Ruijie Networks – Innovation Beyond Networks

RG-EG Implementation Cookbook (V1.0)

Copyright Statement

Exemption Statement

This document is provided “as is”. The contents of this document are subject to change without any notice. Please obtain the latest information through the Ruijie Networks website. Ruijie Networks endeavors to ensure content accuracy and will not shoulder any responsibility for losses and damages caused due to content omissions, inaccuracies or errors.

1 Preface

Audience

- Network Engineers
- Network Administrator

Obtain Technical Assistance

- Ruijie Networks Websites: http://www.ruijienetworks.com
- Ruijie Service Portal: http://caseportal.ruijienetworks.com

Welcome to report error and give advice in any Ruijie manual to Ruijie Service Portal

Revision History

Date	Change contents	Reviser
2019.5	Initial publication V1.0	GTAC

Contents

2 Product Introduction

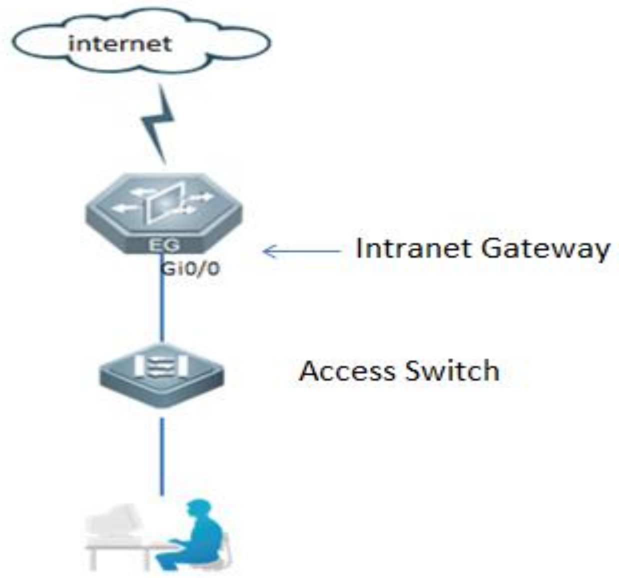
2.1 Product Abstract

RG-EG series business assurance gateway (Following will call it RG-EG) is the product that Ruijie research and develop by itself. RG-EG aimed at soloving export problems for small and medium-sized enterprises. RG-EG series product is equiped with advanced software and firmware structure. Not only has efficient NAT forwarding performance as professional export device, but also equiped with flow control, intelligent routing, behavior management, security, WEB authentication, VPN and other function. We don't need to consider using router, firewall or flow control device, only using a RG-EG series product can meet all your requirements.

2.2 Working Mode

EG has 3 working modes：Gateway mode, bridge mode and bypass mode. Gateway mode and bridge mode are common used. (EG 2100-P don’t have bridge mode)

A. Gateway Mode：Regard EG as the export of network and supports the forwarding of NAT and routing.

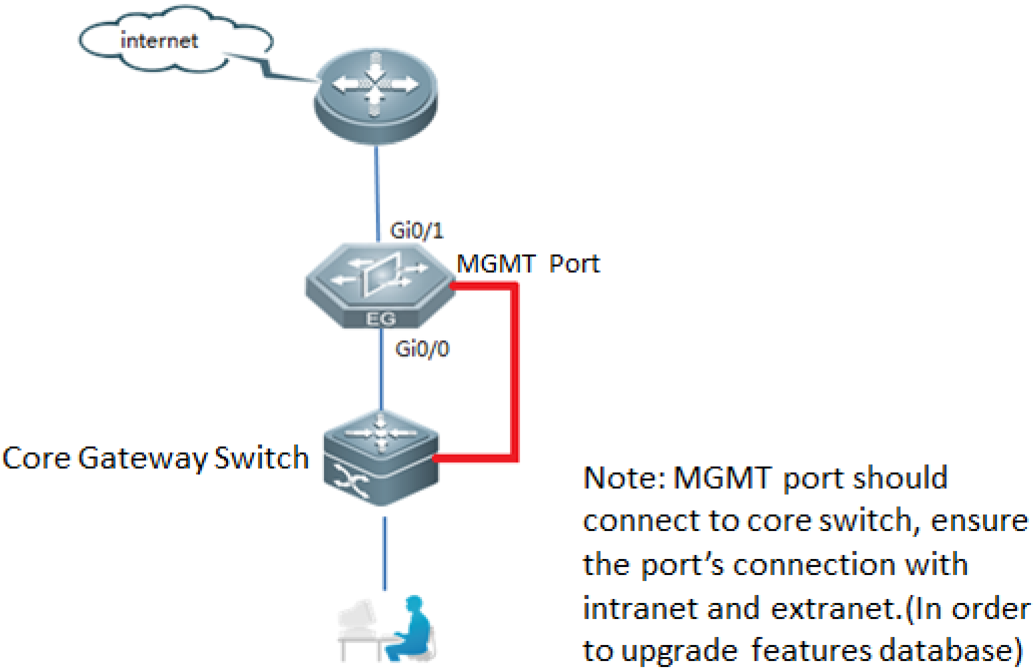


B. Bridge Mode：Regard EG as a bridge, Deploy EG in between intranet core switch and extranet gateway export. Bridge mode is divided into 3 types：Forward/Sniffer/Bypass.

Foeward：Can realize flow audit, application recognition, application block, flow control.

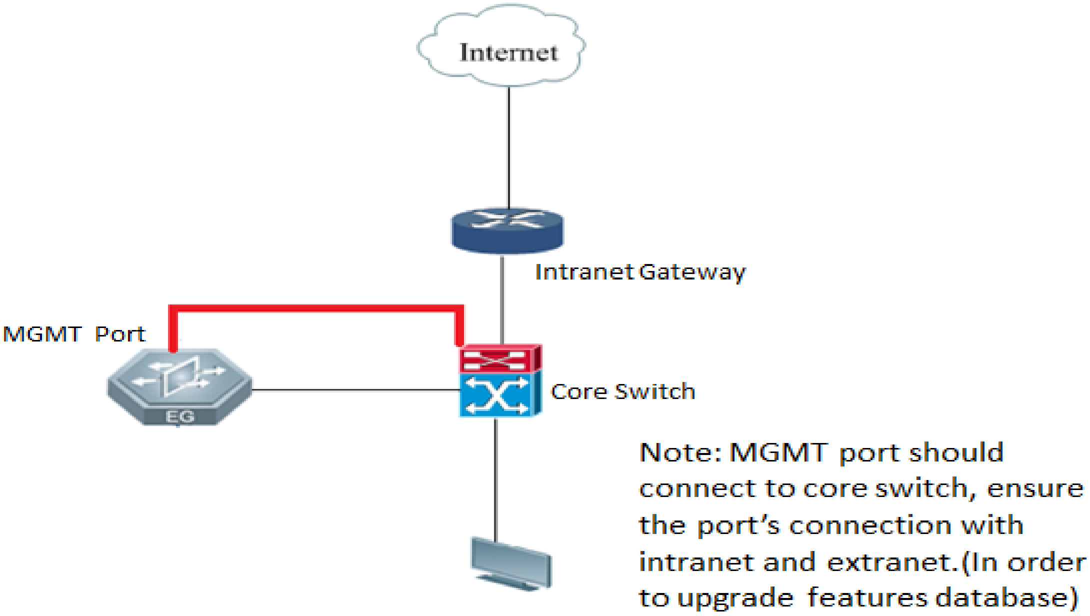
Sniffer：Can realize flow audit, application recognition.

bypass：Packets can be forwarded without dealing with.



Note: MGMT port should connect to core switch, ensure the port's connection with intranet and extranet.(In order to upgrade features database)

C. Bypass Mode： Can only realize application recognition, only receieve packet, not forward.



Note: MGMT port should connect to core switch, ensure the port's connection with intranet and extranet.(In order to upgrade features database)

3 Daily Maintenance

3.1 Device Login

3.1.1 WEB Login

1) Modify the IP address of PC.

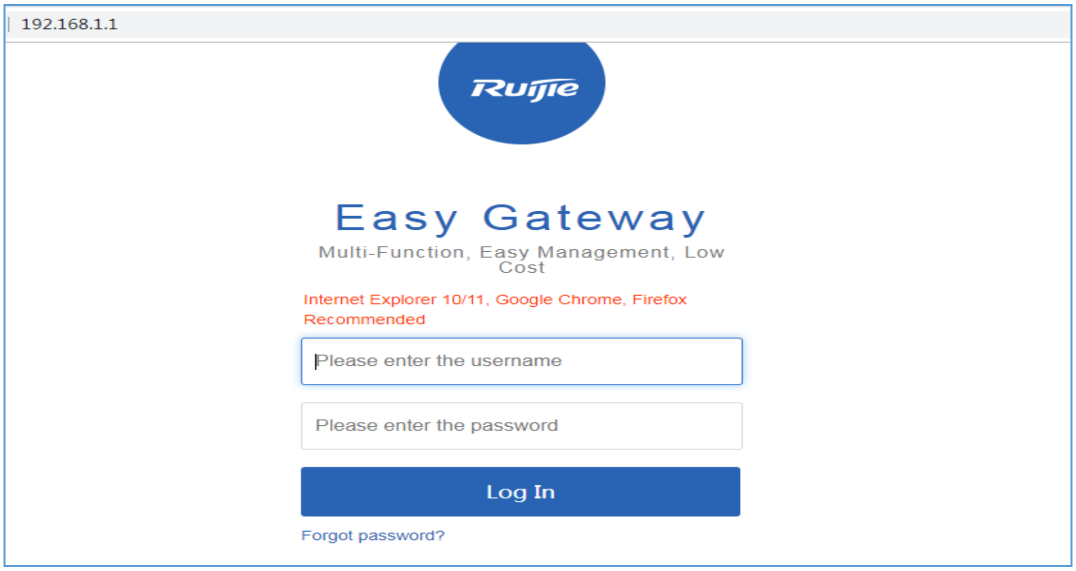
IP address: 192.168.1.x (except 192.168.1.1)

Subnet mask: 255.255.255.0

Default gateway: 192.168.1.1 (default LAN IP)

2) Connect the PC to any port (except WAN0) on the device.

3) Visit http://192.168.1.1 by Chrome browser.



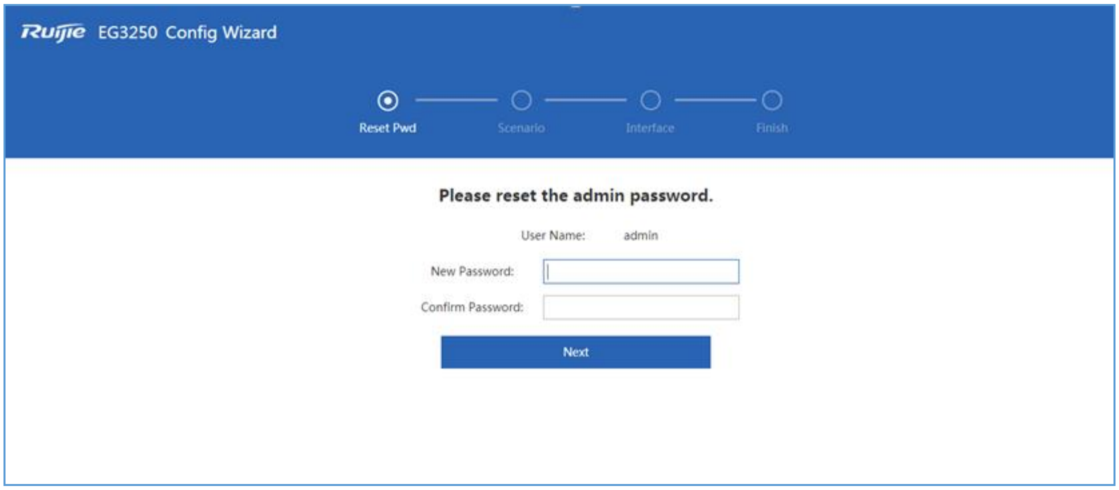
192.168.1.1
Ruijie
Easy Gateway
Multi-Function, Easy Management, Low Cost
Internet Explorer 10/11, Google Chrome, Firefox Recommended
Please enter the username
Please enter the password
Log In
Forgot password?

4) Enter the username and password on the login page and click “Log In”.

Default Username: admin

Default Password: admin

5) Change the password at the first login.



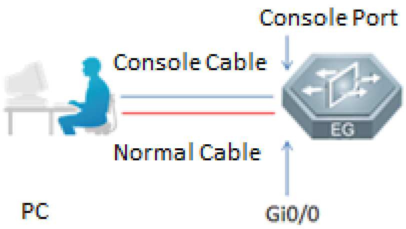
Please reset the admin password.

User Name: admin

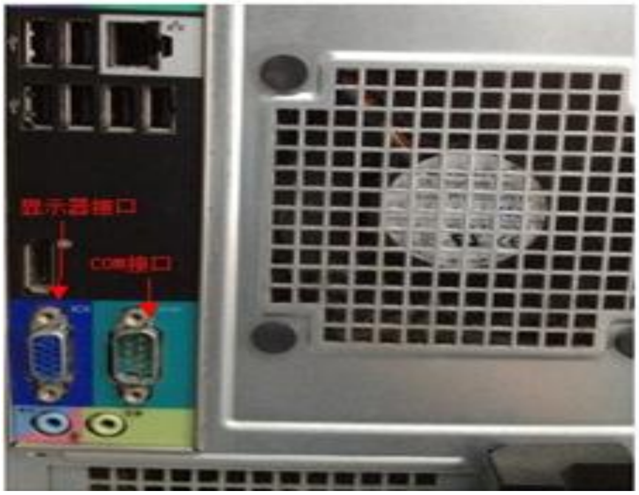
New Password:

Confirm Password:

3.1.2 Console Login



- Tools Needed：PUTTY (or others) software in your computer, console cable (as shown on the left), computer with COM port. If your computer doesn't have COM port, please buy COM to USB cable (as shown on the right) by yourself.

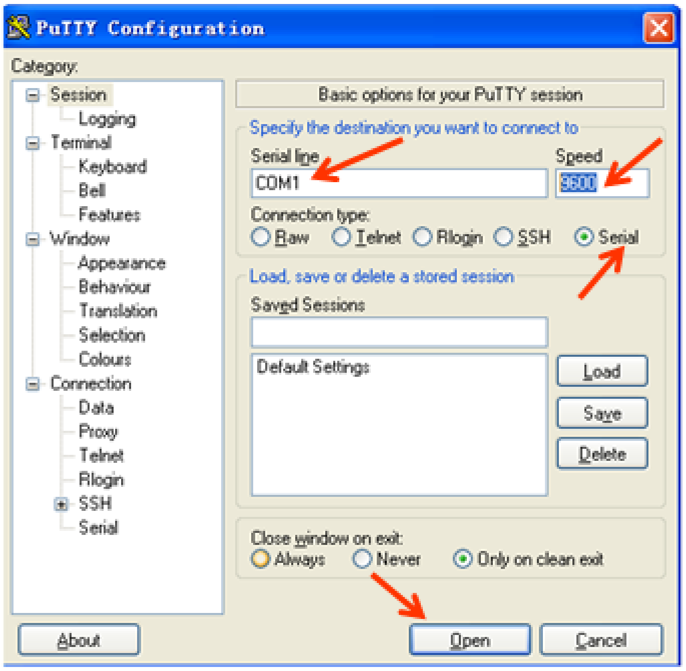


- Operation Steps:

Step 1-Connect console cable to EG console port.

Step 2-Check your COM port number in your computer 'Device manager'. You should install drivers first or you won't see the COM port number.

Step 3-Open PUTTY and change the protocol to 'Serial'.Choose your COM port number, set baud rate to 9600, uncheck RTS/CTS.Then click 'Open' button.



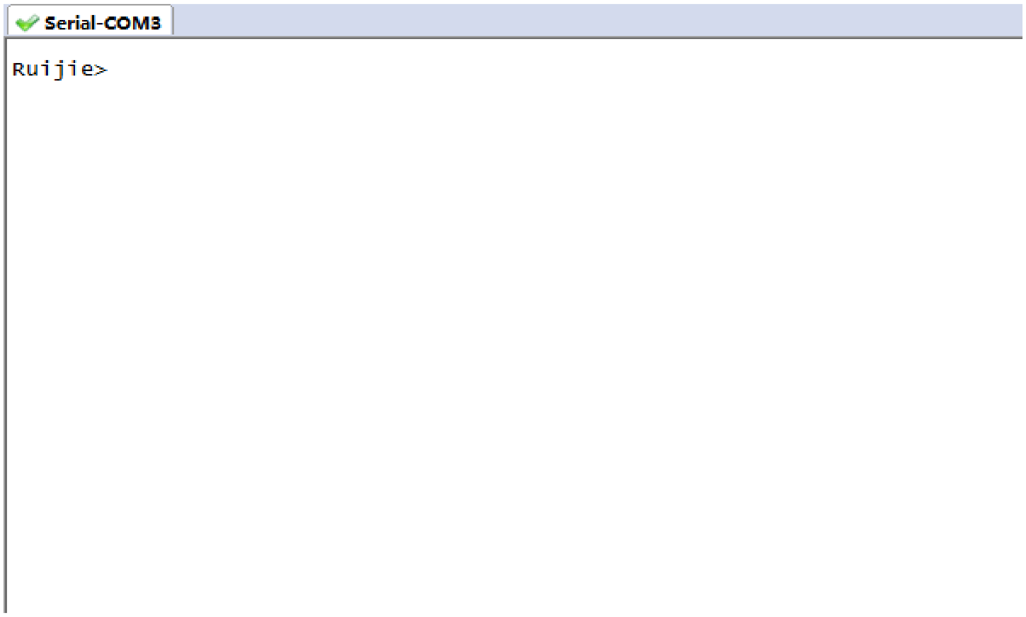
Serial line: COM1

Speed: 9600

Connection type: ○ Raw ○ Telnet ○ Rlogin ○ SSH ● Serial

Close window on exit: ○ Always ○ Never ● Only on clean exit

Step 4-Press 'Enter' to enter user mode.



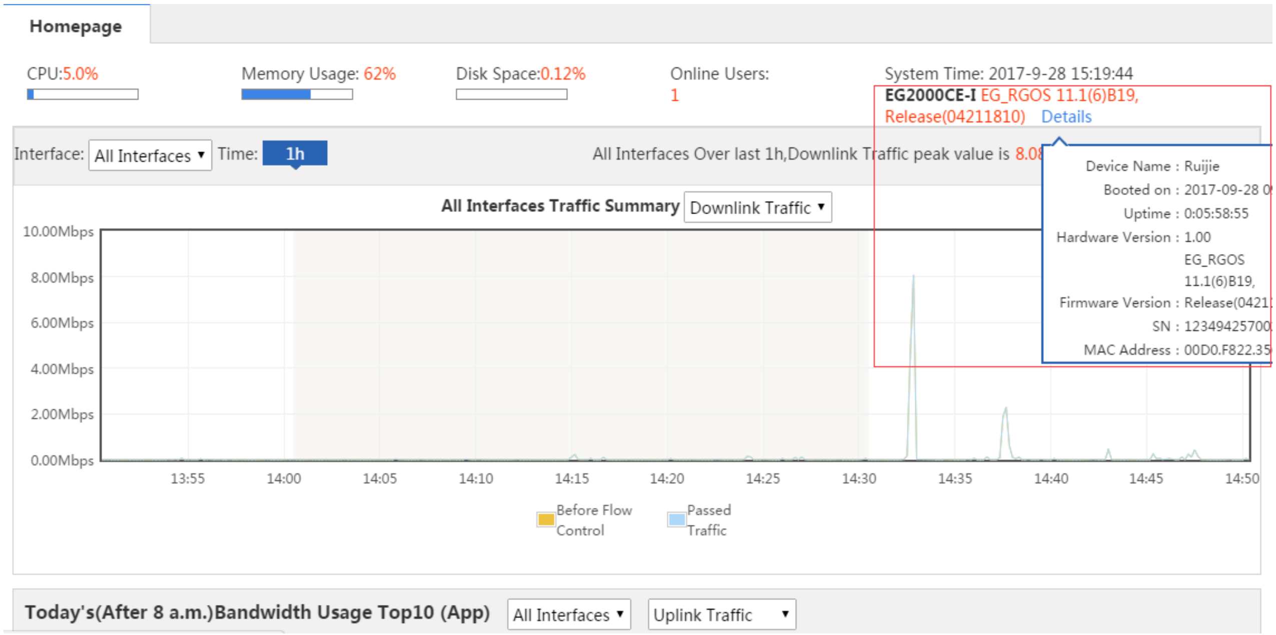
```
Ruijie>
```

3.2 Software Maintenance

3.2.1 Software Information Check

Main Process Software Version Check：

You can see product model and software version information on web home page.



CPU:5.0%

Memory Usage: 62%

Disk Space:0.12%

Online Users: 1

System Time: 2017-9-28 15:19:44

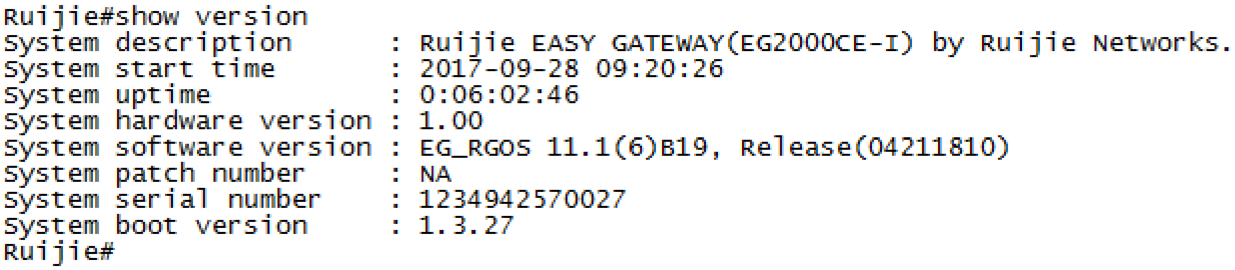
EG2000CE-I EG_RGOS 11.1(6)B19, Release(04211810) Details

All Interfaces Over last 1h,Downlink Traffic peak value is 8.08

Device Name : Ruijie
Booted on : 2017-09-28 0
Uptime : 0:05:58:55
Hardware Version : 1.00
Firmware Version : EG_RGOS 11.1(6)B19, Release(0421
SN : 12349425700
MAC Address : 00D0.F822.35

Today's(After 8 a.m.)Bandwidth Usage Top10 (App)

You can also use the command ‘show version’ in CLI.



```
Ruijie#show version
System description      : Ruijie EASY GATEWAY(EG2000CE-I) by Ruijie Networks.
System start time       : 2017-09-28 09:20:26
System uptime           : 0:06:02:46
System hardware version : 1.00
System software version : EG_RGOS 11.1(6)B19, Release(04211810)
System patch number     : NA
System serial number    : 1234942570027
System boot version     : 1.3.27
Ruijie#
```

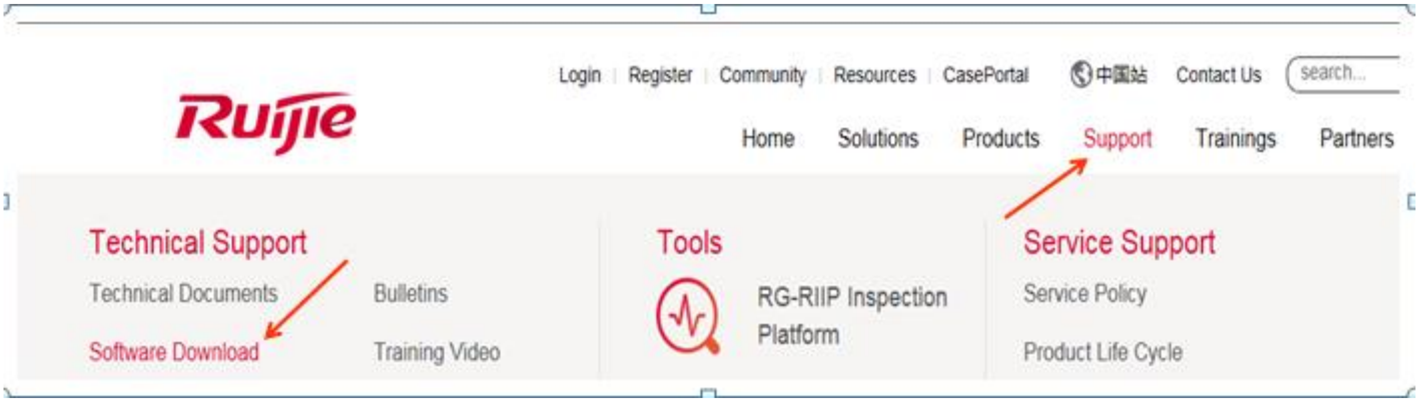
3.2.2 Software Version Upgrade

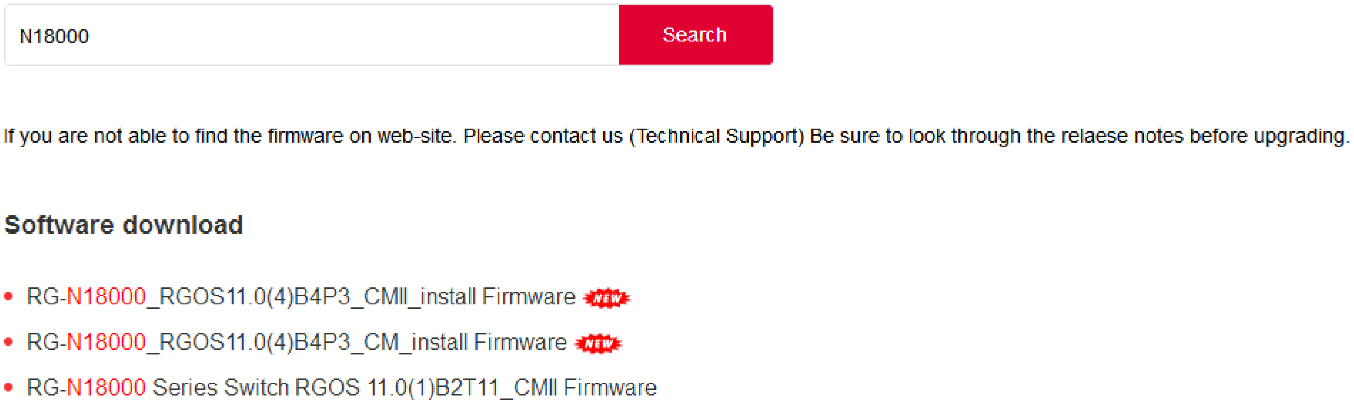
Note:

1. Upgrading needs to restart, please upgrade in the time section that allow to break network. Upgrading will last about 10 minutes.

2. Download corresponding software version according to product model. Ensure software version and device model are matching. Please read version issue statement carefully before upgrading.

Note: Download software on our official website (http://www.ruijienetworks.com/), click ‘Support’ then choose ‘Software Download’. Then you should input your product model or key words to search the latest software version and other versions. Take RG-N18000 as an example.





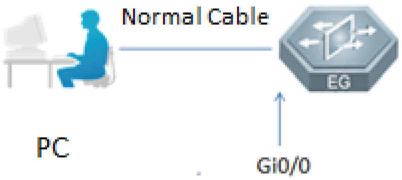
If you are not able to find the firmware on web-site. Please contact us (Technical Support) Be sure to look through the relaese notes before upgrading.

Software download

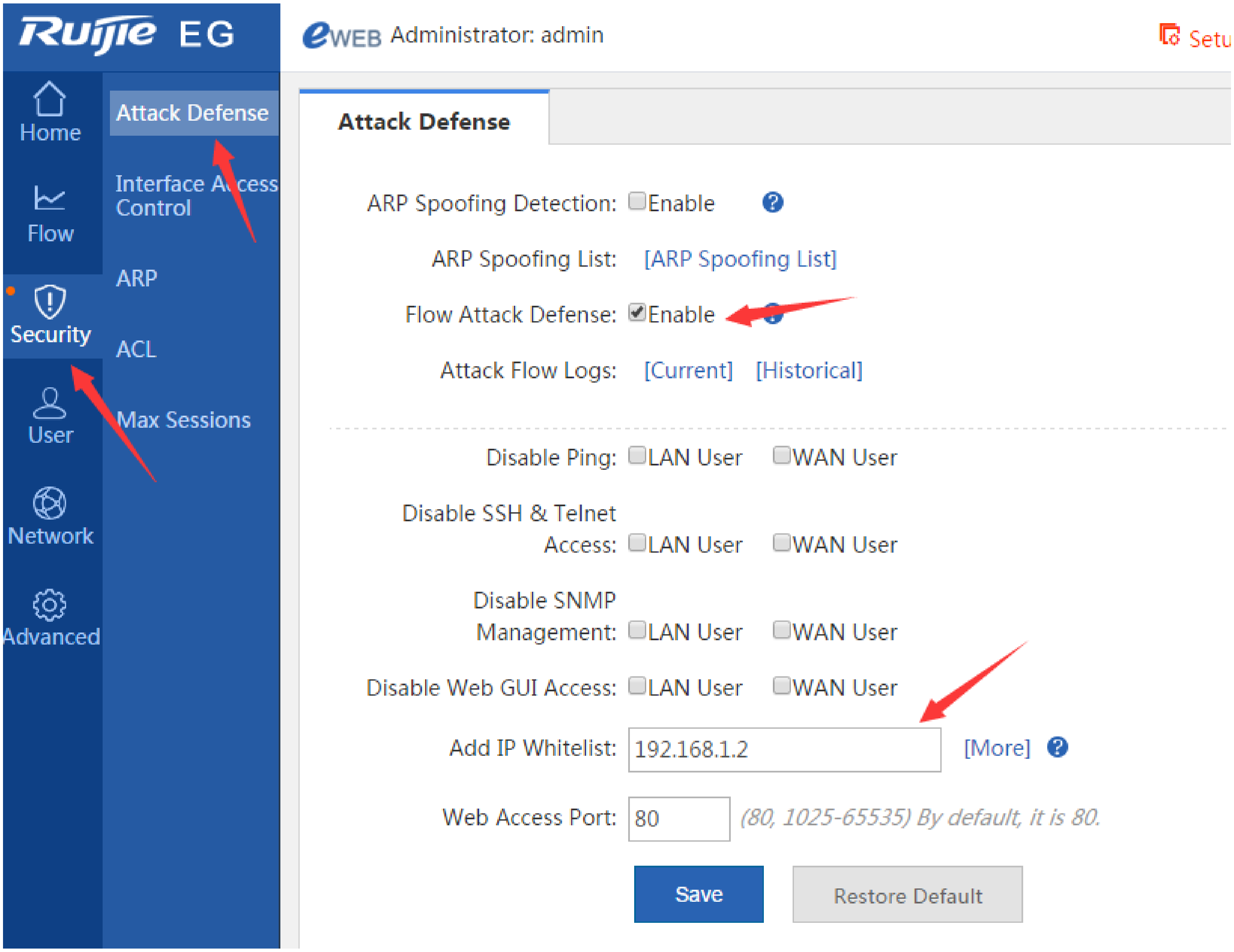
- RG-N18000_RGOS11.0(4)B4P3_CMII_install Firmware NEW
- RG-N18000_RGOS11.0(4)B4P3_CM_install Firmware NEW
- RG-N18000 Series Switch RGOS 11.0(1)B2T11_CMII Firmware

3. Shut down EG attack defense function, or add the PC IP address for upgrading into management IP address.

A. Use WEB to upgrade



1. You can shut down attack defense function or add management IP address as below. If you have shut down ‘Flow Attack Defense’, you don’t need to add management IP.



ARP Spoofing Detection: □Enable

ARP Spoofing List: [ARP Spoofing List]

Flow Attack Defense: ☑Enable

Attack Flow Logs: [Current] [Historical]

Disable Ping: □LAN User □WAN User

Disable SSH & Telnet Access: □LAN User □WAN User

Disable SNMP Management: □LAN User □WAN User

Disable Web GUI Access: □LAN User □WAN User

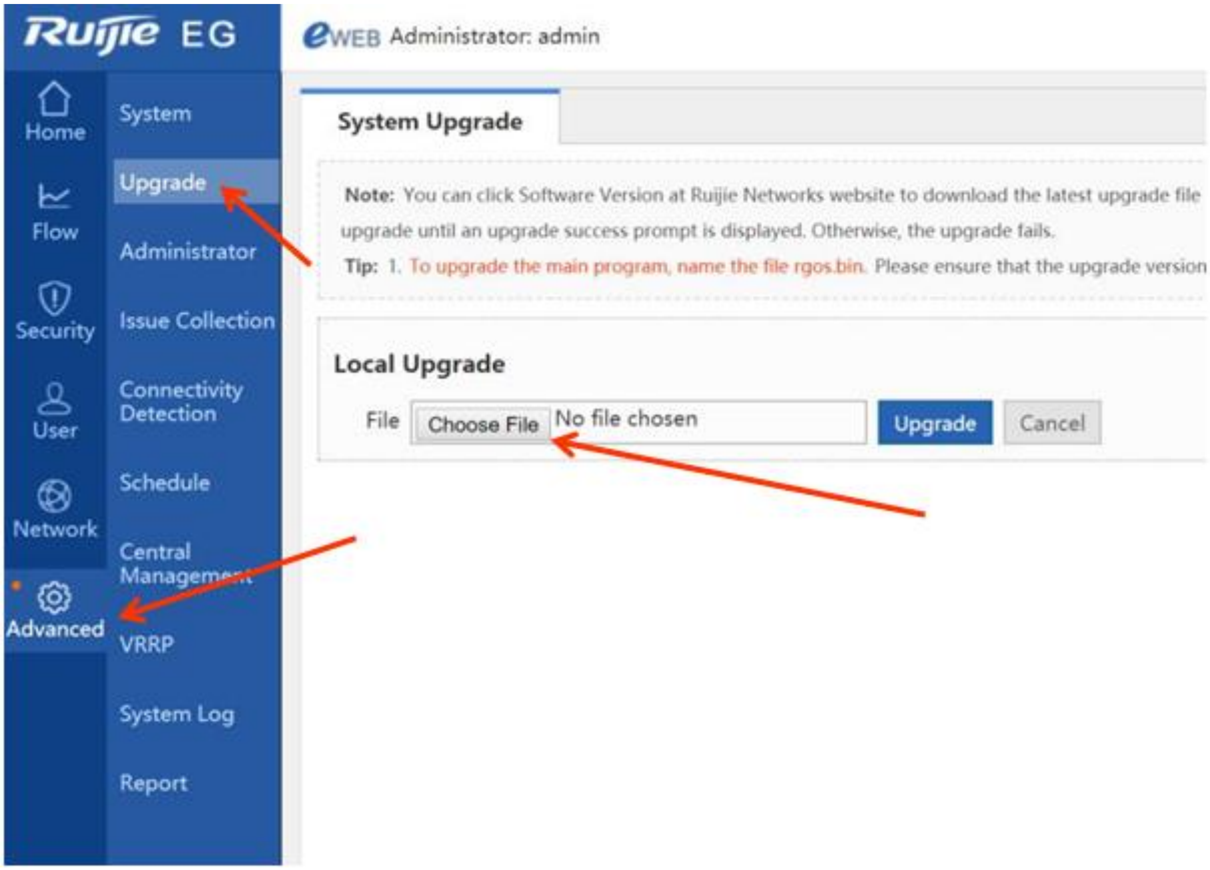
Add IP Whitelist: 192.168.1.2 [More]

Web Access Port: 80 *(80, 1025-65535) By default, it is 80.*

2. Then click ‘Advanced’, choose ‘Upgrade’, click ‘Browse’ to choose the upgrading file you downloaded then click ‘Upgrade’.

Note： Before choosing the upgrading file, you should change the file name as ‘rgos.bin’.

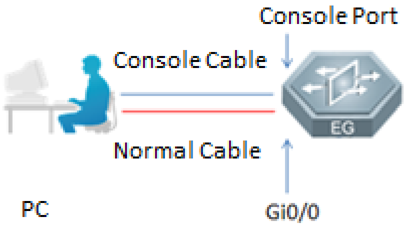
After finishing upgrading, it prompt you to restart device, you should click ‘OK’. After restarting, upgrading is successful.



Note: You can click Software Version at Ruijie Networks website to download the latest upgrade file upgrade until an upgrade success prompt is displayed. Otherwise, the upgrade fails.

Tip: 1. To upgrade the main program, name the file rgos.bin. Please ensure that the upgrade version

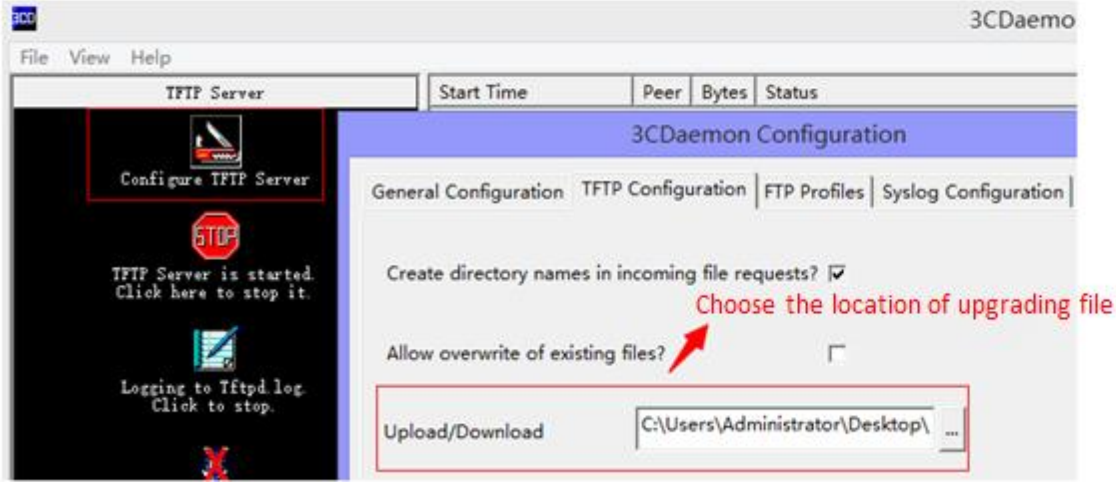
B. Use console to upgrade



1. Change the file name as ‘rgos.bin. Because of 11.X version is large, so using CLI to upgrade should download ‘3CDaemon’ tftp tool. If you don’t use this tool, it will lead to upgrading failure.

Note：Please check windows firewall, anti-virus software setting, system security and so on before upgrading. You can only open 1 TFTP server to prevent port conflicts.

2. Open 3CDaemon to run TFTP server and choose file location.



Create directory names in incoming file requests? ☑

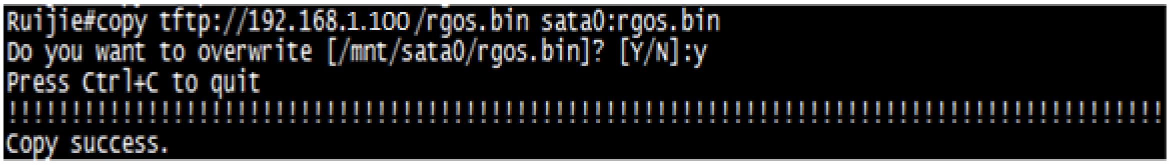
Choose the location of upgrading file

Allow overwrite of existing files? □

Upload/Download C:\Users\Administrator\Desktop\

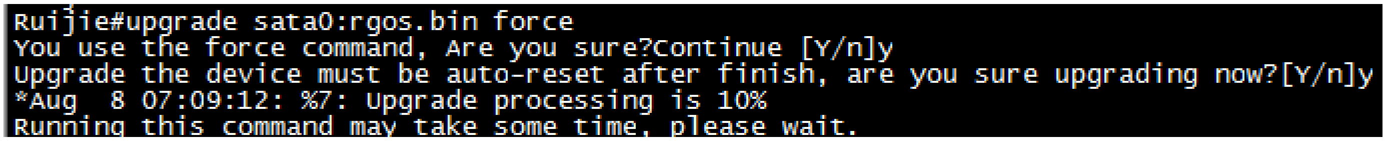
3. Using console login device. Input command ‘copy tftp://192.168.1.100/rgos.bin sata0:rgos.bin’ and press ‘Enter’.

Note：192.168.1.100 is your computer IP address.



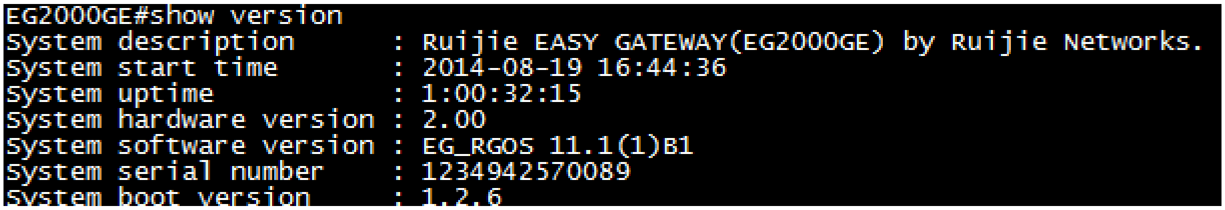
```
Ruijie#copy tftp://192.168.1.100/rgos.bin sata0:rgos.bin
Do you want to overwrite [/mnt/sata0/rgos.bin]? [Y/N]:y
Press Ctrl+C to quit
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Copy success.
```

4. After importing main process, don’t restart. Input command ‘upgrade sata0:rgos.bin force’ to update main process.



```
Ruijie#upgrade sata0:rgos.bin force
You use the force command, Are you sure?Continue [Y/n]y
Upgrade the device must be auto-reset after finish, are you sure upgrading now?[Y/n]y
*Aug  8 07:09:12: %7: Upgrade processing is 10%
Running this command may take some time, please wait.
```

5. You can input command ‘show version’ to check version information.



```
EG2000GE#show version
System description      : Ruijie EASY GATEWAY(EG2000GE) by Ruijie Networks.
System start time       : 2014-08-19 16:44:36
System uptime           : 1:00:32:15
System hardware version : 2.00
System software version : EG_RGOS 11.1(1)B1
System serial number    : 1234942570089
System boot version     : 1.2.6
```

3.3 Password Recovery

Note：

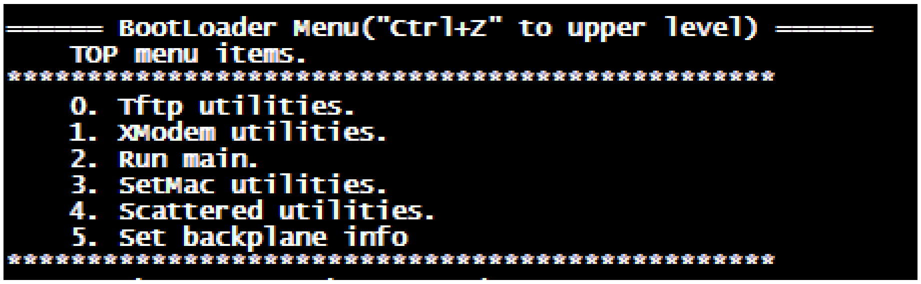
1. Please prepare console cable ahead of time.

2. Password recovery will lead to device restart and break network. Please choose the time section allowing network broken.

- Operation Steps：

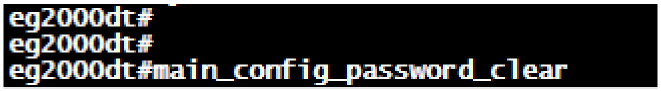
Step 1-Open your PUTTY or other control softwares, press ‘Enter’ to enter user mode. (Ruijie>)

Step 2-Turn off the power then turn on, input ‘ctrl+c’ in PUTTY consecutively until following menu appear.



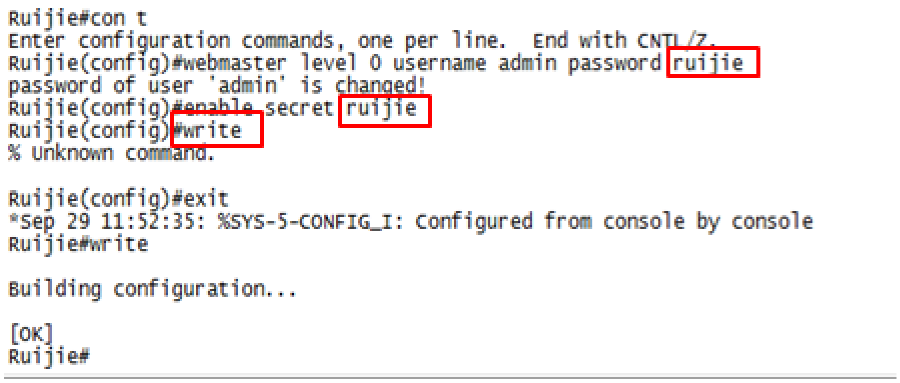
```
====== BootLoader Menu("Ctrl+Z" to upper level) ======
    TOP menu items.
************************************************
    0. Tftp utilities.
    1. XModem utilities.
    2. Run main.
    3. SetMac utilities.
    4. Scattered utilities.
    5. Set backplane info
************************************************
```

Step 3-Press ‘ctrl+q’ to enter uboot CLI, input command ‘main_config_password_clear’ then press ‘Enter’. After that device will restart, and don’t need password to enter system this time.



```
eg2000dt#
eg2000dt#
eg2000dt#main_config_password_clear
```

Step 4-Change your password in privileged mode. For example, in the following picture 1, we set new web management and CLI privileged mode password as ‘ruijie’ then input ‘write’ to save your configuration.

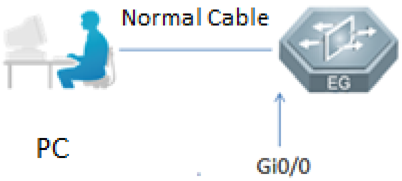


```
Ruijie#con t
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#webmaster level 0 username admin password ruijie
password of user 'admin' is changed!
Ruijie(config)#enable secret ruijie
Ruijie(config)#write
% Unknown command.

Ruijie(config)#exit
*Sep 29 11:52:35: %SYS-5-CONFIG_I: Configured from console by console
Ruijie#write

Building configuration...

[OK]
Ruijie#
```

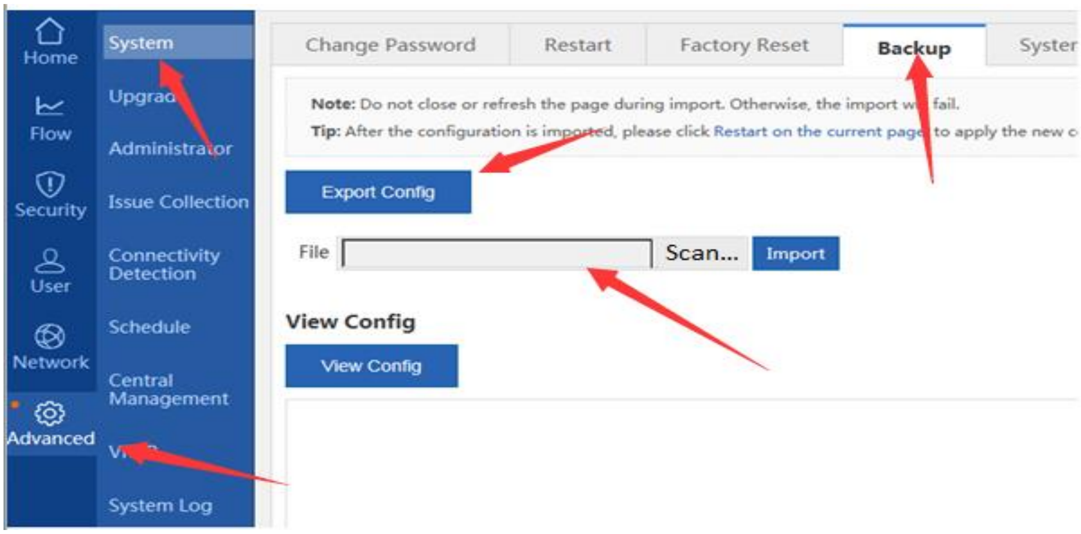
Step 5-You could access web page to confirm if it is successful.

3.4 Configuration Backups

- Use WEB to backups



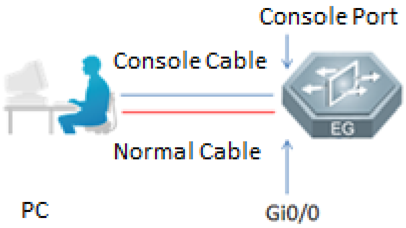
Click ‘Advanced’, choose ‘System’, choose ‘Backup’, click ‘Export Config’ and choose save location for configuration export. Click ‘Scan…’ and choose configuration file then click ‘Import’ for import.



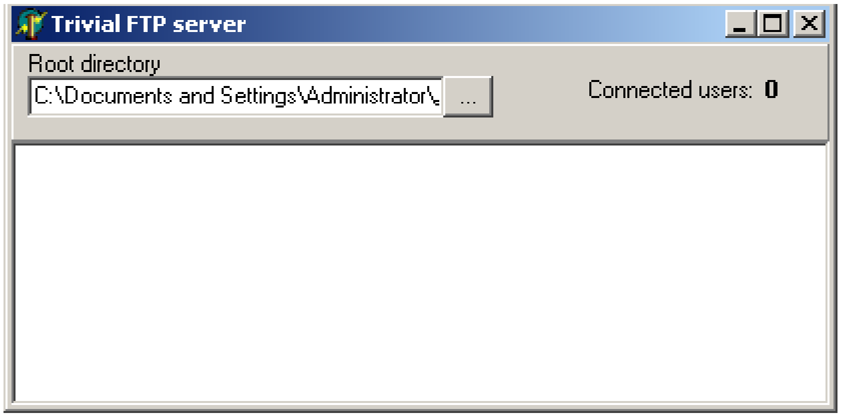
Note: Do not close or refresh the page during import. Otherwise, the import will fail.

Tip: After the configuration is imported, please click Restart on the current page to apply the new c

➢ Use CLI to backups



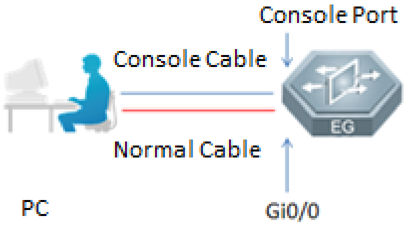
1. Open TFTP software in your computer.



2. Input command 'copy flash:config.text tftp://192.168.1.100/config.text', 192.16.1.100 is your computer IP address.

3. If you see the prompt 'Transmission success,file length 50281 bytes', it means successful.

3.5 Main Process Recovery (Layer Ctrl Upgrade)



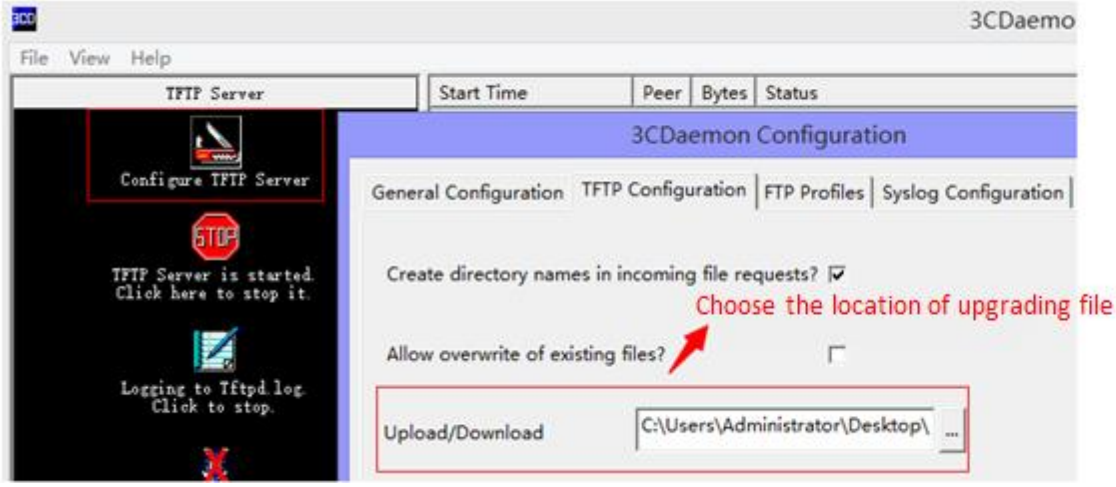
Note： If the main process of device is lost because of some reasons, please try to recover it through ctrl layer. Main process lost will lead to PWR and SYS light always on, but other port lights not on.

➢ Operation Steps：

Step 1-Download the main process from our official website. Detailed steps please refer to 4.2.2.

Step 2-Change file name as 'rgos.bin'.

Step 3-Open 3CDaemon to run TFTP server and choose file location.



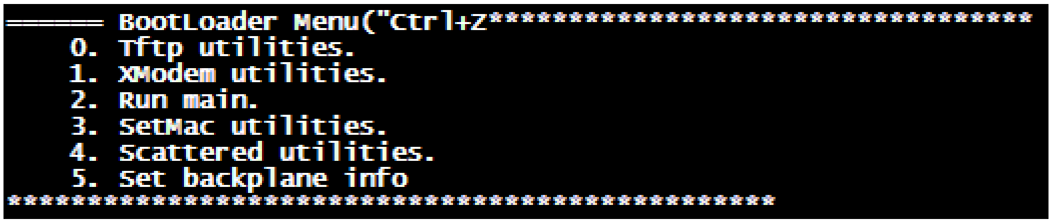
Create directory names in incoming file requests? ☑

Allow overwrite of existing files? ☐

Upload/Download C:\Users\Administrator\Desktop\

Choose the location of upgrading file

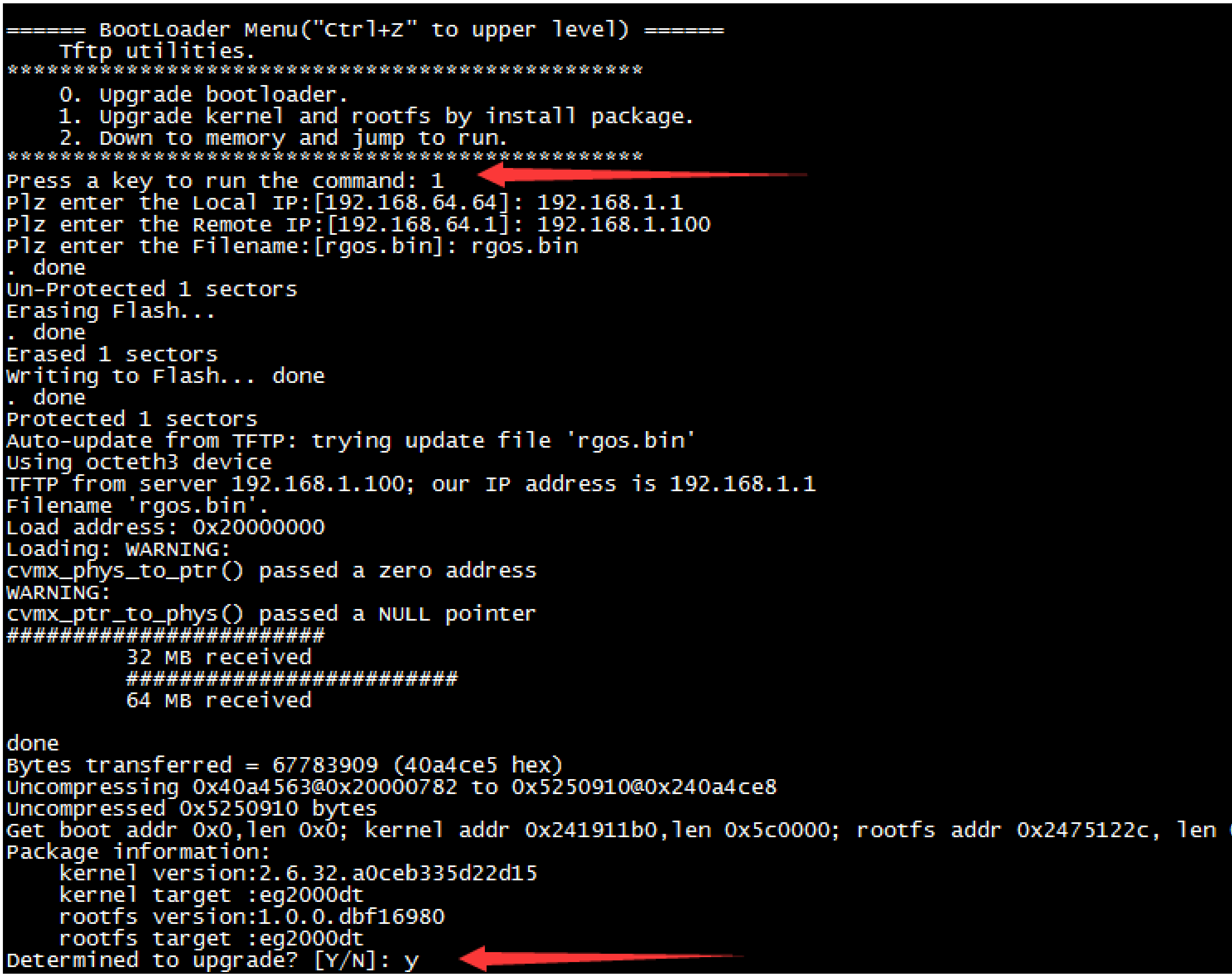
Step 4-Open PUTTY, turn off power then turn on. Input 'ctrl+c' in PUTTY consecutively until following menu appear.



```
====== BootLoader Menu("Ctrl+Z********************************************
    0. Tftp utilities.
    1. XModem utilities.
    2. Run main.
    3. SetMac utilities.
    4. Scattered utilities.
    5. Set backplane info
****************************************************
```

Step 5-Input '0' behind the prompt 'Press a key to run the command'.

Step 6-Then input '1' behind the prompt 'Press a key to run the command'. Input 'y' behind the prompt 'Determined to upgrade?' .



```
====== BootLoader Menu("Ctrl+Z" to upper level) ======
    Tftp utilities.
************************************************
    0. Upgrade bootloader.
    1. Upgrade kernel and rootfs by install package.
    2. Down to memory and jump to run.
************************************************
Press a key to run the command: 1
Plz enter the Local IP:[192.168.64.64]: 192.168.1.1
Plz enter the Remote IP:[192.168.64.1]: 192.168.1.100
Plz enter the Filename:[rgos.bin]: rgos.bin
. done
Un-Protected 1 sectors
Erasing Flash...
. done
Erased 1 sectors
Writing to Flash... done
. done
Protected 1 sectors
Auto-update from TFTP: trying update file 'rgos.bin'
Using octeth3 device
TFTP from server 192.168.1.100; our IP address is 192.168.1.1
Filename 'rgos.bin'.
Load address: 0x20000000
Loading: WARNING:
cvmx_phys_to_ptr() passed a zero address
WARNING:
cvmx_ptr_to_phys() passed a NULL pointer
########################
         32 MB received
         #########################
         64 MB received

done
Bytes transferred = 67783909 (40a4ce5 hex)
Uncompressing 0x40a4563@0x20000782 to 0x5250910@0x240a4ce8
Uncompressed 0x5250910 bytes
Get boot addr 0x0,len 0x0; kernel addr 0x241911b0,len 0x5c0000; rootfs addr 0x2475122c, len 
Package information:
    kernel version:2.6.32.a0ceb335d22d15
    kernel target :eg2000dt
    rootfs version:1.0.0.dbf16980
    rootfs target :eg2000dt
Determined to upgrade? [Y/N]: y
```

Step 7-Press ‘ctrl+z‘back to upper menu. Input ‘2’ behind the prompt ‘Press a key to run the command’ to restart and load main process.

Step 8-You could access web page to confirm if it is successful.

3.6 Factory Reset

Note：

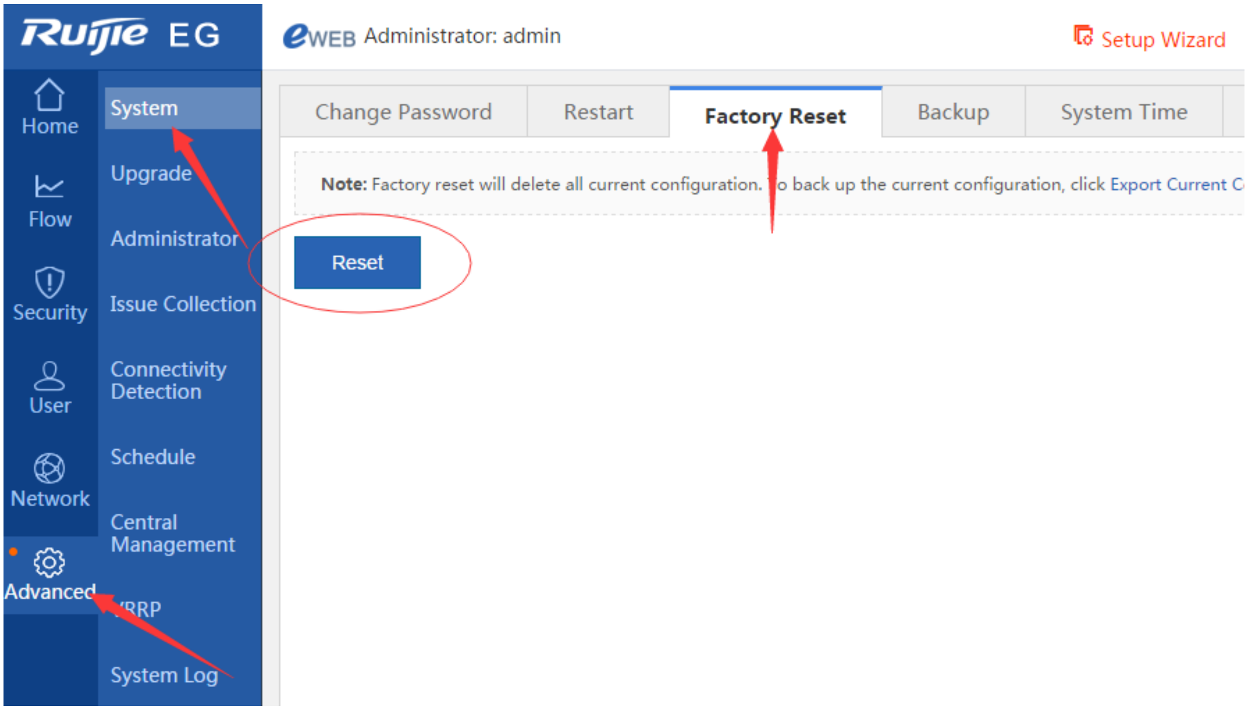
1. After factory reset, existing configuration will be deleted.

2. Factory reset needs to restart.

3. If you can not login web page, please use CLI for factory reset.

➢ Use WEB to factory reset

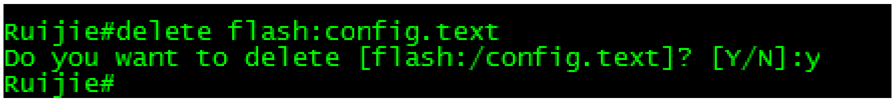
Click ‘Advanced’, choose ‘System’, choose ‘Factory Reset’, and then click ‘Reset’.



Note: Factory reset will delete all current configuration. To back up the current configuration, click Export Current C

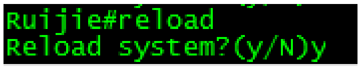
➢ Use CLI to factory reset

Open PUTTY or other softwares (telnet is also OK). Input the command ‘delete flash:config.text’, and then press ‘Enter’. Input ‘y’ behind the prompt ‘Do you want to delete [Flash:/config.text]?’, and then press ‘Enter’.



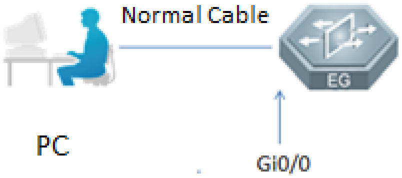
```
Ruijie#delete flash:config.text
Do you want to delete [flash:/config.text]? [Y/N]:y
Ruijie#
```

After that input the command ‘reload’ to restart device. Input ‘y’ behind the prompt ‘Reload system?’ and press ‘Enter’. Device reloading will spend about 5 minutes.



```
Ruijie#reload
Reload system?(y/N)y
```

3.7 View Alarm Log



➢ Alarm Functions：

1. Flow Attack Alarm：If there are large number of flow alarm information existing and lasting long. We suggest turning on ‘Attack Defense’ funcition. If attacks are from intranet, you should check up if there is a virus in a host in your intranet. If attacks are from extranet, you should contact carrier to help you solve the problem.

2. Signature Database Alarm：There some applications lost in the new signature database, and you configured some strategies about these applications before, there will be an alarm here.

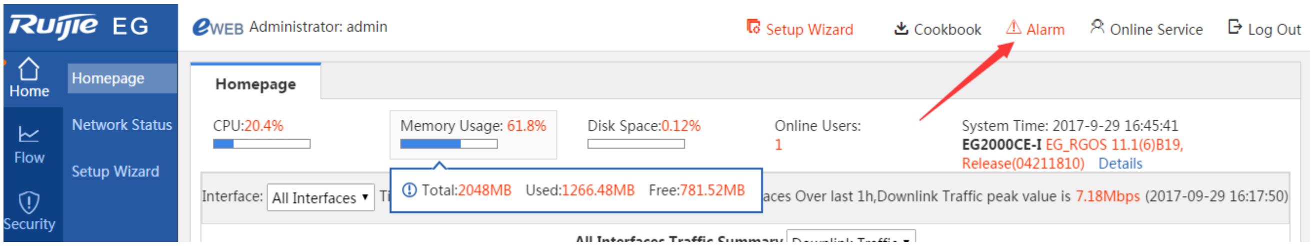
3. SATA Disk Alarm：There will not be an alarm appear here in normal status, if not please contact us.

4. Config File Alarm：Prompt you for the size of current configuration file.

5. Default Route Alarm：If you have no default route, it will have an alarm here.

➢ Opreation Steps：

Step 1-If you find the ‘Alarm’ turn to be red or twinkle, please click it to check. (Normal status is black)



Administrator: admin

CPU:20.4%　Memory Usage: 61.8%　Disk Space:0.12%　Online Users: 1

System Time: 2017-9-29 16:45:41
EG2000CE-I EG_RGOS 11.1(6)B19, Release(04211810) Details

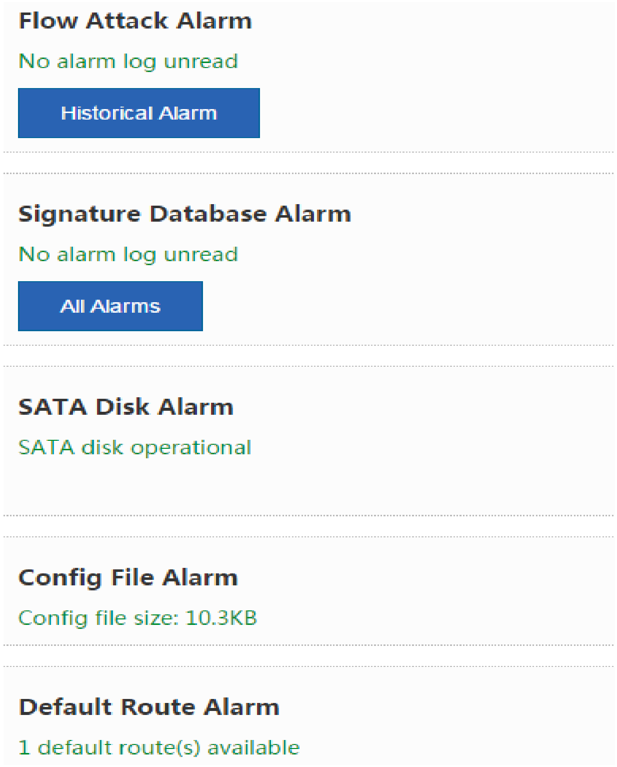
Interface: All Interfaces　Ti

Total:2048MB Used:1266.48MB Free:781.52MB

aces Over last 1h,Downlink Traffic peak value is 7.18Mbps (2017-09-29 16:17:50)

All Interfaces Traffic Summary Downlink Traffic

Step 2-You can see which kinds of alarm appear; the alarm item will turn to be red either. Green means all are normal, just like the following picture.



