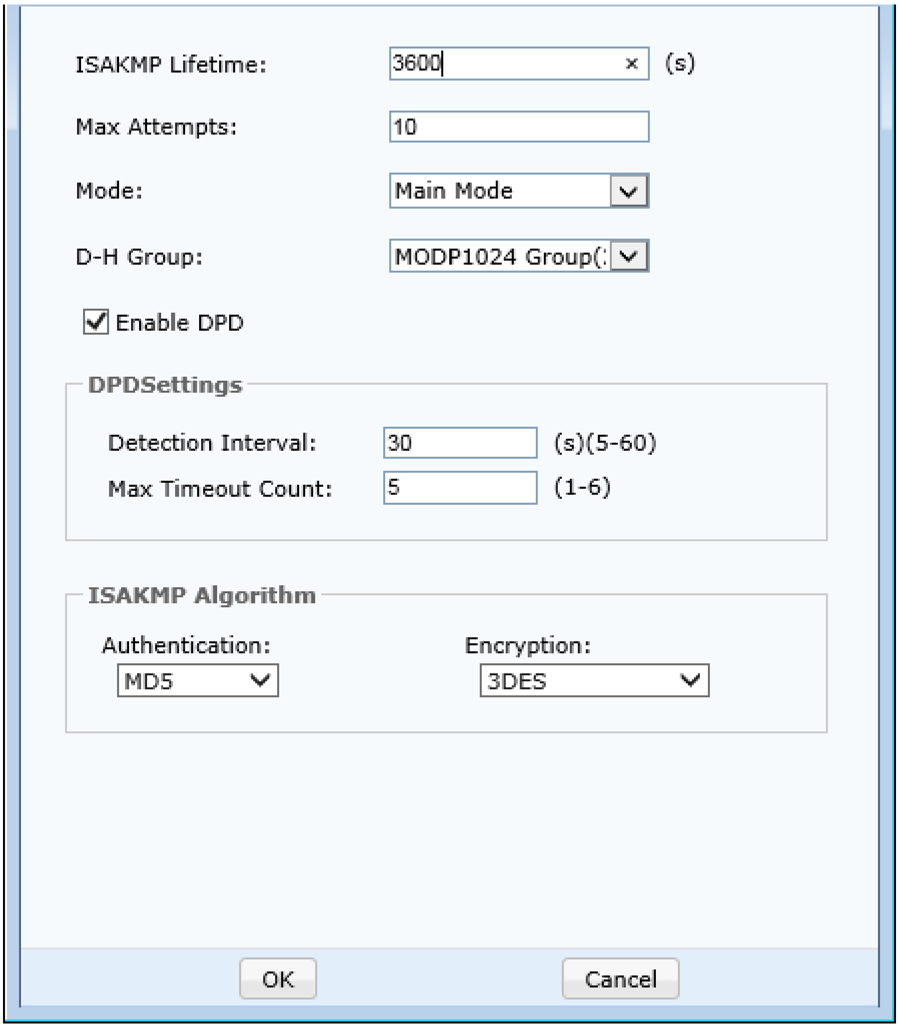
It serves as standby device.
Please change DPD settings in Advanced so that failover can occur when the maximum number of detection retries is reached.

『Enable Device』: Enable Phase 1 settings.

『Enable Active Connection』: This phase is connected to the peer actively.

⚠ **Note: The standard IPSEC does not allow two sides of the connection to adopt dynamic IP, and only allow one of them using dynamic IP.**

Click Advanced to display the dialog box - 【Advanced Options】 for other advanced settings as shown below:



ISAKMP Lifetime: 3600 (s)

Max Attempts: 10

Mode: Main Mode

D-H Group: MODP1024 Group(:

☑ Enable DPD

DPDSettings

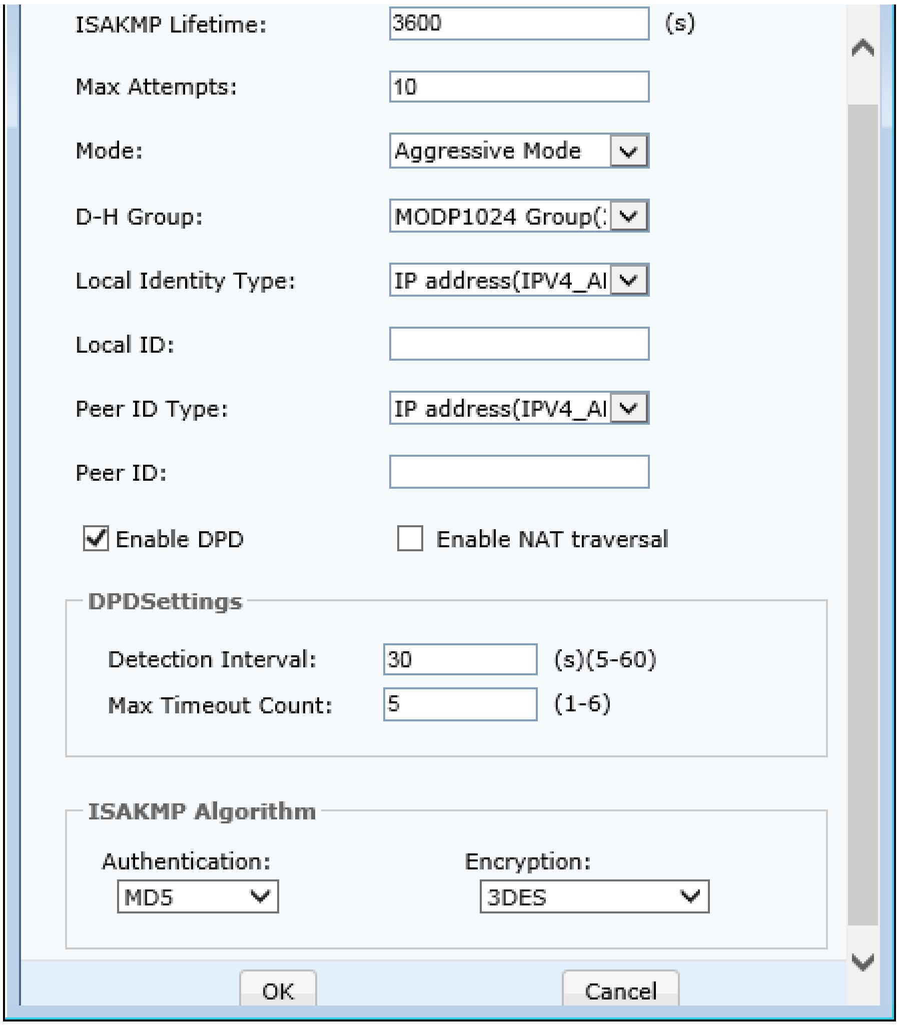
Detection Interval: 30 (s)(5-60)

Max Timeout Count: 5 (1-6)

ISAKMP Algorithm

Authentication: MD5

Encryption: 3DES



ISAKMP Lifetime: 3600 (s)

Max Attempts: 10

Mode: Aggressive Mode

D-H Group: MODP1024 Group(:

Local Identity Type: IP address(IPV4_AI

Local ID:

Peer ID Type: IP address(IPV4_AI

Peer ID:

☑ Enable DPD　　☐ Enable NAT traversal

DPDSettings

Detection Interval: 30 (s)(5-60)

Max Timeout Count: 5 (1-6)

ISAKMP Algorithm

Authentication: MD5

Encryption: 3DES

『ISAKMP Survival Time』: The survival time in the first phase of standard IPSEC negotiation. Only supports timing by second.

『Max Attempts』: When the VPN is disconnected due to breakdown, it is not connected when the number of retries exceed the specified times, no active connection would be initiated, unless there is VPN traffic triggering for initiating the connection again.

『Mode』: Include main mode and aggressive mode. The main mode is applicable to the case where both sides of the connection adopt static IP or one side uses the dynamic domain name, but does not support NAT penetration; The aggressive mode is applicable to the case where one side adopts dials, and support NAT penetration.

『D-H Group』: A cluster-type for Diffie-Hellman key switching, including 8 types such as 1, 2, 5, 14, 15, 16, 17 and 18. Please keep consistent with the configuration of peer device.

『Enable DPD』: IPSEC employs DPD (Dead Peer Detection) to detect whether the Peer is alive or not. "DPD Settings" includes the detection interval and timeout times. After several times of detection timeout, the device would consider the peer invalid and be disconnected.

『ISAKMP Algorithms List』 includes the authentication algorithm and encryption algorithm:

"Authentication Algorithm": Select the data authentication algorithms such as MD5, SHA1, SHA2-256, SHA2-384 and SHA2-512.

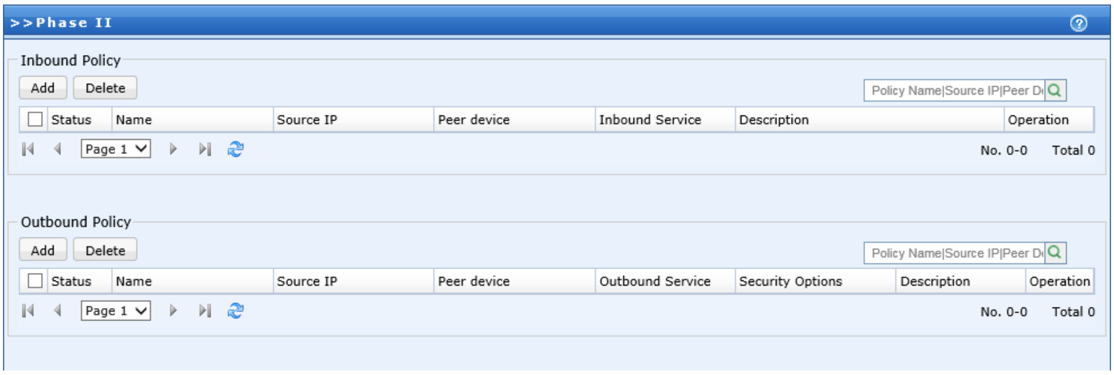
"Encryption Algorithm": Select the data encryption algorithms such as DES, 3DES, AES, AES-192, AES-256 and SANGFOR_DES.

⚠ **SANGFOR_DES algorithm can be employed only when both sides of the connection are SANGFOR devices, and cannot be used when connecting with other manufacturers' devices.**

The identity ID in aggressive mode has three expressions: the IP address (IPV4_ADDR) format, the domain name string (FQDN) format, which can be any URL or a string of strings, and the user string (USER_FQDN) in the format "xxx@xxx.xxx".

2.5.7.2. Phase 2

『Inbound Policy』 is used to set the rules for packets sent from the peer to the local. In case of many policies, they will be displayed in pages automatically. In the top right corner, search the policy name, source IP and the name of peer device; for source IP, a policy of "subnet+mask", search the subnet only, not the mask.



Inbound Policy

□ Status	Name	Source IP	Peer device	Inbound Service	Description	Operation

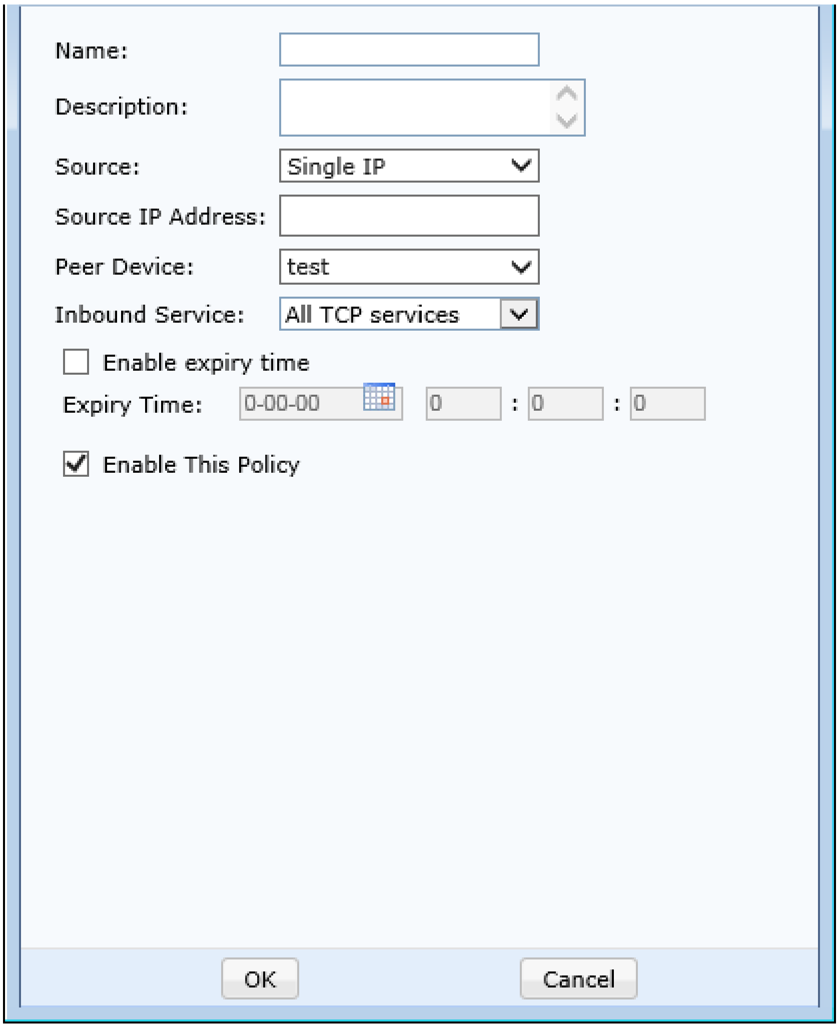
No. 0-0 Total 0

Outbound Policy

□ Status	Name	Source IP	Peer device	Outbound Service	Security Options	Description	Operation

No. 0-0 Total 0

Click Add to pop up the dialog box of policy settings as below:


Name:

Description:

Source: Single IP

Source IP Address:

Peer Device: test

Inbound Service: All TCP services

□ Enable expiry time

Expiry Time: 0-00-00 0 : 0 : 0

☑ Enable This Policy

『Policy Name』 and『Description』 : Customization.

『Source IP Type』: Include a single IP, subnet+mask, Specify the source IP of the peer VPN data to be a single IP or an entire segment, respectively, and fill in the source address of the peer VPN data. Note that you must set one of the first phase to "As Backup Device", then configure two inbound policies for the same source segment, otherwise it will cause conflicts.

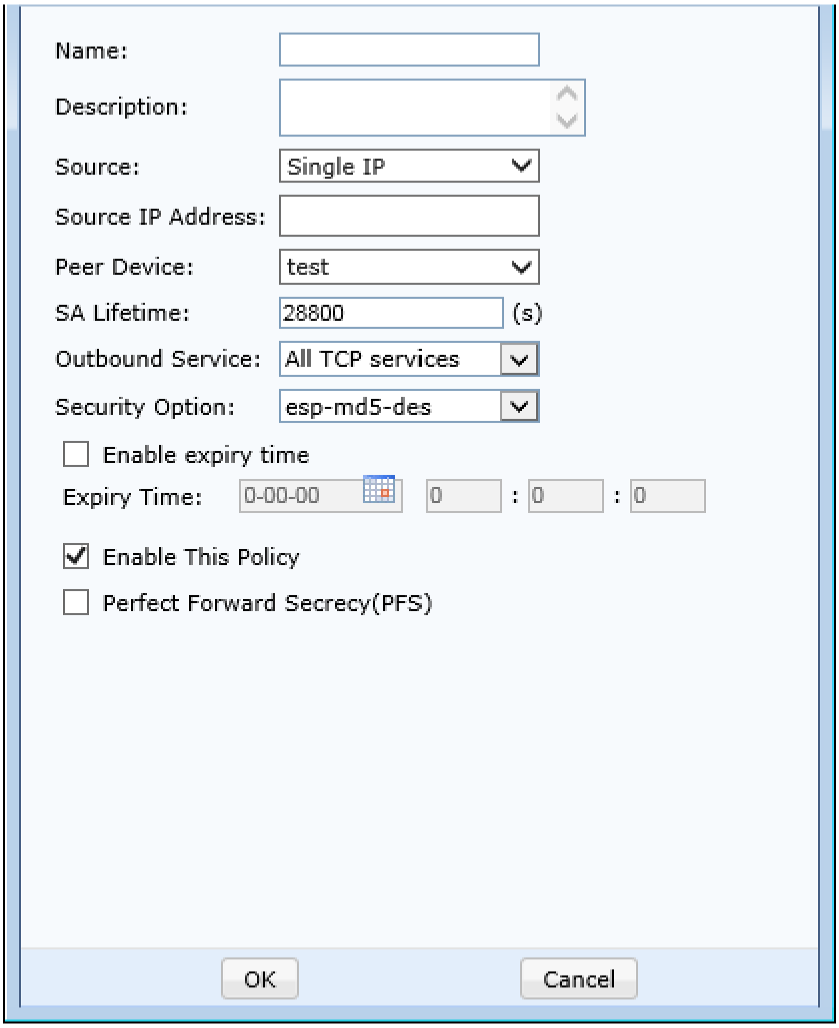
『Peer Device』: The peer device to be associated with this outbound policy.

『Inbound Service』: Define the types of services in the peer allowed to enter the VPN tunnel for transmission to the local LAN.

『Effective Time』 and 『Expiration Time』: Within what time frame, the inbound policy is effective.

『Dynamic Routing Update』: Once enabled, the corresponding policy routing would be added or deleted when connected or disconnected. This is applicable to scenarios where there are other types of backup routes for this policy.

『Outbound Policy』 is used to set the rules for packets sent from the local to the peer. Click Add to pop up the dialog box - 【Policy Settings】 as shown below:



Name:	
Description:	
Source:	Single IP
Source IP Address:	
Peer Device:	test
SA Lifetime:	28800 (s)
Outbound Service:	All TCP services
Security Option:	esp-md5-des

□ Enable expiry time

Expiry Time: 0-00-00 0 : 0 : 0

☑ Enable This Policy

□ Perfect Forward Secrecy(PFS)

『Policy Name』 and 『Description』: Customization.

『Source IP Type』: Include a single IP and subnet+mask. Specify the source IP of the VPN data to be a single IP or an entire segment, respectively, and fill in the source address of VPN data correctly.

『Peer Device』: The peer device to be associated with this outbound policy.

『SA Survival Time』: The survival time in the second phase of standard IPSEC negotiation only supports timing by second.

『Outbound Service』: Define the types of services allowed to enter the VPN tunnel for transmission to the peer LAN.

『Security Options』: The security options to be associated with this outbound policy.

『Effective Time』 and 『Expiration Time』: Within what time frame, the outbound policy is effective.

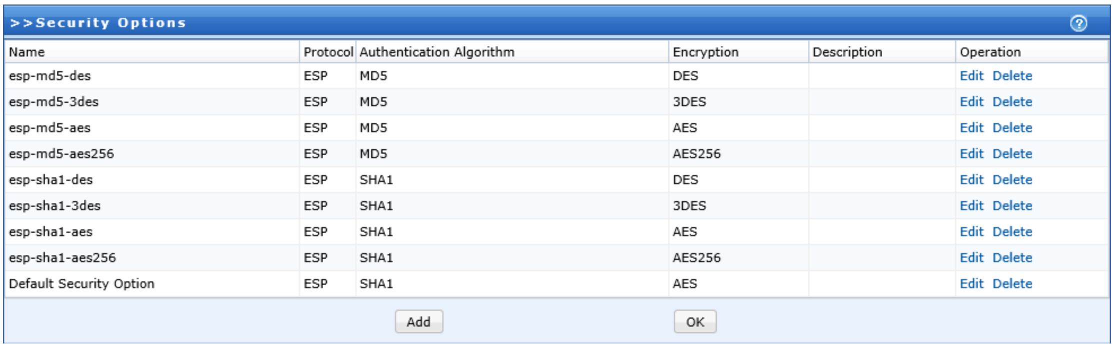
⚠**Note: The 『Effective Time』 module can take effect only when both sides of the connection are SANGFOR devices, and would not be effective when connected to other manufacturers' devices.**

『Enable Key for Perfect Forward Secrecy』: As the case of peer devices may be, if the peer enables PFS, the local needs to check this option, otherwise, there is no need to check it.

⚠**Note: 『Outbound Service』,『Inbound Service』 and 『Time Settings』in 『Outbound Policy』 and 『Inbound Policy』 are extended rules of SANGFOR, and can only take effect at the local devices. In the VPN connection to third-party devices, these rules would be triggered. The source IP addresses corresponding to 『Outbound Policy』 and 『Inbound Policy』 are the source IP intersection set in 『Source IP Type』 and 『Inbound Policy』.**

2.5.7.3. Security Options

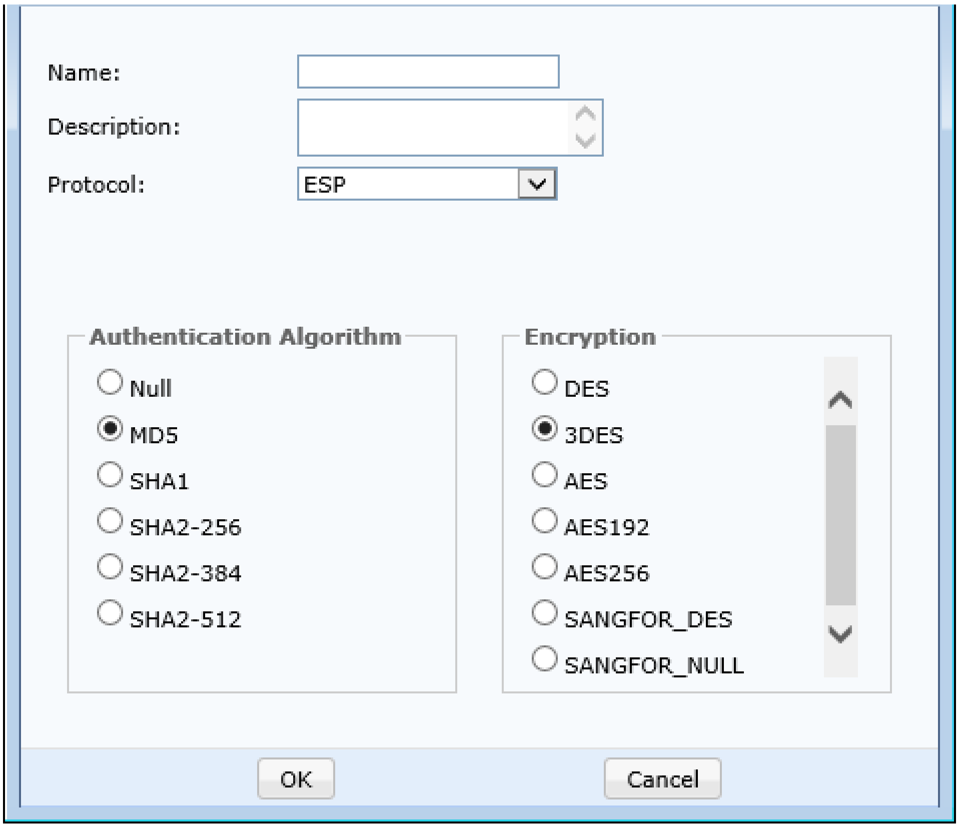
『Security Options』includes the parameters used in establishing standard IPSec connection with the peer. See the page below:



>>Security Options

Name	Protocol	Authentication Algorithm	Encryption	Description	Operation
esp-md5-des	ESP	MD5	DES		Edit Delete
esp-md5-3des	ESP	MD5	3DES		Edit Delete
esp-md5-aes	ESP	MD5	AES		Edit Delete
esp-md5-aes256	ESP	MD5	AES256		Edit Delete
esp-sha1-des	ESP	SHA1	DES		Edit Delete
esp-sha1-3des	ESP	SHA1	3DES		Edit Delete
esp-sha1-aes	ESP	SHA1	AES		Edit Delete
esp-sha1-aes256	ESP	SHA1	AES256		Edit Delete
Default Security Option	ESP	SHA1	AES		Edit Delete

Before establishing IPSec connection with third-party devices, please confirm which connection policies are used by the peer devices, including the use of『Protocol』(AH orESP), 『Authentication Algorithm』(MD5 or SHA1, SHA2-256, etc.), 『Encryption Algorithm』(DES, 3DES, AES, AES192, etc.). Click Add to add new options as follows:



Name:

Description:

Protocol: ESP

Authentication Algorithm

○ Null
● MD5
○ SHA1
○ SHA2-256
○ SHA2-384
○ SHA2-512

Encryption

○ DES
● 3DES
○ AES
○ AES192
○ AES256
○ SANGFOR_DES
○ SANGFOR_NULL

The MIG hardware devices would establish IPSec connection with the peer by using the set connection policy.

『Encryption Algorithm』in 『Security Options』is used to set the data encryption algorithm used in the second phase of standard IPSec connection. If you want to interconnect with multiple devices with different connection policies, add the connection policies used by each device to『Security Options』.

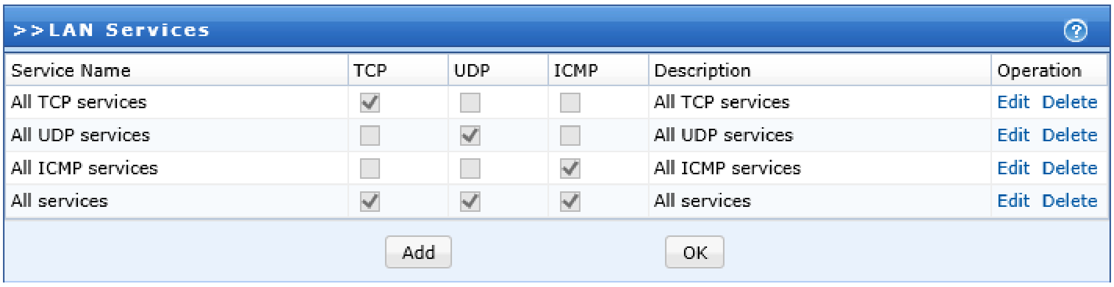
2.5.8. Advanced Settings

It includes 『LAN Services Settings』, 『VPN Interface Settings』 and 『Multicast Service Settings』.

2.5.8.1. LAN Services Settings

SANGFOR hardware devices can specific corresponding access permissions for accessed VPN users, allow a certain IP in a certain branch user LAN, a branch user to only access specific services of a specific computer in LAN, and set the service parameters of inbound and outbound policies when connected to a third-party device.

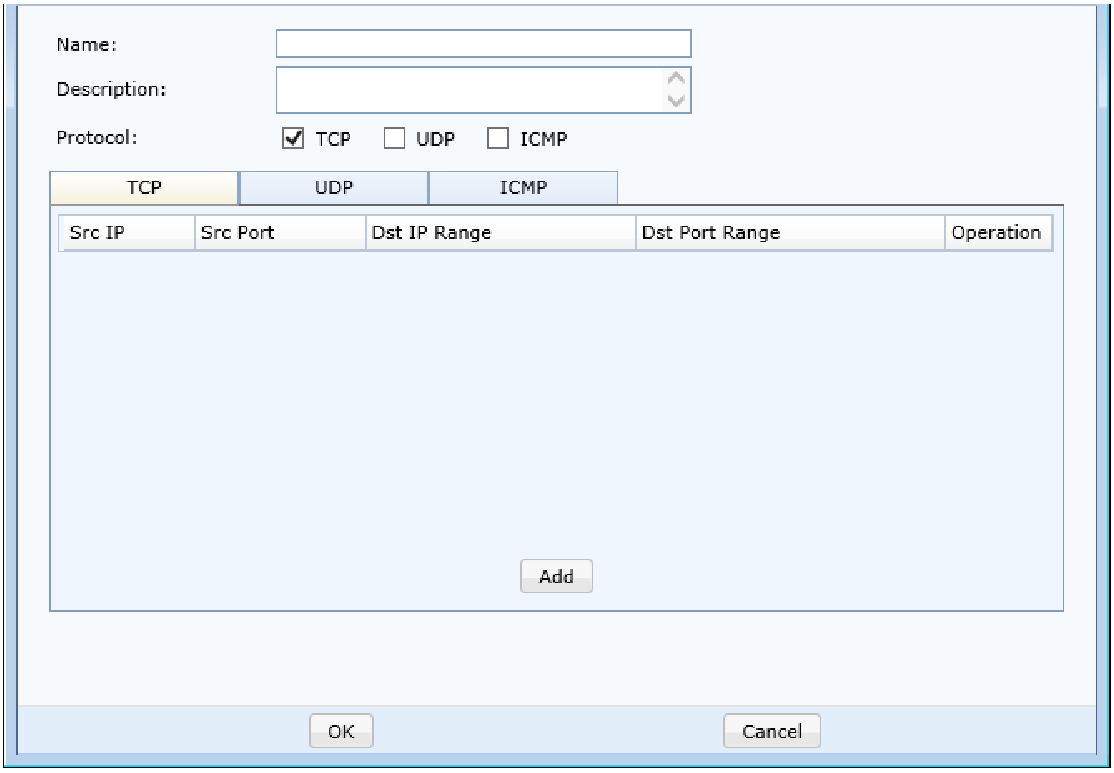
For example: only the user "test" is allowed to access the WEB services of WEB servers at the headquarters, and the requests for the access to other services of the WEB servers are rejected; Only one IP in the LAN of branch user "test" is allowed to access the SQL server at the headquarters, and other IPs in the branch LAN would be prohibited to access it. Security management in VPN tunnel can be realized by authorizing service access through appropriate permission settings. The page is shown as follows:



>>LAN Services

Service Name	TCP	UDP	ICMP	Description	Operation
All TCP services	☑	□	□	All TCP services	Edit Delete
All UDP services	□	☑	□	All UDP services	Edit Delete
All ICMP services	□	□	☑	All ICMP services	Edit Delete
All services	☑	☑	☑	All services	Edit Delete

Click Add to manually add LAN services according to the protocol types, as shown below:



Name:

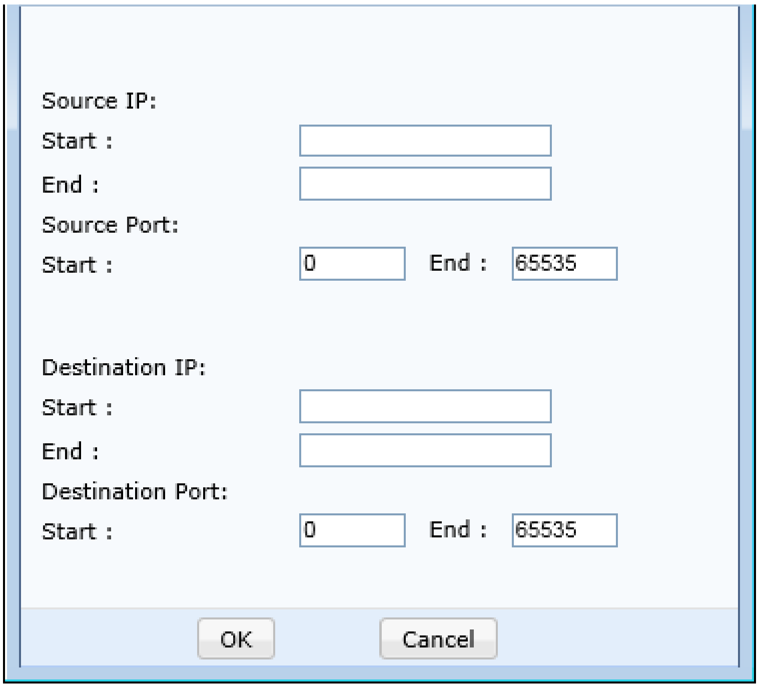
Description:

Protocol: ☑ TCP □ UDP □ ICMP

『Service Name』 and 『Description』 can be customized for easy management.

『Protocol』 is used to select the protocols used by LAN services to be defined.

Select [TCP List] or [UDP List], and set the source IP, source port, target IP and target ports. Click Add as shown below:



Source IP:

Start :

End :

Source Port:

Start : 0 End : 65535

Destination IP:

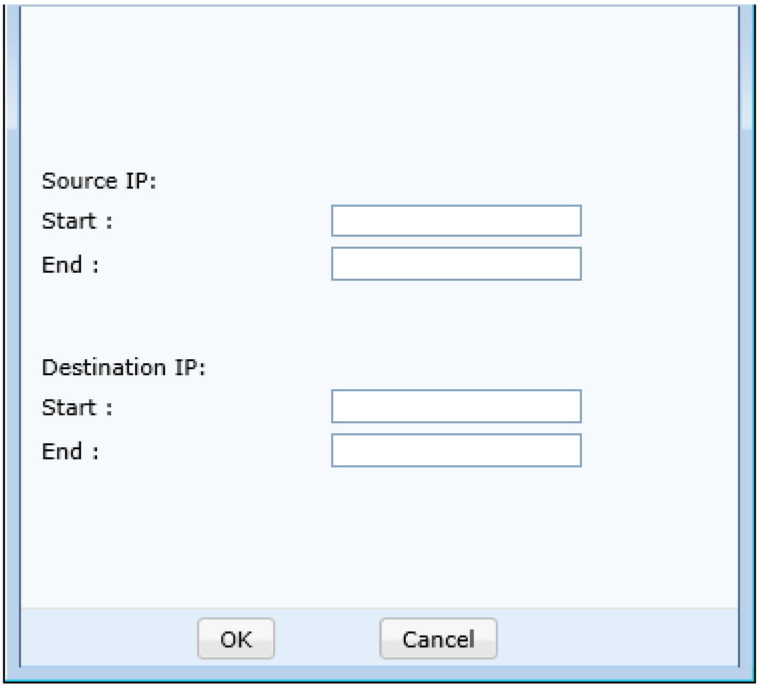
Start :

End :

Destination Port:

Start : 0 End : 65535

Select [ICMP Protocol] and set the source IP range and target IP range as shown below:



Source IP:

Start :

End :

Destination IP:

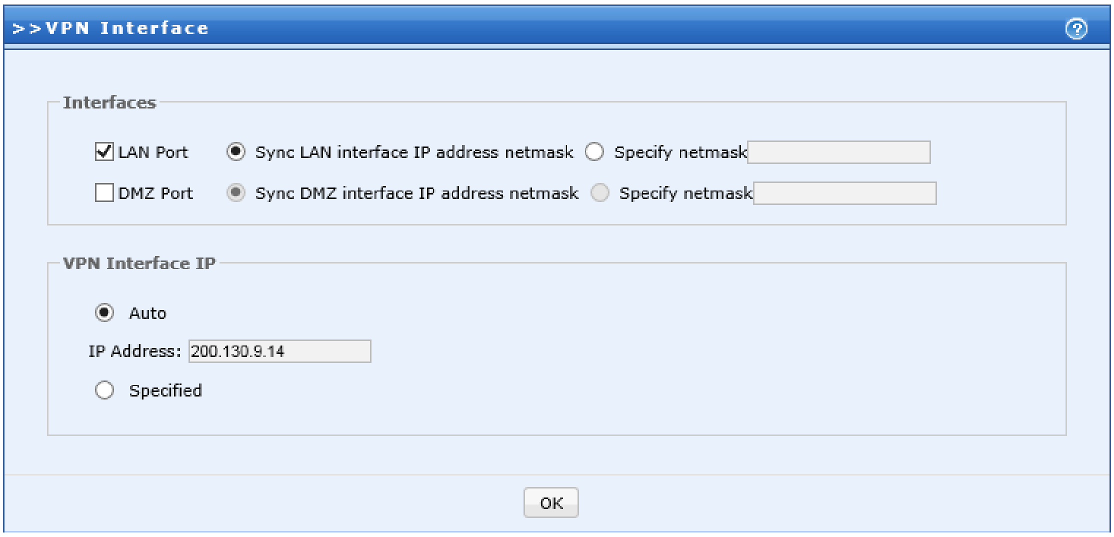
Start :

End :

After setting the configuration, click "OK" to save the configuration.

2.5.8.2. VPN Interface Settings

It's used to set the subnet mask of VPN segment, that's to say, the IP address within the mask range is considered as the VPN data, and the IP address at other segments is non-VPN data. The page is shown as follows:



>>VPN Interface

Interfaces

☑ LAN Port ● Sync LAN interface IP address netmask ○ Specify netmask

□ DMZ Port ● Sync DMZ interface IP address netmask ○ Specify netmask

VPN Interface IP

● Auto

IP Address: 200.130.9.14

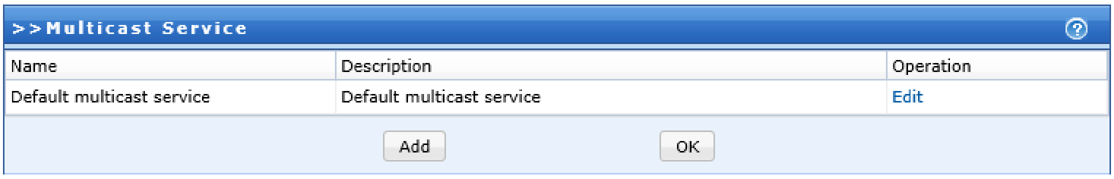
○ Specified

"VPN LAN Settings" include the VPN LAN subnet mask settings for LAN interface and DMZ interface. "Auto Sync Mask" is a subnet mask directly using LAN interface or DMZ interface, and "Custom Mask" is a subnet mask with VPN interfaces filled in manually.

"Local VPN Interface" is used to set the IP address of VPN interface for local devices, which can be automatically assigned or manually defined.

2.5.8.3. Multicast Services Settings

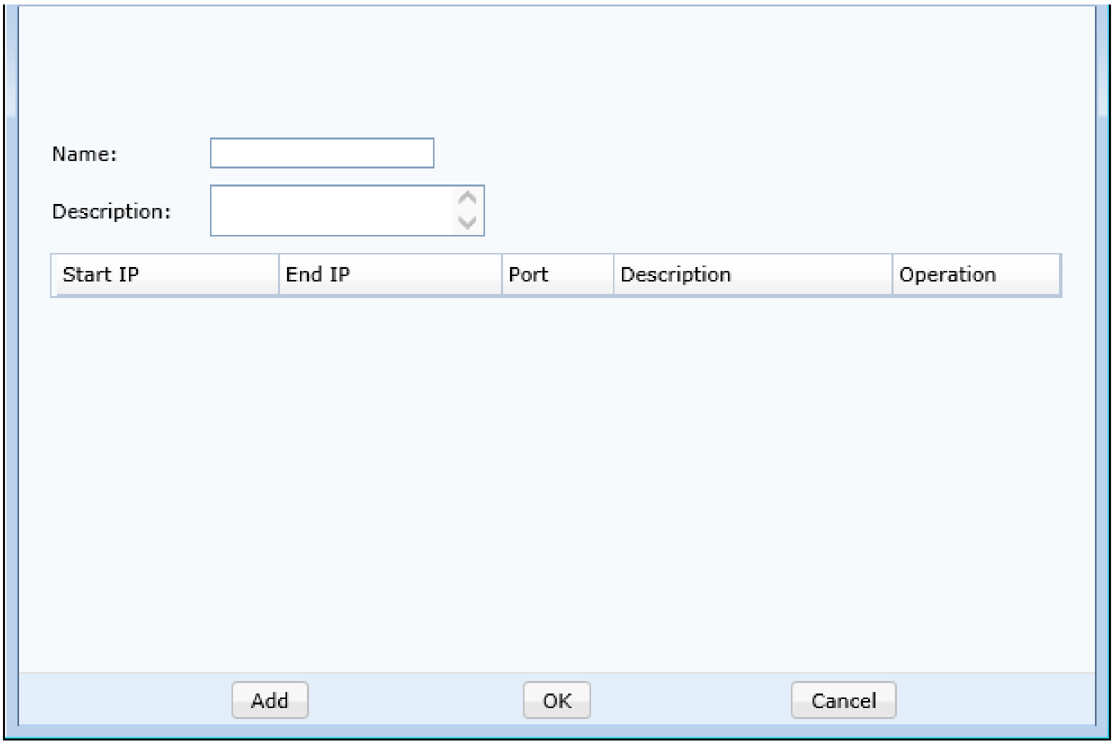
To meet VOIP and video meetings, the MIG hardware gateway supports the inter-tunnel transmission of multicast services. Here you can define the multicast services, with IP range of 224.0.0.1-239.255.255.255 and port range being 1-65535. The page is shown as follows:



>>Multicast Service

Name	Description	Operation
Default multicast service	Default multicast service	Edit

Click Add to pop up a page for editing multicast services. Here you can set the multicast address and port for multicast services. The page is shown as follows:

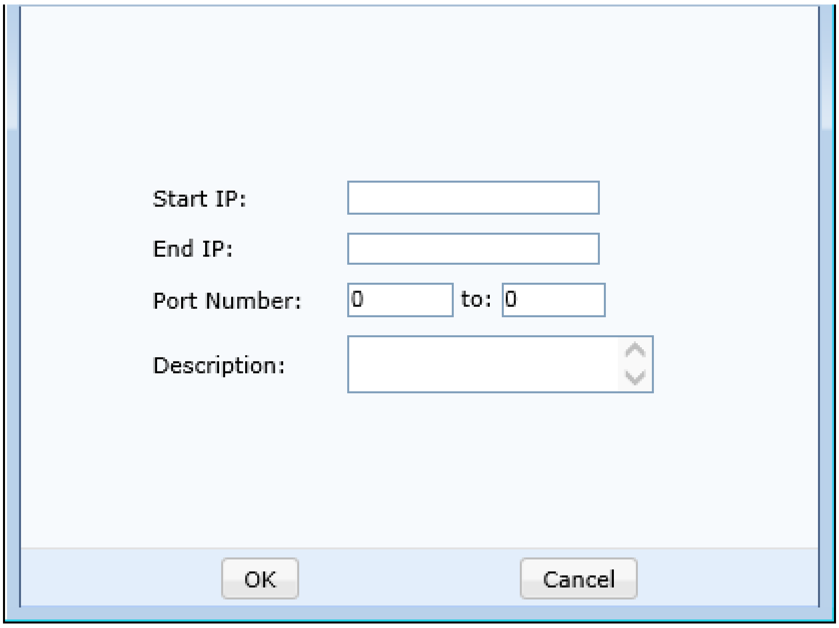


Name:

Description:

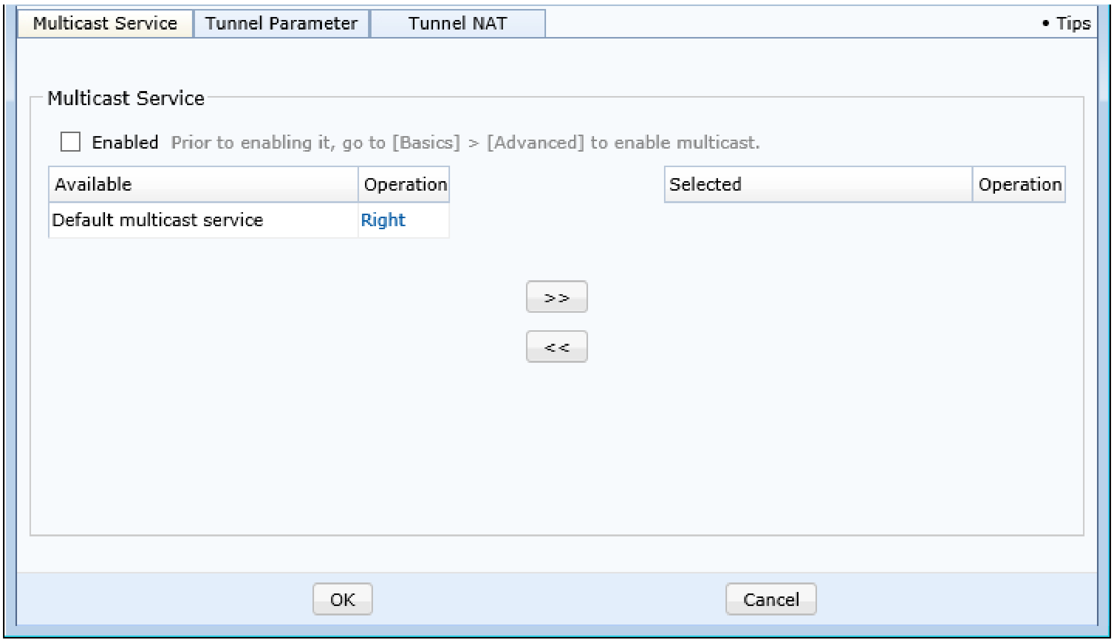
Start IP	End IP	Port	Description	Operation

Define『Name』and『Description』. Click Add and set the multicast address and port for multicast services.



Start IP:	
End IP:	
Port Number:	0 to: 0
Description:	

After defining the multicast services, create a new user in 『VPN Information Settings』 → 『User Management』, and then configure the multicast services in 『Advanced』 → 『Multicast Services Settings』. The page is shown as follows:



Multicast Service

□ Enabled Prior to enabling it, go to [Basics] > [Advanced] to enable multicast.

Available	Operation
Default multicast service	Right

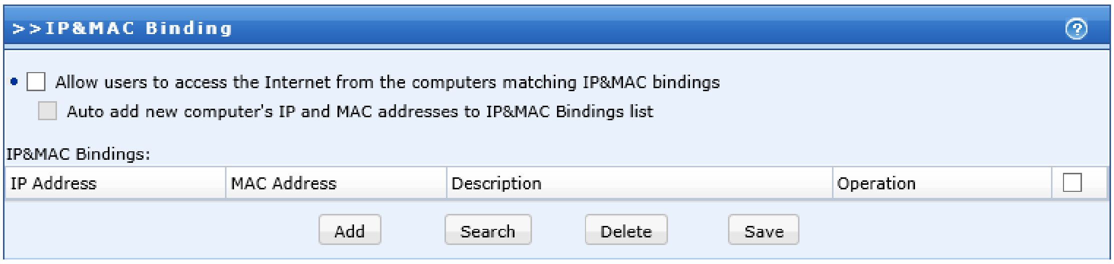
Selected	Operation

2.6. Access Control

It includes 『IPMAC Authentication Settings』, 『Authentication Options Settings』 and 『Access Policy Settings』. Note that this function is only for normal Internet traffic, but not for VPN traffic.

2.6.1. IPMAC Authentication Settings

『IPMAC Authentication Settings』 is mainly used to set MIG hardware gateway configuration information related to user authentication. The configuration interface is shown as follows:



>>IP&MAC Binding

- □ Allow users to access the Internet from the computers matching IP&MAC bindings
  □ Auto add new computer's IP and MAC addresses to IP&MAC Bindings list

IP&MAC Bindings:

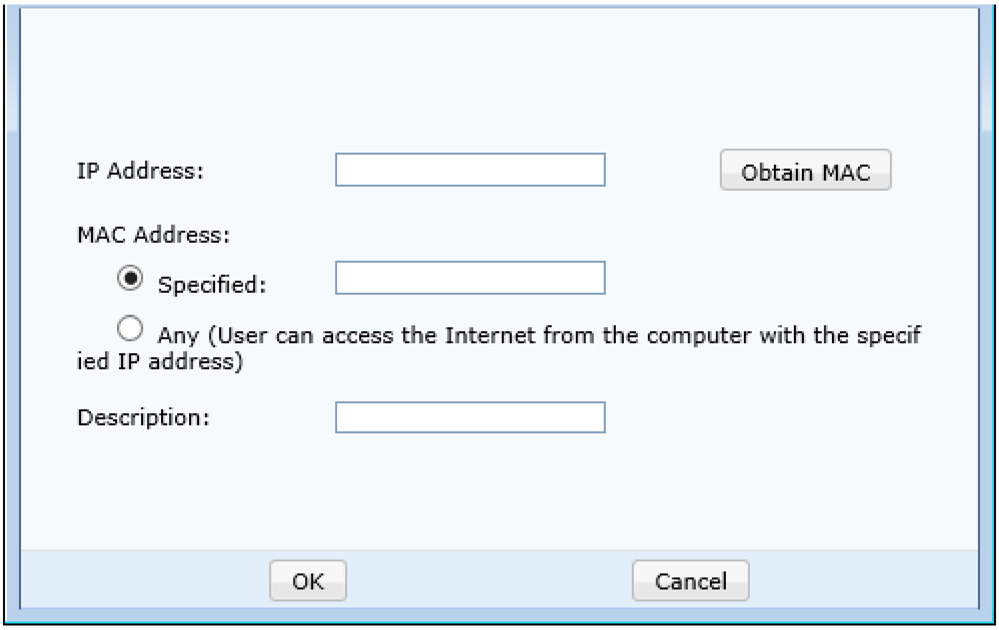
IP Address	MAC Address	Description	Operation	□

Here you can enable 『Only Allow the Computers in Authorization List to Access the Internet』 and 『Auto Add New Computers to the Authorization List』.

By checking『Only Allow the Computers in Authorization List to Access the Internet』, the computers in the authorization list and passing the IP or MAC binding authentication can access the Internet, and those not in the list or without matched IP/MAC binding are not allowed to access the Internet.

By checking『Auto Add New Computers to the Authorization List』, the new computers would auto enter the authorization list.

[Specify MAC Address]: Click Add and fill in IP and MAC information for binding IP/MAC address. Or only enter IP address, then click Auto Acquire to acquire the MAC address of corresponding computers. The configuration interface is shown as follows:



IP Address:

MAC Address:

● Specified:

○ Any (User can access the Internet from the computer with the specified IP address)

Description:

『Not Specify MAC Address』: It means that once binding an IP, any computer configured with this IP would match this authorization rule.

By clicking "Acquire MAC" and setting the search range, the system will automatically search the IP/MAC of the computers within the set IP address range.

Click Delete to delete the authorization rules selected.

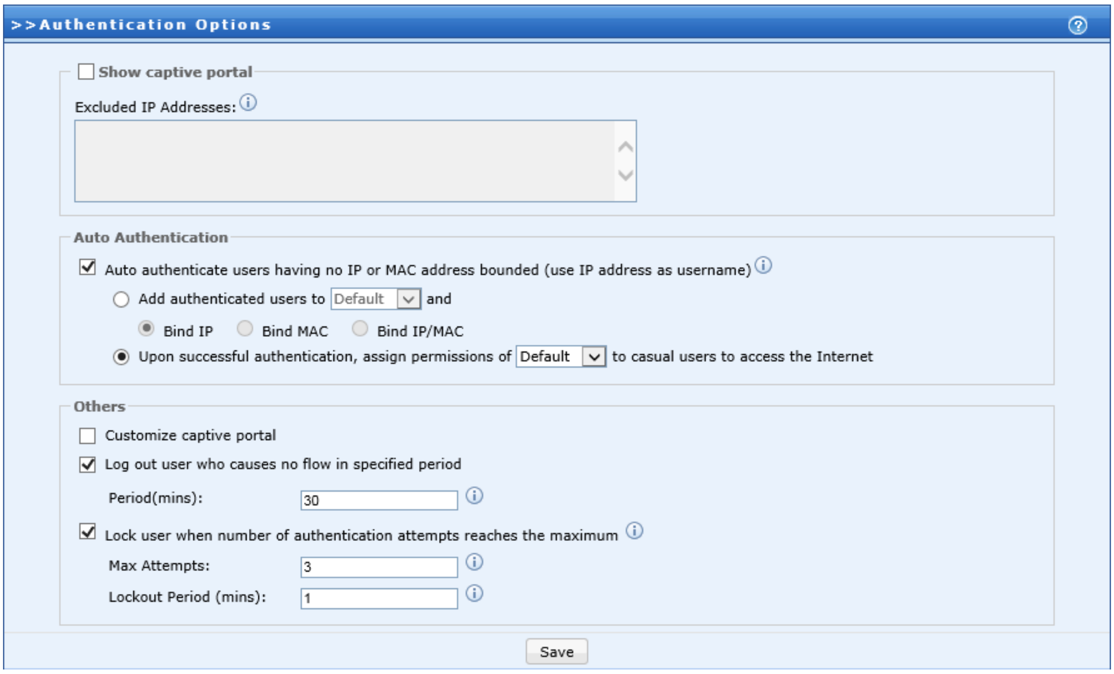
Click OK to save the settings.

⚠The IP/MAC binding refers to the binding of the MAC addresses of three-layer devices using computer IP in case of three-layer environment in the LAN. Because our device supports multiple IPs corresponding to a MAC, but not multiple MACs to one IP.

⚠With automatic search, we can only obtain the IP in local area network where the machine is located and corresponding MAC address. Meanwhile, the MAC addresses corresponding to existing IPs would be updated. No more addresses will be added when there are more than 100 addresses. This function can only be used at Layer 2.

2.6.2. Authentication Options Settings

『Authentication Options Settings』 is mainly used to set the Internet authentication test for LAN users, authentication IP range, automatic authentication settings, and other options. The figure is shown as below:



>>Authentication Options

□ Show captive portal

Excluded IP Addresses:

Auto Authentication

☑ Auto authenticate users having no IP or MAC address bounded (use IP address as username)

○ Add authenticated users to Default and

● Bind IP ○ Bind MAC ○ Bind IP/MAC

● Upon successful authentication, assign permissions of Default to casual users to access the Internet

Others

□ Customize captive portal

☑ Log out user who causes no flow in specified period

Period(mins): 30

☑ Lock user when number of authentication attempts reaches the maximum

Max Attempts: 3

Lockout Period (mins): 1

『Enable Authentication Box』 Enable this authentication.

『IP Excluding List』 The IP in the IP Excluding List will no longer be subject to the authentication policy.

『Automatic Authentication』 Automatically bind the user's IP/MAC and display the user by IP. After the authentication, add them to corresponding groups and use the corresponding group policies. There are three auto binding ways: ①Bind IP; ②Bind mac; ③Bind IP and MAC. There are two [Binding Methods]: one-way binding and two-way binding.

One-way binding: The user can only use specified address for authentication, but other users can also use this address for authentication.

Two-way binding: The user can only use specified address for authentication, and this address can only be used by this user.

『Custom Authentication Page』 supports users to customize the page, but the file must be zip file.

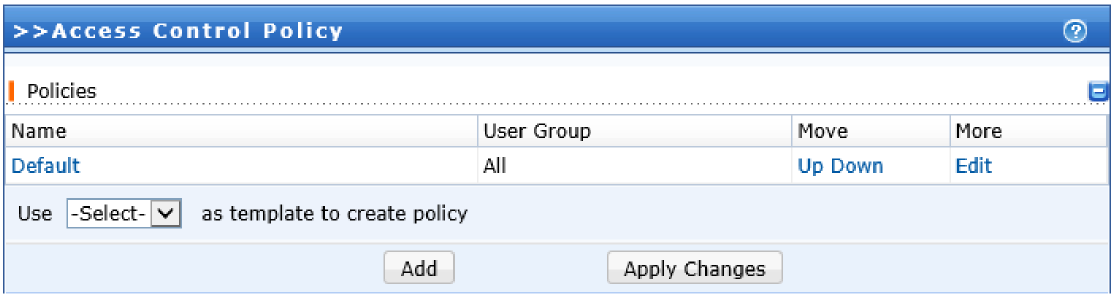
『Automatic Logout of Non-traffic Users』: If the user produces no traffic in LAN within set time, it will be written off.

『Suspend Users with Failed Attempts Exceeding the Maximum Value』: In case of failed authentication attempts exceeding the limit, the user will be suspended.

2.6.3. Access Policy Settings

『Access Policy Settings』 is mainly used to set the network policies for LAN users, which include『APP Services Control』,『Network Services Control』 and『URL Control』.

The policy objects set here can be used to control the Internet access behaviors of multiple user groups. The configuration interface is shown as follows:



>>Access Control Policy

Policies

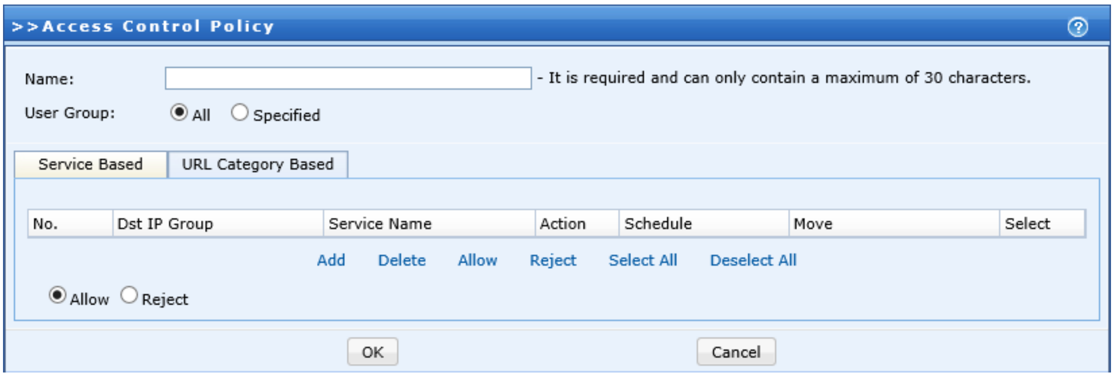
Name	User Group	Move	More
Default	All	Up Down	Edit

Use -Select- as template to create policy

『Access Policy List』 is used to display the policy objects having been set. It will display『Policy Name』,『User Group』,『Adjustment』and『Operation』, and will be matched from top to bottom.

By clicking Apply Changes in『Access Policy Settings』, all policies will take effect.

Click Add in 『Access Policy Settings』, and enter the policy editing page as shown below:



>>Access Control Policy

Name: - It is required and can only contain a maximum of 30 characters.

User Group: ● All ○ Specified

No.	Dst IP Group	Service Name	Action	Schedule	Move	Select

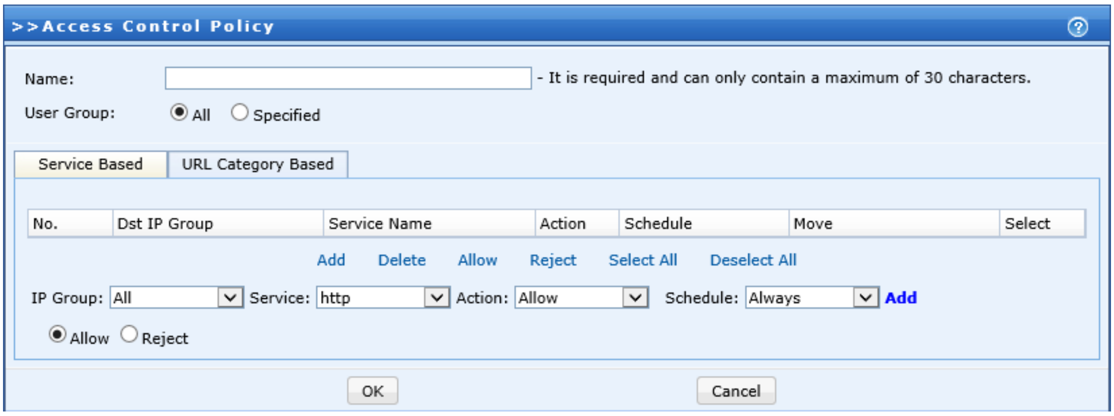
● Allow ○ Reject

『Policy Name』 can be texts easy to understand. It's recommended to use the text easy to identify.

『Applicable User Group』 Select "All" or "Custom". Select the user group having been defined.

『Network Services Control』: To help the network administrators restrict the Internet access behavior of LAN users, MIG hardware gateway provides the destination IP address, protocol ports and time segment to control network services.

Click Add to pop up a page as follows:



Select 『Destination IP Group』, 『Service』, 『Action』 and 『Effective Time』, then click Add to complete the settings of an 『Network Services Control』 rule. For example, if you want to restrict the LAN user from browsing the web pages during working hours, just reject the HTTP service (regarding the definition of the target IP group, service, and time, please refer to the relevant chapters of the previous 『Object Settings』).

Select quickly the Internet access permissions to be edited with the combination of Check All and Inverse.

Click Allow, Reject or Delete to allow, reject or delete the selected Internet access permissions.

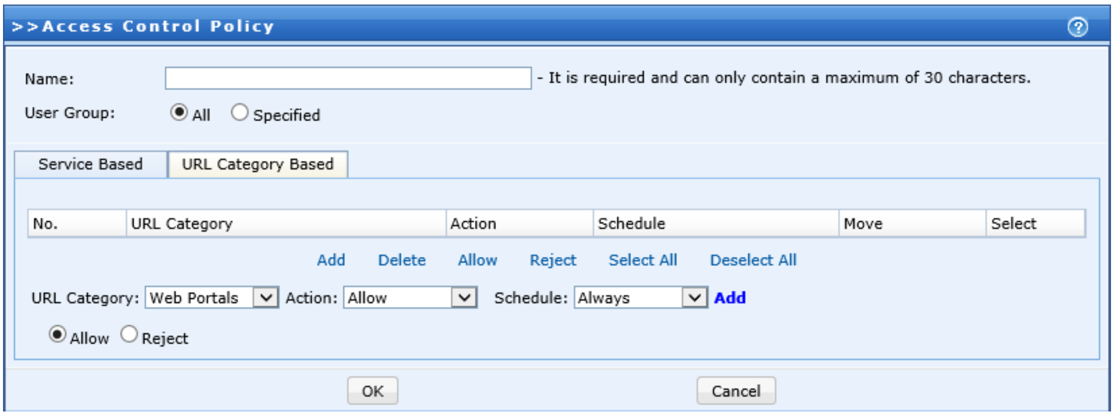
Click Up and Down to move the order of the selected Internet access permissions.

『Allow by Default』 and 『Reject by Default』 are used with the Internet access permissions rules defined in the above list. If it cannot match the rules in the above list, the default actions here would be executed.

Finally, click OK to save the settings.

『URL Control』 is used to control the access to web pages by LAN users.

Click the Add button, select 『URL Group Name』, 『Action』 and 『Effective Time』, then click Add, and the setting of a "URL Control" rule is completed. For example, if you want to restrict the LAN user from browsing online video websites such as Youku in working hours, you can select the video website in the 『URL Group Name』, select Reject in the action, and select Working Hours in the Effective Time. as follows:


>>Access Control Policy

Name: - It is required and can only contain a maximum of 30 characters.

User Group: ● All ○ Specified

No.	URL Category	Action	Schedule	Move	Select

URL Category: Web Portals Action: Allow Schedule: Always

● Allow ○ Reject

Select quickly the Internet access permissions to be edited with the combination of Check All and Inverse.

Click Allow, Reject or Delete to allow, reject or delete the selected Internet access permissions.

Click Up and Down to move the order of the selected Internet access permissions.

The 『Allow by Default』 and 『Reject by Default』options represent the actions to be performed when the URL rules set above cannot be matched.

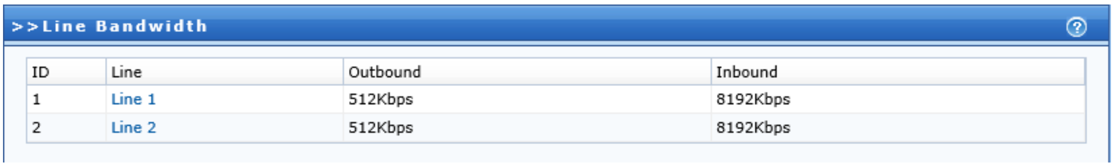
Finally, click OK to save the settings.

2.7. Traffic Management

The MIG6.2.1 volume management system provides powerful bandwidth guarantee and bandwidth limitation functions, which can not only ensure the access to bandwidth of important applications, but also limit the total uplink and downlink bandwidth, and can also establish bandwidth guarantee and bandwidth limitation policy against the service types, user groups, and single users. .

2.7.1. Line Bandwidth Configuration

The actual uplink and downlink bandwidth used to configure the device's external network line is the basis for bandwidth guarantee and bandwidth limitation. The configuration interface is shown as follows:



>>Line Bandwidth

ID	Line	Outbound	Inbound
1	Line 1	512Kbps	8192Kbps
2	Line 2	512Kbps	8192Kbps

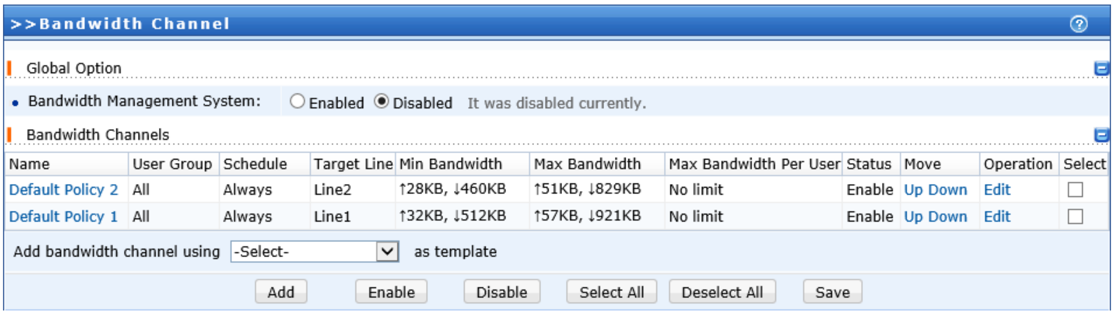
『Line Bandwidth』: used to set the actual uplink and downlink bandwidth of the device's external network line.

『Line type』: Two line types are available, Ethernet and ADSL. After setting the line type to ADSL, the bandwidth set in the traffic control policy will automatically be multiplied by 90%. For example, if the bandwidth limitation set in the traffic control policy is 30%, after the ADSL is set, the actual bandwidth limitation will be 27% (The displayed percentage does not change, but the corresponding actual value will become "Bandwidth*90%*30%").

The improper configuration of line bandwidth may result in the waste of bandwidth (if the setting is small) or line congestion (if the setting is large).

2.7.2. Traffic Policy Settings

The bandwidth allocation function provided by the MIG hardware gateway is used to guarantee and limit the bandwidth of the Internet. The application service, the applicable object, and the effective time can be used as the basis for selecting the bandwidth allocation policy and defining the traffic channel to achieve bandwidth guarantee or bandwidth limitation. In the traffic control policy list, the matching order can be set from top to bottom, and can be adjusted by the Up or Down operation. The configuration interface is shown as follows:



\>>Bandwidth Channel

Global Option

- Bandwidth Management System: ○ Enabled ● Disabled It was disabled currently.

Bandwidth Channels

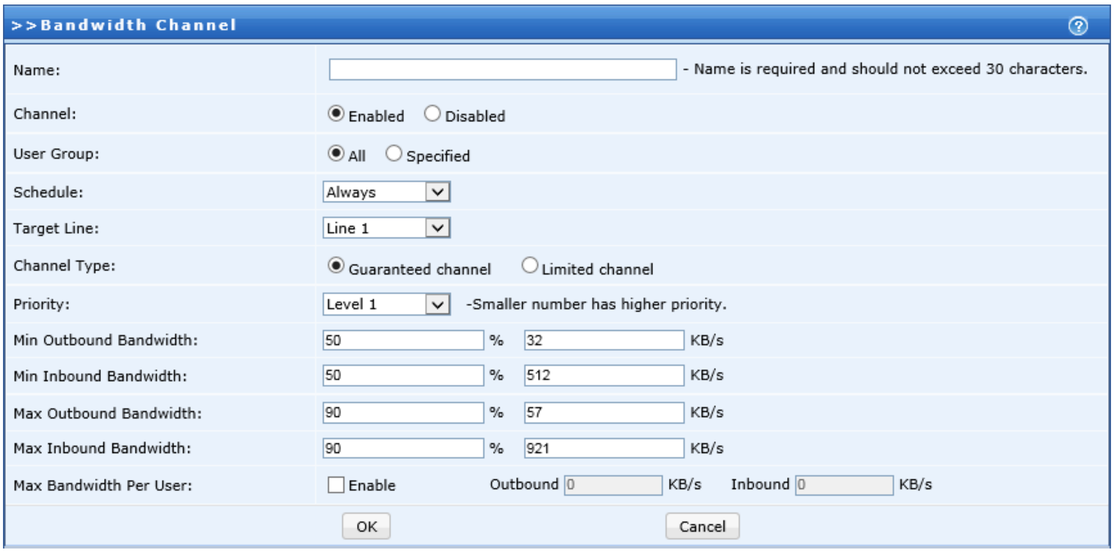
Name	User Group	Schedule	Target Line	Min Bandwidth	Max Bandwidth	Max Bandwidth Per User	Status	Move	Operation	Select
Default Policy 2	All	Always	Line2	↑28KB, ↓460KB	↑51KB, ↓829KB	No limit	Enable	Up Down	Edit	□
Default Policy 1	All	Always	Line1	↑32KB, ↓512KB	↑57KB, ↓921KB	No limit	Enable	Up Down	Edit	□

Add bandwidth channel using -Select- as template

『System Config』 is used to enable the traffic management function. You can select 『Enable』 or 『Disable』 and click OK to enable or disable this function.

『Control Policy List』 shows the traffic control policy that the user has set.

Click Add and the following page appears:



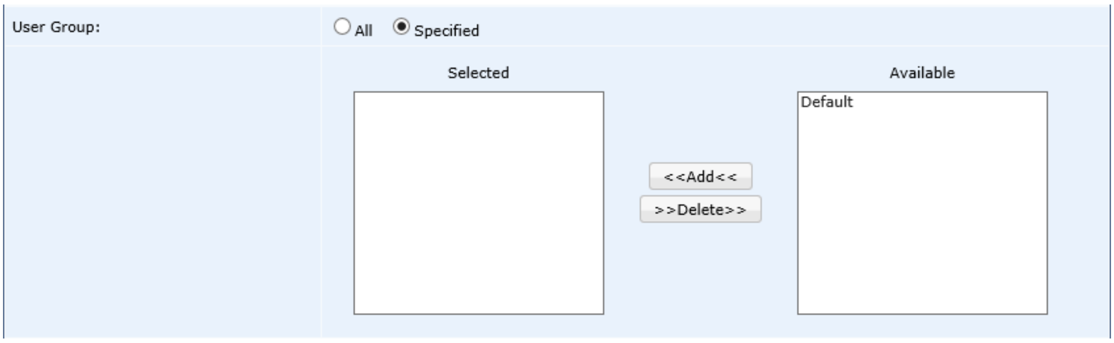
>>Bandwidth Channel

Name:	- Name is required and should not exceed 30 characters.
Channel:	● Enabled ○ Disabled
User Group:	● All ○ Specified
Schedule:	Always
Target Line:	Line 1
Channel Type:	● Guaranteed channel ○ Limited channel
Priority:	Level 1 -Smaller number has higher priority.
Min Outbound Bandwidth:	50 % 32 KB/s
Min Inbound Bandwidth:	50 % 512 KB/s
Max Outbound Bandwidth:	90 % 57 KB/s
Max Inbound Bandwidth:	90 % 921 KB/s
Max Bandwidth Per User:	□ Enable Outbound 0 KB/s Inbound 0 KB/s

『Policy Name』: used to name the policy. The name cannot be empty and cannot exceed 30 characters.

『Enable Channel』 : select whether to enable the policy.

『Applicable User Group』 : used for the user group that is valid based on the rule, can be applied to all user groups or to select some user groups. The interface is as follows:



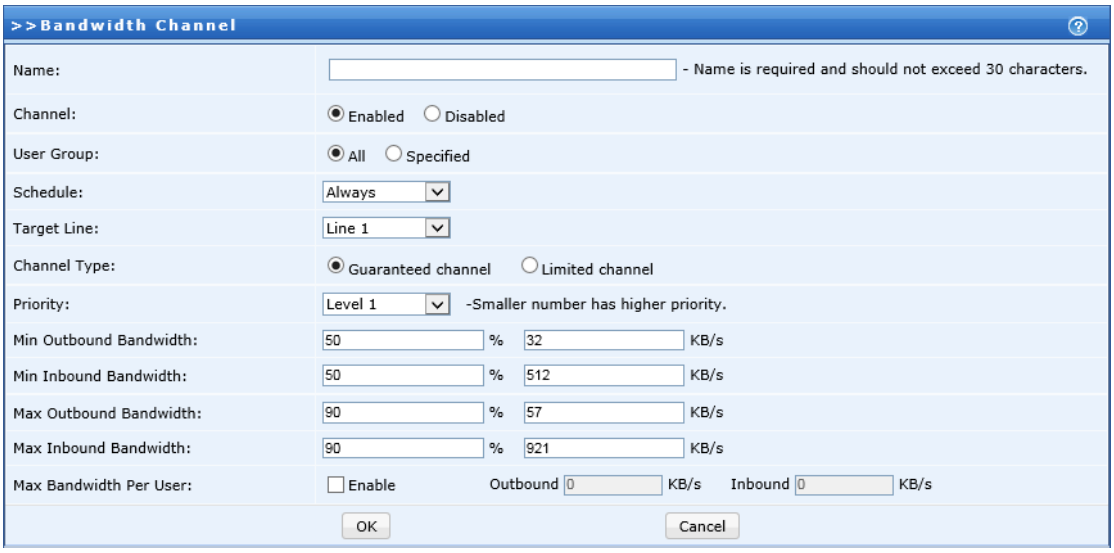
User Group: ○ All ● Specified

Selected	Available
	Default

Click the Add button and select the 『Application Name』 under the 『Application Type』, by which you can select the application type and application name as needed.

『Time in Force』: used to set the time range in which the rule takes effect.

『Bandwidth Allocation Policy Type』: used to select whether the traffic policy is bandwidth guarantee or bandwidth limitation. If selecting the bandwidth guarantee policy, you can guarantee the minimum bandwidth for the user and limit the maximum uplink and downlink bandwidth. If selecting the bandwidth limitation, you only limit the bandwidth for Internet services. The bandwidth guarantee interface is shown below:



>>Bandwidth Channel

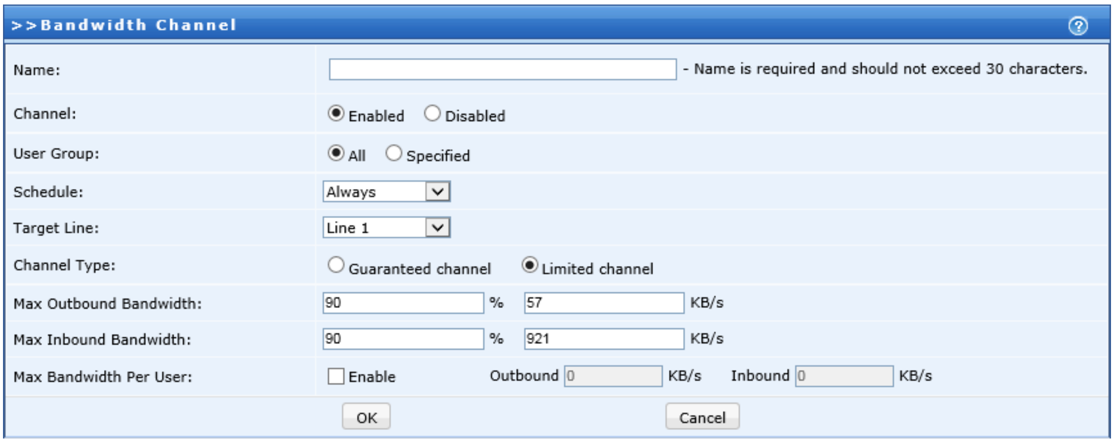
Name:	- Name is required and should not exceed 30 characters.
Channel:	● Enabled ○ Disabled
User Group:	● All ○ Specified
Schedule:	Always
Target Line:	Line 1
Channel Type:	● Guaranteed channel ○ Limited channel
Priority:	Level 1 -Smaller number has higher priority.
Min Outbound Bandwidth:	50 % 32 KB/s
Min Inbound Bandwidth:	50 % 512 KB/s
Max Outbound Bandwidth:	90 % 57 KB/s
Max Inbound Bandwidth:	90 % 921 KB/s
Max Bandwidth Per User:	□ Enable Outbound 0 KB/s Inbound 0 KB/s

『Priority』: Priority 1, Priority 2, Priority 3, Priority 4 can be selected. Priority can be used to guarantee that the idle bandwidth, if any, can be occupied first.

『Outbound Bandwidth Guarantee』 and 『Inbound Bandwidth Guarantee』: used to set the ratio of reserved bandwidth to total Internet bandwidth.

『Maximum Outbound Bandwidth』 and 『Maximum Inbound Bandwidth』: used to set the total upper limit for the uplink and downlink bandwidth limitation of this channel.

The interface for bandwidth limitation settings is shown below:



>>Bandwidth Channel

Name:	- Name is required and should not exceed 30 characters.
Channel:	● Enabled ○ Disabled
User Group:	● All ○ Specified
Schedule:	Always
Target Line:	Line 1
Channel Type:	○ Guaranteed channel ● Limited channel
Max Outbound Bandwidth:	90 % 57 KB/s
Max Inbound Bandwidth:	90 % 921 KB/s
Max Bandwidth Per User:	□ Enable Outbound 0 KB/s Inbound 0 KB/s

『Restrict Single User's Maximum Bandwidth』: used to limit the maximum uplink and downlink bandwidth of a single user. Check [Enable] to enable it.

The single user bandwidth limitation is related to the fixed bandwidth rather than the percentage and is not affected by changes in the line bandwidth setting; while the bandwidth guarantee and bandwidth limitation are the percentage of the current traffic, which vary with the line bandwidth setting.

2.8. Firewall Settings

The MIG hardware gateway integrates a high-performance enterprise-level state inspection firewall, which can effectively protect the internal network from attacks from the Internet, other local area networks connected by VPN and more. At the same time, the built-in anti-DOS attack function can not only effectively prevent DOS attacks from external networks, but also defend against DOS attacks initiated by LAN computers. The MIG hardware gateway includes such modules as『Filtering Rule Settings』, 『NAT Settings』, 『Anti-DOS Settings』, and ARP Spoofing Protection』.

2.8.1. Filtering Rules Settings

The MIG hardware gateway firewall adopts the state detection packet filtering technology, which can implement packet filtering based on the protocol type, source IP, and destination IP in combination with the time plan in multiple data transmission directions.

『Filtering Rules Settings』 includes the rule settings of local rules, LAN<-> DMZ, DMZ<-> WAN, WAN<-> LAN, VPN<-> LAN, VPN<-> WAN, VPN<-> DMZ, four network interfaces, and twelve directions.

As all VPN data is transmitted via the VPN interface (e.g., the data communication between the computer under the local device LAN interface and the VPN peer computer is transmitted via the device LAN interface and the VPN interface), the VPN data can be controlled through firewall filtering rules.

『Local Rules』 is used to set the permissions for the configuration, management, and maintenance of the external network user through the public network IP.

『LAN<-> DMZ』 is used to set the firewall filtering rules for bidirectional data transmission between the LAN interface and the DMZ interface of the MIG device.

『DMZ<-> WAN』 is used to set the firewall filtering rules for bidirectional data transmission between the DMZ interface and the WAN interface of the MIG device.

『WAN<-> LAN』 is used to set the firewall filtering rules for bidirectional data transmission between the WAN interface and the LAN interface of the MIG device.

『VPN<-> LAN』 is used to set the firewall filtering rules for bidirectional data transmission between the VPN interface and the LAN interface of the MIG device.

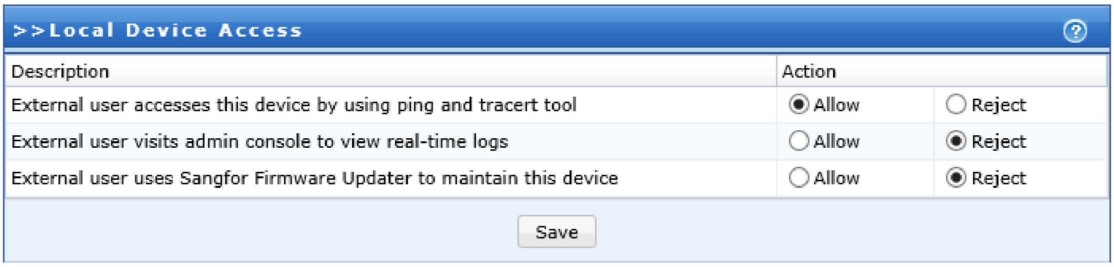
『VPN<-> WAN』 is used to set the firewall filtering rules for bidirectional data transmission between the VPN interface and the WAN interface of the MIG device. (If the peer of the VPN connection is set to take the local end as the 『Destination Routing User』 in the 『Inter-tunnel Routing Settings』 and enable 『Internet access to users through the destination route』, you can set the VPN <-> WAN filtering rule on the local end to implement control over the branch's Internet data.

『LAN<-> DMZ』 is used to set the firewall filtering rules for bidirectional data transmission between the LAN interface and the DMZ interface of the MIG device.

Below, let's introduce the general steps of setting filtering rules by taking local rules, LAN<-> WAN, VPN<-> LAN as examples:

1. Local rules

『Local Rules』 is used to set the permissions for the configuration, management, and maintenance of the external network user through the public network IP.



>>Local Device Access

Description	Action	
External user accesses this device by using ping and tracert tool	● Allow	○ Reject
External user visits admin console to view real-time logs	○ Allow	● Reject
External user uses Sangfor Firmware Updater to maintain this device	○ Allow	● Reject

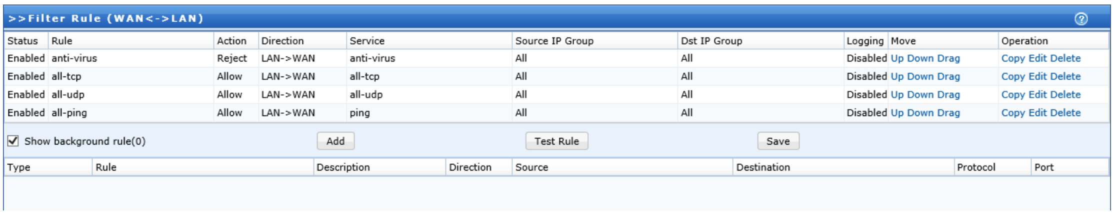
『Allow external network to ping and tracert local device』: allows external users to directly ping the local WAN interface, mainly used to test the network connectivity, etc.

『Allow the external network user to log in to the device to view real-time log』: used for maintenance by manufacturer personnel

『Allow the external network user to use the upgrade client for maintenance』: used for the external network user to connect the device through the upgrade client for upgrading, debugging, etc.

2、LAN<->WAN

This interface is used to set firewall filtering rules for data transmission between the LAN port and the WAN port, which can release or reject certain service data according to the actual environment. For example, to achieve full interconnection between the LAN and the WAN interface and to conduct tests by using the PING command, all TCP, UDP, and ICMP filtering rules need to be opened in both directions. The page is shown as follows:



>>Filter Rule (WAN<->LAN)

Status	Rule	Action	Direction	Service	Source IP Group	Dst IP Group	Logging	Move	Operation
Enabled	anti-virus	Reject	LAN->WAN	anti-virus	All	All	Disabled	Up Down Drag	Copy Edit Delete
Enabled	all-tcp	Allow	LAN->WAN	all-tcp	All	All	Disabled	Up Down Drag	Copy Edit Delete
Enabled	all-udp	Allow	LAN->WAN	all-udp	All	All	Disabled	Up Down Drag	Copy Edit Delete
Enabled	all-ping	Allow	LAN->WAN	ping	All	All	Disabled	Up Down Drag	Copy Edit Delete

☑ Show background rule(0)

Type	Rule	Description	Direction	Source	Destination	Protocol	Port

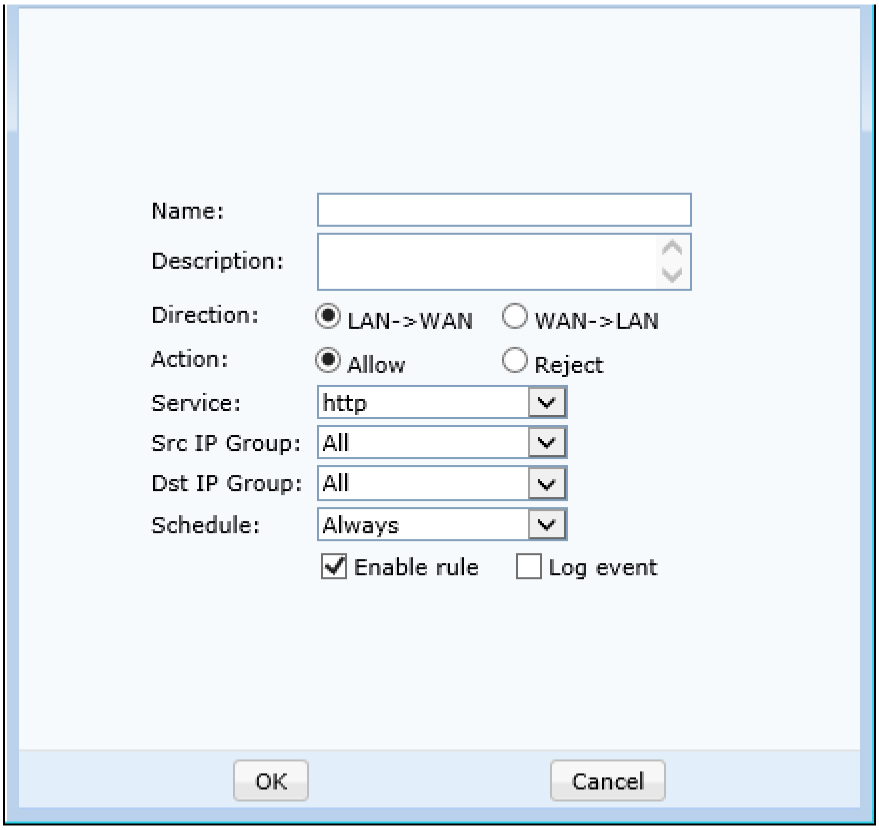
Click the Up or Down button, the rule can be moved up or down for one item. Firewall rules are matched one after another from top to bottom, and you can use "Up" or "Down" to adjust the priority for different policies.

Click the Drag button and hold down the left mouse button, the rule can be moved to the desired position.

Click the Copy button, you can copy the rule, and you can also modify the rule and save it as a new one.

Checking [Show Implicit Rules] will display the firewall filtering rules that are for the network access by the proxy server or automatically released by the port mapping rules, without the need to manually release them once more.

Pay attention to the direction and action of the data when setting the rules. The page is as follows:



Name:

Description:

Direction: ● LAN->WAN ○ WAN->LAN

Action: ● Allow ○ Reject

Service: http

Src IP Group: All

Dst IP Group: All

Schedule: Always

☑ Enable rule □ Log event

『Rule Name』 : set the custom rule name.

『Rule Direction』 : set which direction of the data this rule is valid for.

『Rule Action』 : set the execution action after the data matches this rule.

『Service』 : set the service type that the rule will match.

『Source IP Group』 : set the source IP address that the rule will match.

『Destination IP Group』 : set the destination IP address that the rule will match.

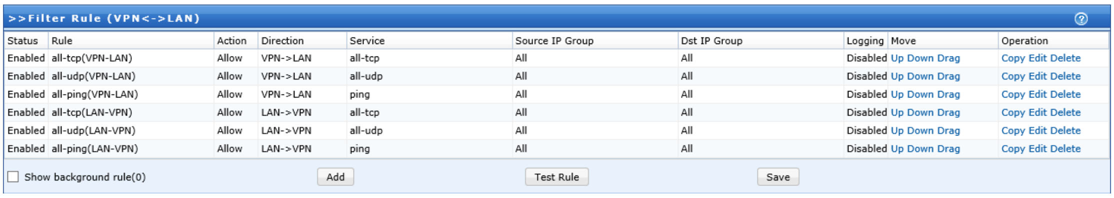
『Schedule』 : set the time when the rule takes effect.