Flow Attack Alarm

No alarm log unread

Signature Database Alarm

No alarm log unread

SATA Disk Alarm

SATA disk operational

Config File Alarm

Config file size: 10.3KB

Default Route Alarm

1 default route(s) available

3.8 System Log View and Export

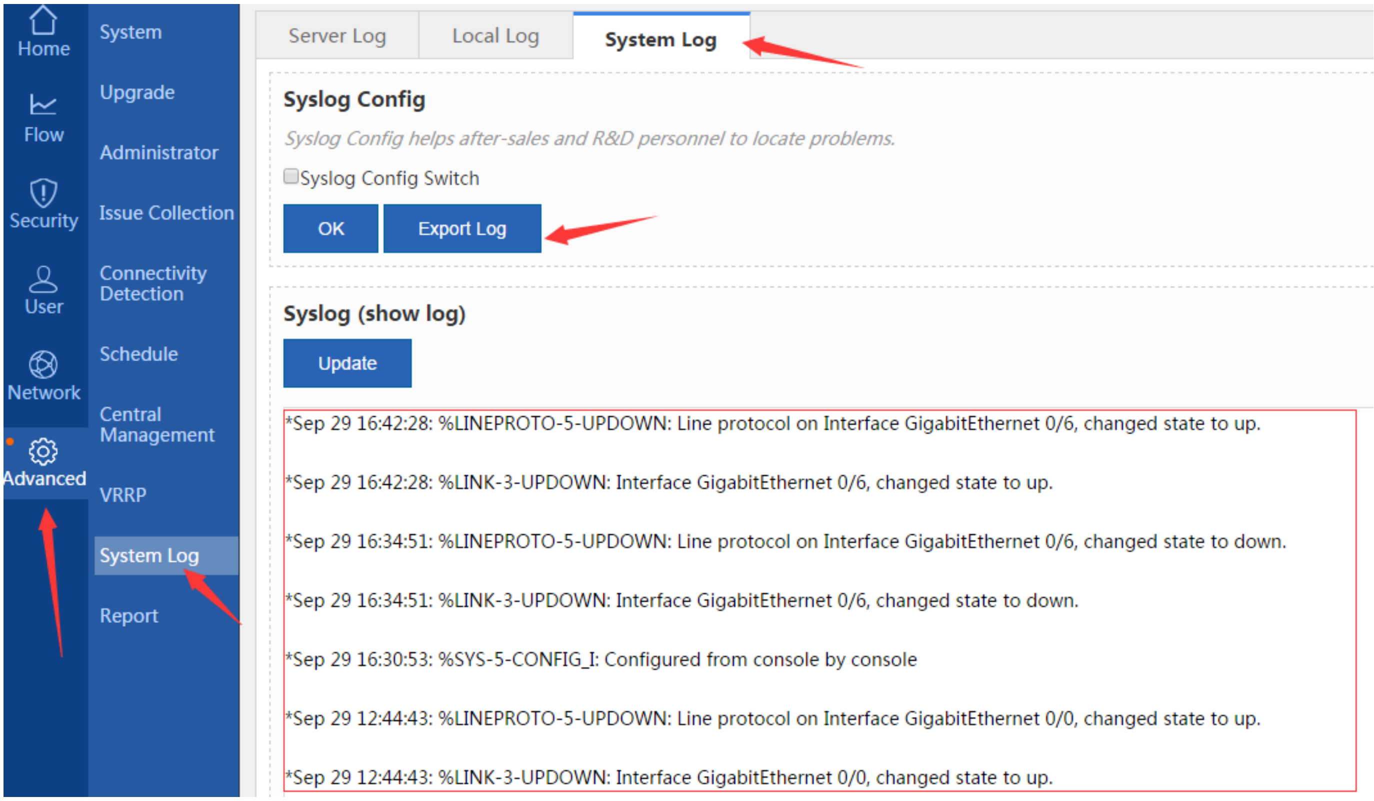
Click ‘Advanced’, choose ‘System Log’, choose ‘System Log’. If you want to view syslog, you should click ‘Update’ and then start scanning it.

You can export syslog by click ‘Export Log’, it will packet the log information and download in your computer.

Note：

1. Sever Log：You can associate EG to your log sever by configuring this function. In that case, your log server will record designated log by you.

2. Local Log：You can save flow-log or NAT-log in the disk of device.



Syslog Config

Syslog Config helps after-sales and R&D personnel to locate problems.

□Syslog Config Switch

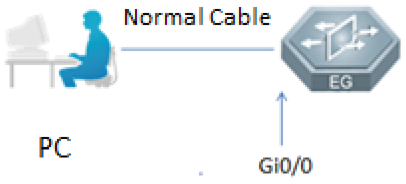
Syslog (show log)

```
*Sep 29 16:42:28: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet 0/6, changed state to up.

*Sep 29 16:42:28: %LINK-3-UPDOWN: Interface GigabitEthernet 0/6, changed state to up.

*Sep 29 16:34:51: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet 0/6, changed state to down.

*Sep 29 16:34:51: %LINK-3-UPDOWN: Interface GigabitEthernet 0/6, changed state to down.

*Sep 29 16:30:53: %SYS-5-CONFIG_I: Configured from console by console

*Sep 29 12:44:43: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet 0/0, changed state to up.

*Sep 29 12:44:43: %LINK-3-UPDOWN: Interface GigabitEthernet 0/0, changed state to up.
```

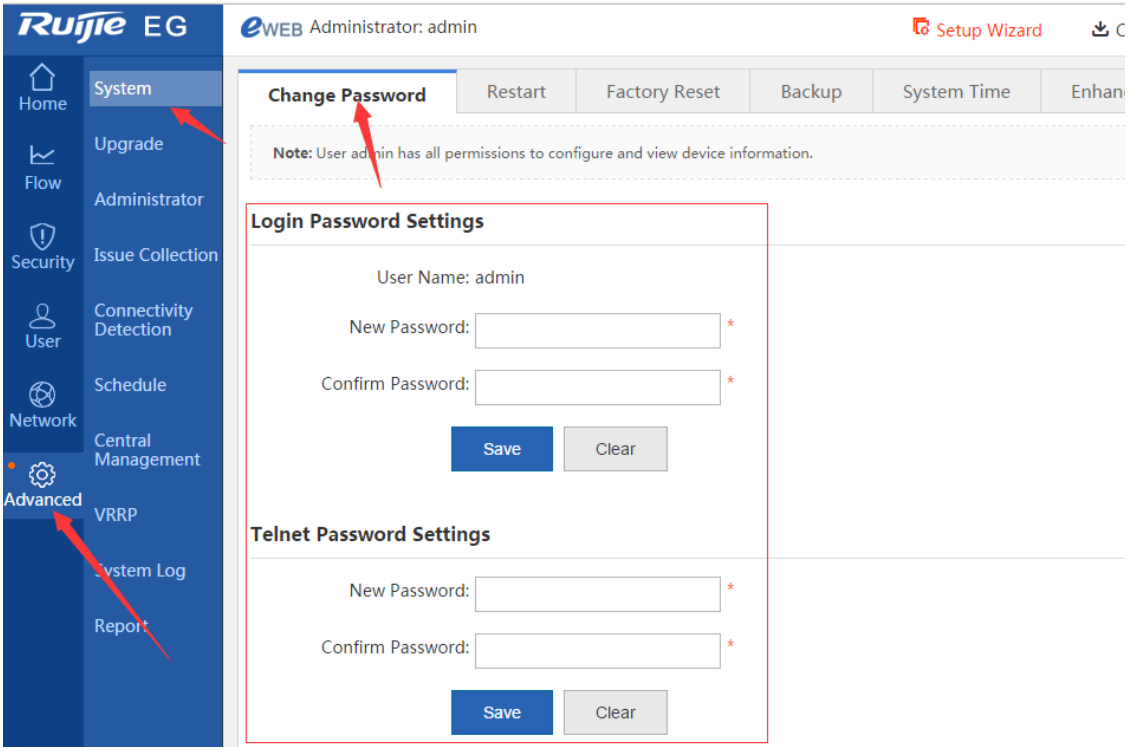
3.9 Change Password

Note: Device only has web management password when leaving factory. Default user and password are ‘admin’ for web management.

➢ Use WEB to change password



Click ‘Advanced’, choose ‘System’, and choose ‘Change Password’. You can change your web management and telnet password here. CLI privileged mode password is the same as telnet password, if you don’t set other configurations by CLI.



Note: User admin has all permissions to configure and view device information.

Login Password Settings

User Name: admin

New Password: *

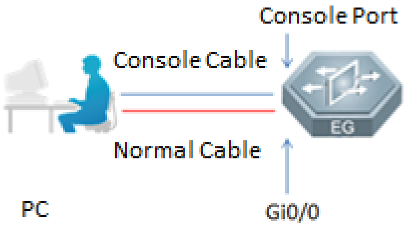
Confirm Password: *

Telnet Password Settings

New Password: *

Confirm Password: *

➢ Use CLI to change password



```
Ruijie#configure
Ruijie(config)#webmaster level 0   username admin password ruijie       //change admin password as ruijie
Ruijie(config)#enable secret ruijie                          //change privileged mode password as ruijie

Ruijie(config)#line vty 0   4
Ruijie(config-line)#password   ruijie                        //change telnet password as ruijie
Ruijie(config-line)#end
Ruijie#write
```

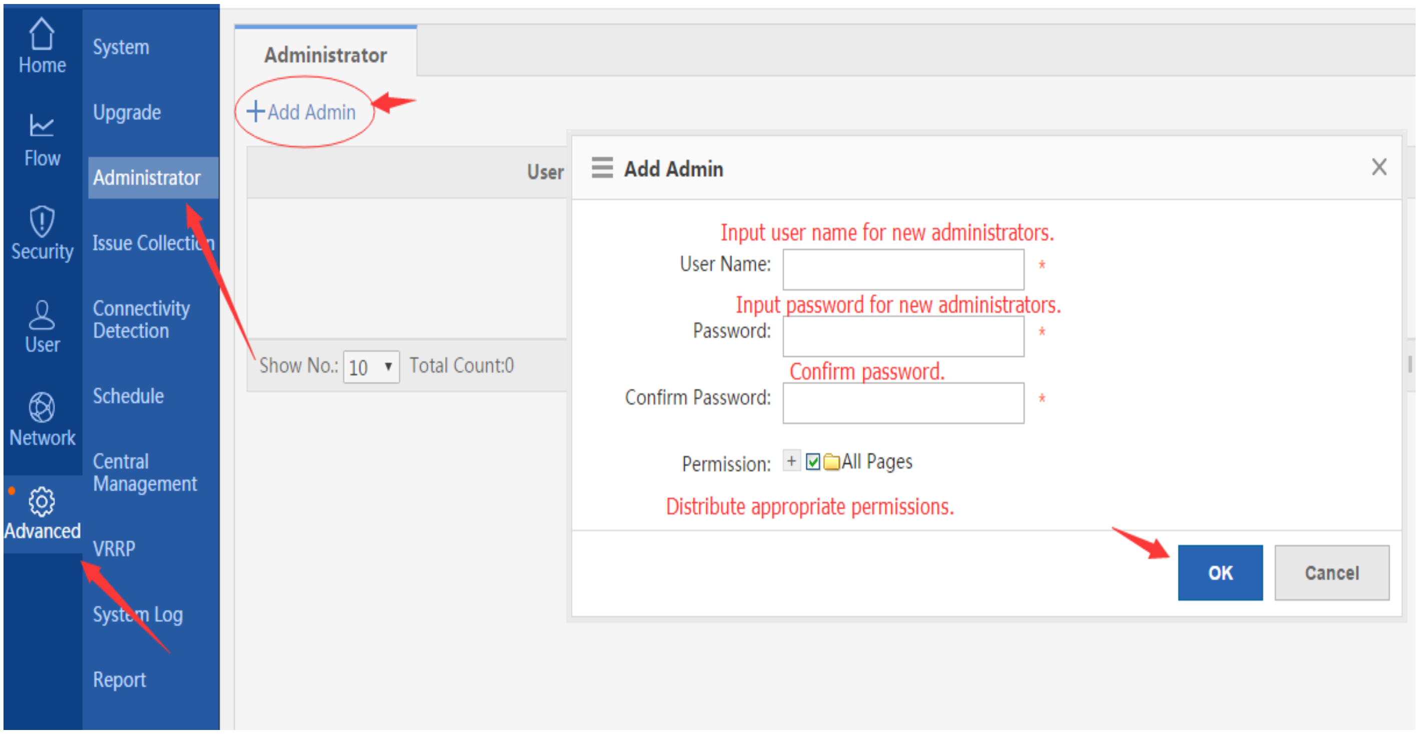
3.10 Administrator Authority Setting

Note：

1. If your company has many administrators, in charge of different functions. You can use this function to configure.

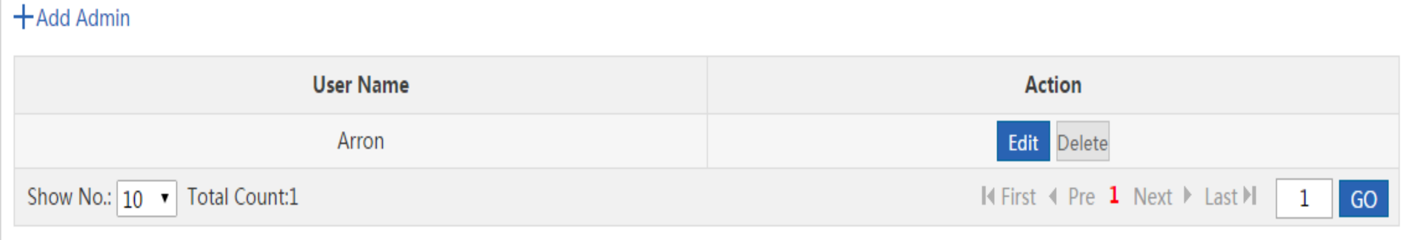
2. These administrators can use web to login, but can not login by telnet.

3. These administrators can change their own passwords, but can not change admin's password. If these new administrators foreget their passwords, you can login admin to reset.



Input user name for new administrators.
User Name: *
Input password for new administrators.
Password: *
Confirm password.
Confirm Password: *
Permission: + ☑ All Pages
Distribute appropriate permissions.

You can click 'edit to reset password. Only inputting a new password and then confirming is ok.



User Name	Action
Arron	Edit Delete

4 EG Quick Start

4.1 EG2100-P Quick Start Guide

4.1.1 Setup via EG local Web

1) Modify the IP address of PC.

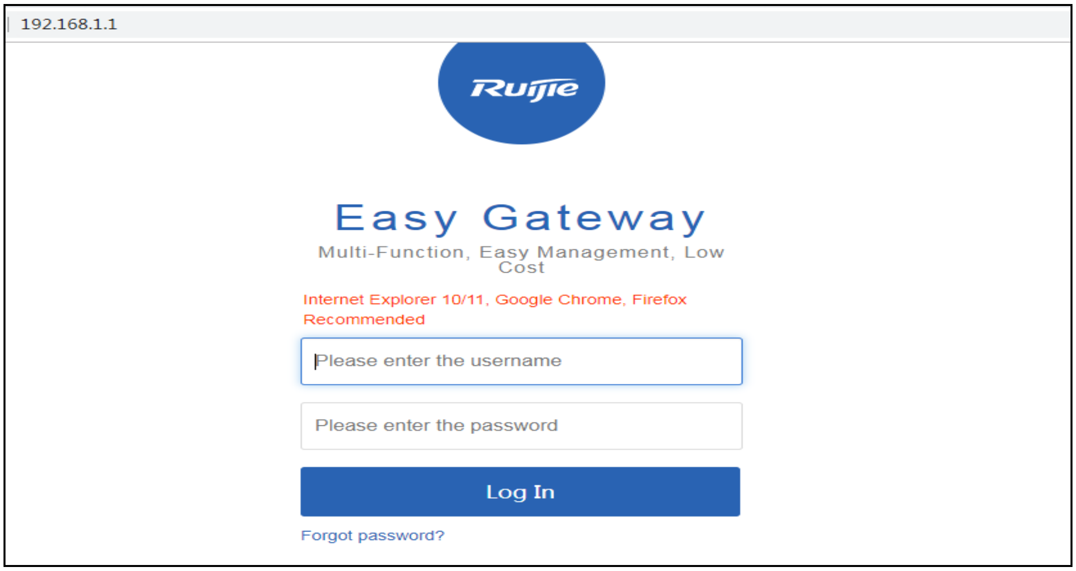
IP address: 192.168.1.x (except 192.168.1.1)

Subnet mask: 255.255.255.0

Default gateway: 192.168.1.1 (default LAN IP)

2) Connect the PC to any port (except WAN0) on the device.

3) Visit http://192.168.1.1 by Chrome browser.



192.168.1.1

Easy Gateway

Multi-Function, Easy Management, Low Cost

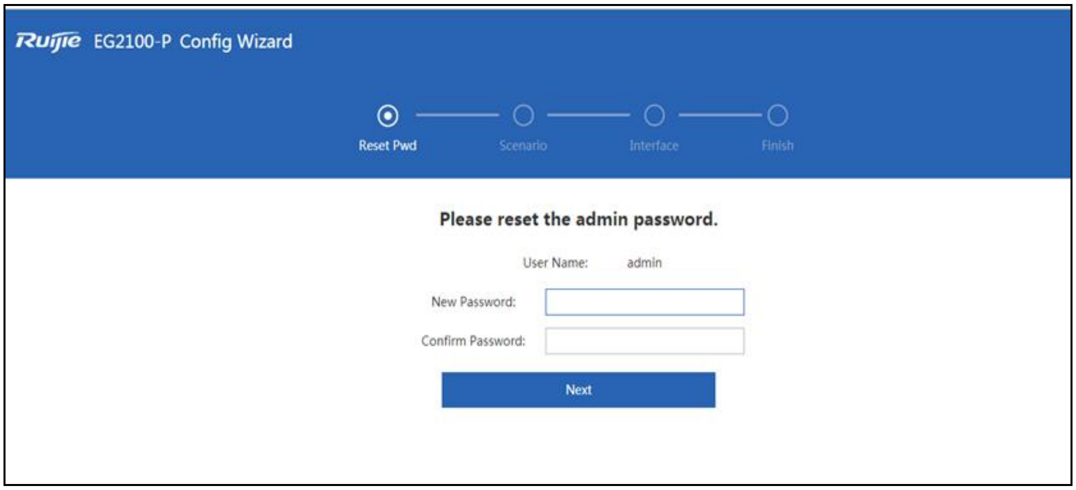
Internet Explorer 10/11, Google Chrome, Firefox Recommended

4) Enter the username and password on the login page and click “Log In”.

Default Username: admin

Default Password: admin

5) Change the password at the first login.



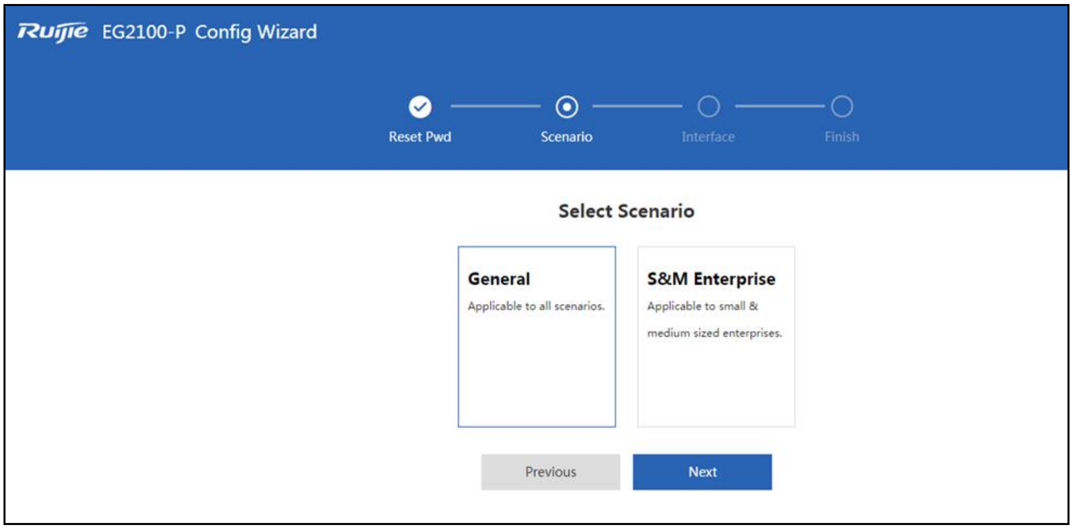
Please reset the admin password.

User Name: admin

New Password:

Confirm Password:

Select a scenario.



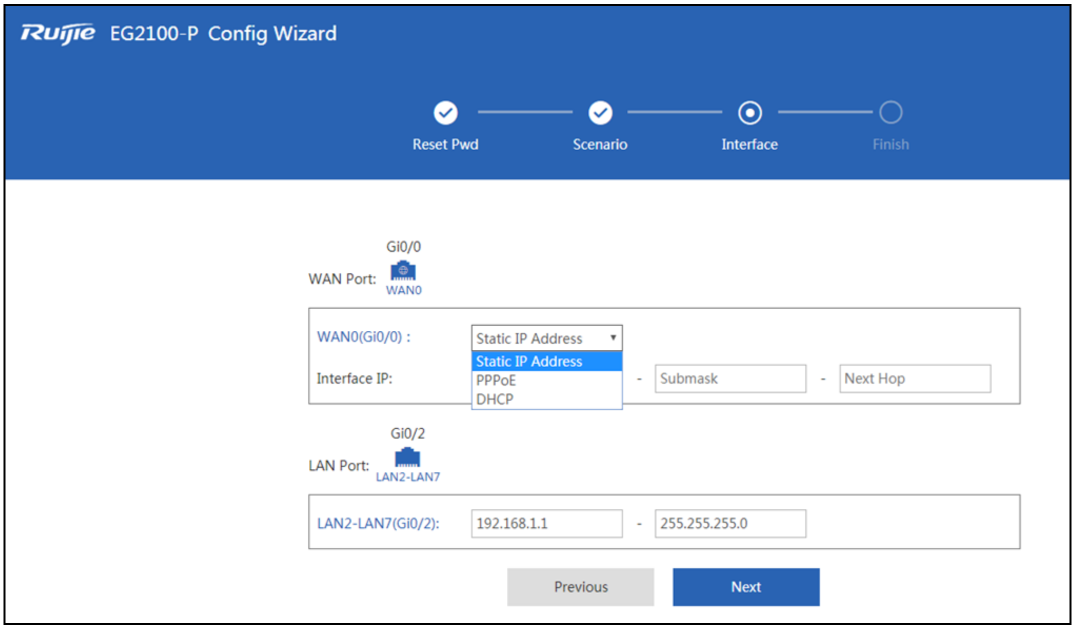
Select Scenario

General Applicable to all scenarios.

S&M Enterprise Applicable to small & medium sized enterprises.

Configure the WAN port (DHCP, Static IP or PPPoE).

It is not recommended to change the IP of LAN port; otherwise, you may need to log in and configure again. After wizard completes, you can configure LAN port on the interface configuration page.



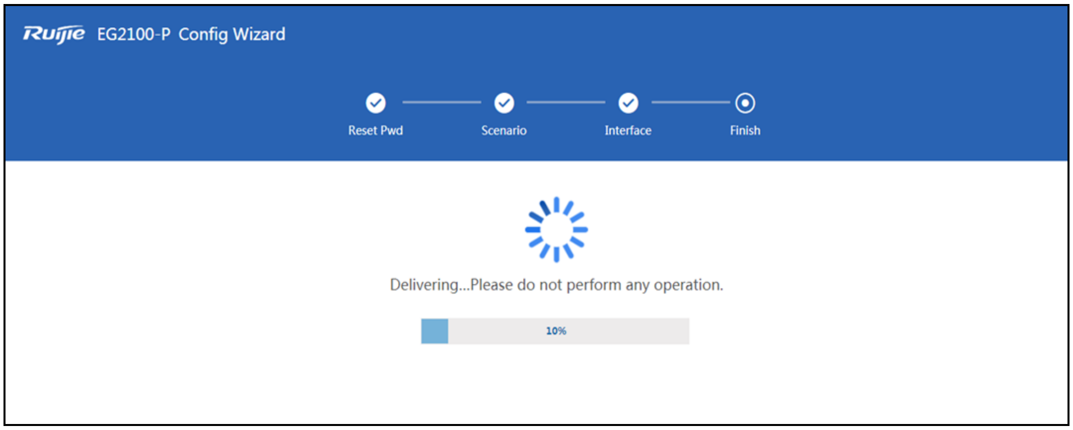
WAN Port: Gi0/0 WAN0

WAN0(Gi0/0) : Static IP Address

Interface IP: - Submask - Next Hop

LAN Port: Gi0/2 LAN2-LAN7

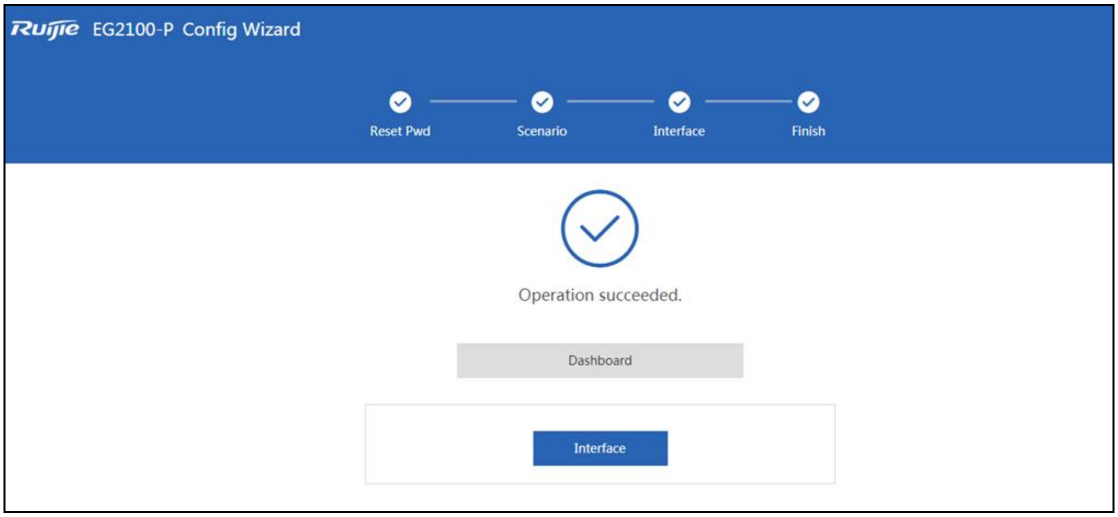
LAN2-LAN7(Gi0/2): 192.168.1.1 - 255.255.255.0



Delivering...Please do not perform any operation.

10%

6) Click Dashboard to open the homepage, or click Interface to enter the interface configuration page. If the WAN port is connected to the Internet, you can access the Internet now and add the EG to the Cloud.



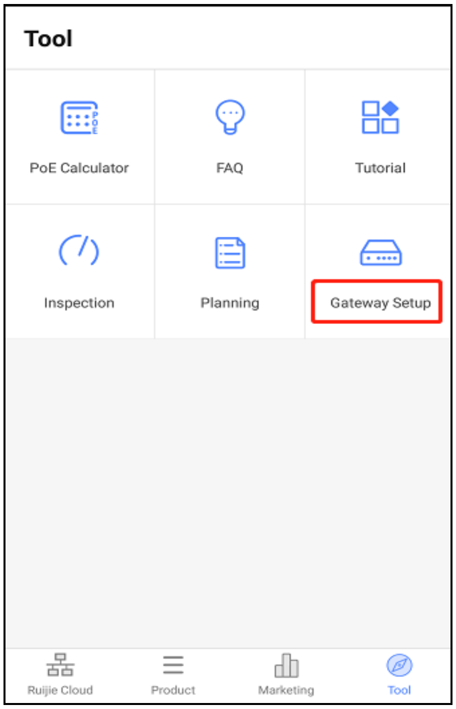
Operation succeeded.

4.1.2 Setup via Mobile App (Recommended)

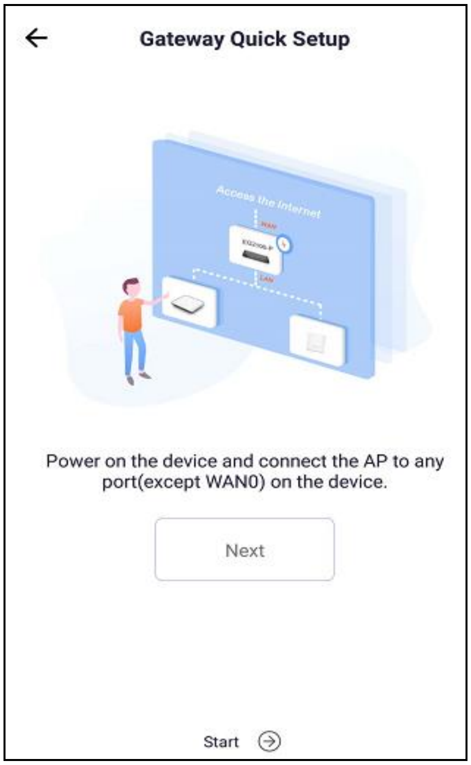
4.1.2.1 Configure WAN Uplink Port

1) Connect AP710 to any of LAN1-LAN7 ports on EG2100-P. After AP is powered on, it will broadcast the default SSID: RJ-xxxxxx (xxxxxx is the last six digits of EG2100-P SN).

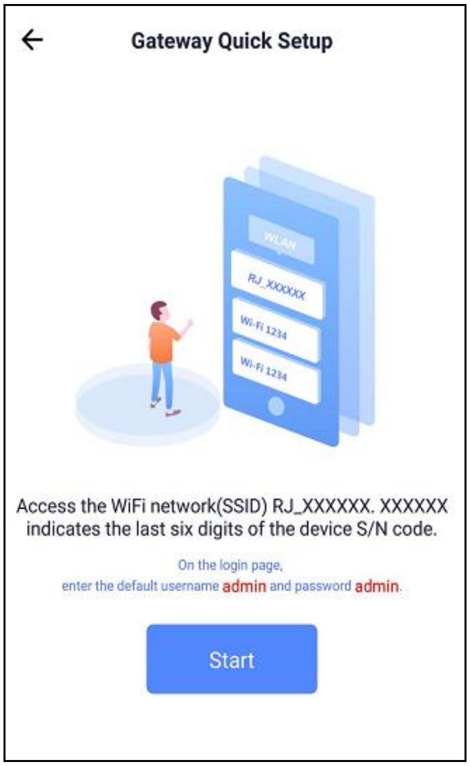
2) Launch Ruijie Cloud App, tap Tool menu, and tap Gateway Setup to start the Gateway Quick Setup, as shown below:



3) Log in with the default account (username: admin, password: admin).

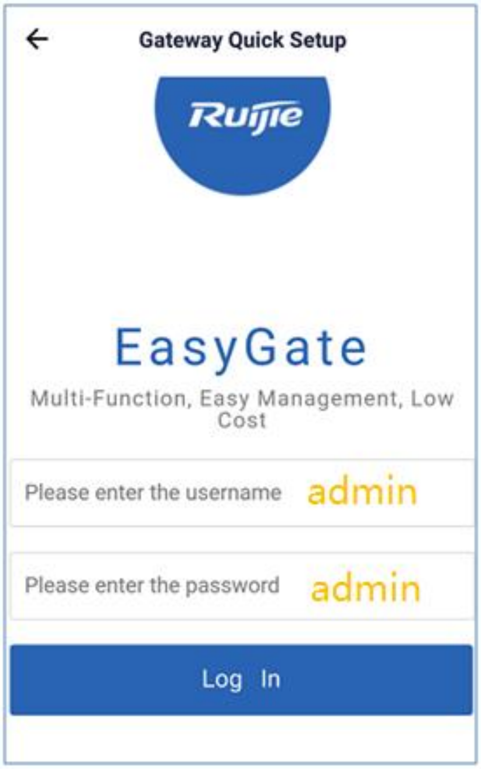


Power on the device and connect the AP to any port(except WAN0) on the device.



Access the WiFi network(SSID) RJ_XXXXXX. XXXXXX indicates the last six digits of the device S/N code.

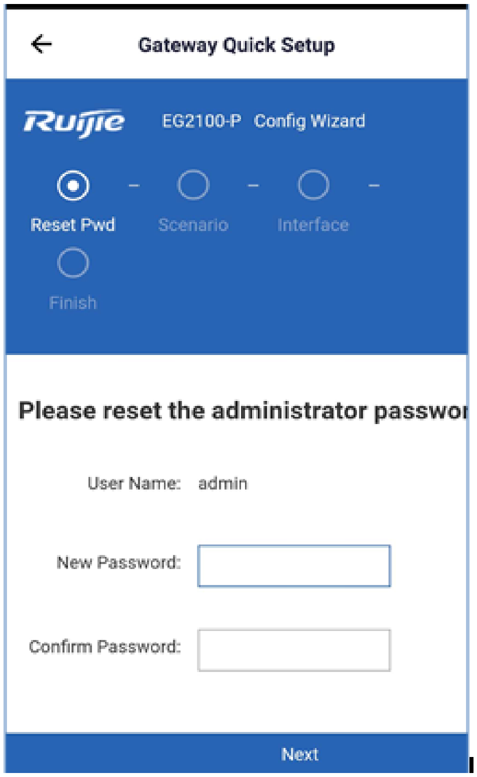
On the login page,
enter the default username admin and password admin.



Please enter the username admin

Please enter the password admin

4) Reset the Web management password, and tap Next (Note: This password is required when you add EGs by scanning the QR-code).



Gateway Quick Setup

EG2100-P Config Wizard

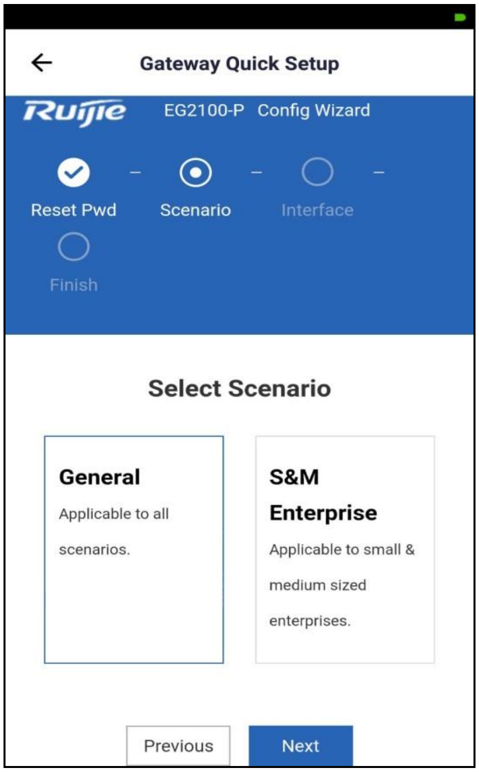
Please reset the administrator passwor

User Name: admin

New Password:

Confirm Password:

5) Select a Scenario. If you select the S&M Enterprise, Flow Control Configuration will be added to the wizard. Here you can just tap Next to enter the Interface settings.



Gateway Quick Setup

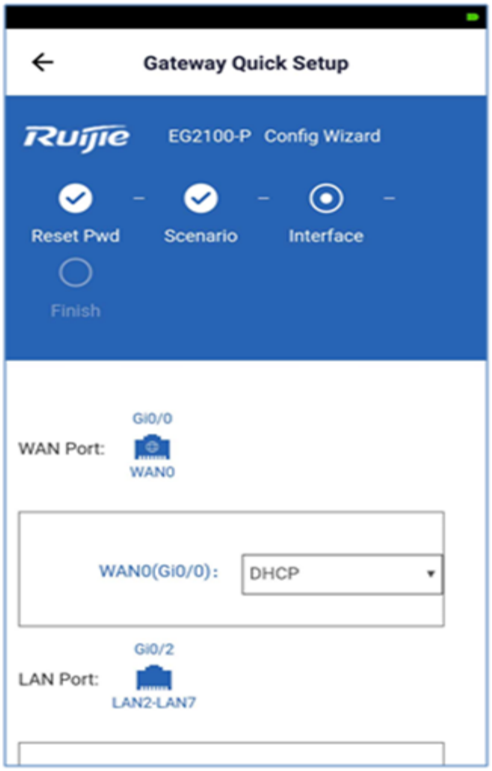
EG2100-P Config Wizard

Select Scenario

General Applicable to all scenarios.

S&M Enterprise Applicable to small & medium sized enterprises.

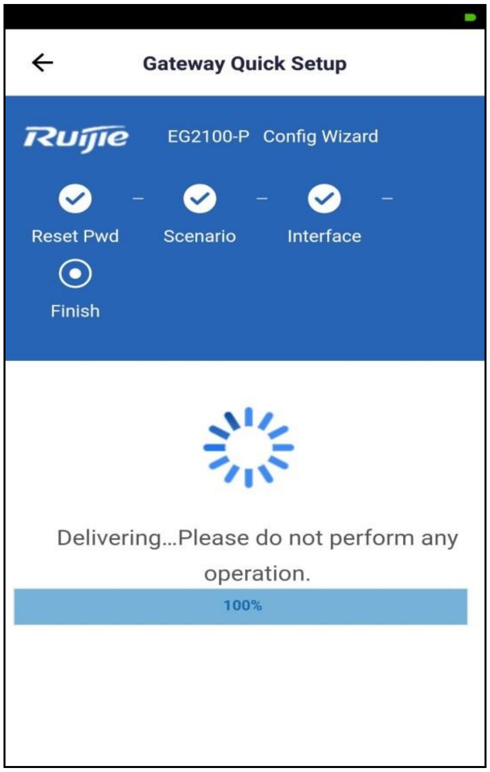
6) Configure the WAN port (PPPoE, Static IP or DHCP), tap Next and wait for about 5 seconds until a success message is displayed. (Note: After the message is displayed, EG will restart).



WAN Port:

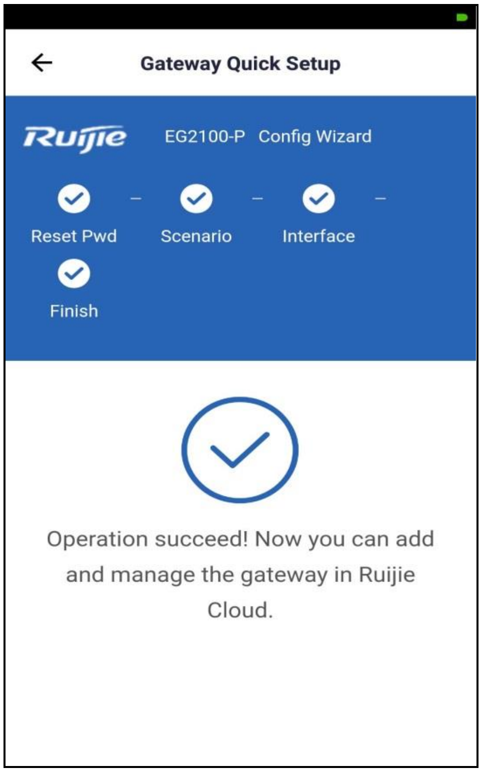
WAN0(Gi0/0): DHCP

LAN Port:



Delivering...Please do not perform any operation.

100%

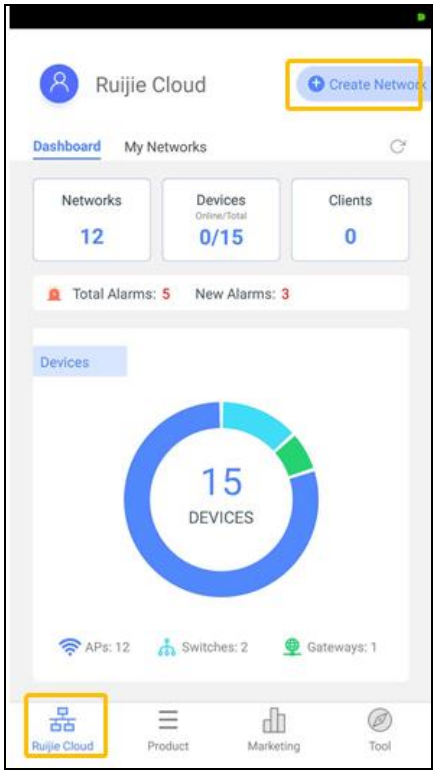


Operation succeed! Now you can add and manage the gateway in Ruijie Cloud.

7) The initial configuration complete. Now you can create the network and add devices on App.

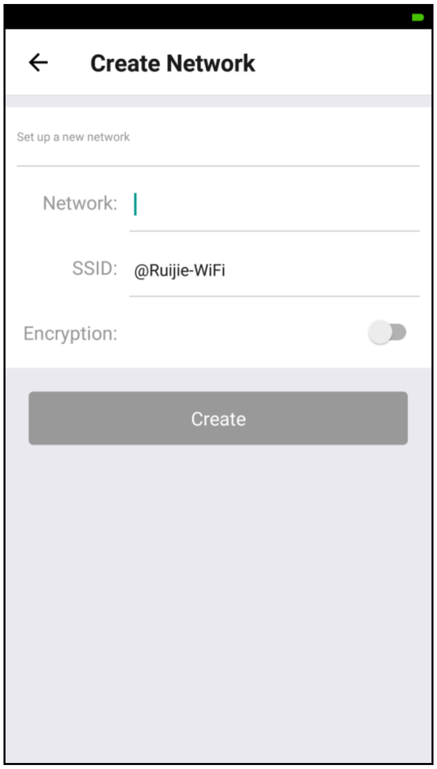
4.1.2.2 Add Network and Device

1) Open the Ruijie Cloud App, tap Create Network, and enter the network name and SSID.



Networks	Devices Online/Total	Clients
12	0/15	0

Total Alarms: 5 New Alarms: 3

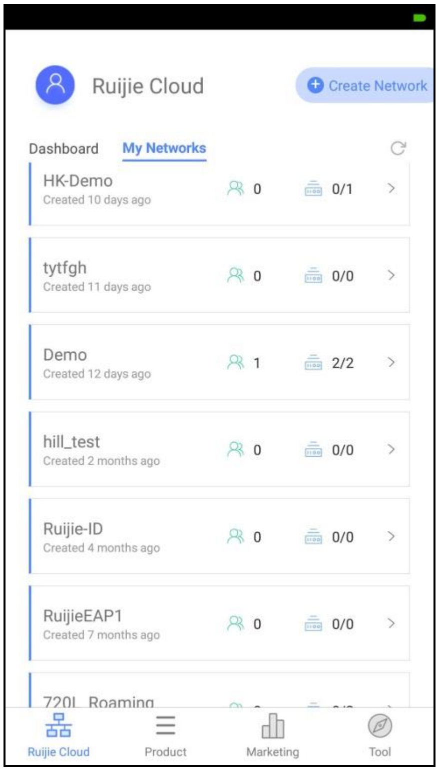


Network:

SSID: @Ruijie-WiFi

Encryption:

2) After the network is created, enter the network and tap Add Device to add AP and EG2100-P by scanning the QR code (AP SN/MAC) on the back of the device. (Note: When adding an EG, you need to enter its Web management password.)



HK-Demo Created 10 days ago 0 0/1

tytfgh Created 11 days ago 0 0/0

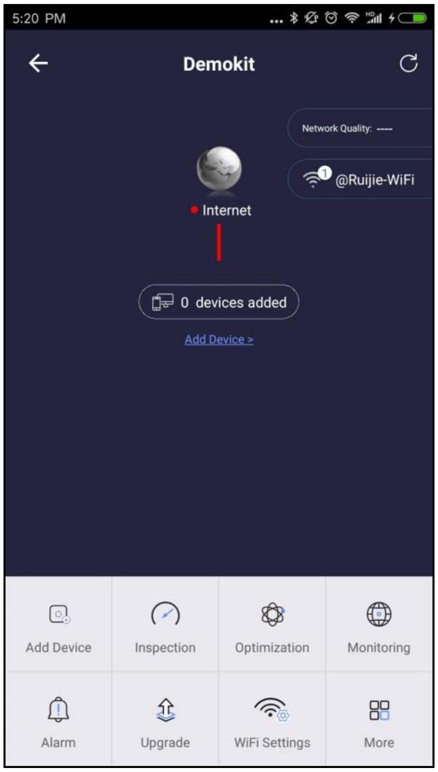
Demo Created 12 days ago 1 2/2

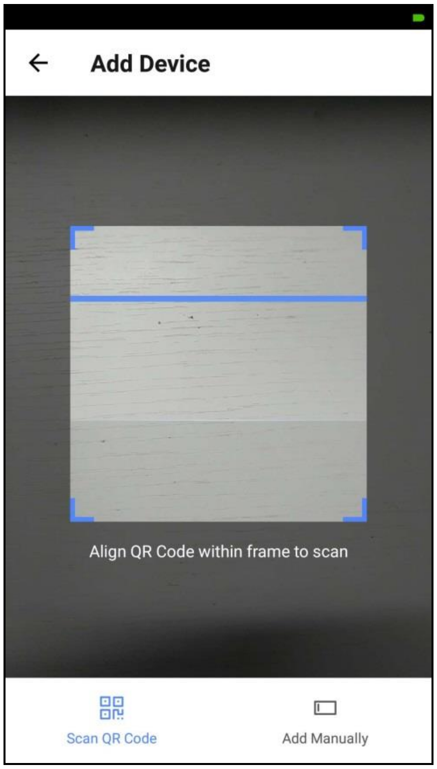
hill_test Created 2 months ago 0 0/0

Ruijie-ID Created 4 months ago 0 0/0

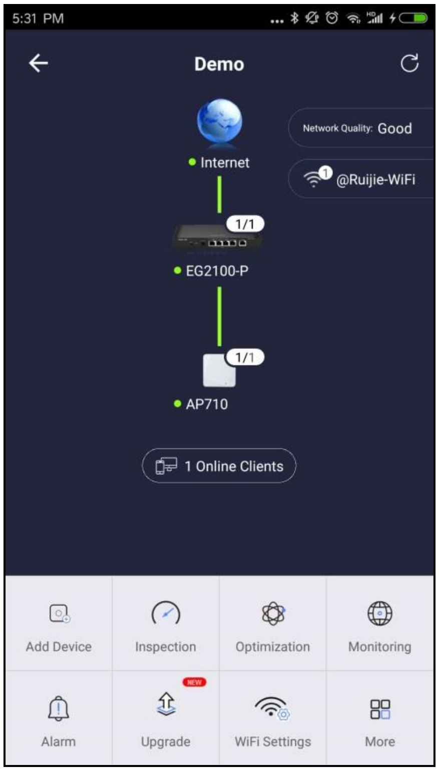
RuijieEAP1 Created 7 months ago 0 0/0

720L_Roaming

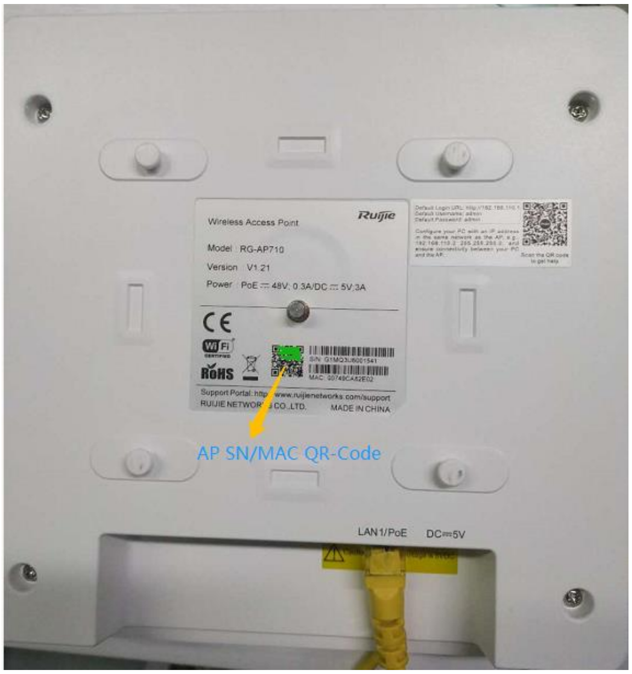




3) Wait for about 3 to 5 minutes, and you can see the online status of AP and EG devices.

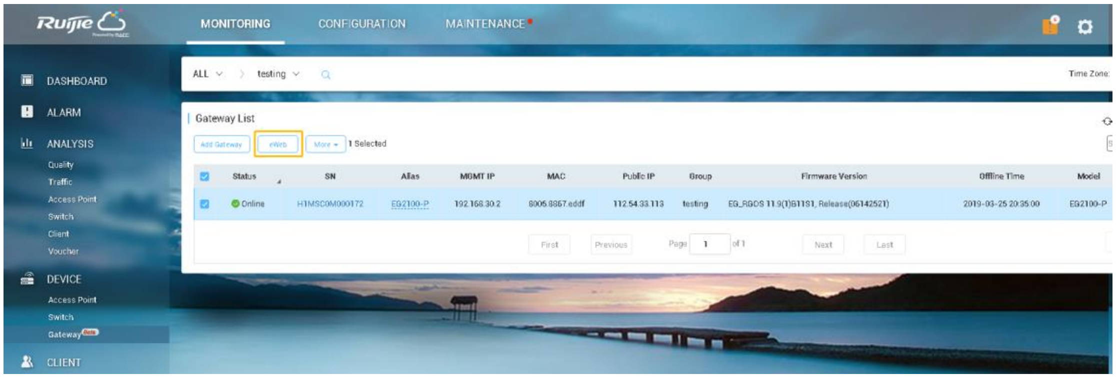


The SN/MAC QR-Code demo on the back of AP:



4.1.2.3 Access EG Web from Cloud

1) After an EG comes online on the Ruijie Cloud, you can visit its eWeb page for advanced configuration. Select the EG in the Gateway List, and click eWeb.

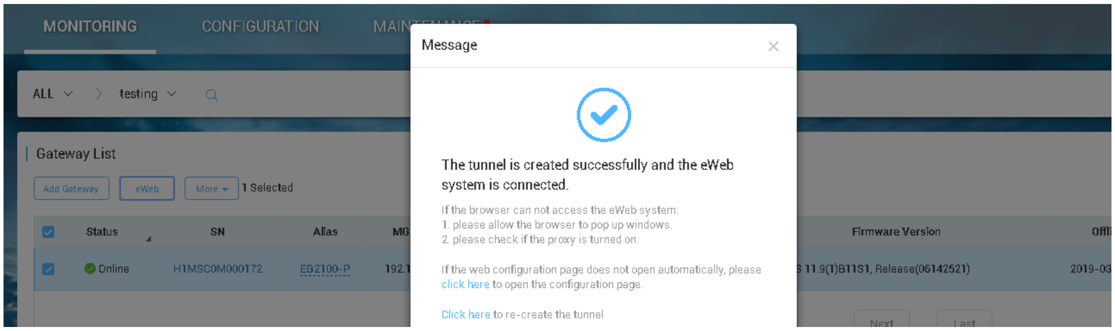


Gateway List

1 Selected

☑	Status	SN	Alias	MGMT IP	MAC	Public IP	Group	Firmware Version	Offline Time	Model
☑	Online	H1MSC0M000172	EG2100-P	192.168.30.2	8005.8867.eddf	112.54.33.113	testing	EG_RGOS 11.9(1)B11S1, Release(06142521)	2019-03-25 20:35:00	EG2100-P

2) After the tunnel is created, the Web management page will open automatically, as shown below:



Message

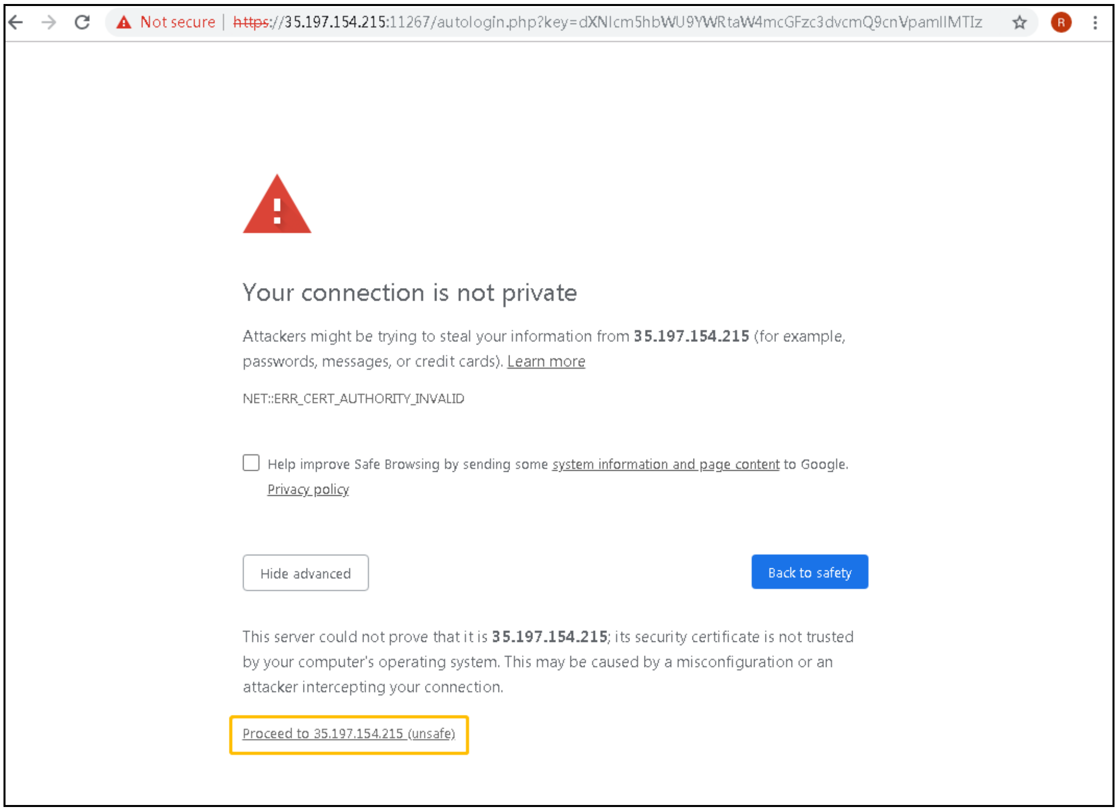
The tunnel is created successfully and the eWeb system is connected.

If the browser can not access the eWeb system:
1. please allow the browser to pop up windows.
2. please check if the proxy is turned on.

If the web configuration page does not open automatically, please click here to open the configuration page.

Click here to re-create the tunnel

3) If the following information is displayed, click Proceed to enter the eWeb system.


Not secure
https://35.197.154.215:11267/autologin.php?key=dXNlcm5hbWU9YWRtaW4mcGFzc3dvcmQ9cnVpamllMTIz

Your connection is not private

Attackers might be trying to steal your information from **35.197.154.215** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

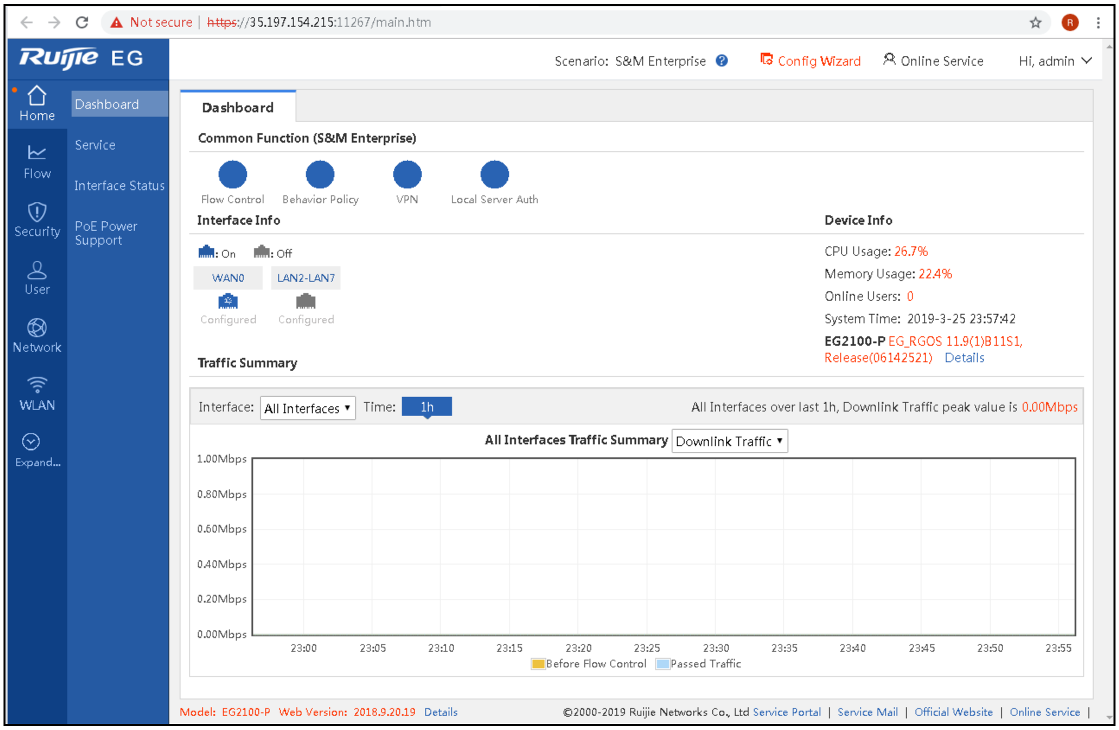
□ Help improve Safe Browsing by sending some system information and page content to Google. Privacy policy

Hide advanced

Back to safety

This server could not prove that it is **35.197.154.215**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to 35.197.154.215 (unsafe)



Scenario: S&M Enterprise

CPU Usage: 26.7%
Memory Usage: 22.4%
Online Users: 0
System Time: 2019-3-25 23:57:42
EG2100-P EG_RGOS 11.9(1)B11S1, Release(06142521) Details

Interface: All Interfaces Time: 1h All Interfaces over last 1h, Downlink Traffic peak value is 0.00Mbps

Downlink Traffic

Model: EG2100-P Web Version: 2018.9.20.19 Details ©2000-2019 Ruijie Networks Co., Ltd

4.2 EG3000 Series Quick Start Guide

4.2.1 WAN Uplink Quick Setup

1) Modify the IP address of PC.

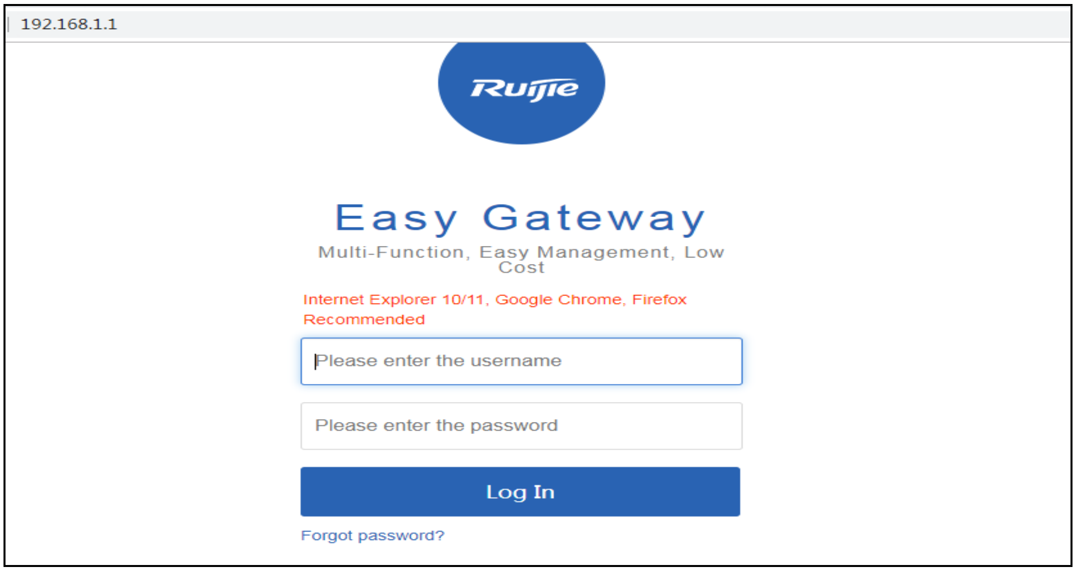
IP address: 192.168.1.x (except 192.168.1.1)

Subnet mask: 255.255.255.0

Default gateway: 192.168.1.1 (default LAN IP)

2) Connect the PC to any port (except WAN0) on the device.

3) Visit http://192.168.1.1 by Chrome browser.



192.168.1.1

Easy Gateway

Multi-Function, Easy Management, Low Cost

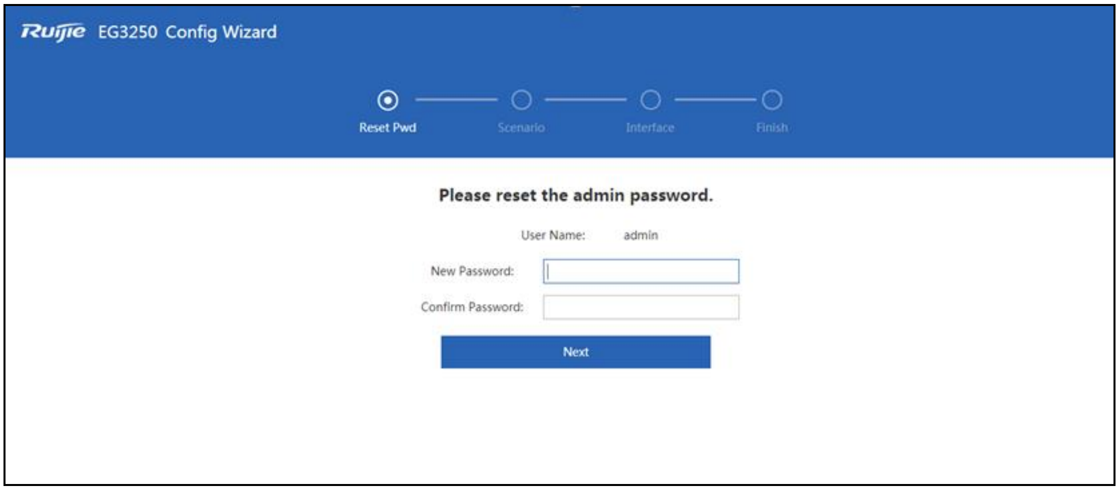
Internet Explorer 10/11, Google Chrome, Firefox Recommended

4) Enter the username and password on the login page and click “Log In”.

Default Username: admin

Default Password: admin

5) Change the password at the first login.



EG3250 Config Wizard

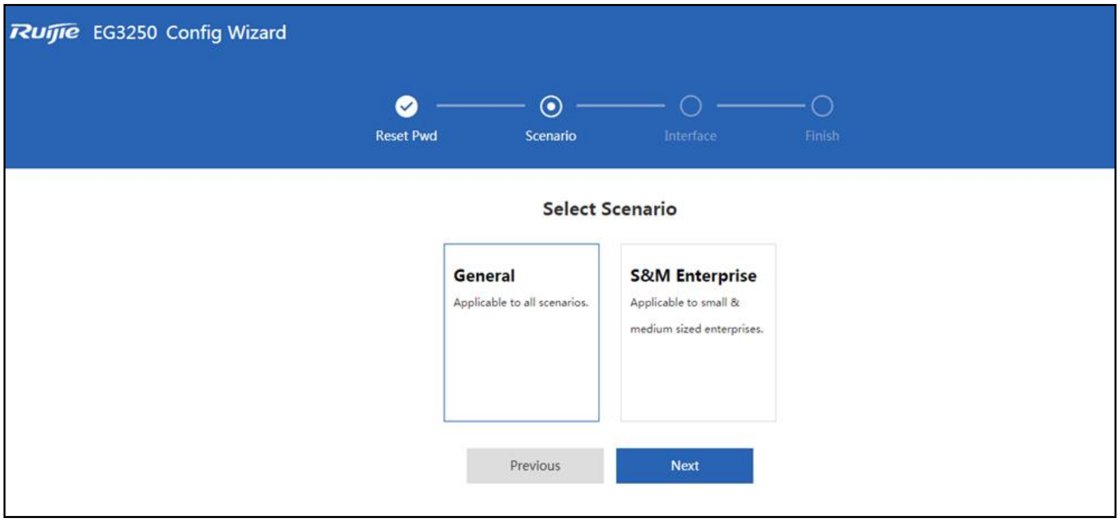
Please reset the admin password.

User Name: admin

New Password:

Confirm Password:

Select a scenario.



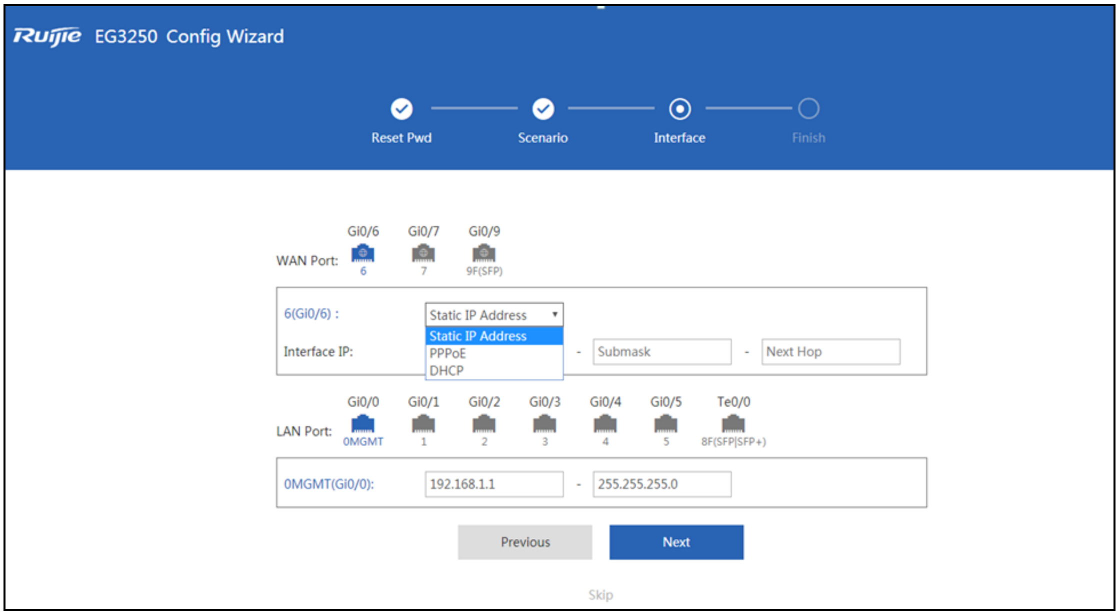
Select Scenario

General
Applicable to all scenarios.

S&M Enterprise
Applicable to small & medium sized enterprises.

Configure the WAN port (DHCP, Static IP or PPPoE).

It is not recommended to change the IP of LAN port; otherwise, you may need to log in and configure again. After wizard completes, you can configure LAN port on the interface configuration page.



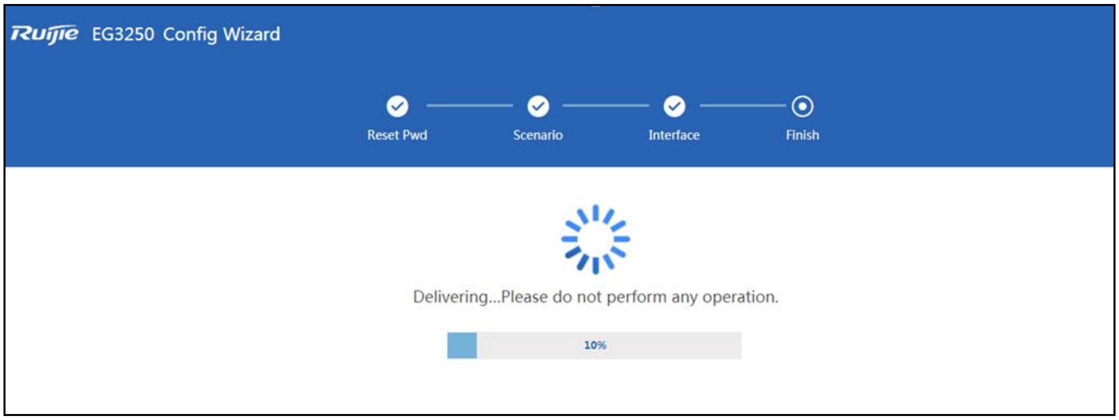
WAN Port:

6(Gi0/6) : Static IP Address

Interface IP: - Submask - Next Hop

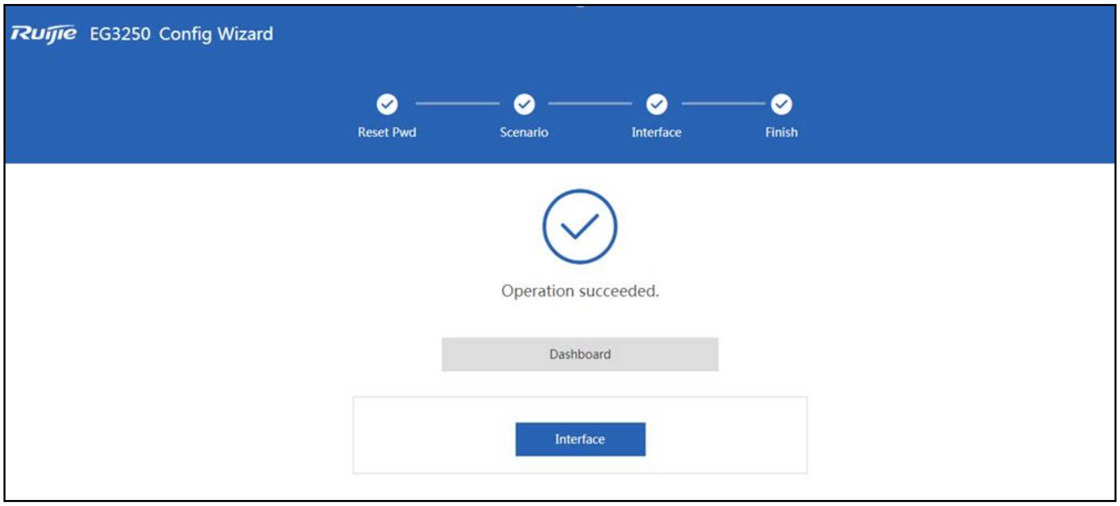
LAN Port:

0MGMT(Gi0/0): 192.168.1.1 - 255.255.255.0



Delivering...Please do not perform any operation.

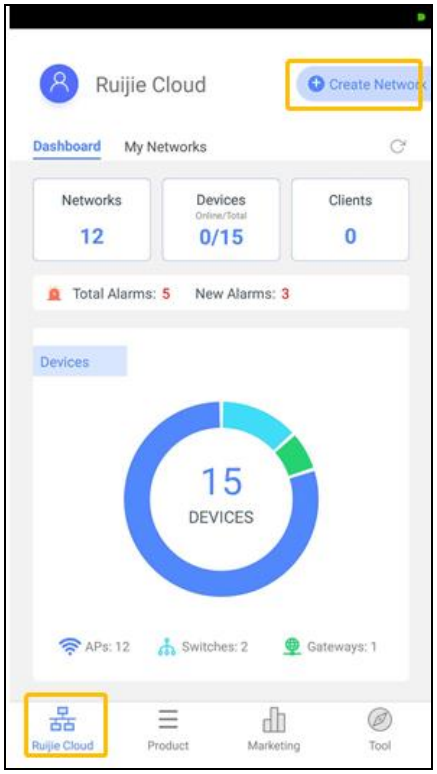
6) Click Dashboard to open the homepage, or click Interface to enter the interface configuration page. If the WAN port is connected to the Internet, you can access the Internet now and add the EG to the Cloud.

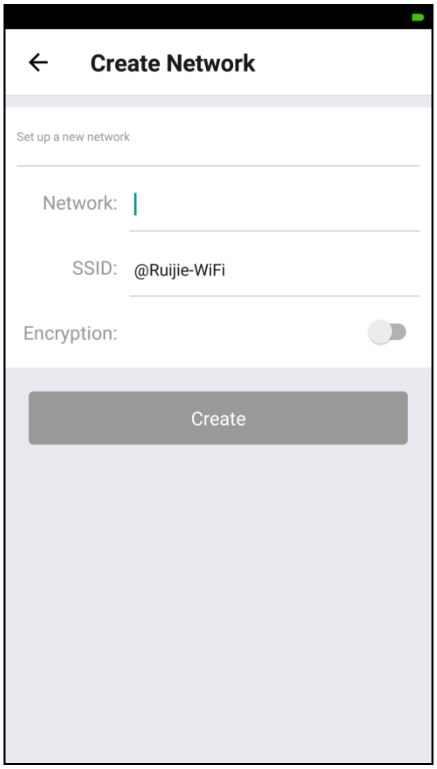


Operation succeeded.

4.2.2 Add Device to Ruijie Cloud

1) Open the Ruijie Cloud App, tap Create Network, and enter the network name and SSID.



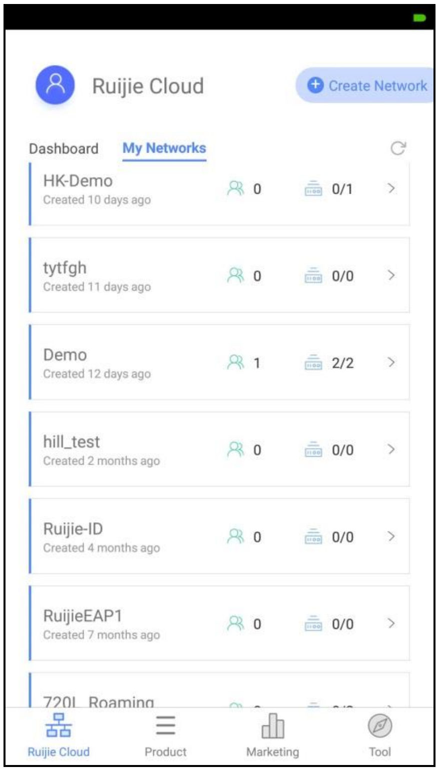


Network:

SSID: @Ruijie-WiFi

Encryption:

2) After the network is created, enter the network and tap Add Device to add AP and EG3250 by scanning the QR code (AP SN/MAC) on the back of the device (Note: There is no QR code behind EG3000UE/XE, so please manually enter SN). When adding an EG, you need to enter its Web management password.



Ruijie Cloud

Dashboard My Networks

HK-Demo Created 10 days ago 0 0/1

tytfgh Created 11 days ago 0 0/0

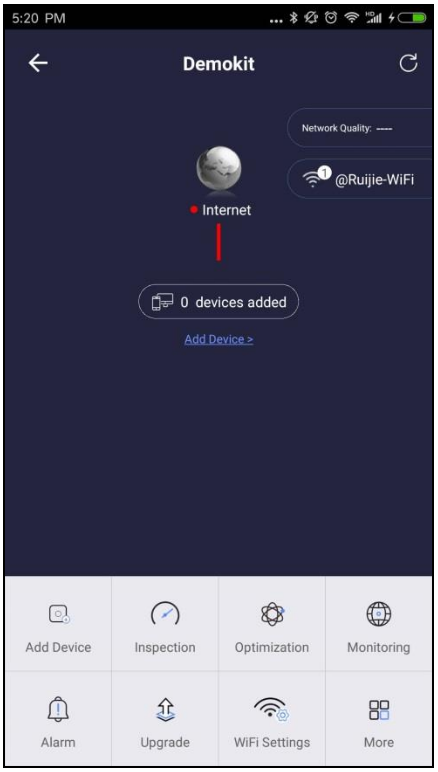
Demo Created 12 days ago 1 2/2

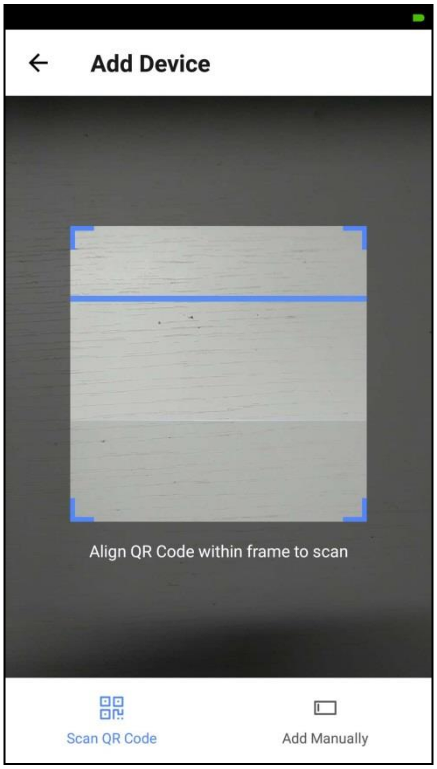
hill_test Created 2 months ago 0 0/0

Ruijie-ID Created 4 months ago 0 0/0

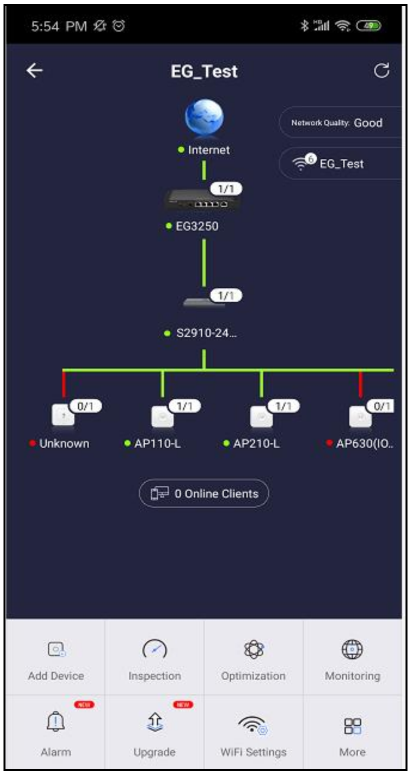
RuijieEAP1 Created 7 months ago 0 0/0

720L_Roaming





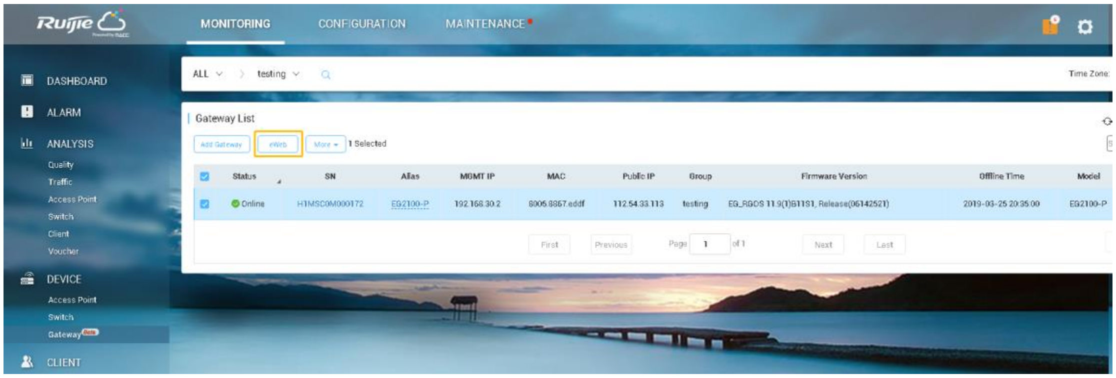
3) Wait for about 3 to 5 minutes, and you can see the online status of EG device.



The SN/MAC QR-Code demo on the back of EG:

4.2.3 Access EG Web from Cloud

1) After an EG comes online on the Ruijie Cloud, you can visit its eWeb page for advanced configuration. Select the EG in the Gateway List, and click eWeb.



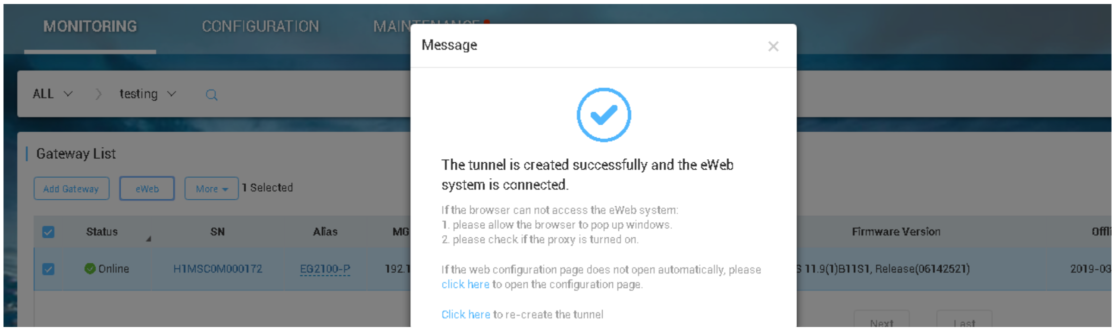
Gateway List

1 Selected

☑	Status	SN	Alias	MGMT IP	MAC	Public IP	Group	Firmware Version	Offline Time	Model
☑	Online	H1MSC0M000172	EG2100-P	192.168.30.2	8005.8867.eddf	112.54.33.113	testing	EG_RGOS 11.9(1)B11S1, Release(06142521)	2019-03-25 20:35:00	EG2100-P

First Previous Page 1 of 1 Next Last

2) After the tunnel is created, the Web management page will open automatically, as shown below:



	Status	SN	Alias	MG	Firmware Version	Offl
☑	Online	H1MSC0M000172	EG2100-P	192.1	11.9(1)B11S1, Release(06142521)	2019-03

Message

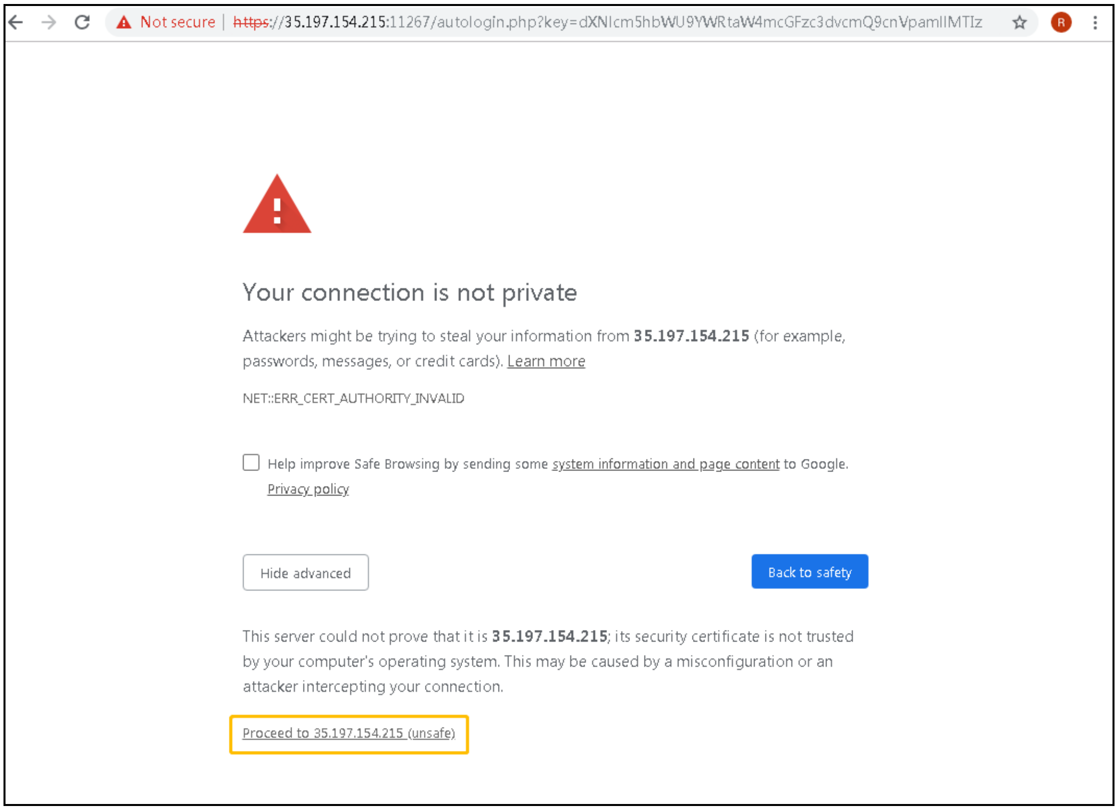
The tunnel is created successfully and the eWeb system is connected.

If the browser can not access the eWeb system:
1. please allow the browser to pop up windows.
2. please check if the proxy is turned on.

If the web configuration page does not open automatically, please click here to open the configuration page.

Click here to re-create the tunnel

3) If the following information is displayed, click Proceed to enter the eWeb system.


Not secure | ~~https~~://35.197.154.215:11267/autologin.php?key=dXNIcm5hbWU9YWRtaW4mcGFzc3dvcmQ9cnVpamlIMTIz

Your connection is not private

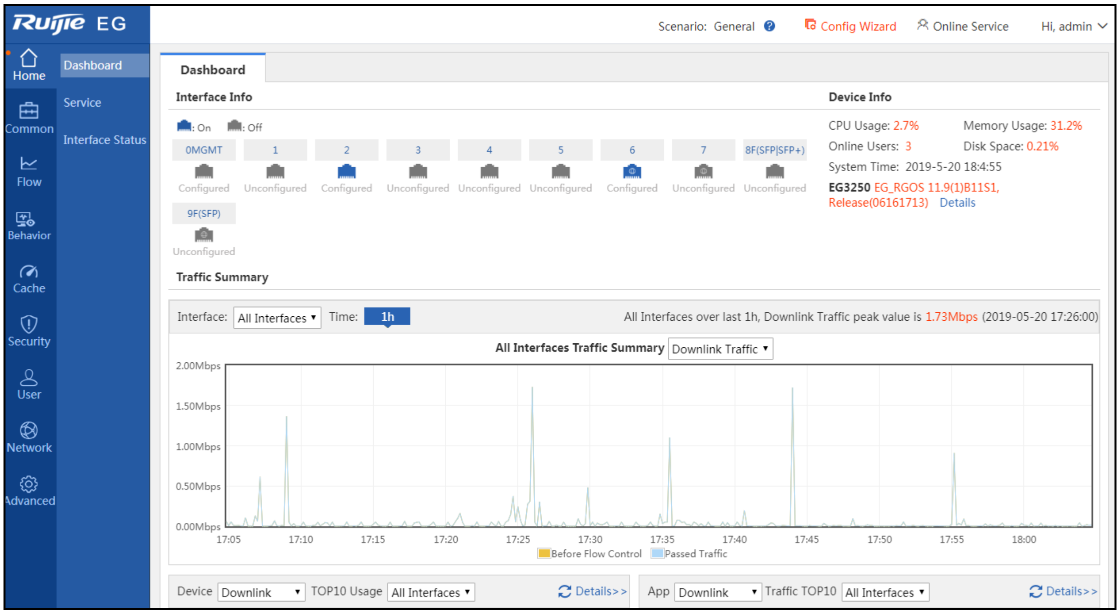
Attackers might be trying to steal your information from **35.197.154.215** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

□ Help improve Safe Browsing by sending some system information and page content to Google. Privacy policy

This server could not prove that it is **35.197.154.215**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to 35.197.154.215 (unsafe)



Scenario: General

CPU Usage: 2.7% Memory Usage: 31.2%

Online Users: 3 Disk Space: 0.21%

System Time: 2019-5-20 18:4:55

EG3250 EG_RGOS 11.9(1)B11S1, Release(06161713) Details

Interface: All Interfaces Time: 1h

All Interfaces over last 1h, Downlink Traffic peak value is 1.73Mbps (2019-05-20 17:26:00)

All Interfaces Traffic Summary: Downlink Traffic

Device Downlink TOP10 Usage All Interfaces

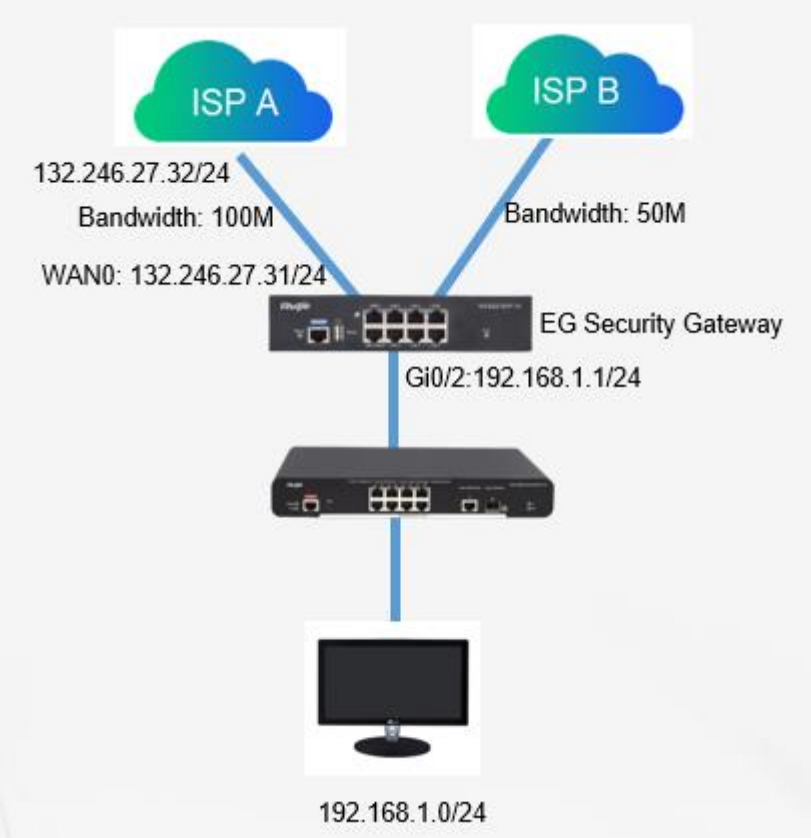
App Downlink Traffic TOP10 All Interfaces

5 Basic Function Configuration

5.1 WAN Load Balance

The load balancing function distributes the data to multiple WAN interfaces to avoid the traffic congestion and provide redundancy.

Network Topology

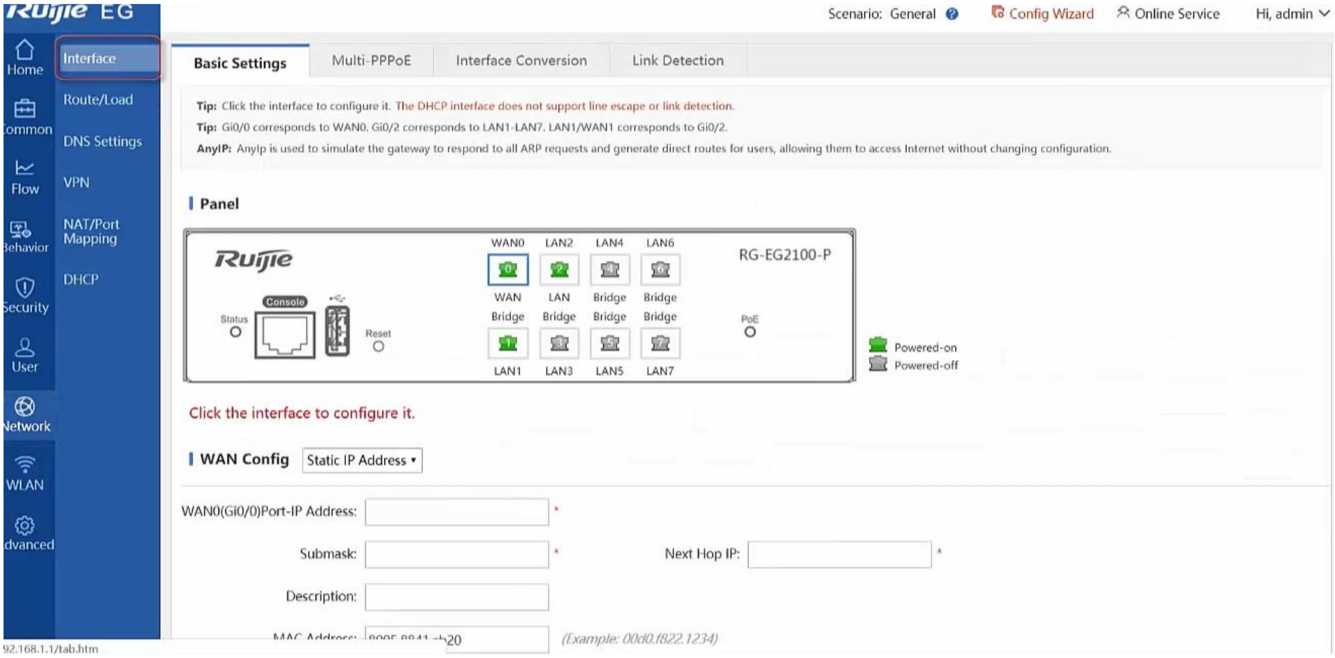


Configuration Key Points

1. Configure IP address of the WAN ports and default routes.
2. Enable the load balancing policy.
3. Customize interface weight to ensure that traffic goes through the different egress according to weight.

Configuraiton Steps

Step 1: Configure WAN 0



Tip: Click the interface to configure it. The DHCP interface does not support line escape or link detection.

Tip: Gi0/0 corresponds to WAN0. Gi0/2 corresponds to LAN1-LAN7. LAN1/WAN1 corresponds to Gi0/2.

AnyIP: AnyIp is used to simulate the gateway to respond to all ARP requests and generate direct routes for users, allowing them to access Internet without changing configuration.

Panel

Click the interface to configure it.

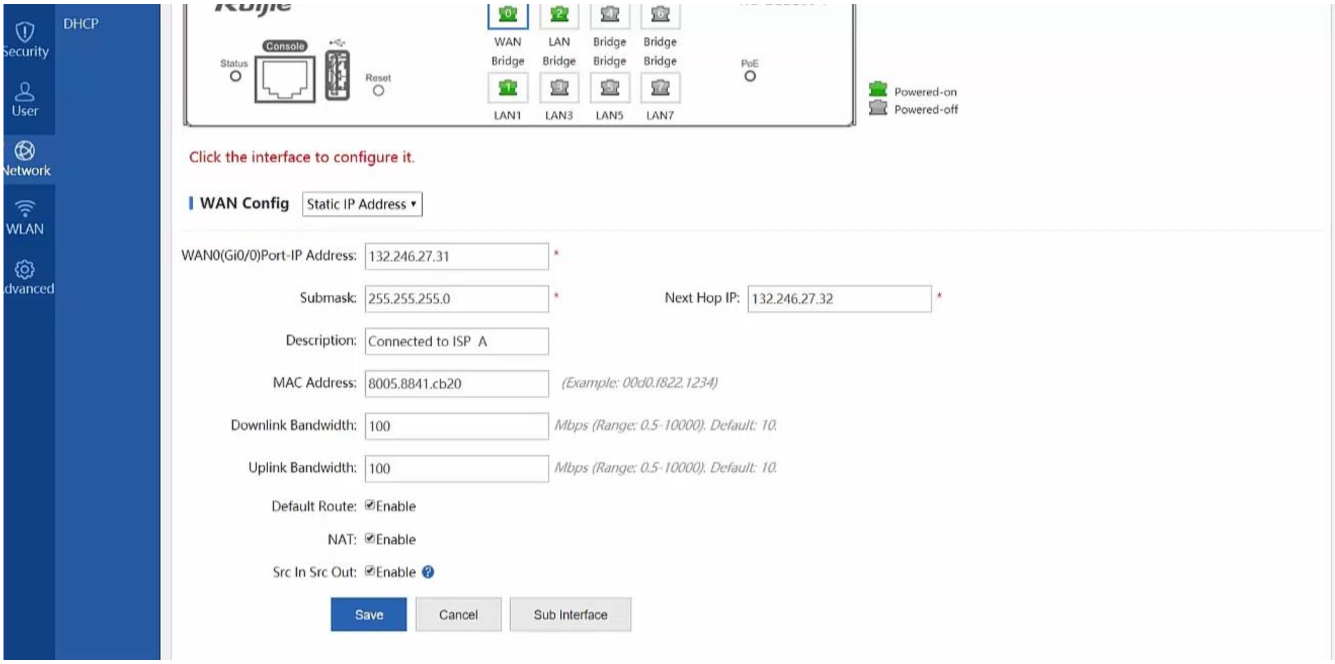
WAN Config Static IP Address

WAN0(Gi0/0)Port-IP Address: *

Submask: * Next Hop IP: *

Description:

MAC Address: 8005.8841.cb20 (Example: 00d0.f822.1234)



Click the interface to configure it.

WAN Config Static IP Address

WAN0(Gi0/0)Port-IP Address: 132.246.27.31 *

Submask: 255.255.255.0 * Next Hop IP: 132.246.27.32 *

Description: Connected to ISP A

MAC Address: 8005.8841.cb20 (Example: 00d0.f822.1234)

Downlink Bandwidth: 100 Mbps (Range: 0.5-10000). Default: 10.

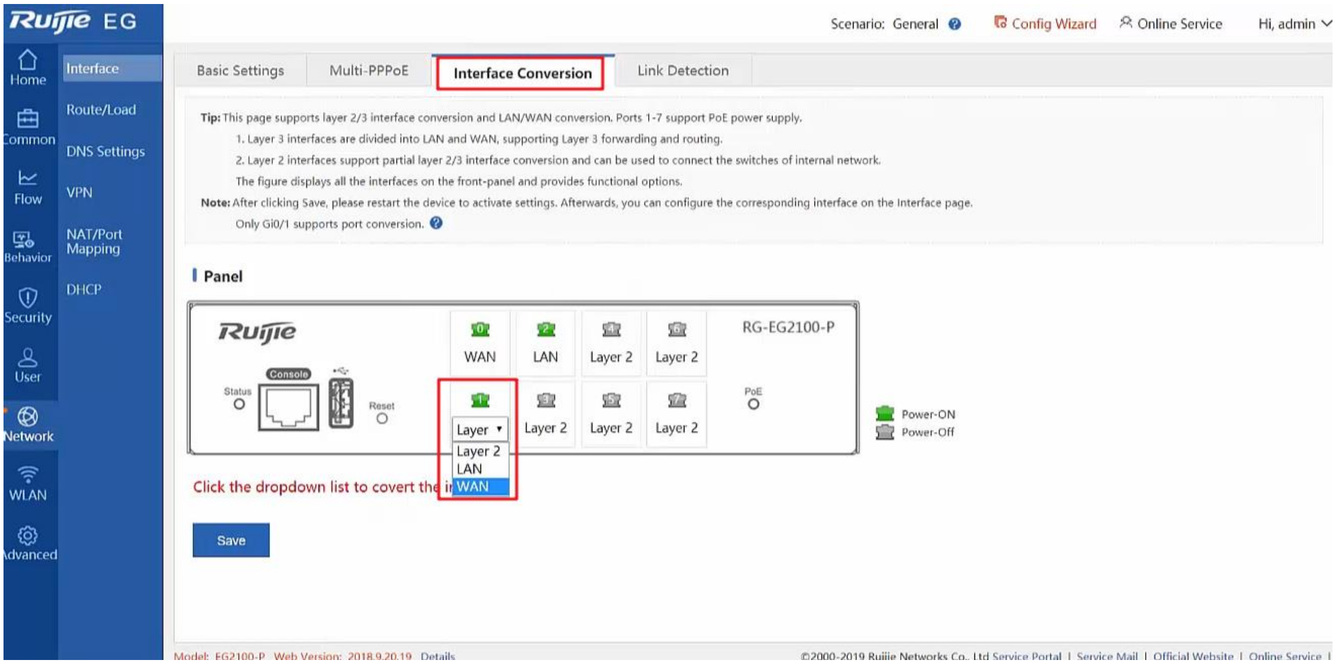
Uplink Bandwidth: 100 Mbps (Range: 0.5-10000). Default: 10.

Default Route: ☑Enable

NAT: ☑Enable

Src In Src Out: ☑Enable

Step 2: Change the LAN1 port to WAN port



Tip: This page supports layer 2/3 interface conversion and LAN/WAN conversion. Ports 1-7 support PoE power supply.

1. Layer 3 interfaces are divided into LAN and WAN, supporting Layer 3 forwarding and routing.
2. Layer 2 interfaces support partial layer 2/3 interface conversion and can be used to connect the switches of internal network.

The figure displays all the interfaces on the front-panel and provides functional options.

Note: After clicking Save, please restart the device to activate settings. Afterwards, you can configure the corresponding interface on the Interface page.

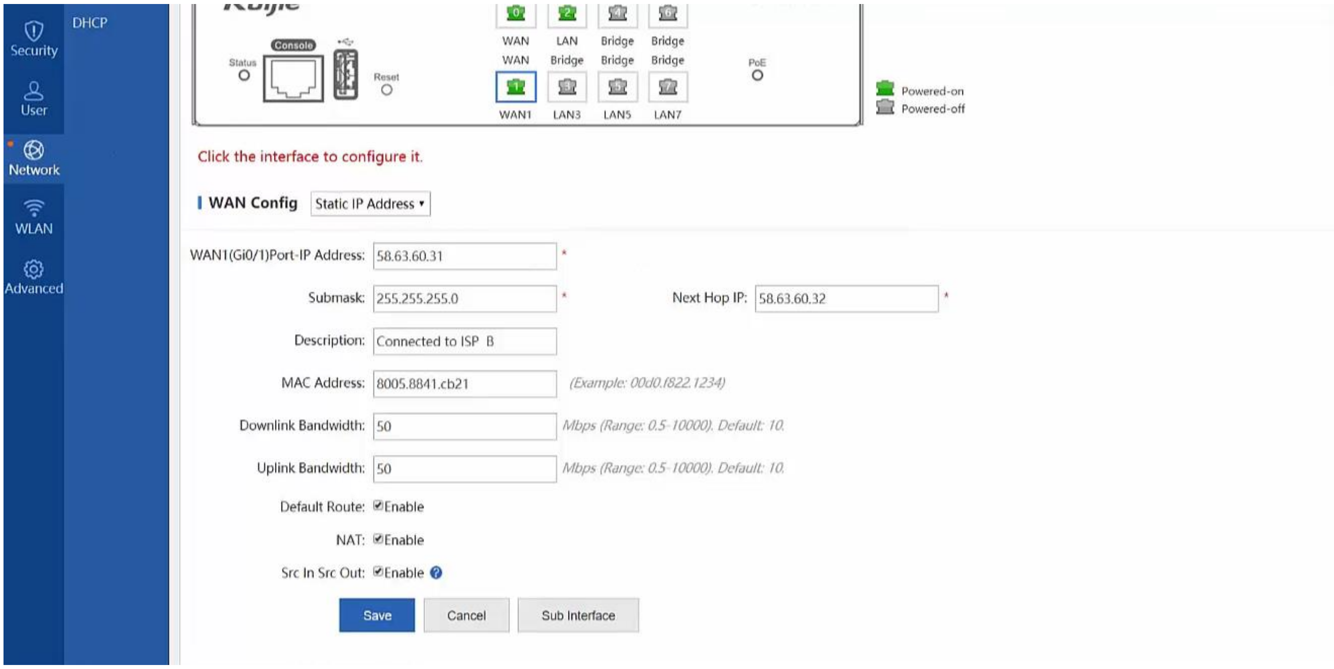
Only Gi0/1 supports port conversion.

Panel

Click the dropdown list to covert the i

Model: EG2100-P Web Version: 2018.9.20.19 Details ©2000-2019 Ruijie Networks Co., Ltd Service Portal | Service Mail | Official Website | Online Service |

Step 3: Configure WAN 1



Click the interface to configure it.

WAN Config Static IP Address

WAN1(Gi0/1)Port-IP Address: 58.63.60.31 *

Submask: 255.255.255.0 * Next Hop IP: 58.63.60.32 *

Description: Connected to ISP B

MAC Address: 8005.8841.cb21 (Example: 00d0.f822.1234)

Downlink Bandwidth: 50 Mbps (Range: 0.5-10000). Default: 10.

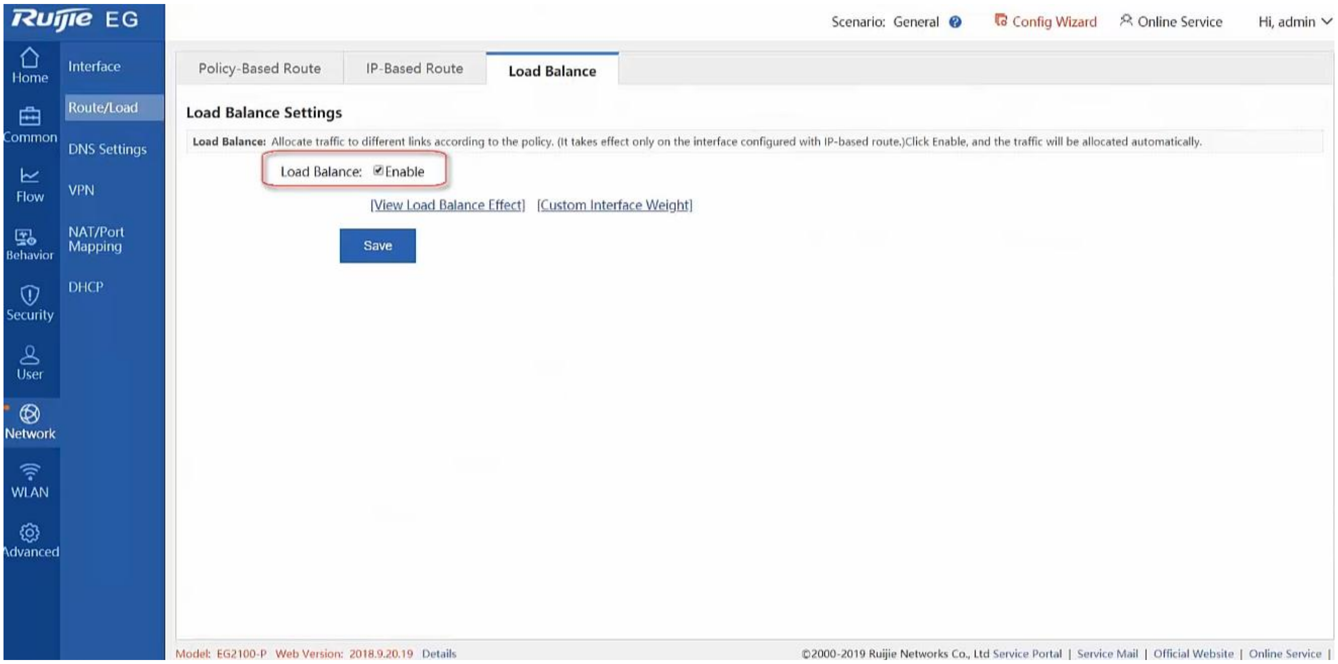
Uplink Bandwidth: 50 Mbps (Range: 0.5-10000). Default: 10.

Default Route: ☑Enable

NAT: ☑Enable

Src In Src Out: ☑Enable

Step 4: Enable Load Balance



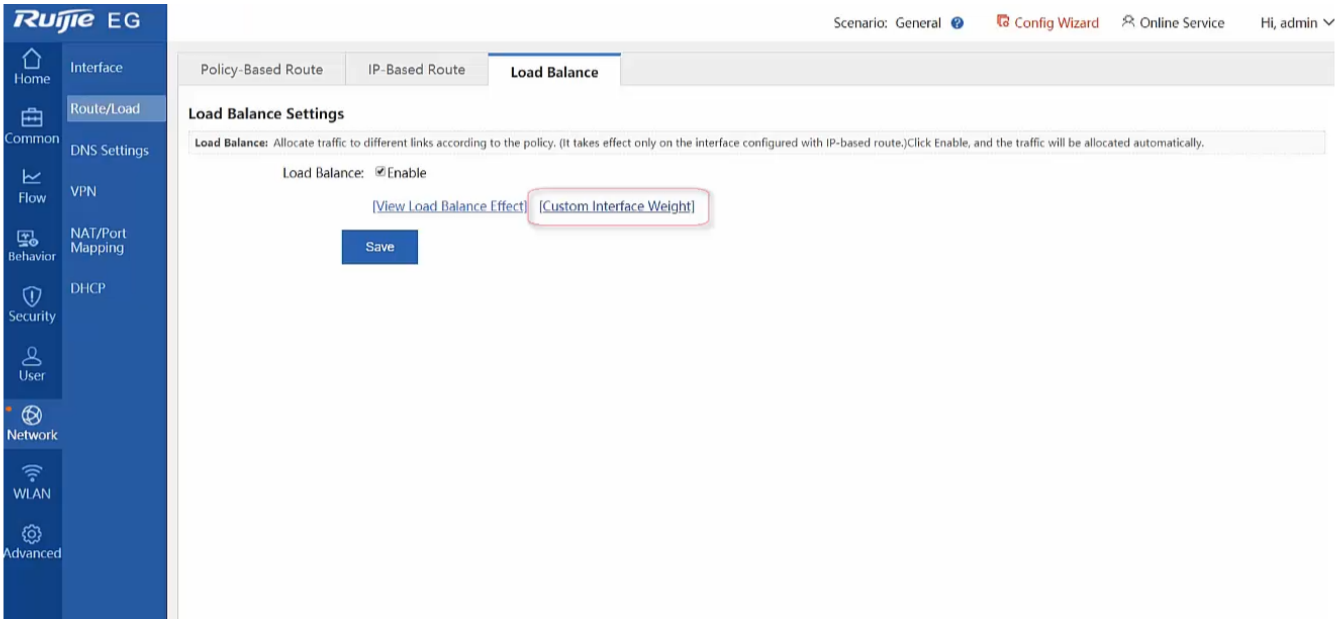
Load Balance Settings

Load Balance: Allocate traffic to different links according to the policy. (It takes effect only on the interface configured with IP-based route.)Click Enable, and the traffic will be allocated automatically.

Load Balance: ☑Enable

[View Load Balance Effect] [Custom Interface Weight]

Step 5: Configure the interface weight

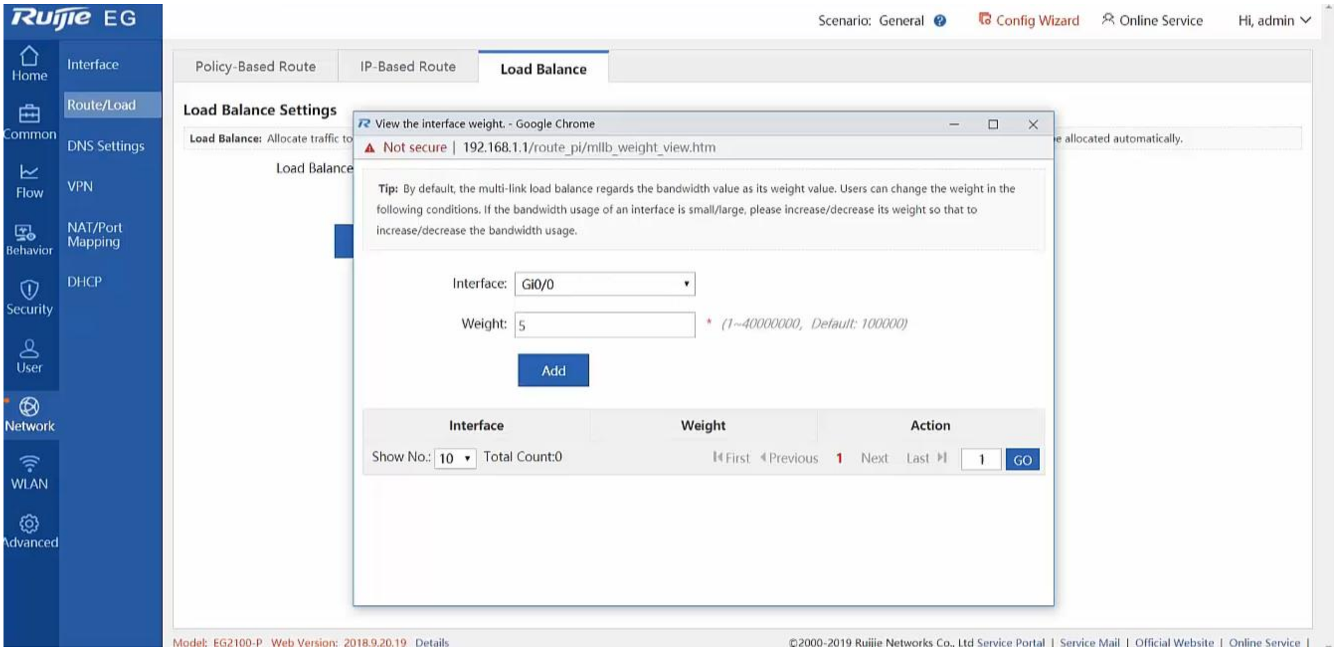


Load Balance Settings

Load Balance: Allocate traffic to different links according to the policy. (It takes effect only on the interface configured with IP-based route.)Click Enable, and the traffic will be allocated automatically.

Load Balance: ☑Enable

[View Load Balance Effect] [Custom Interface Weight]



Load Balance Settings

Load Balance: Allocate traffic to ... e allocated automatically.

Load Balance

View the interface weight. - Google Chrome

Not secure | 192.168.1.1/route_pi/mllb_weight_view.htm

Tip: By default, the multi-link load balance regards the bandwidth value as its weight value. Users can change the weight in the following conditions. If the bandwidth usage of an interface is small/large, please increase/decrease its weight so that to increase/decrease the bandwidth usage.

Interface: Gi0/0

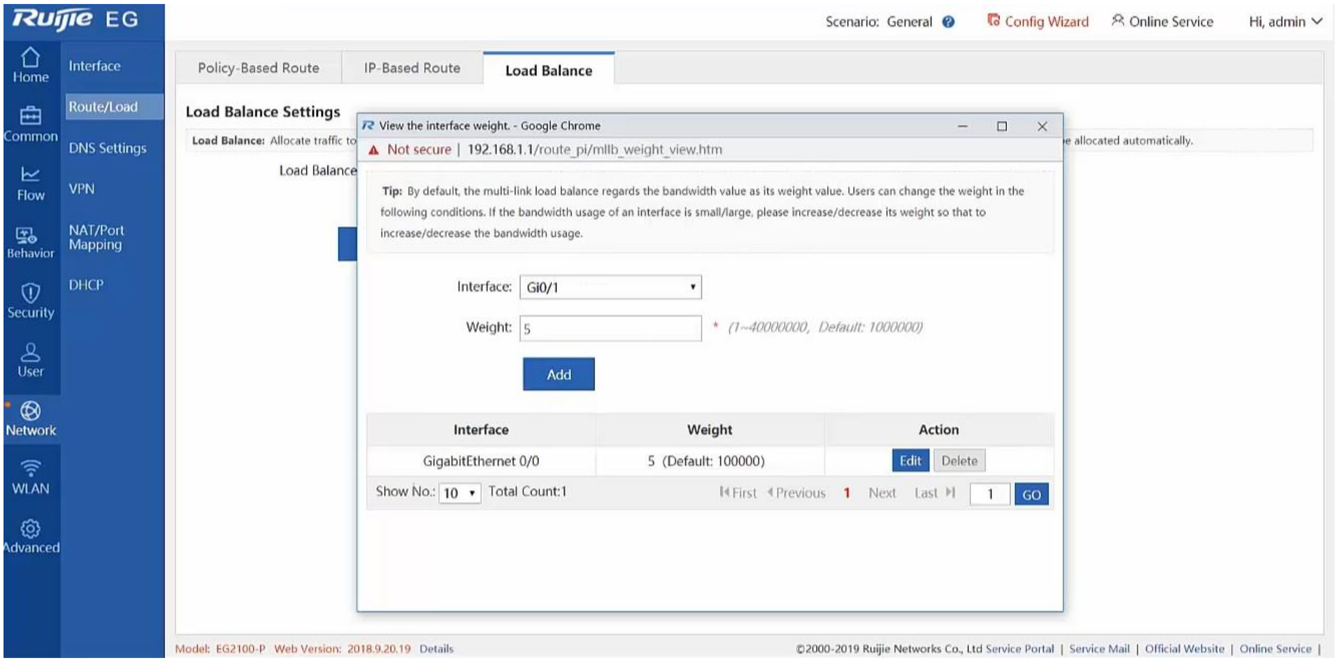
Weight: 5 * (1~40000000, Default: 100000)

Add

Interface	Weight	Action

Show No.: 10 Total Count:0 First Previous 1 Next Last 1 GO

Model: EG2100-P Web Version: 2018.9.20.19 Details ©2000-2019 Ruijie Networks Co., Ltd Service Portal | Service Mail | Official Website | Online Service |



Load Balance Settings

Load Balance: Allocate traffic to ... e allocated automatically.

Load Balance

View the interface weight. - Google Chrome

Not secure | 192.168.1.1/route_pi/mllb_weight_view.htm

Tip: By default, the multi-link load balance regards the bandwidth value as its weight value. Users can change the weight in the following conditions. If the bandwidth usage of an interface is small/large, please increase/decrease its weight so that to increase/decrease the bandwidth usage.

Interface: Gi0/1

Weight: 5 * (1~40000000, Default: 1000000)

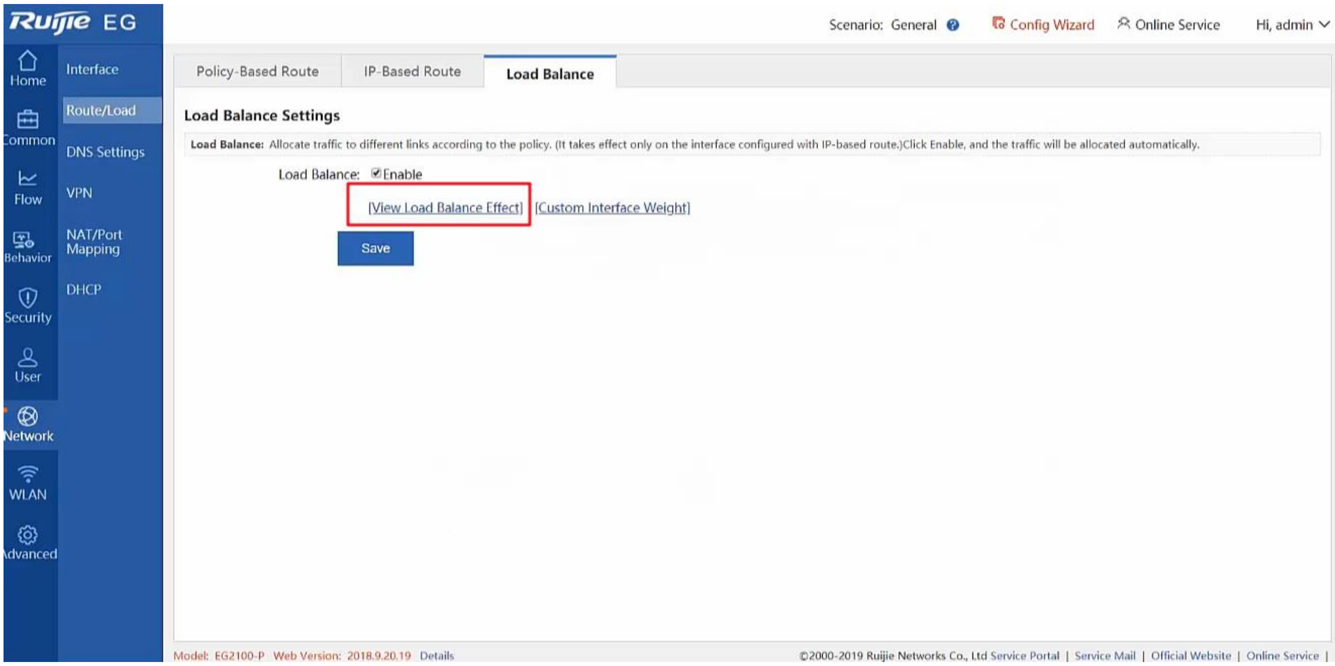
Add

Interface	Weight	Action
GigabitEthernet 0/0	5 (Default: 100000)	Edit Delete

Show No.: 10 Total Count:1 First Previous 1 Next Last 1 GO

Model: EG2100-P Web Version: 2018.9.20.19 Details ©2000-2019 Ruijie Networks Co., Ltd Service Portal | Service Mail | Official Website | Online Service |

Configuration Verfication

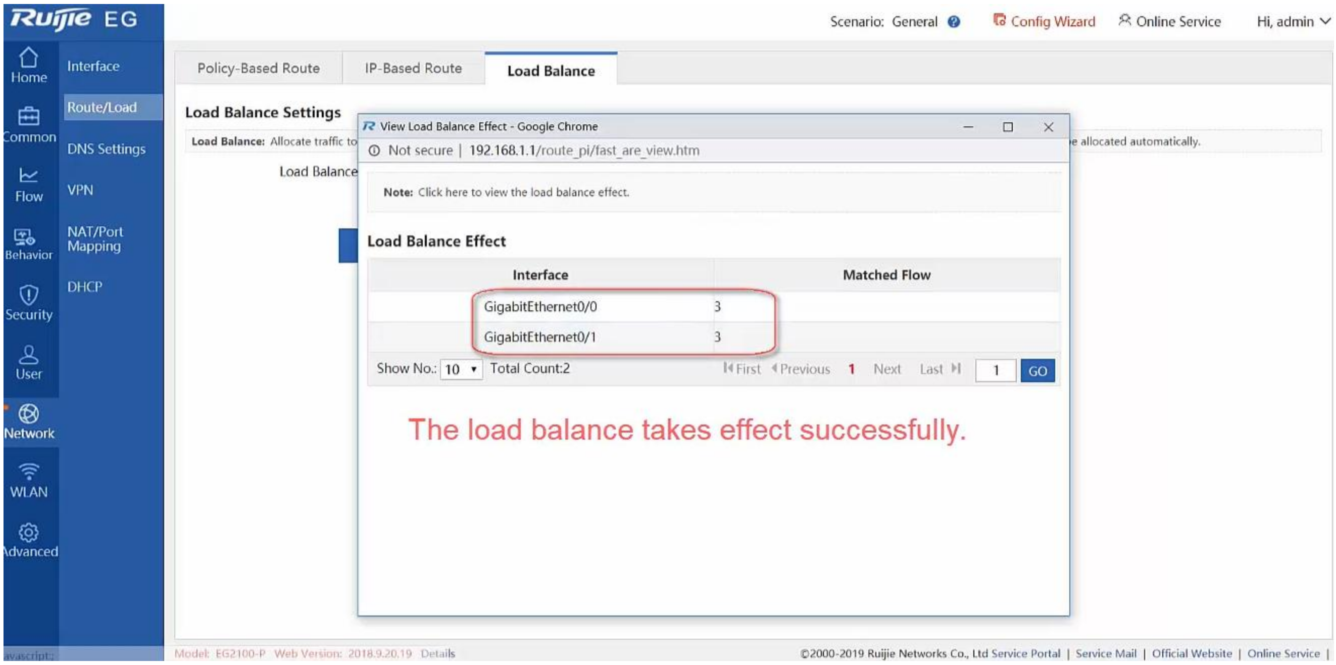


Load Balance Settings

Load Balance: Allocate traffic to different links according to the policy. (It takes effect only on the interface configured with IP-based route.)Click Enable, and the traffic will be allocated automatically.

Load Balance: ☑Enable

[View Load Balance Effect] [Custom Interface Weight]



Note: Click here to view the load balance effect.

Load Balance Effect

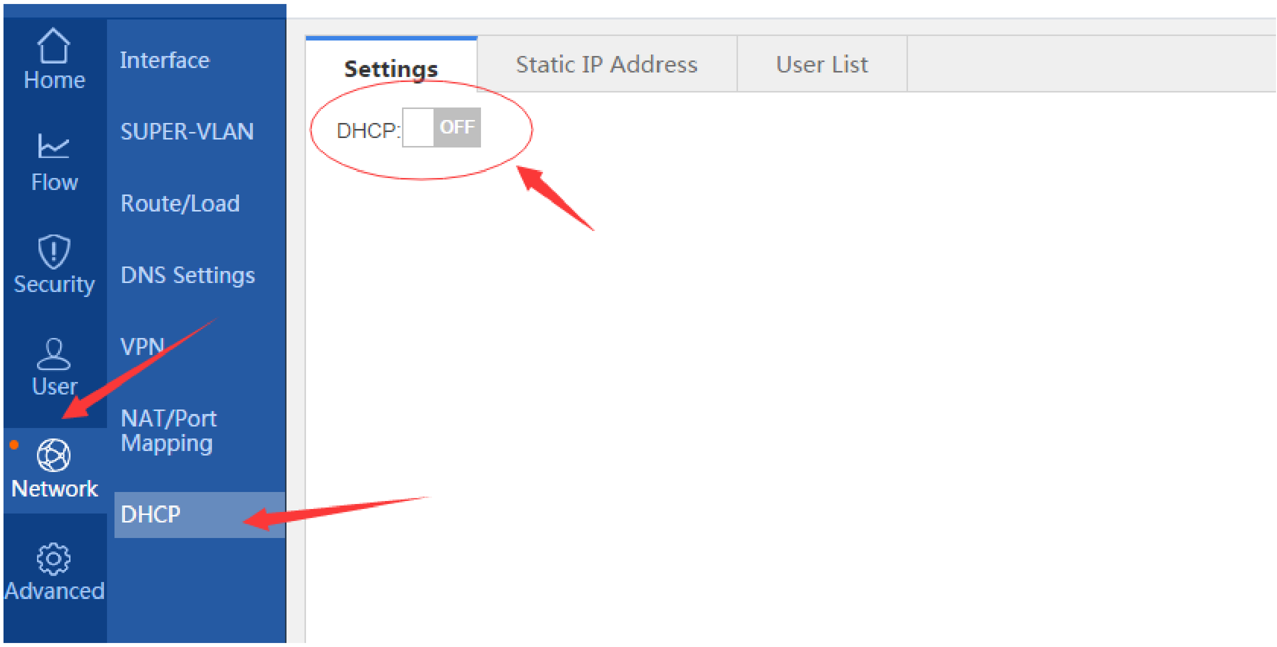
Interface	Matched Flow
GigabitEthernet0/0	3
GigabitEthernet0/1	3

Total Count:2

The load balance takes effect successfully.

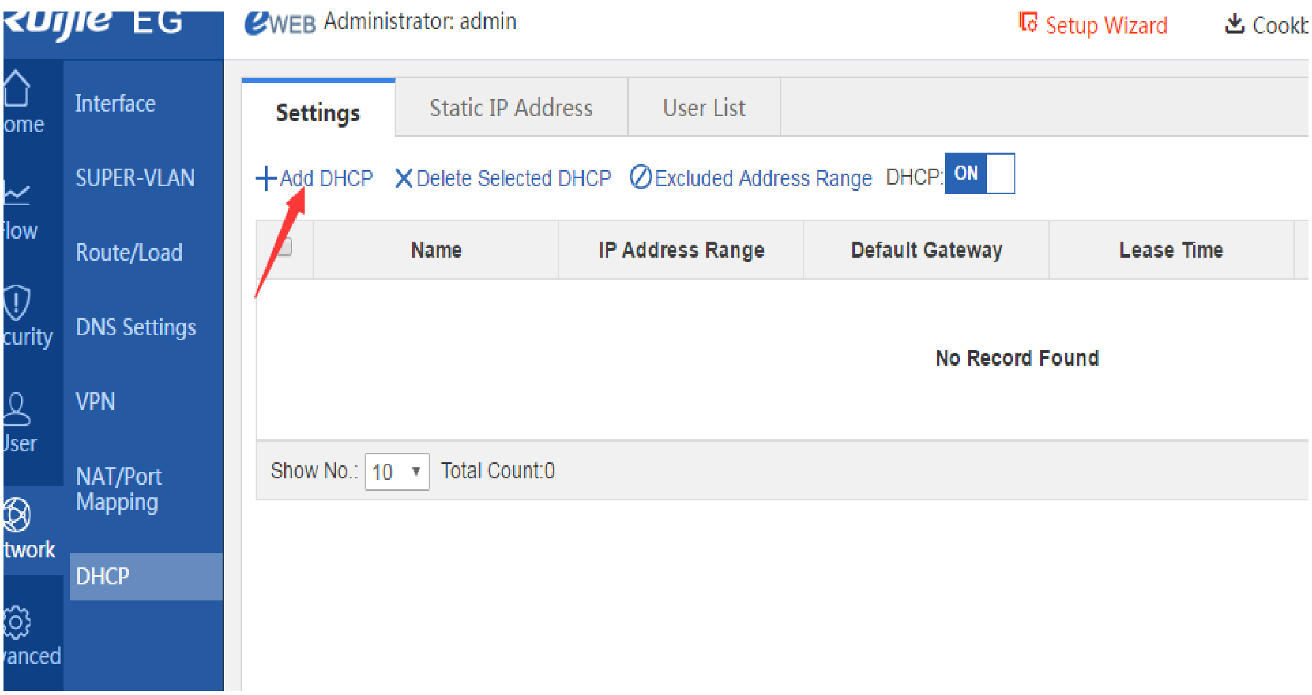
5.2 DHCP Configuration

Step 1-Turn on ‘DHCP’ service in ‘Network-DHCP’.



DHCP: OFF

Step 2-Click ‘Add DHCP’.



DHCP: ON

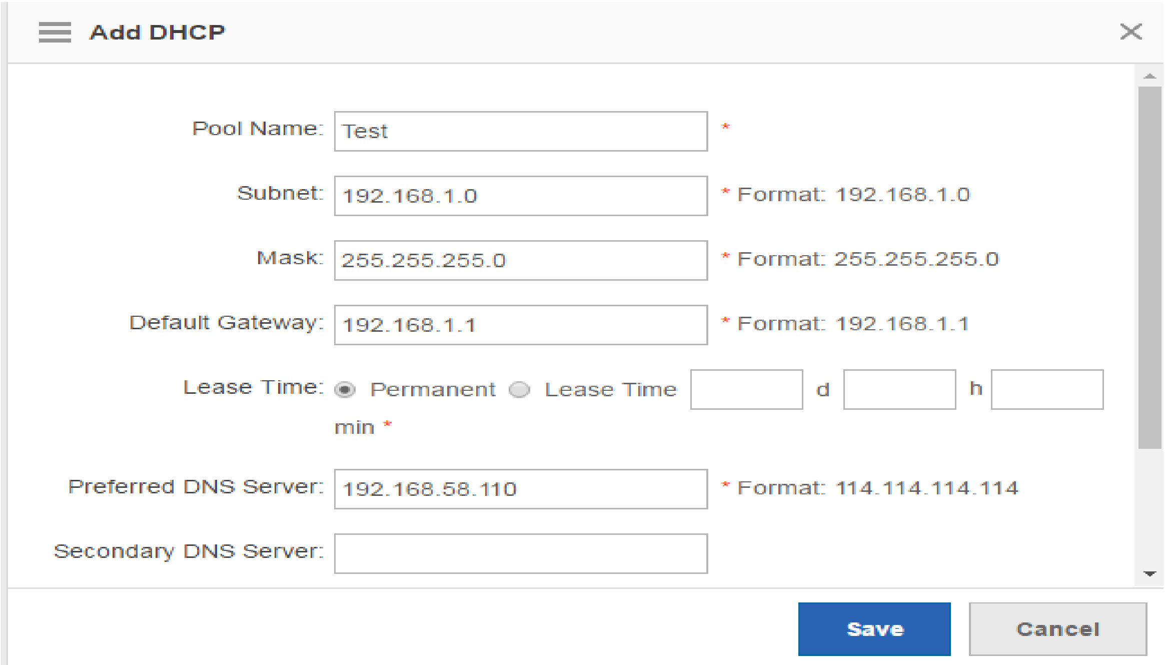
□	Name	IP Address Range	Default Gateway	Lease Time

No Record Found

Show No.: 10 ▾ Total Count:0

Step 3-Set necessary configuration, such as ‘DHCP Pool Name’, ‘Subnet’ and so on. Then click ‘Save’.

Note： You can also set option 43 or 138 for wireless AP getting AC’s IP address here.



Add DHCP

Pool Name: Test *

Subnet: 192.168.1.0 * Format: 192.168.1.0

Mask: 255.255.255.0 * Format: 255.255.255.0

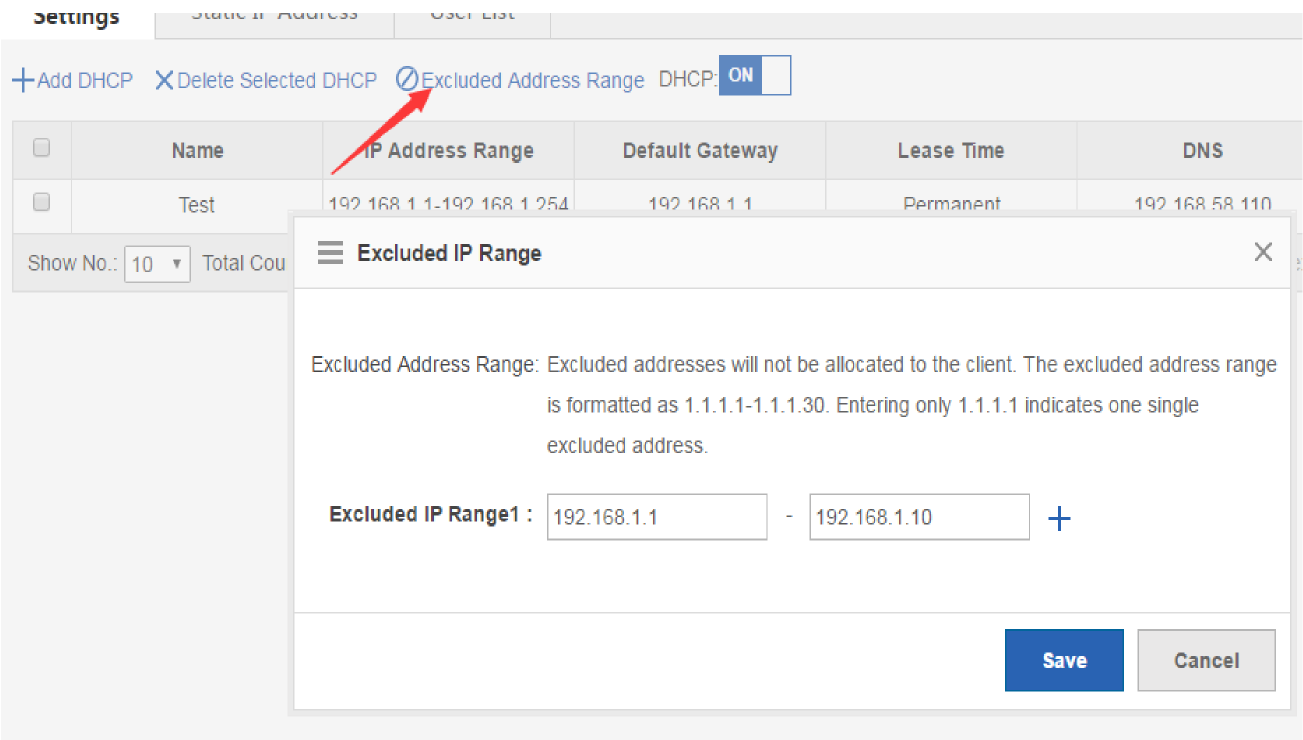
Default Gateway: 192.168.1.1 * Format: 192.168.1.1

Lease Time: ● Permanent ○ Lease Time d h min *

Preferred DNS Server: 192.168.58.110 * Format: 114.114.114.114

Secondary DNS Server:

Step 4-Set ‘Excluded Address Range’ to retain some IP address for servers or others if necessary.



□	Name	IP Address Range	Default Gateway	Lease Time	DNS
□	Test	192.168.1.1-192.168.1.254	192.168.1.1	Permanent	192.168.58.110

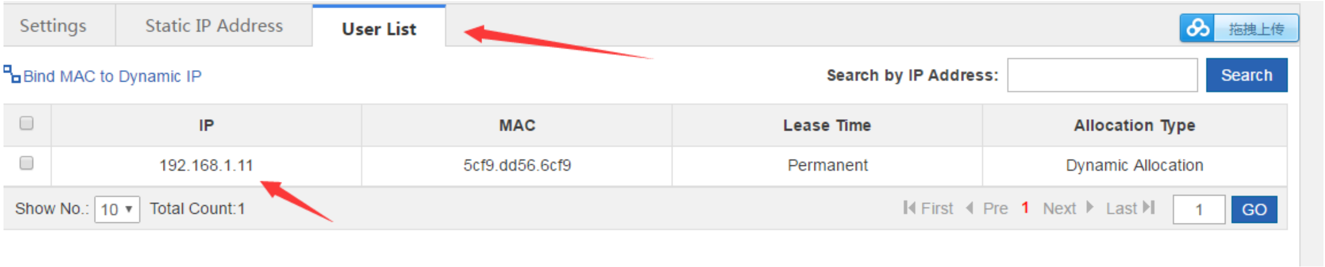
Show No.: 10 Total Cou

Excluded IP Range

Excluded Address Range: Excluded addresses will not be allocated to the client. The excluded address range is formatted as 1.1.1.1-1.1.1.30. Entering only 1.1.1.1 indicates one single excluded address.

Excluded IP Range1 : 192.168.1.1 - 192.168.1.10 +

Step 5-Test it, clear your PC IP address and change IP address getting way to automatic getting. Click ‘User List’, if your operation is effective, you will see your PC in this list.



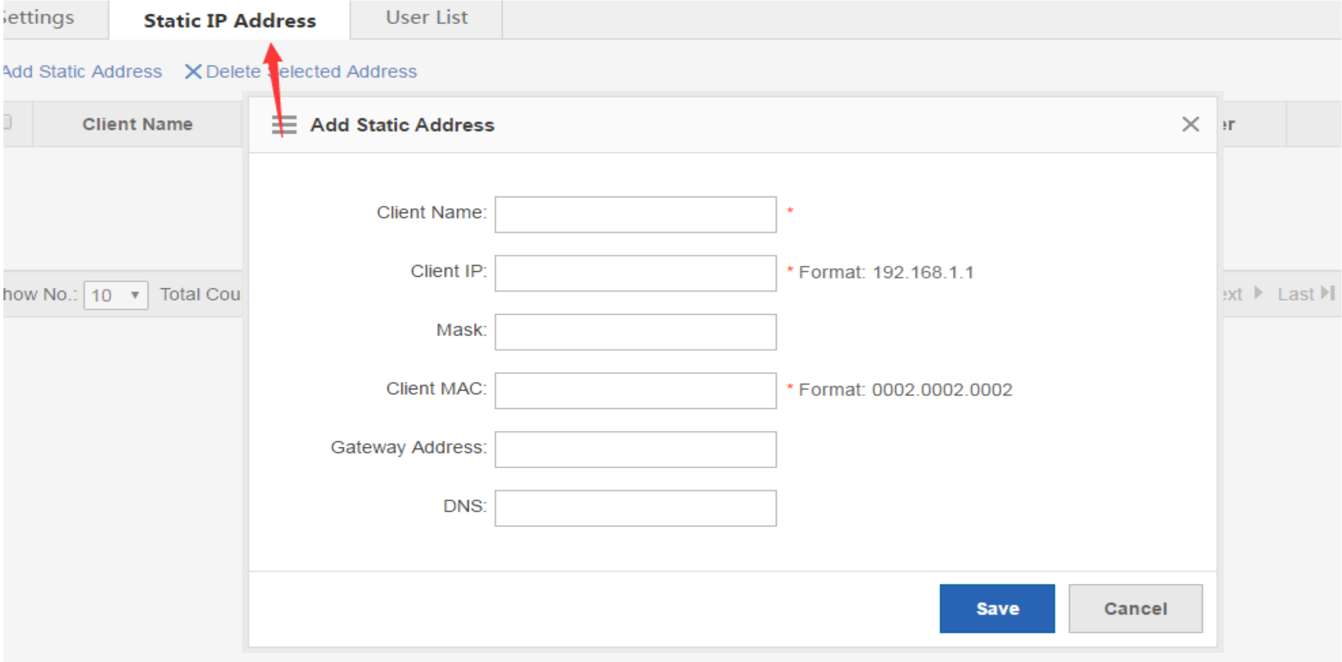
Bind MAC to Dynamic IP

Search by IP Address: [ ] Search

□	IP	MAC	Lease Time	Allocation Type
□	192.168.1.11	5cf9.dd56.6cf9	Permanent	Dynamic Allocation

Show No.: 10 ▾ Total Count:1

Added Step: If you want to give some terminals designated IP addresses from DHCP pool every time, you can configure 'Static IP Address' for them.