Check the [Enable Rule] option, and this rule will take effect as soon as it is set.

Check the [Enable Log] option, all data packages matching this rule will be recorded by the log system when passing the device. In general, please do not enable it, for fear that a large amount of log will be generated by the system.

3、VPN<->LAN

This interface is used to set firewall filtering rules for data transmission between the VPN interface and the LAN interface. The default rule has released all TCP, UDP, and ICMP data in both directions. The page is as follows:



>>Filter Rule (VPN<->LAN)

Status	Rule	Action	Direction	Service	Source IP Group	Dst IP Group	Logging	Move	Operation
Enabled	all-tcp(VPN-LAN)	Allow	VPN->LAN	all-tcp	All	All	Disabled	Up Down Drag	Copy Edit Delete
Enabled	all-udp(VPN-LAN)	Allow	VPN->LAN	all-udp	All	All	Disabled	Up Down Drag	Copy Edit Delete
Enabled	all-ping(VPN-LAN)	Allow	VPN->LAN	ping	All	All	Disabled	Up Down Drag	Copy Edit Delete
Enabled	all-tcp(LAN-VPN)	Allow	LAN->VPN	all-tcp	All	All	Disabled	Up Down Drag	Copy Edit Delete
Enabled	all-udp(LAN-VPN)	Allow	LAN->VPN	all-udp	All	All	Disabled	Up Down Drag	Copy Edit Delete
Enabled	all-ping(LAN-VPN)	Allow	LAN->VPN	ping	All	All	Disabled	Up Down Drag	Copy Edit Delete

☐ Show background rule(0)

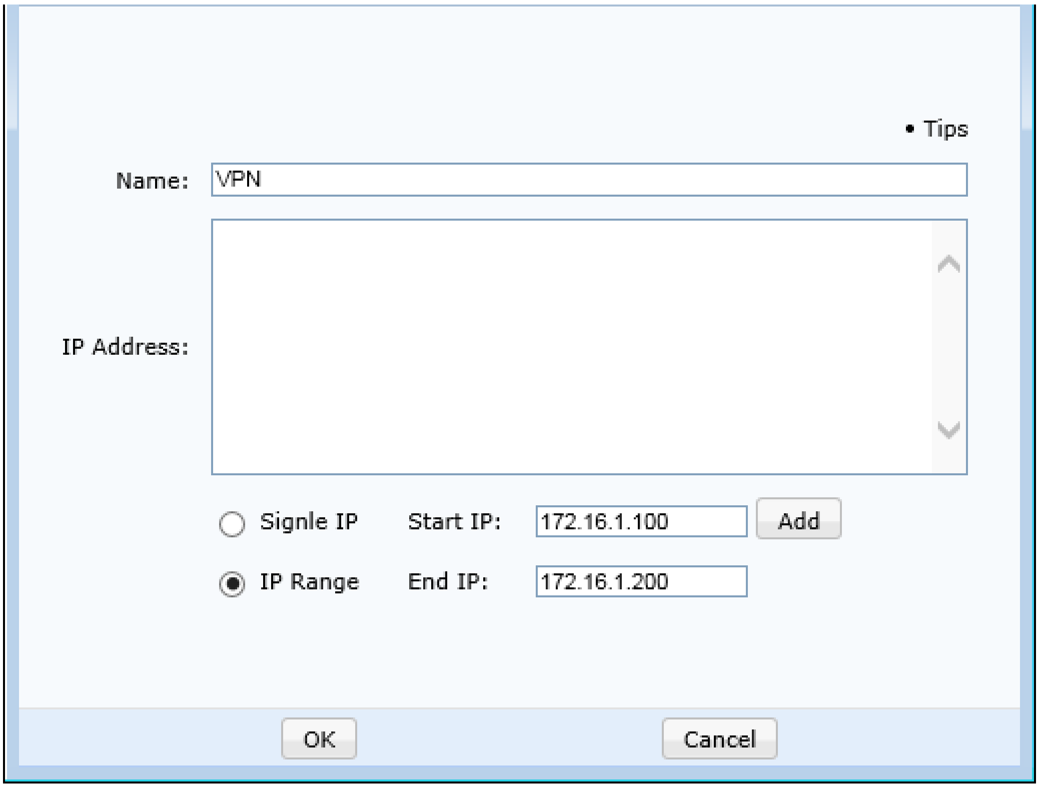
2.8.1.1. Case Study

The headquarters of a company only allows some of the IP addresses (172.16.1.100-172.16.1.200) of the VPN branch (172.16.1.0/24) that is connected to the headquarters to access the web service of the headquarters' LAN server (192.168.10.20), but the access to the SQL SERVER service is prohibited.

The setup steps are as follows:

First, perform the "IP Group Settings" in 『Object Settings』→『IP Group Settings』.

The page of the VPN branch configuration is as follows:



• Tips

Name: VPN

IP Address:

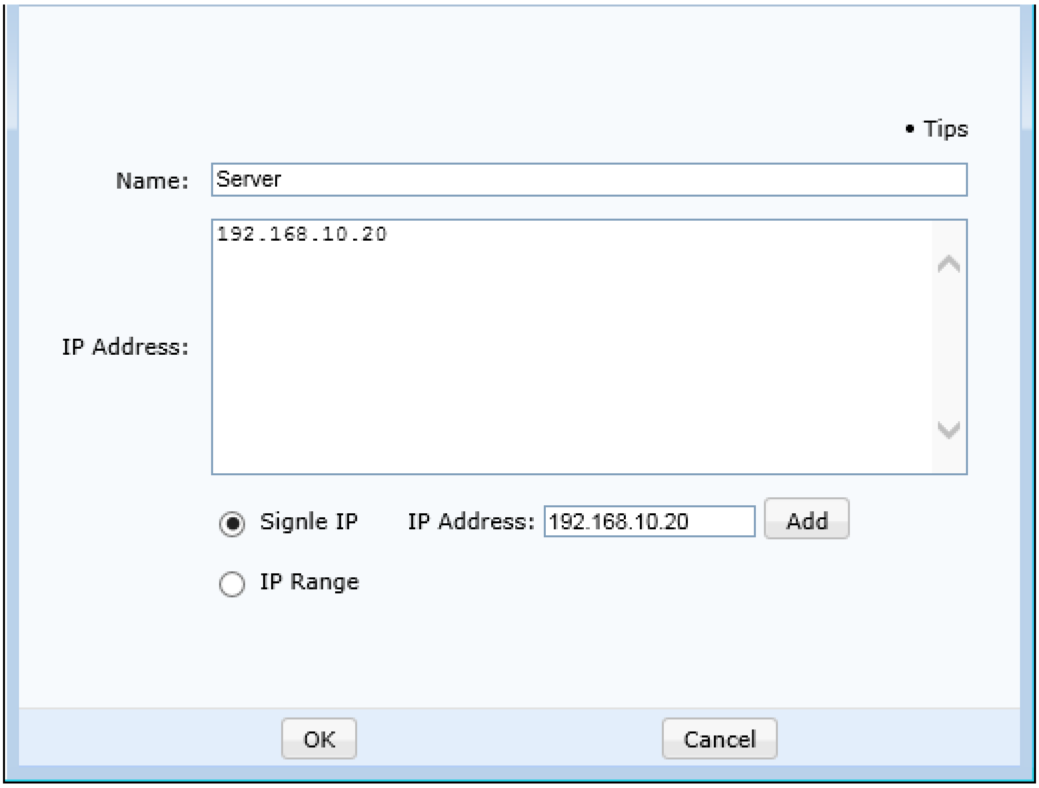
○ Signle IP Start IP: 172.16.1.100

● IP Range End IP: 172.16.1.200

『IP Group Name』: Name the IP or IP segment to be defined at will.

『IP Group』: select the IP range, fill in the IP address segment that the branch allows to access: start IP: 172.16.1.100, end IP: 172.16.1.200, and then click “Add”, it will be added to the IP Group Definition box; click "Ok" and the setting of the "vpn branch 1" IP group is completed.

The page of the LAN server configuration is as follows:



Name: Server

IP Address: 192.168.10.20

● Signle IP IP Address: 192.168.10.20

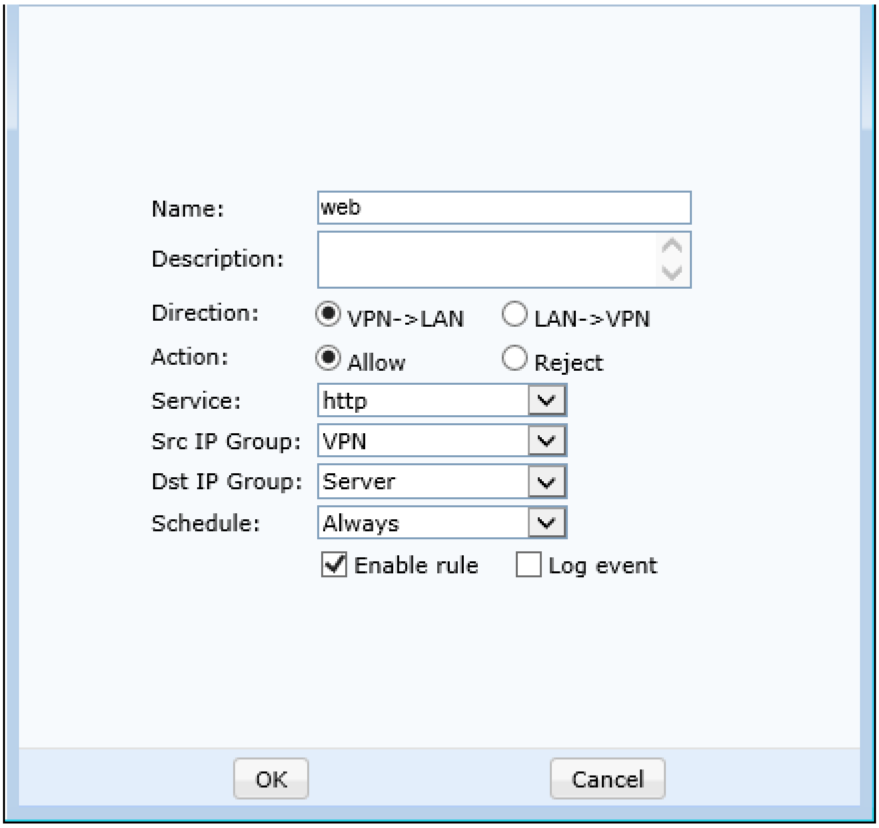
○ IP Range

『IP Group Name』: Name the IP or IP segment to be defined at will.

『IP Group』: select a single IP 192.168.10.20, fill it out, then click Add, it will be added to the IP group definition box; click OK, then it will be added to 『Object Settings』 → 『IP Group Settings』 list.

Then click OK on the page to save the configuration.

Then create a new WEB service filtering rule, and the configuration page is as follows:



Name: web

Description:

Direction: ● VPN->LAN ○ LAN->VPN

Action: ● Allow ○ Reject

Service: http

Src IP Group: VPN

Dst IP Group: Server

Schedule: Always

☑ Enable rule □ Log event

『Rule Name』: set the custom rule name.

『Rule Direction』: set to VPN-> LAN.

『Rule Action』: set to letting such data pass

『Service』: set to HTTP.

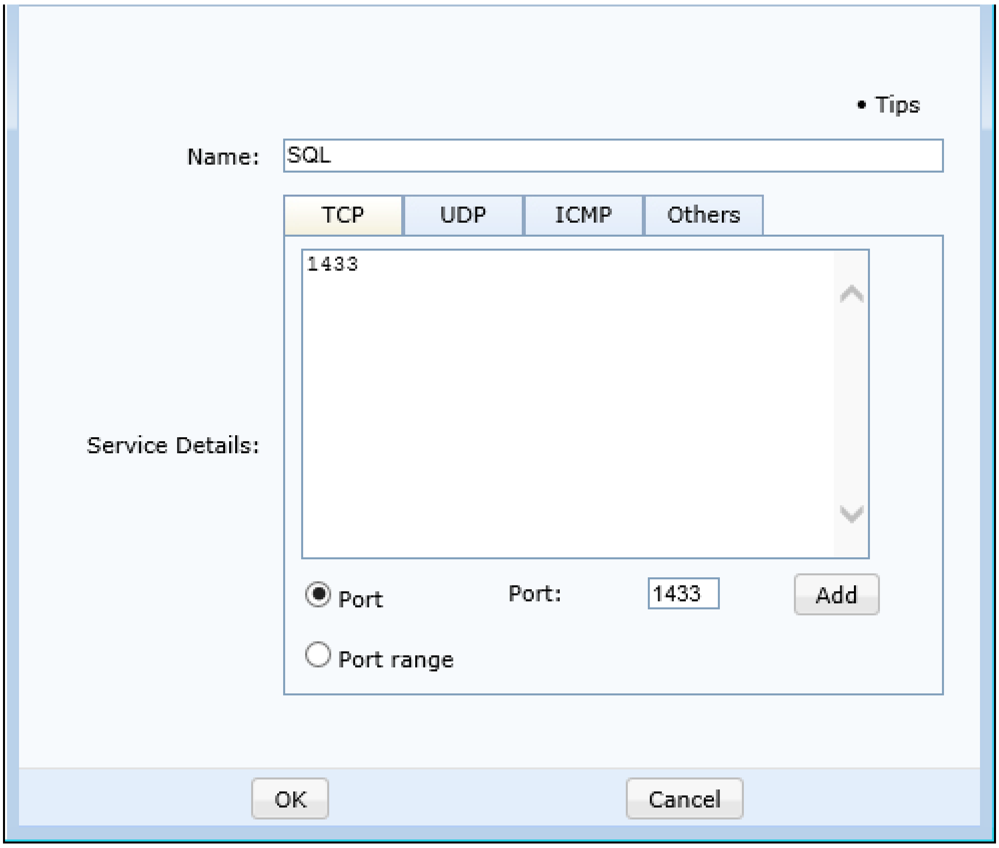
『Source IP Group』: select the set IP group "VPN branch".

『Destination IP Group』: select the set IP group "Server".

『Schedule』: set the time when the rule takes effect.

Check the [Enable the Rule] option and click Ok.

Next, set the service filtering rules of the SQL SERVER. Firstly, define the service. The page is as follows:



Name: SQL

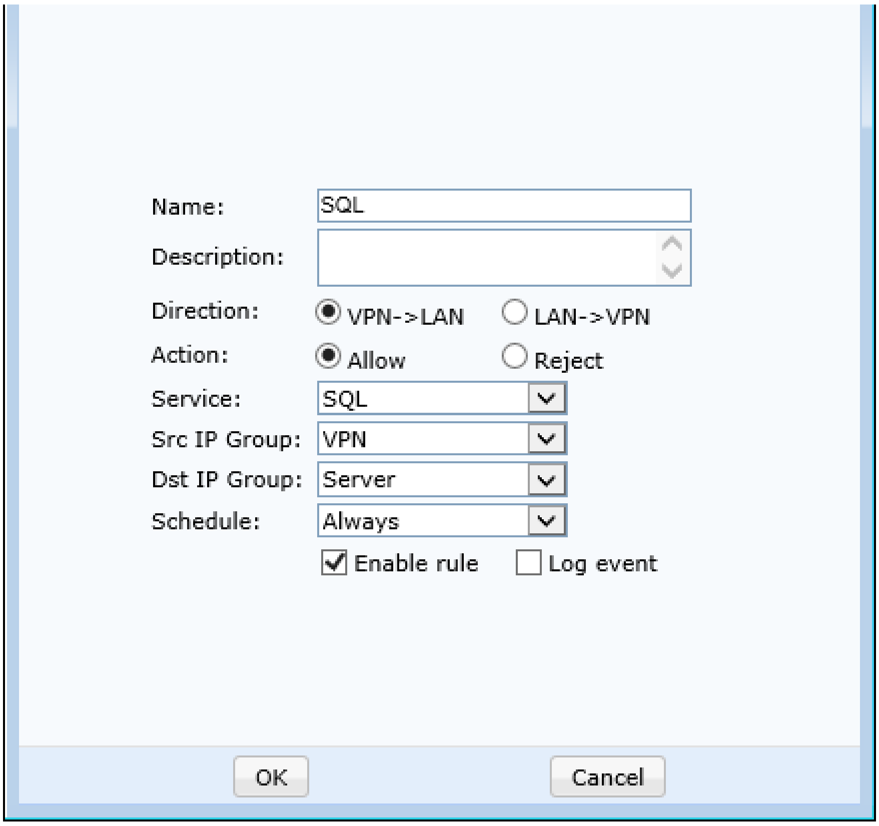
Service Details: 1433

● Port Port: 1433

○ Port range

The『Service Name』 can be customized (in this case, it can be set to: SQL). Select TCP in 『protocol』, fill in 1433 in 『Port Number』, then click Add to add it to the service definition box; click Ok to add the service to the "Object Settings" → "Network Service Settings" list , then click Ok to save the setting, thus to complete the definition of the SQL SERVER service.

Next, set the service filtering rules of the SQL SERVER. The page is as follows:



Name: SQL

Description:

Direction: ● VPN->LAN ○ LAN->VPN

Action: ● Allow ○ Reject

Service: SQL

Src IP Group: VPN

Dst IP Group: Server

Schedule: Always

☑ Enable rule □ Log event

『Name』: customized as SQL.

『Direction』: set to VPN-> LAN.

『Rule Action』: set to reject such data.

『Service』: set to SQL.

『Source IP Group』: set to the partial IP address of the branch LAN, 172.16.1.100-172.16.1.200.

『Destination IP Group』: set to the server IP of the headquarters LAN, 192.168.10.20.

『Schedule』: set the rule to being effective for all day.

Check the [Enable the Rule] option and click OK.

After completing the above settings, you can achieve the requirements described in the case.

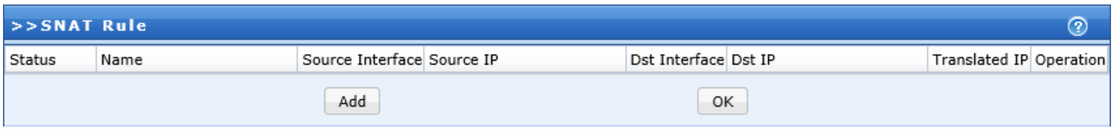
Other requirements such as restricting the access of the headquarters to the branch service and restricting the data of the branch through the headquarters can be achieved by setting filtering rules between the corresponding interfaces.

2.8.2. NAT Settings

The NAT settings include 『Proxy Internet Access Settings』 and 『Port Mapping Settings』.

2.8.2.1. Proxy Internet Access Settings

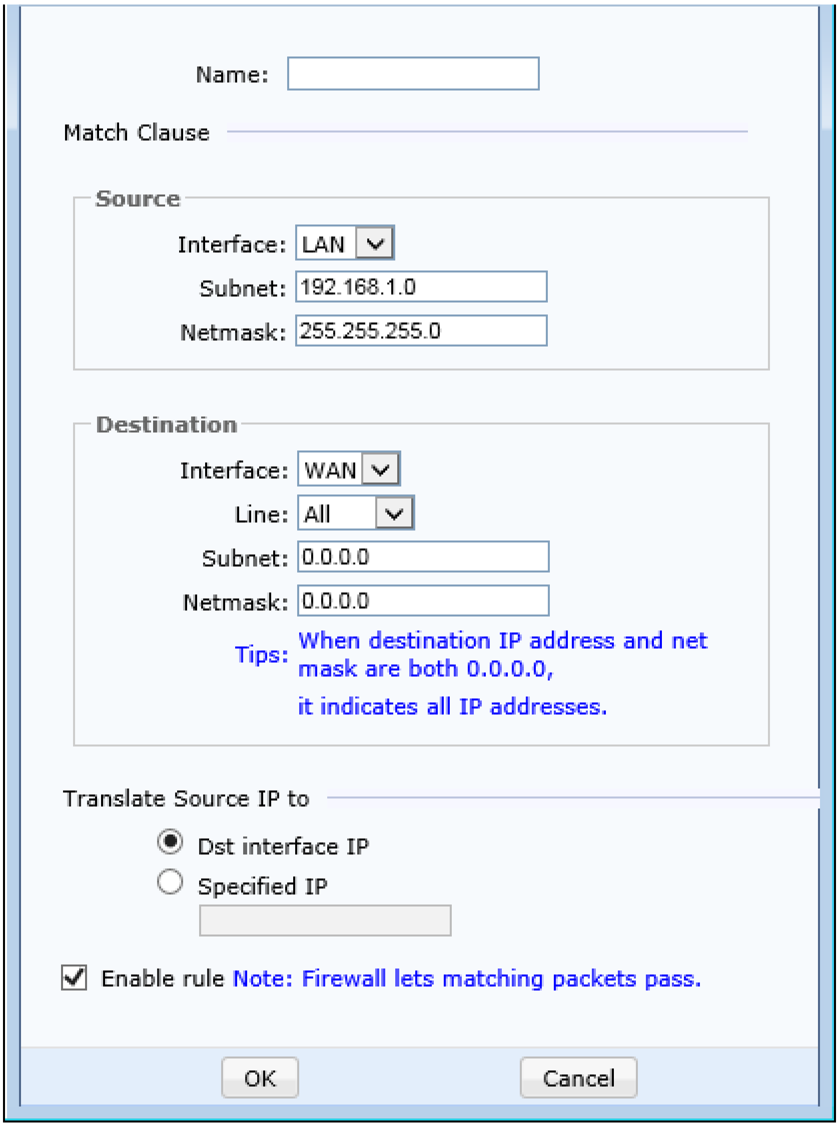
『Proxy Internet Access Settings』 is used to set the firewall rules for Internet access via proxy by the local area network. The MIG hardware gateway not only has the basic function of accessing the Internet via NAT but also can control the LAN Internet service by cooperating with the filtering rules. The rules for Internet access via proxy on this page can be sorted by 『Status』, 『Name』, 『Source Interface』, 『Source Address』, 『Destination Interface』, etc. The page is as follows:



>>SNAT Rule

Status	Name	Source Interface	Source IP	Dst Interface	Dst IP	Translated IP	Operation

The default settings of the device does not include the proxy rule, which needs to be added manually. Click Add, the 『Name』 can be customized, fill in the proxy network segment and click OK. The page is as follows:



Name:

Match Clause

Source

Interface: LAN

Subnet: 192.168.1.0

Netmask: 255.255.255.0

Destination

Interface: WAN

Line: All

Subnet: 0.0.0.0

Netmask: 0.0.0.0

Tips: When destination IP address and net mask are both 0.0.0.0, it indicates all IP addresses.

Translate Source IP to

● Dst interface IP

○ Specified IP

☑ Enable rule Note: Firewall lets matching packets pass.

[Name] is used to set the custom rule name

[Conversion Condition / Source Address] The source interface is used to set the source interface address of the data packet, indicating that the data coming from the interface will continue to match. You can choose LAN, DMZ or VPN. The subnet segment and subnet mask are used to set the source address segment that needs to be converted.

[Conversion Condition / Destination Address] The destination interface is used to set the outbound interface address of the data packet, indicating that the data going out from the interface will be matched downwards. You can choose LAN, DMZ or VPN. The subnet segment and subnet mask are used to set the matching conditions, indicating that the destination IP address of the packet is within the set range, and the rule can be matched.

[Convert Source Address to] is used to set the packet conversion source address that meets the specified conditions to "destination interface address" or "specified address". If the destination interface address is selected, the source address of the packet is converted to the IP address of the interface selected by the destination interface. If the "specified address" is selected, you need to manually set an IP address.

Check [Enable the Rule], the rule will take effect, and the firewall will automatically set the corresponding filtering rules.

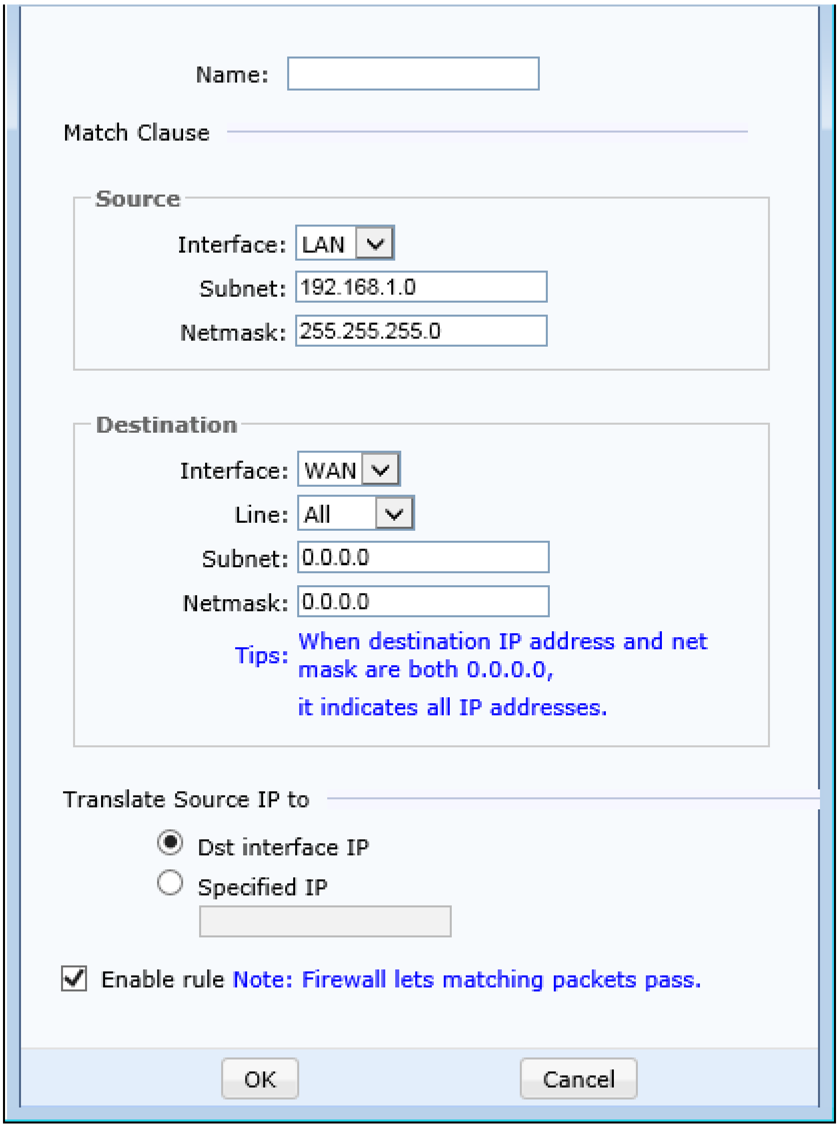
Below is a simple example to illustrate how the rules for Internet access via proxy are set. Examples are as follows:

Example one of Internet access via proxy:

The network egress of a customer is a MIG 1200 device, the WAN interface is ADSL dial-up, the IP address of the LAN interface is 192.168.1.1, the LAN PCs reside in 192.168.1.0/24 network segment, and the gateway direction is 192.168.1.1. After the deployment of the MIG 1200 device, it is necessary to ensure that the LAN PC can access the public network. The configuration method is as follows:

Step 1: Configure the IP address of the device interface, please refer to the chapter 『System Setup』 - 『Network Interface Settings』. The details won't be repeated here.

Step 2: Configure the proxy to access the Internet, select the LAN in the source interface, and fill in network segment of LAN interface in the subnet segment. The outbound interface is the WAN interface of the public network, the destination IP address is all IP addresses, and convert the source address to the IP address of WAN interface. The interface is as follows:



Name:

Match Clause

Source

Interface: LAN

Subnet: 192.168.1.0

Netmask: 255.255.255.0

Destination

Interface: WAN

Line: All

Subnet: 0.0.0.0

Netmask: 0.0.0.0

Tips: When destination IP address and net mask are both 0.0.0.0, it indicates all IP addresses.

Translate Source IP to

● Dst interface IP

○ Specified IP

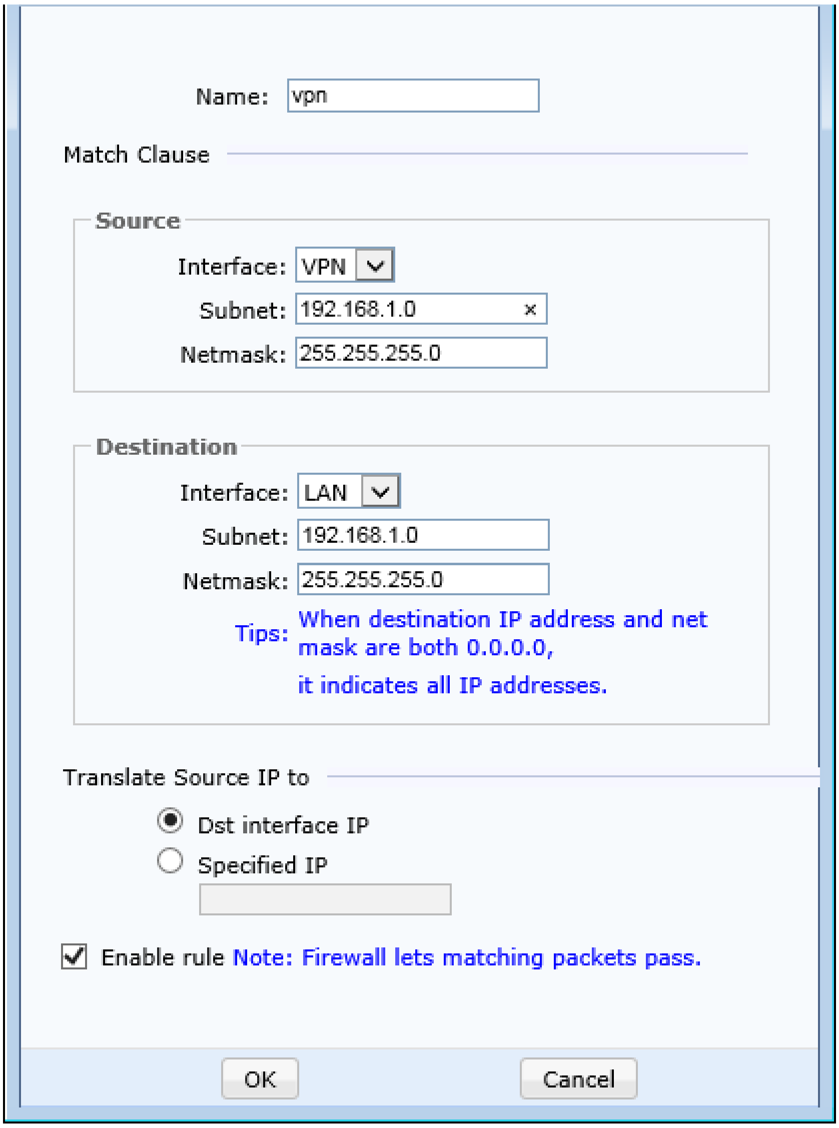
☑ Enable rule Note: Firewall lets matching packets pass.

Example two of Internet access via proxy:

The headquarters of a customer and their branch are connected by SANGFOR VPN, and a VPN tunnel is connected. The headquarters uses MIG 1200 device, the branch uses VPN 1110 device, and the branch LAN segment is 192.168.1.0/24. The customer wants all the users of the branch to go online through the network of the headquarters rather than that of the branch. The configuration method is as follows:

Step 1: Configure the inter-tunnel route on the MIG device of the branch, and check the “Internet access through the destination route”. For details, please refer to the chapter “VPN Information Settings” - “Inter-tunnel Routing Settings”.

Step 2: Configure Internet access via proxy rule on the MIG device at the headquarters. Select the VPN interface in the source interface (because the data is coming from the VPN peer), fill in the 192.168.1.0/24 in the source address, and select the WAN in destination interface. The interface is as follows:



Name: vpn

Match Clause

Source

Interface: VPN

Subnet: 192.168.1.0

Netmask: 255.255.255.0

Destination

Interface: LAN

Subnet: 192.168.1.0

Netmask: 255.255.255.0

Tips: When destination IP address and net mask are both 0.0.0.0, it indicates all IP addresses.

Translate Source IP to

● Dst interface IP

○ Specified IP

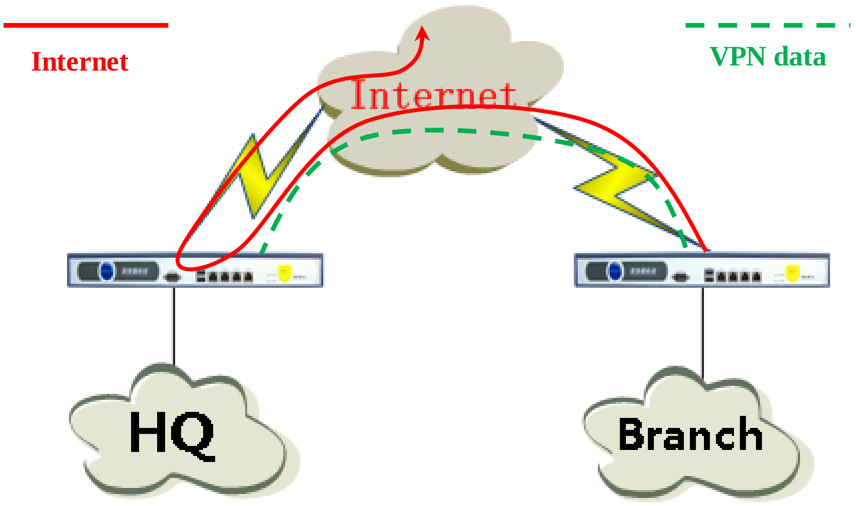
☑ Enable rule Note: Firewall lets matching packets pass.

For advanced application scenarios and examples of selecting VPN as the source

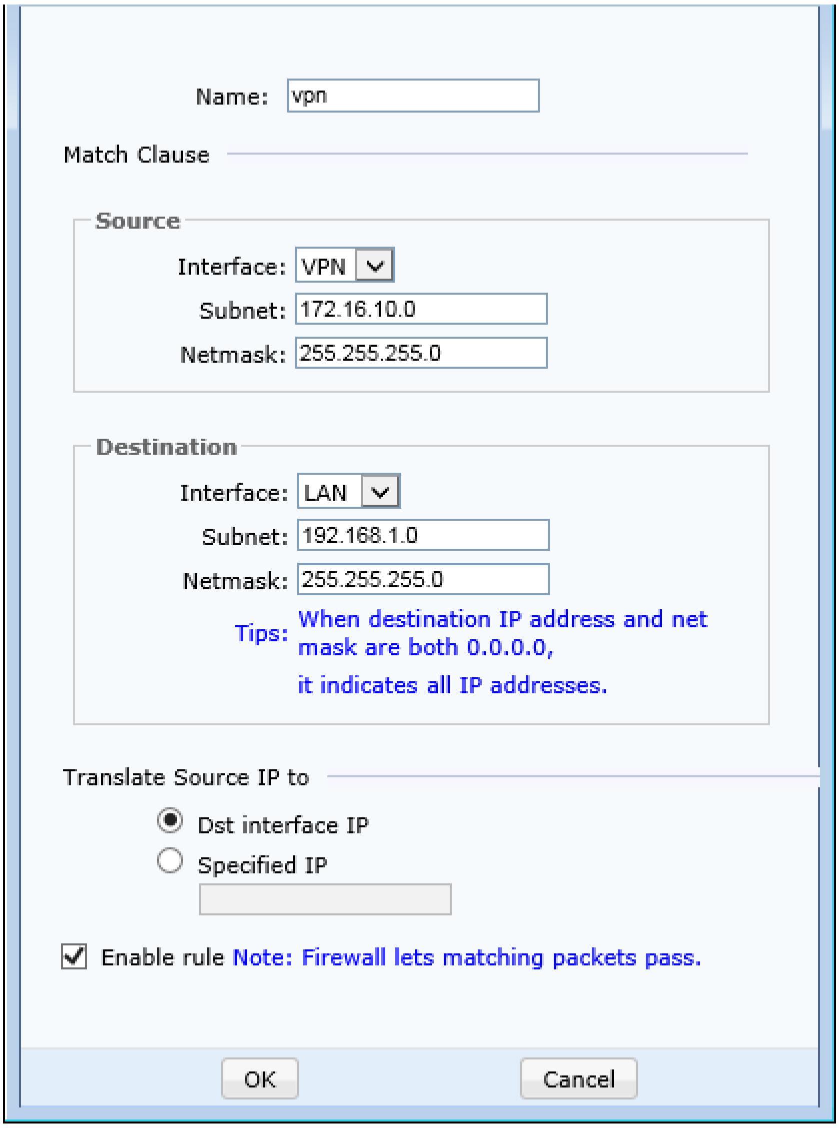
interface, please refer to 『Case Study』

2.8.2.1.1 Case Study

The headquarters SANGFOR device adopts the routing mode to deploy, and the branch (172.16.10.0/24) needs to access the internet by connecting to the headquarters through VPN. The topology is as follows:



In the case of a normal VPN connection, the SANGFOR device of the branch needs to add inter-tunnel routing (see section **Error! Reference source not found.** 『Inter-tunnel Routing Settings』 for details), while the SANGFOR device at the headquarters needs to add 『LAN Interface』 as the proxy rule of the VPN and add the LAN segment of the branch. The page is as follows:



Name: vpn

Match Clause

Source

Interface: VPN

Subnet: 172.16.10.0

Netmask: 255.255.255.0

Destination

Interface: LAN

Subnet: 192.168.1.0

Netmask: 255.255.255.0

Tips: When destination IP address and net mask are both 0.0.0.0, it indicates all IP addresses.

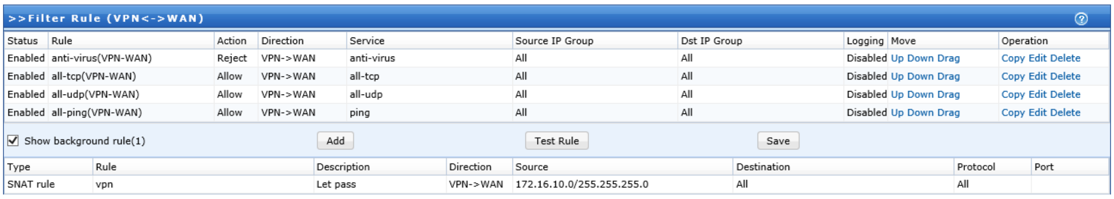
Translate Source IP to

● Dst interface IP

○ Specified IP

☑ Enable rule Note: Firewall lets matching packets pass.

Firewall rules are automatically released, with no need to manually release them. Click 『Firewall Settings』→ 『Filtering Rule Settings』 → 『VPN<-> WAN』, check Show Implicit Rules, you can see the automatically released firewall rules. The page is as follows:



>>Filter Rule (VPN<->WAN)

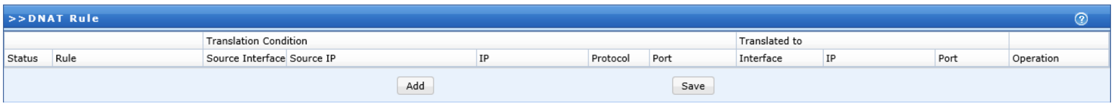
Status	Rule	Action	Direction	Service	Source IP Group	Dst IP Group	Logging	Move	Operation
Enabled	anti-virus(VPN-WAN)	Reject	VPN->WAN	anti-virus	All	All	Disabled	Up Down Drag	Copy Edit Delete
Enabled	all-tcp(VPN-WAN)	Allow	VPN->WAN	all-tcp	All	All	Disabled	Up Down Drag	Copy Edit Delete
Enabled	all-udp(VPN-WAN)	Allow	VPN->WAN	all-udp	All	All	Disabled	Up Down Drag	Copy Edit Delete
Enabled	all-ping(VPN-WAN)	Allow	VPN->WAN	ping	All	All	Disabled	Up Down Drag	Copy Edit Delete

☑ Show background rule(1)

Type	Rule	Description	Direction	Source	Destination	Protocol	Port
SNAT rule	vpn	Let pass	VPN->WAN	172.16.10.0/255.255.255.0	All	All	

2.8.2.2. Port Mapping Settings

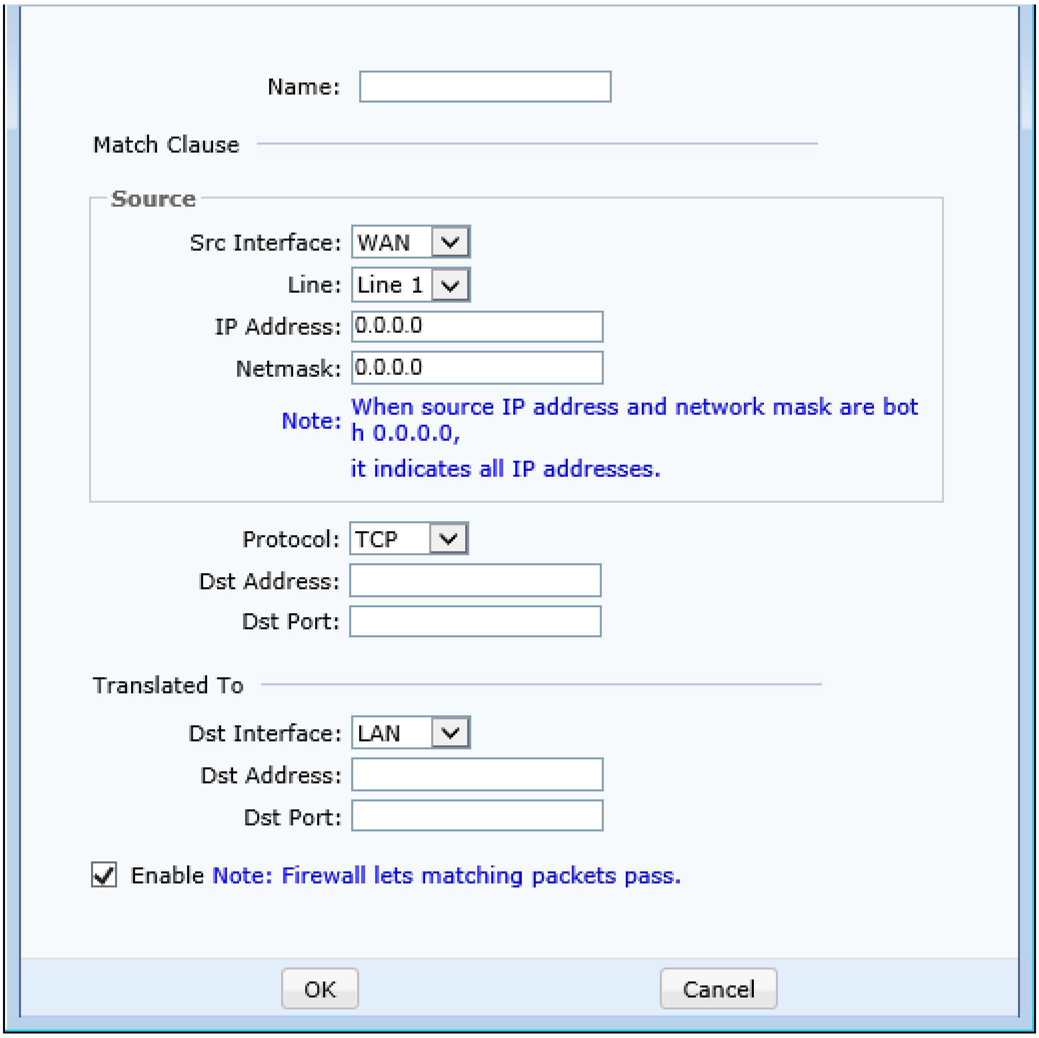
The『Port Mapping Settings』 is used to set the DNAT rules of the firewall. If the server in the local area network needs to provide services to the external network, you need to add 『Rule Name』,『Source Interface』,『Source IP』,『Source Port』,『Destination Interface』,『Destination IP』,『Destination Port』and『protocol』. The page is as follows:



>>DNAT Rule

		Translation Condition					Translated to			
Status	Rule	Source Interface	Source IP	IP	Protocol	Port	Interface	IP	Port	Operation

Click Add to add a port mapping. The page is as follows:



Name:

Match Clause

Source

Src Interface: WAN

Line: Line 1

IP Address: 0.0.0.0

Netmask: 0.0.0.0

Note: When source IP address and network mask are bot
h 0.0.0.0,
it indicates all IP addresses.