Add Static Address

Client Name: [ ] *

Client IP: [ ] * Format: 192.168.1.1

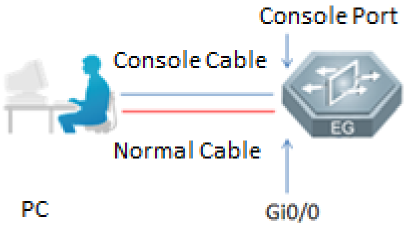
Mask: [ ]

Client MAC: [ ] * Format: 0002.0002.0002

Gateway Address: [ ]

DNS: [ ]

- Use CLI configure DHCP



Command is as follow:

```
Ruijie>enable
Ruijie#configure   ter
Ruijie(config)#service dhcp ------>Set DHCP service enable.
Ruijie(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.10 ------>Retain 192.168.1.1-192.168.1.10.

Ruijie(config)#ip dhcp pool Test ------>Creat a DHCP pool named 'Test'.

Ruijie(dhcp-config)#lease 0 1 0------> Set lease time，'0 1 0' means 0 day，1 hour，0 minute. Default lease time is 24 hours.

Ruijie(dhcp-config)#network 192.168.1.0 255.255.255.0 ------>Set IP address section for DHCP pool.
```

*The following is static IP distribution in DHCP.

```
Ruijie(dhcp-config)# hardware-address 0026.b90b.a48a      ------>Set terminal MAC address as '0026.b90b.a48a'.
Ruijie(dhcp-config)# host 192.168.1.150   255.255.255.0   ------>Set static IP and Mask.
```

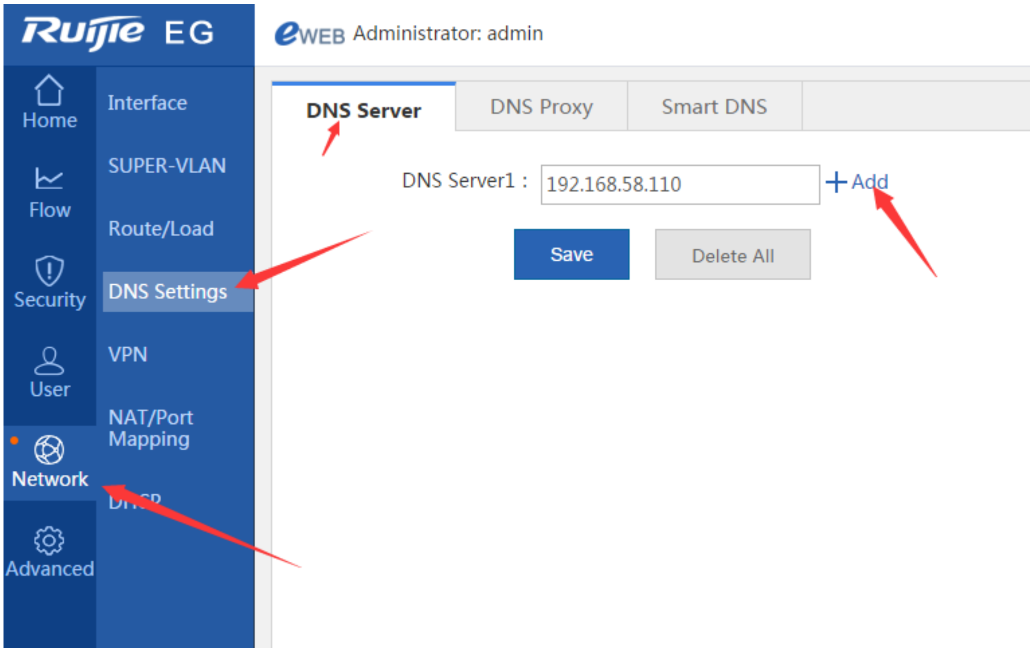
*The above is static IP distribution in DHCP.

```
Ruijie(dhcp-config)#dns-server 192.168.58.110   8.8.8.8------>192.168.58.110 is major DNS server，8.8.8.8 is backup.

Ruijie(dhcp-config)#default-router 192.168.1.1   ------>Set gateway IP address.

Ruijie(dhcp-config)#end

Ruijie#write             ------>Save configuration.
```

5.3 DNS Configuration

➢ Regular Configuration

Choose 'Network', choose 'DNS Settings', click 'DNS Server', add DNS server and save.



DNS Server1 : 192.168.58.110

➢ DNS Proxy

1. Working Principle

If you turn on DNS proxy, EG LAN port will intercept DNS message. Replace destination DNS server IP address with others which have been configured in WAN port. And then send the message to that new DNS server. That case, terminal will associate to the new DNS server.

2. Effect

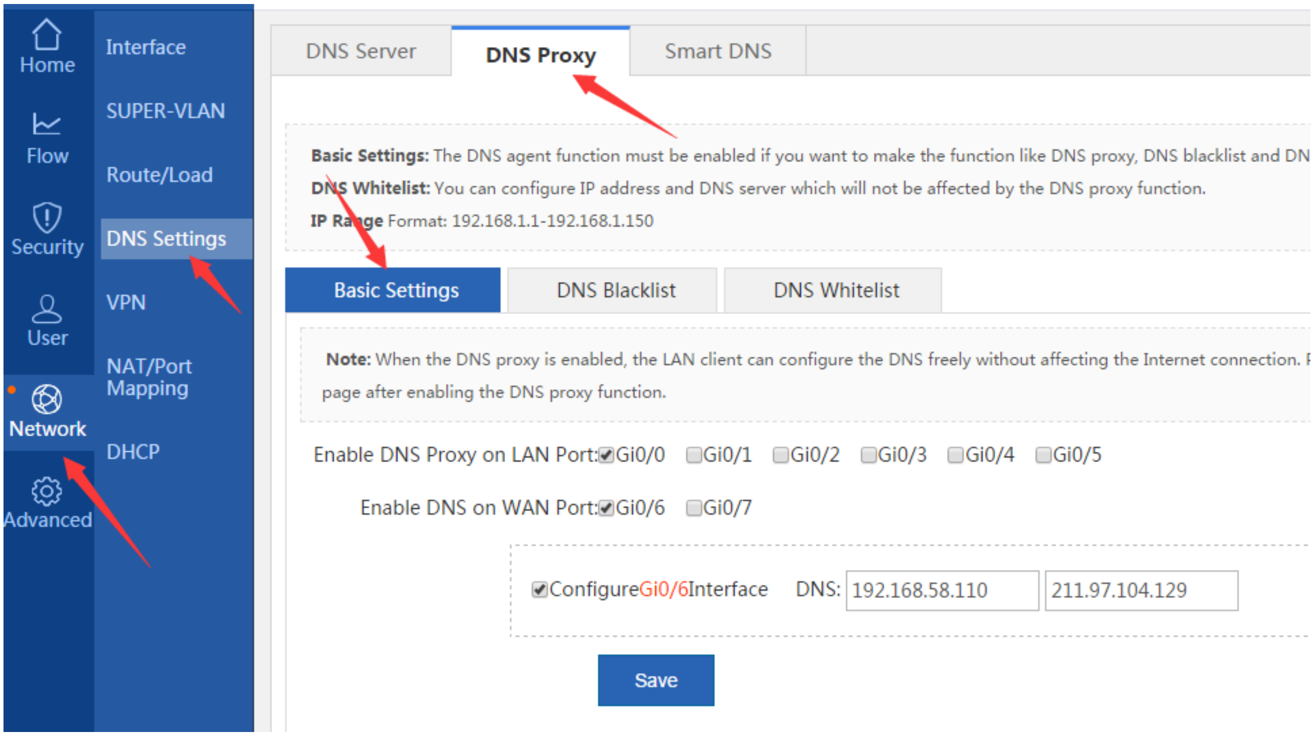
A. Realize load balance. When a link has loaded heavily, LAN port can intercept the message which destination DNS server is in that link. And then replace destination with other DNS server not in that link.

B. Users can set DNS server in his PC freely. If a user set a wrong DHCP IP address, LAN port can intercept the message and replace it with a right destination.

C. Detect faulty actively and switch to a new available DNS sever.

3. Operation Steps：

Step 1- Choose ‘Network’, choose ‘DNS Settings’, click ‘DNS Proxy’, choose ‘Basic Settings’.



Basic Settings: The DNS agent function must be enabled if you want to make the function like DNS proxy, DNS blacklist and DN

DNS Whitelist: You can configure IP address and DNS server which will not be affected by the DNS proxy function.

IP Range Format: 192.168.1.1-192.168.1.150

Note: When the DNS proxy is enabled, the LAN client can configure the DNS freely without affecting the Internet connection. F page after enabling the DNS proxy function.

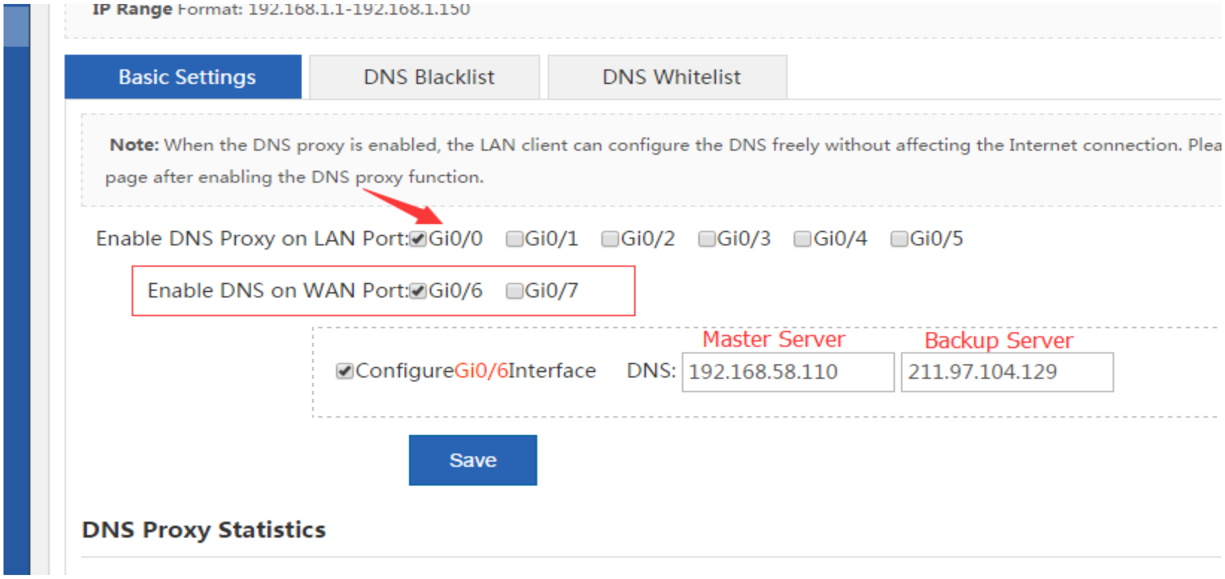
Enable DNS Proxy on LAN Port: ☑Gi0/0 □Gi0/1 □Gi0/2 □Gi0/3 □Gi0/4 □Gi0/5

Enable DNS on WAN Port: ☑Gi0/6 □Gi0/7

☑ConfigureGi0/6Interface DNS: 192.168.58.110 211.97.104.129

Step 2-Choose your intranet gateway to intercept DNS message. (Take Gi0/0 as an example)

Step 3-Choose your extranet port (Take Gi0/6 as an example), and input correct DNS server IP address.The first one is master server, the second one is backup server. And then click ‘Save’.



IP Range Format: 192.168.1.1-192.168.1.150

Note: When the DNS proxy is enabled, the LAN client can configure the DNS freely without affecting the Internet connection. Plea page after enabling the DNS proxy function.

Enable DNS Proxy on LAN Port:☑Gi0/0 □Gi0/1 □Gi0/2 □Gi0/3 □Gi0/4 □Gi0/5

Enable DNS on WAN Port:☑Gi0/6 □Gi0/7

Master Server Backup Server

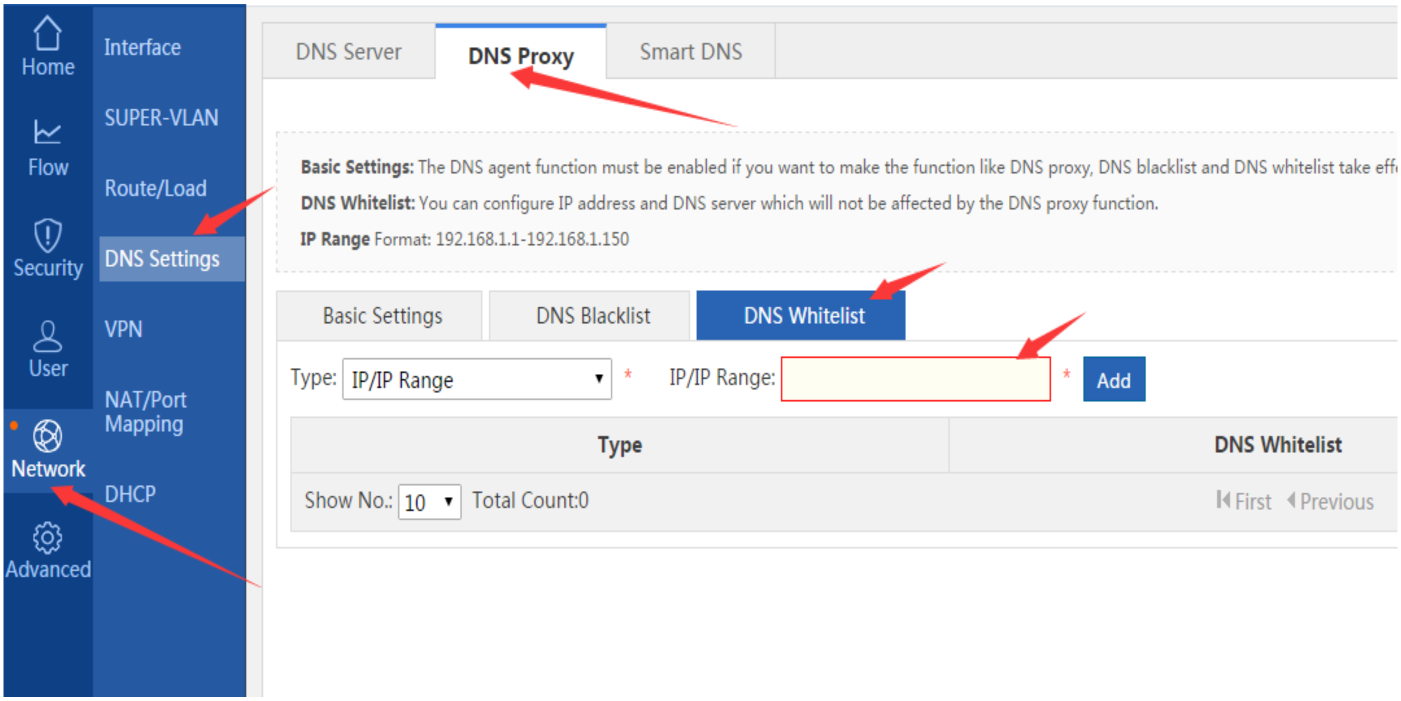
☑ConfigureGi0/6Interface DNS: 192.168.58.110 211.97.104.129

DNS Proxy Statistics

Step 4-You can change DNS server IP address in your computer to test if you can succeed to access other websites.

Step 5-Add IP address into ‘DNS Whitelist’. This way, DNS proxy will not have an influence on these IP/IP range. DNS whitelist effect is as the following picture.

Note：It is necessary to set nexthop IP address in WAN port (Except getting IP address by dialer and DHCP). For example, if Gi0/7 port needs to be set DNS proxy, you should set nethop IP address xxx.xxx.xxxx.xxx in Gi0/7.



Basic Settings: The DNS agent function must be enabled if you want to make the function like DNS proxy, DNS blacklist and DNS whitelist take eff

DNS Whitelist: You can configure IP address and DNS server which will not be affected by the DNS proxy function.

IP Range Format: 192.168.1.1-192.168.1.150

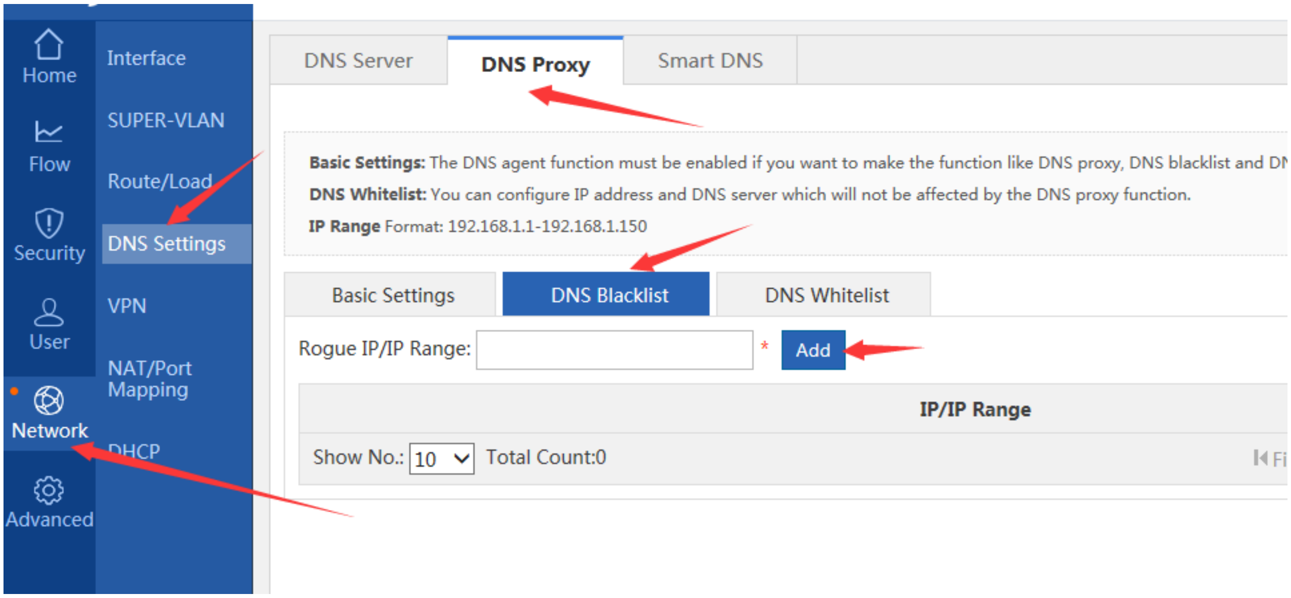
Type: IP/IP Range * IP/IP Range: *

Type	DNS Whitelist

Show No.: 10 Total Count:0

➢ DNS Blacklist

Add IP address into ‘DNS blacklist’. This way, DNS proxy will intercept DNS response packet, and discard it. Generally speaking, this function can prevent users from some malicious website attack.



Basic Settings: The DNS agent function must be enabled if you want to make the function like DNS proxy, DNS blacklist and DN

DNS Whitelist: You can configure IP address and DNS server which will not be affected by the DNS proxy function.

IP Range Format: 192.168.1.1-192.168.1.150

Rogue IP/IP Range: *

Show No.: 10 Total Count:0

5.4 Behavior Policies

5.4.1 Basic Settings

5.4.1.1 Enabling of All Audit Functions

Networking Requirements

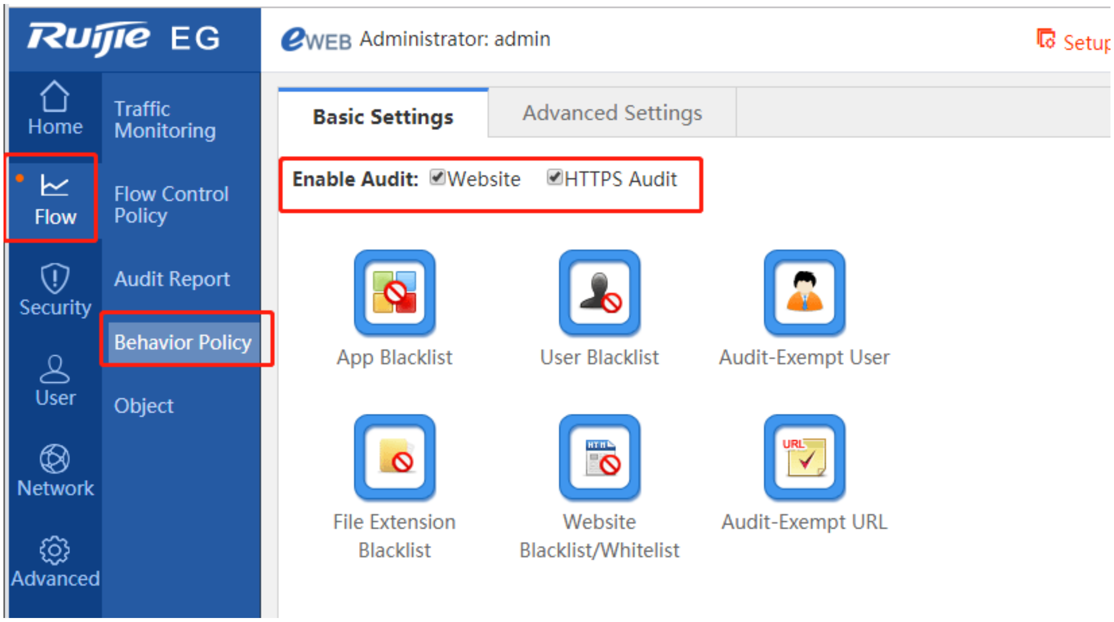
1. The EG device serves as an egress and can access the Internet by using a static IP address. The LAN user gateway is configured on the LAN port of the EG device, to implement the basic Internet access function.
2. The WAN bandwidth is 10 Mbps, the WAN port address is 192.168.33.56/24, the WAN gateway address is 192.168.33.1, and the LAN is in the 192.168.1.0/24 network segment.
3. Users in the LAN business security group (192.168.1.2 to 192.168.1.100) are prohibited from accessing the Internet.

Configuration Key Points

Enable all audit functions on Basic Settings.

Configuration Steps

Choose Flow > Behavior Policy > Basic Settings and select all audit functions.



Configuration Verification

View audit records of services in behavior reports.

5.4.1.2 User Blacklist

Networking Requirements

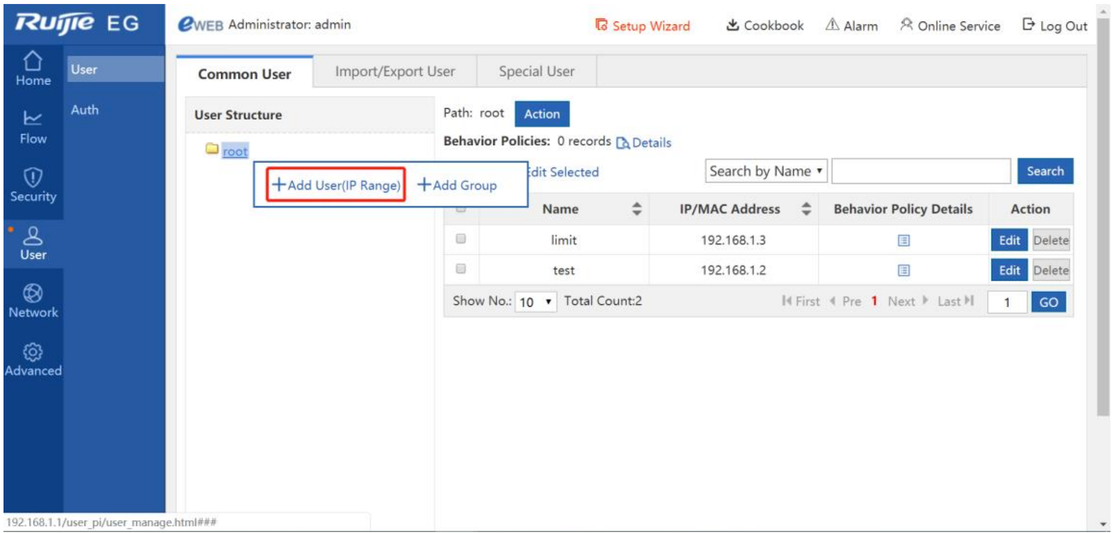
1. The EG device serves as an egress and can access the Internet by using a static IP address. The LAN user gateway is configured on the LAN port of the EG device, to implement the basic Internet access function.
2. The WAN bandwidth is 10 Mbps, the WAN port address is 192.168.33.56/24, the WAN gateway address is 192.168.33.1, and the LAN is in the 192.168.1.0/24 network segment.
3. Users in the LAN business security group (192.168.1.2 to 192.168.1.100) are prohibited from accessing the Internet.

Configuration Key Points

1. Choose User > User to add users to be prohibited from accessing the Internet.
2. Choose Flow > Behavior Policy > Basic Settings and click User Blacklist.

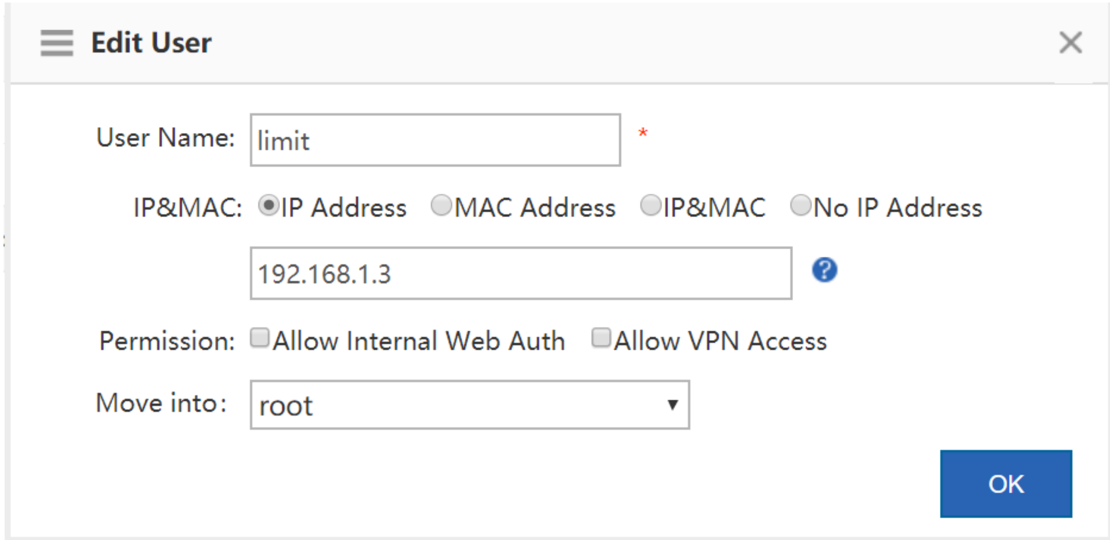
Configuration Steps

Choose User > User > Common User and add the IP addresses of users to be prohibited from accessing the Internet.



Name	IP/MAC Address	Behavior Policy Details	Action
limit	192.168.1.3	▤	Edit Delete
test	192.168.1.2	▤	Edit Delete

Show No.: 10 Total Count:2 First Pre 1 Next Last 1 GO



User Name: limit *

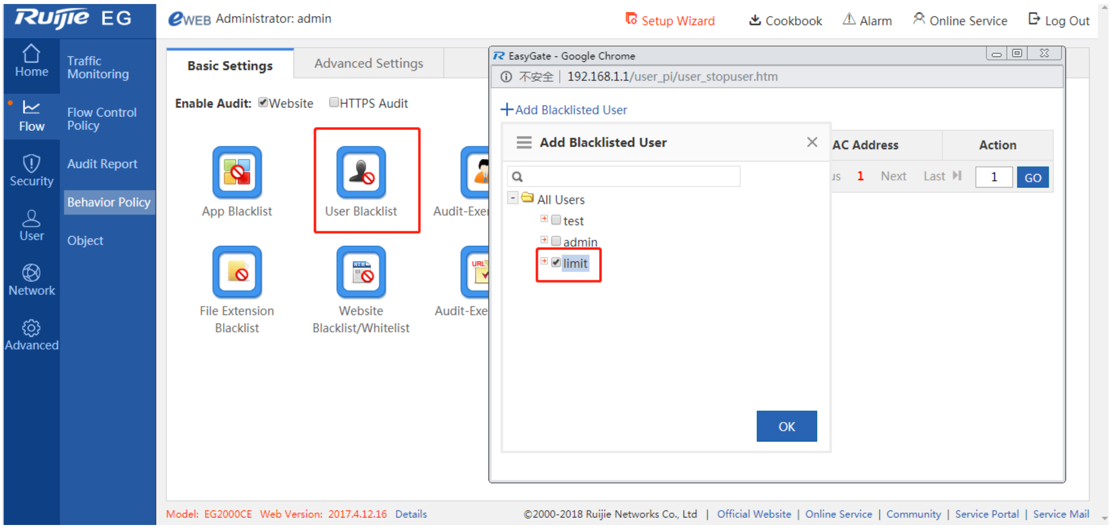
IP&MAC: ● IP Address ○ MAC Address ○ IP&MAC ○ No IP Address

192.168.1.3

Permission: □ Allow Internal Web Auth □ Allow VPN Access

Move into: root

Choose Flow > Behavior Policy > Basic Settings and click User Blacklist.



Enable Audit: ☑Website □HTTPS Audit

Click Add Blacklisted User.

Note: If the IP address of a blacklisted user is added to the audit-exempt user list, all applications of the user are limited by no policy.

5.4.1.3 Website Blacklist

Networking Requirements

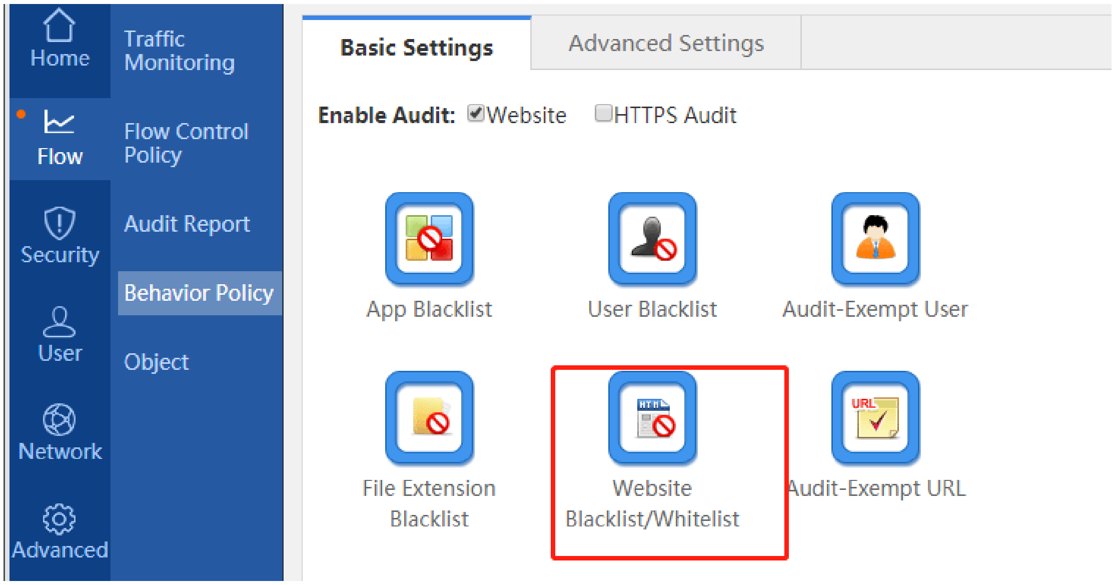
1. The EG device serves as an egress and can access the Internet by using a static IP address. The LAN user gateway is configured on the LAN port of the EG device, to implement the basic Internet access function.
2. The WAN bandwidth is 10 Mbps, the WAN port address is 192.168.33.56/24, the WAN gateway address is 192.168.33.1, and the LAN is in the 192.168.1.0/24 network segment.
3. All LAN users are prohibited from accessing the website www.baidu.com.

Configuration Key Points

1. Choose User > User > Common User and add users to be prohibited from accessing the website www.baidu.com.
2. Choose Flow > Behavior Policy > Basic Settings, click Website Blacklist/Whitelist, and click Blacklist Mode.

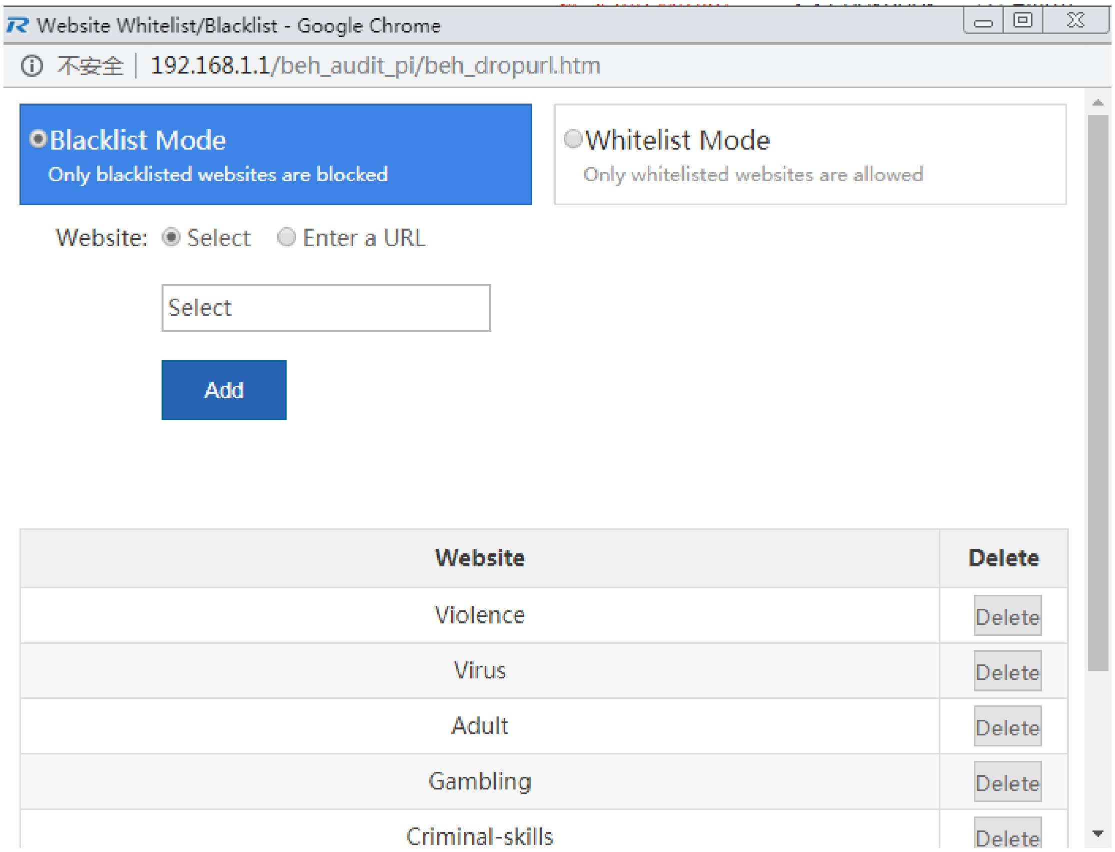
Configuration Steps

1. Choose Flow > Behavior Policy > Basic Settings and click Website Blacklist/Whitelist.



Enable Audit: ☑Website ☐HTTPS Audit

2. Click Blacklist Mode and add a website to the blacklist.



Website Whitelist/Blacklist - Google Chrome

不安全 | 192.168.1.1/beh_audit_pi/beh_dropurl.htm

● Blacklist Mode
Only blacklisted websites are blocked

○ Whitelist Mode
Only whitelisted websites are allowed

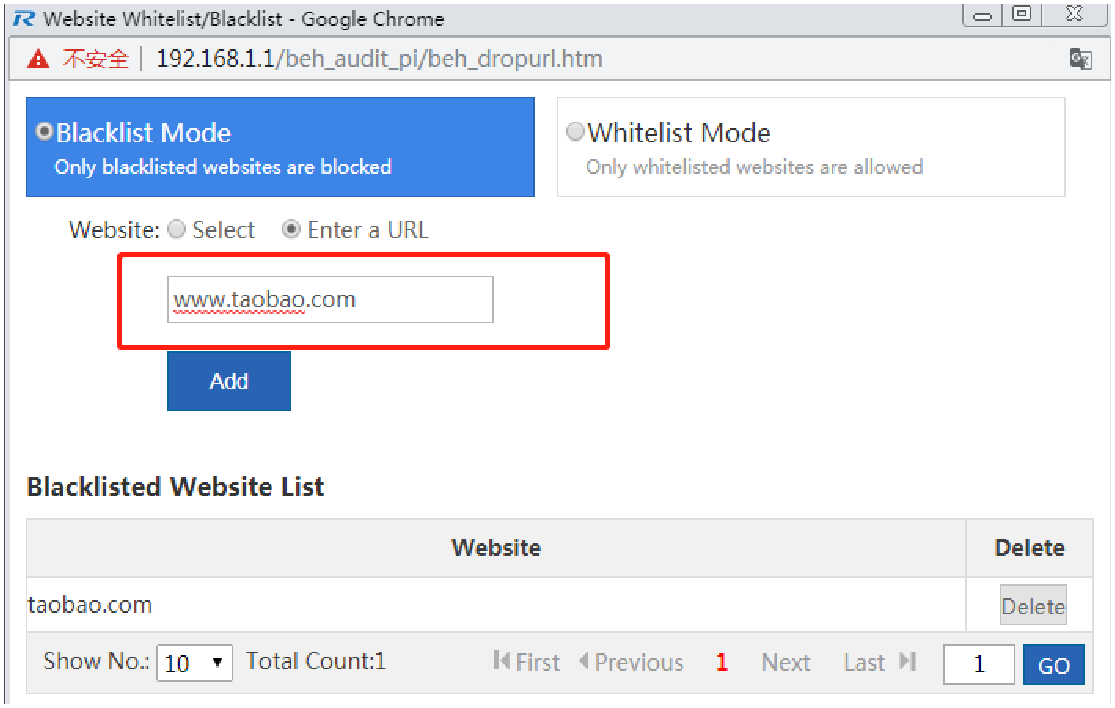
Website: ● Select ○ Enter a URL

Select

Add

Website	Delete
Violence	Delete
Virus	Delete
Adult	Delete
Gambling	Delete
Criminal-skills	Delete

The URL categories displayed after clicking Select are default website classifications of the device. Alternatively, you can click Enter a URL to enter a URL.



Website Whitelist/Blacklist - Google Chrome

不安全 | 192.168.1.1/beh_audit_pi/beh_dropurl.htm

● Blacklist Mode
Only blacklisted websites are blocked

○ Whitelist Mode
Only whitelisted websites are allowed

Website: ○ Select ● Enter a URL

www.taobao.com

Add

Blacklisted Website List

Website	Delete
taobao.com	Delete

Show No.: 10 ▼ Total Count:1 First Previous 1 Next Last 1 GO

Keyword matching is adopted here. You only need to enter the keyword of the primary domain name to be blacklisted even if there are secondary domain names or multi-level directories.

Configuration Verification

When a LAN user accesses www.baidu.com, a prompt is displayed, indicating that the user is prohibited from accessing this website and needs to contact the website administrator.

5.4.1.4 Website Whitelist

Networking Requirements

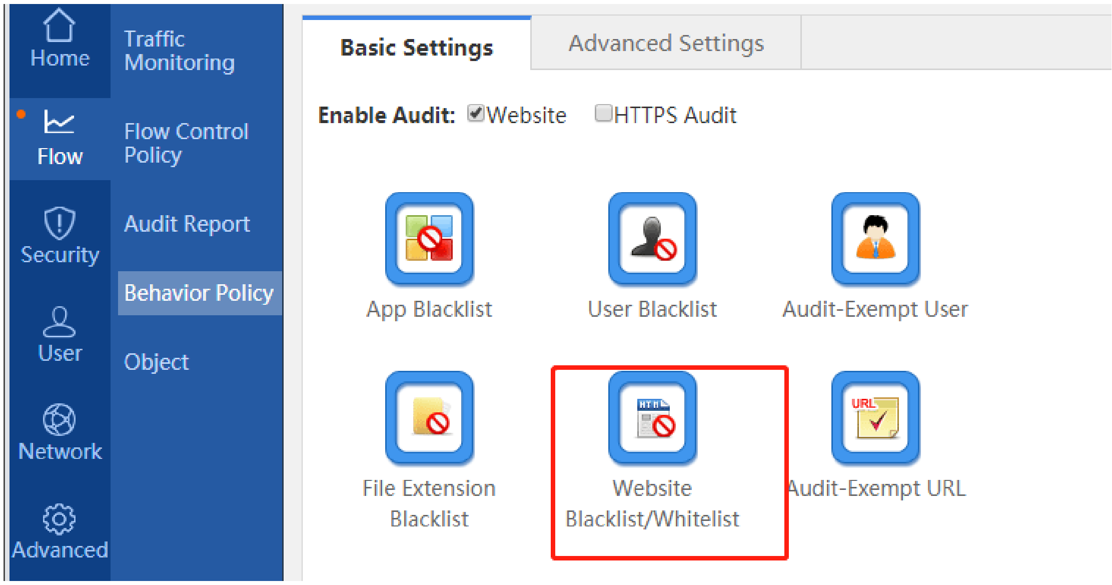
1. The EG device serves as an egress and can access the Internet by using a static IP address. The LAN user gateway is configured on the LAN port of the EG device, to implement the basic Internet access function.
2. The WAN bandwidth is 10 Mbps, the WAN port address is 192.168.33.56/24, the WAN gateway address is 192.168.33.1, and the LAN is in the 192.168.1.0/24 network segment.
3. LAN users are allowed to access only the specified website www.126.com.

Configuration Key Points

1. Choose User > User and add user IP addresses.
2. Choose Flow > Behavior Policy > Basic Settings, click Website Blacklist/Whitelist, and click Whitelist Mode.

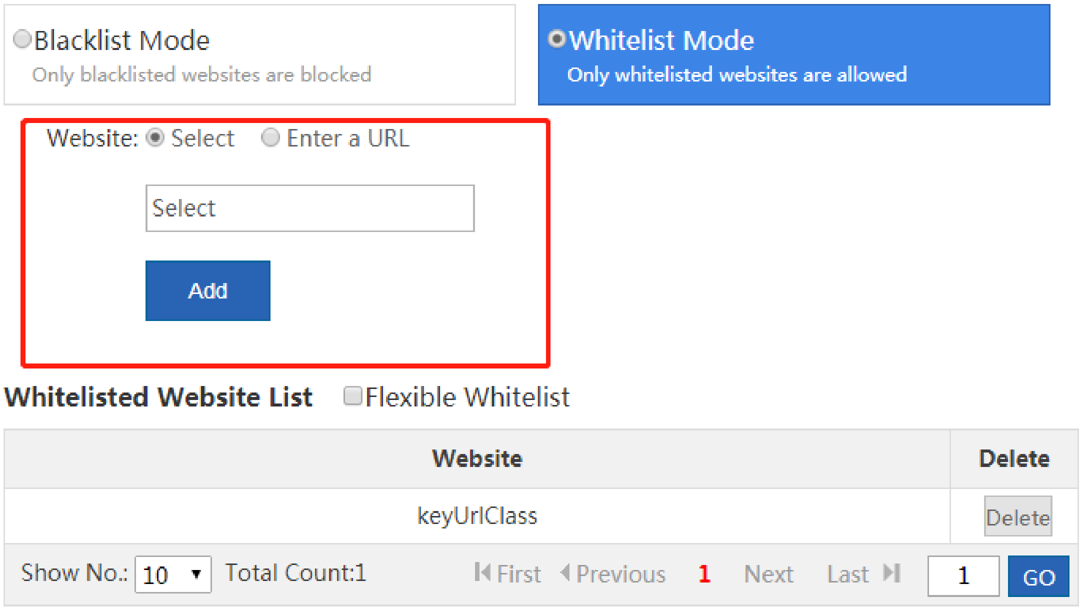
Configuration Steps

1. Choose Flow > Behavior Policy > Basic Settings and click Website Blacklist/Whitelist.



Enable Audit: ☑Website ☐HTTPS Audit

2. Click Whitelist Mode and add a website to the whitelist.



○ Blacklist Mode
Only blacklisted websites are blocked

● Whitelist Mode
Only whitelisted websites are allowed

Website: ● Select ○ Enter a URL

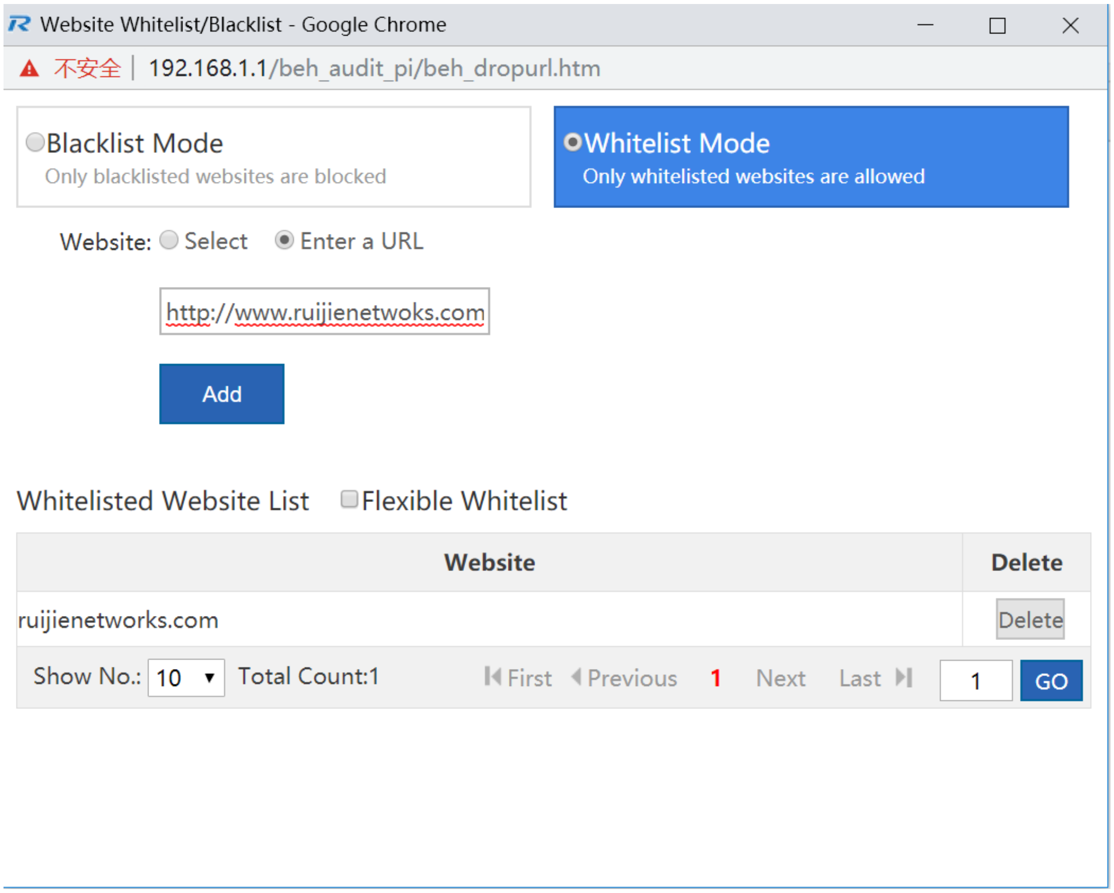
Select

Whitelisted Website List □ Flexible Whitelist

Website	Delete
keyUrlClass	Delete

Show No.: 10 ▾ Total Count:1

The URL categories displayed after clicking Select are default website classifications of the device. Alternatively, you can click Enter a URL to enter a URL.



Website Whitelist/Blacklist - Google Chrome

不安全 | 192.168.1.1/beh_audit_pi/beh_dropurl.htm

○ Blacklist Mode
Only blacklisted websites are blocked

● Whitelist Mode
Only whitelisted websites are allowed

Website: ○ Select ● Enter a URL

http://www.ruijienetwoks.com

Add

Whitelisted Website List □ Flexible Whitelist

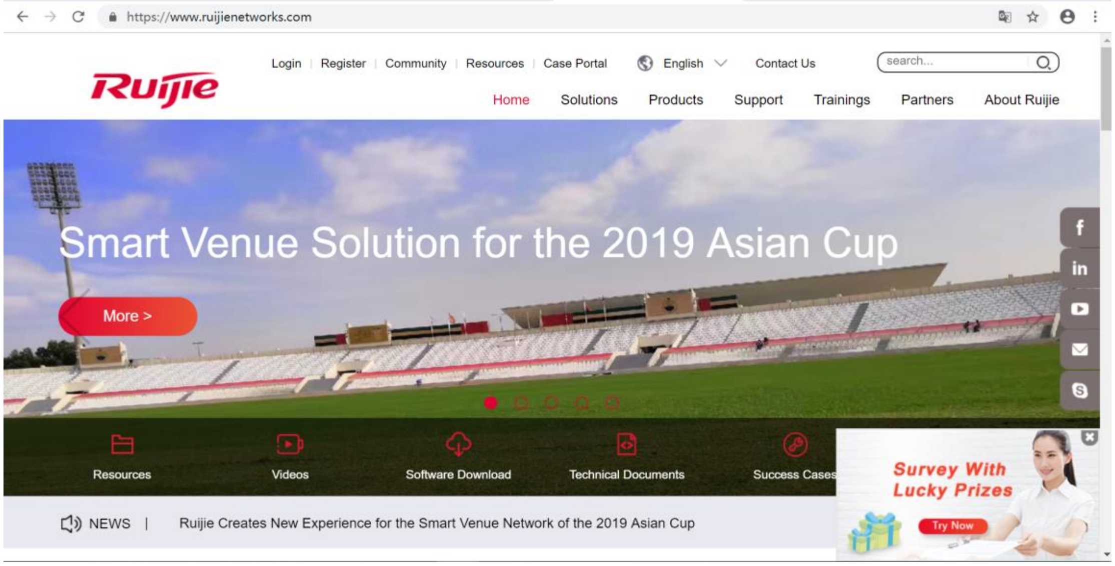
Website	Delete
ruijienetworks.com	Delete

Show No.: 10 ▾ Total Count:1 First Previous 1 Next Last 1 GO

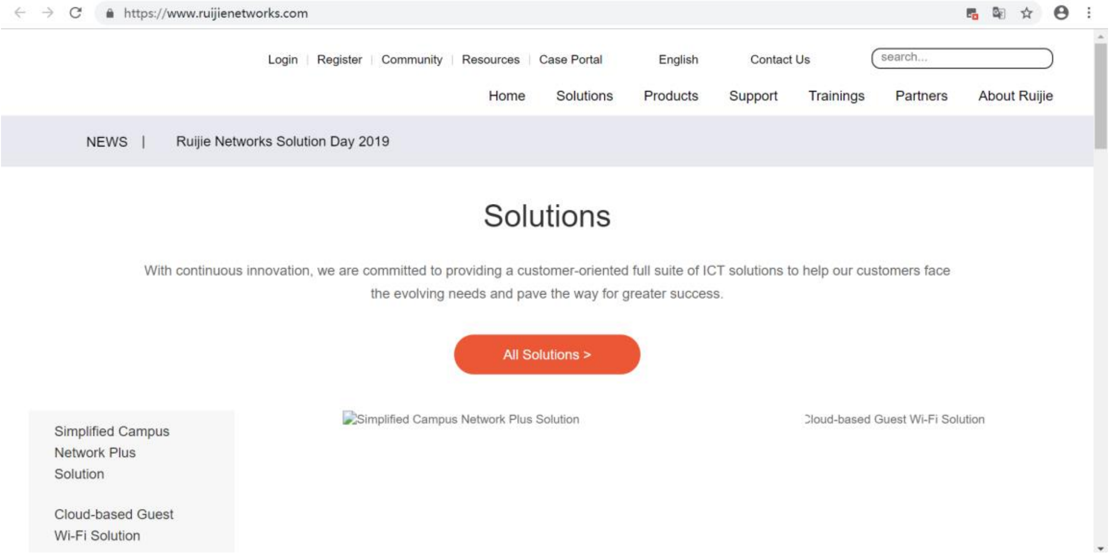
Flexible Whitelist: After Flexible Whitelist is selected, some pictures not belonging to a whitelisted website can be normally displayed when the whitelisted website is accessed. For the test process, see "Configuration Verification."

Configuration Verification

Test whether www.ruijienetworks.com can be accessed. The website can be normally accessed but other websites cannot.


https://www.ruijienetworks.com
Login | Register | Community | Resources | Case Portal
English
Contact Us
search...
Ruijie
Home
Solutions
Products
Support
Trainings
Partners
About Ruijie
Smart Venue Solution for the 2019 Asian Cup
More >
Resources
Videos
Software Download
Technical Documents
Success Cases
Survey With Lucky Prizes
Try Now
NEWS | Ruijie Creates New Experience for the Smart Venue Network of the 2019 Asian Cup

The following figure shows the website displayed when Flexible Whitelist is not selected.


https://www.ruijienetworks.com
Login | Register | Community | Resources | Case Portal
English
Contact Us
search...
Home
Solutions
Products
Support
Trainings
Partners
About Ruijie
NEWS | Ruijie Networks Solution Day 2019
All Solutions >
Simplified Campus Network Plus Solution
Cloud-based Guest Wi-Fi Solution
Simplified Campus Network Plus Solution
Cloud-based Guest Wi-Fi Solution

Solutions

With continuous innovation, we are committed to providing a customer-oriented full suite of ICT solutions to help our customers face the evolving needs and pave the way for greater success.

The access to other websites is prohibited.

5.4.1.5 Audit-Exempt URL

Networking Requirements

1. The EG device serves as an egress and can access the Internet by using a static IP address. The LAN user gateway is configured on the LAN port of the EG device, to implement the basic Internet access function.
2. The WAN bandwidth is 10 Mbps, the WAN port address is 192.168.33.56/24, the WAN gateway address is 192.168.33.1, and the LAN is in the 192.168.1.0/24 network segment.
3. All LAN users can access the audit-exempt website www.google.com.

Configuration Key Points

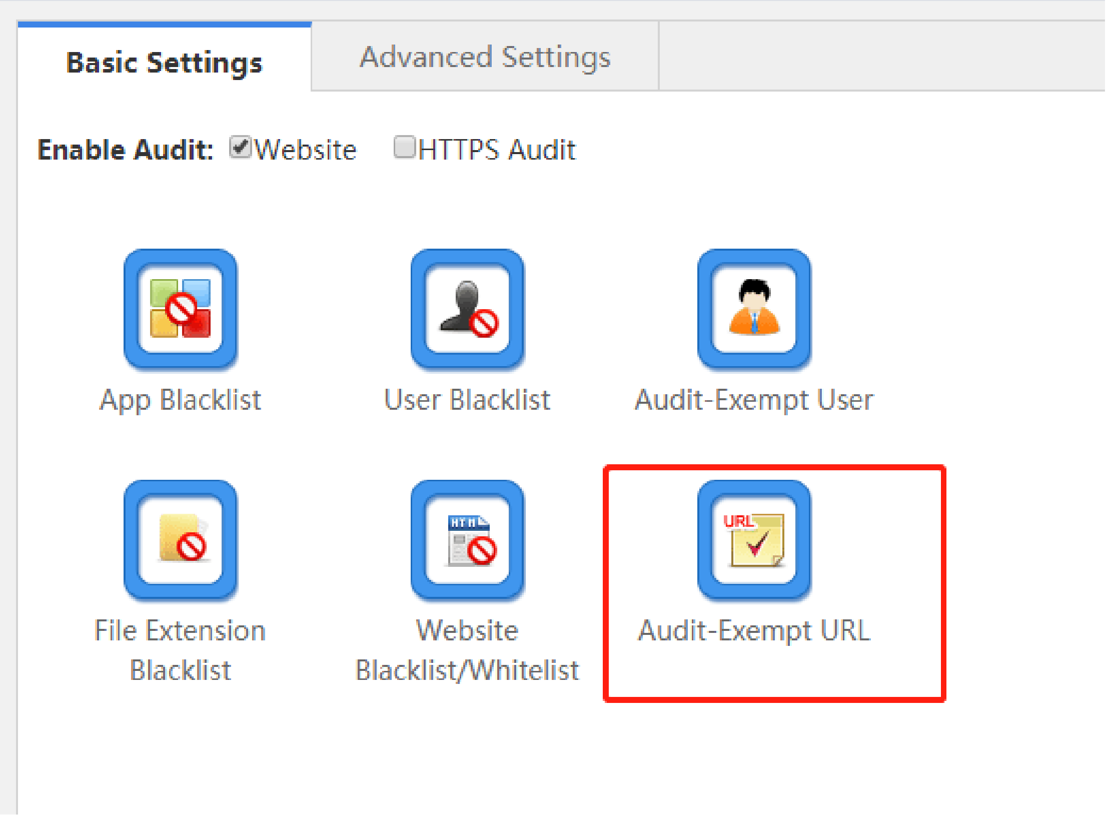
1. Choose User > User > Common User and add users who can access the audit-exempt website www.google.com.
2. Choose Flow > Behavior Policy > Basic Settings, and click Audit-Exempt URL to add audit-exempt URLs.

Note: If you select Shield Invalid/Virus Websites in wizard-based setup or enable website access in default audit in Behavior Policy, the system automatically delivers one audit-exempt website policy to exempt the websites of the unknown category and system upgrade category from audit, to prevent junk data audit. The priority of the website audit exemption policy is high. If you block the websites of the preceding two categories in Behavior Policy > Advanced Settings, the blocking may fail.

For example, a customer configures a behavior policy to block www.360safe.com, which belongs to the system upgrade category by default. The website audit exemption policy has a higher priority and users can still access www.360safe.com even if this website is configured in a different category. To avoid such a case: (1) Check whether the category of the website www.360safe.com is correct. If no, contact R&D engineers. (2) Run commands on the CLI to delete the system upgrade category from the website audit exemption policy. If you still want to exempt other websites of the system upgrade category from audit, configure websites with priorities lower than that of the policy for blocking www.360safe.com on Advanced Settings.

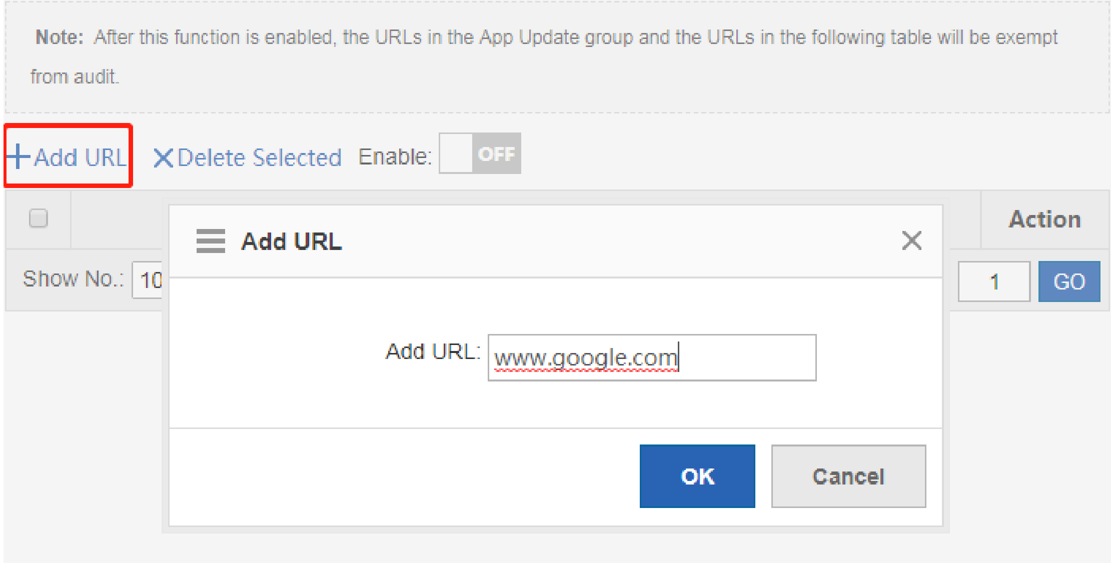
Configuration Steps

Choose Flow > Behavior Policy > Basic Settings, and click Audit-Exempt URL.



Enable Audit: ☑Website ☐HTTPS Audit

Click Add URL to specify a required URL.



Note: After this function is enabled, the URLs in the App Update group and the URLs in the following table will be exempt from audit.

Enable: OFF

Add URL: www.google.com

Configuration Verification

LAN users can access www.google.com successfully and there is no audit record in the behavior audit report. An audit record is generated after you delete www.google.com from audit-exempt websites and access the website again.

5.4.2 Advanced Settings

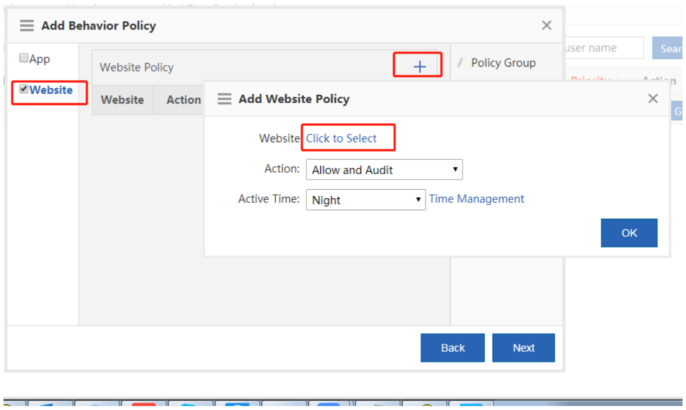
5.4.2.1 Website Access Policy

Networking Requirements

1. The EG device serves as an egress and can access the Internet by using a static IP address. The LAN user gateway is configured on the LAN port of the EG device, to implement the basic Internet access function.
2. The WAN bandwidth is 10 Mbps, the WAN port address is 192.168.33.56/24, the WAN gateway address is 192.168.33.1, and the LAN is in the 192.168.1.0/24 network segment.
3. All LAN users are prohibited from accessing online shopping websites such as www.taobao.com.

Configuration Key Points

1. Choose **Flow** > **Behavior Policy** and click the **Advanced Settings**.
2. Configure a website access policy during policy creation.



Website: Click to Select

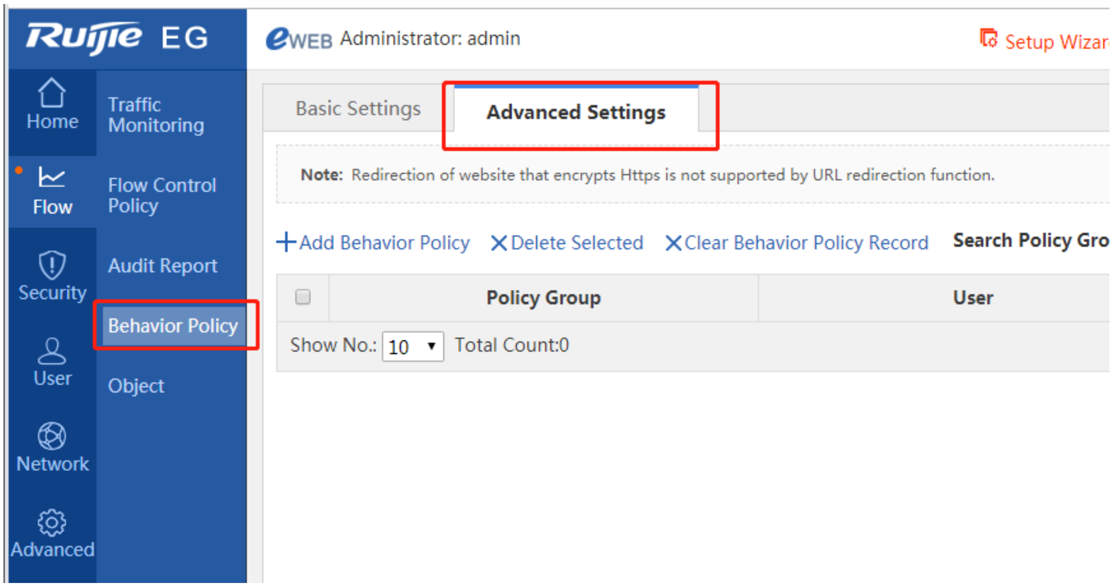
Action: Allow and Audit

Active Time: Night

3. If the policy does not take effect after the configuration is complete, check whether the user objects, application time, and selected applications are correct in policy configuration.

Configuration Steps

1. Choose **Flow** > **Behavior Policy** and click the **Advanced Settings** tab.

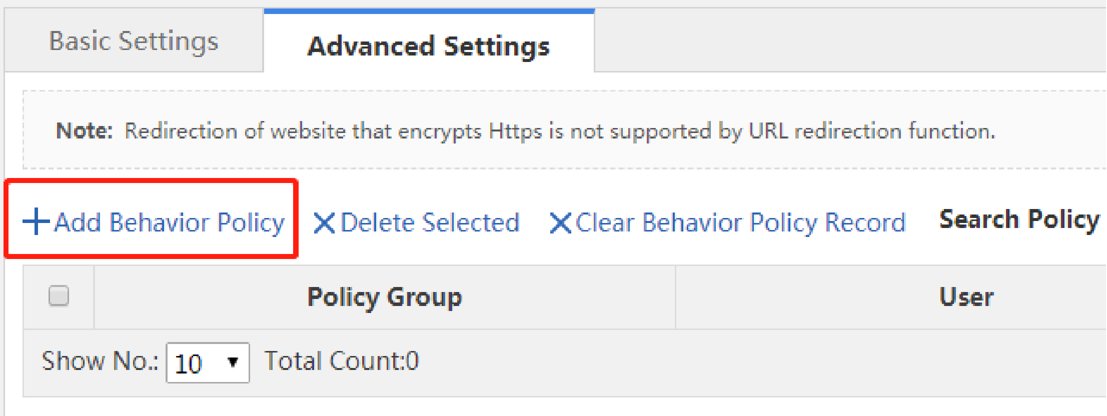


Note: Redirection of website that encrypts Https is not supported by URL redirection function.

□	Policy Group	User

Show No.: 10 ▾ Total Count:0

Click **Add Behavior Policy**.

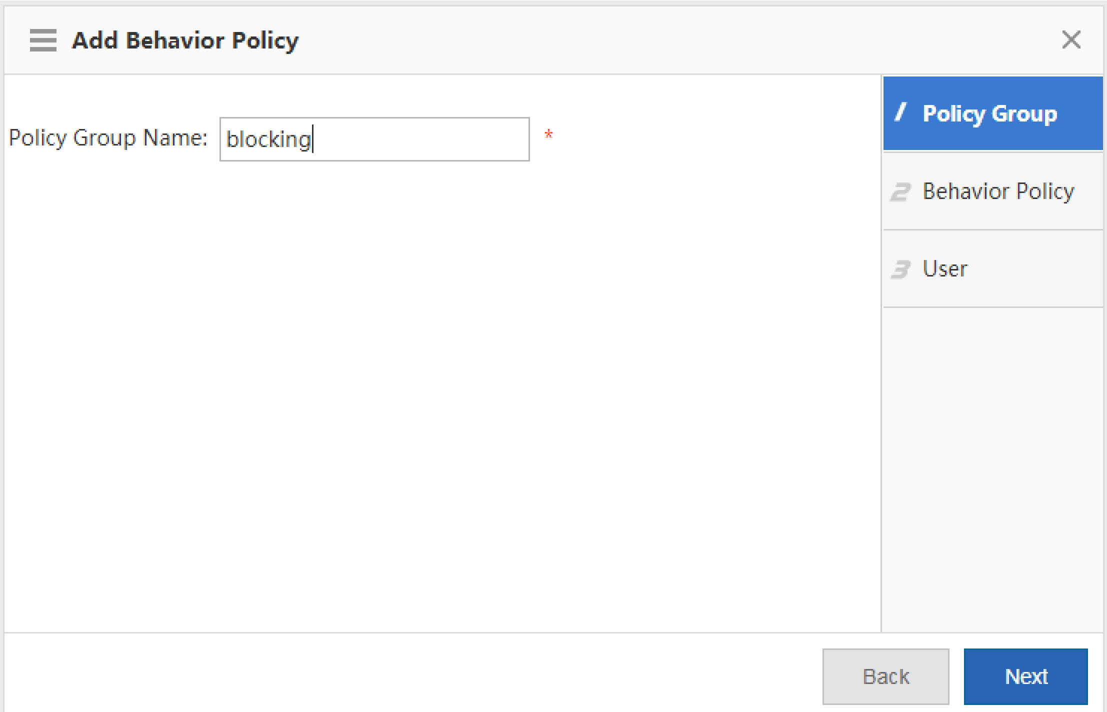


Note: Redirection of website that encrypts Https is not supported by URL redirection function.

□	Policy Group	User

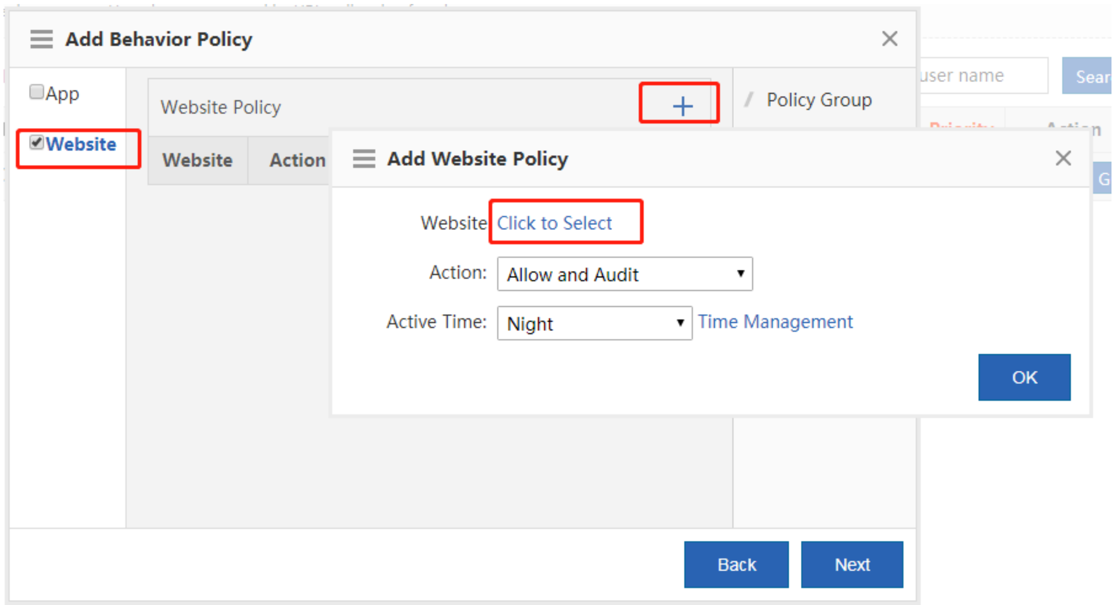
Show No.: 10 ▾ Total Count:0

a. Define the name of a policy.