Protocol: TCP

Dst Address:

Dst Port:

Translated To

Dst Interface: LAN

Dst Address:

Dst Port:

☑ Enable Note: Firewall lets matching packets pass.

[Name] is used to set the custom rule name

The source interface of [Conversion Condition / Source Address] is used to set the source interface address of the data packet, indicating that the data coming in from the interface will continue the matching downward. The LAN, DMZ, or WAN can be selected. Selecting the WAN port also needs to set the corresponding line in the case of dual line. The subnet segment and subnet mask are used to set the matching conditions for the source address , indicating that the source IP address of the data packet is within the set range, then it can be matched downward.

The [Conversion condition/protocol] is used to set the conversion condition of the protocol, indicating that the package protocol of the data packet meets the set conditions, and will continue the matching downward.

The [Conversion Condition / Destination Address] is used to set the conversion condition, indicating that the destination address of the packet meets the set conditions, and will continue the matching downward.

The [Conversion condition/port] is used to set the conversion condition, indicating that the destination port of the packet meets the set conditions, and will continue the matching downward.

The [Convert to / destination interface] is used to set the outbound interface of the data packet that meets the above conditions, indicating that the above-mentioned setting conditions are met, and the conversion of destination packet and destination port will also be performed for the packet outgoing from the destination interface.

The [Convert to / Destination Address] is used to set the destination address of the converted packet, indicating the packet that meets all the above conditions, and the destination address of the packet will be converted to the set value.

The [Convert to / Destination Port] is used to set the destination port of the converted packet, indicating the packet that meets all the above conditions, and the firewall will convert the destination port of the packet to the set value.

Check [Enable the Rule], the rule will take effect, and the firewall will automatically set the corresponding filtering rules.

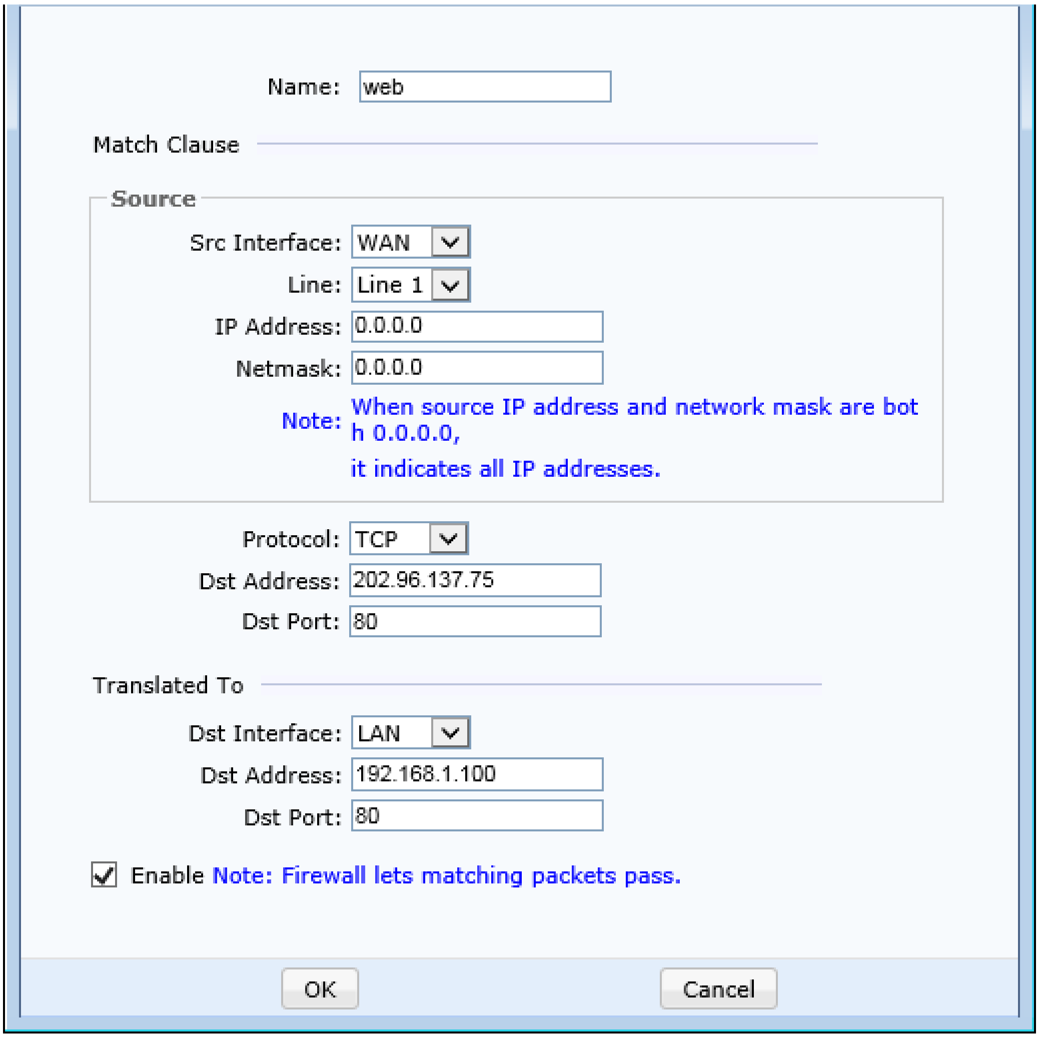
Below is a simple example to illustrate how the rules for Internet access via proxy are set. Examples are as follows:

Port Mapping Settings

The network egress deployment of a customer is MIG 1200, a telecommunication line is connected to device line 1, the IP address of the WAN interface is 202.96.137.75, the IP address of the LAN interface is 192.168.1.1, and the LAN has a WEB server (80 port provides service) with the IP address of 192.168.1.100. Now the customer wants public network users to access the server 192.168.1.100. The configuration method is as follows: The configuration method is as follows:

Step 1: Configure the basic network. For details on how to configure the interface IP address, see the section of network interface configuration. The details will not be mentioned again here.

Step 2: Deploy the port mapping. The configuration information in this case is shown in the figure:



Name: web

Match Clause

Source

Src Interface: WAN

Line: Line 1

IP Address: 0.0.0.0

Netmask: 0.0.0.0

Note: When source IP address and network mask are bot h 0.0.0.0, it indicates all IP addresses.

Protocol: TCP

Dst Address: 202.96.137.75

Dst Port: 80

Translated To

Dst Interface: LAN

Dst Address: 192.168.1.100

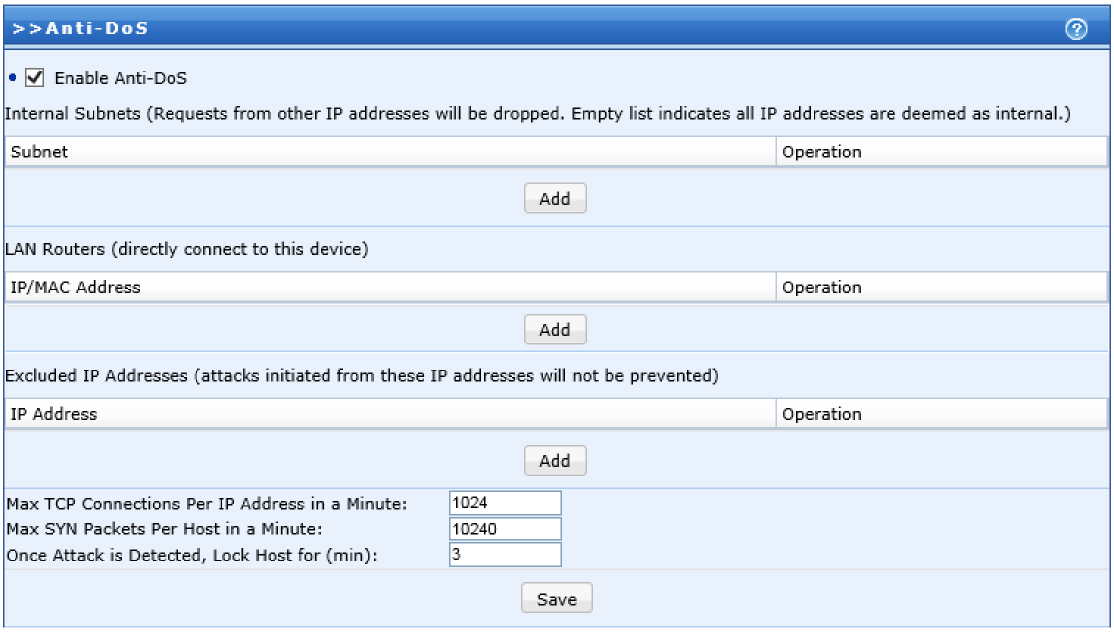
Dst Port: 80

☑ Enable Note: Firewall lets matching packets pass.

⚠ Note: The LAN server that provides services by setting the port mapping through the SANGFOR VPN hardware device must use the VPN hardware device as the NAT proxy to access the Internet (the gateway points to the VPN or the Internet route and eventually points to the VPN), otherwise the port mapping will not take effect.

2.8.3. Anti-DOS attacks

The firewall is not only responsible for blocking the illegal attacks on the local area network from the users on the Internet. In many cases, the computer in the local area network may also be infected, and a large number of data packets will be sent to the gateway, which may cause bandwidth blocking or gateway crash. The MIG series hardware device integrates the 『anti-DOS attack』function, which can monitor how much data an IP sends to the gateway per unit time. When a certain value is exceeded, the MIG series hardware device will consider it as a DOS attack from this IP, and will block this IP for a period of time to protect itself. The page is shown as follows:



>>Anti-DoS

● ☑ Enable Anti-DoS

Internal Subnets (Requests from other IP addresses will be dropped. Empty list indicates all IP addresses are deemed as internal.)

Subnet	Operation

LAN Routers (directly connect to this device)

IP/MAC Address	Operation

Excluded IP Addresses (attacks initiated from these IP addresses will not be prevented)

IP Address	Operation

Max TCP Connections Per IP Address in a Minute: 1024
Max SYN Packets Per Host in a Minute: 10240
Once Attack is Detected, Lock Host for (min): 3

Add the network segment included in the local area network in the 『LAN Network Segment List』. When it is empty, it means that the IP address is not checked. After the LAN segment is added, if the source IP does not belong to the network segment listed in the 『LAN Network Segment List』, the packet will be immediately discarded. If it belongs to the 『LAN Network Segment List』 range, the calculation and detection of the following anti-DOS attack settings will be performed for corresponding processing.

Similarly, the function of 『LAN Router List』 is similar to that of the『LAN Network Segment List』. After the LAN router address is added, the MIG device will automatically obtain the MAC address of the LAN router and does not detect the DOS attack against the MAC address of the Router. If it is incorrectly filled in, the LAN router may be blocked by mistake. As a result, all users passing the router will be unable to access the Internet.

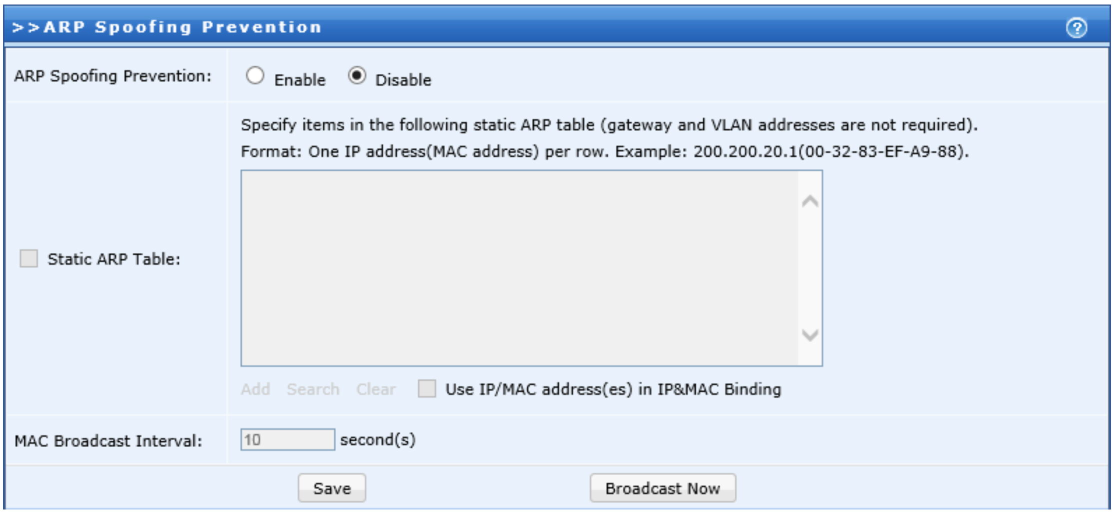
Other options can be set according to the situation, such as 『Maximum Number of TCP Connections』, 『Maximum Number of SYN Packets』 and 『Lock Time for Preventing DOS Attacks』.

2.8.4. ARP Spoofing Protection

ARP spoofing is a common LAN virus. A computer with a virus will send broadcast packets with ARP spoofing to the LAN from time to time, causing the normal communication of the LAN machine to be interfered and damaged. In severe cases, the entire network will be disconnected.

MIG protects the ARP cache of the MIG local by rejecting ARP requests or replies with attack signatures to achieve its own immunity. If there is a bound IP/MAC in the authorization list of the MIG access control, the MIG will take the bound IP/MAC information as the standard.

The configuration interface is shown as follows:



>>ARP Spoofing Prevention

ARP Spoofing Prevention: ○ Enable ● Disable

□ Static ARP Table:

Specify items in the following static ARP table (gateway and VLAN addresses are not required).
Format: One IP address(MAC address) per row. Example: 200.200.20.1(00-32-83-EF-A9-88).

□ Use IP/MAC address(es) in IP&MAC Binding

MAC Broadcast Interval: 10 second(s)

『Enable ARP Spoofing Protection』: is the master switch that enables the ARP spoofing protection.

『Static ARP Settings』: You can check [Enable]. If the LAN PC's gateway is not the MIG interface, you need to set it here. Otherwise, when receiving the LAN PC gateway IP, the MIG will regard it as not the corresponding IP/MAC, resulting in packet loss; if the gateway of the LAN PC is MIG, there is no need to set it here.

『Gateway MAC Broadcasting Time』: is the time interval for setting the MAC of the broadcast gateway (i.e, the LAN interface of the AC). It is recommended to set it to 10 seconds.

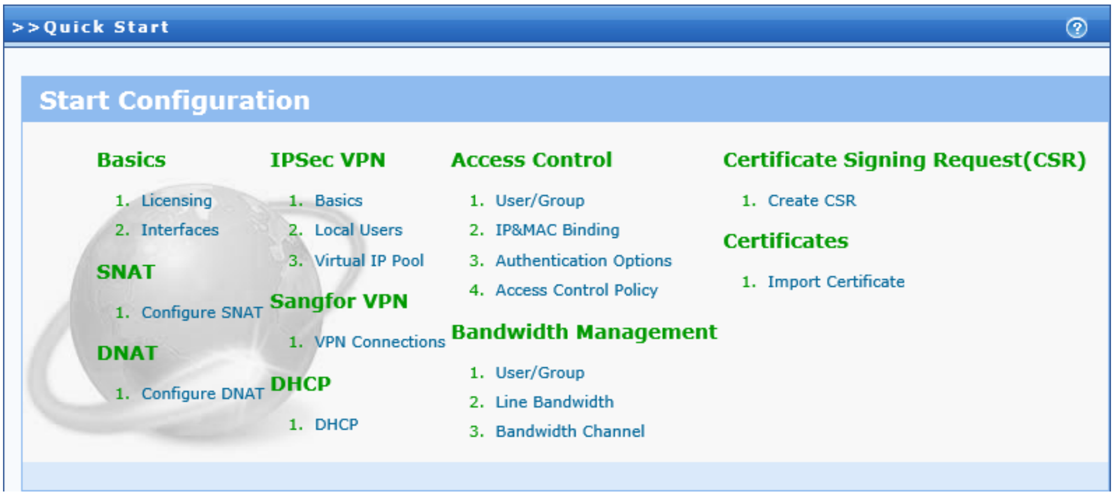
Click OK to save the configuration.

Click the Broadcasting Gateway MAC, the MAC address of the device LAN interface will immediately be broadcasted. When LAN ARP spoofing is cleared, this button can be used to quickly restore the LAN PC's ARP table.

2.9. System maintenance

2.9.1. Newbie Wizard

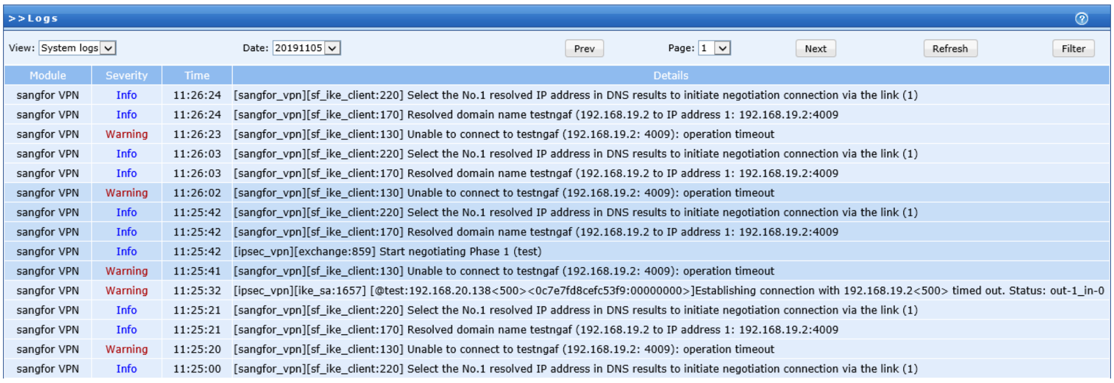
Here you can follow the wizard to complete your configuration



According to the configuration prompt of the Newbie Wizard, you can click the appropriate link and complete the configuration based on your needs.

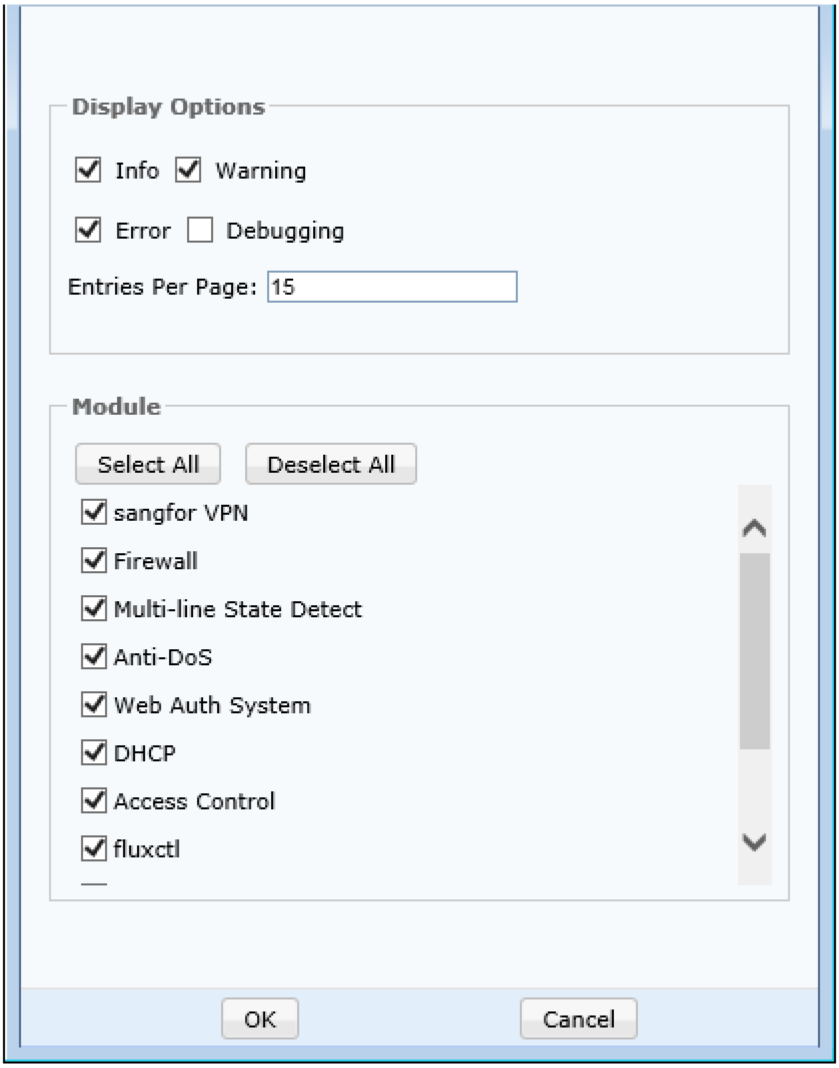
2.9.2. View Log

『View Log』 is used to view the running log and error prompt of the device. The running log includes two types, one is the service log, which can view the system log information of the current device. Select the date you want to view and the log record at the corresponding time will be displayed. The page is shown as follows:



Module	Severity	Time	Details
sangfor VPN	Info	11:26:24	[sangfor_vpn][sf_ike_client:220] Select the No.1 resolved IP address in DNS results to initiate negotiation connection via the link (1)
sangfor VPN	Info	11:26:24	[sangfor_vpn][sf_ike_client:170] Resolved domain name testngaf (192.168.19.2 to IP address 1: 192.168.19.2:4009
sangfor VPN	Warning	11:26:23	[sangfor_vpn][sf_ike_client:130] Unable to connect to testngaf (192.168.19.2: 4009): operation timeout
sangfor VPN	Info	11:26:03	[sangfor_vpn][sf_ike_client:220] Select the No.1 resolved IP address in DNS results to initiate negotiation connection via the link (1)
sangfor VPN	Info	11:26:03	[sangfor_vpn][sf_ike_client:170] Resolved domain name testngaf (192.168.19.2 to IP address 1: 192.168.19.2:4009
sangfor VPN	Warning	11:26:02	[sangfor_vpn][sf_ike_client:130] Unable to connect to testngaf (192.168.19.2: 4009): operation timeout
sangfor VPN	Info	11:25:42	[sangfor_vpn][sf_ike_client:220] Select the No.1 resolved IP address in DNS results to initiate negotiation connection via the link (1)
sangfor VPN	Info	11:25:42	[sangfor_vpn][sf_ike_client:170] Resolved domain name testngaf (192.168.19.2 to IP address 1: 192.168.19.2:4009
sangfor VPN	Info	11:25:42	[ipsec_vpn][exchange:859] Start negotiating Phase 1 (test)
sangfor VPN	Warning	11:25:41	[sangfor_vpn][sf_ike_client:130] Unable to connect to testngaf (192.168.19.2: 4009): operation timeout
sangfor VPN	Warning	11:25:32	[ipsec_vpn][ike_sa:1657] [@test:192.168.20.138<500><0c7e7fd8cefc53f9:00000000>]Establishing connection with 192.168.19.2<500> timed out. Status: out-1_in-0
sangfor VPN	Info	11:25:21	[sangfor_vpn][sf_ike_client:220] Select the No.1 resolved IP address in DNS results to initiate negotiation connection via the link (1)
sangfor VPN	Info	11:25:21	[sangfor_vpn][sf_ike_client:170] Resolved domain name testngaf (192.168.19.2 to IP address 1: 192.168.19.2:4009
sangfor VPN	Warning	11:25:20	[sangfor_vpn][sf_ike_client:130] Unable to connect to testngaf (192.168.19.2: 4009): operation timeout
sangfor VPN	Info	11:25:00	[sangfor_vpn][sf_ike_client:220] Select the No.1 resolved IP address in DNS results to initiate negotiation connection via the link (1)

Click Filter, you can set the specified system log range for viewing. The page is shown as follows:



Display Options

☑ Info ☑ Warning

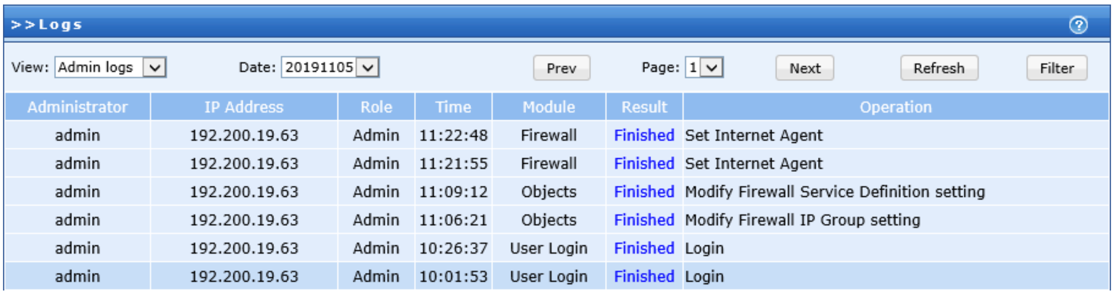
☑ Error □ Debugging

Entries Per Page: 15

Module

☑ sangfor VPN
☑ Firewall
☑ Multi-line State Detect
☑ Anti-DoS
☑ Web Auth System
☑ DHCP
☑ Access Control
☑ fluxctl

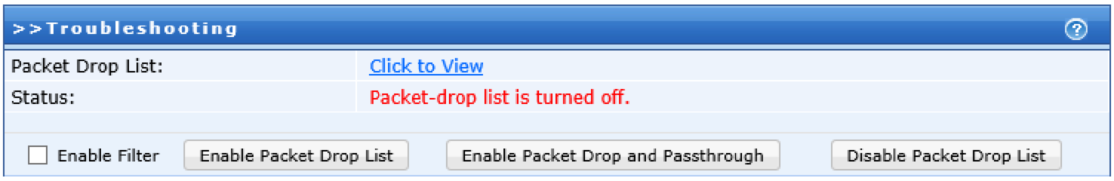
The other is log management, you can view the operation log information of the current device administrator on the device. Select the date you want to view and the log record at the corresponding time will be displayed.



Administrator	IP Address	Role	Time	Module	Result	Operation
admin	192.200.19.63	Admin	11:22:48	Firewall	Finished	Set Internet Agent
admin	192.200.19.63	Admin	11:21:55	Firewall	Finished	Set Internet Agent
admin	192.200.19.63	Admin	11:09:12	Objects	Finished	Modify Firewall Service Definition setting
admin	192.200.19.63	Admin	11:06:21	Objects	Finished	Modify Firewall IP Group setting
admin	192.200.19.63	Admin	10:26:37	User Login	Finished	Login
admin	192.200.19.63	Admin	10:01:53	User Login	Finished	Login

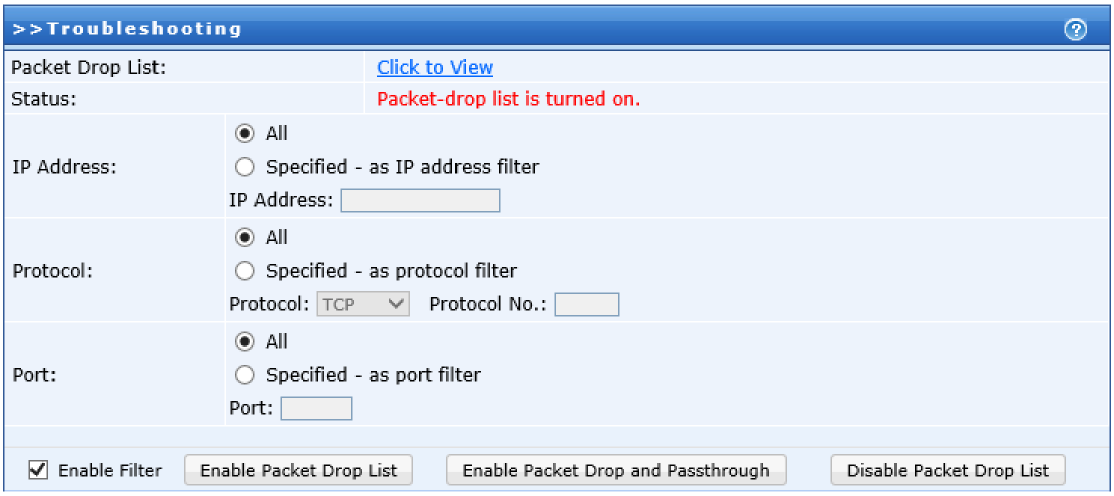
2.9.3. Policy Troubleshooting

『Policy Troubleshooting』 is used to search by which module the data packet is rejected when passing through the gateway and why it is rejected, so as to quickly locate the configuration error, or to test whether some rules take effect, as shown in the following figure:



Packet Drop List: Click to View
Status: Packet-drop list is turned off.

Click Enable Filter to set various conditions for filtering, including 『IP Address』, 『Protocol Type』 and 『port』, as shown below:



>>Troubleshooting

Packet Drop List:	Click to View
Status:	Packet-drop list is turned on.
IP Address:	● All ○ Specified - as IP address filter IP Address:
Protocol:	● All ○ Specified - as protocol filter Protocol: TCP Protocol No.:
Port:	● All ○ Specified - as port filter Port:

☑ Enable Filter

『IP Address』: used to set the reject list for the specified IP address. By default, all network segments are included.

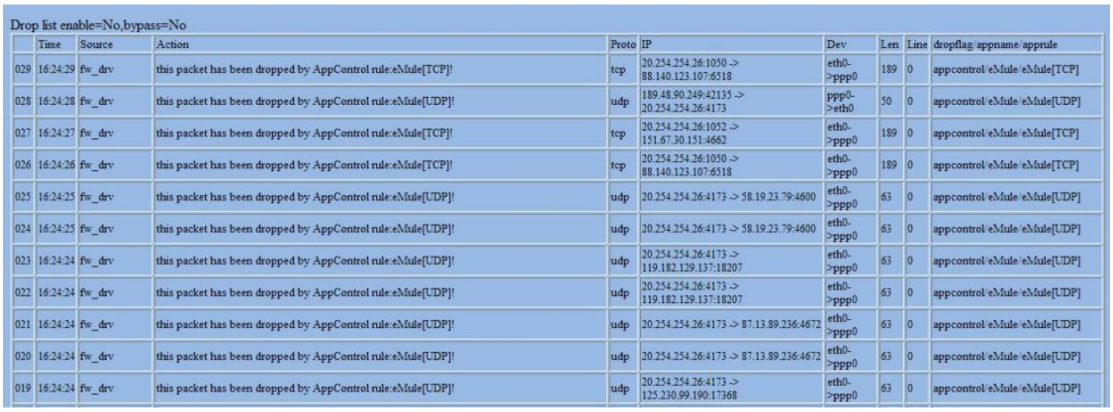
『Protocol Type』 and 『port』: only setting the rejection conditions of packets that match the specified protocol type and port can such packets be output to the access control list.

Clicking Click to View will open the reject list. At this moment, all the policies of the device will still be effective, and packets that should be rejected according to the policy settings will be rejected by the device. At the same time, the conditions where the packet should be rejected according to the policy settings will be output to a WEB page. On the page, click View here, you can open the page to see such rejection conditions.

Click Open the reject list and the direct connection, you can open the reject list and enable the direct connection. At this time, the set access policy, traffic control policy and authentication options will not take effect. Packets that conform to the policy settings and should be rejected will be released by the device. Meanwhile, packets that conform to the policy settings and should be rejected will be output to a WEB page. Through this function, it is possible to quickly locate which module configuration error causes network interruption and other errors, and manually recover the network failure caused by the policy configuration error. Click View here to automatically open the browser to view the rejection of the packet.

Close the reject list is used to close the output of the reject list and close pass-through.

Click View here to automatically open the browser to view the rejection of the packet. as follows:



Drop list enable=No,bypass=No

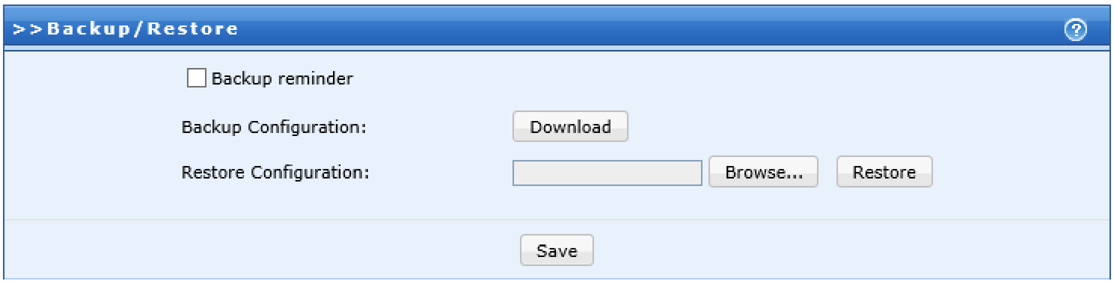
	Time	Source	Action	Proto	IP	Dev	Len	Line	dropflag/appname/apprule
029	16:24:29	fw_drv	this packet has been dropped by AppControl rule:eMule[TCP]!	tcp	20.254.254.26:1050 -> 88.140.123.107:6518	eth0->ppp0	189	0	appcontrol/eMule/eMule[TCP]
028	16:24:28	fw_drv	this packet has been dropped by AppControl rule:eMule[UDP]!	udp	189.48.90.249:42135 -> 20.254.254.26:4173	ppp0->eth0	50	0	appcontrol/eMule/eMule[UDP]
027	16:24:27	fw_drv	this packet has been dropped by AppControl rule:eMule[TCP]!	tcp	20.254.254.26:1052 -> 151.67.30.151:4662	eth0->ppp0	189	0	appcontrol/eMule/eMule[TCP]
026	16:24:26	fw_drv	this packet has been dropped by AppControl rule:eMule[TCP]!	tcp	20.254.254.26:1050 -> 88.140.123.107:6518	eth0->ppp0	189	0	appcontrol/eMule/eMule[TCP]
025	16:24:25	fw_drv	this packet has been dropped by AppControl rule:eMule[UDP]!	udp	20.254.254.26:4173 -> 58.19.23.79:4600	eth0->ppp0	63	0	appcontrol/eMule/eMule[UDP]
024	16:24:25	fw_drv	this packet has been dropped by AppControl rule:eMule[UDP]!	udp	20.254.254.26:4173 -> 58.19.23.79:4600	eth0->ppp0	63	0	appcontrol/eMule/eMule[UDP]
023	16:24:24	fw_drv	this packet has been dropped by AppControl rule:eMule[UDP]!	udp	20.254.254.26:4173 -> 119.182.129.137:18207	eth0->ppp0	63	0	appcontrol/eMule/eMule[UDP]
022	16:24:24	fw_drv	this packet has been dropped by AppControl rule:eMule[UDP]!	udp	20.254.254.26:4173 -> 119.182.129.137:18207	eth0->ppp0	63	0	appcontrol/eMule/eMule[UDP]
021	16:24:24	fw_drv	this packet has been dropped by AppControl rule:eMule[UDP]!	udp	20.254.254.26:4173 -> 87.13.89.236:4672	eth0->ppp0	63	0	appcontrol/eMule/eMule[UDP]
020	16:24:24	fw_drv	this packet has been dropped by AppControl rule:eMule[UDP]!	udp	20.254.254.26:4173 -> 87.13.89.236:4672	eth0->ppp0	63	0	appcontrol/eMule/eMule[UDP]
019	16:24:24	fw_drv	this packet has been dropped by AppControl rule:eMule[UDP]!	udp	20.254.254.26:4173 -> 125.230.99.190:17368	eth0->ppp0	63	0	appcontrol/eMule/eMule[UDP]

1. Generally speaking, the "Opening Conditions" need to be set in detail, which can effectively filter useless information and make the debugging process simpler.

2. After using this function, remember to close the reject list. Because this function will consume certain system resources. In addition, if the pass-through function is turned on without turning off the reject list, all restriction functions will be invalidated.

2.9.4. Backup/Recovery Configuration

The configuration that can be used as a backup and recovery MIG gateway device. The page is shown as follows:



『Backup Reminder』: It can set the interval within which there is no backup configuration, and then remind you after logging into the device configuration interface.

『Backup Configuration』: Click Backup Configuration to back up the current configuration of the device to the local device.

『Restore Configuration』: Click Restore Configuration to restore the local backup configuration file to the device. Click Restore Configuration to restore the configuration automatically backed up by the device at the last backup point to the current configuration.

1. When restoring the configuration, ensure that the version model of the configuration file must be the same as the version model of the current device, otherwise it may cause an exception.

2. To prevent accidental configuration changes, it is recommended that you back up the configuration regularly.

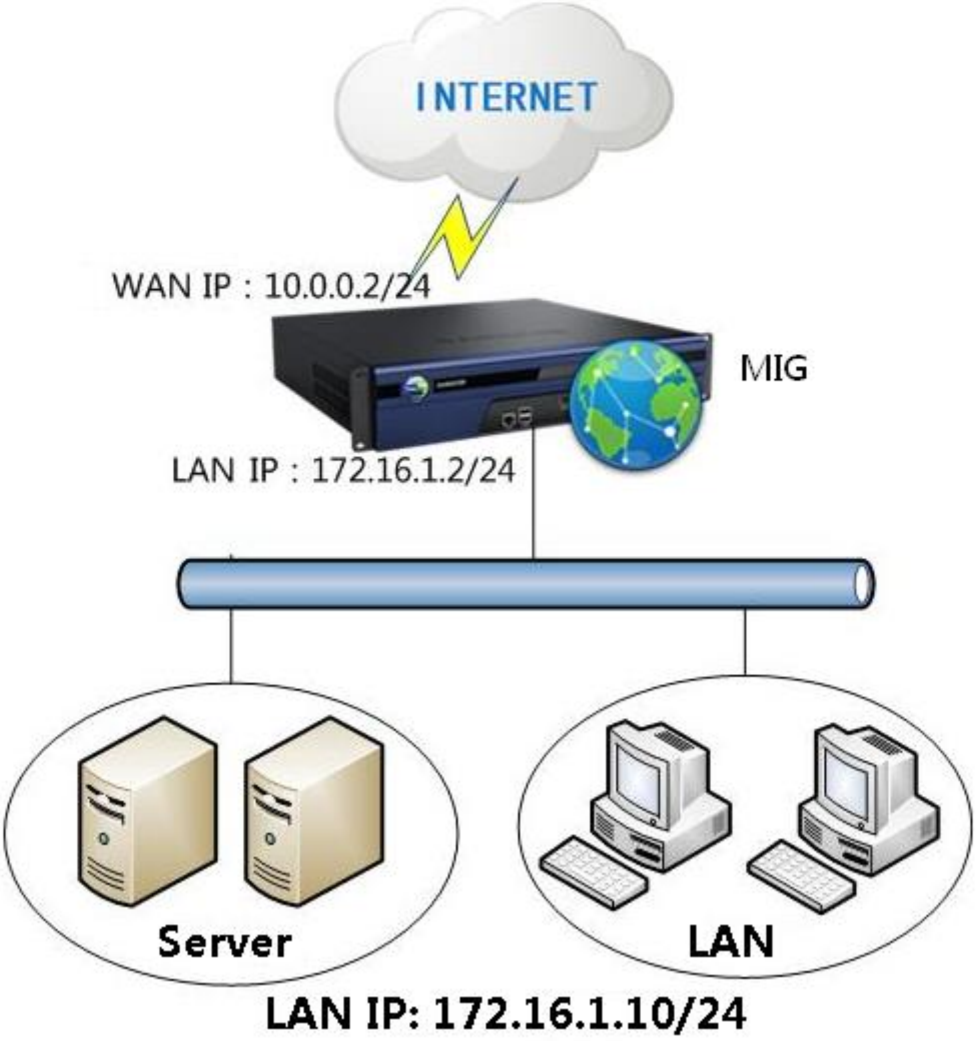
⚠Attention: The configuration of the same model and version is required to realize mutual conductance. For example, the configuration of MIG 1200 cannot be imported into MIG 1110 device, and the configuration of DLAN 4.3 version cannot be imported into DLAN 4.6 version device.

MIG version 4.0 began to support penetration of H323, GRE, PPTP, FTP, TFTP and other commonly used protocols.

3 Case Set

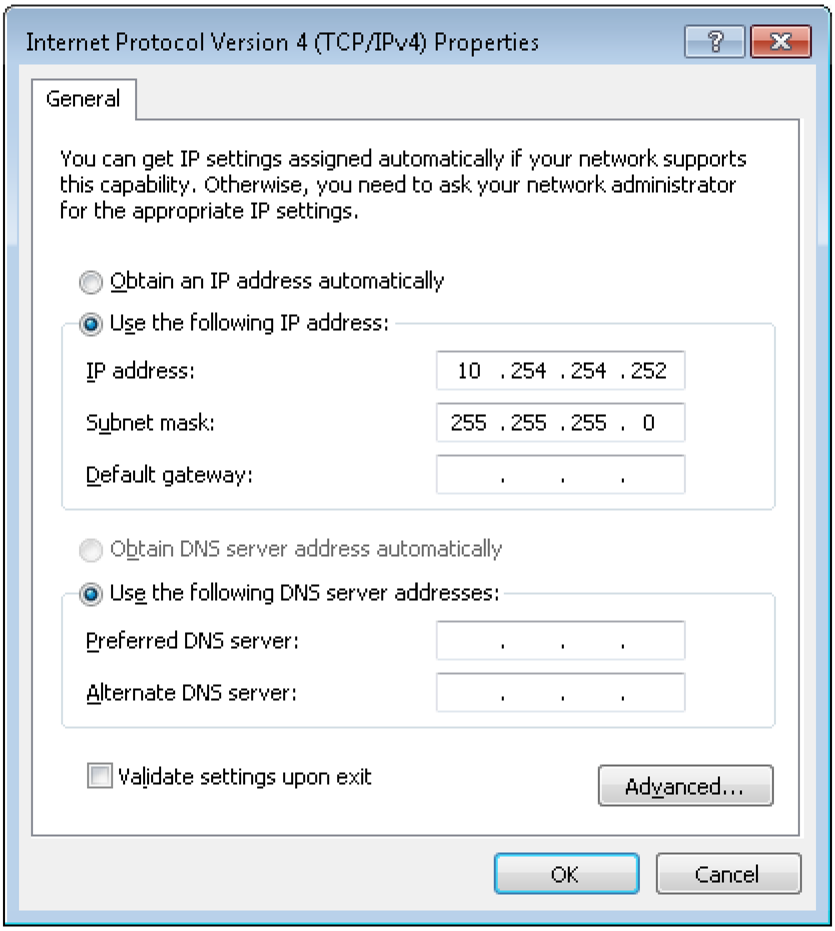
3.1. Routing Mode Deployment Case

Customer environment and requirements: the topology of a customer network is as follows: There is an operator link, and the original router is used as an egress. It is hoped that MIG device gateway mode will be deployed at the network egress to proxy LAN users and servers to access the internet, and finally establish VPN connection with other MIG device.