Policy Group Name: blocking *

b. Configure a behavior control policy.

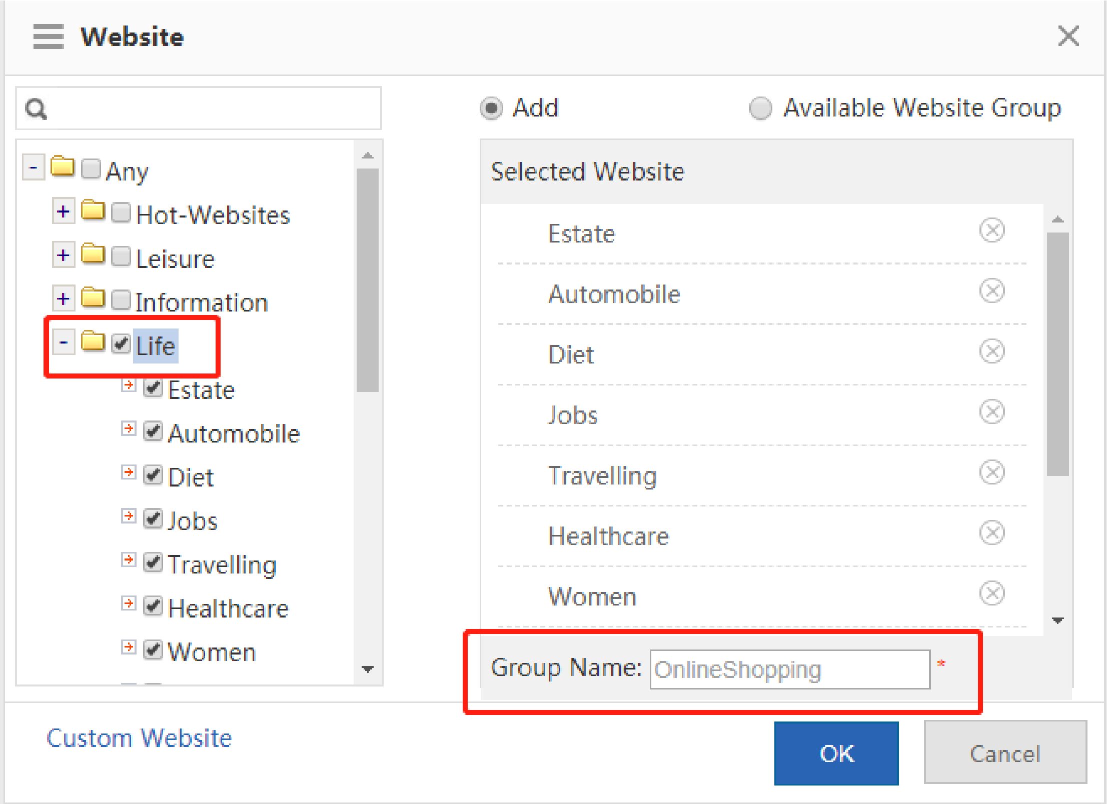


Website Click to Select

Action: Allow and Audit

Active Time: Night

c. Select the URL category: Select the online shopping website defined previously.

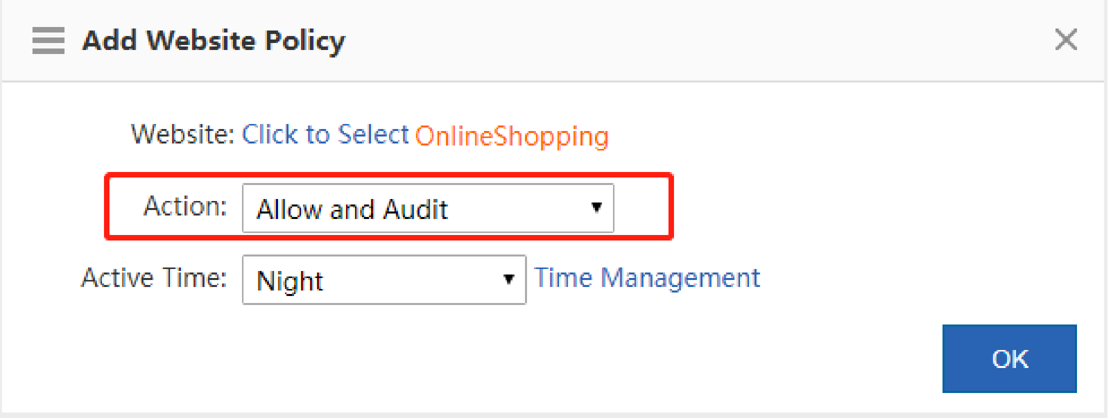


Selected Website

- Estate
- Automobile
- Diet
- Jobs
- Travelling
- Healthcare
- Women

Group Name: OnlineShopping *

d. Select **Deny and Audit** from **Action**.

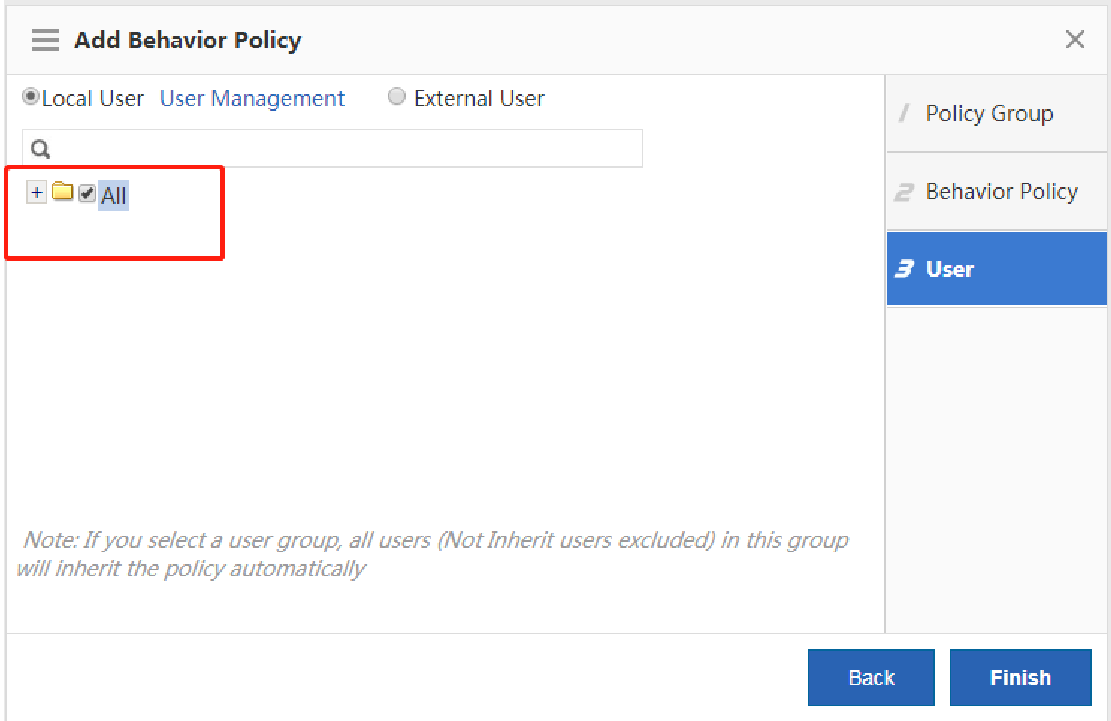


Website: OnlineShopping

Action: Allow and Audit

Active Time: Night

e. Associate users.

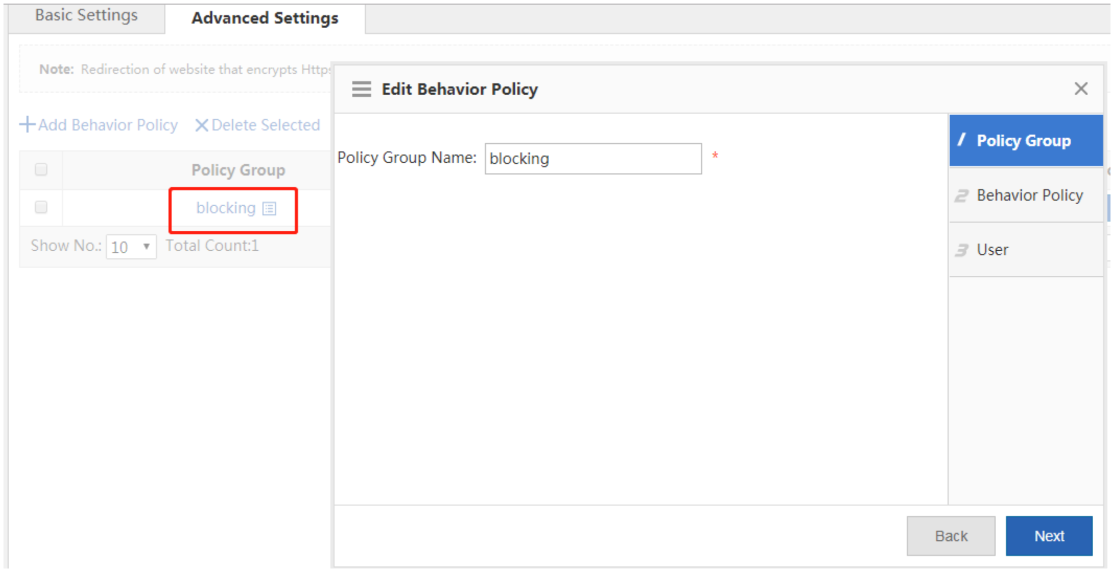


Note: If you select a user group, all users (Not Inherit users excluded) in this group will inherit the policy automatically

Click **Finish** to generate the policy.

Note: In the external authentication server environment, select external server users as user objects.

2. View the configured policy on **Advanced Settings**.



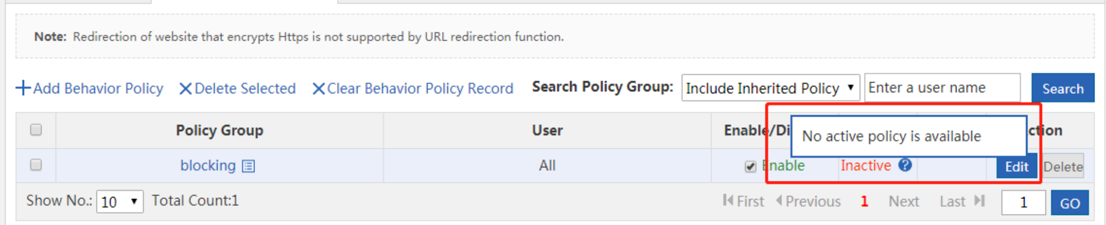
Policy Group Name: blocking *

Note: A policy configured later takes effect prior to a policy configured earlier. Policies are matched from top down.

Configuration Verification

When a user accesses www.taobao.com, a prompt is displayed, indicating that the user is prohibited from accessing this website and needs to contact the website administrator.

If a policy does not take effect, click **?** to view the cause for the failure, as shown in the figure below.



Note: Redirection of website that encrypts Https is not supported by URL redirection function.

No active policy is available

☐	Policy Group	User	Enable/Di	ction
☐	blocking	All	☑ Enable Inactive ?	Edit Delete

Show No.: 10 Total Count:1

5.4.2.2 Audit Record Clearing

Networking Requirements

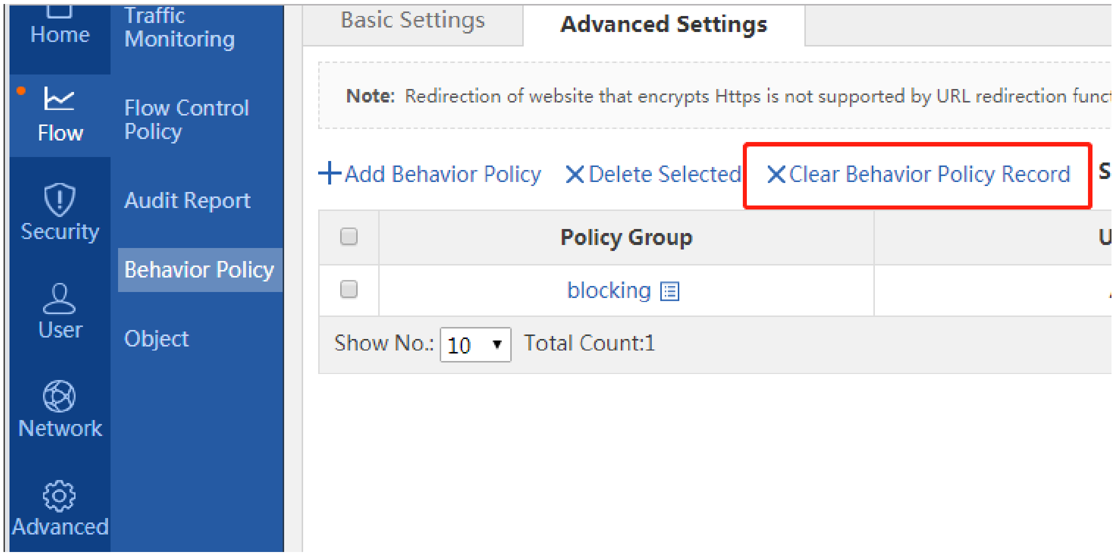
When considerable audit records stored on the hard disk lead to space insufficiency or some audit records need to be forcibly deleted, administrators need to clear the audit records.

Configuration Key Points

After you confirm the cleanup operation, the device needs several to dozens of minutes to clear the audit records, and automatically restarts after the clearing.

Configuration Steps

When you need to clear content audit records on the device, choose Flow > Behavior Policy > Advanced Settings, and click Clear Behavior Policy Record.



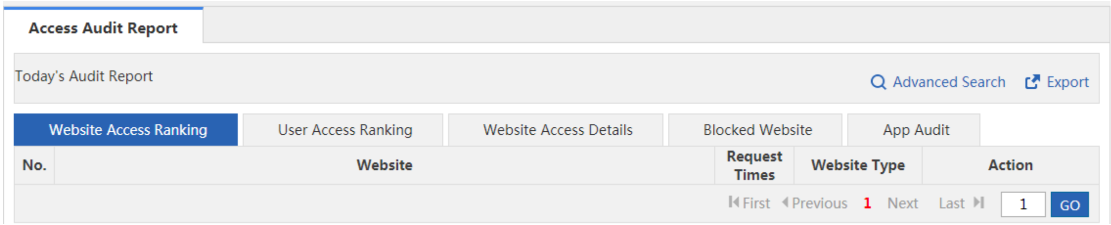
Note: Redirection of website that encrypts Https is not supported by URL redirection funct

☐	Policy Group	U
☐	blocking	

Show No.: 10 Total Count:1

Configuration Verification

Check whether audit records are cleared after device restart.



No.	Website	Request Times	Website Type	Action

5.4.2.3 HTTPS Domain Name Filtering and Audit

Networking Requirements

1. The EG device serves as an egress and can access the Internet by using a static IP address. The LAN user gateway is configured on the LAN port of the EG device, to implement the basic Internet access function.
2. The access of LAN users to HTTPS websites can be audited and blocked.

Note: The EG device of version 11.1(6)B4 and later versions support HTTPS website domain name filtering and audit.

Network Topology

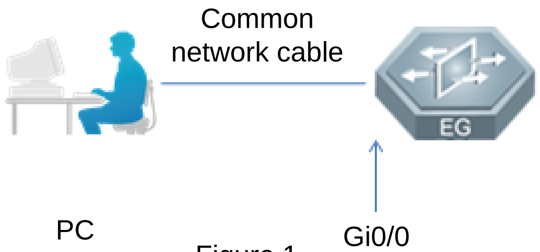


Figure 1

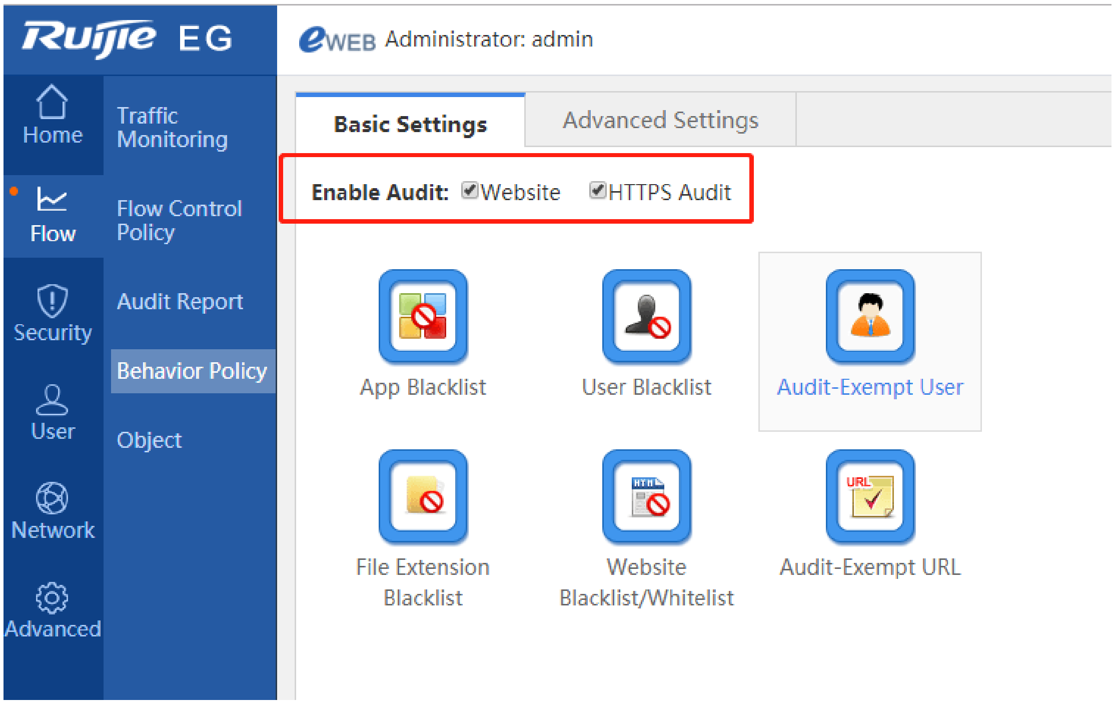
Configuration Key Points

1. On Basic Settings, use the default audit policy to audit the domain names of HTTPS websites.
2. On Basic Settings, select the blacklist mode to block specified websites.
3. On Basic Settings, select the whitelist mode to restrict accessible websites.
4. On Advanced Settings, configure the website blocking/allowing and audit/audit exemption functions.

Configuration steps

Method 1: Enable the HTTPS domain name audit on Basic Settings.

Log in to the Web page of the gateway, choose Flow > Behavior Policy > Basic Settings and select Website and HTTPS Audit in Enable Audit to enable the HTTPS domain name audit.

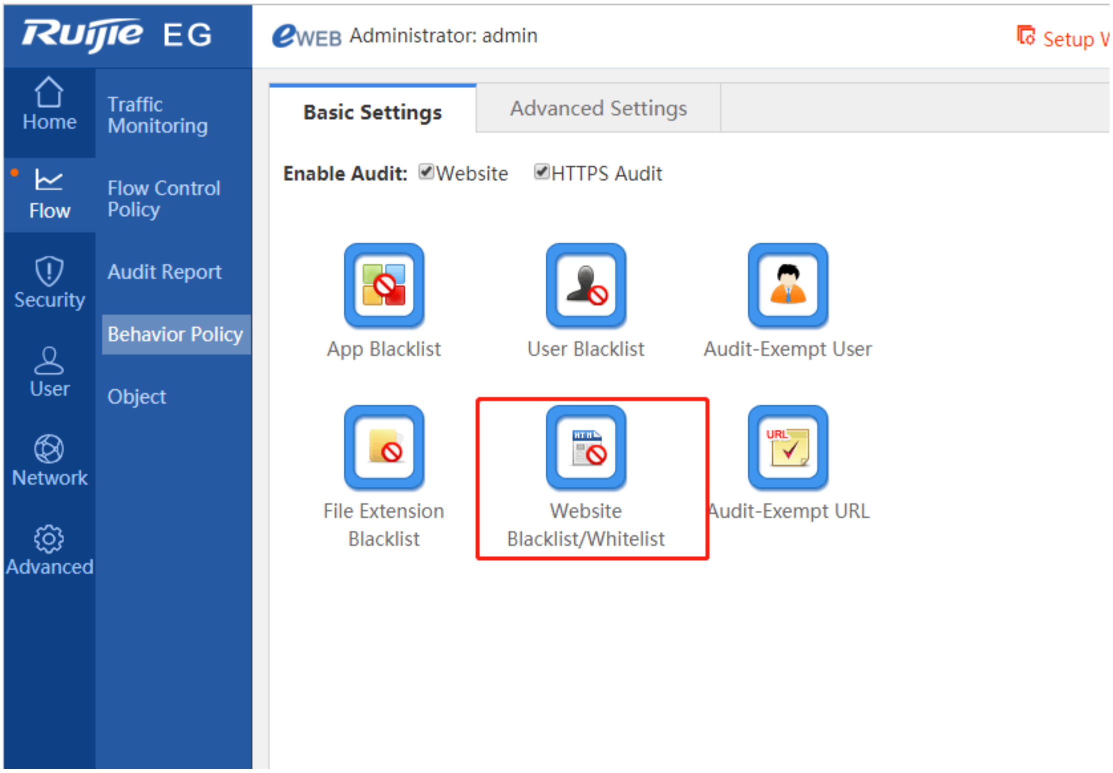


Enable Audit: ☑Website ☑HTTPS Audit

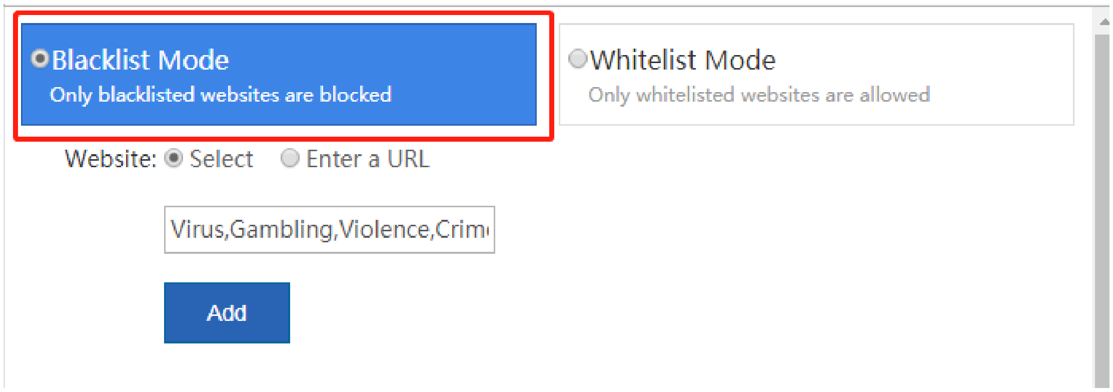
Method 2: Blacklist websites on Basic Settings.

(1) Choose Flow > Behavior Policy > Basic Settings and select HTTPS Audit in Enable Audit to enable the HTTPS website audit.

(2) Choose Flow > Behavior Policy > Basic Settings, click Website Blacklist/Whitelist, and click Blacklist Mode.



Enable Audit: ☑Website ☑HTTPS Audit

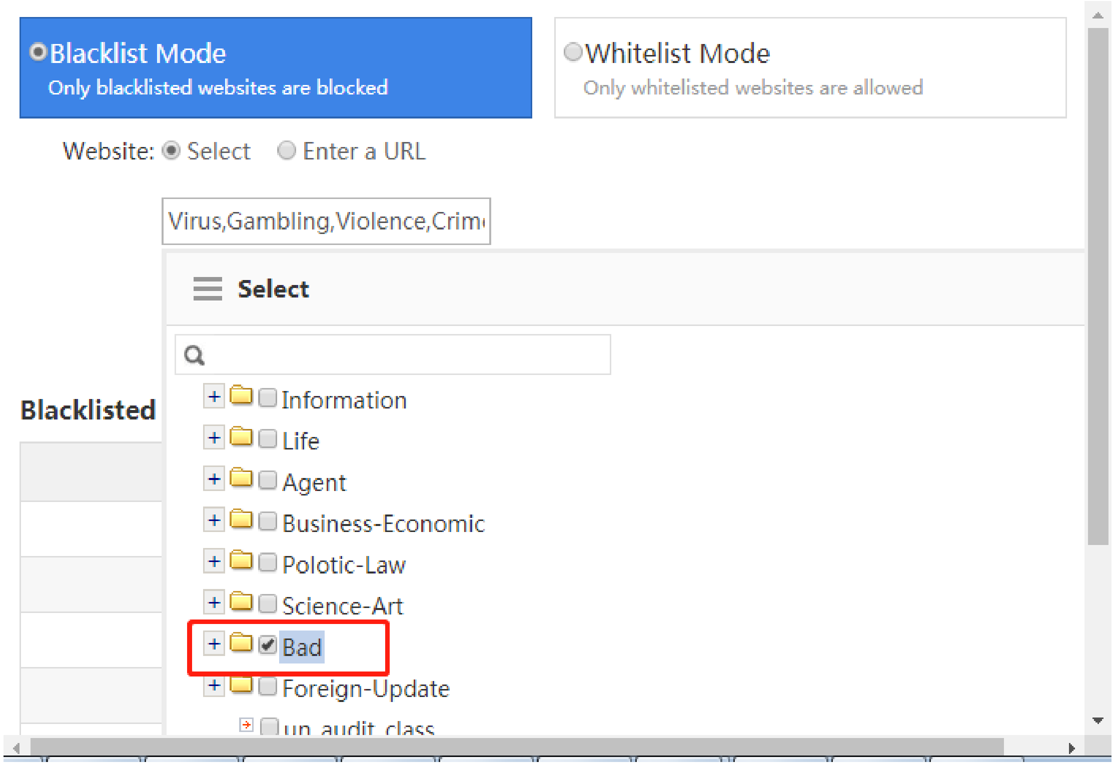

● Blacklist Mode
Only blacklisted websites are blocked

○ Whitelist Mode
Only whitelisted websites are allowed

Website: ● Select ○ Enter a URL

Virus,Gambling,Violence,Crim

(3) Click Select, click the entry box, and select websites to be blocked.



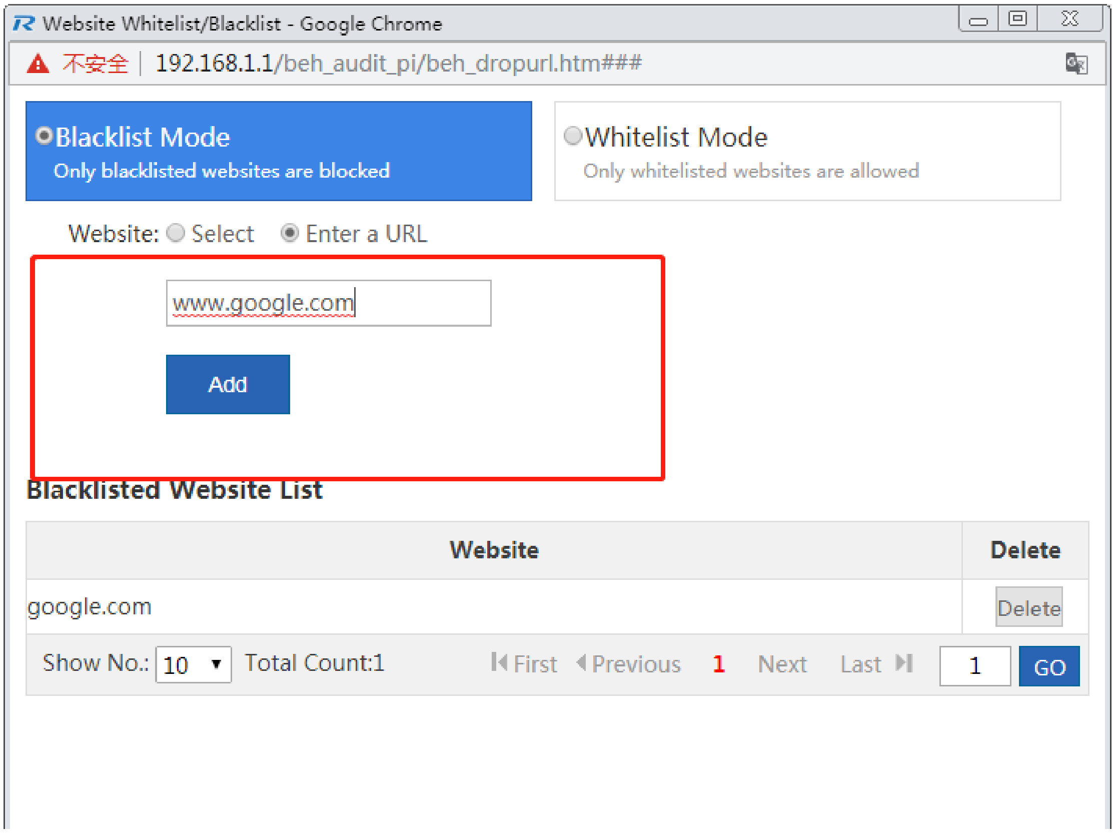
● Blacklist Mode
Only blacklisted websites are blocked

○ Whitelist Mode
Only whitelisted websites are allowed

Website: ● Select ○ Enter a URL

Virus,Gambling,Violence,Crim

(4) Click Enter a URL and enter the website to be blocked in the entry box.



Website Whitelist/Blacklist - Google Chrome

不安全 | 192.168.1.1/beh_audit_pi/beh_dropurl.htm###

● Blacklist Mode
Only blacklisted websites are blocked

○ Whitelist Mode
Only whitelisted websites are allowed

Website: ○ Select ● Enter a URL

www.google.com

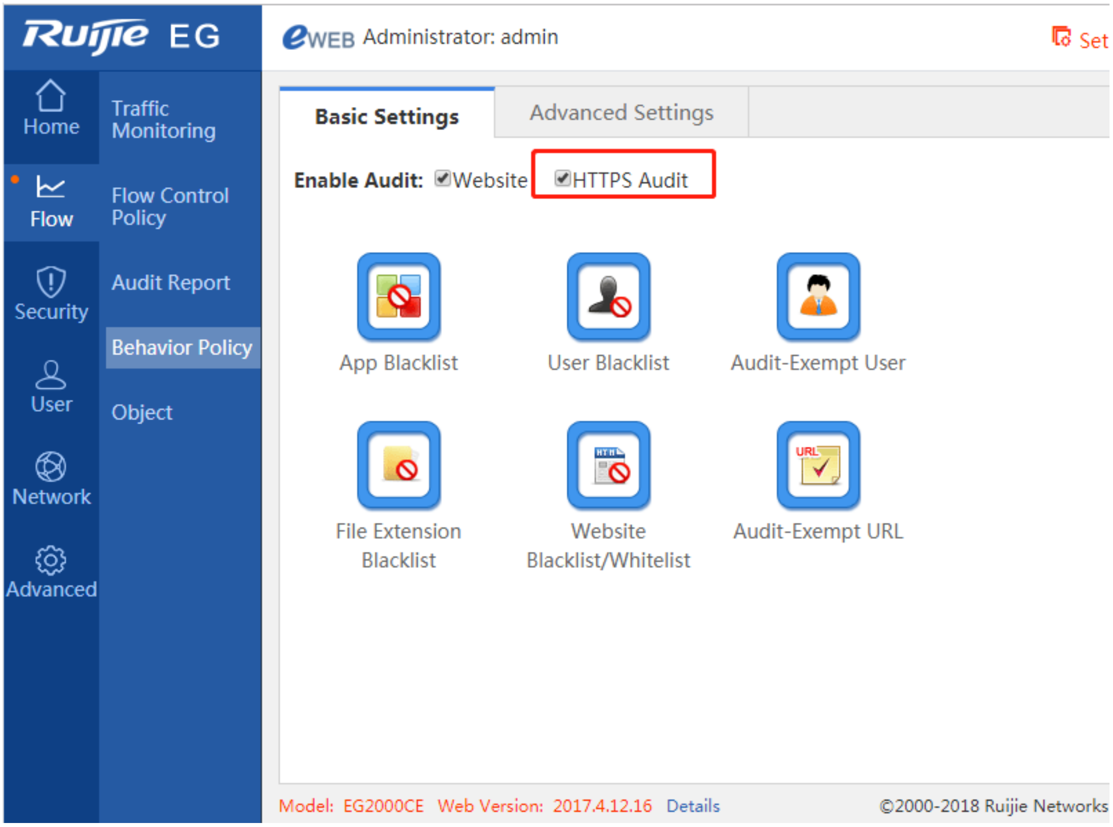
Blacklisted Website List

Website	Delete
google.com	Delete

Show No.: 10 Total Count:1

Method 3: Whitelist websites on Basic Settings.

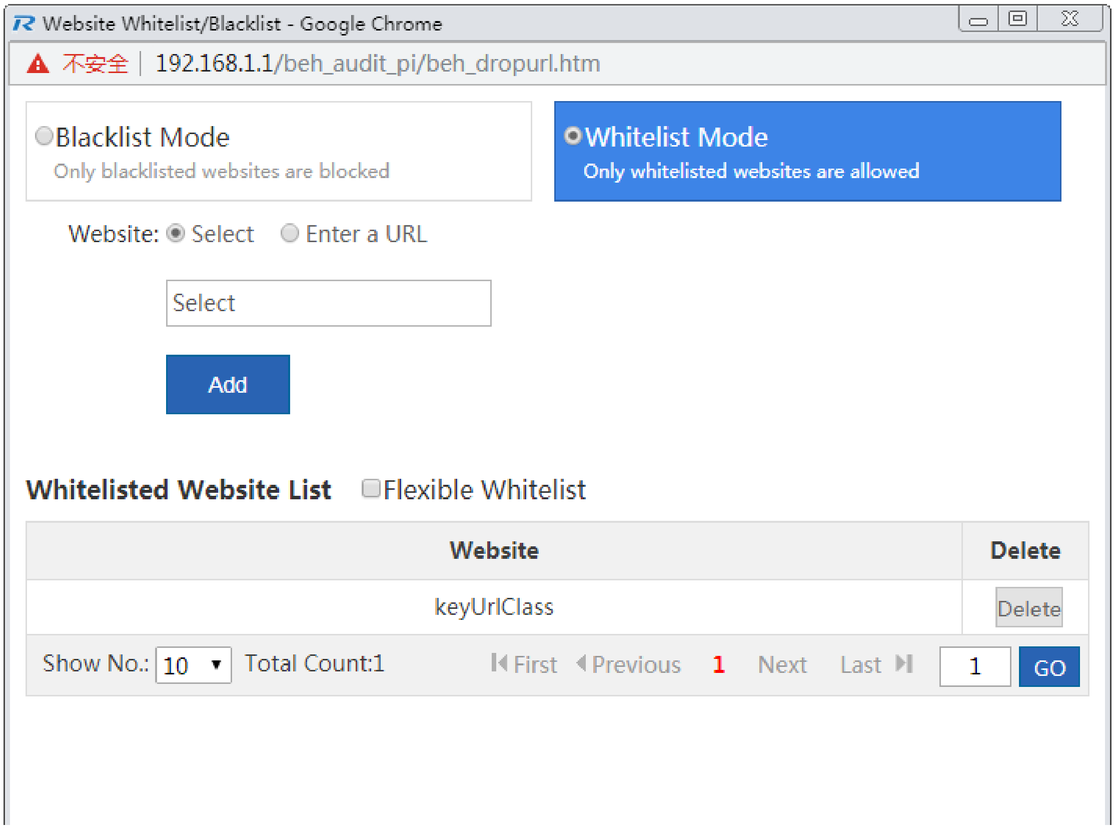
(1) Choose Flow > Behavior Policy > Basic Settings and select HTTPS Audit in Enable Audit to enable the HTTPS website audit.



Enable Audit: ☑Website ☑HTTPS Audit

Model: EG2000CE Web Version: 2017.4.12.16 Details ©2000-2018 Ruijie Networks

(2) Choose Flow > Behavior Policy > Basic Settings, click Website Blacklist/Whitelist and click Whitelist Mode.


Website Whitelist/Blacklist - Google Chrome
不安全 | 192.168.1.1/beh_audit_pi/beh_dropurl.htm
Add
First
Previous
Next
Last
GO

○ Blacklist Mode
Only blacklisted websites are blocked

● Whitelist Mode
Only whitelisted websites are allowed

Website: ● Select ○ Enter a URL

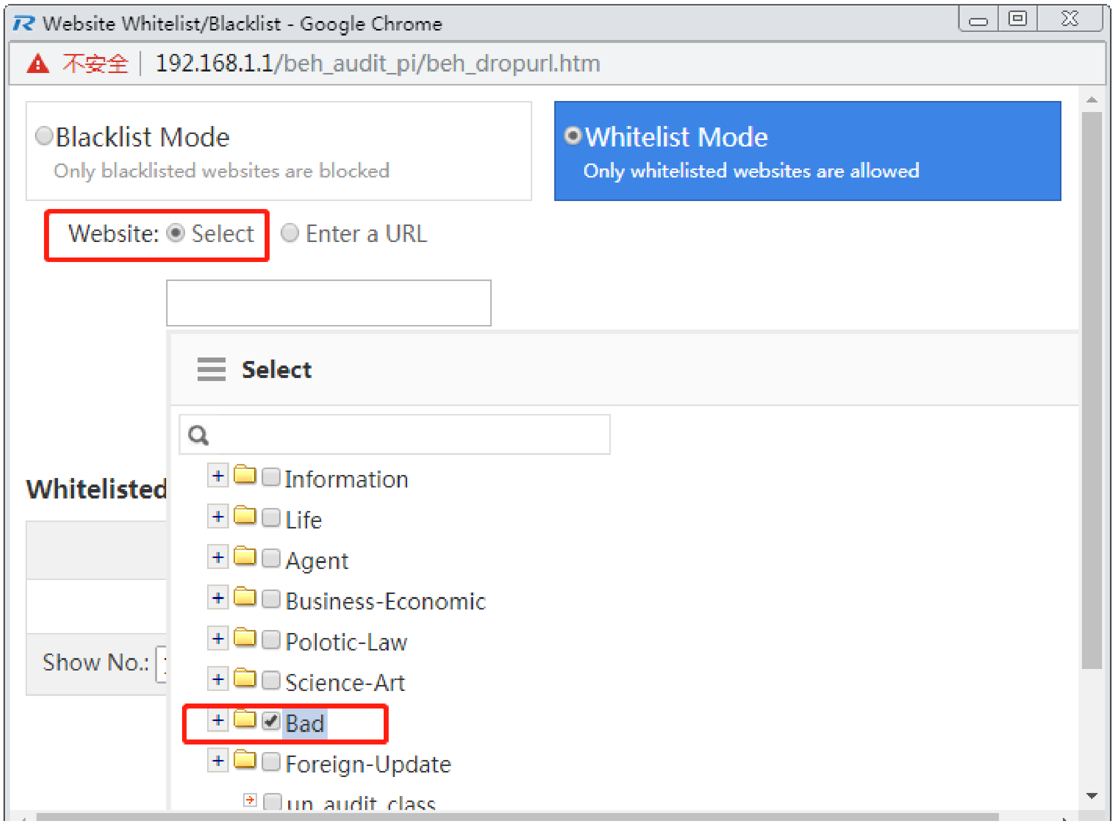
Select

Whitelisted Website List □ Flexible Whitelist

Website	Delete
keyUrlClass	Delete

Show No.: 10 Total Count:1 1 1

(3) Click Select, click the entry box, and select websites that are allowed.


Website Whitelist/Blacklist - Google Chrome
不安全 | 192.168.1.1/beh_audit_pi/beh_dropurl.htm
Whitelisted
Show No.:

○ Blacklist Mode
Only blacklisted websites are blocked

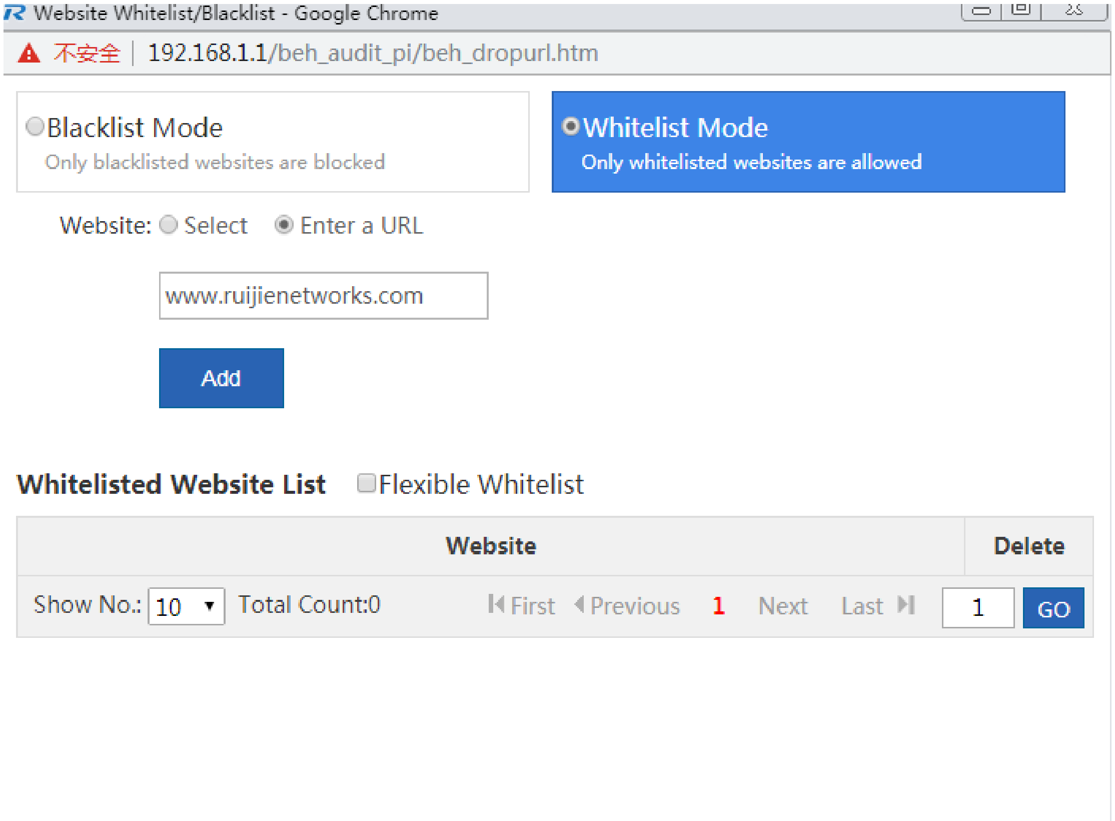
● Whitelist Mode
Only whitelisted websites are allowed

Website: ● Select ○ Enter a URL

Select

- + □ Information
- + □ Life
- + □ Agent
- + □ Business-Economic
- + □ Polotic-Law
- + □ Science-Art
- + ☑ Bad
- + □ Foreign-Update
- □ un_audit_class

(4) Click Enter a URL and enter an allowed website in the entry box.


Website Whitelist/Blacklist - Google Chrome
不安全 | 192.168.1.1/beh_audit_pi/beh_dropurl.htm

○ Blacklist Mode
Only blacklisted websites are blocked

● Whitelist Mode
Only whitelisted websites are allowed

Website: ○ Select ● Enter a URL

www.ruijienetworks.com

Add

Whitelisted Website List □ Flexible Whitelist

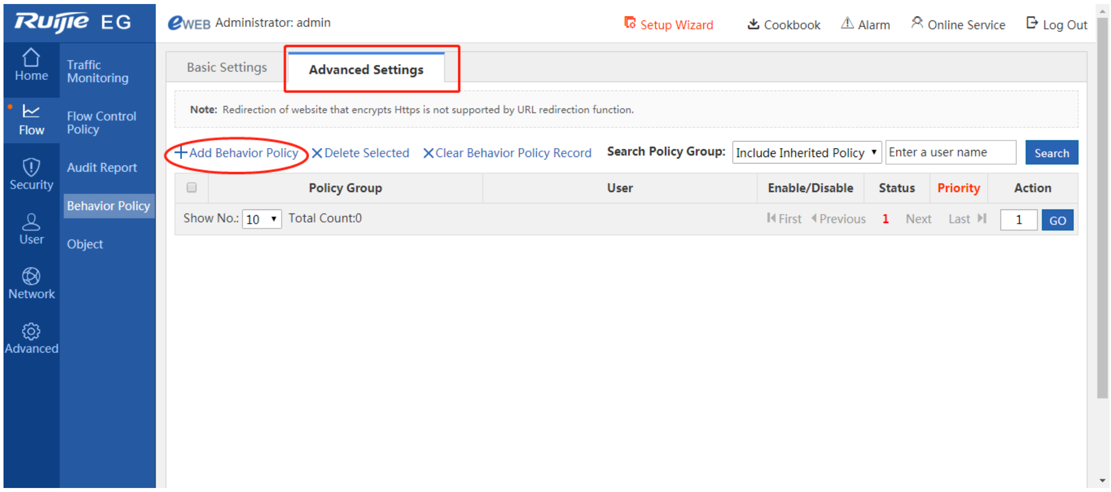
Website	Delete

Show No.: 10 ▾ Total Count:0 First Previous 1 Next Last 1 GO

Method 4: Configure the HTTPS website blocking/allowing and audit/audit exemption functions on Advanced Settings.

(1) Choose Flow > Behavior Policy > Basic Settings and select HTTPS Audit in Enable Audit to enable the HTTPS website audit.

(2) Choose Flow > Behavior Policy > Advanced Settings and click Add Behavior Policy to create a behavior policy. Alternatively, click an existing behavior policy in the list for modification.



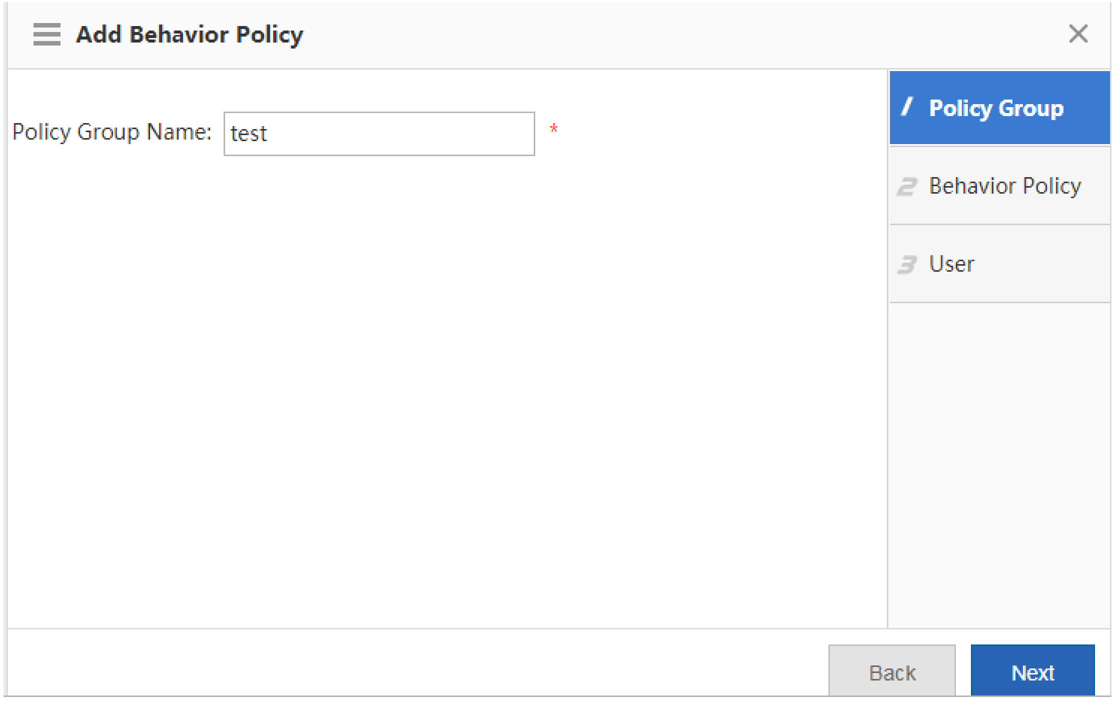
Note: Redirection of website that encrypts Https is not supported by URL redirection function.

+Add Behavior Policy ✕Delete Selected ✕Clear Behavior Policy Record **Search Policy Group:** Include Inherited Policy ▾ Enter a user name Search

□	Policy Group	User	Enable/Disable	Status	Priority	Action

Show No.: 10 ▾ Total Count:0 First Previous 1 Next Last 1 GO

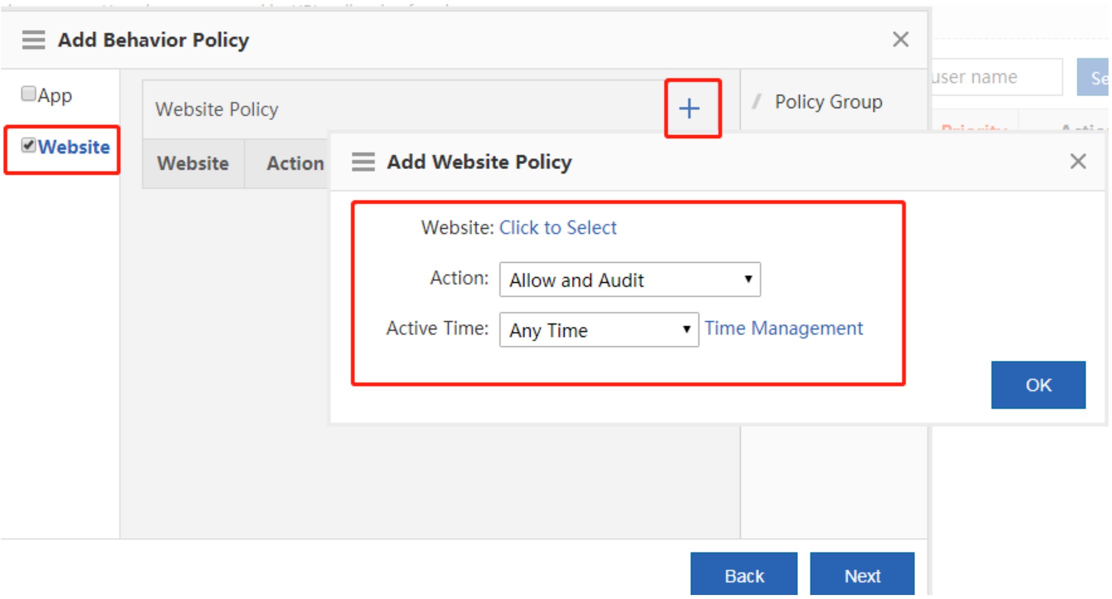
(3) Click Policy Group to set the name of a policy group.



Add Behavior Policy

Policy Group Name: test *

(4) Click Behavior Policy to add a behavior control policy.



Add Behavior Policy

☐ App

☑ Website

Website Policy

Website	Action

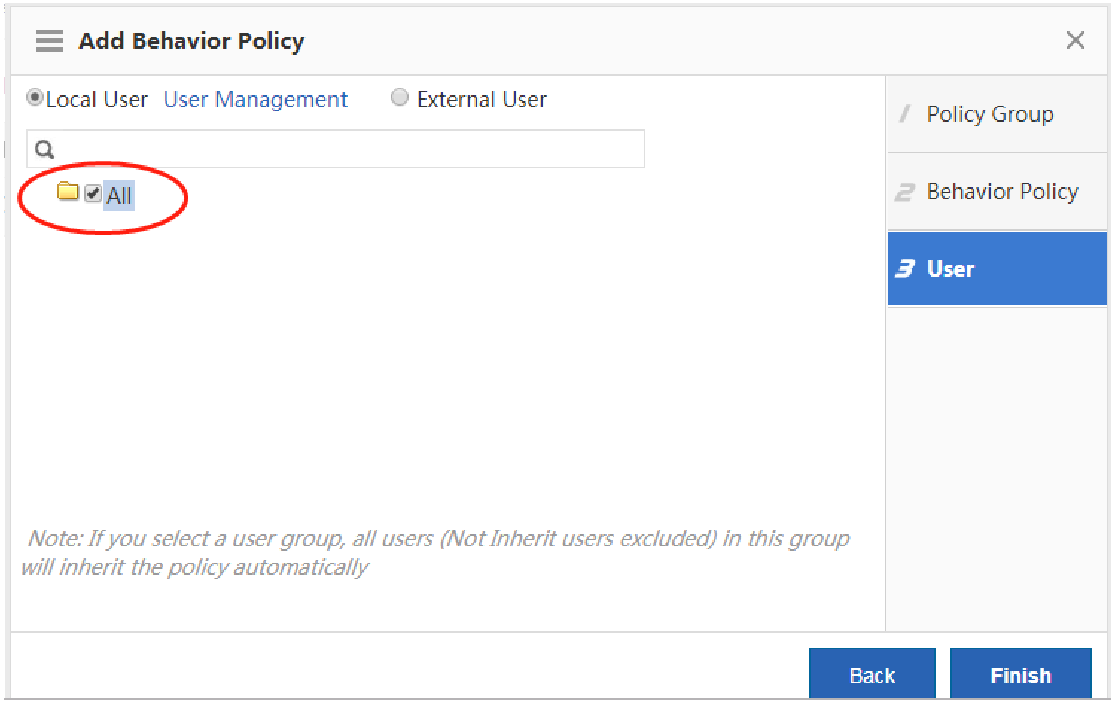
Add Website Policy

Website: Click to Select

Action: Allow and Audit

Active Time: Any Time

(5) Click User to apply the policy group to users or a user group.



Note: If you select a user group, all users (Not Inherit users excluded) in this group will inherit the policy automatically

Configuration Verification

1. Test procedure:

(1) Bind a static IP address to the test PC or enable the test PC to succeed in real-time authentication for Internet access.

(2) Use the test PC to access a specified website from a browser.

(3) Choose Flow > Audit Report > Access Audit Report > Website Access Details on the EG device to view audit content.

2. Test results:

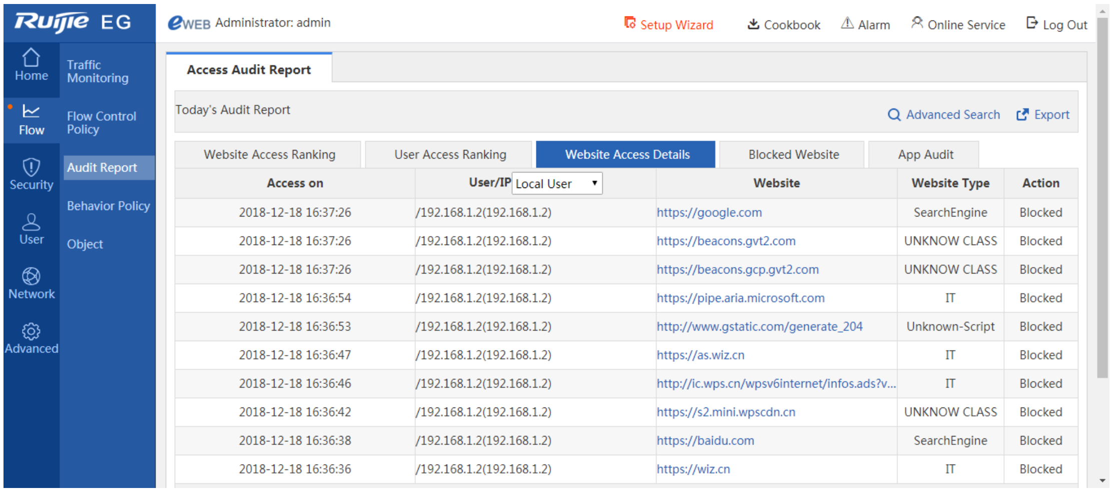
(1) After HTTPS domain name audit is enabled on Basic Settings, the domain names of HTTPS websites accessed by the user are all audited.

(2) HTTPS websites configured in blacklist mode on Basic Settings cannot be accessed.

(3) Only HTTPS websites configured in whitelist mode on Basic Settings can be accessed.

(4) HTTPS websites blocked on Advanced Settings cannot be accessed.

(5) The behavior audit report displays the access records.

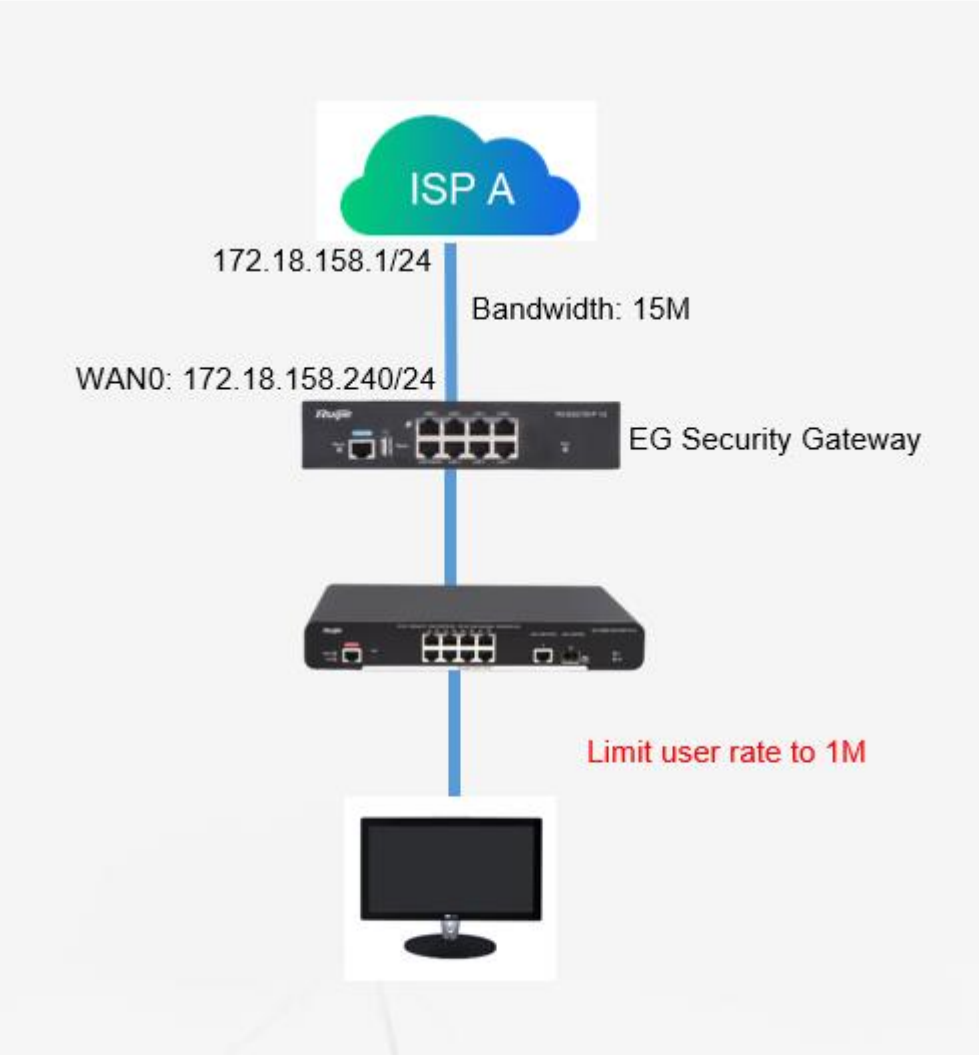


Access on	User/IP Local User	Website	Website Type	Action
2018-12-18 16:37:26	/192.168.1.2(192.168.1.2)	https://google.com	SearchEngine	Blocked
2018-12-18 16:37:26	/192.168.1.2(192.168.1.2)	https://beacons.gvt2.com	UNKNOW CLASS	Blocked
2018-12-18 16:37:26	/192.168.1.2(192.168.1.2)	https://beacons.gcp.gvt2.com	UNKNOW CLASS	Blocked
2018-12-18 16:36:54	/192.168.1.2(192.168.1.2)	https://pipe.aria.microsoft.com	IT	Blocked
2018-12-18 16:36:53	/192.168.1.2(192.168.1.2)	http://www.gstatic.com/generate_204	Unknown-Script	Blocked
2018-12-18 16:36:47	/192.168.1.2(192.168.1.2)	https://as.wiz.cn	IT	Blocked
2018-12-18 16:36:46	/192.168.1.2(192.168.1.2)	http://ic.wps.cn/wpsv6internet/infos.ads?v...	IT	Blocked
2018-12-18 16:36:42	/192.168.1.2(192.168.1.2)	https://s2.mini.wpscdn.cn	UNKNOW CLASS	Blocked
2018-12-18 16:36:38	/192.168.1.2(192.168.1.2)	https://baidu.com	SearchEngine	Blocked
2018-12-18 16:36:36	/192.168.1.2(192.168.1.2)	https://wiz.cn	IT	Blocked

5.5 Rate Limit

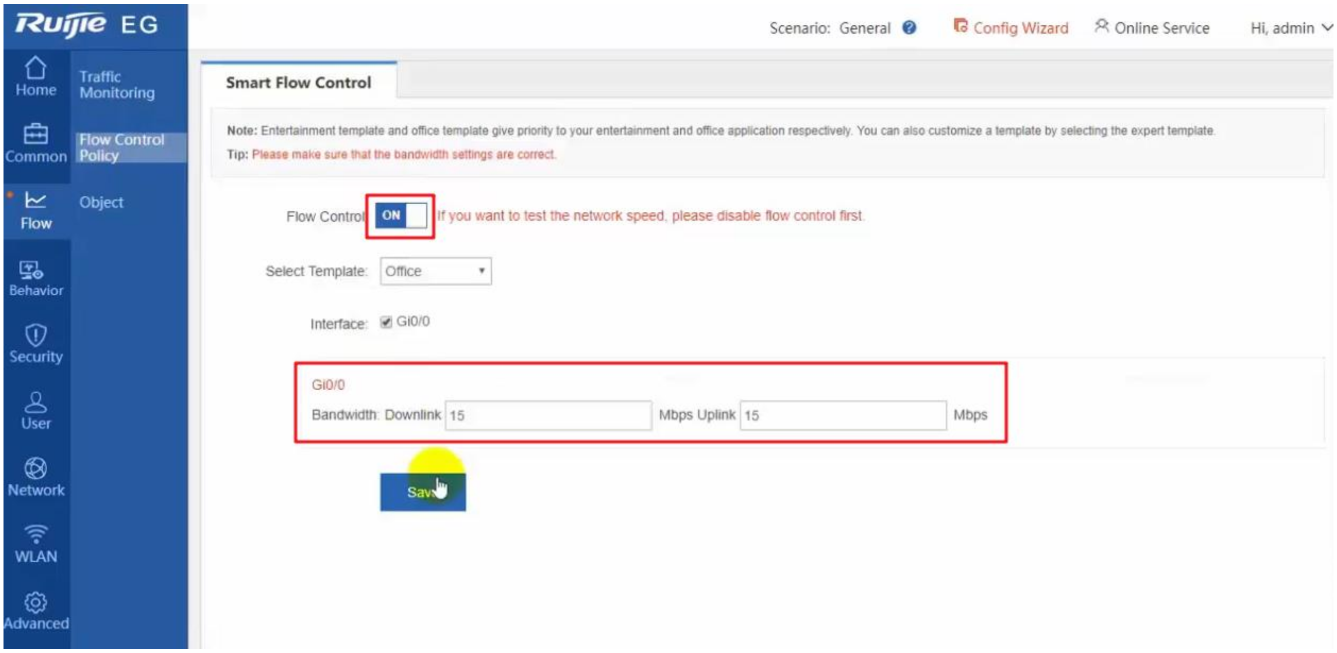
Rate limit is used to control the rate of traffic sent or received by a network interface controller.

Network Topology



Configuration Steps

Step 1：Enable Flow Control



Note: Entertainment template and office template give priority to your entertainment and office application respectively. You can also customize a template by selecting the expert template.

Tip: Please make sure that the bandwidth settings are correct.

Flow Control: ON — If you want to test the network speed, please disable flow control first.

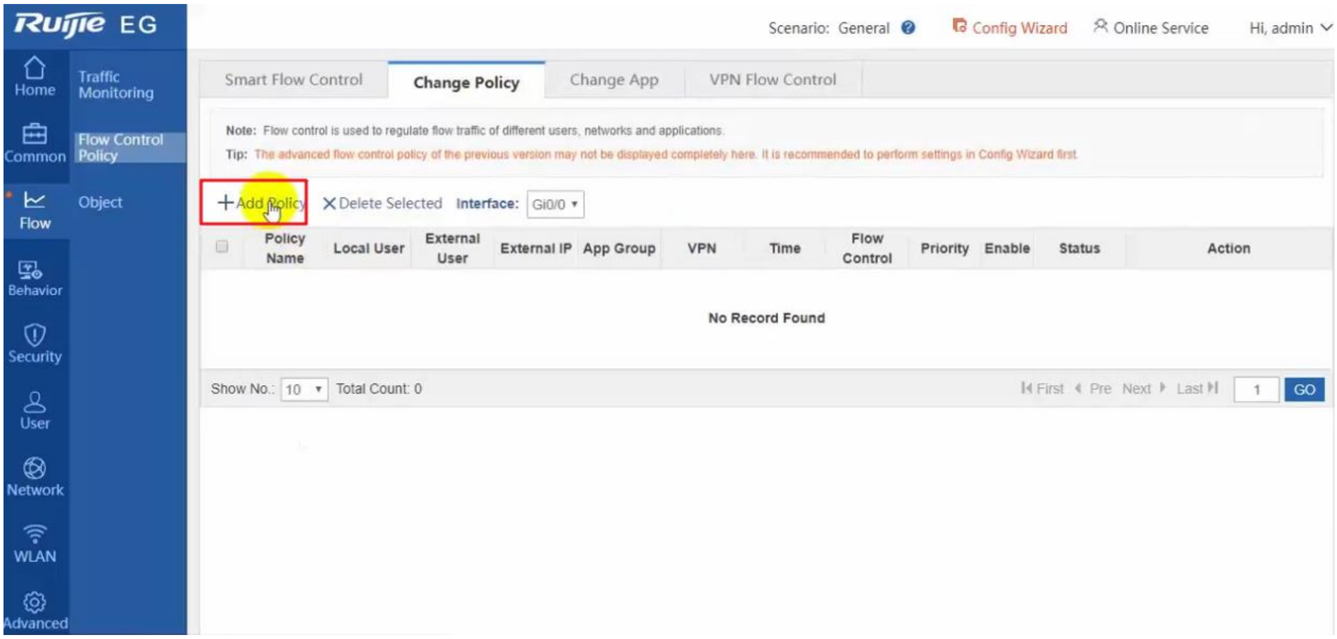
Select Template: Office

Interface: ☑ Gi0/0

Gi0/0

Bandwidth: Downlink 15 Mbps Uplink 15 Mbps

Step 2: Add a flow control policy:

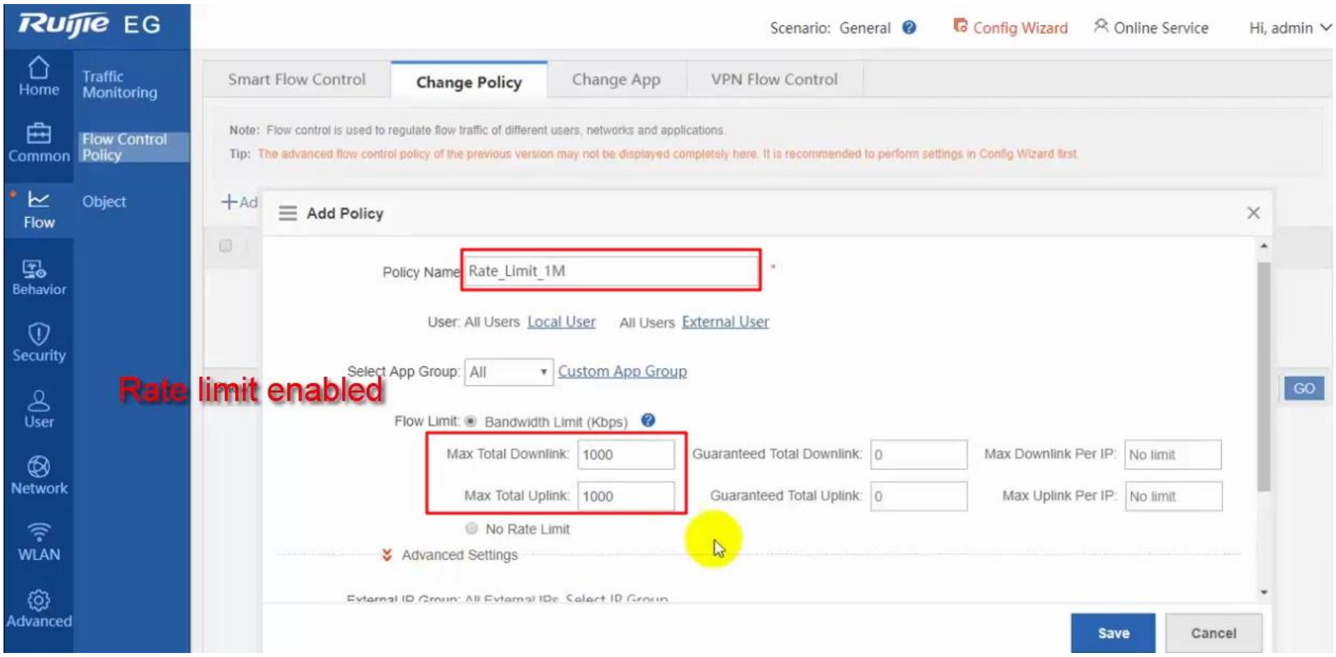


Note: Flow control is used to regulate flow traffic of different users, networks and applications.

Tip: The advanced flow control policy of the previous version may not be displayed completely here. It is recommended to perform settings in Config Wizard first.

□	Policy Name	Local User	External User	External IP	App Group	VPN	Time	Flow Control	Priority	Enable	Status	Action
No Record Found												

Show No.: 10 Total Count: 0



Note: Flow control is used to regulate flow traffic of different users, networks and applications.

Tip: The advanced flow control policy of the previous version may not be displayed completely here. It is recommended to perform settings in Config Wizard first.

Add Policy

Policy Name: Rate_Limit_1M *

User: All Users Local User   All Users External User

Select App Group: All Custom App Group

Flow Limit: ● Bandwidth Limit (Kbps)

Max Total Downlink: 1000   Guaranteed Total Downlink: 0   Max Downlink Per IP: No limit

Max Total Uplink: 1000   Guaranteed Total Uplink: 0   Max Uplink Per IP: No limit

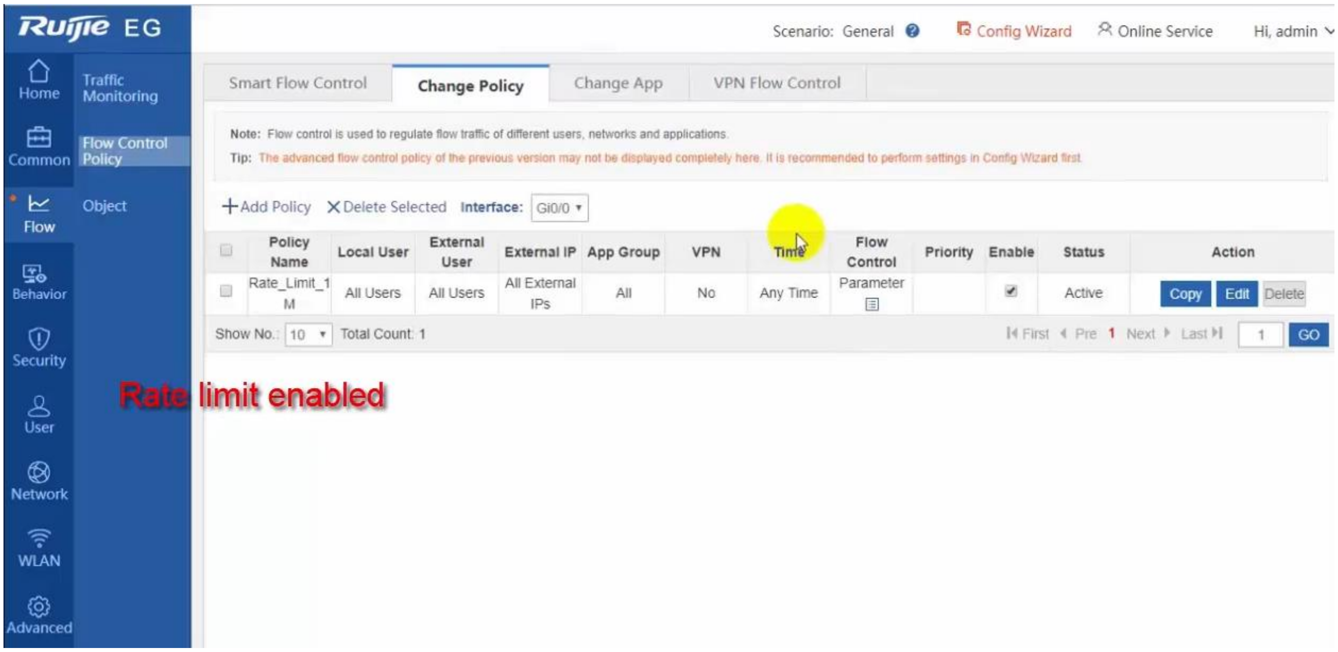
○ No Rate Limit

Advanced Settings

External IP Group: All External IPs Select IP Group

Save   Cancel

Rate limit enabled



Note: Flow control is used to regulate flow traffic of different users, networks and applications.

Tip: The advanced flow control policy of the previous version may not be displayed completely here. It is recommended to perform settings in Config Wizard first.

+Add Policy   ✕Delete Selected   Interface: Gi0/0

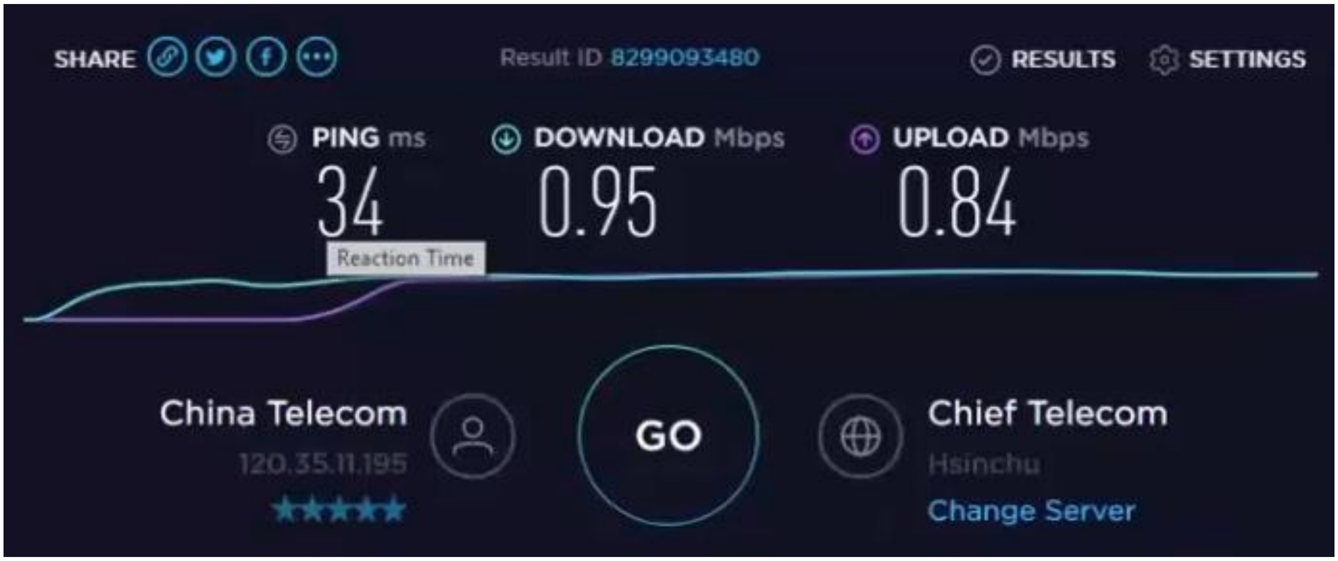
□	Policy Name	Local User	External User	External IP	App Group	VPN	Time	Flow Control	Priority	Enable	Status	Action
□	Rate_Limit_1M	All Users	All Users	All External IPs	All	No	Any Time	Parameter		☑	Active	Copy Edit Delete

Show No.: 10   Total Count: 1   First Pre 1 Next Last 1 GO

Rate limit enabled

Configuration Verification

Use Speed test tool to verify the rate limit setting:



5.6 Port Mapping

Application Scenario

A customer deploys a server on the LAN and enables the HTTP or other services. The server address is a private address. WAN users can neither access this address directly nor use services provided by the server. In this case, you can enable the port mapping function to allow WAN users to access the LAN server.

For example, the server address is 192.168.1.20 and HTTP is enabled. As the server address is a private address, WAN users cannot directly access the HTTP service provided by the server. In this case, you can map the server address and server ports to a public network address on the EG device so that WAN users can access the HTTP service provided by the server.

Networking Requirements

1. The WAN line is a single 10 Mbps fixed fiber line of China Telecom. The address is 192.168.33.56, subnet mask is 255.255.255.0, WAN gateway is 192.168.33.1, and DNS address is 218.85.157.99.
2. There is a remote desktop server on the LAN. The IP address of the server is 192.168.1.150. If the LAN server needs to be accessed from the WAN, port mapping is required to map the interfaces of the LAN server to the public network.

Network Topology

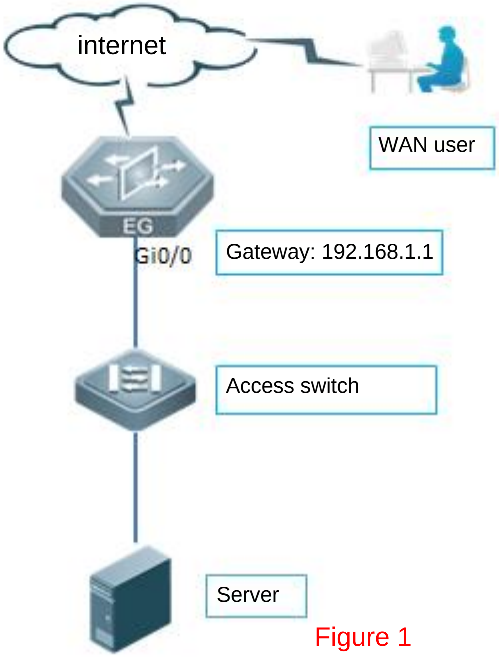


Figure 1

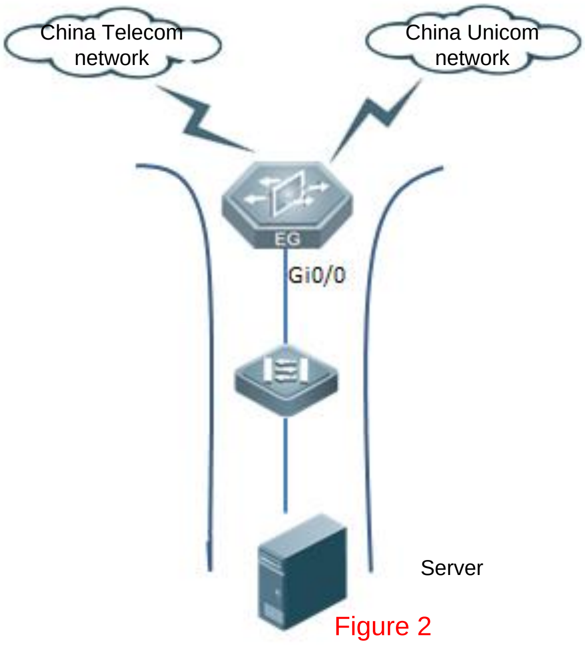


Figure 2

Configuration Key Points

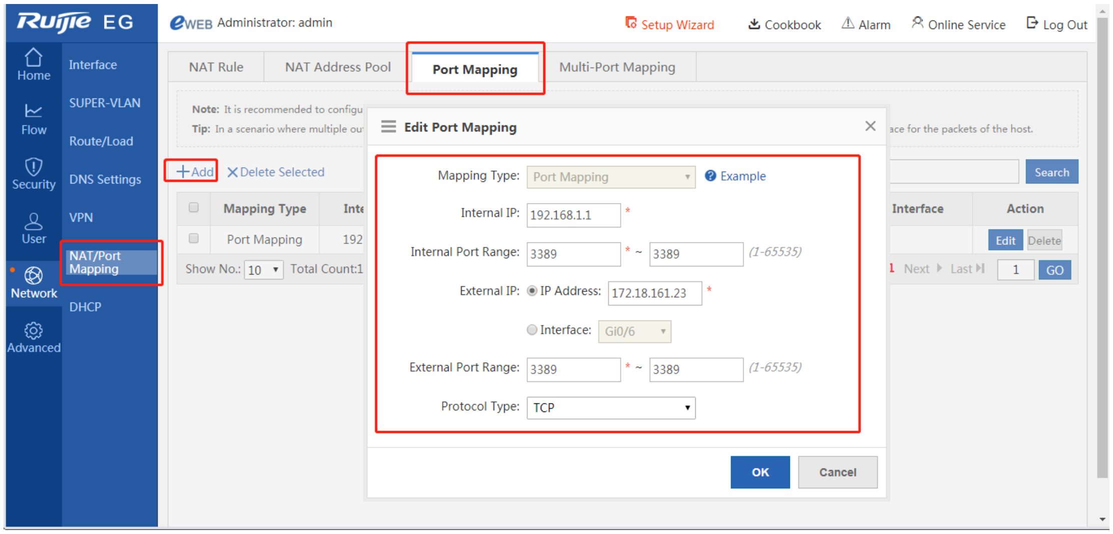
1. Ensure that LAN terminals can access the server normally.
2. The server IP address and gateway are configured, and the server can access the Internet normally.
3. Determine the ports to be mapped on the server, and whether UDP or TCP is required.

4. If there are multiple WAN egresses in the real network environment of a customer (see the topology in Figure 2 above), for example, lines of China Telecom + China Netcom or China Telecom lines, dual-line port mapping needs to be configured on the LAN server. Then, WAN users of different carriers can access the server through their WAN line IP addresses. It is recommended to enable the RPL function on the WAN interfaces.

Configuration Steps

1. Determine that only TCP port 3389 of the server needs to be mapped.

Choose **Network** > **NAT/Port Mapping** > **Port Mapping**.



Mapping Type: Port Mapping

Internal IP: 192.168.1.1 *

Internal Port Range: 3389 * ~ 3389 (1-65535)

External IP: ● IP Address: 172.18.161.23 *

○ Interface: Gi0/6

External Port Range: 3389 * ~ 3389 (1-65535)

Protocol Type: TCP

a. **Mapping Type**: Select **Port Mapping** from the drop-down list, indicating that a port of the LAN server needs to be mapped.

b. **Internal IP**: Indicates the IP address of the server.

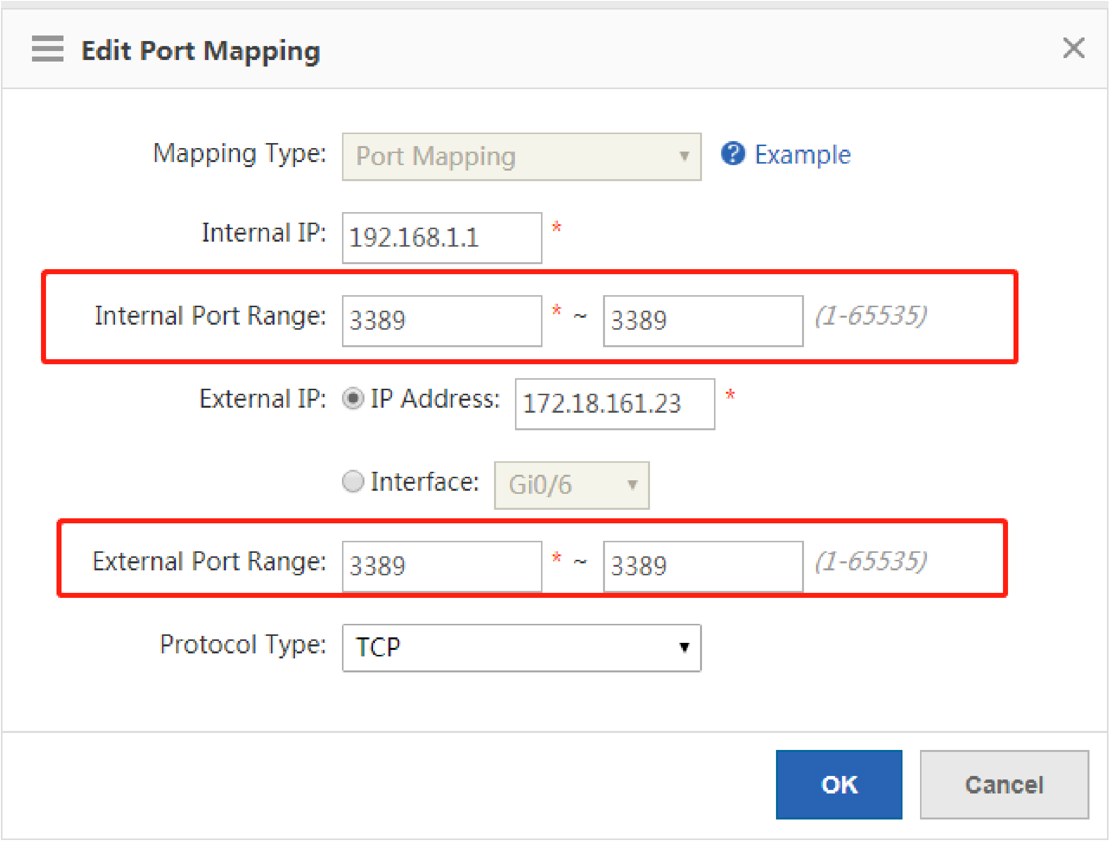
c. **Internal Port Range**: Indicates the port for the server that is to provide external services.

d. **External IP**: Indicates the IP address of a WAN port (**IP Address** is selected when a WAN line is used in a dynamic environment).

e. **External Port Range**: Indicates the target WAN service port of port mapping.

f. **Protocol Type**: Indicates the protocol used by the server to provide services.

Note: EG_RGOS 11.1(6)B9 and later versions support adding continuous ports in batches. See the figure below.



Edit Port Mapping

Mapping Type: Port Mapping

Internal IP: 192.168.1.1 *

Internal Port Range: 3389 * ~ 3389 (1-65535)

External IP: ● IP Address: 172.18.161.23 *

○ Interface: Gi0/6

External Port Range: 3389 * ~ 3389 (1-65535)

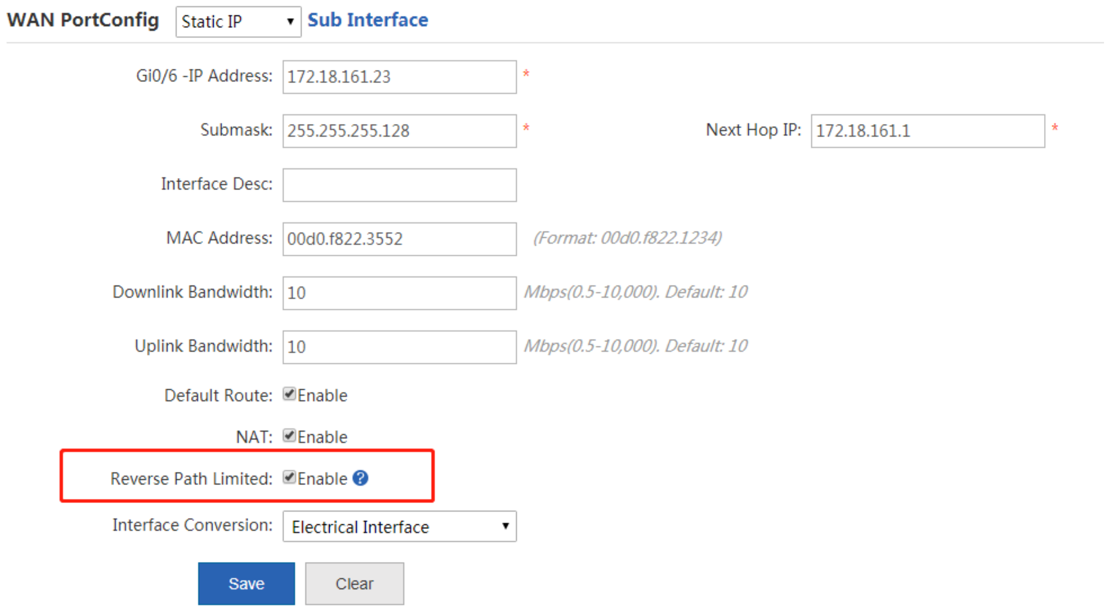
Protocol Type: TCP

2. Command generated on the CLI:

```
ip nat inside source static tcp 192.168.1.150 3389 192.168.33.56 3389 permit-inside
```

3. For multi-egress network environments of customers, it is recommended to enable the RPL function on the WAN interface.

Select **Reverse Path Limited**.



WAN PortConfig: Static IP — Sub Interface

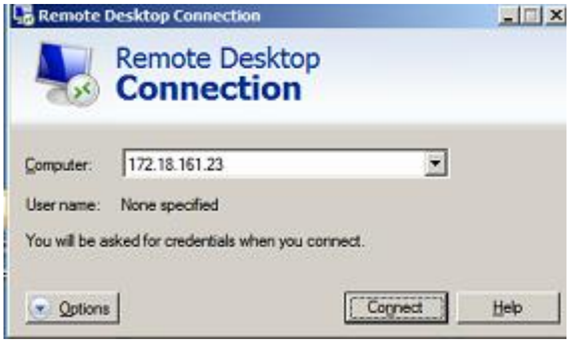
Gi0/6 -IP Address:	172.18.161.23 *
Submask:	255.255.255.128 *
Next Hop IP:	172.18.161.1 *
Interface Desc:	
MAC Address:	00d0.f822.3552 *(Format: 00d0.f822.1234)*
Downlink Bandwidth:	10 *Mbps(0.5-10,000). Default: 10*
Uplink Bandwidth:	10 *Mbps(0.5-10,000). Default: 10*
Default Route:	☑Enable
NAT:	☑Enable
Reverse Path Limited:	☑Enable
Interface Conversion:	Electrical Interface

Commands generated on the CLI:

```
interface GigabitEthernet 0/1

ip nat outside

ip address 192.168.33.57 255.255.255.0

reverse-path-----RPL

nexthop 192.168.33.1
```

Configuration Verification

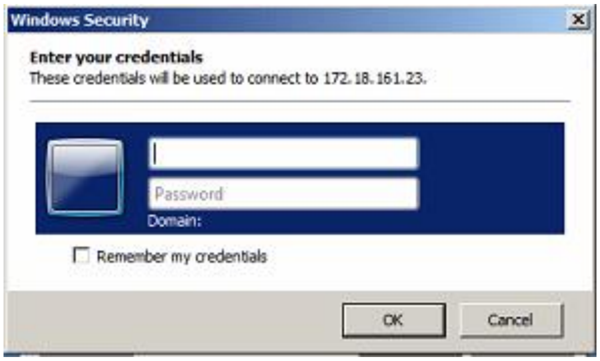
1. Click **Start** and choose **Remote Desktop Connection** to open the **Remote Desktop Connection** dialog box. Enter the IP address of the WAN port.



Computer: 172.18.161.23

User name: None specified

You will be asked for credentials when you connect.



Windows Security

Enter your credentials

These credentials will be used to connect to 172.18.161.23.

Click **Connect**. The server login page is displayed.

5.7 DMZ Host Mapping

Application Scenario

A customer deploys a server on the LAN and enables multiples services. The server address is a private IP address. WAN users cannot access services provided by the server by using the server address. If port mapping is enabled, numerous ports will be involved because many services are enabled. In this case, IP mapping can be configured to meet customer requirements.

For example, the server address is 192.168.1.20, and services such as HTTP, FTP, and video streaming media are enabled. WAN users cannot directly access services provided by the server because the server address is a private IP address. In this case, the server IP address can be mapped to a private IP address in IP mapping mode on the EG device, so that WAN users can access the server.

Networking Requirements

1. The WAN line is a single 10 Mbps fixed fiber line of China Telecom. The address is 192.168.33.56, subnet mask is 255.255.255.0, WAN gateway is 192.168.33.1, and DNS address is 218.85.157.99.
2. There is a remote desktop server on the LAN. The IP address of the server is 192.168.1.150. WAN users can access all services provided by the LAN server.

Network Topology

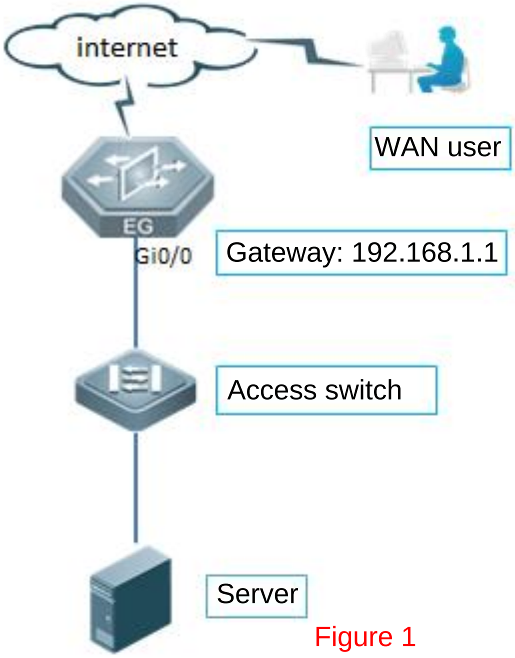


Figure 1

Configuration Key Points

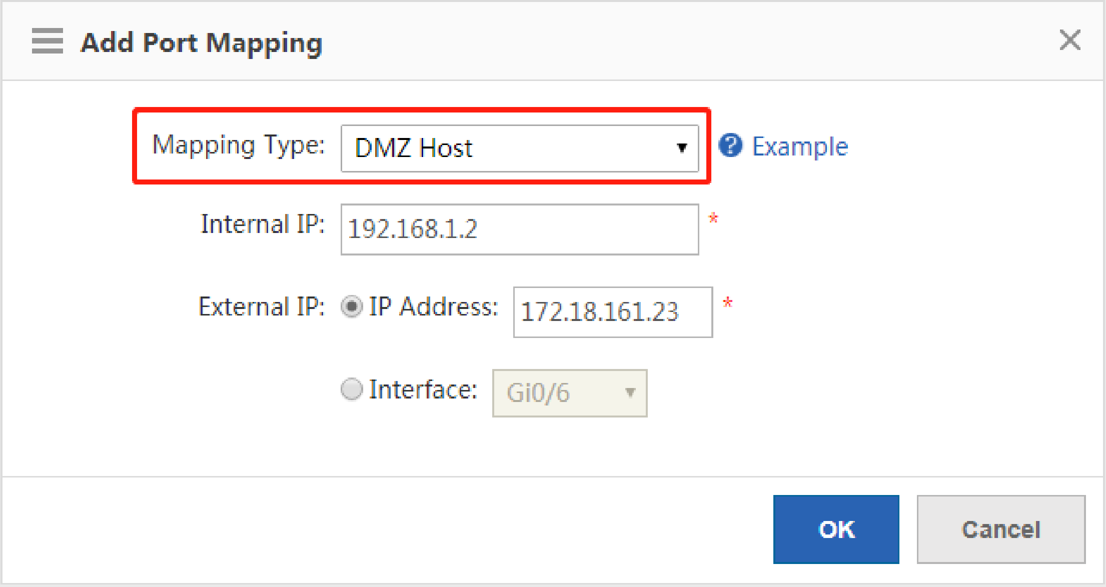
1. Ensure that LAN terminals can access the server normally.
2. The server IP address and gateway are configured, and LAN users can access the Internet normally through this server.

Note: The EG device does not support the mapping from one private IP address to two different public IP addresses..Only the mapping from one private IP address to one public IP address is supported on one line, and the other line uses port mapping.

Configuration Steps

1. Confirm that the TCP port 3389 of the server needs to be mapped.

Choose **Network** > **NAT/Port Mapping** > **Port Mapping**.



Add Port Mapping

Mapping Type: DMZ Host

Internal IP: 192.168.1.2 *

External IP: ● IP Address: 172.18.161.23 *

○ Interface: Gi0/6

a. **Mapping Type**: Select **DMZ Host** from the drop-down list, indicating that all ports of the LAN server need to be mapped.

b. **Internal IP**: Indicates the IP address of the server.

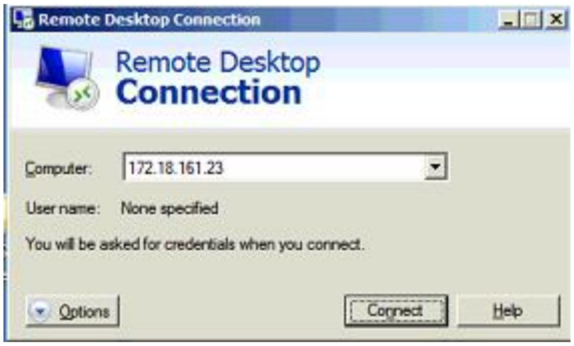
c. **External IP**: Indicates the IP address of a WAN port (**IP Address** is selected when a WAN line is used in a dynamic environment).

2. Commands generated on the CLI:

```
ip nat inside source static 192.168.1.150 192.168.33.56 permit-inside
```

Configuration Verification

1. Click **Start** and choose **Remote Desktop Connection** to open the **Remote Desktop Connection** dialog box. Enter the IP address of the WAN port.

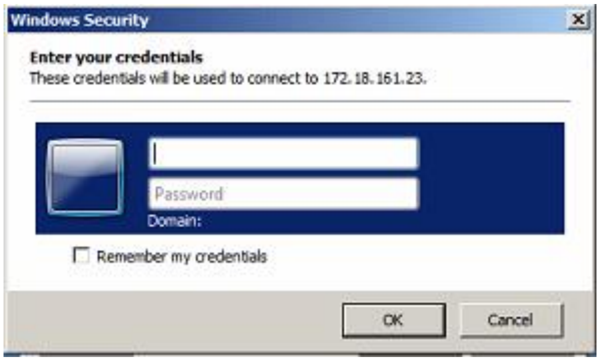


Remote Desktop Connection

Computer: 172.18.161.23

User name: None specified

You will be asked for credentials when you connect.



Windows Security

Enter your credentials

These credentials will be used to connect to 172.18.161.23.

Click **Connect**. The server login page is displayed.

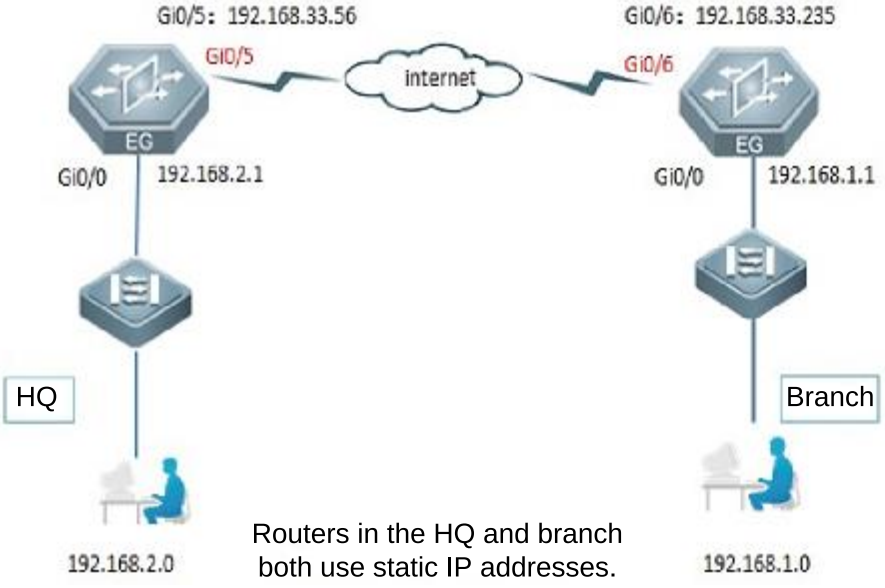
5.8 IPsecVPN

5.8.1 The Branch Router Accesses the HQ Router at a Static IP Address in Dialup Mode

Networking Requirements

The HQ and branch routers use static IP addresses. The HQ router needs to verify the IP address of the branch router.

Network Topology



Configuration Key Points

1. Configure router A in the HQ as the IPsec server.

2. Configure router B in the branch as the IPsec client.

3. Keep parameter settings at both ends consistent. The parameter settings in this case are as follows:

Authentication mode: preshared key, with the key set to ruijie.

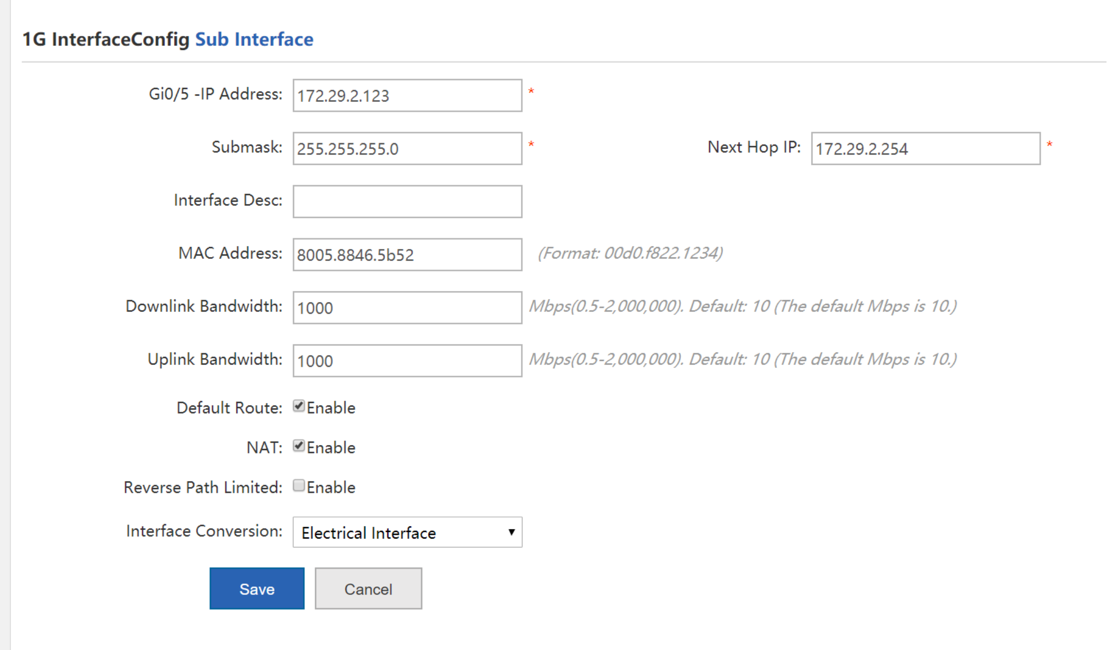
IKE algorithm: 3DES-MD5, DH2

IPsec negotiation scheme: ESP(3DES-MD5)

Configuration Steps

1. Configure router B in the branch.

(1) Complete wizard-based setup to meet basic Internet access requirements of users in the HQ and branch. If the users can access the Internet, check whether the next hop address is configured for the WAN interface.



1G InterfaceConfig Sub Interface

Gi0/5 -IP Address: 172.29.2.123 *

Submask: 255.255.255.0 * Next Hop IP: 172.29.2.254 *

Interface Desc:

MAC Address: 8005.8846.5b52 (Format: 00d0.f822.1234)

Downlink Bandwidth: 1000 Mbps(0.5-2,000,000). Default: 10 (The default Mbps is 10.)

Uplink Bandwidth: 1000 Mbps(0.5-2,000,000). Default: 10 (The default Mbps is 10.)

Default Route: ☑Enable

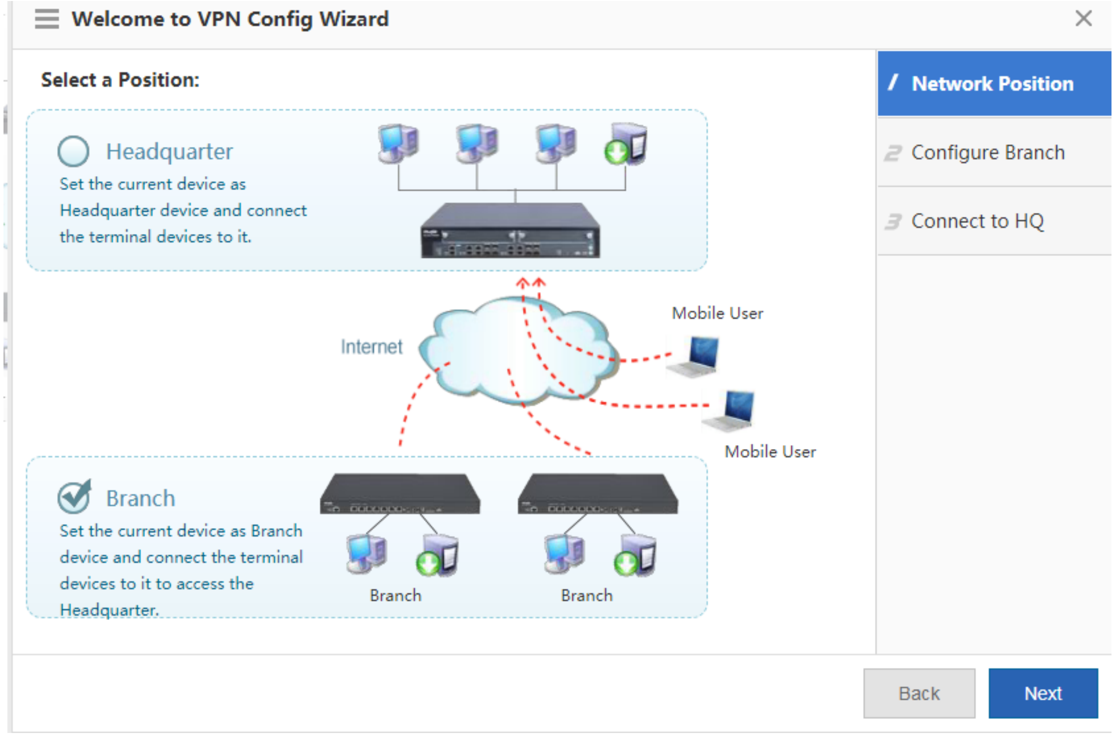
NAT: ☑Enable

Reverse Path Limited: ☐Enable

Interface Conversion: Electrical Interface

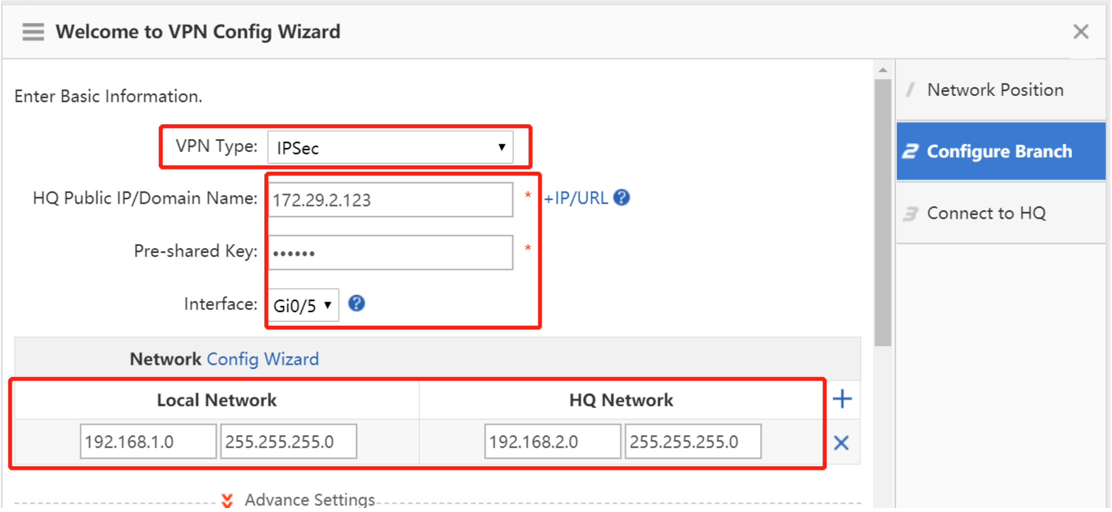
(2) Configure IPsec for router B in the branch.

Choose **Network** > **VPN** and click **Configure**. Select **Branch**, and click **Next**.



Welcome to VPN Config Wizard
Select a Position:
○ Headquarter
Set the current device as Headquarter device and connect the terminal devices to it.
Internet
Mobile User
Mobile User
Branch
Set the current device as Branch device and connect the terminal devices to it to access the Headquarter.
Branch
Branch
1 Network Position
2 Configure Branch
3 Connect to HQ
Back
Next

Configure basic branch information.



Enter Basic Information.

VPN Type: IPSec

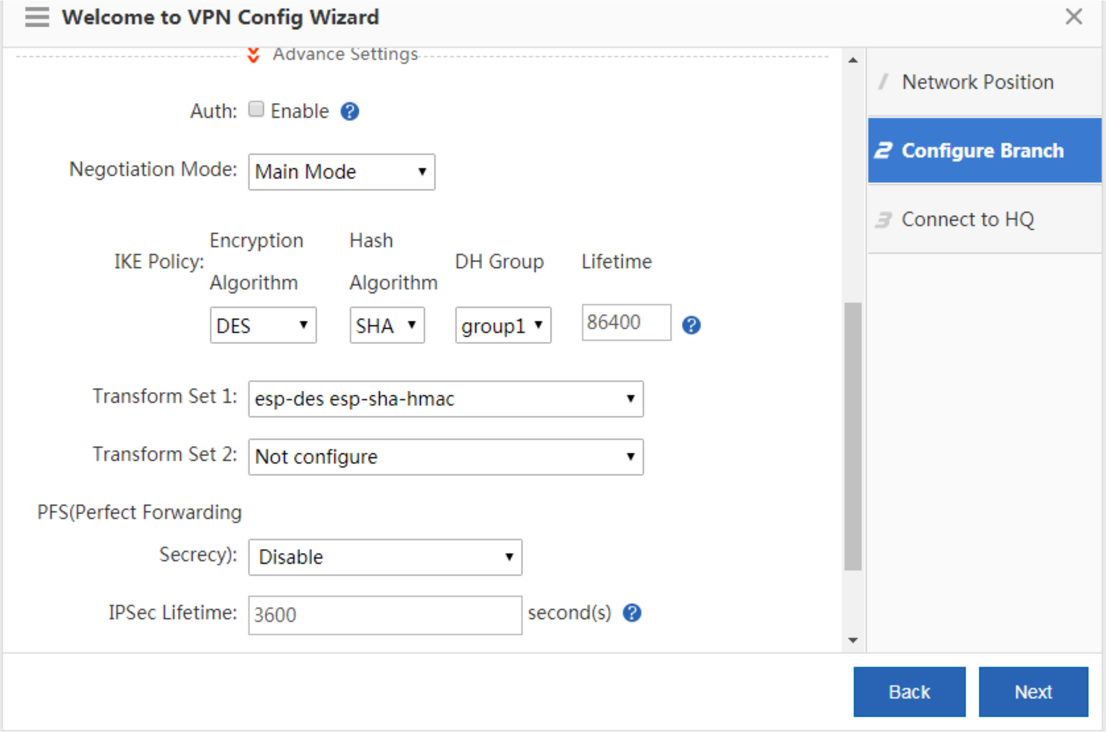
HQ Public IP/Domain Name: 172.29.2.123 * +IP/URL

Pre-shared Key: •••••• *

Interface: Gi0/5

Network Config Wizard

Local Network		HQ Network	
192.168.1.0	255.255.255.0	192.168.2.0	255.255.255.0



Auth: □ Enable

Negotiation Mode: Main Mode

IKE Policy:

Encryption Algorithm	Hash Algorithm	DH Group	Lifetime
DES	SHA	group1	86400

Transform Set 1: esp-des esp-sha-hmac

Transform Set 2: Not configure

PFS(Perfect Forwarding Secrecy): Disable

IPSec Lifetime: 3600 second(s)

Note: Only interfaces configured with the **nexthop** *x.x.x.x* command are displayed in the interface list (after the wizard-based setup is completed on the Web page, this command is configured on the WAN interface of the CLI by default).

The dialer interface can be configured on the Web page.

IKE algorithm: 3DES-MD5, DH2

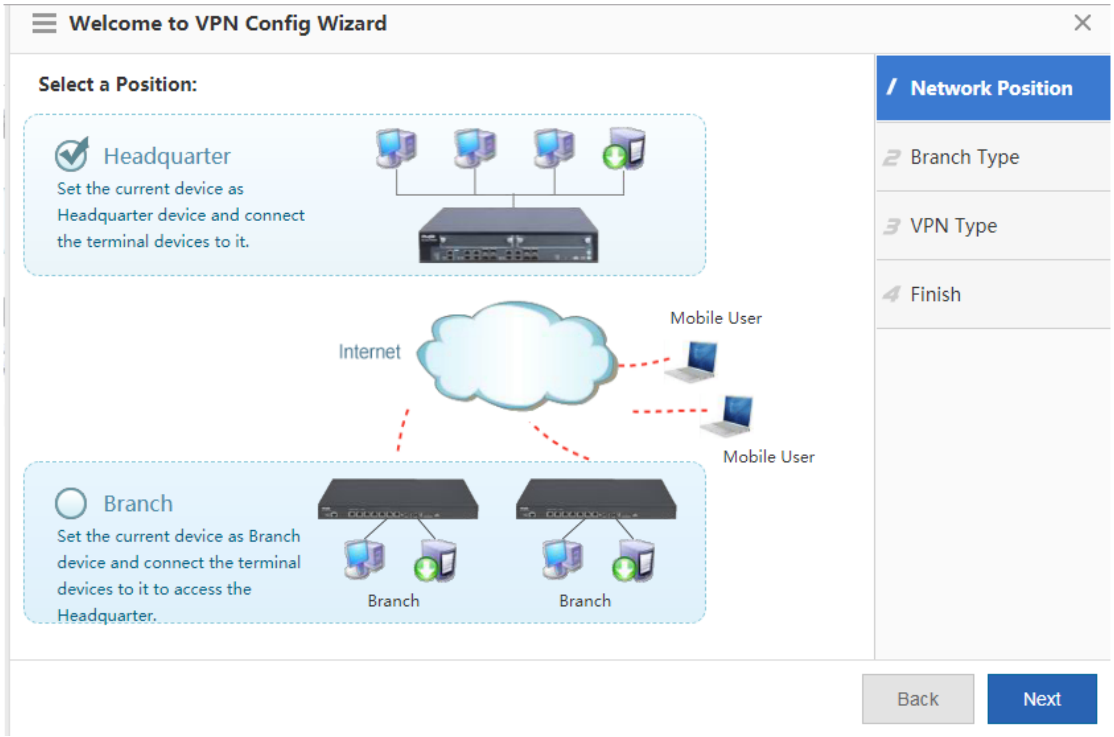
IPsec negotiation scheme: ESP(3DES-MD5)

2. Configure router A in the HQ.

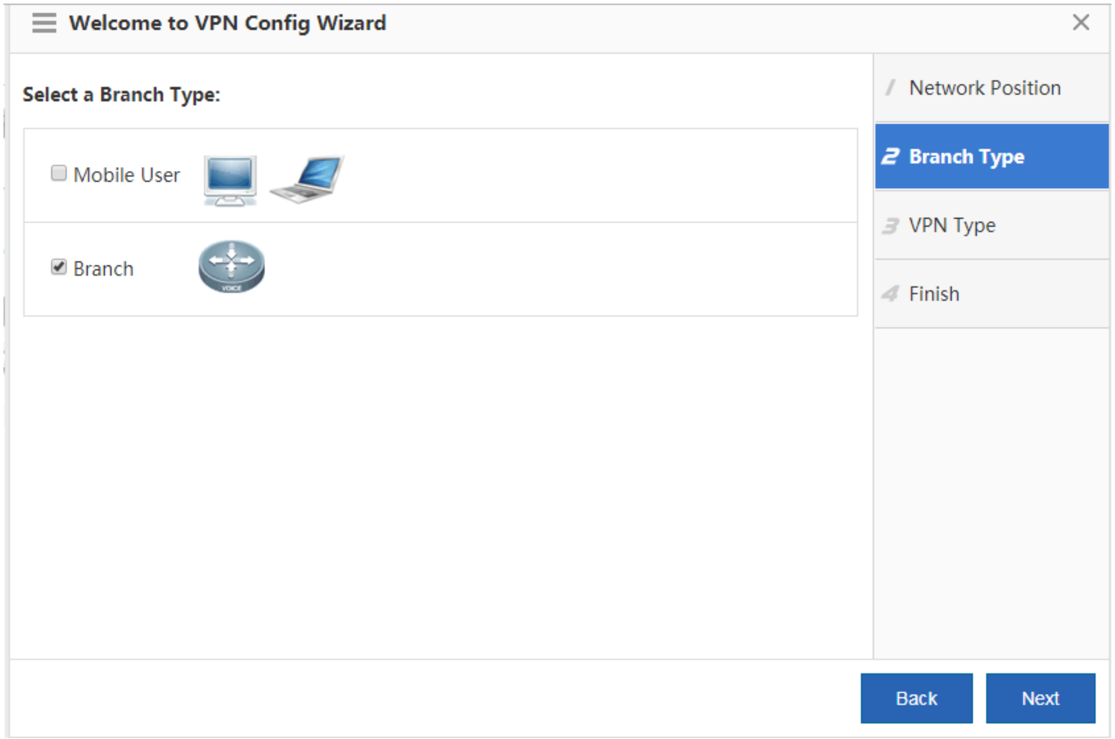
(1) Complete wizard-based setup to implement basic Internet access service of the HQ router.

(2) Configure IPsec for router A in the HQ.

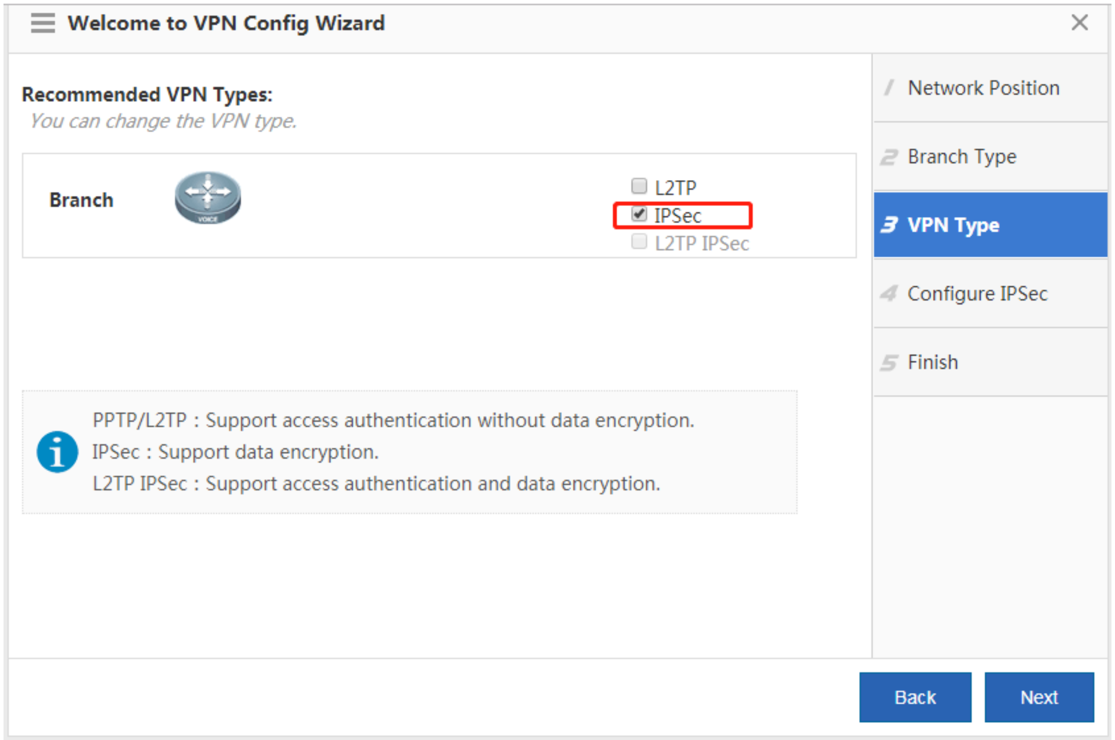
Choose **Network** > **VPN** and click **Configure**. Select **Headquarter**, and click **Next**.


Welcome to VPN Config Wizard
Select a Position:
Headquarter
Set the current device as Headquarter device and connect the terminal devices to it.
Internet
Mobile User
Mobile User
Branch
Set the current device as Branch device and connect the terminal devices to it to access the Headquarter.
Branch
Branch
1 Network Position
2 Branch Type
3 VPN Type
4 Finish
Back
Next

Select **Branch**, and click **Next**.



Select **IPsec**, and click **Next**.



Welcome to VPN Config Wizard

Recommended VPN Types:

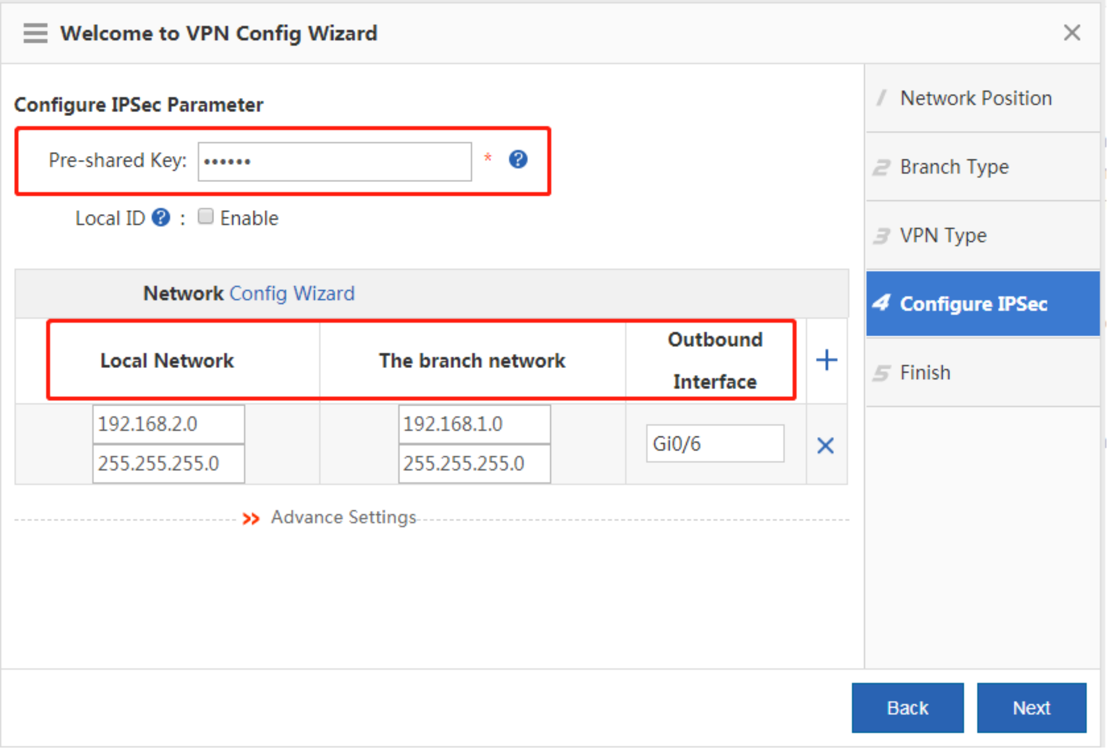
You can change the VPN type.

Branch

□ L2TP
☑ IPSec
□ L2TP IPSec

PPTP/L2TP : Support access authentication without data encryption.
IPSec : Support data encryption.
L2TP IPSec : Support access authentication and data encryption.

Configure the IPsec VPN, and click **Next**.



Welcome to VPN Config Wizard

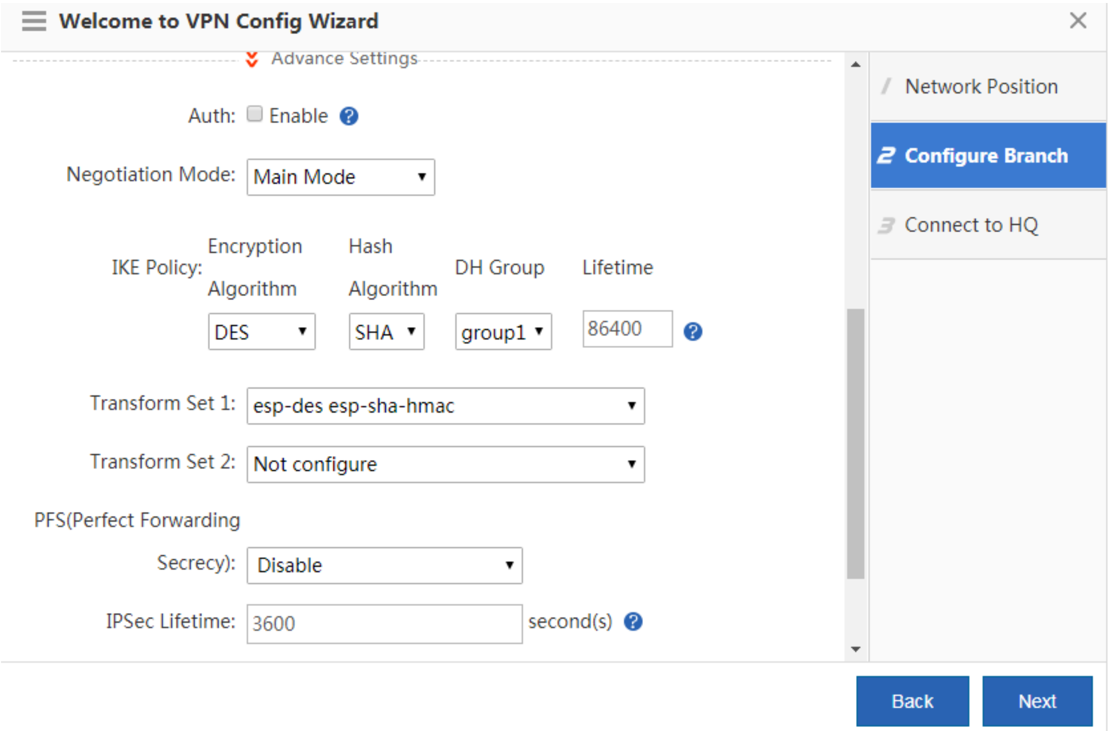
Configure IPSec Parameter

Pre-shared Key: •••••• *

Local ID : □ Enable

Network Config Wizard

Local Network	The branch network	Outbound Interface
192.168.2.0 255.255.255.0	192.168.1.0 255.255.255.0	Gi0/6



Welcome to VPN Config Wizard

Advance Settings

Auth: □ Enable

Negotiation Mode: Main Mode

IKE Policy: Encryption Algorithm: DES; Hash Algorithm: SHA; DH Group: group1; Lifetime: 86400

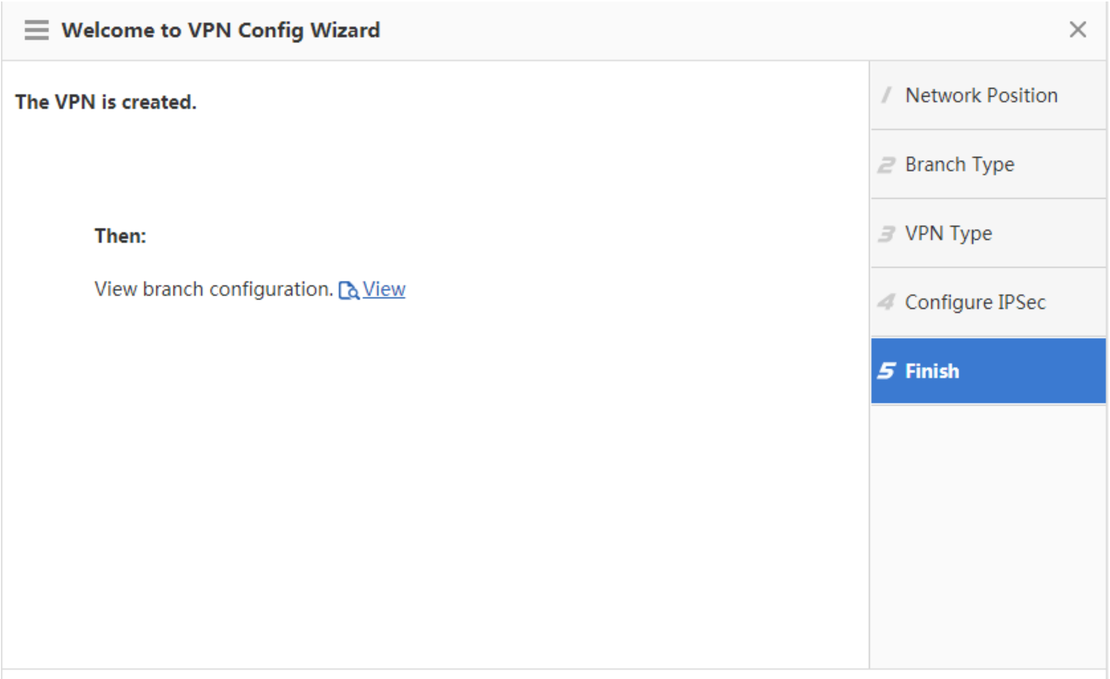
Transform Set 1: esp-des esp-sha-hmac

Transform Set 2: Not configure

PFS(Perfect Forwarding Secrecy): Disable

IPSec Lifetime: 3600 second(s)

The IPsec VPN configuration is complete.



Welcome to VPN Config Wizard

The VPN is created.

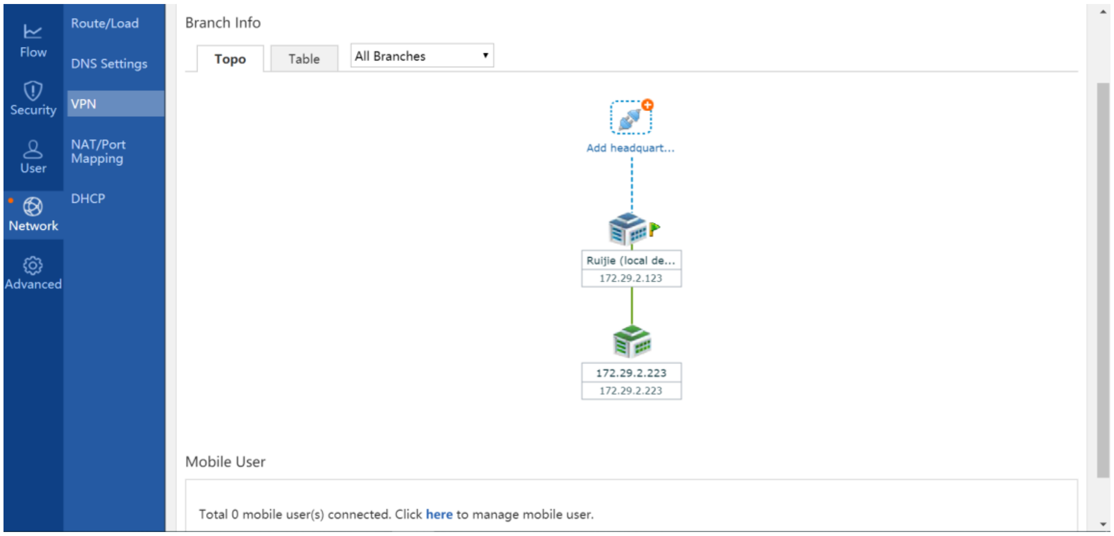
Then:

View branch configuration. View

Configuration Verification

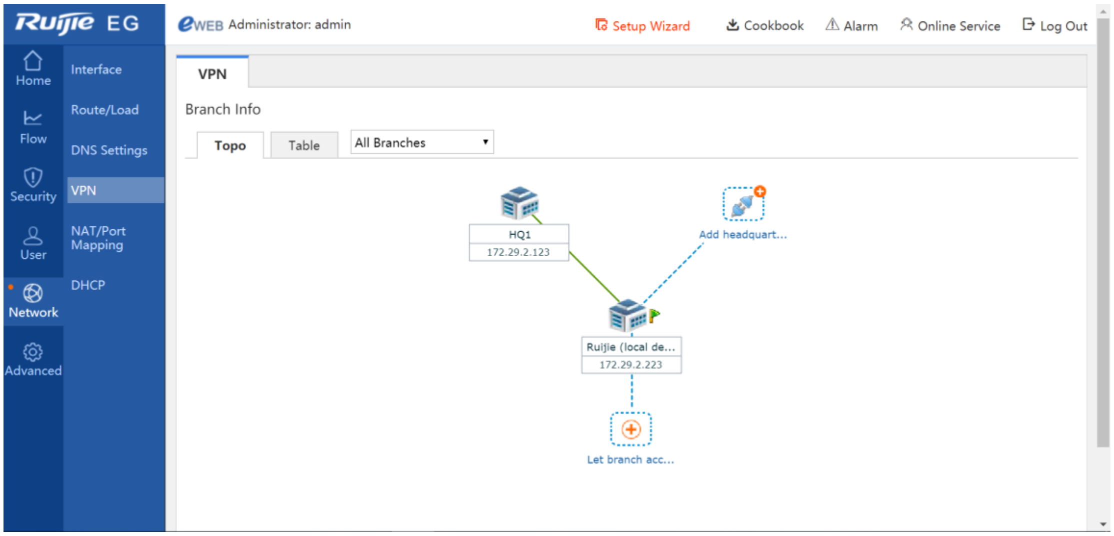
Choose **Network** > **VPN**, and click the **Topo** tab to view the configuration.

Configuration of the HQ router:



Total 0 mobile user(s) connected. Click here to manage mobile user.

Configuration of the branch router:



Check whether the routers in the HQ and branch can access each other.

Notes

1. When the Internet access service is configured via wizard-based setup on the Web of the EG device, IPsec VPN can be configured only after the next hop address is configured on the interface configuration page in the wizard-based setup. If no next hop address is configured for an interface, the interface cannot be selected during VPN configuration.
2. After a VPN is configured, the device automatically delivers AAA configuration (the system prompts you to enter the username and password during device login, and the telnet password needs to be reconfigured).
3. Close the browser after clearing the VPN configuration for the clearing operation to take effect. Otherwise, the system retains the previous VPN configuration.
4. When a WAN port receives an IPsec request but no traffic of interest is configured on the device, the error "Failed to find map" may occur. This error is generated because packets from IPsec port 500 are sent to the CPU when the IPsec map

does not exist, and this does not affect network data forwarding and management, but instead is beneficial to network management. An ACL can be configured to filter out requests from undesired IPsec-compliant device that is connected to the EG device.

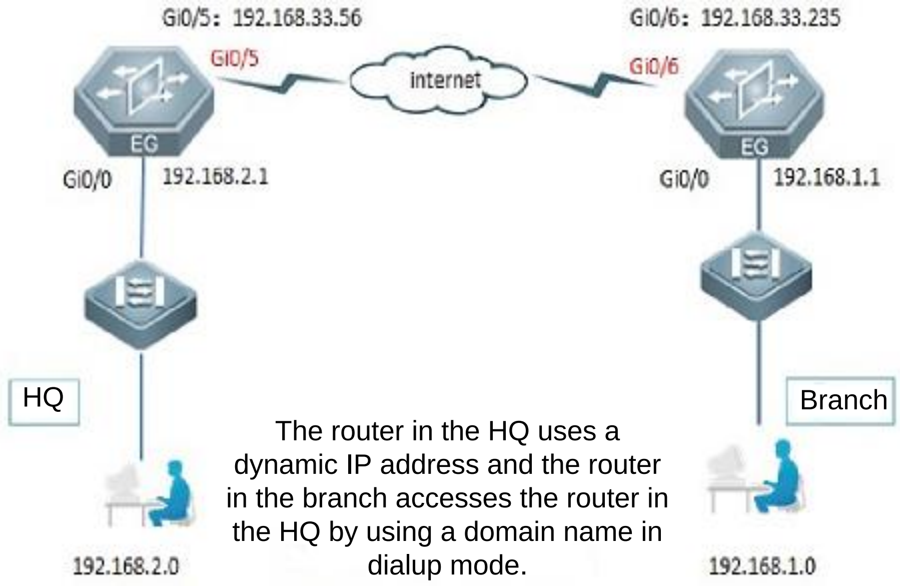
5. Some Web modules use specific ACLs. For example, the VPN module uses ACL 110 and ACL 199, the ARP guard module uses ACL 197 and ACL 2397, and the VWAN module uses ACL 198. Therefore, do not use these ACLs on the CLI, especially ACL 199, which prohibits policy configuration on the CLI. Otherwise, ACEs required by the VPN module fail to be configured on the Web page.

5.8.2 The Branch Router Accesses the HQ Router at a Dynamic IP Address in Dialup Mode

Networking Requirements

The HQ router uses a dynamic IP address and the branch router accesses the HQ router by using the domain name in dialup mode.

Network Topology



The router in the HQ uses a dynamic IP address and the router in the branch accesses the router in the HQ by using a domain name in dialup mode.

Configuration Key Points

1. Configure router A in the HQ as the IPsec server.
2. Configure router B in the branch as the IPsec client.
3. Keep parameter settings at both ends consistent. The parameter settings in this case are as follows:

Authentication mode: preshared key, with the key set to ruijie.

IKE algorithm: 3DES-MD5, DH2

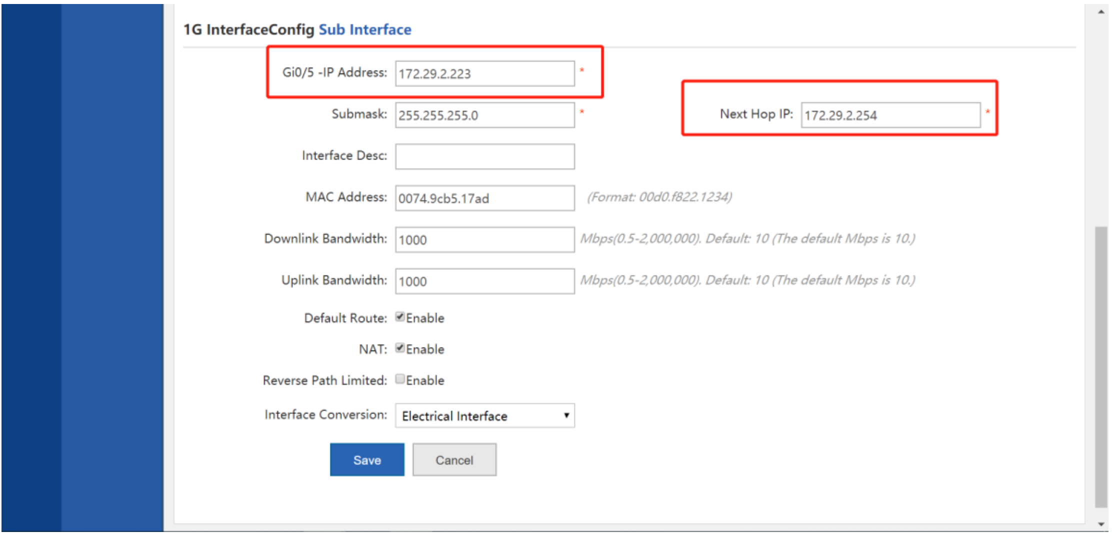
IPsec negotiation scheme: ESP(3DES-MD5)

Configuration Steps

1. Configure router B in the branch.

The Web page does not support dynamic domain names. Therefore, complete configuration on the Web page and then perform modification on the CLI.