Configuration method:

Step 1: Start the device first, connect the EHT0 interface (LAN) of the device with the network cable, and configure the IP of the computer network card to 10.254.254.252 with the following interface:



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 10 . 254 . 254 . 252

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

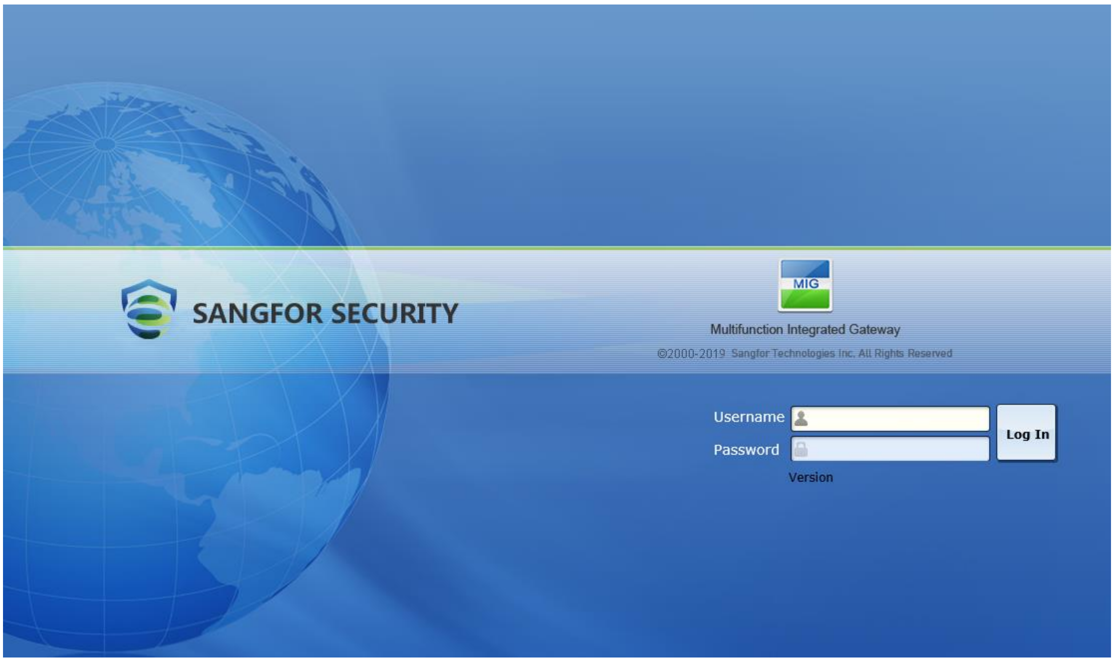
● Use the following DNS server addresses:

Preferred DNS server: . . .

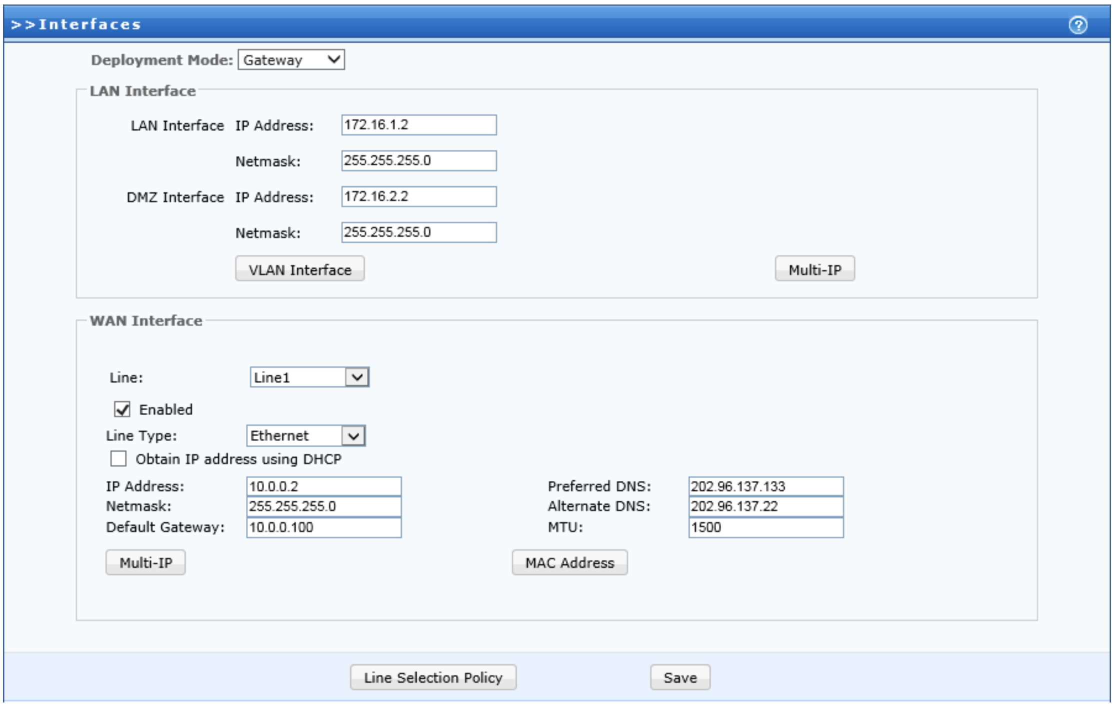
Alternate DNS server: . . .

□ Validate settings upon exit

Step 2: Log in setup page, open IE browser and enter https://10.254.254.253 to enter the login interface. Enter the factory default account and password admin/admin for the device. The interface is as follows:


SANGFOR SECURITY
MIG
Multifunction Integrated Gateway
©2000-2019 Sangfor Technologies Inc. All Rights Reserved
Username
Password
Log In
Version

Step 3: Interface configuration, enter 『System Setup』 → 『Network Interface Deployment』, select the working mode of the device as gateway mode, set the addresses of LAN interface and WAN interface, DNS and other information, and click OK. The interface is as follows:



>>Interfaces

Deployment Mode: Gateway

LAN Interface

LAN Interface IP Address: 172.16.1.2

Netmask: 255.255.255.0

DMZ Interface IP Address: 172.16.2.2

Netmask: 255.255.255.0

VLAN Interface | Multi-IP

WAN Interface

Line: Line1

☑ Enabled

Line Type: Ethernet

□ Obtain IP address using DHCP

IP Address: 10.0.0.2 | Preferred DNS: 202.96.137.133

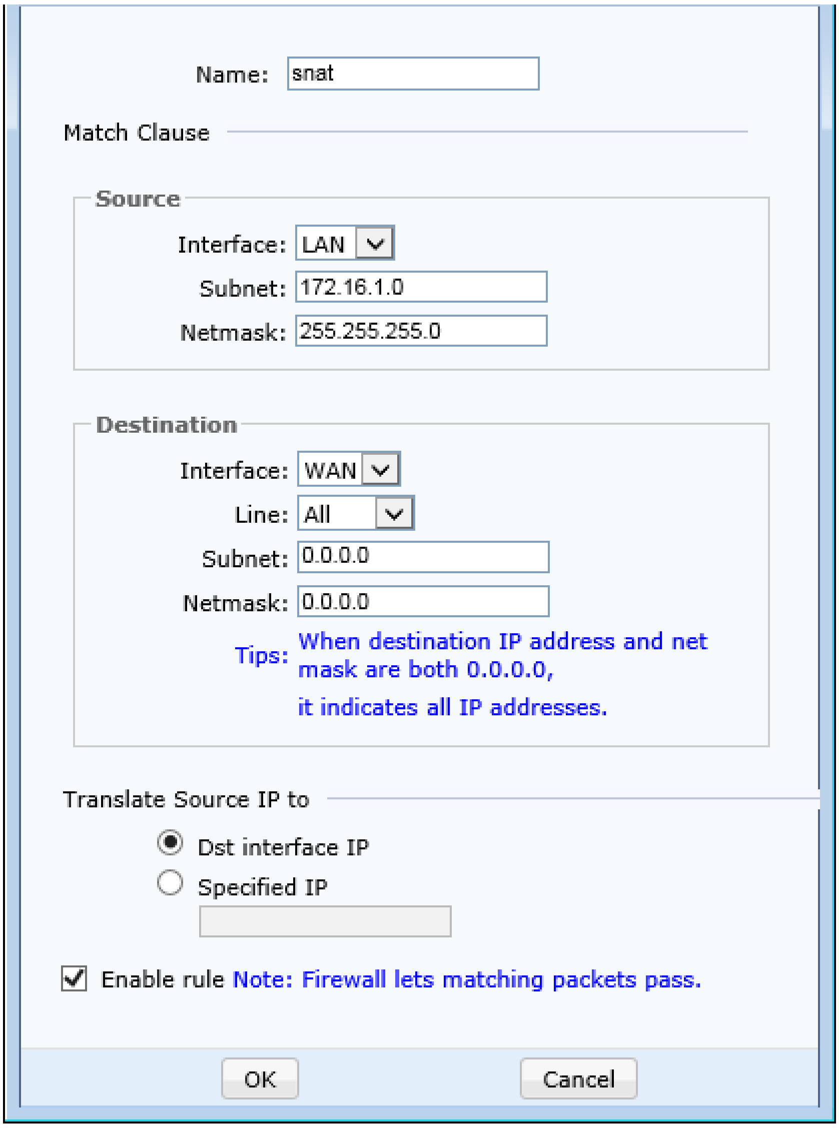
Netmask: 255.255.255.0 | Alternate DNS: 202.96.137.22

Default Gateway: 10.0.0.100 | MTU: 1500

Multi-IP | MAC Address

Line Selection Policy | Save

Step 4: Proxy Internet Settings, enter 『Firewall Settings』→ 『NAT Settings』→ 『Proxy Internet Settings』 , add a rule, define the name of the rule, select the LAN interface, and set the subnet segment and subnet mask. Click OK. The interface is as follows:



Name: snat

Match Clause

Source

Interface: LAN

Subnet: 172.16.1.0

Netmask: 255.255.255.0

Destination

Interface: WAN

Line: All

Subnet: 0.0.0.0

Netmask: 0.0.0.0

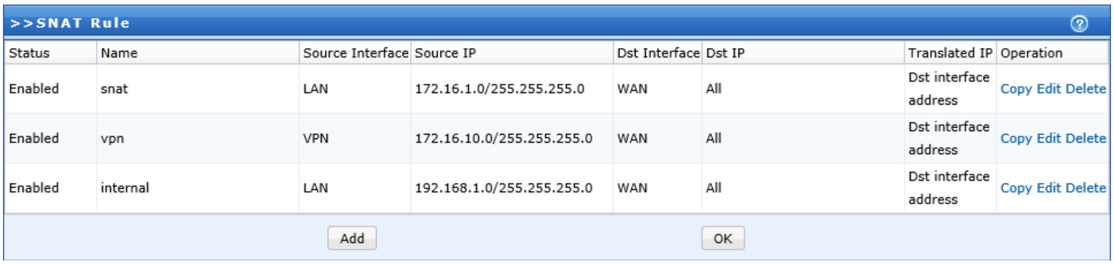
Tips: When destination IP address and net mask are both 0.0.0.0, it indicates all IP addresses.

Translate Source IP to

● Dst interface IP

○ Specified IP

☑ Enable rule Note: Firewall lets matching packets pass.



>>SNAT Rule

Status	Name	Source Interface	Source IP	Dst Interface	Dst IP	Translated IP	Operation
Enabled	snat	LAN	172.16.1.0/255.255.255.0	WAN	All	Dst interface address	Copy Edit Delete
Enabled	vpn	VPN	172.16.10.0/255.255.255.0	WAN	All	Dst interface address	Copy Edit Delete
Enabled	internal	LAN	192.168.1.0/255.255.255.0	WAN	All	Dst interface address	Copy Edit Delete

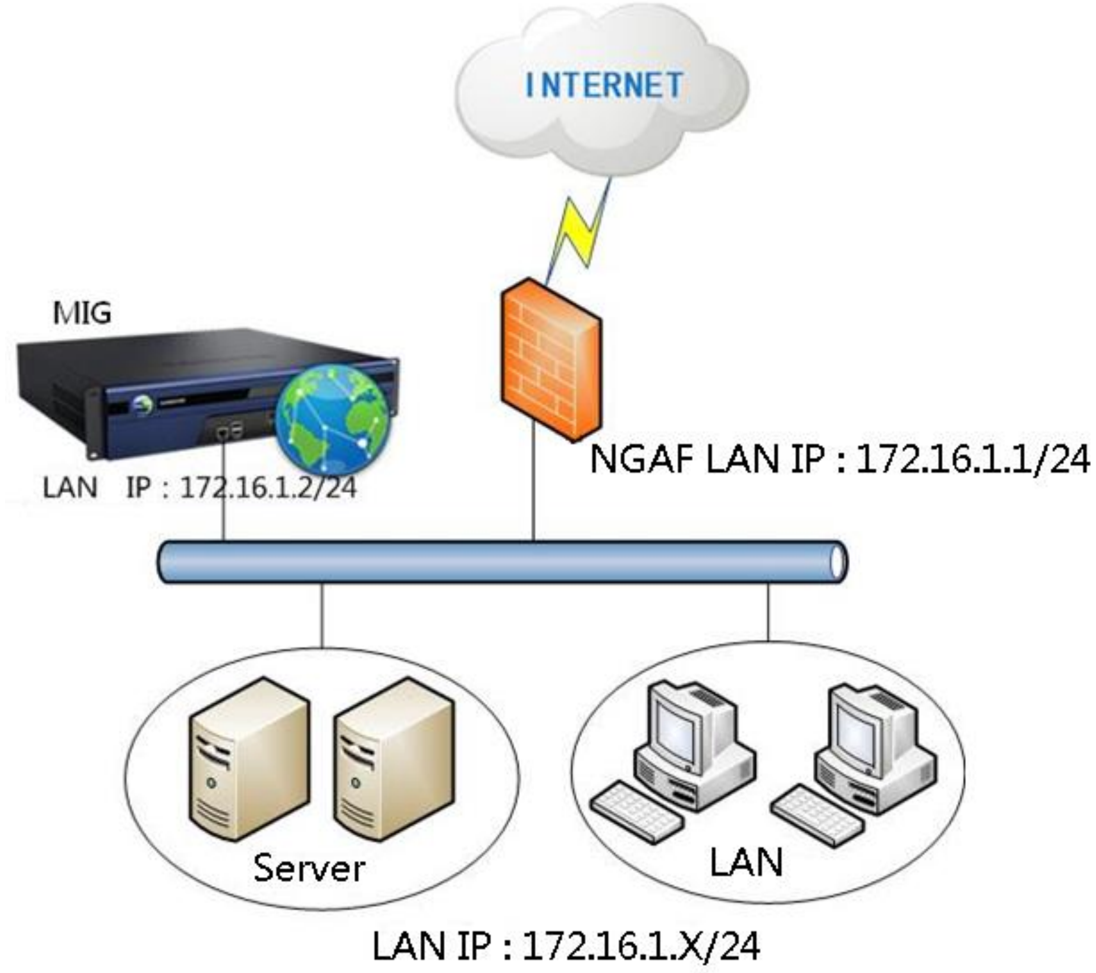
After the above steps are configured, the LAN interface of the device can be connected to the LAN switch, the WAN interface can be connected to the public network link, and the gateway of the LAN computer can be pointed to the LAN interface of the device, so that the device can proxy the LAN to access the Internet.

⚠**When configuring external network lines, the line type can be Ethernet or ADSL according to actual needs.**

After configuring the external interface of the device's LAN, the local IP needs to be modified to the IP of the same network segment as the configured LAN interface.

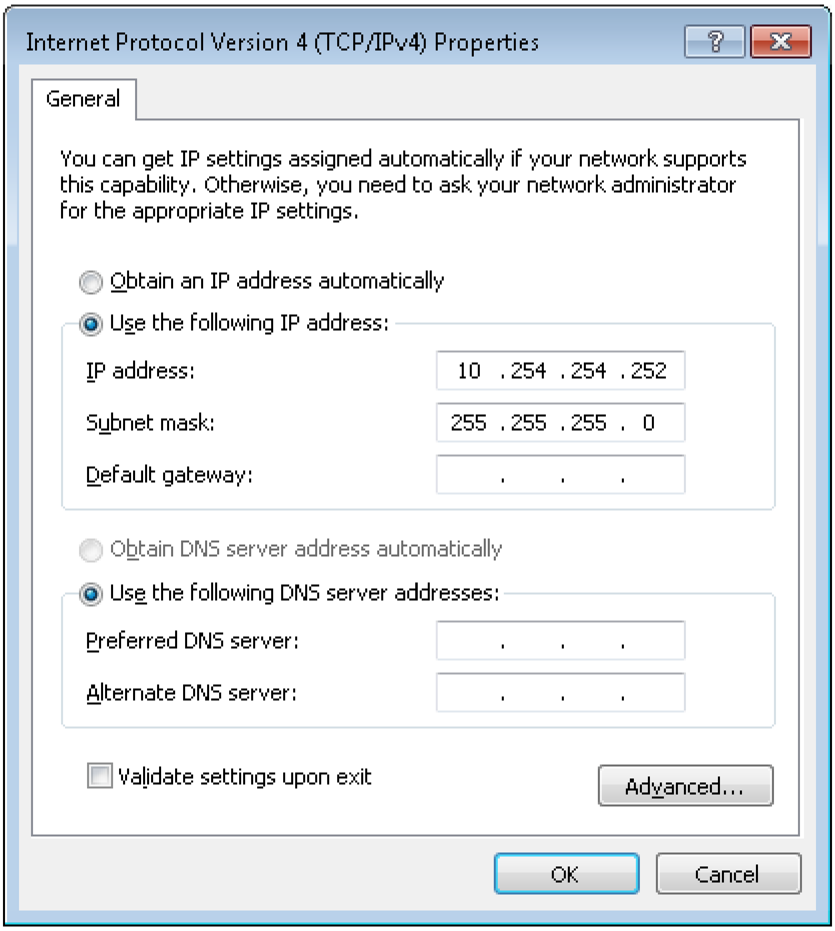
3.2. Deployment Case of One-arm Mode

Customer environment and demand: A customer's topology is as follows: There is an operator link, and LAN users use firewall to access the Internet via proxy. Customers hope that the one-arm mode of MIG device will be deployed to the LAN and eventually realize VPN interconnection with other devices.



Configuration method:

Step 1: Start the device first, connect the EHT0 interface (LAN) of the device with the network cable, and configure the IP of the computer network card to 10.254.254.252 with the following interface:



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 10 . 254 . 254 . 252

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

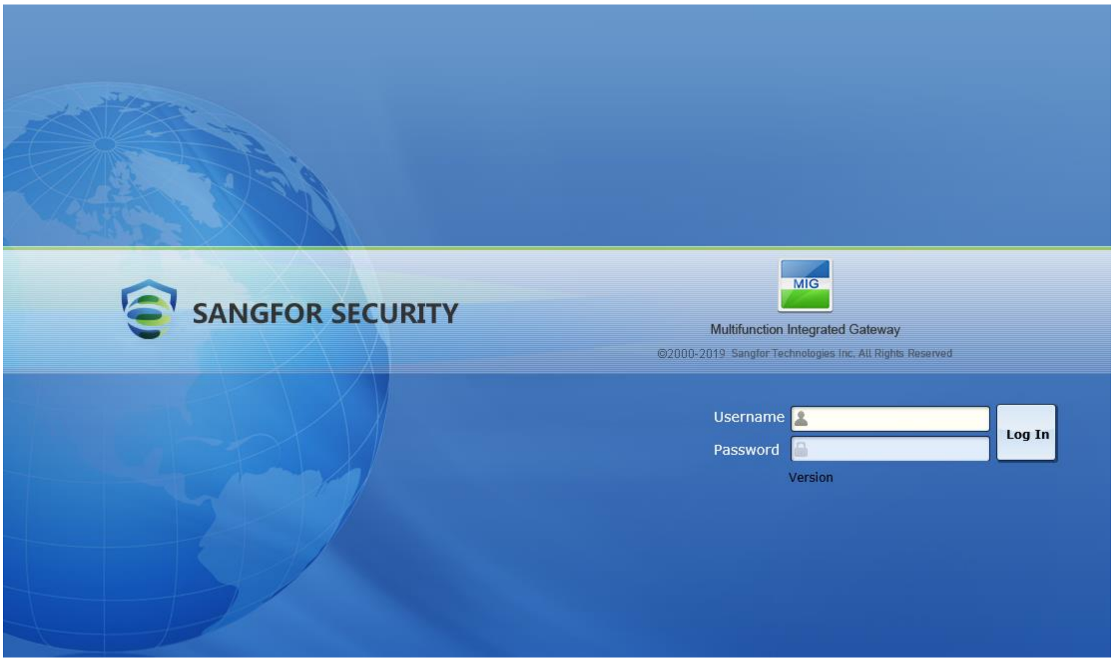
● Use the following DNS server addresses:

Preferred DNS server: . . .

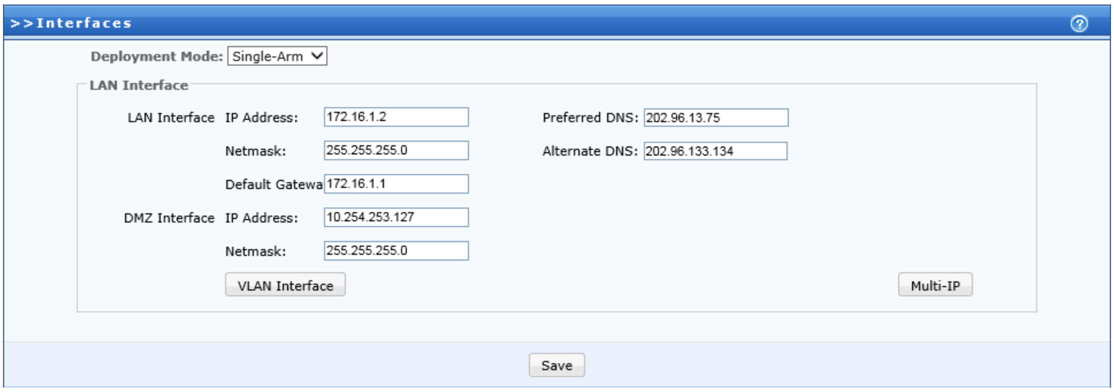
Alternate DNS server: . . .

□ Validate settings upon exit

Step 2: Log in setup page, open IE browser and enter https://10.254.254.253 to enter the login interface. Enter the factory default account and password admin/admin for the device. The interface is as follows:


SANGFOR SECURITY
MIG
Multifunction Integrated Gateway
©2000-2019 Sangfor Technologies Inc. All Rights Reserved
Username
Password
Log In
Version

Step 3: Select the working mode and configure the interface address, enter 『System Setup』→『Network Interface Setting』, select the device working mode as one-arm mode, configure the IP address, subnet mask and gateway of LAN interface, and configure the correct DNS, click OK, and the interface is as follows:


>>Interfaces

Deployment Mode: Single-Arm

LAN Interface

LAN Interface IP Address: 172.16.1.2

Netmask: 255.255.255.0

Default Gatewa 172.16.1.1

Preferred DNS: 202.96.13.75

Alternate DNS: 202.96.133.134

DMZ Interface IP Address: 10.254.253.127

Netmask: 255.255.255.0

Step 4: Since MIG device is connected to the LAN, if the device is deployed at the headquarters during VPN connection, port mapping needs to be done on the front router or firewall, and the port of VPN connection is TCP/UDP 4009. If network-to-network connection is done, network segments routed to the opposite LAN of VPN need to be added on the front gateway device, and the next hop will be handed over to the local VPN. The setting methods of each manufacturer are different, so no screenshot will be made here.

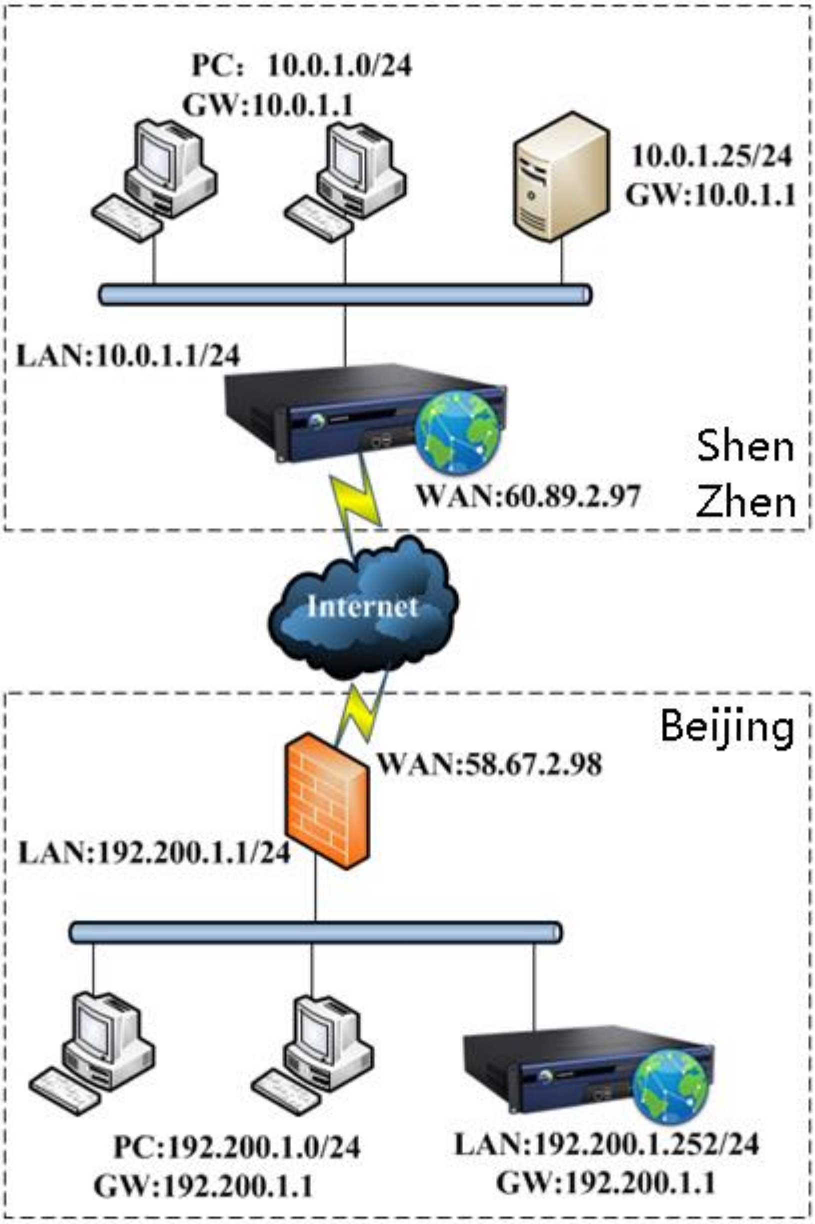
After the above steps are configured, you can connect the LAN interface of the device to the switch and check whether the communication between the device and the LAN is normal.

TCP/UDP 4009 port is the factory default VPN listening port of the device and can be modified. If it is modified, the port mapping needs to map the modified listening port.

One-arm mode must connect the LAN interface of the device to the LAN switch.

3.3. SANGFOR VPN Interconnection Case

The customer's network topology is as follows. He has one MIG device in Shenzhen and one MIG device in Beijing, which are deployed to two local areas in gateway mode and one-arm mode respectively. The customer hopes that the 192.200.1.0/24 PC can access the server 10.0.1.25.



Configuration ideas:

1. Deploy the device to shelves according to the methods in Sections 3.1 and 3.2

2. In order for computers on both ends of the LAN to communicate, VPN connection must be established first.

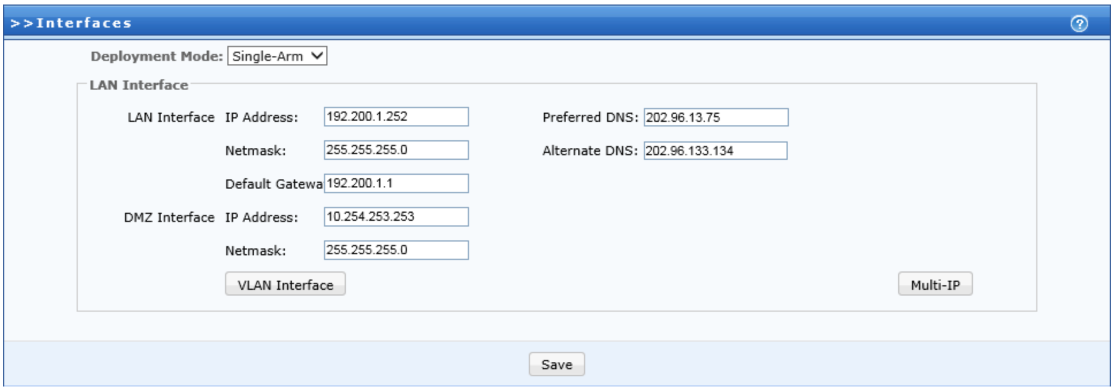
3. Select one MIG device to be the VPN headquarters and the other MIG device to be the VPN branch.

4. Headquarters needs to configure WEBAGENT information and users, meanwhile ensuring that VPN listening ports can be accessed by branch devices, and let LAN PC data pass through VPN. The branch only needs to configure connection management.

The following configuration is based on Beijing device as the headquarters and Shenzhen device as the branch.

Configuration Steps of Headquarter VPN

Step 1: Configure the Sangfor MIG device into gateway mode and put it on the shelf. Please refer to Section 3.1 for details. The interface deployment of Beijing device is as follows:



>>Interfaces

Deployment Mode: Single-Arm

LAN Interface

LAN Interface IP Address: 192.200.1.252

Netmask: 255.255.255.0

Default Gatewa 192.200.1.1

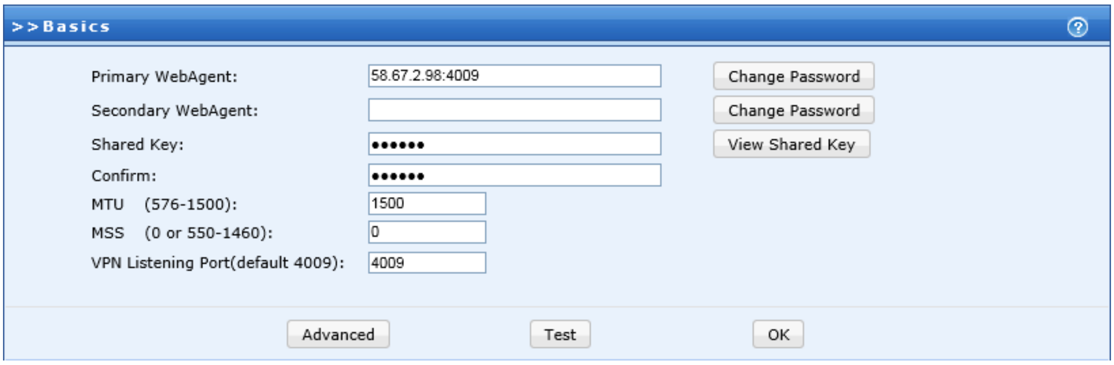
DMZ Interface IP Address: 10.254.253.253

Netmask: 255.255.255.0

Preferred DNS: 202.96.13.75

Alternate DNS: 202.96.133.134

Step 2: Configure the WEBAGENT, enter 『VPN Information Settings』 → 『Basic Settings』, and set the information of the main WEBAGENT. The MTU and the minimum compression value can be set by default. The listening port adopts the default value. The configuration interface of this case is as follows:



>>Basics

Primary WebAgent: 58.67.2.98:4009 [Change Password]

Secondary WebAgent: [Change Password]

Shared Key: •••••• [View Shared Key]

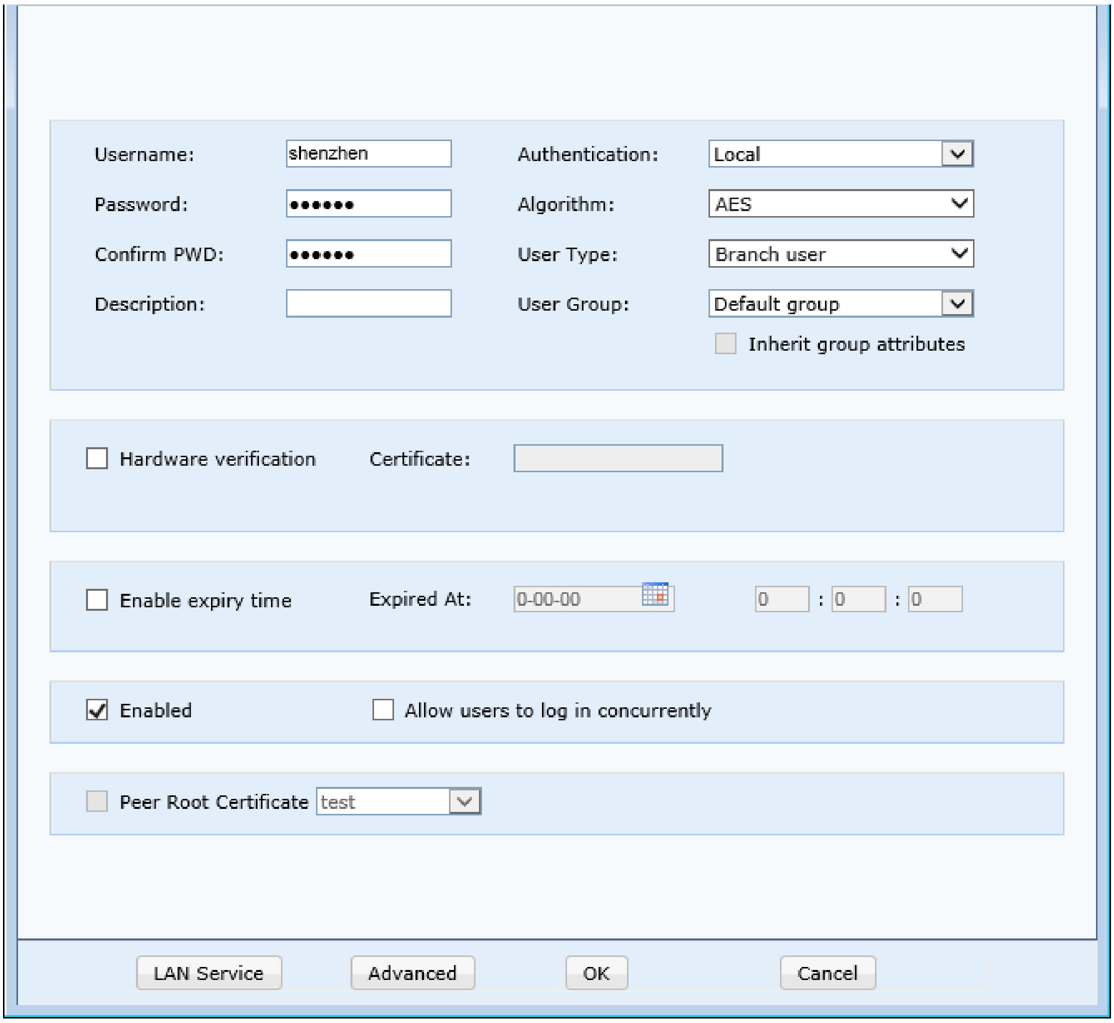
Confirm: ••••••

MTU (576-1500): 1500

MSS (0 or 550-1460): 0

VPN Listening Port(default 4009): 4009

Step 3: Set up a VPN account for the branch, enter 『VPN Information Settings』→『User Management』, add a VPN account, select the type as the branch, and the configuration interface is as follows:



Username: shenzhen

Password: ••••••

Confirm PWD: ••••••

Description:

Authentication: Local

Algorithm: AES

User Type: Branch user

User Group: Default group

□ Inherit group attributes

□ Hardware verification Certificate:

□ Enable expiry time Expired At: 0-00-00 0 : 0 : 0

☑ Enabled □ Allow users to log in concurrently

□ Peer Root Certificate test

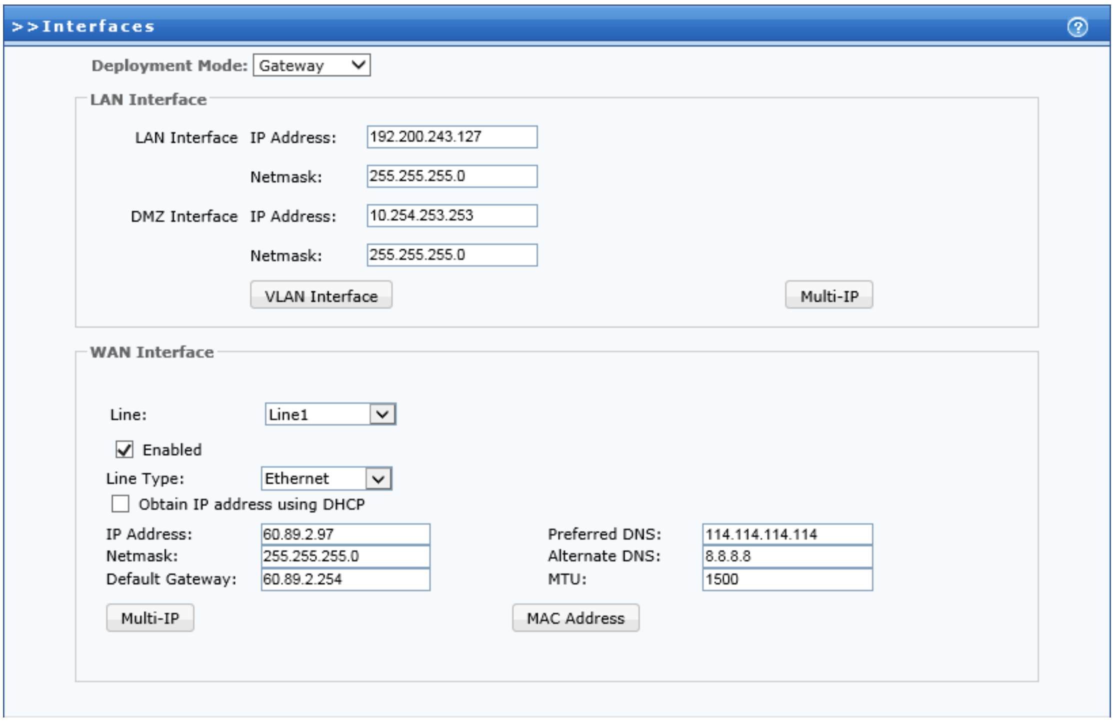
Step 4: Map TCP and UDP 4009 ports of 58.67.2.98 to MIG device in the front-end firewall. Different manufacturers have different configurations, so we will not give an example here.

Step 5: As the MIG device at this end is deployed in one-arm mode, the gateway of the LAN PC points to Firewall. In order to ensure that data accessing 10.0.1.25 passes through MIG device, static routes need to be added to firewall. The target network is 10.0.1.0/24 and the next address is 192.200.1.252.

After the above steps, the headquarters configuration is completed.

Configuration Steps for Branch VPN

Step 1: Configure the Sangfor MIG device into gateway mode and put it on the shelf. The interface address of Shenzhen device is set as follows:



>>Interfaces

Deployment Mode: Gateway

LAN Interface

LAN Interface IP Address: 192.200.243.127

Netmask: 255.255.255.0

DMZ Interface IP Address: 10.254.253.253

Netmask: 255.255.255.0

WAN Interface

Line: Line1

☑ Enabled

Line Type: Ethernet

☐ Obtain IP address using DHCP

IP Address: 60.89.2.97

Netmask: 255.255.255.0

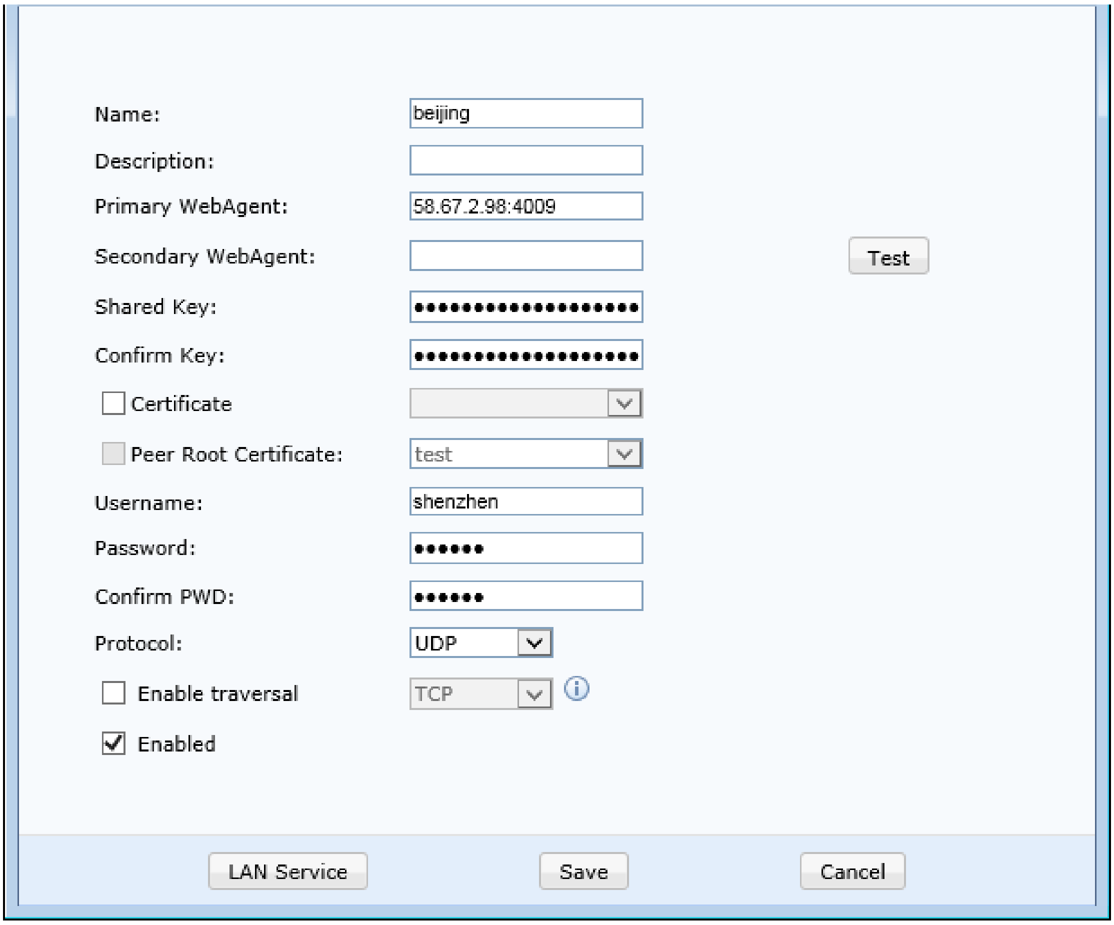
Default Gateway: 60.89.2.254

Preferred DNS: 114.114.114.114

Alternate DNS: 8.8.8.8

MTU: 1500

Step 2: Establish VPN connection, enter "VPN Information Setting"→ "Connection Management", create a new connection, fill in WEBAGNET set by the headquarters, and the VPN account set by the headquarters. The interface is as follows:



Name: beijing

Description:

Primary WebAgent: 58.67.2.98:4009

Secondary WebAgent:

Shared Key: ●●●●●●●●●●●●●●●●●●●

Confirm Key: ●●●●●●●●●●●●●●●●●●●

□ Certificate

□ Peer Root Certificate: test

Username: shenzhen

Password: ●●●●●●

Confirm PWD: ●●●●●●

Protocol: UDP

□ Enable traversal TCP

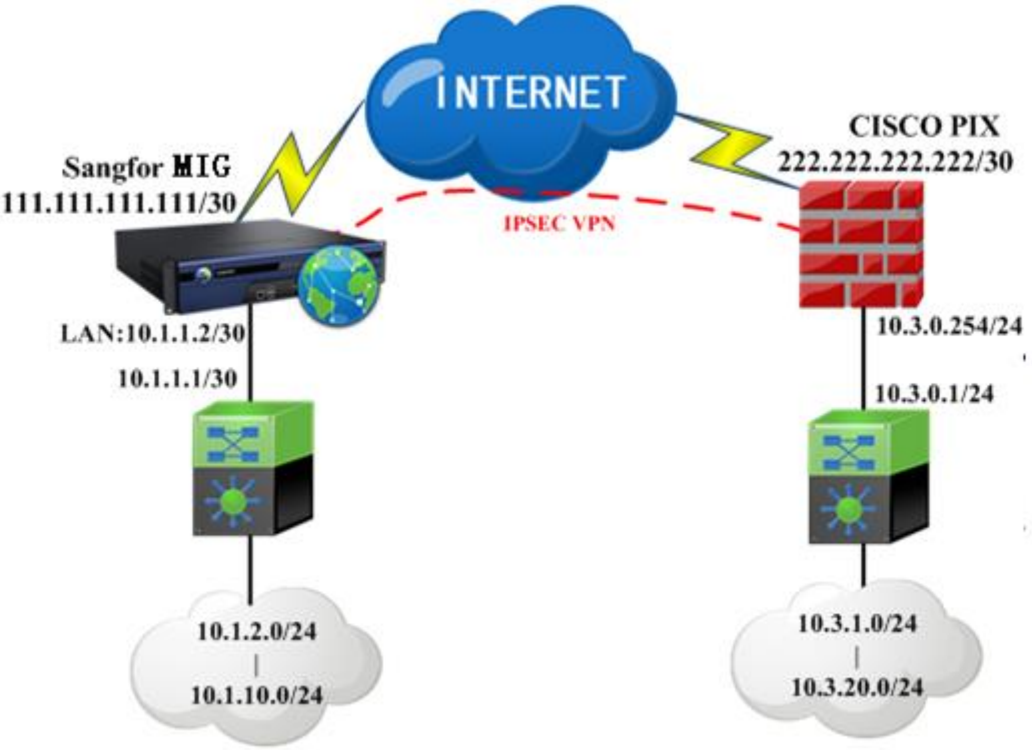
☑ Enabled

After the above configuration is completed, all the steps for the connection between the headquarters and the branch VPN will be completed. If VPN connection is successful, you can check the connection status through DLAN running status.