(1) Complete wizard-based setup to meet basic Internet access requirements of users in the HQ and branch. If the users can access the Internet, check whether the next hop address is configured for the WAN interface.



1G InterfaceConfig Sub Interface

Gi0/5 -IP Address: 172.29.2.223 *

Submask: 255.255.255.0 *

Next Hop IP: 172.29.2.254 *

Interface Desc:

MAC Address: 0074.9cb5.17ad (Format: 00d0.f822.1234)

Downlink Bandwidth: 1000 Mbps(0.5-2,000,000). Default: 10 (The default Mbps is 10.)

Uplink Bandwidth: 1000 Mbps(0.5-2,000,000). Default: 10 (The default Mbps is 10.)

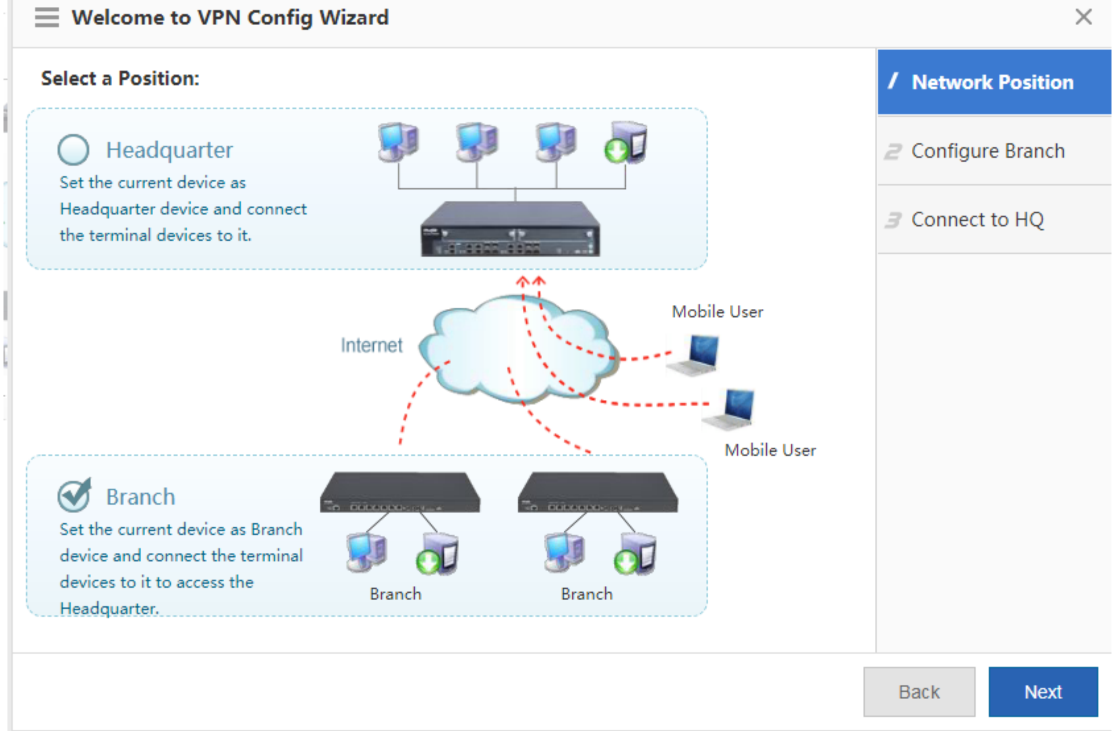
Default Route: ☑Enable

NAT: ☑Enable

Reverse Path Limited: ☐Enable

Interface Conversion: Electrical Interface ▾

(2) Choose **Network** > **VPN** and click **Configure**. Select **Branch**, and click **Next**.



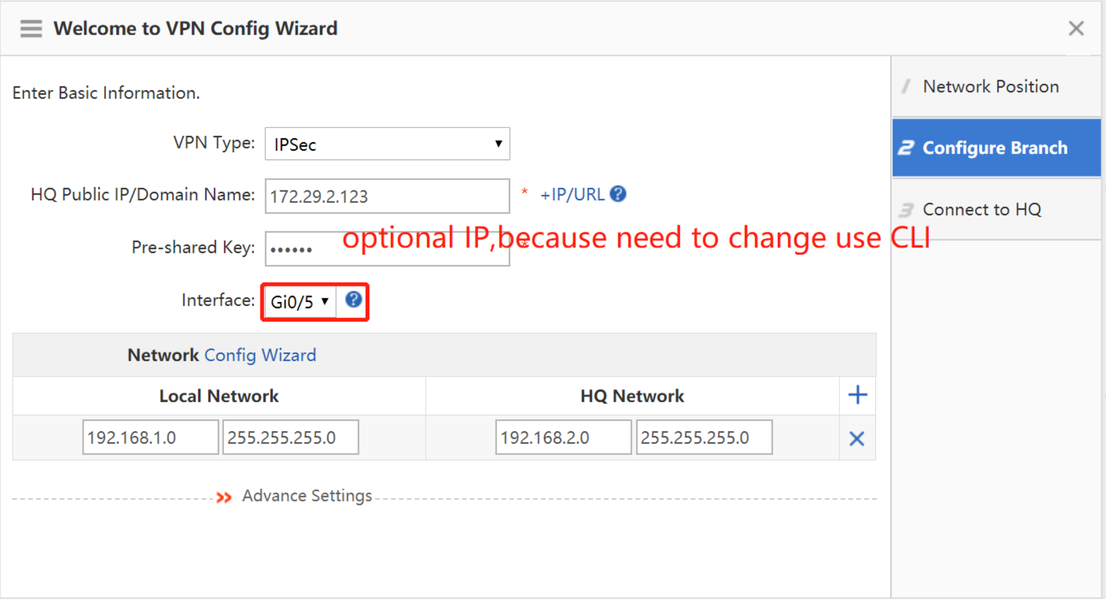
Welcome to VPN Config Wizard

Select a Position:

○ Headquarter
Set the current device as Headquarter device and connect the terminal devices to it.

☑ Branch
Set the current device as Branch device and connect the terminal devices to it to access the Headquarter.

(3) Configure basic IPsec information, and click **Next**.



Welcome to VPN Config Wizard

Enter Basic Information.

VPN Type: IPSec

HQ Public IP/Domain Name: 172.29.2.123 * +IP/URL

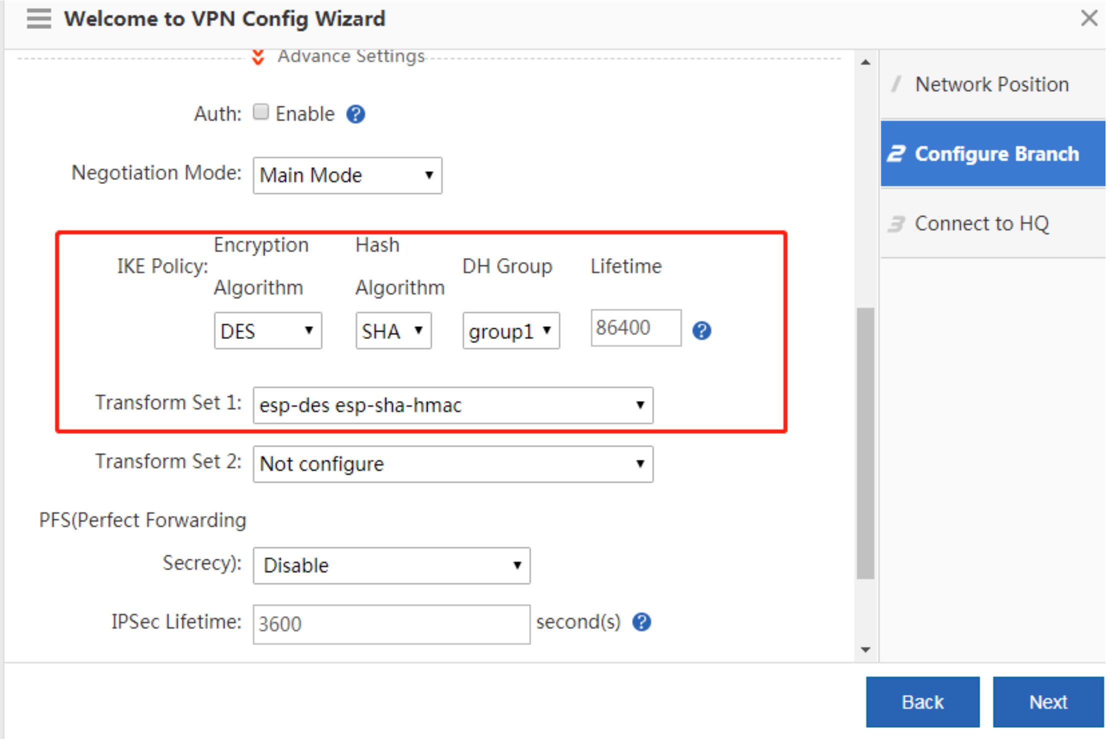
Pre-shared Key: ••••••

optional IP,because need to change use CLI

Interface: Gi0/5

Network Config Wizard

Local Network		HQ Network	
192.168.1.0	255.255.255.0	192.168.2.0	255.255.255.0



Welcome to VPN Config Wizard

Auth: □ Enable

Negotiation Mode: Main Mode

IKE Policy:	Encryption Algorithm	Hash Algorithm	DH Group	Lifetime
	DES	SHA	group1	86400

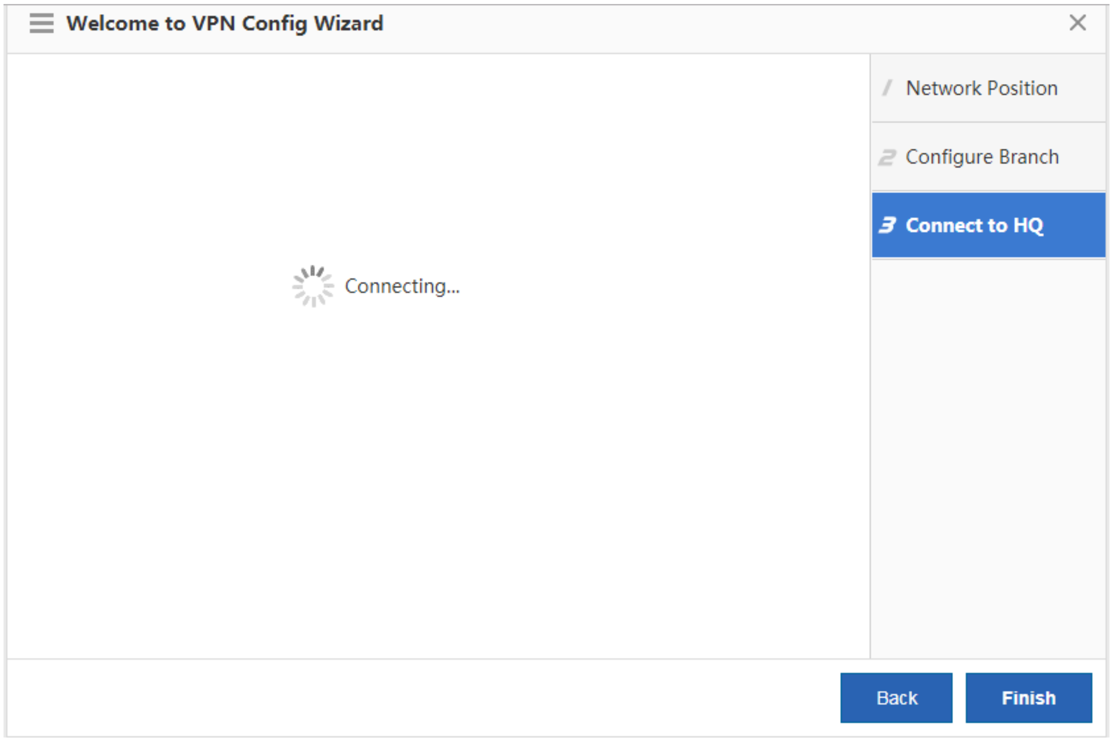
Transform Set 1: esp-des esp-sha-hmac

Transform Set 2: Not configure

PFS(Perfect Forwarding Secrecy): Disable

IPSec Lifetime: 3600 second(s)

(4) Click **Finish**.

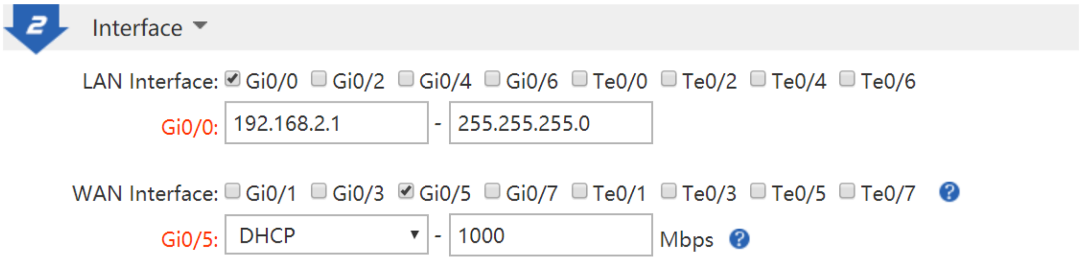


On the CLI, change the public IP address of the HQ router to a dynamic domain name:

```
branch(config)#no crypto isakmp key 0 ruijie address 192.168.2.1

branch(config)#crypto isakmp key 0 ruijie hostnameruijie.xicp.net

branch(config)#crypto map Gi0/6 20 ipsec-isakmp

branch(config-crypto-map)#no set peer 192.168.2.1

branch(config-crypto-map)#set peer ruijie.xicp.net
```

2. Configure router A in the HQ.

On the interface configuration page, click a WAN interface to configure it. Dynamic IP addresses can be allocated in DHCP mode or obtained in dialup mode.

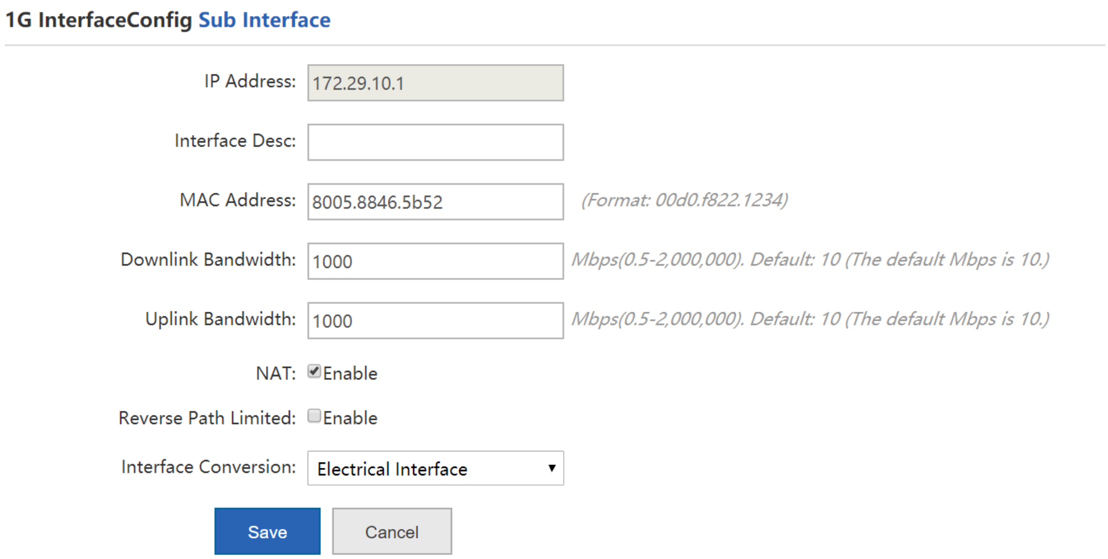


LAN Interface: ☑ Gi0/0 □ Gi0/2 □ Gi0/4 □ Gi0/6 □ Te0/0 □ Te0/2 □ Te0/4 □ Te0/6

Gi0/0: 192.168.2.1 - 255.255.255.0

WAN Interface: □ Gi0/1 □ Gi0/3 ☑ Gi0/5 □ Gi0/7 □ Te0/1 □ Te0/3 □ Te0/5 □ Te0/7

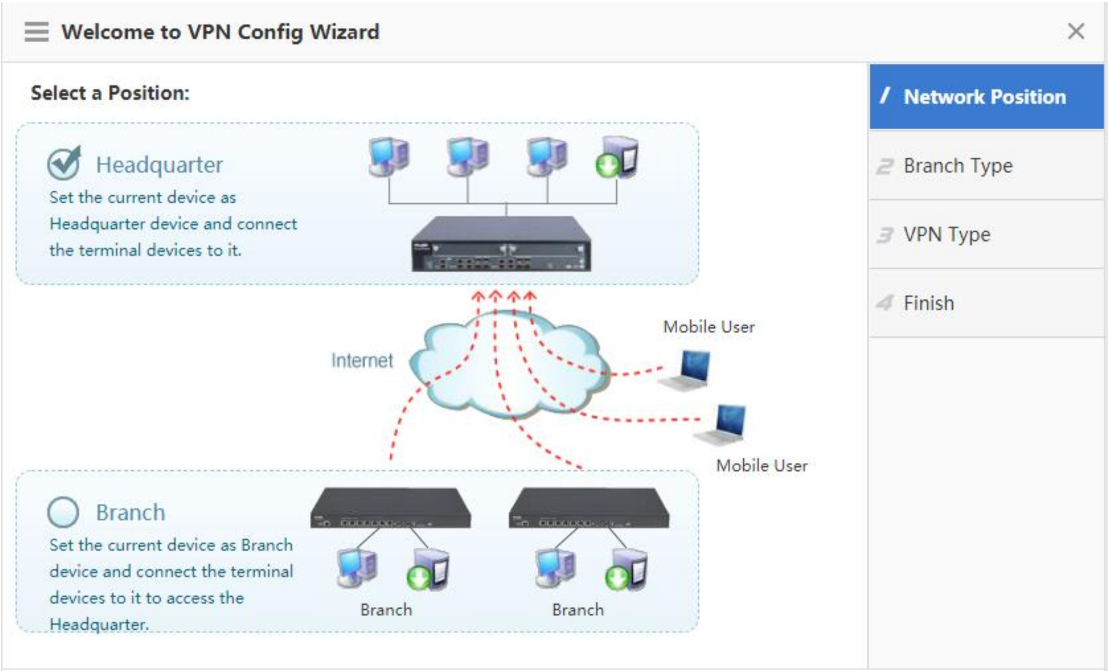
Gi0/5: DHCP - 1000 Mbps



1G InterfaceConfig Sub Interface

IP Address:	172.29.10.1
Interface Desc:	
MAC Address:	8005.8846.5b52 *(Format: 00d0.f822.1234)*
Downlink Bandwidth:	1000 *Mbps(0.5-2,000,000). Default: 10 (The default Mbps is 10.)*
Uplink Bandwidth:	1000 *Mbps(0.5-2,000,000). Default: 10 (The default Mbps is 10.)*
NAT:	☑ Enable
Reverse Path Limited:	☐ Enable
Interface Conversion:	Electrical Interface ▾

Choose **Network** > **VPN** and click **Configure**. Select **Headquarter**, and click **Next**.



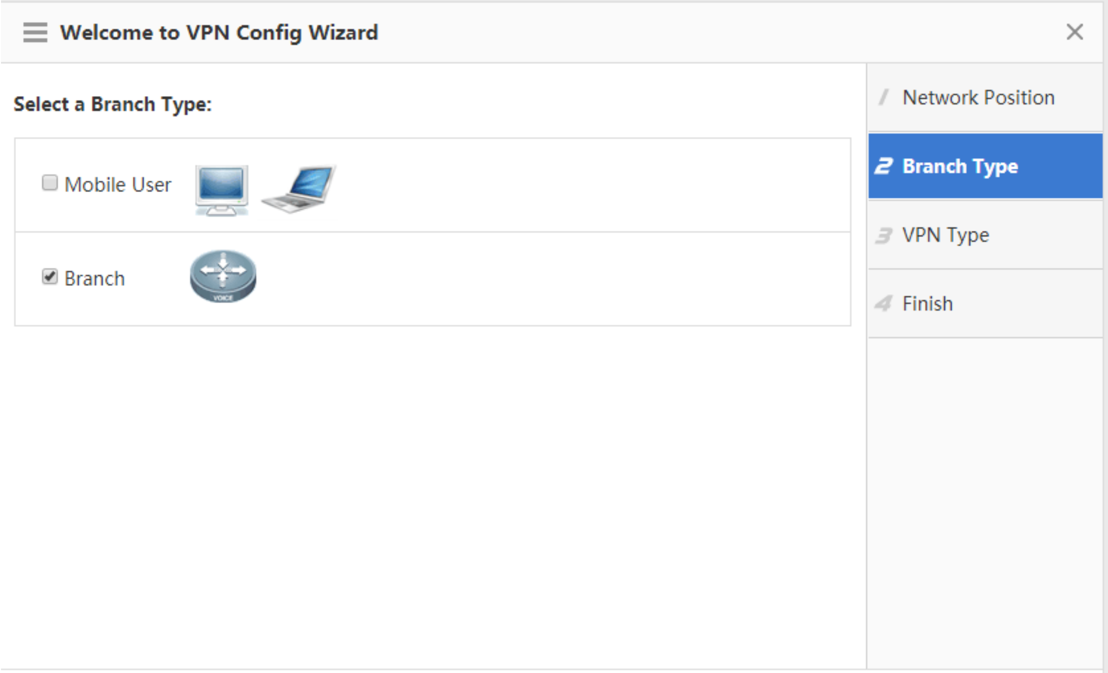
Welcome to VPN Config Wizard

Select a Position:

● Headquarter
Set the current device as Headquarter device and connect the terminal devices to it.

○ Branch
Set the current device as Branch device and connect the terminal devices to it to access the Headquarter.

Select **Branch**, and click **Next**.

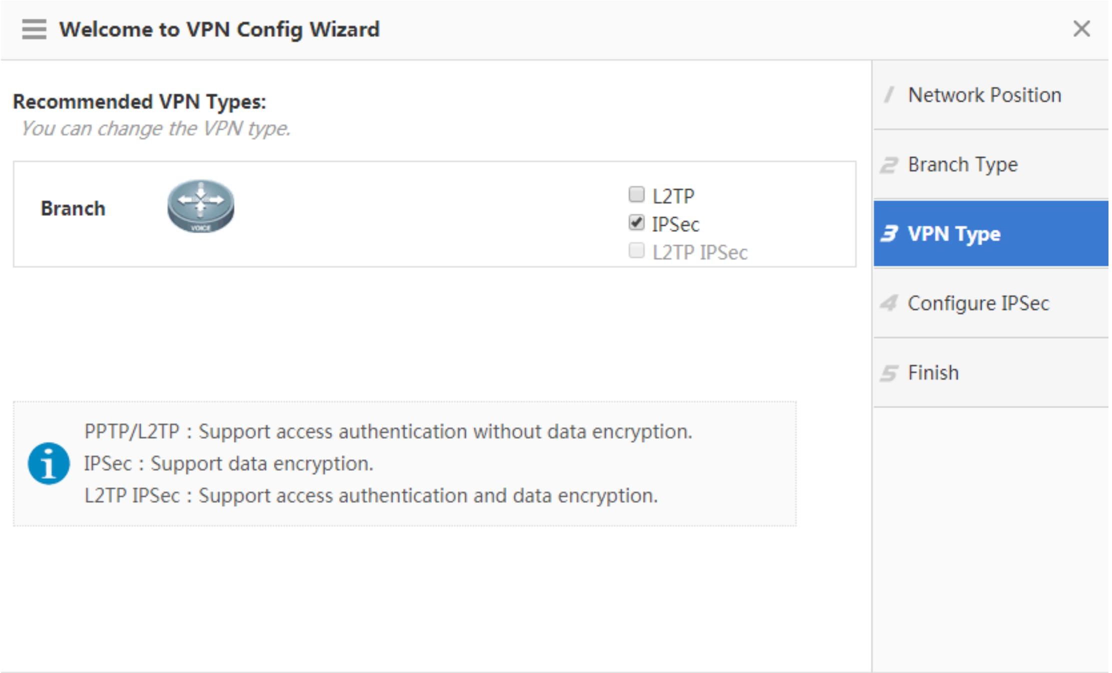


Select a Branch Type:

□ Mobile User

☑ Branch

Select **IPsec**, and click **Next**.



Recommended VPN Types:

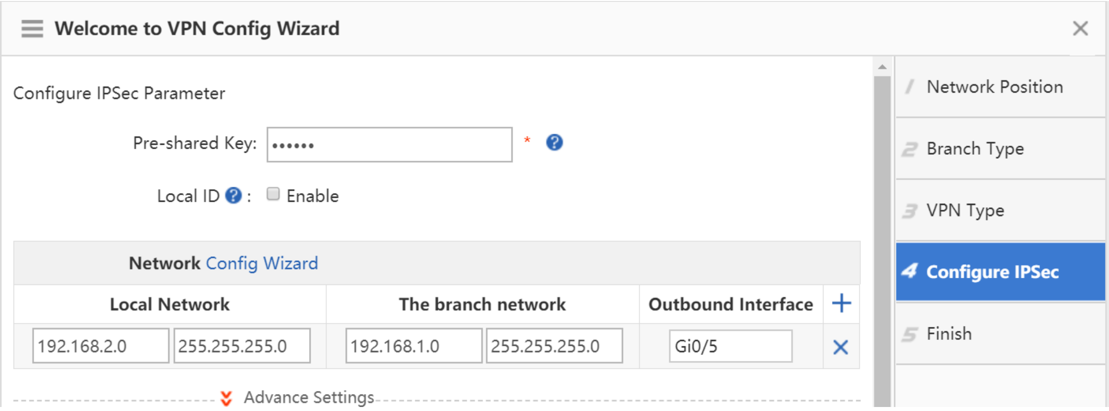
You can change the VPN type.

Branch

□ L2TP
☑ IPSec
□ L2TP IPSec

PPTP/L2TP：Support access authentication without data encryption.
IPSec：Support data encryption.
L2TP IPSec：Support access authentication and data encryption.

Configure IPsec basic information, and click **Next**.



Welcome to VPN Config Wizard

Configure IPSec Parameter

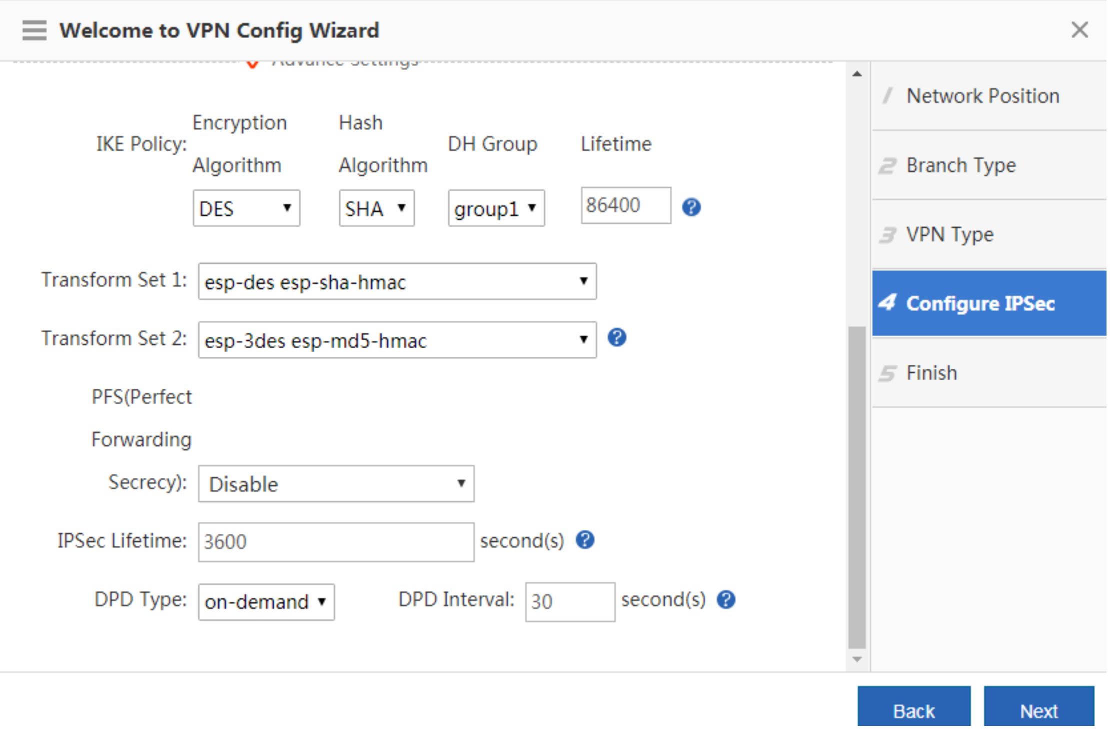
Pre-shared Key: •••••• *

Local ID : □ Enable

Network Config Wizard

Local Network		The branch network		Outbound Interface
192.168.2.0	255.255.255.0	192.168.1.0	255.255.255.0	Gi0/5

Advance Settings



Welcome to VPN Config Wizard

IKE Policy:	Encryption Algorithm	Hash Algorithm	DH Group	Lifetime
	DES	SHA	group1	86400

Transform Set 1: esp-des esp-sha-hmac

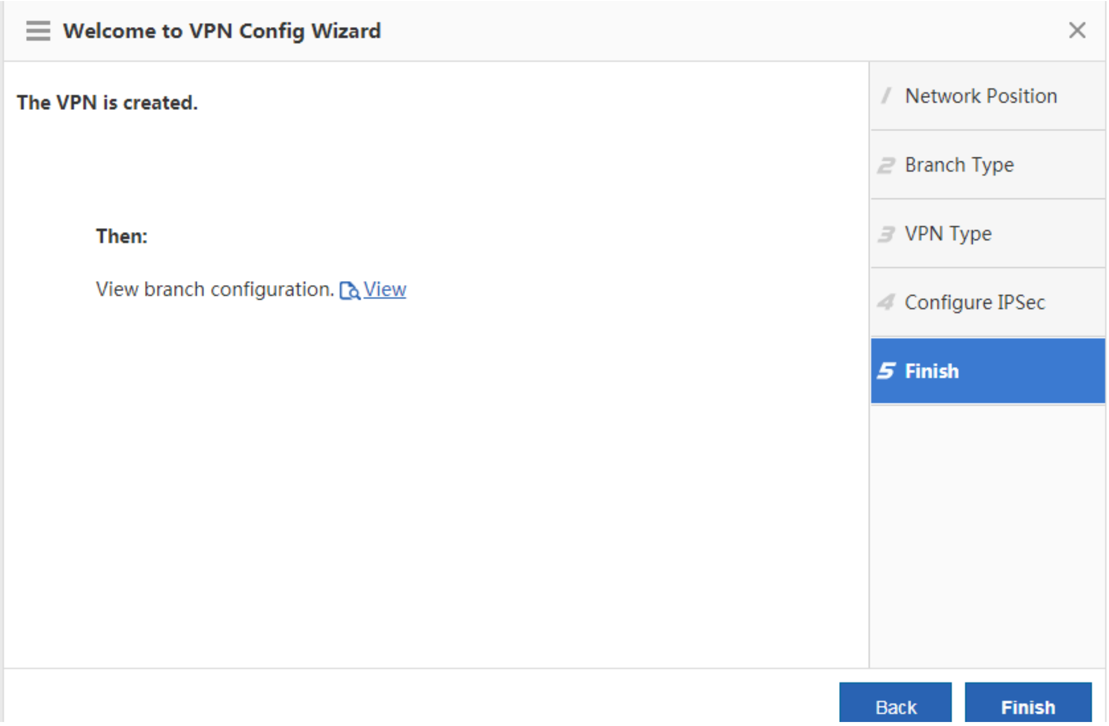
Transform Set 2: esp-3des esp-md5-hmac

PFS(Perfect Forwarding Secrecy): Disable

IPSec Lifetime: 3600 second(s)

DPD Type: on-demand DPD Interval: 30 second(s)

Click **Finish**.



Welcome to VPN Config Wizard

The VPN is created.

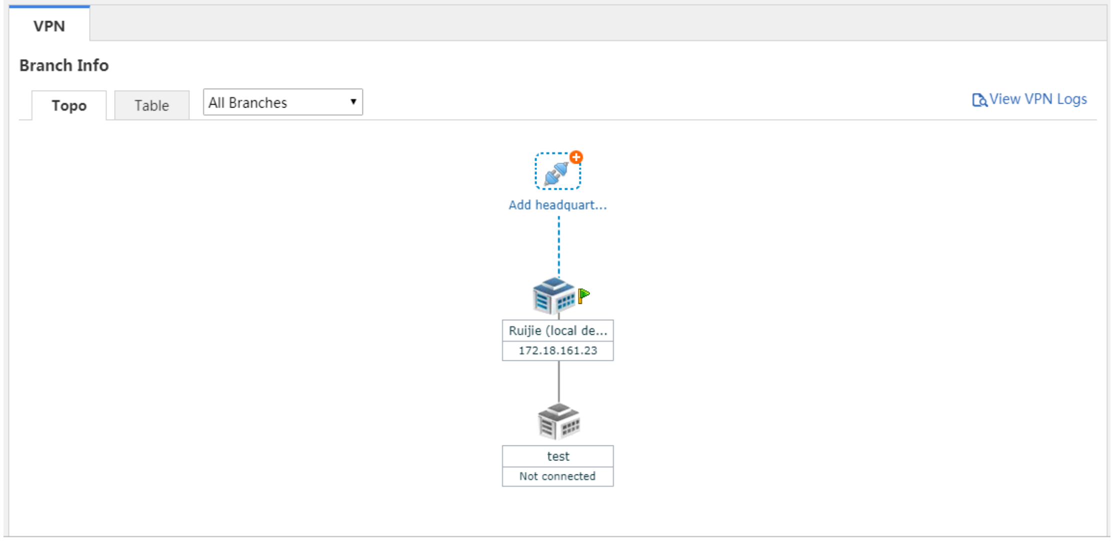
Then:

View branch configuration. View

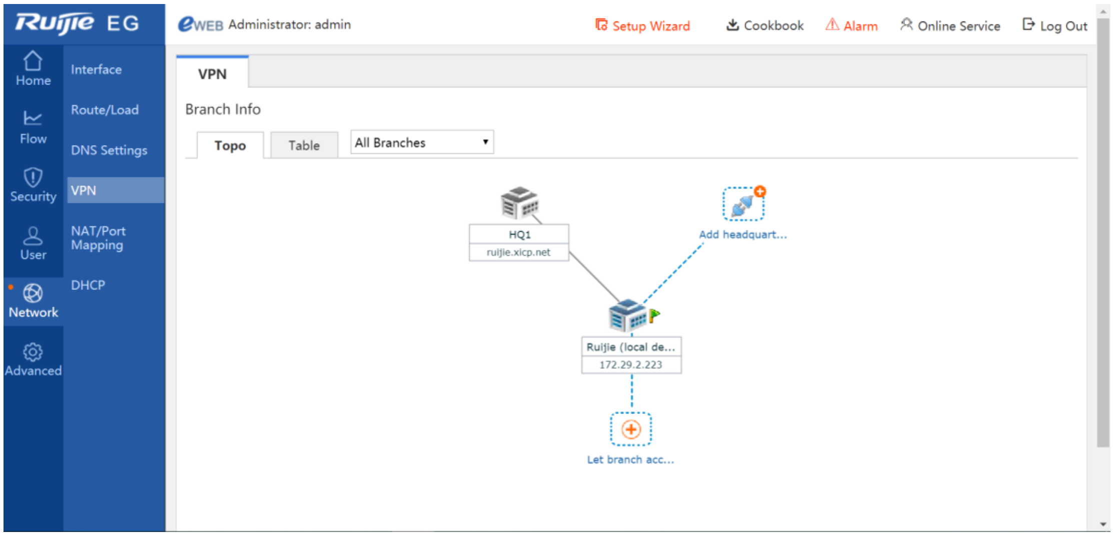
Configuration Verification

Choose **Network** > **VPN**, and click the **Topo** tab to view the configuration.

Configuration of the HQ router:



Configuration of the branch router:



Check whether the HQ router and branch router can access each other.

Notes (Optional)

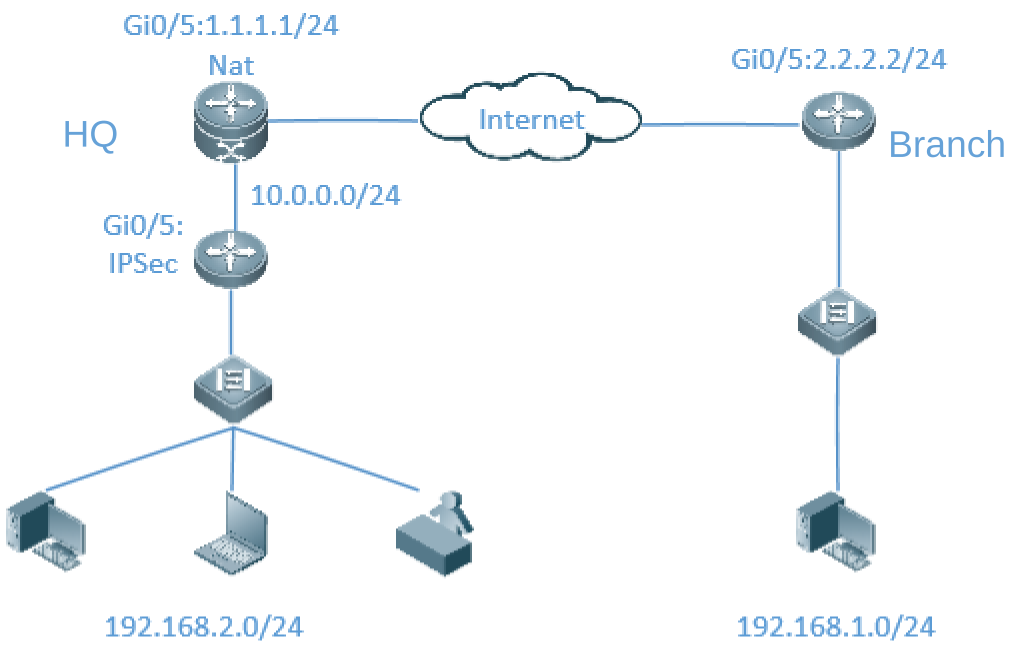
1. On the Web page, IPsec supports only peer IP addresses and does not support domain names. IPsec using domain names needs to be configured on the CLI.
2. When a WAN port receives an IPsec request but no traffic of interest is configured on the device, the error "Failed to find map" may occur. This error is generated because packets from IPsec port 500 are sent to the CPU when the IPsec map does not exist. The error does not affect network data forwarding and management, which is beneficial to network management. An ACL can be configured to filter out requests from undesired IPsec-compliant device that is connected to the EG device.
3. Some Web modules use specific ACLs. For example, the VPN module uses ACL 110 and ACL 199, the ARP guard module uses the ACL 197 and ACL 2397, and the VWAN module uses ACL 198. Therefore, do not use these ACLs on the CLI. especially ACL 199, which prohibits policy configuration on the CLI. Otherwise, ACEs required by the VPN module fail to be configured on the Web page.

5.8.3 The Branch Router Accesses the HQ Router on the LAN in Dialup Mode

Networking Requirements

The HQ router is deployed on the LAN, mapping is configured on the egress of the LAN, and users in the branch access the HQ router in dialup mode.

Network Topology



Configuration Key Points

1. Configure the LAN gateway router A in the HQ as the IPsec server.
2. Configure router B in the branch as the IPsec client.
3. Keep parameter settings at both ends consistent. The parameter settings in this case are as follows:

Authentication mode: preshared key, with the key set to ruijie.

IKE algorithm: 3DES-MD5, DH2

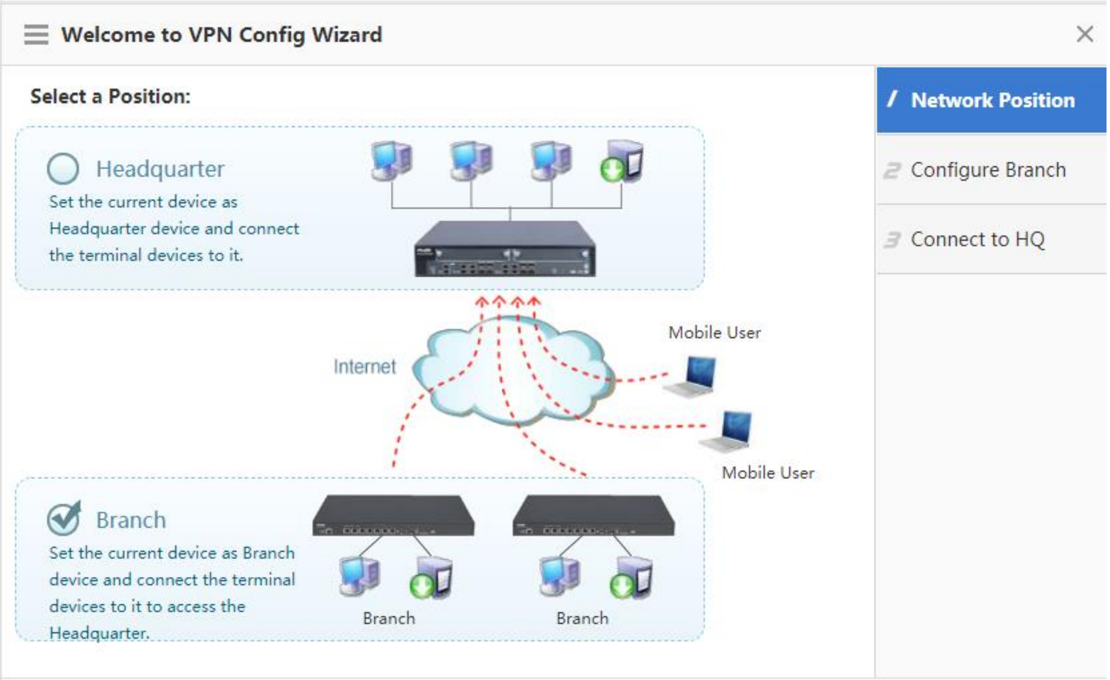
IPsec negotiation scheme: ESP(3DES-MD5)

4. Configure NAT mapping on the outermost egress of the HQ and establish an IPsec connection on the LAN gateway.

Configuration Steps

1. Ensure that basic configuration on the EG device and routers in both the HQ and branch are normal, and LANs users at both ends can access the WAN.
2. Configure router B in the branch.

Choose **Network** > **VPN** and click **Configure**. Select **Branch**, and click **Next**.



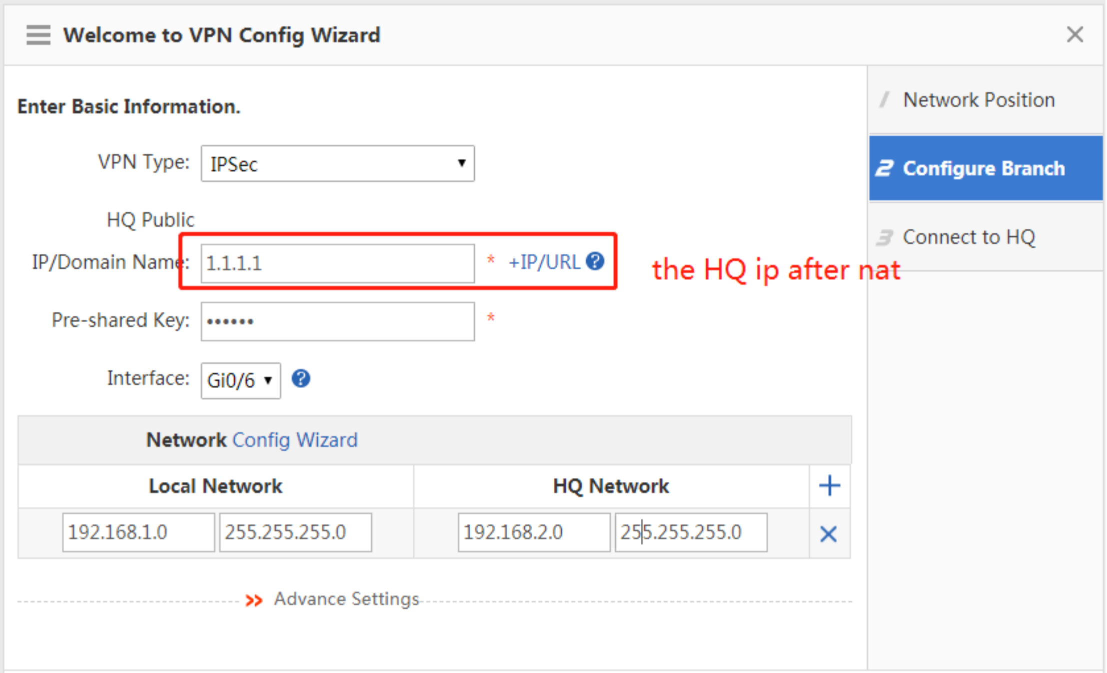
Welcome to VPN Config Wizard

Select a Position:

○ Headquarter
Set the current device as Headquarter device and connect the terminal devices to it.

☑ Branch
Set the current device as Branch device and connect the terminal devices to it to access the Headquarter.

Configure an IPsec policy, set the public IP address of the HQ router to the IP address obtained after NAT, and click **Next**.



Welcome to VPN Config Wizard

Enter Basic Information.

VPN Type: IPSec

HQ Public IP/Domain Name: 1.1.1.1 * +IP/URL

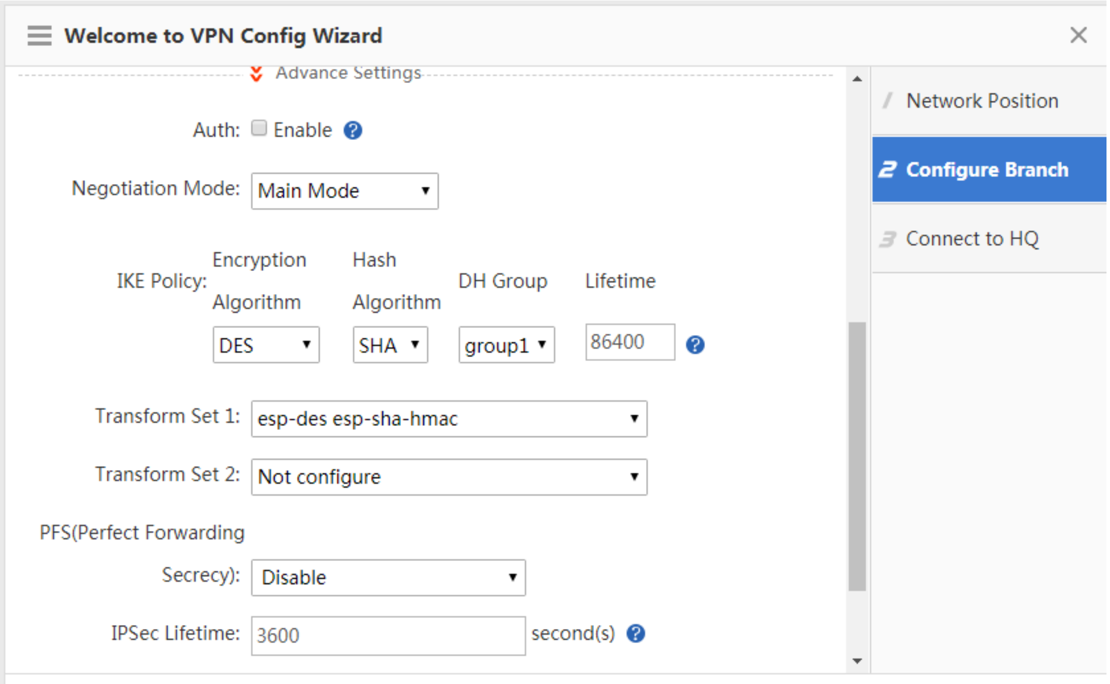
the HQ ip after nat

Pre-shared Key: •••••• *

Interface: Gi0/6

Network Config Wizard

Local Network		HQ Network	
192.168.1.0	255.255.255.0	192.168.2.0	255.255.255.0



Welcome to VPN Config Wizard

Advance Settings

Auth: □ Enable

Negotiation Mode: Main Mode

IKE Policy: Encryption Algorithm: DES; Hash Algorithm: SHA; DH Group: group1; Lifetime: 86400

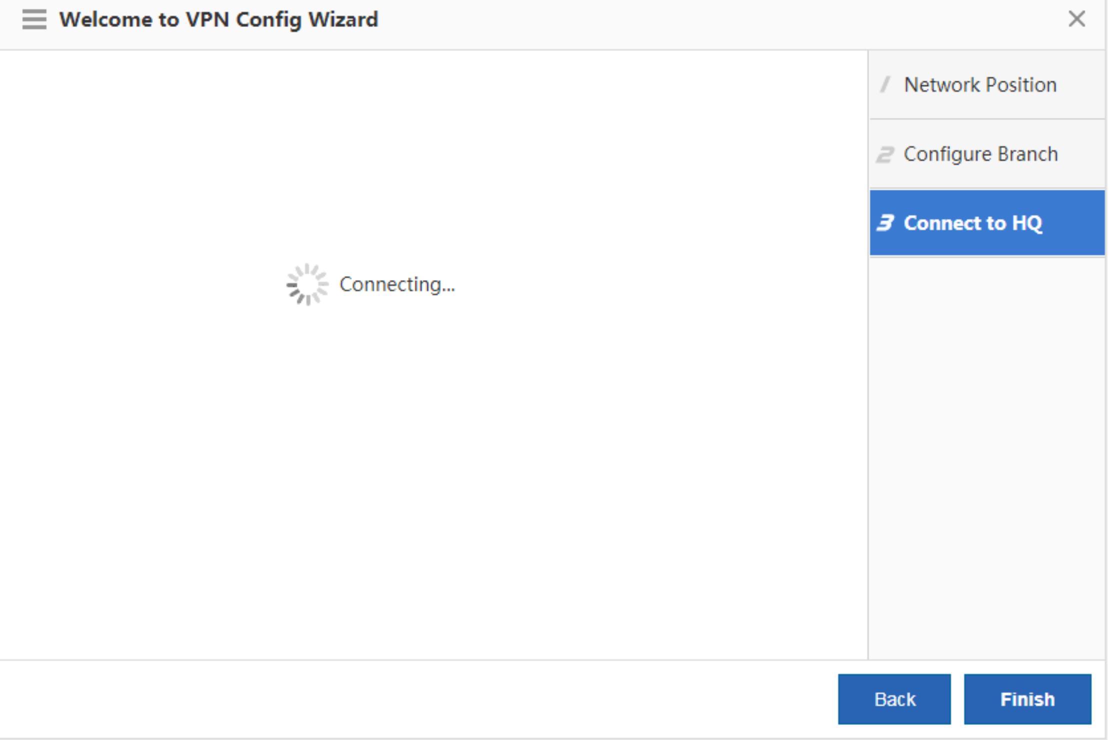
Transform Set 1: esp-des esp-sha-hmac

Transform Set 2: Not configure

PFS(Perfect Forwarding Secrecy): Disable

IPSec Lifetime: 3600 second(s)

Click **Finish**.



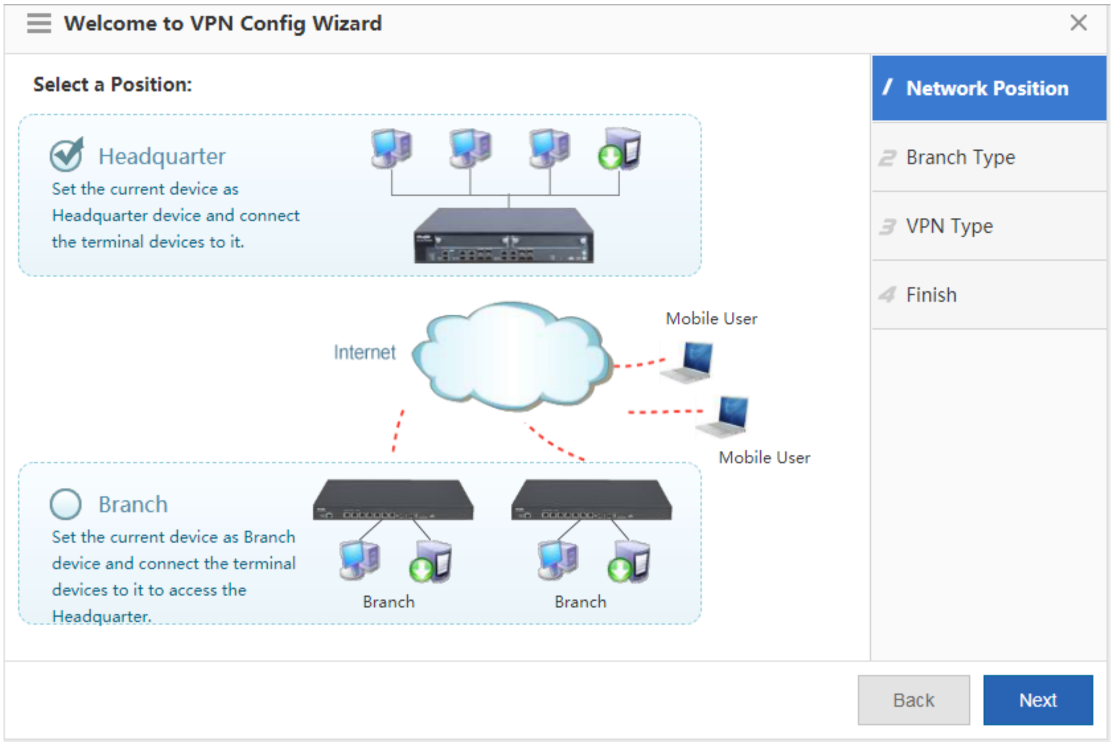
Welcome to VPN Config Wizard

Connecting...

3. Configure router A in the HQ.

Configure IPsec on the LAN EG device.

(1) Choose **Network** > **VPN** and click **Configure**. Select **Headquarter**, and click **Next**.



Welcome to VPN Config Wizard

Select a Position:

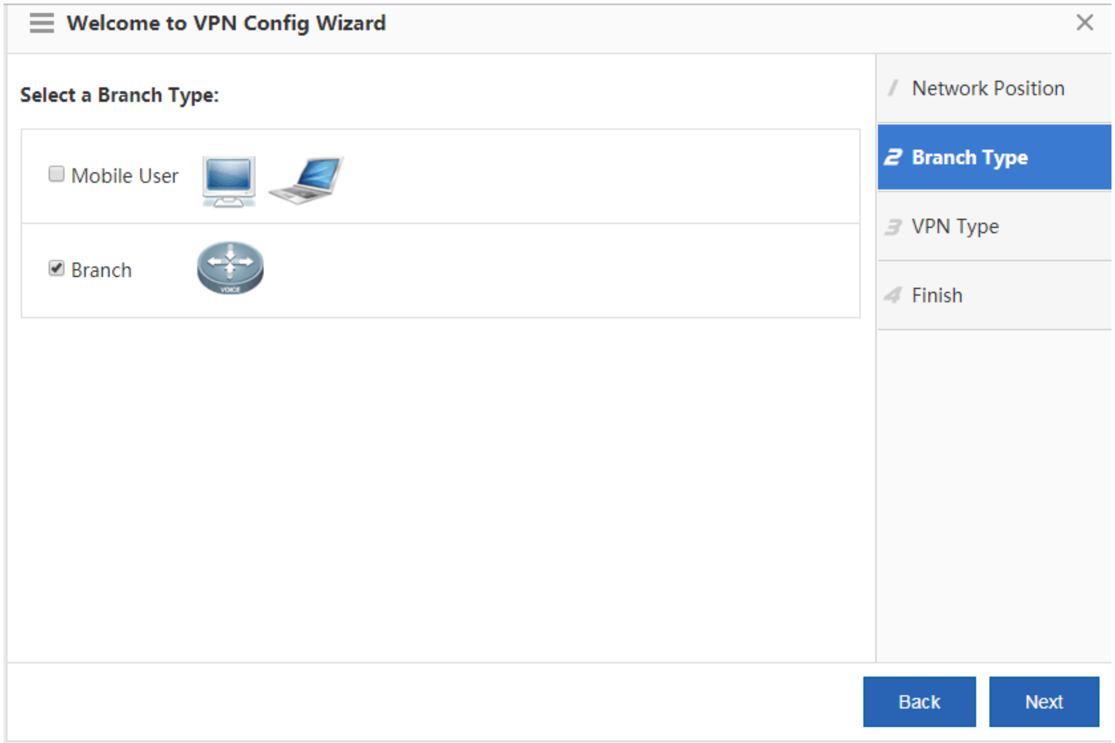
☑ Headquarter

Set the current device as Headquarter device and connect the terminal devices to it.

○ Branch

Set the current device as Branch device and connect the terminal devices to it to access the Headquarter.

(2) Select **Branch**, and click **Next**.



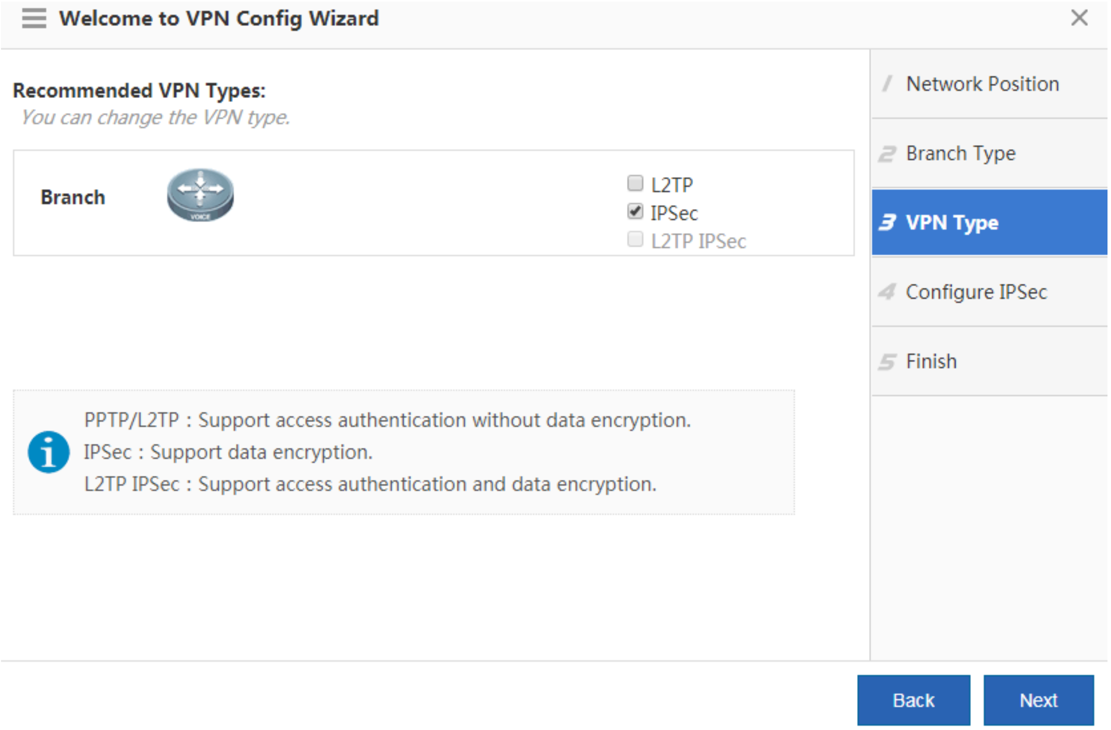
Welcome to VPN Config Wizard

Select a Branch Type:

□ Mobile User

☑ Branch

(3) Select **IPsec**, and click **Next**.



Welcome to VPN Config Wizard

Recommended VPN Types:

You can change the VPN type.

Branch

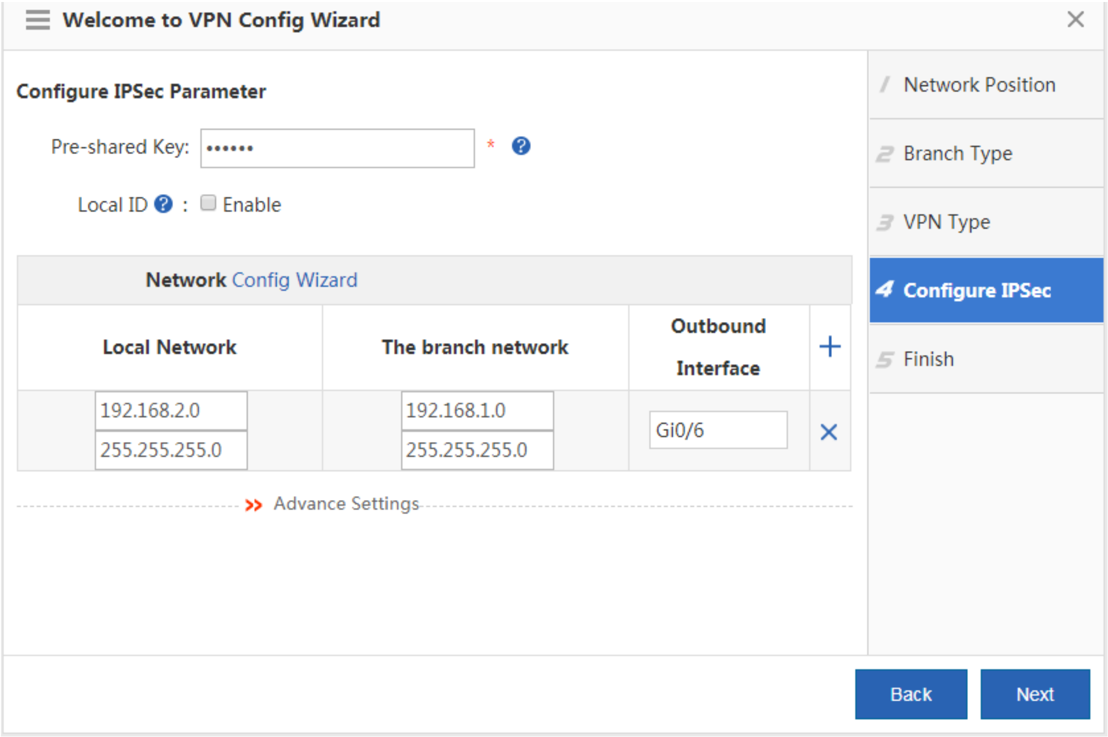
□ L2TP
☑ IPSec
□ L2TP IPSec

PPTP/L2TP : Support access authentication without data encryption.

IPSec : Support data encryption.

L2TP IPSec : Support access authentication and data encryption.

(4) Configure IPsec basic information, and click **Next**.



Welcome to VPN Config Wizard

Configure IPSec Parameter

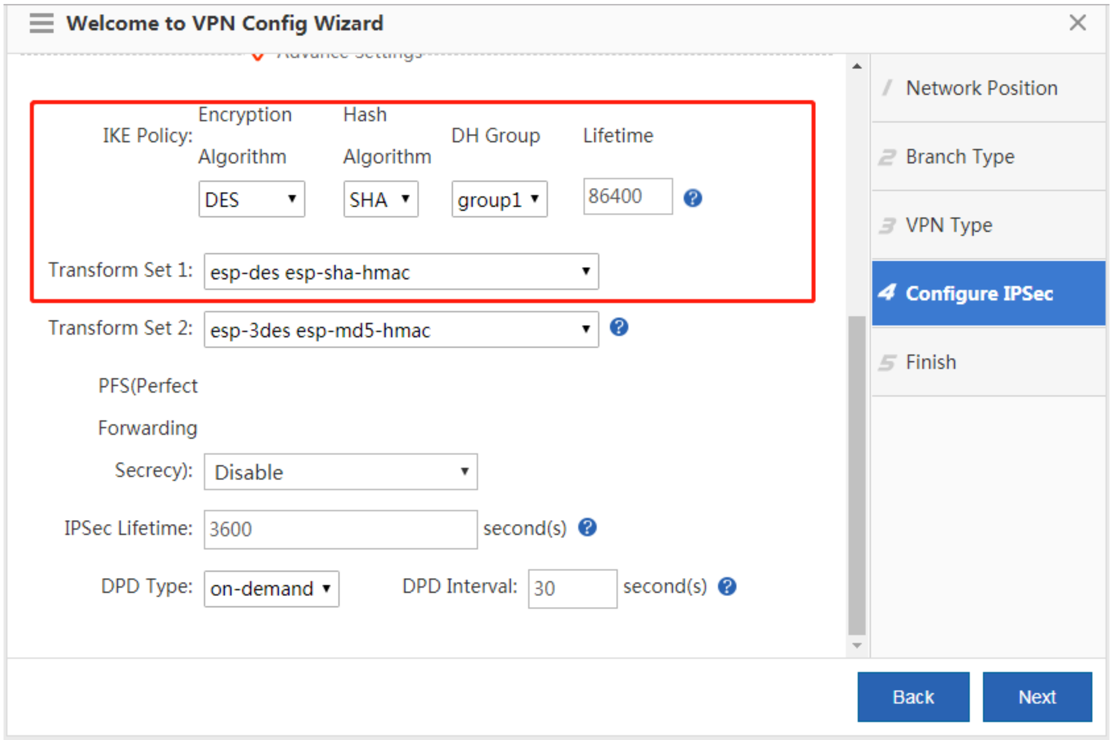
Pre-shared Key: •••••• *

Local ID : □ Enable

Network Config Wizard

Local Network	The branch network	Outbound Interface
192.168.2.0 255.255.255.0	192.168.1.0 255.255.255.0	Gi0/6

» Advance Settings



IKE Policy: Encryption Algorithm DES; Hash Algorithm SHA; DH Group group1; Lifetime 86400

Transform Set 1: esp-des esp-sha-hmac

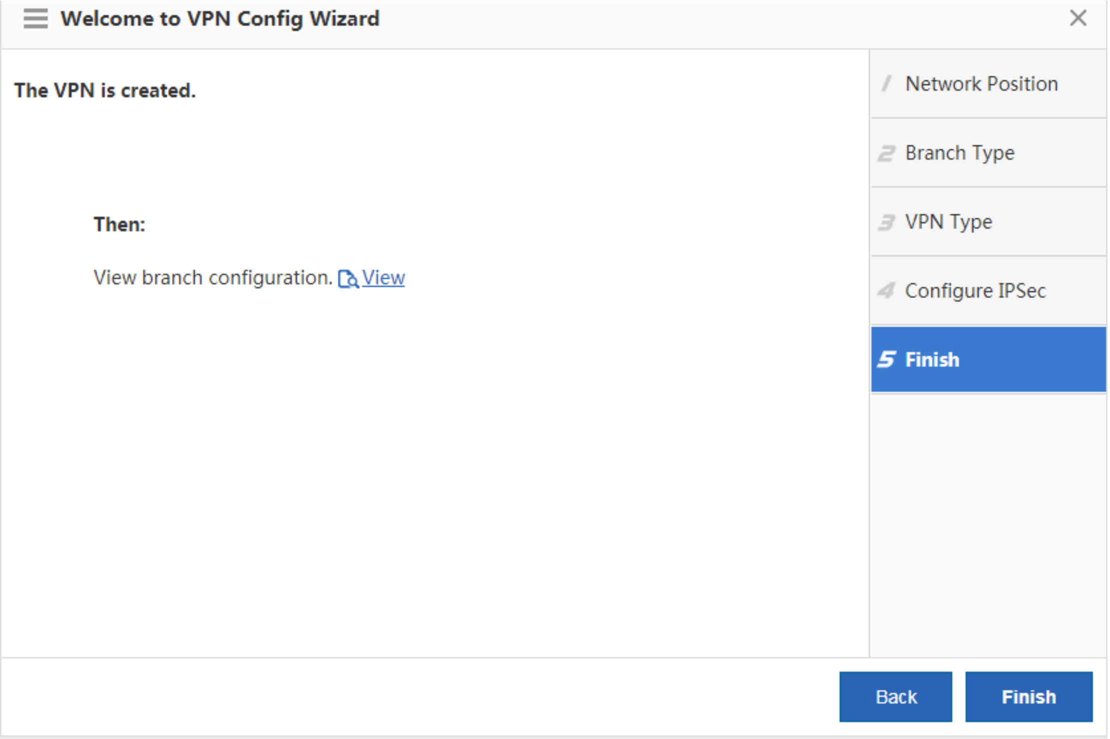
Transform Set 2: esp-3des esp-md5-hmac

PFS(Perfect Forwarding Secrecy): Disable

IPSec Lifetime: 3600 second(s)

DPD Type: on-demand DPD Interval: 30 second(s)

(5) Click **Finish**.



The VPN is created.

Then:

View branch configuration. View

4. IPsec uses UDP ports 500 and 4500. Map UDP ports 500 and 4500 on the egress of the HQ respectively to UDP ports 500 and 4500 of the LAN EG device.