When two devices are interconnected by VPN, it must be ensured that at least one device's VPN connection port can communicate on the public network.

3.4. Case of IPSEC VPN Interconnection with CISCO PIX Standard

The topology diagram of a company is as follows. Cisco Route and MIG device establish standard IPSEC connections. Each branch needs to access the 10.1.10.0/24 server network segment at the headquarters. The network segment of the headquarters is 10.1.0.0/16 and the network segment of the branch is 10.3.0.0/16.



Cisco VPN configuration:

crypto ipsec transform-set *sangfor* esp-des esp-md5-hmac **crypto map** *mymap 10* **ipsec-isakmp**

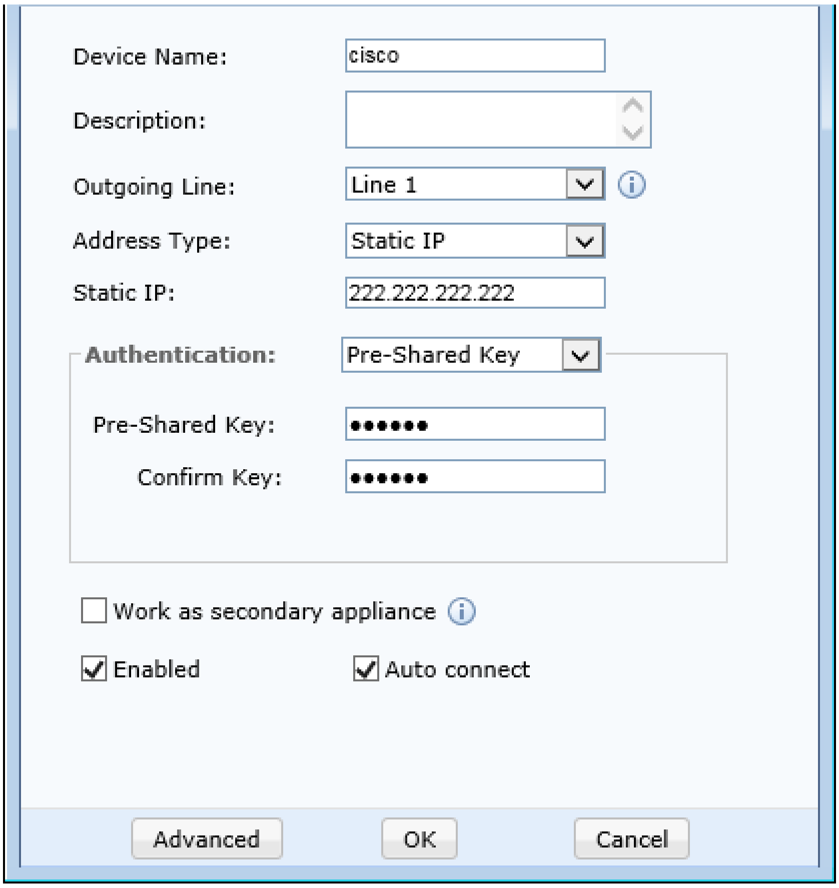
```
crypto map mymap 10 match address 102
crypto map mymap 10 set pfs group2
crypto map mymap 10 set peer 111.111.111.111
crypto map mymap 10 set transform-set sangfor
crypto map mymap interface outside
isakmp enable outside
isakmp key test123 address 222.222.222.222 netmask 255.255.255.252
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash md5
isakmp policy 10 group 2
isakmp policy 10 lifetime 28800
access-list 102 permit ip 10.3.0.0 255.255.0.0 10.1.0.0 255.255.0.0
access-list nonat permit ip 10.3.0.0 255.255.0.0 10.1.0.0 255.255.0.0 global (outside) 1 222.222.222.222
```

nat (inside) *0* **access-list** *nonat*

nat (inside) 1 *10.3.0.0 255.255.0.0 0 0*

VPN configuration for MIG devices:

Step 1: The first phase of configuration, as shown in the following figure:



Device Name: cisco

Description:

Outgoing Line: Line 1

Address Type: Static IP

Static IP: 222.222.222.222

Authentication: Pre-Shared Key

Pre-Shared Key: ●●●●●●

Confirm Key: ●●●●●●

□ Work as secondary appliance

☑ Enabled ☑ Auto connect

『Name』 The first stage policy name is customized to cisco.

『Line Egress』 Line Egress Select Line 1.

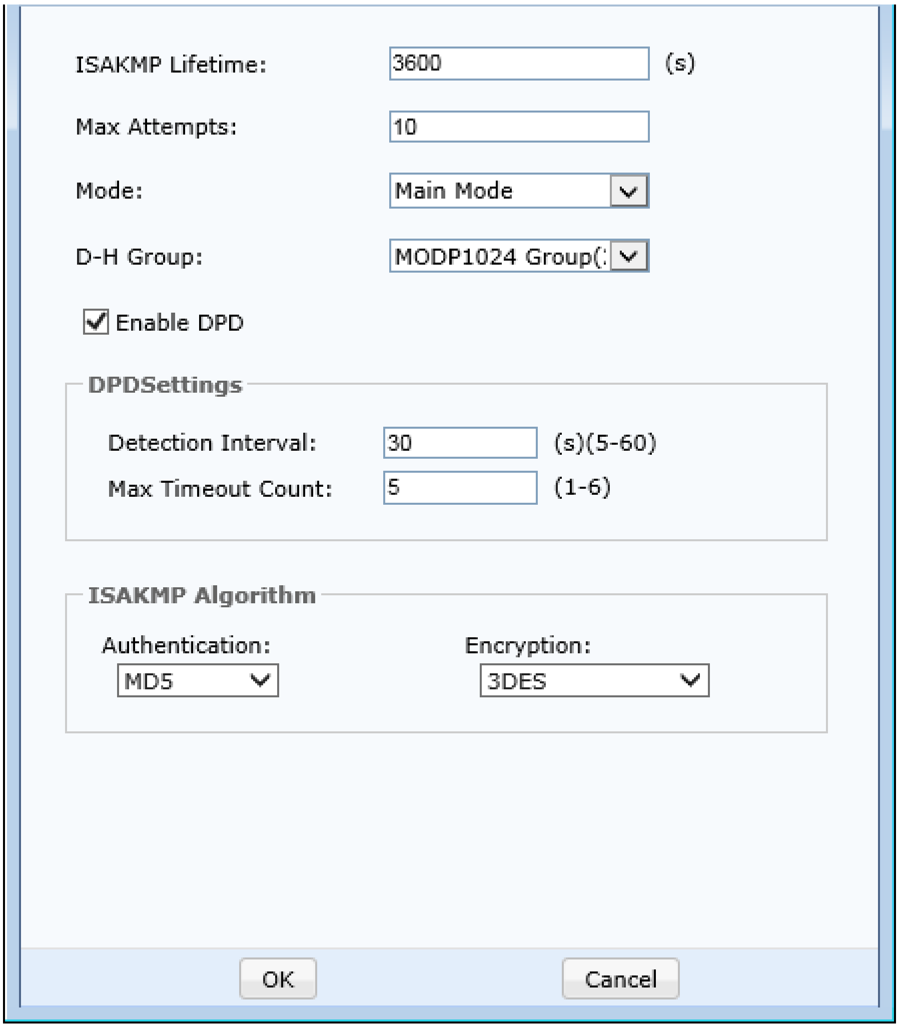
『Address Type』 is selected as Static IP.

『Static IP』 is configured as 222.222.222.222.

『Pre-shared Key』 sets the shared key of both parties negotiated.

Check the [Enable] and [Auto Connect] options, and this policy setting will take effect immediately after completion.

Click Advanced to set the following parameters. The interface is as follows:



ISAKMP Lifetime: 3600 (s)

Max Attempts: 10

Mode: Main Mode

D-H Group: MODP1024 Group(:

☑ Enable DPD

DPDSettings

Detection Interval: 30 (s)(5-60)

Max Timeout Count: 5 (1-6)

ISAKMP Algorithm

Authentication: MD5

Encryption: 3DES

『ISAKMP Survival Time』 is used to set the survival time of the first phase policy to 28,800.

『Max Attempts』 is used to set the number of retries in the first phase negotiation to 10.

『Mode』 selects the mode used in the first stage of negotiation as the main mode.

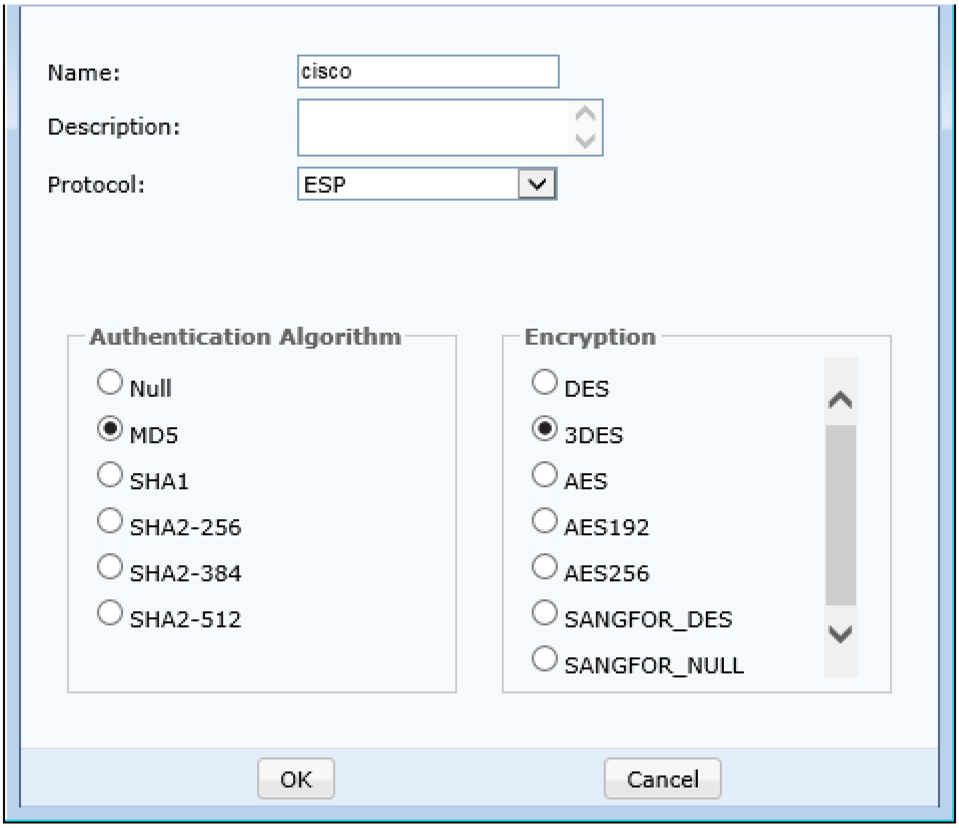
『D-H Group』 is used to set the Differ-Hellman group of the negotiation parties as GROUP 2.

『ISAKMP Encryption Algorithm』 selects 3DES as the encryption algorithm in the first stage.

『ISAKMP Authentication Algorithm』 selects MD5 as the authentication algorithm in the first stage.

Click OK in turn to save the configuration.

Step 2: Configure the security options in the second phase, 『VPN Information Settings』 -> 『Third Party Docking』 -> 『Security Options』, as shown in the following figure:



Name: cisco

Description:

Protocol: ESP

Authentication Algorithm

○ Null
● MD5
○ SHA1
○ SHA2-256
○ SHA2-384
○ SHA2-512

Encryption

○ DES
● 3DES
○ AES
○ AES192
○ AES256
○ SANGFOR_DES
○ SANGFOR_NULL

『Name』 is defined as cisco.

『Protocol』 selects ESP protocol.

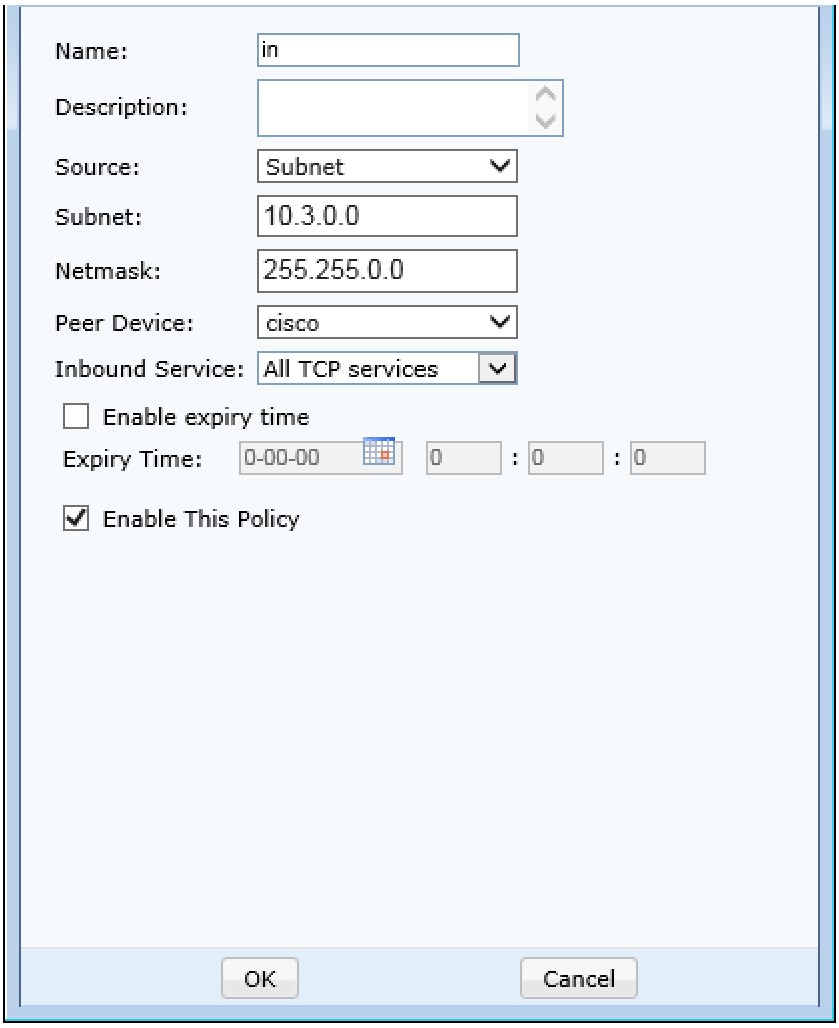
『Authentication Algorithm』 selects MD5 as the authentication algorithm.

『Encryption Algorithm』 selects DES as encryptio algorithm.

Click OK in turn to save the configuration.

Step 3: Configure the outbound and inbound policies for the second phase, 『VPN Information Settings』-> 『Third Party Docking』-> 『Second Phase』:

The configuration interface for inbound policies is as follows:



Name: in

Description:

Source: Subnet

Subnet: 10.3.0.0

Netmask: 255.255.0.0

Peer Device: cisco

Inbound Service: All TCP services

□ Enable expiry time

Expiry Time: 0-00-00 0 : 0 : 0

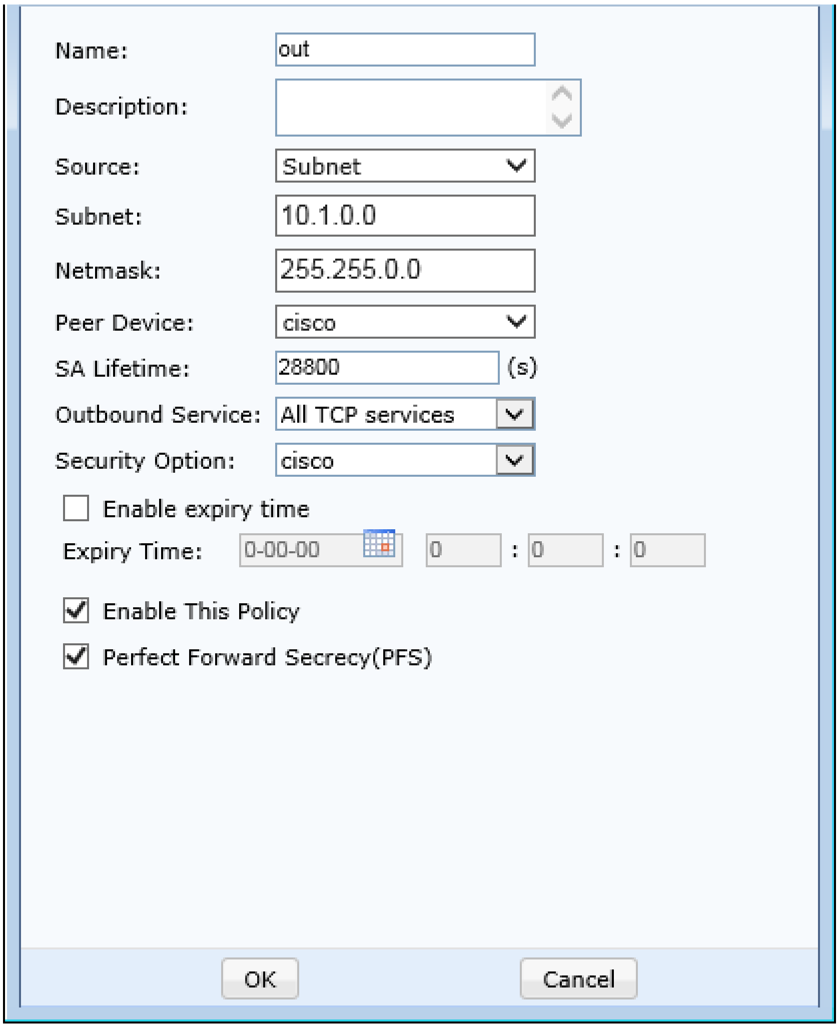
☑ Enable This Policy

『Name』 Inbound name is customized to cisco.

『Service』 Chooses to allow all inbound services.

『Source IP Type』 Set the IP address or IP address segment that the VPN opposite end is allowed to access the local port as a subnet, the subnet segment is 10.3.0.0, and the subnet mask is 255.255.0.0.

The outbound policy configuration is as follows:



Name: out

Description:

Source: Subnet

Subnet: 10.1.0.0

Netmask: 255.255.0.0

Peer Device: cisco

SA Lifetime: 28800 (s)

Outbound Service: All TCP services

Security Option: cisco

□ Enable expiry time

Expiry Time: 0-00-00 0 : 0 : 0

☑ Enable This Policy

☑ Perfect Forward Secrecy(PFS)

『Name』 Outbound name is customized to cisco.

『Service』 Chooses to allow all outbound services.

『Source IP Type』 Set the IP address or IP address segment of the local port that is allowed to access the VPN opposite end as a subnet, the subnet segment is 10.1.0.0, and the subnet mask is 255.255.0.0.

『Peer Device』 select cisco as the peer device, which has been customized as cisco in the first phase.

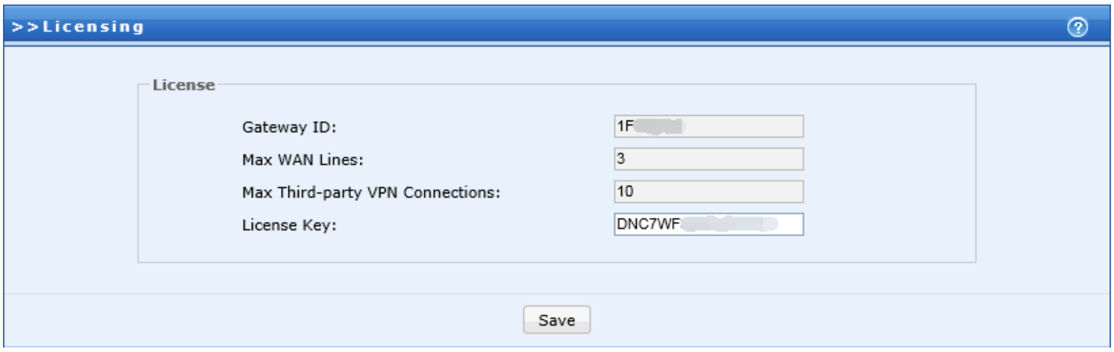
『Security Options』 Cisco is the security policy to be adopted when both parties negotiate.

『SA Keep-alive Time』 Define the policy lifetime as 28,800.

Check [Enable this Policy] to enable this policy, because cisco devices have already set up PFS, which will check [Enable Key Perfect Forward Secrecy] at the same time. Click OK to save and enable the rule.

After the above steps are configured, standard IPSEC VPN docking can be completed.

Before configuring the third-party docking, please confirm that the third-party docking authorization is enabled, and 『System Setup』-> 『Serial No. Setting』. If "number of third-party docking authorizations" is 0, then there is no authorization, and the number of authorizations indicates the number of tunnelings that can establish a standard IPSEC VPN. The interface is shown as follows:



Gateway ID: 1F[redacted]

Max WAN Lines: 3

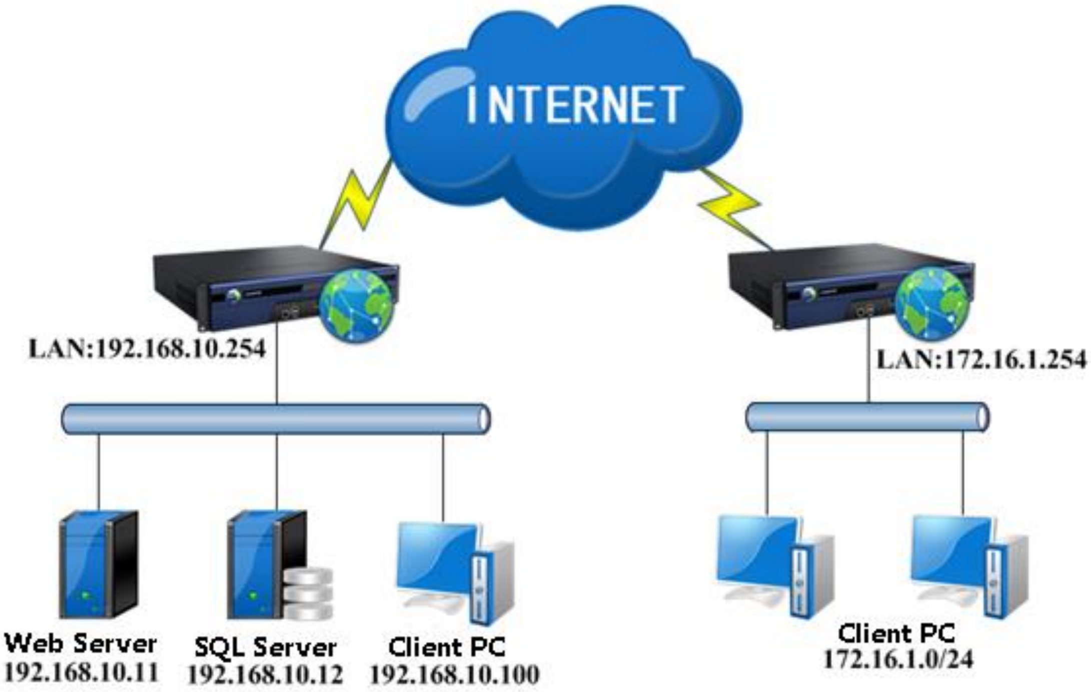
Max Third-party VPN Connections: 10

License Key: DNC7WF[redacted]

3.5. VPN LAN Permission Setting Case

Two MIG devices have been deployed in a headquarters and branch. Now the MIG devices in the headquarters have established VPN connection with the branch as VPN headquarters. The user requires to control the rights of the servers in the branch access headquarters. Only the PC in the branch network is allowed to access the WEB server (port 80) in the headquarters, and access to any other servers (including PC clients) is prohibited. As shown below:

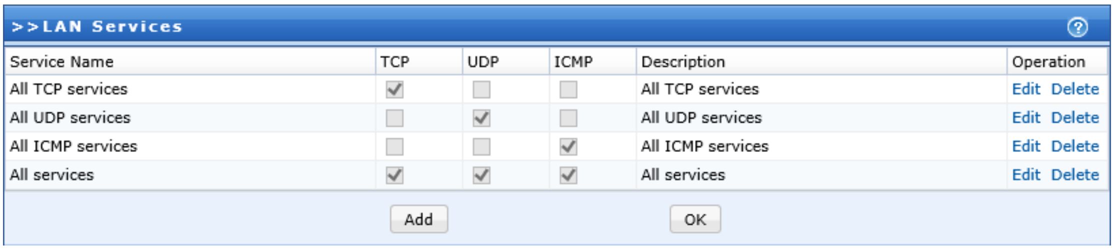
The WEB server (port 80) is prohibited from accessing any other server (including PC clients). As shown below:



The client's requirements can be realized in two ways: through VPN LAN permissions and through firewall filtering rules. The following describes how to configure in these two cases respectively:

Configuration Method 1: Realized through VPN LAN permissions.

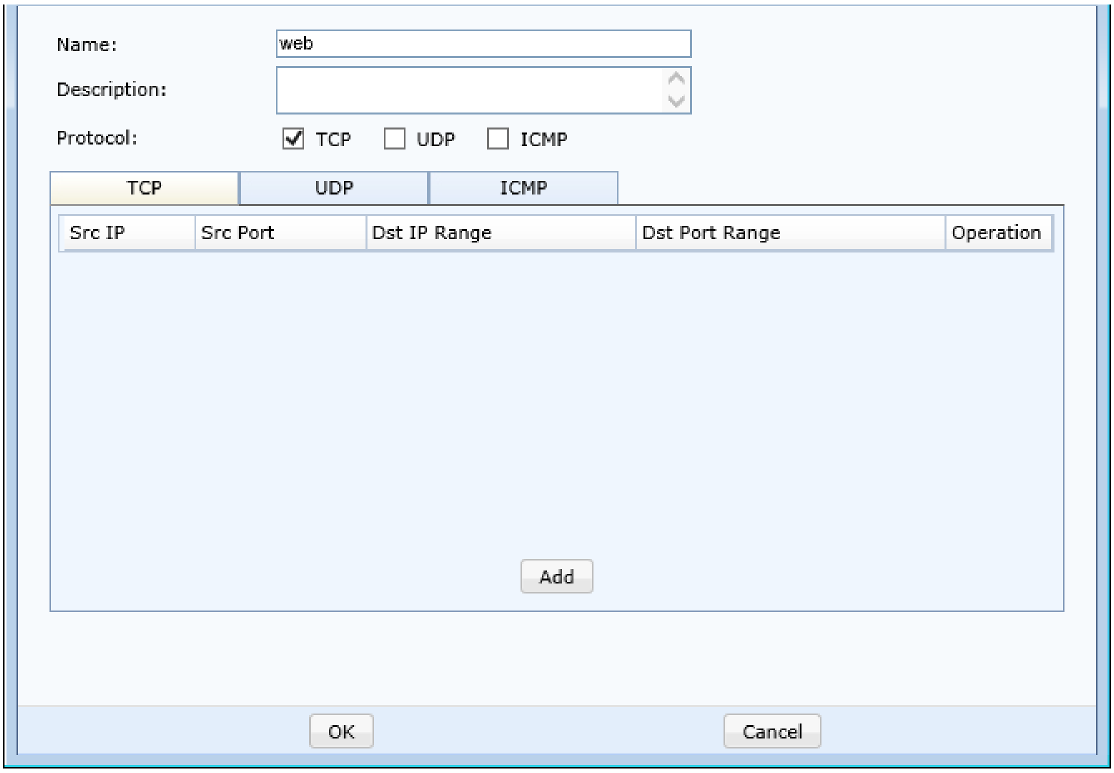
Step 1: On the 『VPN Information Settings』 -> 『Advanced Settings』 -> 『LAN Service Settings』 page of MIG device at headquarters, add a WEB LAN service as shown in the following figure:



>>LAN Services

Service Name	TCP	UDP	ICMP	Description	Operation
All TCP services	☑	□	□	All TCP services	Edit Delete
All UDP services	□	☑	□	All UDP services	Edit Delete
All ICMP services	□	□	☑	All ICMP services	Edit Delete
All services	☑	☑	☑	All services	Edit Delete

Click Add, set the name of the service, and select TCP protocol, as shown in the following figure:



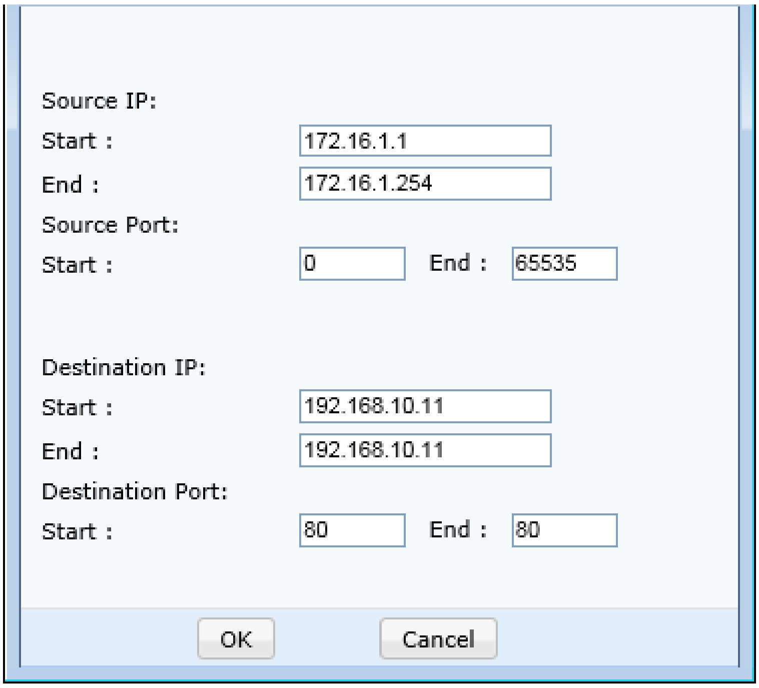
Name: web

Description:

Protocol: ☑ TCP □ UDP □ ICMP

Src IP	Src Port	Dst IP Range	Dst Port Range	Operation

Click Add again to set IP and port range, as shown in the following figure:



Source IP:

Start : 172.16.1.1

End : 172.16.1.254

Source Port:

Start : 0 End : 65535

Destination IP:

Start : 192.168.10.11

End : 192.168.10.11

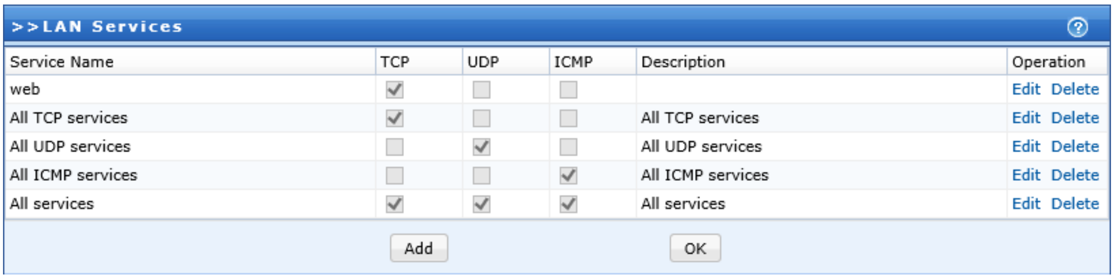
Destination Port:

Start : 80 End : 80

In this case, the source IP is a branched LAN segment, and the source port must be 0-65,535, because the ports initiating the connection are all random ports. The destination

IP can be the LAN WEB server IP of the headquarters, and the destination port is the WEB port 80.

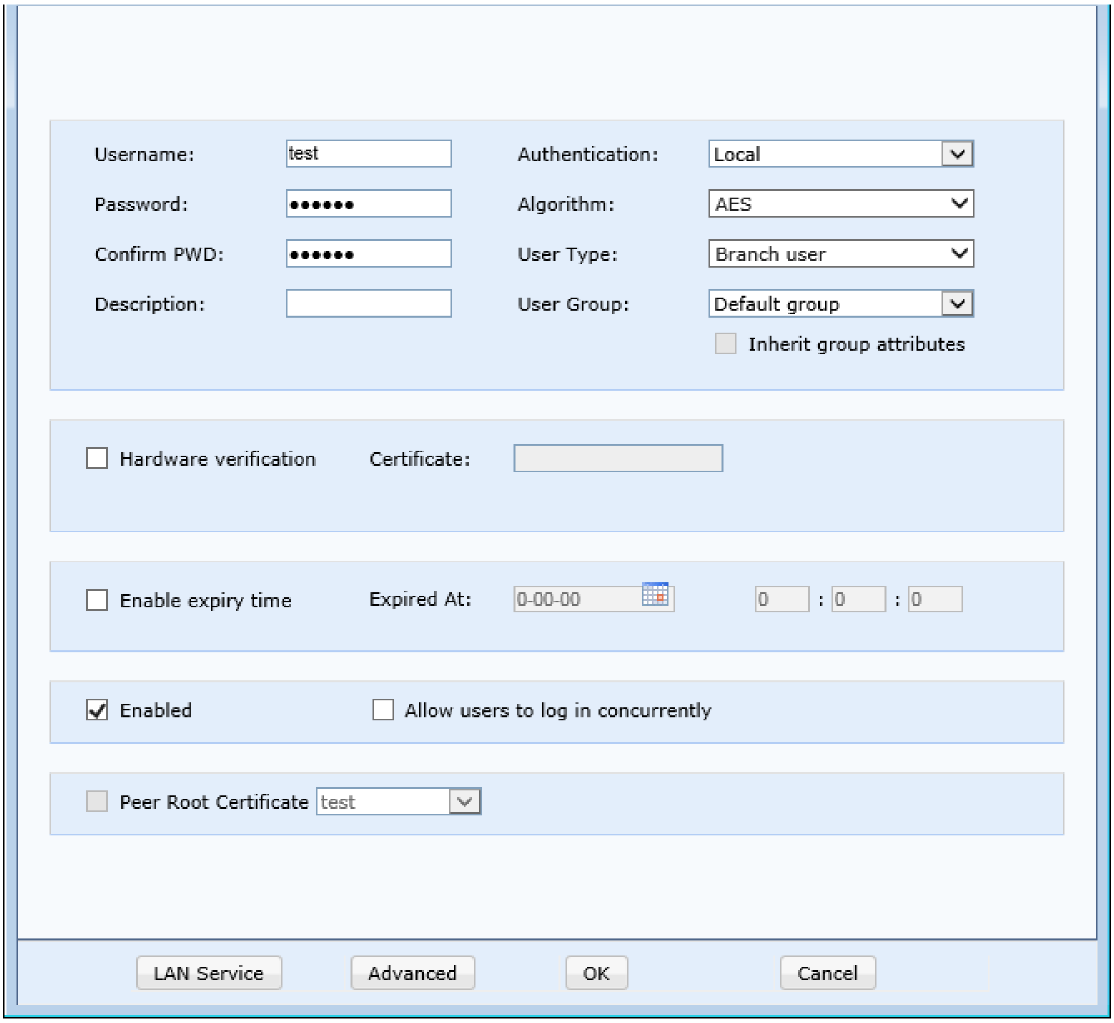
Click OK to complete the configuration. Finally, click the OK button on the console to save the configuration.



>>LAN Services

Service Name	TCP	UDP	ICMP	Description	Operation
web	☑	□	□		Edit Delete
All TCP services	☑	□	□	All TCP services	Edit Delete
All UDP services	□	☑	□	All UDP services	Edit Delete
All ICMP services	□	□	☑	All ICMP services	Edit Delete
All services	☑	☑	☑	All services	Edit Delete

Step 2: On the 『VPN Information Settings』-> 『User Management』 page of the headquarters device, edit the branch users , and click the permission settings, as shown in the following figure:



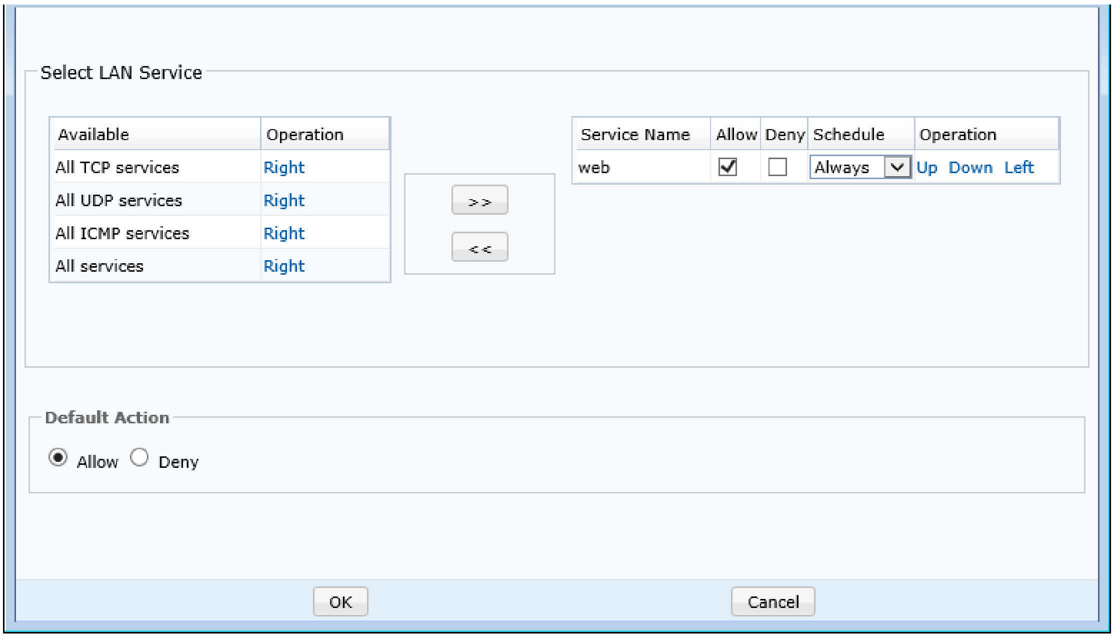
Username:	test	Authentication:	Local
Password:	••••••	Algorithm:	AES
Confirm PWD:	••••••	User Type:	Branch user
Description:		User Group:	Default group
			□ Inherit group attributes

□ Hardware verification Certificate:

□ Enable expiry time Expired At: 0-00-00 0 : 0 : 0

☑ Enabled □ Allow users to log in concurrently

□ Peer Root Certificate test



Select LAN Service

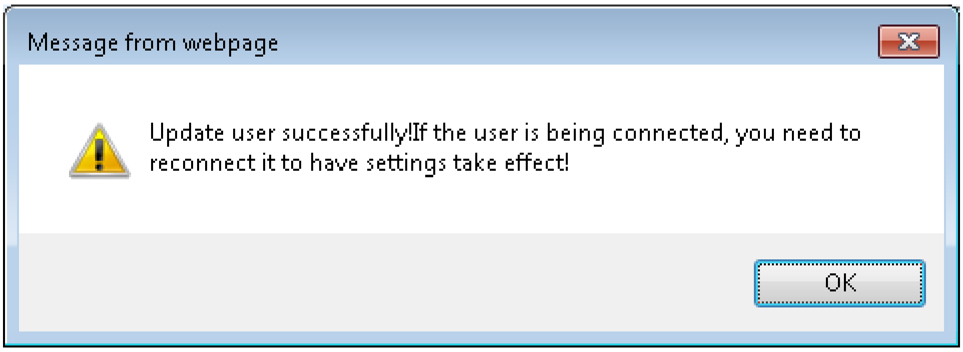
Available	Operation
All TCP services	Right
All UDP services	Right
All ICMP services	Right
All services	Right

Service Name	Allow	Deny	Schedule	Operation
web	☑	□	Always	Up Down Left

Default Action

● Allow ○ Deny

Click OK, then click OK in the dialog box [Edit User-Branch], and the following prompt will appear:



Message from webpage

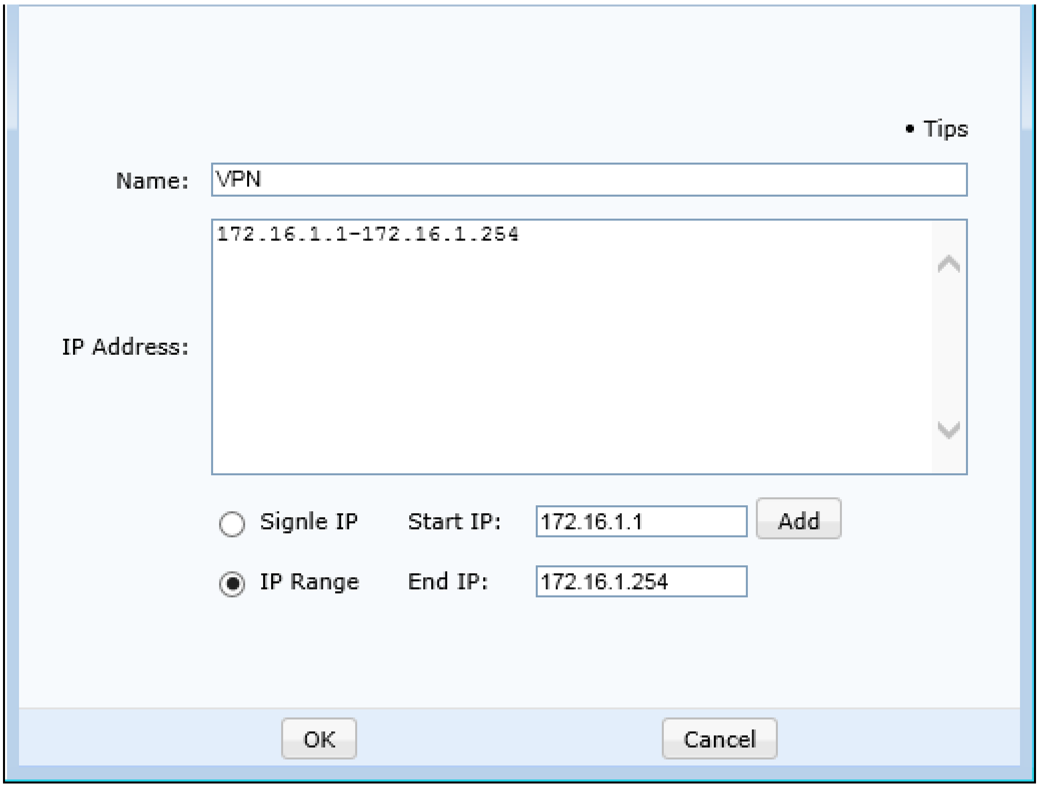
Update user successfully!If the user is being connected, you need to reconnect it to have settings take effect!

After the above steps are completed, the VPN tunnel needs to re-establish the connection to take effect.

⚠ **Attention: Once the VPN LAN permission is set, not only will VPN peer access to the local port be restricted, but local port access to VPN peer will also be controlled by the LAN permission. Since IP and ports of the packets are subject to the LAN permissions, the packets in line with rules conditions would face the same restrictions, regardless of whether the VPN peer initiates a packet or the local initiates a packet while the VPN peer responds accordingly. Through firewall filtering rules, more detailed control can be realized.**

Configuration method 2: Realized through firewall filtering rules.

Step 1: the MIG device in the headquarters 『Firewall settings』-> 『IP Group Definition』 defines the IP group of the branch network segment and the IP group of the headquarters WEB server. The interface is as follows:

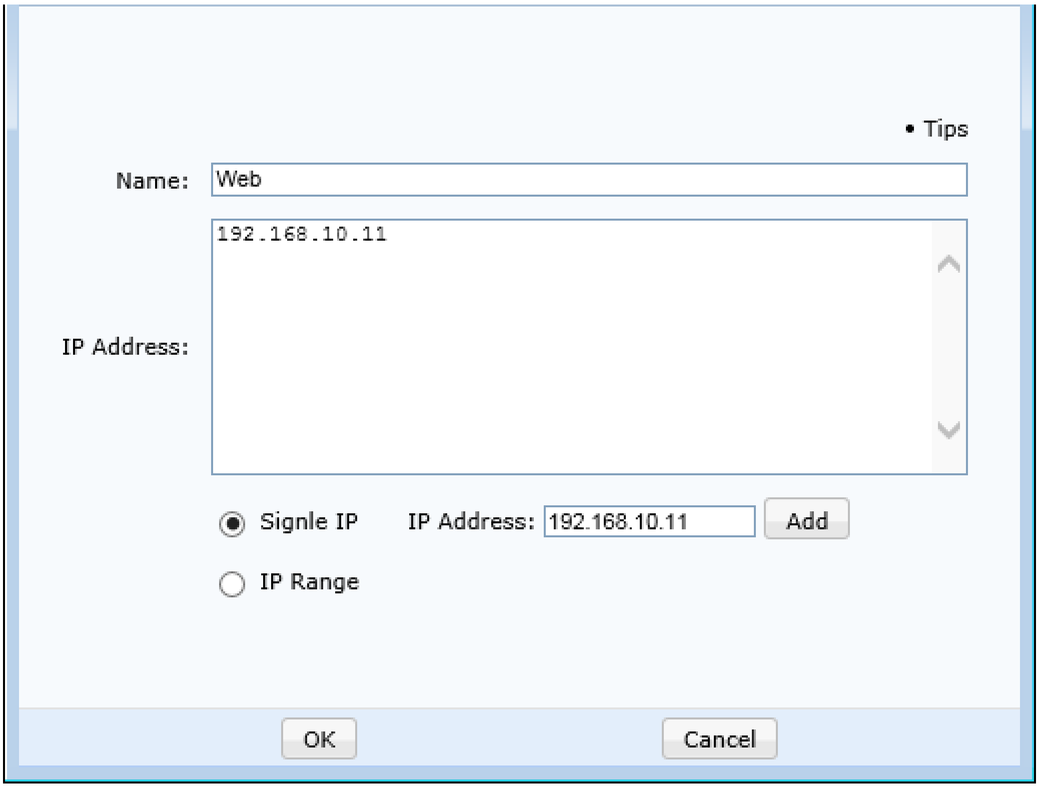


Name: VPN

IP Address: 172.16.1.1-172.16.1.254

○ Signle IP Start IP: 172.16.1.1

● IP Range End IP: 172.16.1.254



Name: Web

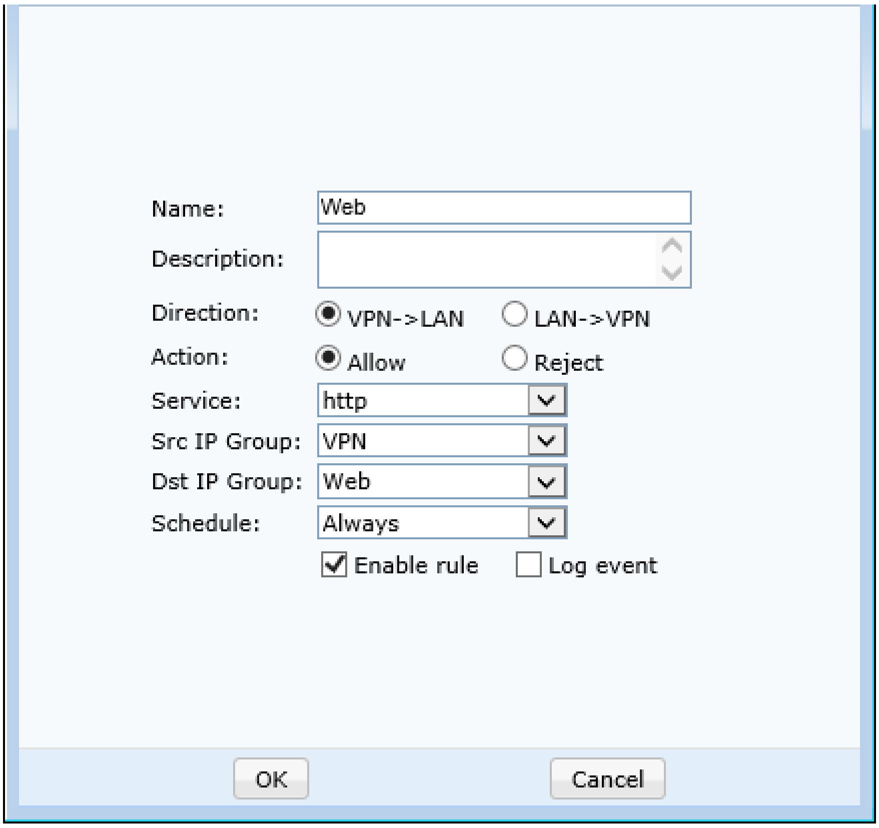
IP Address: 192.168.10.11

● Signle IP IP Address: 192.168.10.11

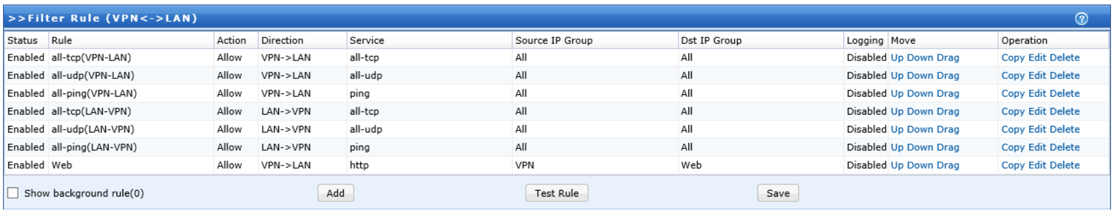
○ IP Range

Finally, click OK to save the configuration.

Step 2: In the 『Firewall settings』-> 『Filtering Rule Settings』--> 『VPN-> LAN』 of MIG device in headquarters, delete the three rules of "VPN-> LAN" (because VPN-> LAN is used to release all data by default), and then add a rule with the following interface:



Name:	Web	
Description:		
Direction:	● VPN->LAN	○ LAN->VPN
Action:	● Allow	○ Reject
Service:	http	
Src IP Group:	VPN	
Dst IP Group:	Web	
Schedule:	Always	
	☑ Enable rule	□ Log event



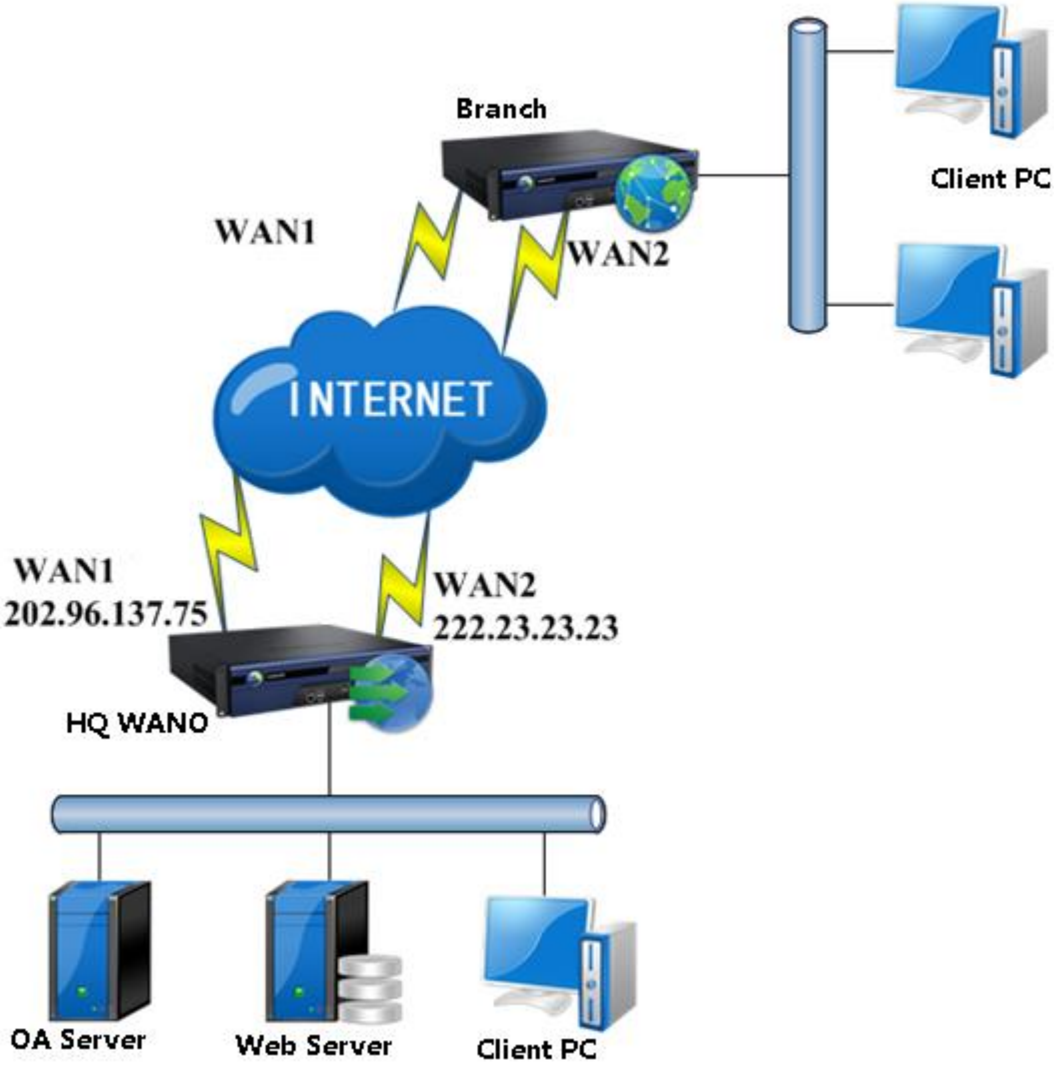
>>Filter Rule (VPN<->LAN)

Status	Rule	Action	Direction	Service	Source IP Group	Dst IP Group	Logging	Move	Operation
Enabled	all-tcp(VPN-LAN)	Allow	VPN->LAN	all-tcp	All	All	Disabled	Up Down Drag	Copy Edit Delete
Enabled	all-udp(VPN-LAN)	Allow	VPN->LAN	all-udp	All	All	Disabled	Up Down Drag	Copy Edit Delete
Enabled	all-ping(VPN-LAN)	Allow	VPN->LAN	ping	All	All	Disabled	Up Down Drag	Copy Edit Delete
Enabled	all-tcp(LAN-VPN)	Allow	LAN->VPN	all-tcp	All	All	Disabled	Up Down Drag	Copy Edit Delete
Enabled	all-udp(LAN-VPN)	Allow	LAN->VPN	all-udp	All	All	Disabled	Up Down Drag	Copy Edit Delete
Enabled	all-ping(LAN-VPN)	Allow	LAN->VPN	ping	All	All	Disabled	Up Down Drag	Copy Edit Delete
Enabled	Web	Allow	VPN->LAN	http	VPN	Web	Disabled	Up Down Drag	Copy Edit Delete

□ Show background rule(0)

3.6. VPN Multiple Lines Configuration Case

A user's headquarters is a dual line, and a SANGFOR WOC device is deployed. The branch is MIG 1200, which is also a dual line. Users need to realize line backup. If any line at the branch end has problems, they need to take another line. When both lines are normal, the fastest line is automatically selected to transmit VPN data.

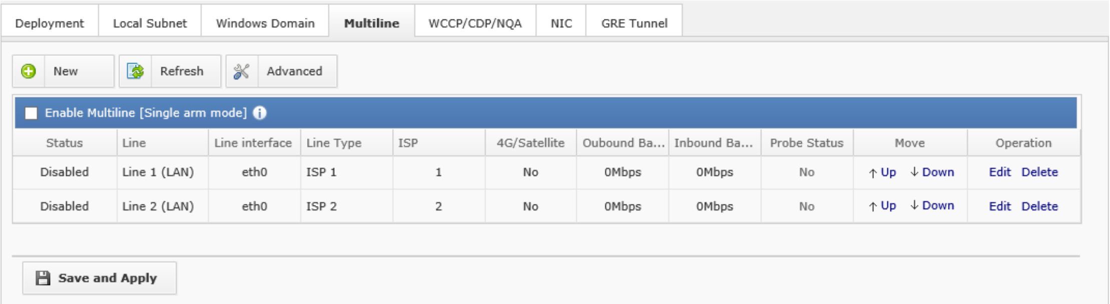


The configuration steps are as follows:

Configuration Method of WOC Device in Headquarters

Step 1: On WOC device at headquarters, configure IP address, proxy Internet access, WEBAGENT and other information .

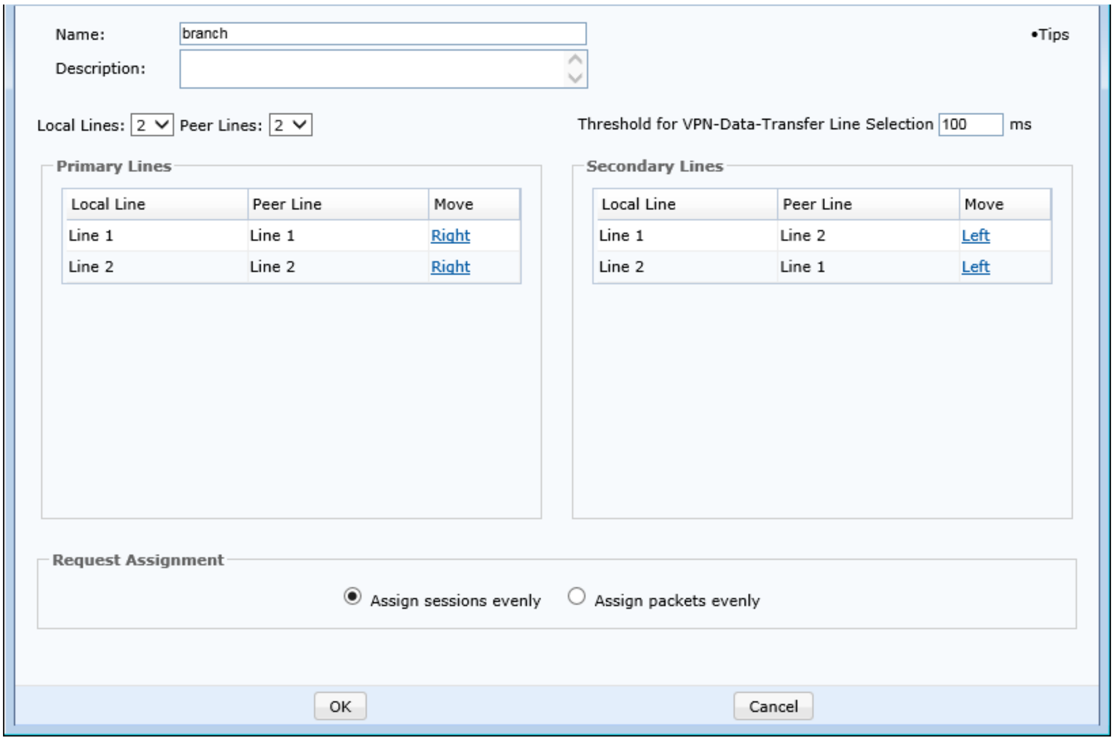
Step 2: In the headquarters WOC device [System]-[Deployment Settings]-[Mult-line Setting], configure [Mult-line Setting], and the interface is as follows:



□ Enable Multiline [Single arm mode]

Status	Line	Line interface	Line Type	ISP	4G/Satellite	Oubound Ba...	Inbound Ba...	Probe Status	Move	Operation
Disabled	Line 1 (LAN)	eth0	ISP 1	1	No	0Mbps	0Mbps	No	↑ Up ↓ Down	Edit Delete
Disabled	Line 2 (LAN)	eth0	ISP 2	2	No	0Mbps	0Mbps	No	↑ Up ↓ Down	Edit Delete

Step 3: In the headquarters WOC device [Sangfor VPN]-[Multi-line], set up nultiple lines of routing policy. The setting interface in this case is as follows:



Name: branch

Description:

Local Lines: 2 Peer Lines: 2

Threshold for VPN-Data-Transfer Line Selection 100 ms

Primary Lines

Local Line	Peer Line	Move
Line 1	Line 1	Right
Line 2	Line 2	Right

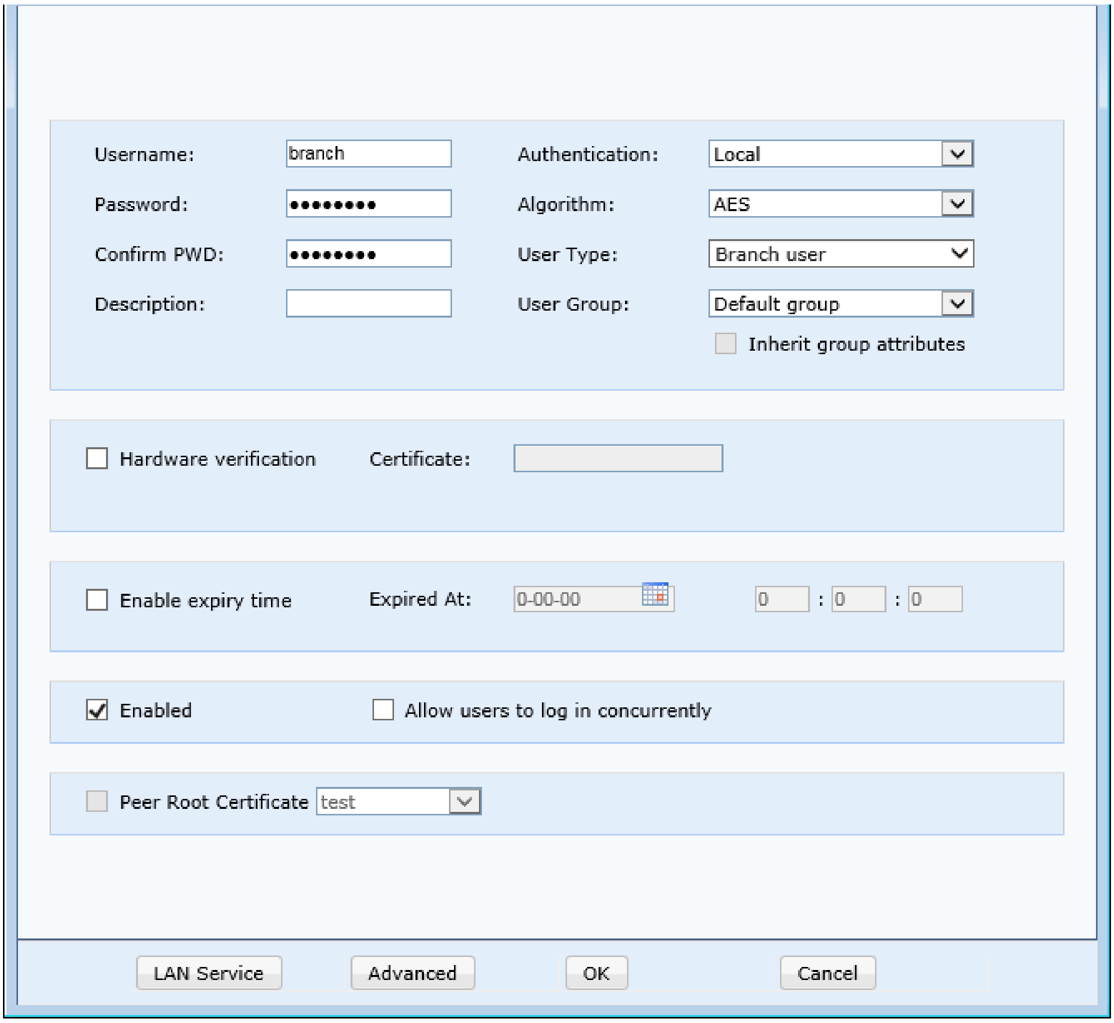
Secondary Lines

Local Line	Peer Line	Move
Line 1	Line 2	Left
Line 2	Line 1	Left

Request Assignment

● Assign sessions evenly ○ Assign packets evenly

Step 4: In [Sangfor VPN]-[Server]-[User Management], set up a new branch to connect with the headquarters account, click Advanced to send routing policy to the user, and the interface is as follows:



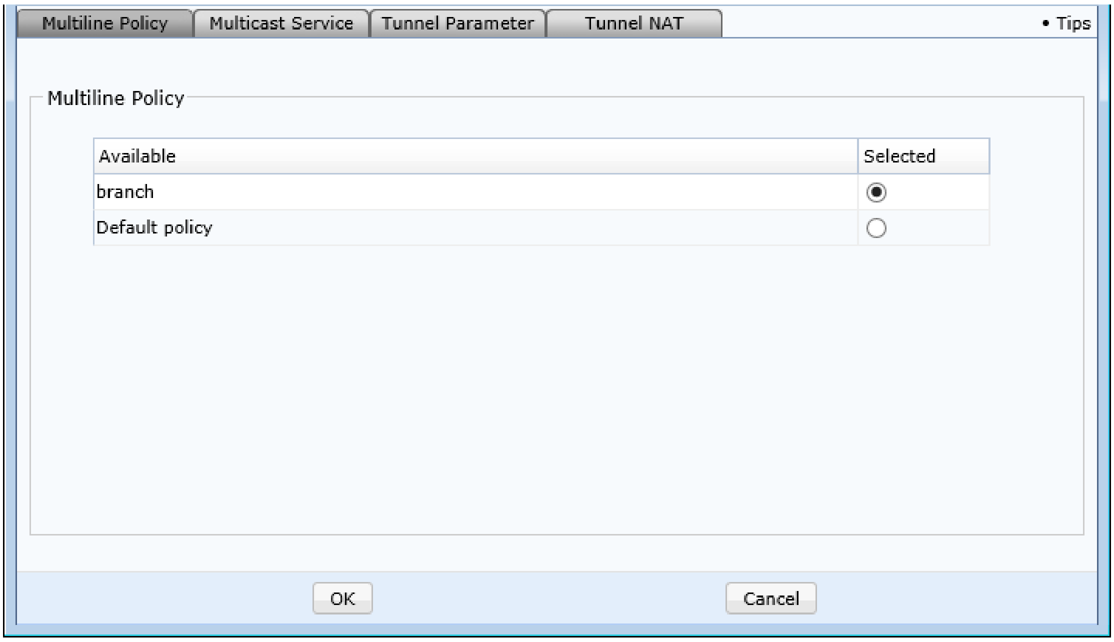
Username:	branch	Authentication:	Local
Password:	••••••••	Algorithm:	AES
Confirm PWD:	••••••••	User Type:	Branch user
Description:		User Group:	Default group
			□ Inherit group attributes

□ Hardware verification Certificate:

□ Enable expiry time Expired At: 0-00-00 0 : 0 : 0

☑ Enabled □ Allow users to log in concurrently

□ Peer Root Certificate test



Multiline Policy

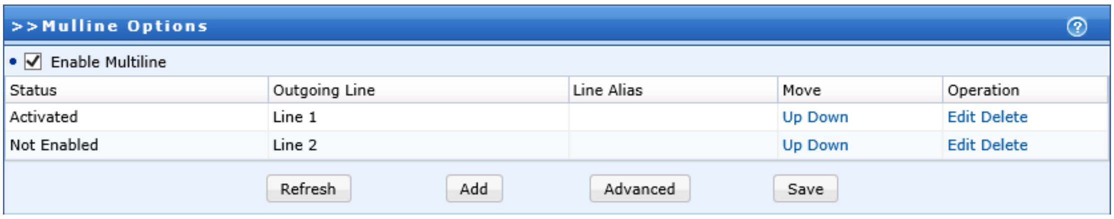
Available	Selected
branch	●
Default policy	○

Click OK in turn to save the configuration.

Configuration method of branch MIG 1200 configuration:

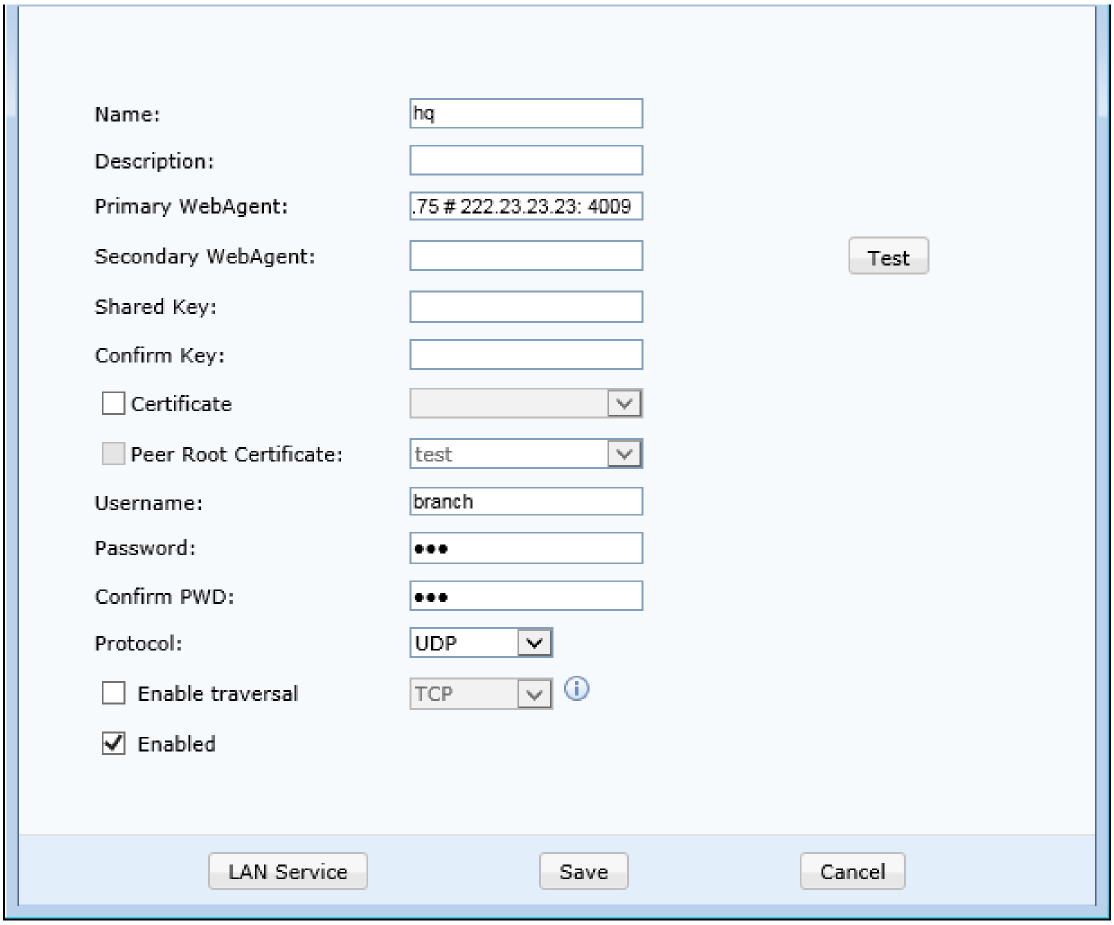
Step 1: Configure basic network configuration information such as interface IP address.

Step 2: At『System Setup』->『Mult-line Setting』, configure multiple line information . The interface is shown as follows:



Status	Outgoing Line	Line Alias	Move	Operation
Activated	Line 1		Up Down	Edit Delete
Not Enabled	Line 2		Up Down	Edit Delete

Step 3: At 『VPN Information Settings』 --> 『Connection Management』 , create a new connection management, and configure the WEBAGENT information and account password information. In this case, the WEBAGENT is configured as 202.96.137.75 # 222.23.23.23: 4009 with the following interface:



Name: hq

Description:

Primary WebAgent: .75 # 222.23.23.23: 4009

Secondary WebAgent:

Shared Key:

Confirm Key:

□ Certificate

□ Peer Root Certificate: test

Username: branch

Password: ●●●

Confirm PWD: ●●●

Protocol: UDP

□ Enable traversal TCP

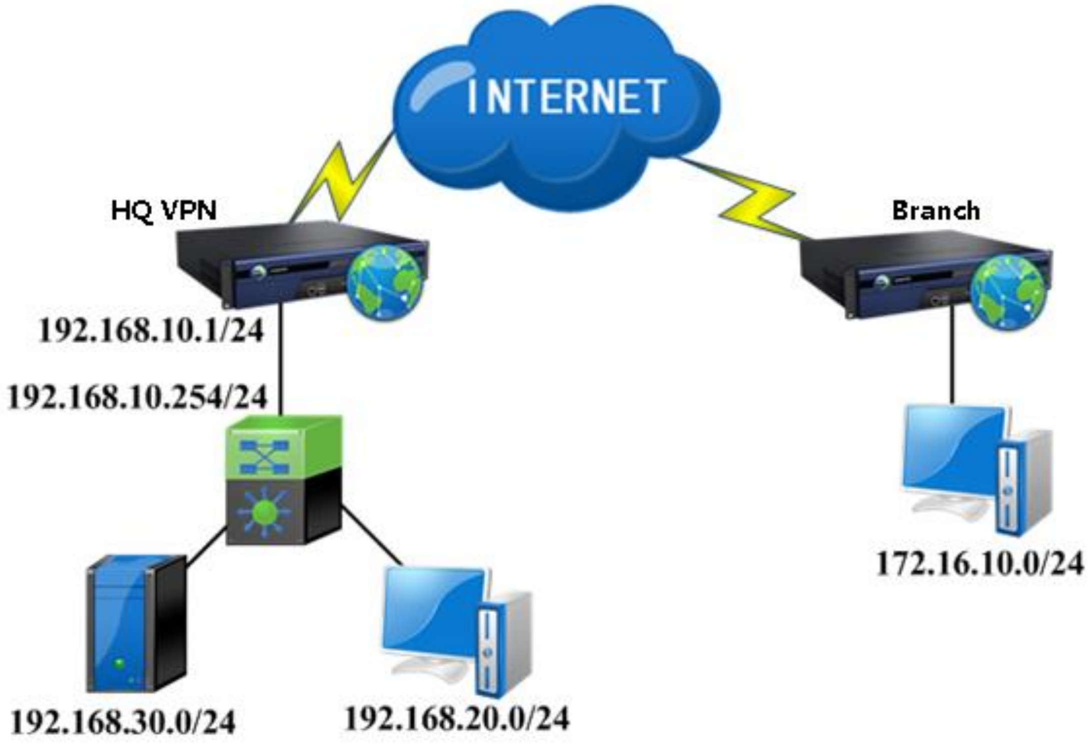
☑ Enabled

After the above steps are configured, the automatic routing function of multi-line can be realized.

⚠ **1. MIG 1200 cannot configure multi-line routing policy. In general, the multi-line of MIG 1200 is used in the scenario of redundant backup of branch dual lines.**

3.7. VPN Multi-subnet Configuration Case

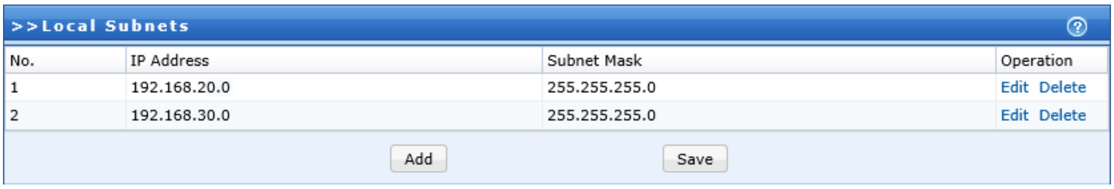
The headquarters has three subnets (192.168.10.0/24, 192.168.20.0/24 and 192.168.30.0/24). After the branch accesses the headquarters through VPN, it needs to access the three subnets in the headquarters LAN. The topology diagram is as follows:



This requirement can be realized by configuring the "local subnet" and adding 192.168.20.0/24 and 192.168.30.0/24 network segments and corresponding static routes.

The specific configuration is as follows: (Skip VPN configuration steps)

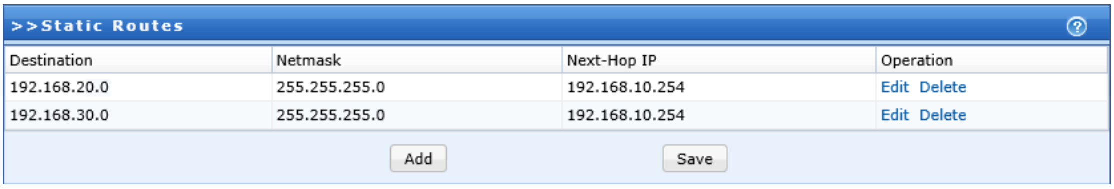
Step 1: At the "Local Sub-List" of MIG device at headquarters, add 192.168.20.0/24 and 192.168.30.0/24 sub-segments, as shown in the following figure:



No.	IP Address	Subnet Mask	Operation
1	192.168.20.0	255.255.255.0	Edit Delete
2	192.168.30.0	255.255.255.0	Edit Delete

Step 2: In 『System Setup』-> 『Routing settings』-> 『System Routing Settings』,

set static routes for the two VPN local subnets. as follows:



Destination	Netmask	Next-Hop IP	Operation
192.168.20.0	255.255.255.0	192.168.10.254	Edit Delete
192.168.30.0	255.255.255.0	192.168.10.254	Edit Delete

After the configuration is completed and the branch is connected to the headquarters, all three network segments of the headquarters can be accessed normally.

1. The [Local Subnet] here is only equivalent to a "declaration" function. The network segments defined here will be regarded as VPN network segments by our MIG devices and software clients. All data packets accessing these network segments will be encapsulated into VPN tunneling after passing through MIG device or software. Therefore, in general, a subnet segment is added to the 『Local Subnet』, which needs to cooperate with the 『static route』 to complete access to multiple subnets.

2. If static routes were configured when the device was put on shelves, there is no need to repeat the configuration here. Ensure that the device system route can reach the route of the LAN segment.

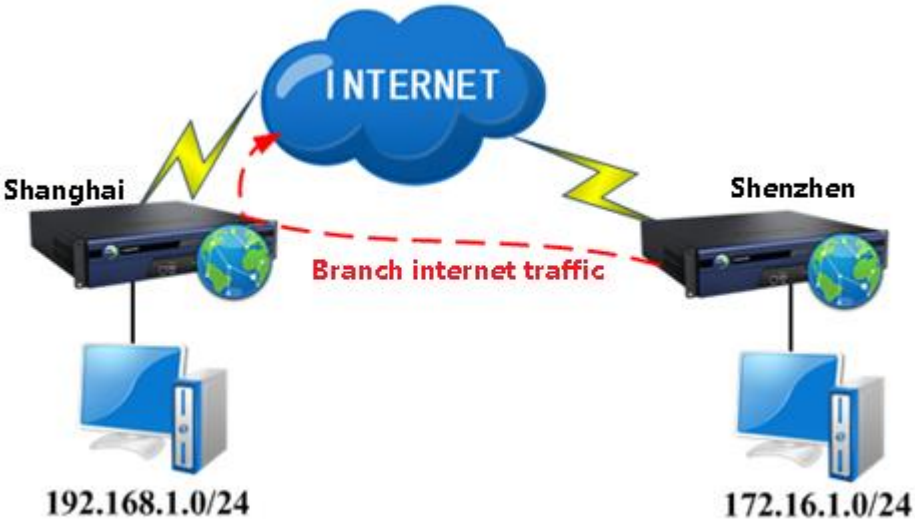
3.8. Cases of Inter-branch Exchange Accesses Through Inter-tunnel Routing

The headquarters ("Shenzhen" 192.168.1.0/24) and branches ("Beijing"

172.16.1.0/24) and ("Guangzhou" 10.1.1.0/24) have established VPN connections (branches "Beijing" and "Guangzhou" connect with the headquarters through connection management). However, there is no VPN connection between "Beijing" and "Guangzhou". By setting appropriate inter-tunnel routing rules, mutual access between "Beijing" and "Guangzhou" can be realized. The topology diagram is as follows:

3.9. Cases of Internet Access by Users via Destination Routing

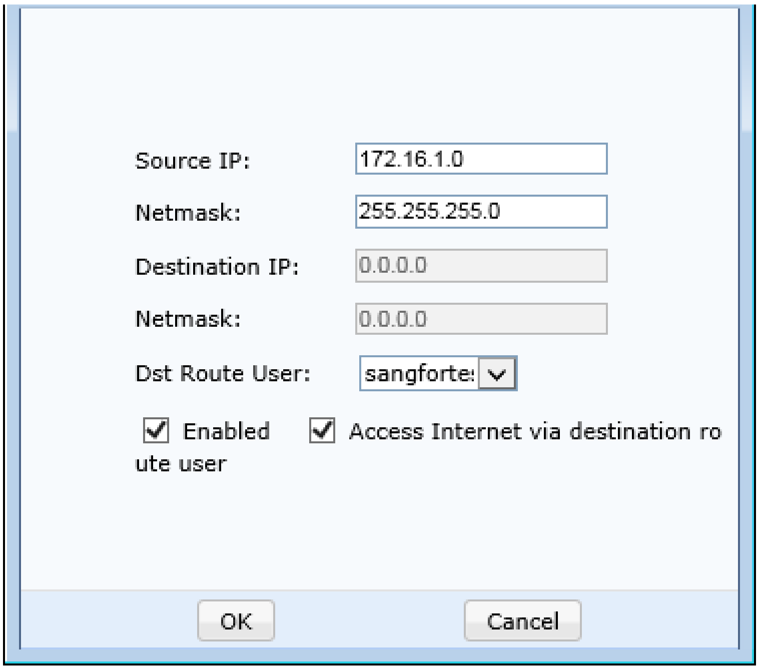
In MIG device, inter-tunnel routing can also be used to send all branch internet access data to the headquarters and access the internet through the public network egress of the headquarters. For example, the branch "Shenzhen" is set up to access the Internet through the headquarters "Shanghai". The topology diagram is as follows:



The configuration steps are as follows:

VPN tunnel configuration steps are skipped here. On the basis of the VPN tunnel has been established, do the following configuration:

Step 1: Add an inter-tunnel route to the "Shenzhen" device, 『VPN Information Settings』 -> 『Inter-tunnel Route』, click Add, fill in the local LAN segment, and check the option [Access the Internet Via Destination Route Users], as shown in the following figure:



Source IP: 172.16.1.0

Netmask: 255.255.255.0

Destination IP: 0.0.0.0

Netmask: 0.0.0.0

Dst Route User: sangforte:

☑ Enabled ☑ Access Internet via destination route user

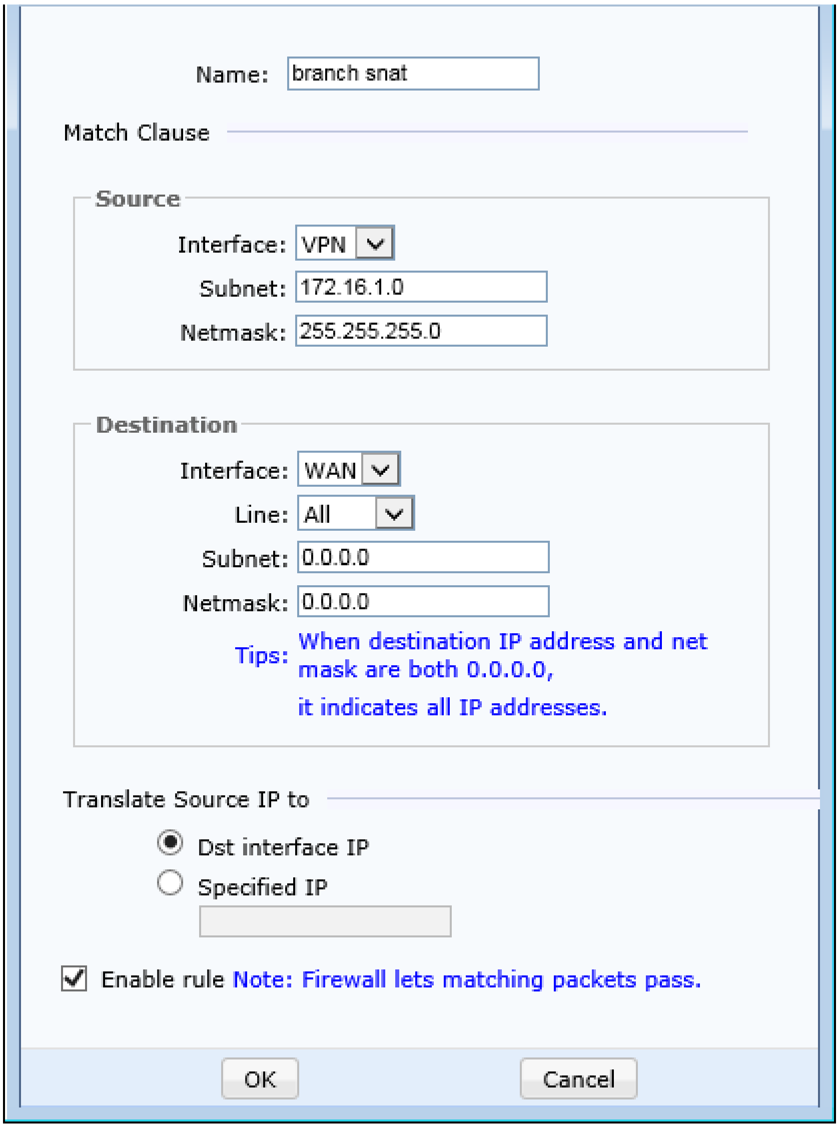
[Network Number (Source)]: Set the network number of the source address, and set the network number of this port that needs to be connected to the Internet through the headquarters, such as 172.16.1.0.

[Subnet Mask (Source)]: Sets the subnet mask of the source address. In this example, it should be set to 255.255.255.0.

[Destination Routing User]: Set the VPN connection user to which the route points. In this example, it should be set to "Shenzhen".

Finally, check [Internet Access for Users Via Destination Route] to enable the setting. When checked, the destination IP and mask will both change to 0.0.0.0

Step 2: Add proxy Internet access rules to the "Shanghai" device, and 『Firewall』-> 『NAT』-> 『Proxy Internet Access Settings』will proxy internet access to the data sent from the branch "Shenzhen", as shown in the following figure:



Name: branch snat

Match Clause

Source

Interface: VPN

Subnet: 172.16.1.0

Netmask: 255.255.255.0

Destination

Interface: WAN

Line: All

Subnet: 0.0.0.0

Netmask: 0.0.0.0

Tips: When destination IP address and net mask are both 0.0.0.0, it indicates all IP addresses.

Translate Source IP to

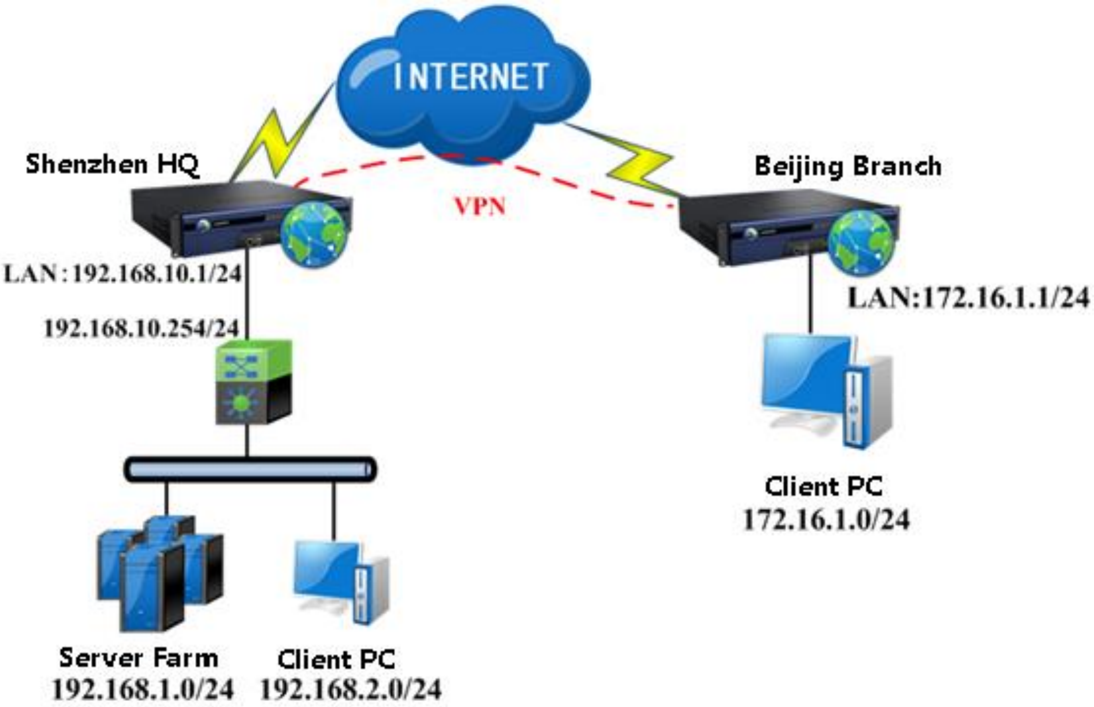
● Dst interface IP

○ Specified IP

☑ Enable rule Note: Firewall lets matching packets pass.

3.10. SNAT Case of VPN Tunnel LAN Interface

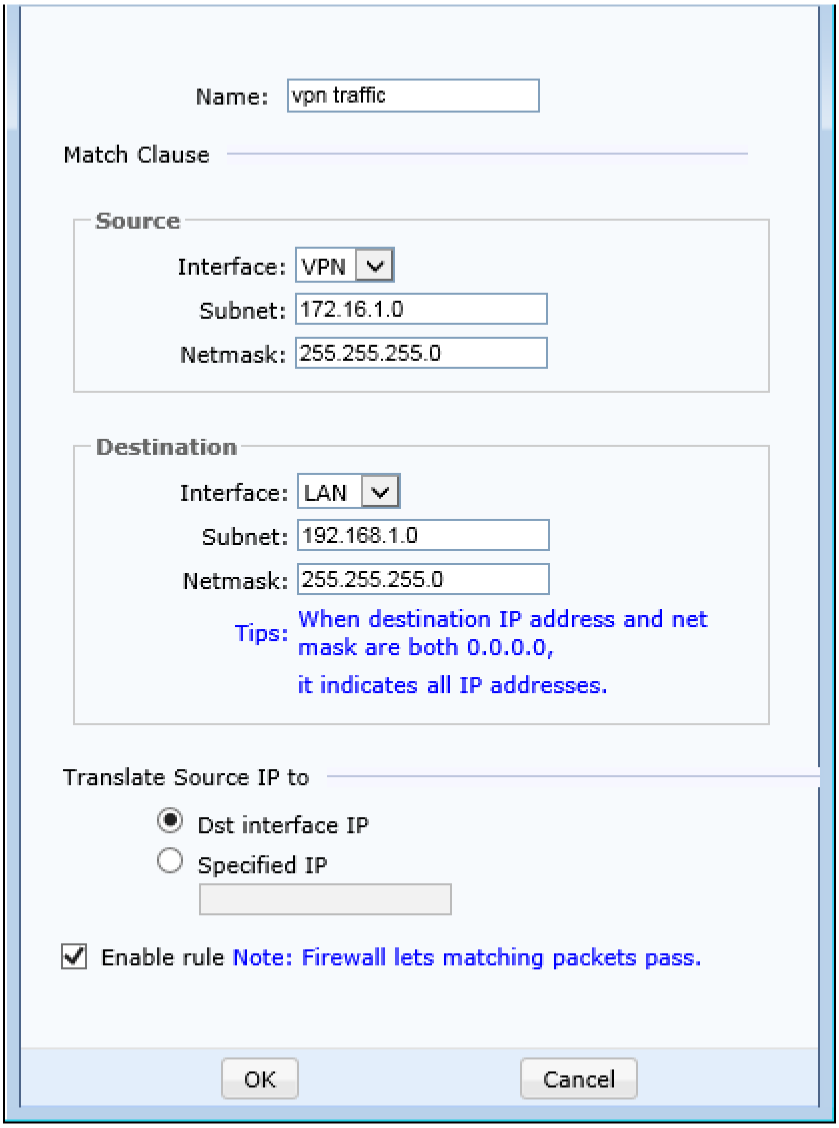
A user's network structure is as follows: Shenzhen headquarters and Beijing branch have deployed a MIG device respectively, and VPN tunnel has been established. Because the server restricted access to the source IP address, only the 192.168.0.0/16 network segment of the headquarters is allowed to access, and the rest of the network segments cannot access the server. Therefore, users in the Beijing branch cannot access the server through VPN, and users hope that the source IP addresses of data packets for users in the Beijing branch to access the headquarters server can all be converted to 192.168.10.1 to solve the problem.



The configuration steps are as follows:

Step 1: VPN Interconnect Configuration. In this topology, the headquarters needs to configure WEBAGENT, user management, local subnet and system routing. Branch configure connection management. Please refer to section 3.3 for details, which will not be repeated here.

Step 2: after the VPN tunnel is connected, set up a proxy internet access rule for VPN tunnel on MIG device in Shenzhen headquarters, 『Firewall』-> 『NAT』-> 『Proxy Internet Access Settings』 and add a new rule.



Name: vpn traffic

Match Clause

Source

Interface: VPN

Subnet: 172.16.1.0

Netmask: 255.255.255.0

Destination

Interface: LAN

Subnet: 192.168.1.0

Netmask: 255.255.255.0

Tips: When destination IP address and net mask are both 0.0.0.0, it indicates all IP addresses.

Translate Source IP to

● Dst interface IP

○ Specified IP

☑ Enable rule Note: Firewall lets matching packets pass.

[Source Address/Source Interface]: Since the data is sent from the VPN peer, the source interface is selected as VPN

[Source Address/Subnet Segment/Subnet Mask]: The LAN segment at the VPN opposite end is 172.16.1.0/24, so fill in this segment here.

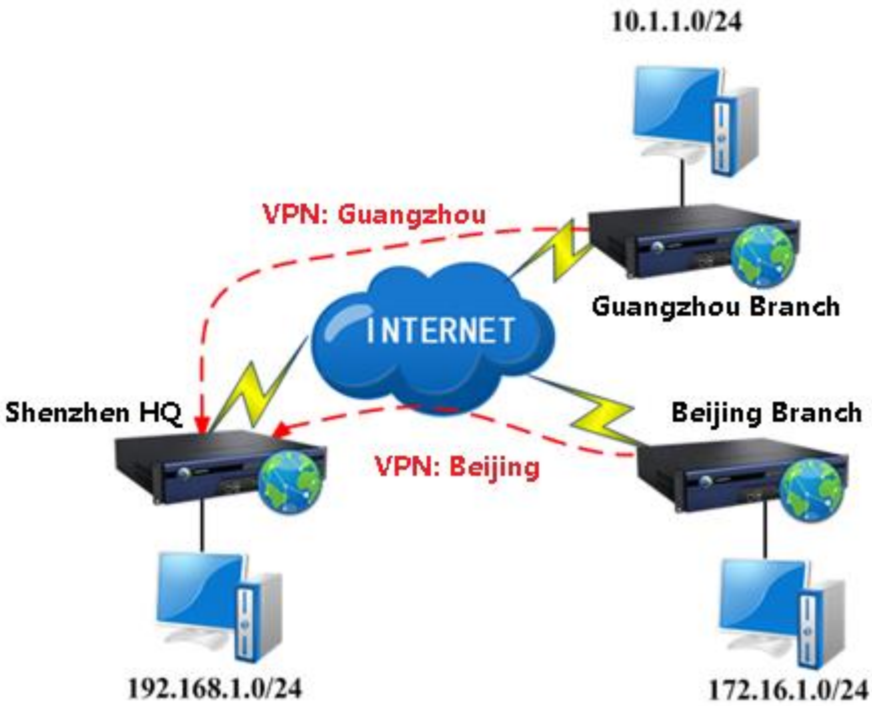
[Destination Address/Destination Interface]: The data of VPN peer access server is in the direction of the LAN interface of MIG device, and the data needs to be forwarded from the LAN interface, so the LAN interface is selected for the outbound interface.

[Destination Address/Subnet Segment/Subnet Mask]: Fill in the IP address of the server segment.

[Source IP Conversion to]: According to the client's requirements, it needs to be converted to 192.168.10.1, which is the LAN interface address of MIG device.

Click OK in turn to save the configuration.

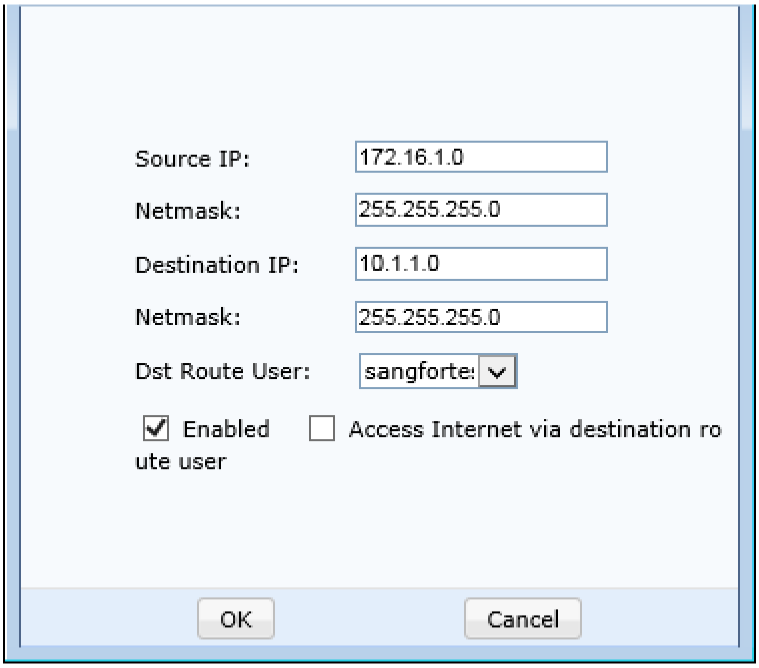
After the above rule configuration takes effect, the branch will convert to the LAN interface IP address 192.168.10.1 when accessing the headquarters server network segment 192.168.1.0/24, that is, the source IP address of the packet seen by the server is 192.168.10.1. However, the original IP address 172.16.1.0/24 was still used by the branch when accessing the 192.168.2.0/24 users in the headquarters LAN. This is because the network segment filled in by the destination address conversion conditions in the above rules does not include LAN users.



The configuration steps are as follows:

Step 1: First configure the VPN interconnection between the two branches and the headquarters (the configuration process is skipped here).

Step 2: Check [Enable Routing] in 『Inter-Tunnel Routing』 of Beijing Branch, click Add, and add the route to "Guangzhou". The configuration is as follows:


Source IP: 172.16.1.0

Netmask: 255.255.255.0

Destination IP: 10.1.1.0

Netmask: 255.255.255.0

Dst Route User: sangforte:

☑ Enabled ☐ Access Internet via destination route user

[Network Number (Source)]: Sets the source address network number. In this example, it should be set to 172.16.1.0.

[Subnet Mask (Source)]: Sets the subnet mask of the source address. In this example, it should be set to 255.255.255.0.

[Network Number (Destination)]: Set the destination address network number. In this example, it should be set to 10.1.1.0.

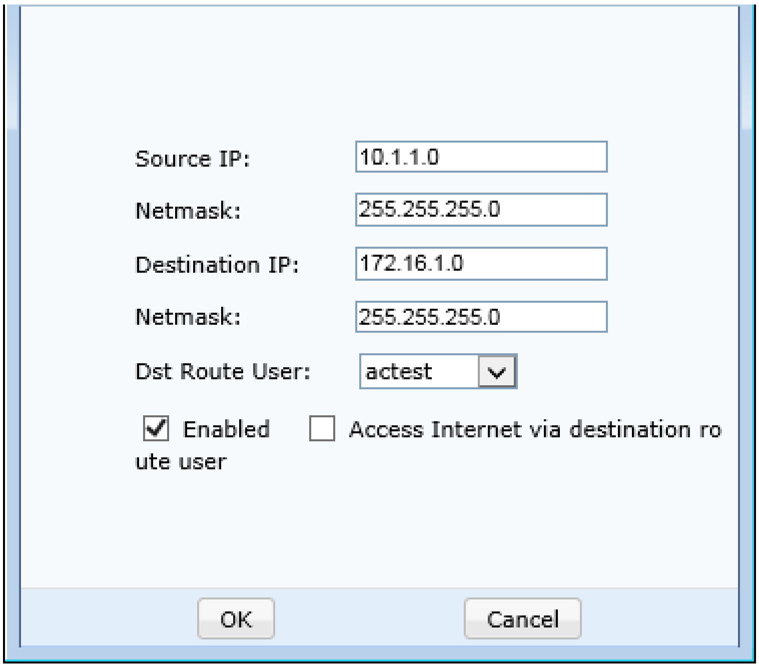
[Subnet Mask (Destination)]: Set the subnet mask of the destination address. In this example, it should be set to 255.255.255.0.

[Destination Routing User]: Set the VPN connection user to which the route points. In this example, it should be set to "Beijing".

⚠ **Attention: 『Network Number (Source)』 and 『Network Number (Destination)』 are** used to match the source IP address and destination IP address of the data. When the data transmitted in the VPN tunnel matches the setting, the routing setting takes effect and the data will be forwarded to the corresponding MIG device. The 『Destination Routing User』 can be understood as "to which MIG device will the routed data be sent". In this example, the Beijing branch has set up a VPN connection with the headquarters using the user name 『Beijing』 in the 『Connection Management』, so the data routed between tunnels is sent to the Shenzhen headquarters using the user name 『Beijing』 sign.

⚠Attention: The users used to add inter-tunnel routes must be users who do not allow multiple users to log in.

Step 3:In the 『Inter-tunnel Route Setting』 of the branch "Guangzhou", check [Enable], click Add, and add the route to "Beijing". The configuration is as follows:



Source IP: 10.1.1.0

Netmask: 255.255.255.0

Destination IP: 172.16.1.0

Netmask: 255.255.255.0

Dst Route User: actest

☑ Enabled □ Access Internet via destination route user

[Network Number (Source)]: Set the source address network number. In this example, it should be set to 10.1.1.0.

[Subnet Mask (Source)]: Sets the subnet mask of the source address. In this example, it should be set to 255.255.255.0.

[Network Number (Destination)]: Set the destination address network number. In this example, it should be set to 172.16.1.0.

[Subnet Mask (Destination)]: Set the subnet mask of the destination address. In this example, it should be set to 255.255.255.0.

[Destination Routing User]: Set the VPN connection user to which the route points. In this example, it should be set to "Guangzhou".

⚠ **Inter-tunnel routing does not need to be set up at the headquarters, but only needs to be configured at the two branch ends to realize mutual accesses between the two branches.**

4 Introduction of BBC's Management and Control of MIG

4.1. AutoVPN

At BBC end, AutoVPN can create SANGFOR VPN topology, configure basic information of VPN headquarters, select corresponding branch device, and other information is automatically generated by BBC.

After the VPN device is connected to the BBC, the establishment of the SANGFOR VPN network is completed by the BBC, and the branches do not need to do other configurations. The first is the BBC's automatic identification device, and then the VPN docking information of the headquarters and branches is configured in the BBC. The users and passwords of the branches connected to the headquarters are also automatically generated by the BBC.

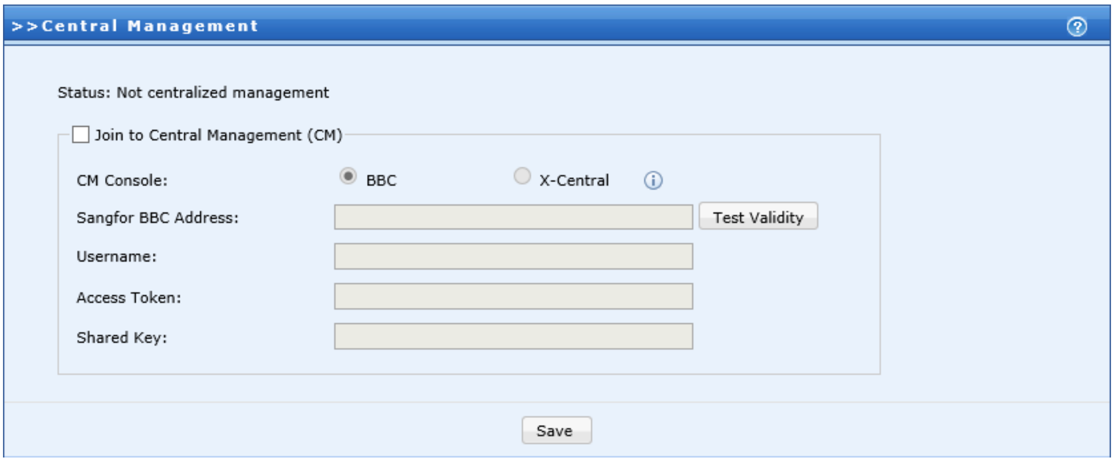
Finally, the SANGFOR VPN configuration will be issued, and the device connected to the BBC can get the corresponding configuration. The branch device then initiates a SANGFOR VPN connection to the VPN headquarters device and finally establishes a SANGFOR VPN network. The whole process realizes the scheme which is better than the traditional VPN network that requires device configuration at both the headquarters and branches.

After connecting to the BBC, the configuration of all the SANGFOR VPN networks is in the hands of the BBC, and there is also a general vision of planning. Maintenance personnel only need to configure in the BBC, which avoids the possibility of misconfiguration between branches and VPN headquarters in the previous version, and also reduces the configuration and maintenance costs of branches.

4.1.1. Establishment of SANGFOR VPN

The headquarters and branches join the BBC first, and the SANGFOR VPN configuration of the headquarters and branches will be configured on the BBC respectively. The branches and headquarters will obtain the configuration from the BBC subsequently.

VPN headquarters and branches respectively configure device to join BBC, as shown in the figure:



\>>Central Management

Status: Not centralized management

□ Join to Central Management (CM)

CM Console: ● BBC ○ X-Central

Sangfor BBC Address:

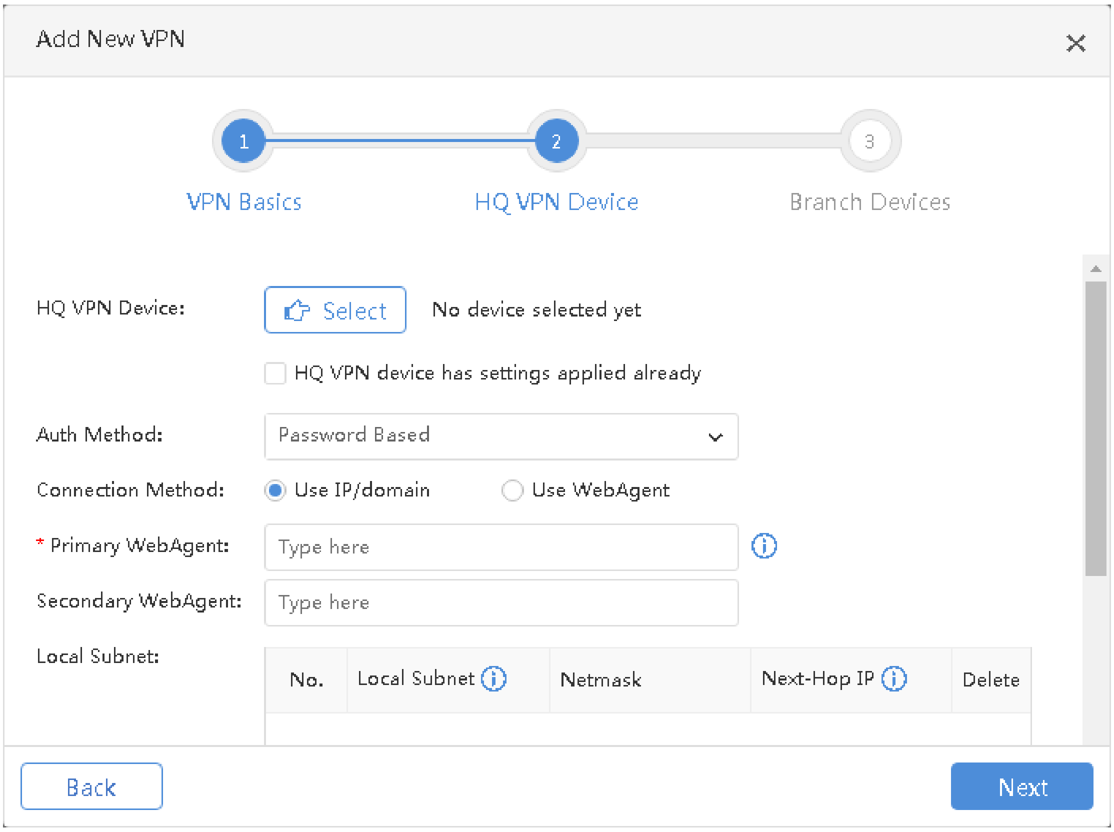
Username:

Access Token:

Shared Key:

Then, create a VPN topology on the BBC and set up the configuration of the headquarters and branches respectively.

Headquarter VPN Device Configuration: On BBC 【VPN】-【VPN Topology Management】-【New VPN Topology】, select the headquarter device connected to BBC (only device connected to BBC can be selected to form VPN network). Configure VPN related configuration, including webagent, VPN port, shared key, local subnet, etc. As shown below:



Add New VPN

HQ VPN Device: Select No device selected yet

□ HQ VPN device has settings applied already

Auth Method: Password Based

Connection Method: ● Use IP/domain ○ Use WebAgent

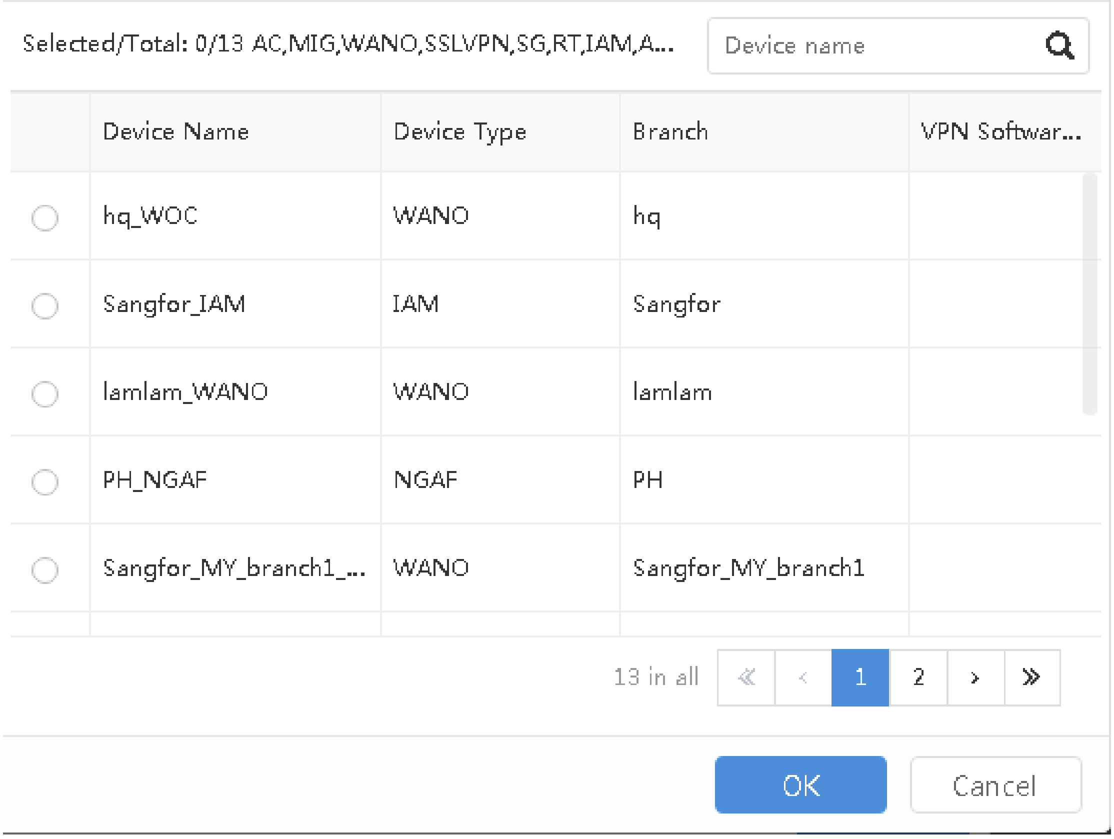
* Primary WebAgent: Type here

Secondary WebAgent: Type here

Local Subnet:

No.	Local Subnet	Netmask	Next-Hop IP	Delete

Branch VPN Device Configuration: After the headquarters device is configured in the above figure, select the corresponding branch network in 【VPN Branch Device】. It is no longer necessary to configure branch connection management as in the traditional scheme. Here, only the branch device needs to be selected, as shown in the figure:

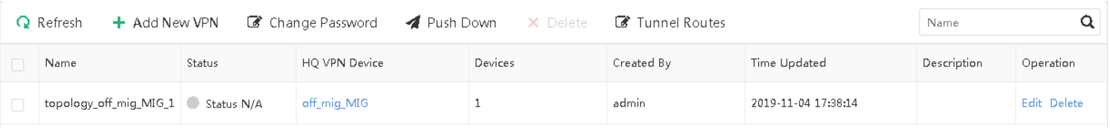


	Device Name	Device Type	Branch	VPN Softwar...
○	hq_WOC	WANO	hq	
○	Sangfor_IAM	IAM	Sangfor	
○	lamlam_WANO	WANO	lamlam	
○	PH_NGAF	NGAF	PH	
○	Sangfor_MY_branch1_...	WANO	Sangfor_MY_branch1	

After the configuration is completed, you can choose to issue the configuration to VPN hardware devices. The branch initiates VPN connection to the headquarters according to its own configuration, and finally forms VPN network.

4.1.2. VPN Topology Reporting

The existing VPN connection topology can be automatically reported to BBC. When the controlled end accesses the BBC for the first time, it will report the existing VPN connection configuration, and the BBC will automatically identify the VPN topology according to the reported VPN connection. As shown below:



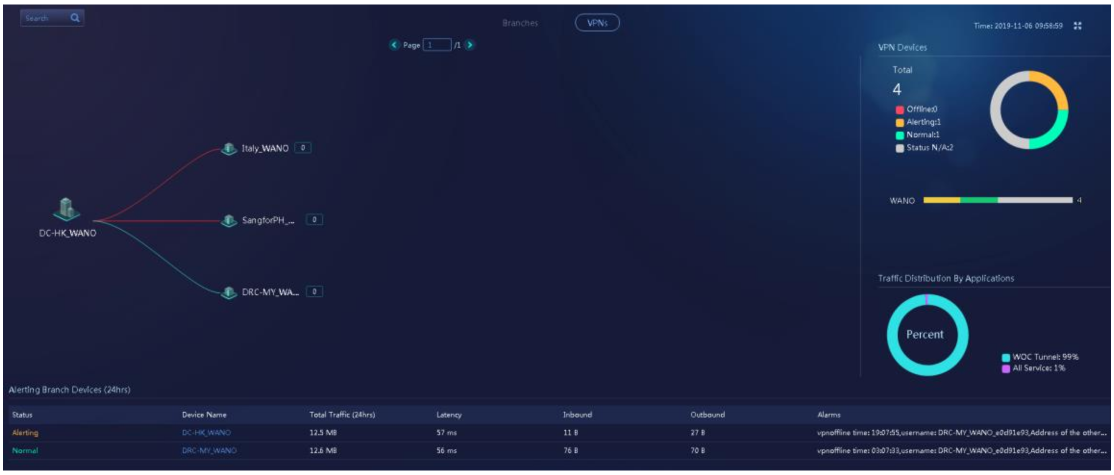
□	Name	Status	HQ VPN Device	Devices	Created By	Time Updated	Description	Operation
□	topology_off_mig_MIG_1	● Status N/A	off_mig_MIG	1	admin	2019-11-04 17:38:14		Edit Delete

Attention: When the VPN topology is automatically reported, the BBC can recognize the topology only if the webagent set in the basic configuration of the VPN headquarters is consistent with the webagent set in the branch connection management configuration.

4.1.3. VPN Status Visualization-Topology Large Screen

After the VPN identifies the topology, it can display on a large screen. On the BBC port, at the path of 【VPN】-【VPN Device Overview】-【VPN Status Large Screen】, a large screen of topology can be displayed . It can directly view the VPN link status, traffic composition and other information.

As shown below:

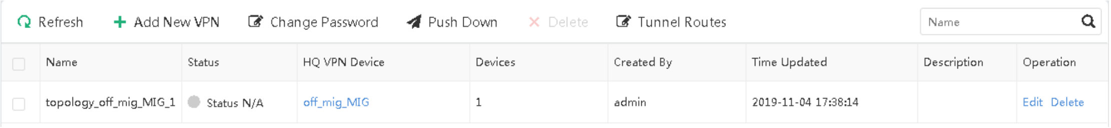


Alerting Branch Devices (24hrs)

Status	Device Name	Total Traffic (24hrs)	Latency	Inbound	Outbound	Alarms
Alerting	DC-HK_WANO	12.5 MB	57 ms	11 B	27 B	vpnoffline time: 19:07:55,username: DRC-MY_WANO_e0d91e93,Address of the other...
Normal	DRC-MY_WANO	12.6 MB	56 ms	76 B	70 B	vpnoffline time: 03:07:33,username: DRC-MY_WANO_e0d91e93,Address of the other...

4.1.4. VPN Status Visualization-Device List

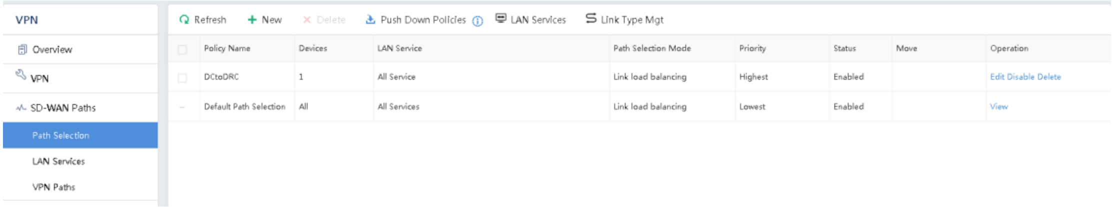
The BBC can show the status of VPN sites across the network through a list, and click on specific VPN devices to see which VPN devices are connected to the VPN devices and their corresponding connection status. As shown below:



□	Name	Status	HQ VPN Device	Devices	Created By	Time Updated	Description	Operation
□	topology_off_mig_MIG_1	● Status N/A	off_mig_MIG	1	admin	2019-11-04 17:38:14		Edit Delete

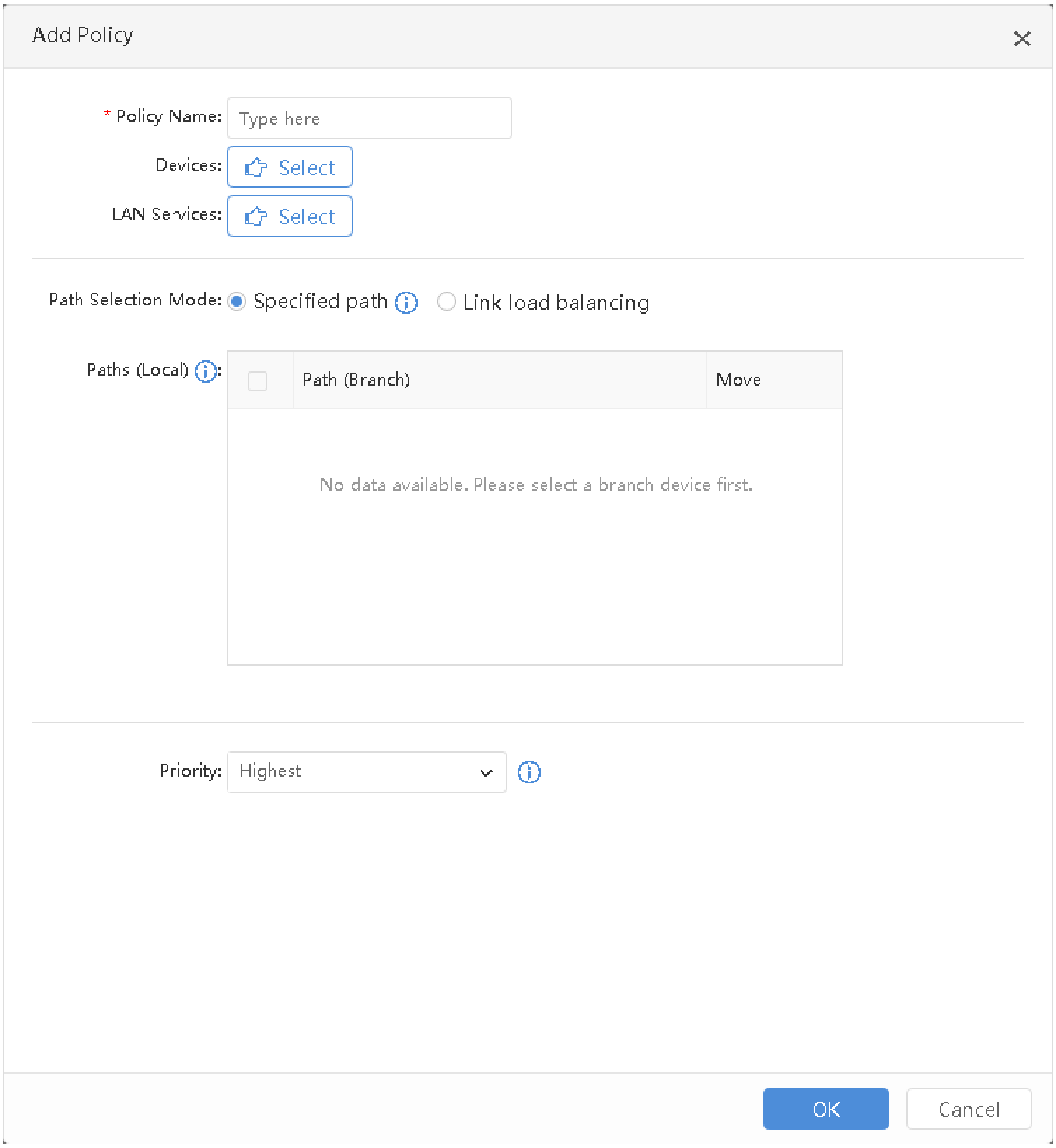
4.2. SD-WAN Intelligent Routing

In the BBC, 【VPN】-【SD-WAN Intelligent Routing】-【Policy Issuance】 can issue the SD-WAN policy configuration on the BBC to MIG branches. On MIG, the issued SD-WAN policy cannot be viewed. The interface is shown as follows:



□	Policy Name	Devices	LAN Service	Path Selection Mode	Priority	Status	Move	Operation
□	DCtoDRC	1	All Service	Link load balancing	Highest	Enabled		Edit Disable Delete
-	Default Path Selection	All	All Services	Link load balancing	Lowest	Enabled		View

Click 【Add】, and the interface is as follows:



Add Policy

* Policy Name: Type here

Devices: Select

LAN Services: Select

Path Selection Mode: ● Specified path ○ Link load balancing

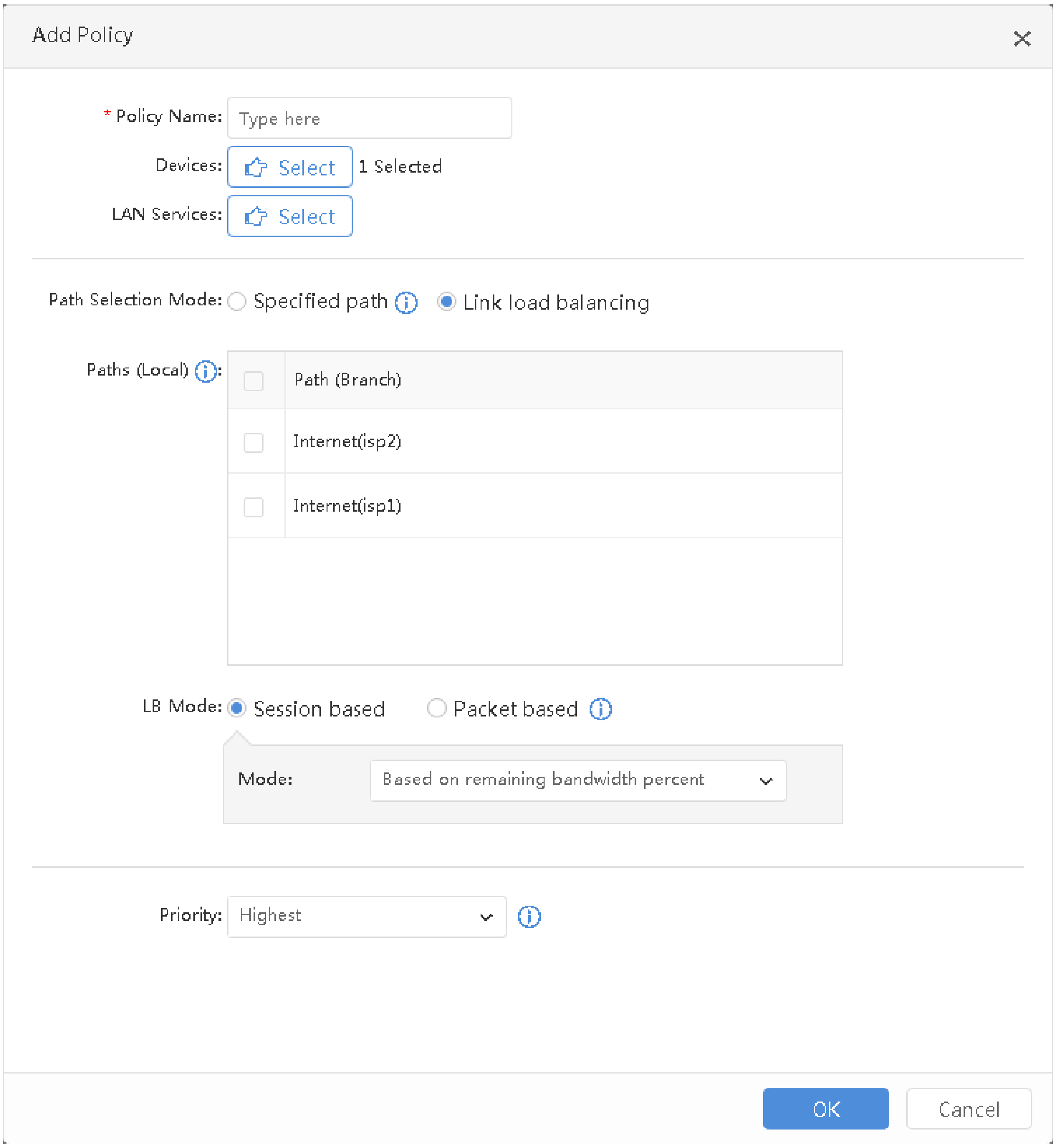
Paths (Local):

□	Path (Branch)	Move

No data available. Please select a branch device first.

Priority: Highest

Enter the name of VPN topology, select the effective device, LAN service, routing mode, flow control priority and other configurations. If you choose to configure the multi-line load instead of configuring the designated line for running application, the interface description is as follows:



Add Policy

* Policy Name: Type here

Devices: Select 1 Selected

LAN Services: Select

Path Selection Mode: ○ Specified path ● Link load balancing

Paths (Local):

□	Path (Branch)
□	Internet(isp2)
□	Internet(isp1)

LB Mode: ● Session based ○ Packet based

Mode: Based on remaining bandwidth percent

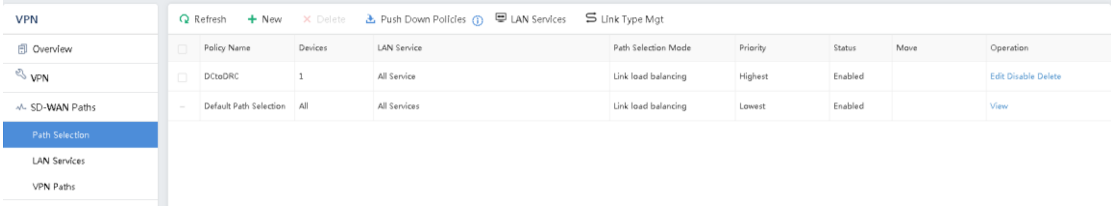
Priority: Highest

Description:

1. The proportional load of the remaining bandwidth is to select the optimal line according to the proportion of the remaining bandwidth.

2. Line quality routing is to calculate a line with the best quality according to the packet loss probability, delay and jitter of the line, and then select the routing.

After the configuration is completed, click 【OK】 to save. After saving, you can see the established policy, as shown in figure:



□	Policy Name	Devices	LAN Service	Path Selection Mode	Priority	Status	Move	Operation
□	DCtoDRC	1	All Service	Link load balancing	Highest	Enabled		Edit Disable Delete
–	Default Path Selection	All	All Services	Link load balancing	Lowest	Enabled		View

Click 【Policy Delivery】 to issue the configured routing policy to the device connected to BBC.

⚠Attention:

1. If SD-WAN configuration is not issued immediately, it will not be automatically issued until 30 minutes later.

2. In addition to the designated line, the routing policy of SD-WAN can also choose the route according to the proportion of the remaining bandwidth of the line and the priority of using the line with the best quality.

Appendix: Use the RESET key to restore the default configuration and password.

When MIG device is powered on, press and hold the RESET key. After 3 seconds, the ALARM indicator will start blinking red. Then release the RESET key, and the ALARM indicator will keep on. When the ALARM indicator goes out, it means that the default configuration is restored successfully. At this time, the device can be logged in using the default factory IP address through the device LAN/DMZ interface, and the login user name and password are restored to the default values.