(1) Map UDP port 500.

```
ip nat inside source static udp 10.0.0.1 500 1.1.1.1 500
```

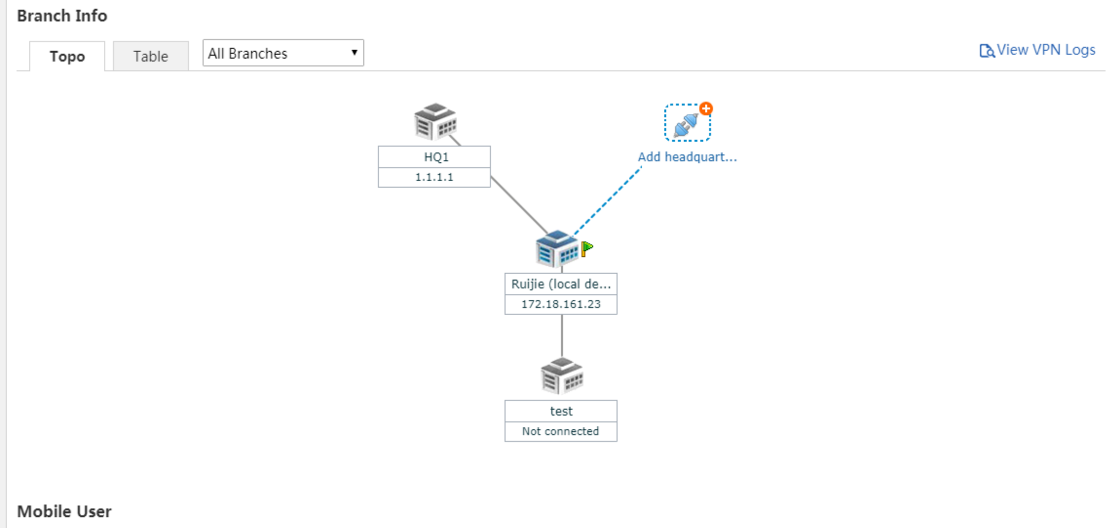
(2) Map UDP port 4500.

```
ip nat inside source static udp 10.0.0.1 4500 1.1.1.1 4500
```

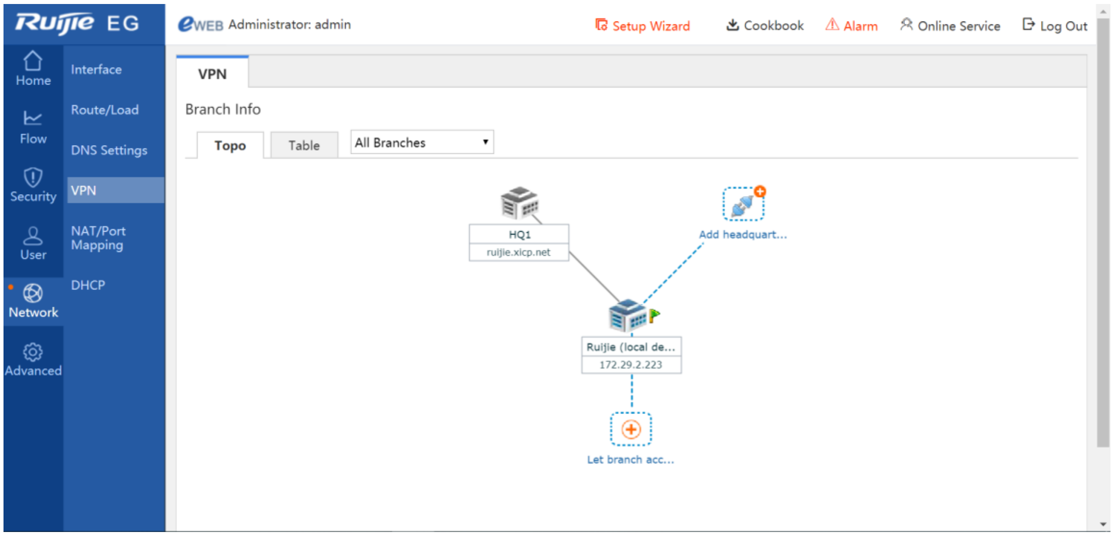
Configuration Verification

Choose **Network** > **VPN**, and click the **Topo** tab to view the configuration.

Configuration of the HQ router:



Configuration of the branch router:



Check whether the HQ router and branch router can access each other.

5.9 Local Web Authenticaiton

Networking Requirements

1. LAN users access the Internet through the EG device.

2. The WAN bandwidth is 10 Mbps, the address of the WAN port is 192.168.33.56/24, the address of the WAN gateway is 192.168.33.1, and the addresses of LAN ports are in the 192.168.1.1/24 network segment.

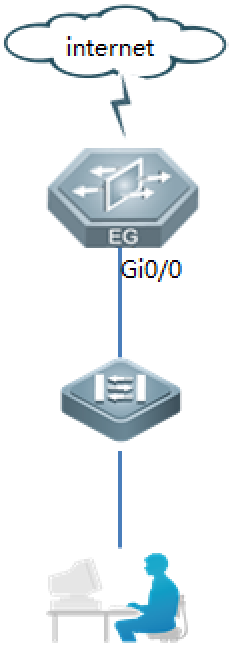
3. LAN users can access the WAN only after succeeding in identity authentication.

4. The EG device of RGOS10.3 (4B8) and later versions support subinterface Web authentication. The configuration method is the same as that of common Web authentication.

5. Internal Web authentication allows users to proactively add the go-offline page to favorites and modify passwords. It also supports the following functions: forbidding users from accessing the Internet (blocking user accounts) and kicking users offline.

Note: The IP addresses above are used in a simulated environment and are not provided by carriers.

Network Topology



Configuration Key Points

1. Perform wizard-based setup to ensure that LAN users can successfully access the WAN.

2. Select the internal Web authentication server function in the real-name Internet access policy.

Notes:

1. If advertisement push is enabled, the entered advertisement address cannot contain the character "?".

2. If Web authentication is enabled and port mapping is configured, the LAN server IP address used for port mapping needs to be added to the authentication-exempt IP address list. Otherwise, port mapping will fail.

3. After Web authentication is enabled, the remote login password (that is, telnet password) needs to be changed.

Auxiliary information:

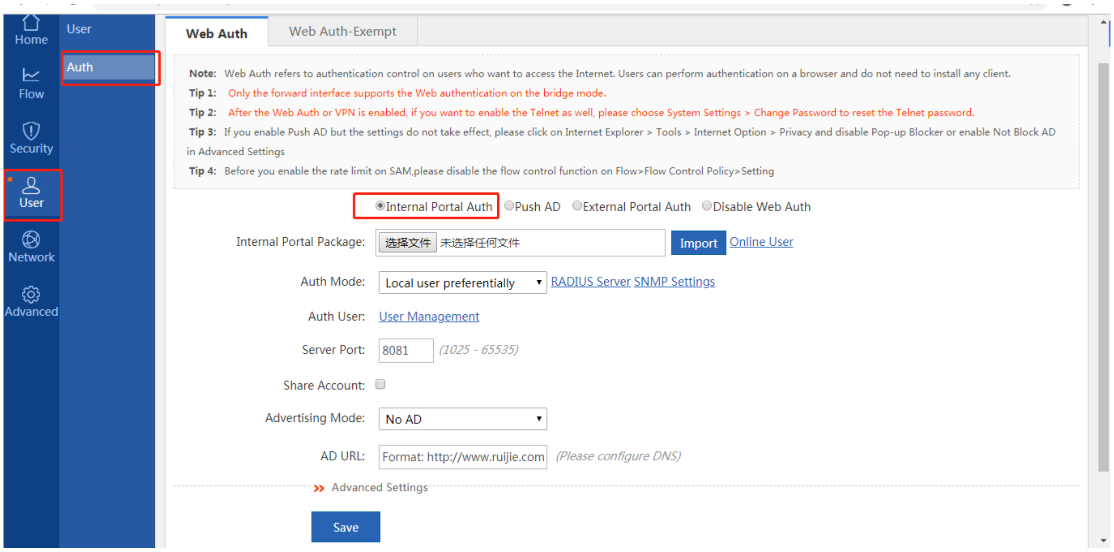
1. The Web authentication function of the EG device allows the Dynamic Host Configuration Protocol (DHCP), DNS, and Address Resolution Protocol (ARP) traffic to pass by default, without a need of additional settings.

2. When you log in to the EG device in telnet mode with Web authentication enabled, if you enter a wrong username or password for more than 3 consecutive times for the EG device of RGOS4B8 or 50 consecutive times for the EG device of RGOS4B10, the account will be locked. The account will be unlocked after 15 hours by default and then you can log in with the account again. You are recommended to run the following commands to modified two parameters after configuring Web authentication:

```
Ruijie(config)#aaa local authentication lockout-time 1     //Unlocking an account 1 hour after the account is locked
Ruijie(config)#aaa local authentication attempts 10     //Setting the allowable login attempts to 10.
```

Configuration Steps

Choose User > Auth and click Internal Portal Auth on the Web Auth tab page to enable the internal authentication function, as shown in the figure below.



Note: Web Auth refers to authentication control on users who want to access the Internet. Users can perform authentication on a browser and do not need to install any client.

Tip 1: Only the forward interface supports the Web authentication on the bridge mode.

Tip 2: After the Web Auth or VPN is enabled, if you want to enable the Telnet as well, please choose System Settings > Change Password to reset the Telnet password.

Tip 3: If you enable Push AD but the settings do not take effect, please click on Internet Explorer > Tools > Internet Option > Privacy and disable Pop-up Blocker or enable Not Block AD in Advanced Settings

Tip 4: Before you enable the rate limit on SAM,please disable the flow control function on Flow>Flow Control Policy>Setting

● Internal Portal Auth ○ Push AD ○ External Portal Auth ○ Disable Web Auth

Internal Portal Package: 选择文件 未选择任何文件

Auth Mode: Local user preferentially

Server Port: 8081 (1025 - 65535)

Share Account: □

Advertising Mode: No AD

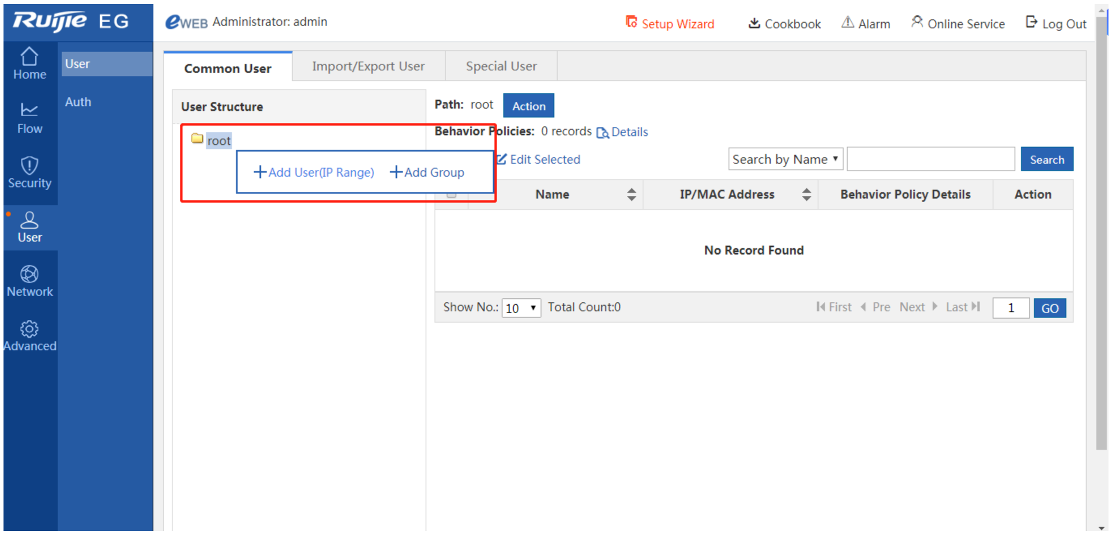
AD URL: Format: http://www.ruijie.com (Please configure DNS)

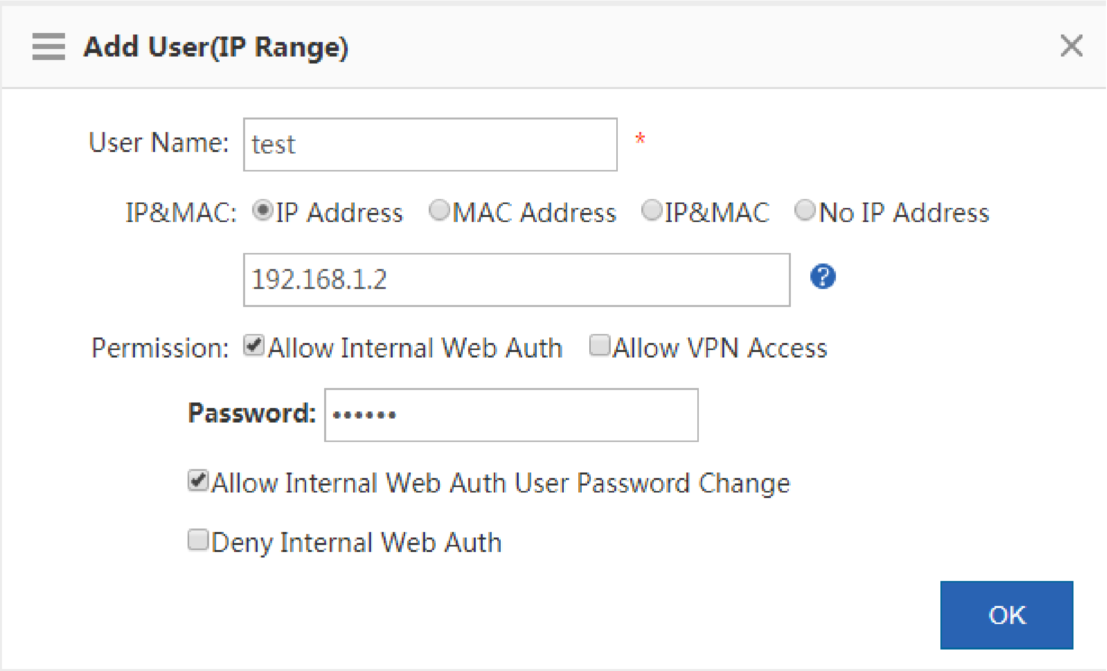
a. Internal Portal Auth: Refers to the internal authentication server of the EG device.

b. Auth Mode: A users needs to be authenticated before accessing the Internet. Specify the server matching priority for authentication information here.

c. Advertising Mode: Ruijie EG device provides the advertisement push function, for example, a hotel can use this function to push the hotel homepage to guests and promote the hotel brand. You can also set the mode to No AD, Display AD Before Auth, or Display AD After Auth.

Add a user to be authenticated: Click a user group in the user organization structure on the left, add a user (IP range) to the user group, and configure the username and password, as shown in the figure below.





Add User(IP Range)

User Name: test *

IP&MAC: ● IP Address ○ MAC Address ○ IP&MAC ○ No IP Address

192.168.1.2

Permission: ☑ Allow Internal Web Auth □ Allow VPN Access

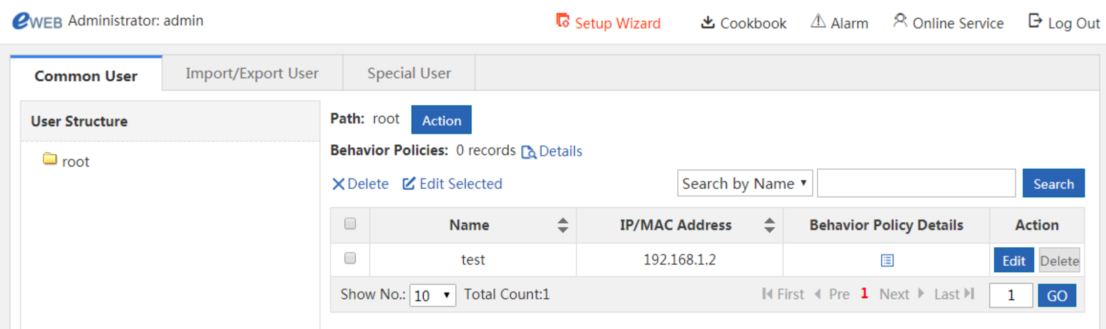
Password: ••••••

☑ Allow Internal Web Auth User Password Change

□ Deny Internal Web Auth

OK

A user added successfully is displayed in the user list, as shown in the figure below.



Path: root

Behavior Policies: 0 records

□	Name	IP/MAC Address	Behavior Policy Details	Action
□	test	192.168.1.2	▤	Edit Delete

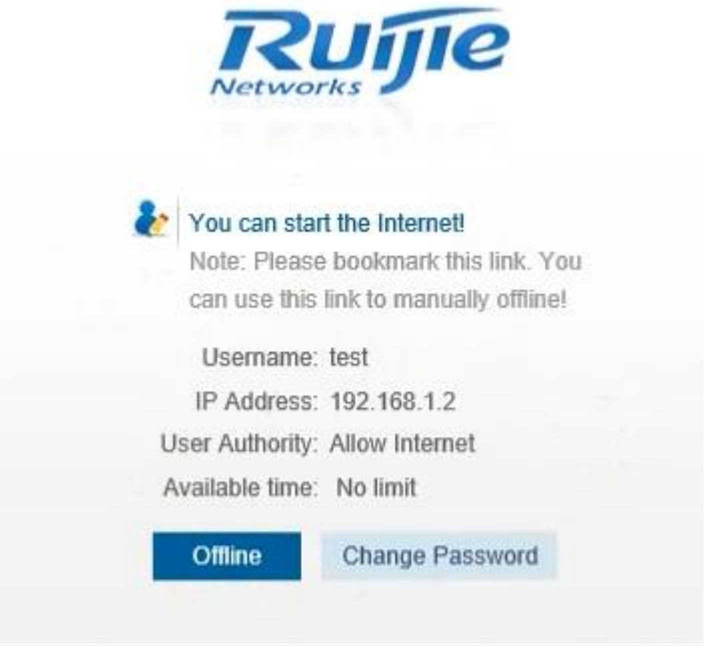
Show No.: 10 Total Count:1

The user configuration method on the CLI is as follows:

#Add a user named ruijie under the root directory, set the password to 111, and configure the account to use only Web authentication.

```
Ruijie(config)# subscriber static name "ruijie" parent "/" password 111
Ruijie(config)# subscriber allow "ruijie" privilege webauth
```

If you select Allow Internal Web Auth User Password Change when configuring a username and password. The Change Password option is displayed after Web authentication is successful.



You can start the Internet!

Note: Please bookmark this link. You can use this link to manually offline!

Username: test

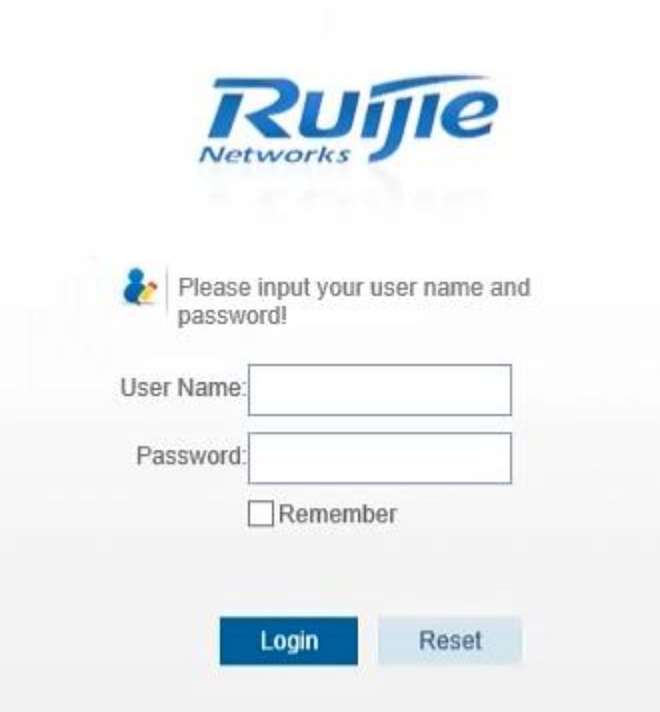
IP Address: 192.168.1.2

User Authority: Allow Internet

Available time: No limit

Configuration Verification

After the configuration is complete, the authentication page is displayed when a user browses a Web page for the first time.



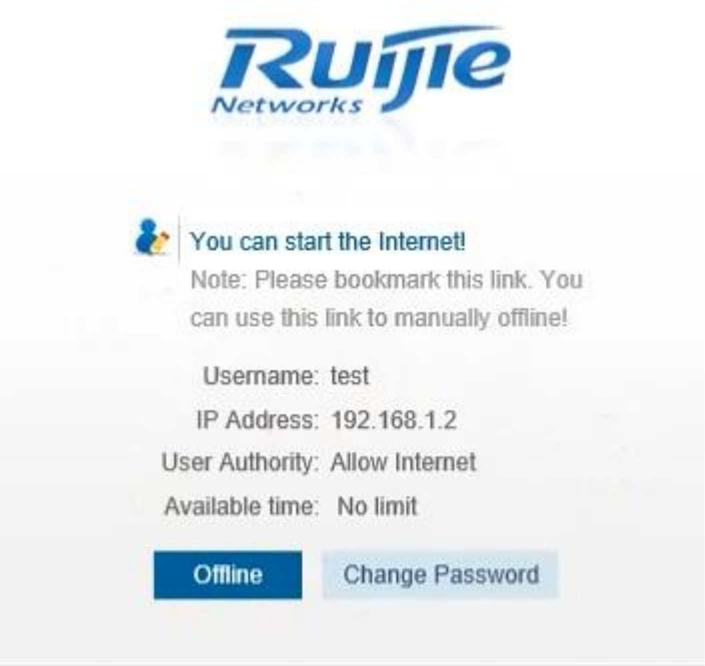
Please input your user name and password!

User Name:

Password:

□ Remember

Enter the correct username and password and click Login. The authentication success page is displayed.



You can start the Internet!

Note: Please bookmark this link. You can use this link to manually offline!

Username: test

IP Address: 192.168.1.2

User Authority: Allow Internet

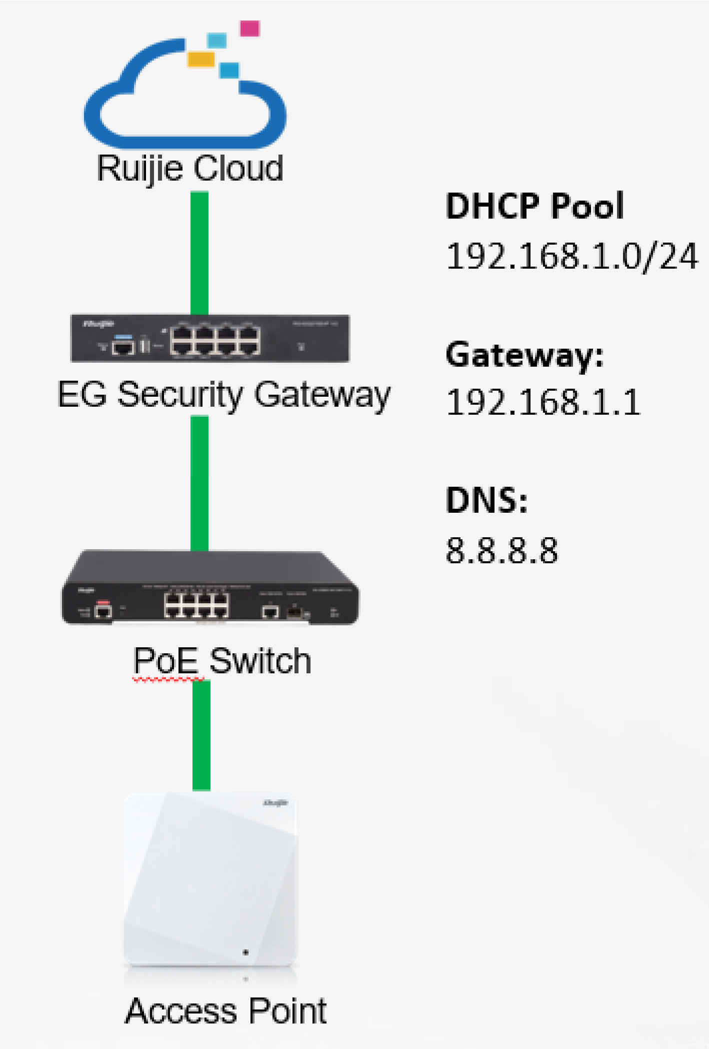
Available time: No limit

5.10 Voucher Authentication Acceleration

Voucher authentication on Ruijie Cloud allows you to charge users for wireless network access using access codes. Concurrent users, time period and data quota limit can be customized and offered to your guests.

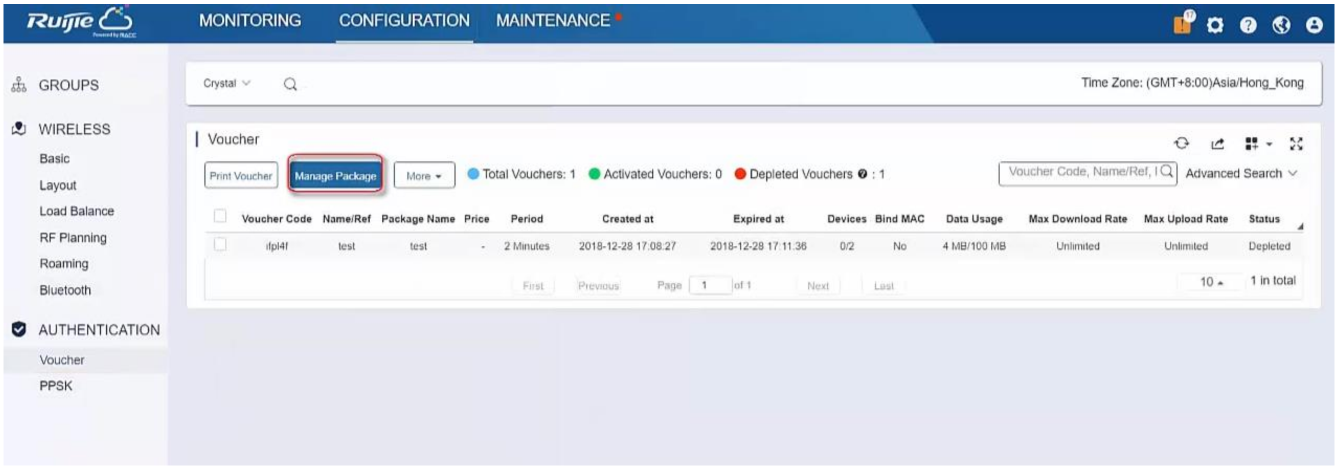
With EG and Ruijie Could integration, the voucher data can be synchronized from Cloud to local EG device. The authentication process will be accelerated significantly.

Network Topology



Configuration Steps

Step 1: Login to Ruijie Cloud and create the voucher package.



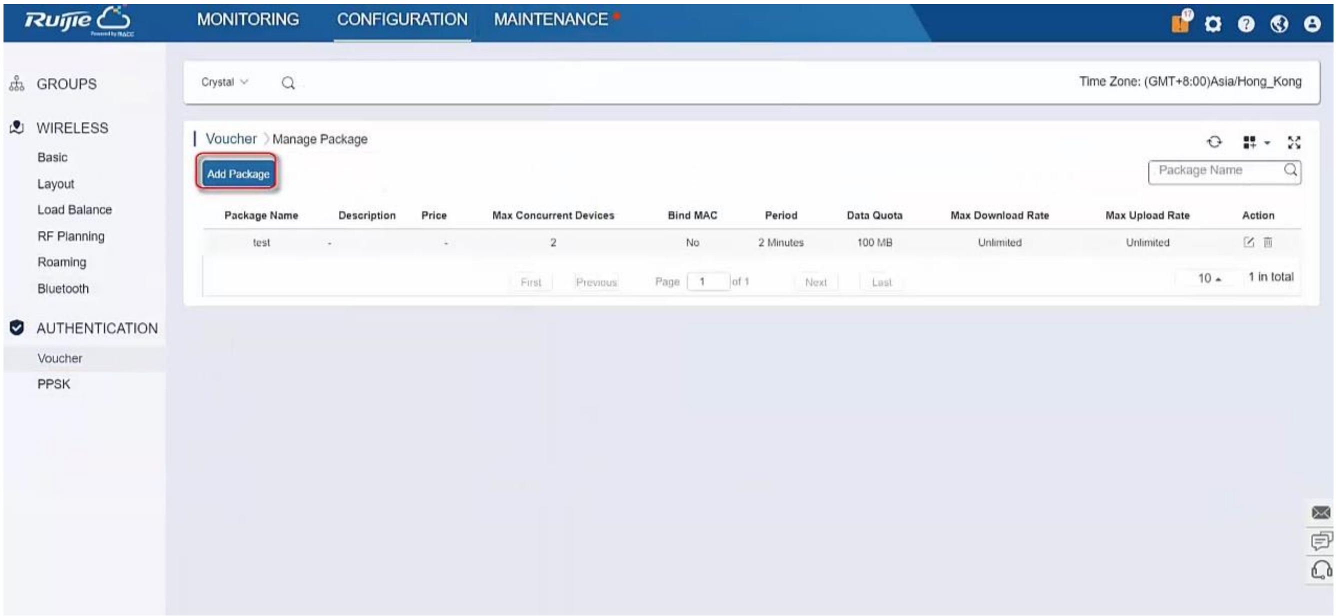
Time Zone: (GMT+8:00)Asia/Hong_Kong

Voucher

● Total Vouchers: 1 ● Activated Vouchers: 0 ● Depleted Vouchers : 1

□	Voucher Code	Name/Ref	Package Name	Price	Period	Created at	Expired at	Devices	Bind MAC	Data Usage	Max Download Rate	Max Upload Rate	Status
□	ifpl4f	test	test	-	2 Minutes	2018-12-28 17:08:27	2018-12-28 17:11:36	0/2	No	4 MB/100 MB	Unlimited	Unlimited	Depleted

First Previous Page 1 of 1 Next Last 10 1 in total

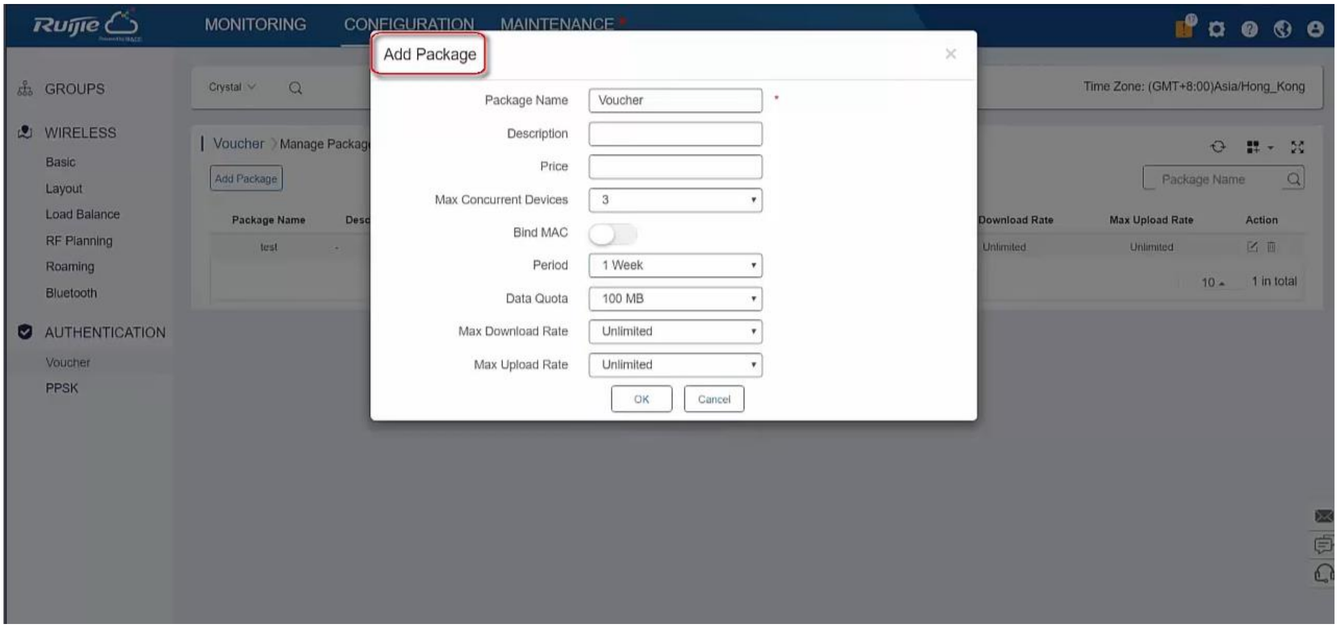


Time Zone: (GMT+8:00)Asia/Hong_Kong

Voucher > Manage Package

Package Name	Description	Price	Max Concurrent Devices	Bind MAC	Period	Data Quota	Max Download Rate	Max Upload Rate	Action
test	-	-	2	No	2 Minutes	100 MB	Unlimited	Unlimited	

First Previous Page 1 of 1 Next Last 10 1 in total



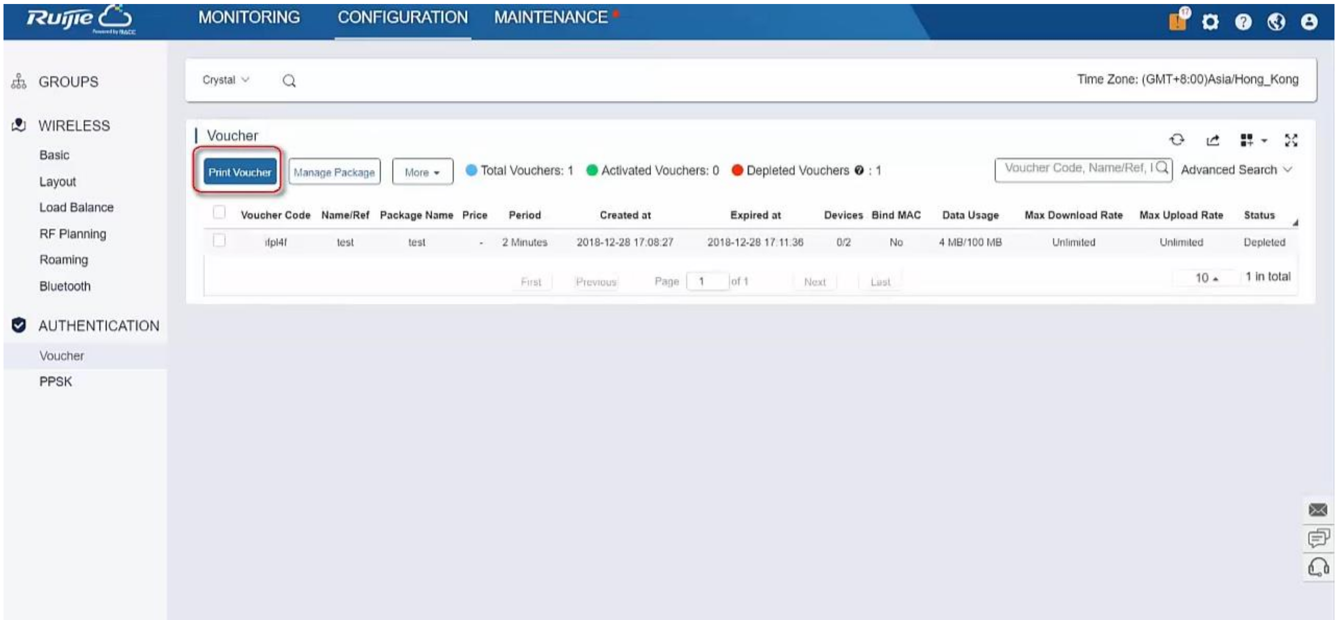
Add Package

Package Name	Voucher
Description	
Price	
Max Concurrent Devices	3
Bind MAC	
Period	1 Week
Data Quota	100 MB
Max Download Rate	Unlimited
Max Upload Rate	Unlimited

Package Name	Desc	Download Rate	Max Upload Rate	Action
test	-	Unlimited	Unlimited	

10 ▴ 1 in total

Step 2: Print voucher on Ruijie cloud.



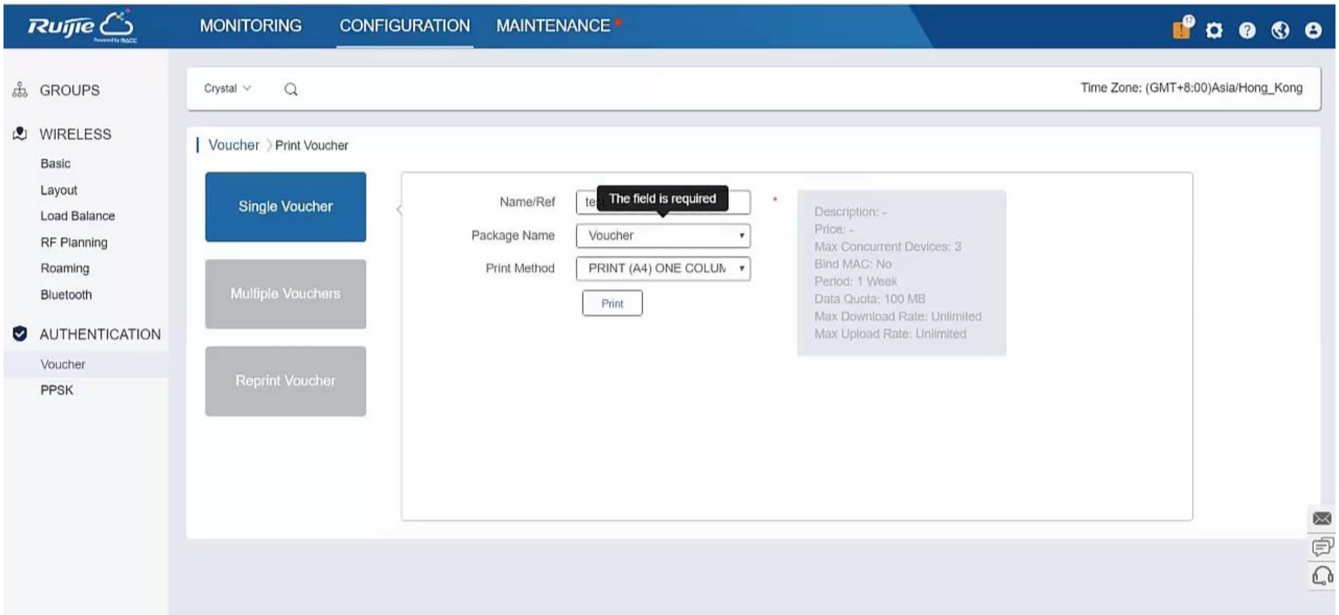
Time Zone: (GMT+8:00)Asia/Hong_Kong

Voucher

● Total Vouchers: 1 ● Activated Vouchers: 0 ● Depleted Vouchers : 1

Voucher Code	Name/Ref	Package Name	Price	Period	Created at	Expired at	Devices	Bind MAC	Data Usage	Max Download Rate	Max Upload Rate	Status
ifpl4f	test	test	-	2 Minutes	2018-12-28 17:08:27	2018-12-28 17:11:36	0/2	No	4 MB/100 MB	Unlimited	Unlimited	Depleted

Page 1 of 1 10 ▴ 1 in total



Time Zone: (GMT+8:00)Asia/Hong_Kong

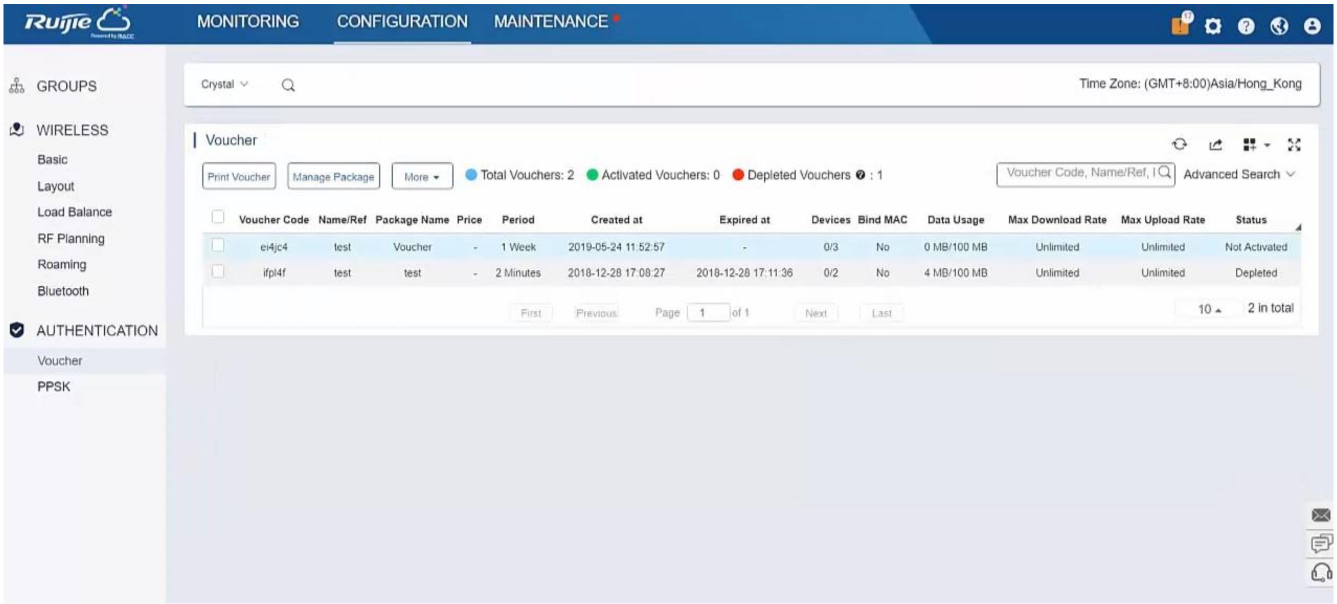
Voucher > Print Voucher

Name/Ref: te The field is required *

Package Name: Voucher

Print Method: PRINT (A4) ONE COLUM

Description: -
Price: -
Max Concurrent Devices: 3
Bind MAC: No
Period: 1 Week
Data Quota: 100 MB
Max Download Rate: Unlimited
Max Upload Rate: Unlimited



Time Zone: (GMT+8:00)Asia/Hong_Kong

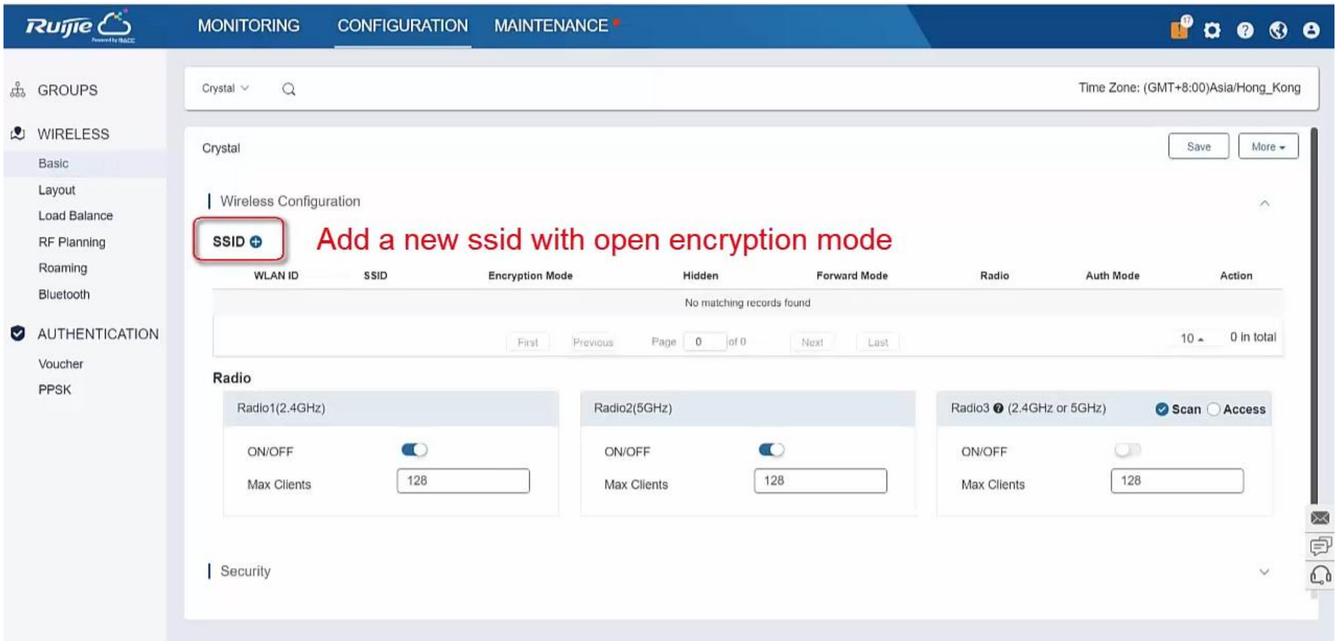
Voucher

● Total Vouchers: 2 ● Activated Vouchers: 0 ● Depleted Vouchers : 1

□	Voucher Code	Name/Ref	Package Name	Price	Period	Created at	Expired at	Devices	Bind MAC	Data Usage	Max Download Rate	Max Upload Rate	Status
□	ei4jc4	test	Voucher	-	1 Week	2019-05-24 11:52:57	-	0/3	No	0 MB/100 MB	Unlimited	Unlimited	Not Activated
□	ifpl4f	test	test	-	2 Minutes	2018-12-28 17:08:27	2018-12-28 17:11:36	0/2	No	4 MB/100 MB	Unlimited	Unlimited	Depleted

Page 1 of 1 10 2 in total

Step 3: Enable the open authentication on AP connected to EG.



Crystal

Time Zone: (GMT+8:00)Asia/Hong_Kong

Wireless Configuration

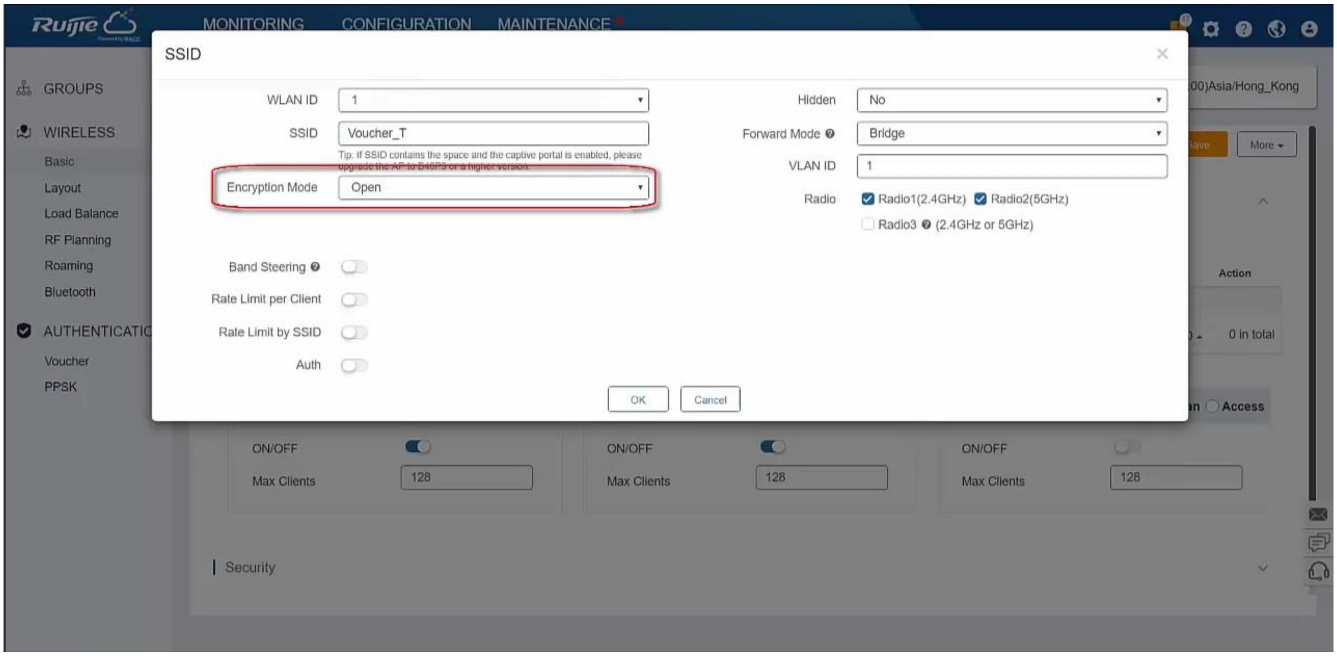
Add a new ssid with open encryption mode

WLAN ID	SSID	Encryption Mode	Hidden	Forward Mode	Radio	Auth Mode	Action
No matching records found							

Page 0 of 0 — 10 — 0 in total

Radio

Radio1(2.4GHz)		Radio2(5GHz)		Radio3 (2.4GHz or 5GHz) ☑ Scan ○ Access	
ON/OFF	on	ON/OFF	on	ON/OFF	off
Max Clients	128	Max Clients	128	Max Clients	128



SSID

WLAN ID: 1

SSID: Voucher_T

Tip: If SSID contains the space and the captive portal is enabled, please upgrade the AP to B46P3 or a higher version.

Encryption Mode: Open

Band Steering: off

Rate Limit per Client: off

Rate Limit by SSID: off

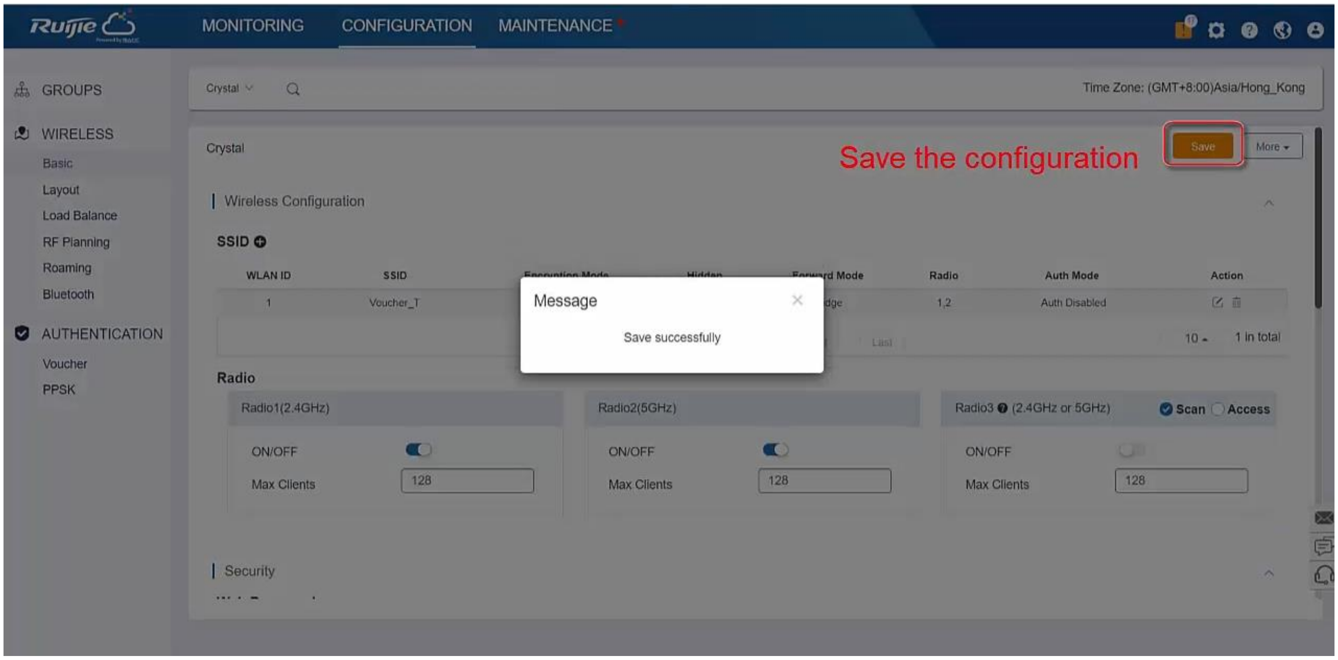
Auth: off

Hidden: No

Forward Mode: Bridge

VLAN ID: 1

Radio: ☑ Radio1(2.4GHz) ☑ Radio2(5GHz) □ Radio3 (2.4GHz or 5GHz)



Time Zone: (GMT+8:00)Asia/Hong_Kong

Save the configuration

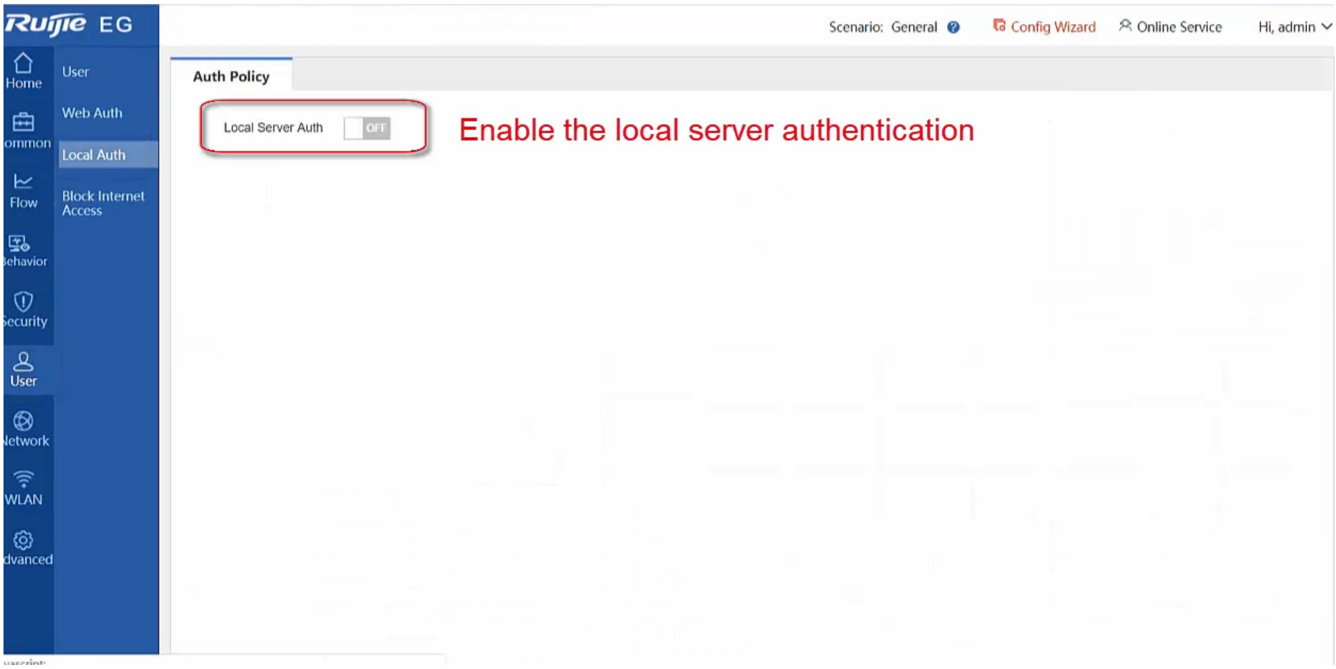
WLAN ID	SSID	Encryption Mode	Hidden	Forward Mode	Radio	Auth Mode	Action
1	Voucher_T			...dge	1,2	Auth Disabled	

Message

Save successfully

Radio1(2.4GHz)		Radio2(5GHz)		Radio3 (2.4GHz or 5GHz) ☑ Scan ○ Access	
ON/OFF	ON	ON/OFF	ON	ON/OFF	OFF
Max Clients	128	Max Clients	128	Max Clients	128

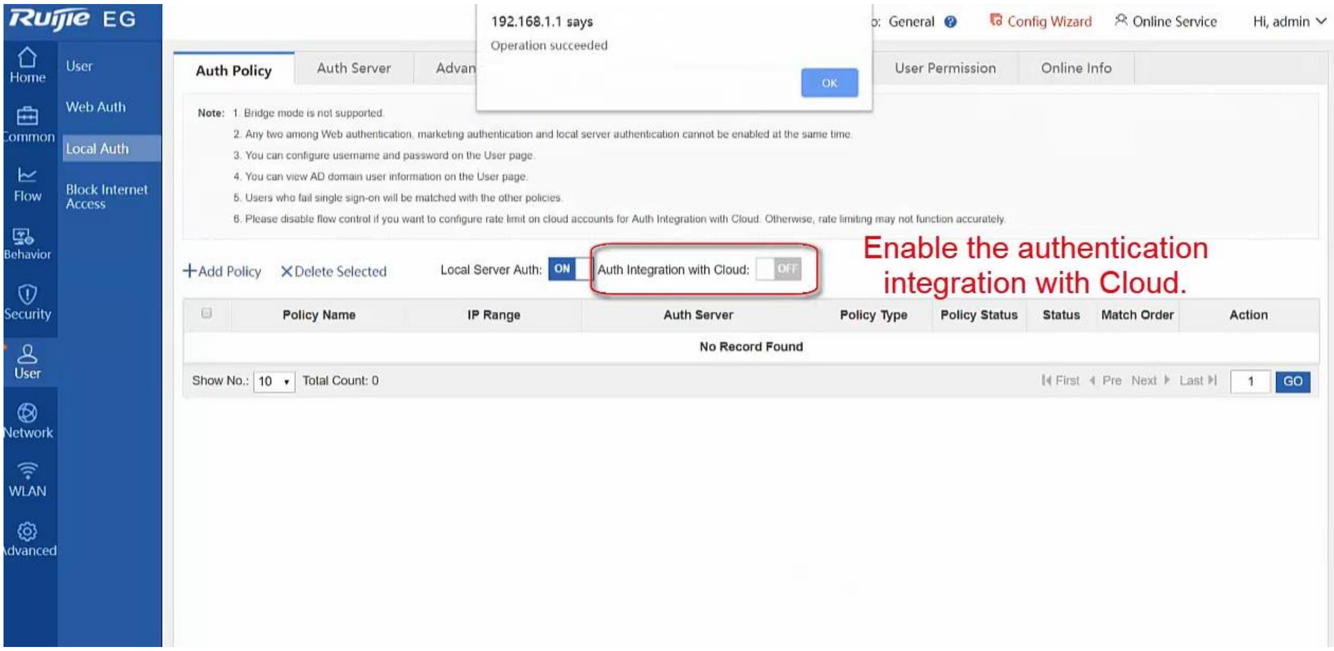
Step 4: Enable the local authentication on EG.



Local Server Auth OFF

Enable the local server authentication

Step 5: Enable the authentication integration with Cloud on EG.



192.168.1.1 says

Operation succeeded

OK

Note: 1. Bridge mode is not supported.
2. Any two among Web authentication, marketing authentication and local server authentication cannot be enabled at the same time.
3. You can configure username and password on the User page.
4. You can view AD domain user information on the User page.
5. Users who fail single sign-on will be matched with the other policies.
6. Please disable flow control if you want to configure rate limit on cloud accounts for Auth Integration with Cloud. Otherwise, rate limiting may not function accurately.

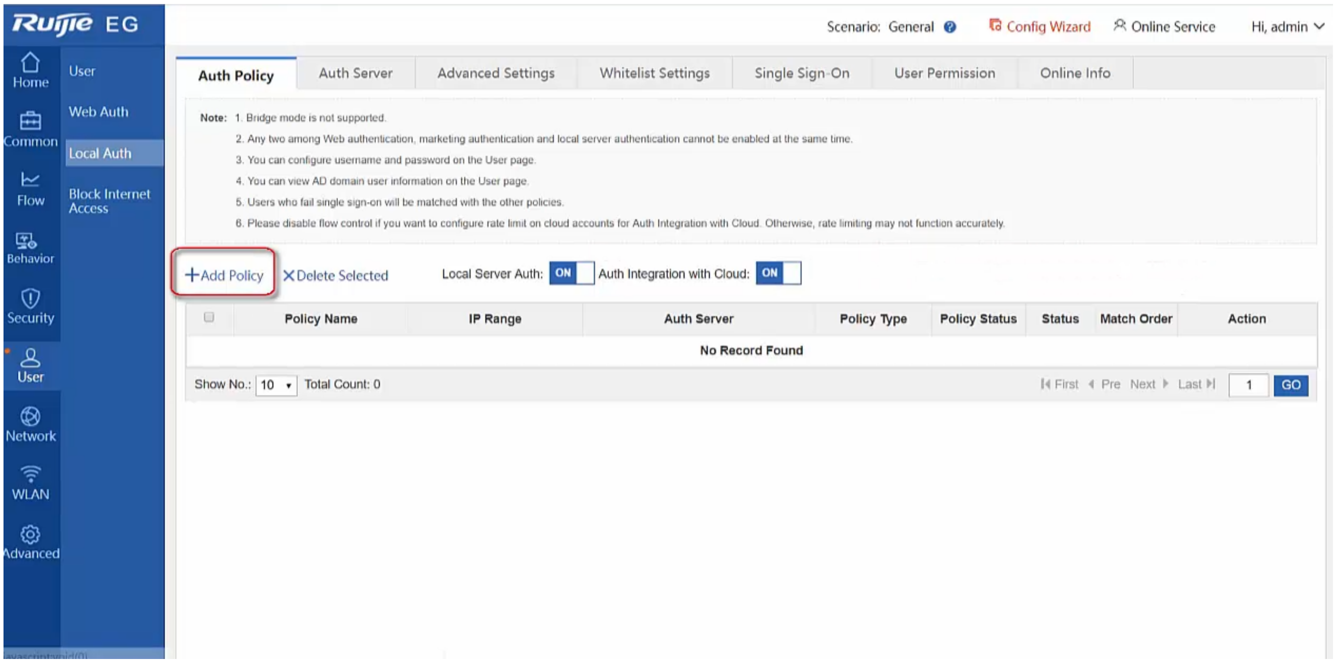
Local Server Auth: ON

Auth Integration with Cloud: OFF

Enable the authentication integration with Cloud.

□	Policy Name	IP Range	Auth Server	Policy Type	Policy Status	Status	Match Order	Action
No Record Found								

Step 6: Add the authentication IP range for voucher authentication on EG.

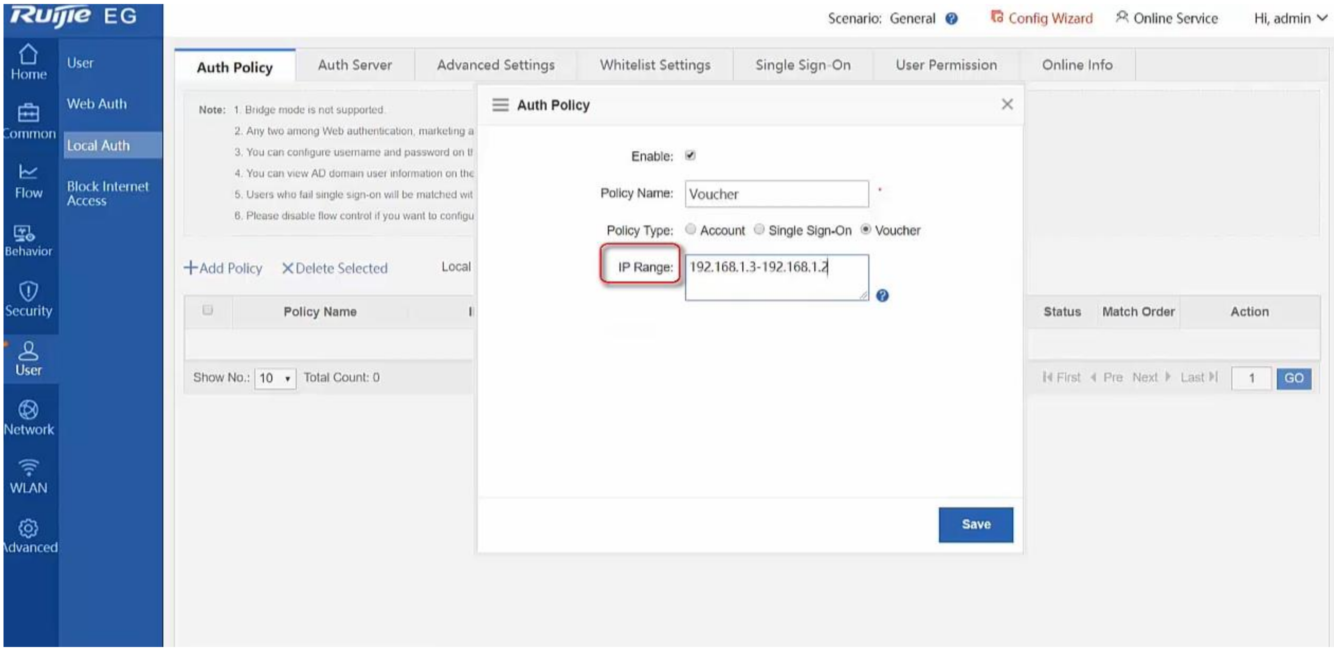


Note: 1. Bridge mode is not supported.
2. Any two among Web authentication, marketing authentication and local server authentication cannot be enabled at the same time.
3. You can configure username and password on the User page.
4. You can view AD domain user information on the User page.
5. Users who fail single sign-on will be matched with the other policies.
6. Please disable flow control if you want to configure rate limit on cloud accounts for Auth Integration with Cloud. Otherwise, rate limiting may not function accurately.

Local Server Auth: ON

Auth Integration with Cloud: ON

□	Policy Name	IP Range	Auth Server	Policy Type	Policy Status	Status	Match Order	Action
No Record Found								



Note: 1. Bridge mode is not supported.
2. Any two among Web authentication, marketing a
3. You can configure username and password on tl
4. You can view AD domain user information on the
5. Users who fail single sign-on will be matched wit
6. Please disable flow control if you want to configu

Show No.: 10 Total Count: 0

Auth Policy

Enable: ☑

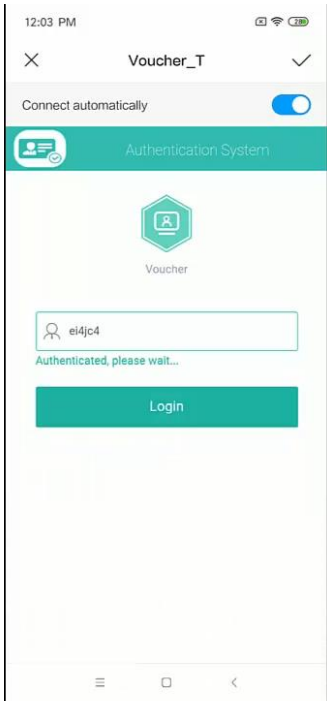
Policy Name: Voucher *

Policy Type: ○ Account ○ Single Sign-On ● Voucher

IP Range: 192.168.1.3-192.168.1.2

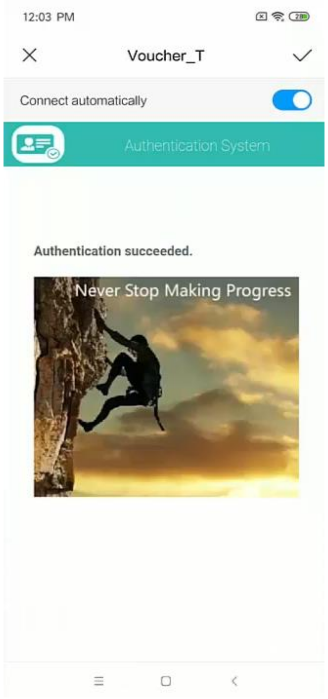
Configuration Verfication

Connect to the SSID and the authentication page will pop up.



ei4jc4

Authenticated, please wait...



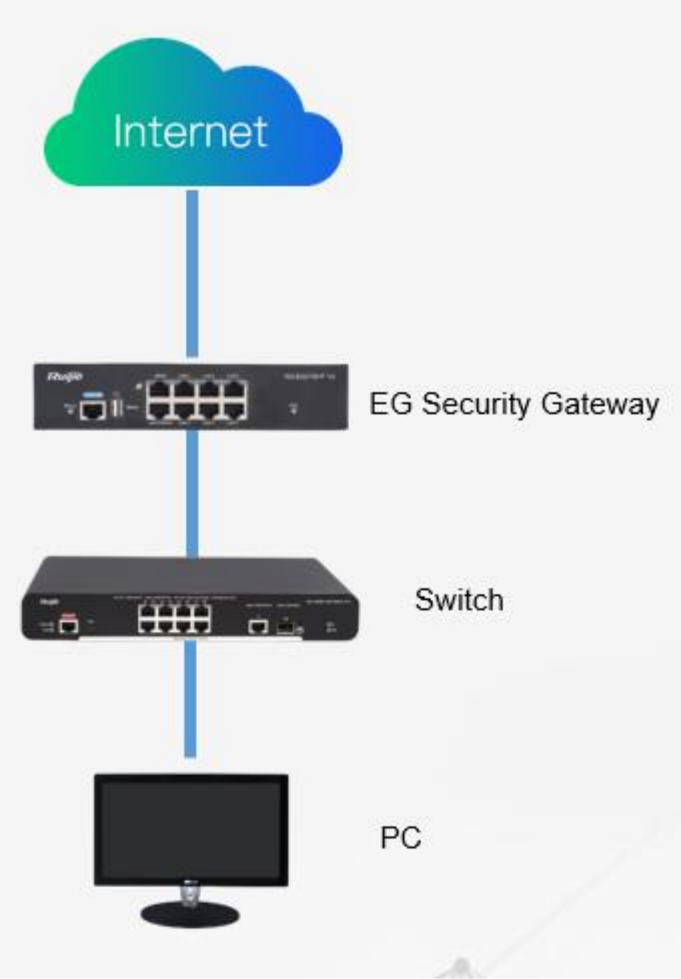
Authentication succeeded.

5.11 Resource Cache

Resource cache refers to synchronizing resource from the specified server to a device. Afterwards, users can get the resource directly from the device without crossing WAN.

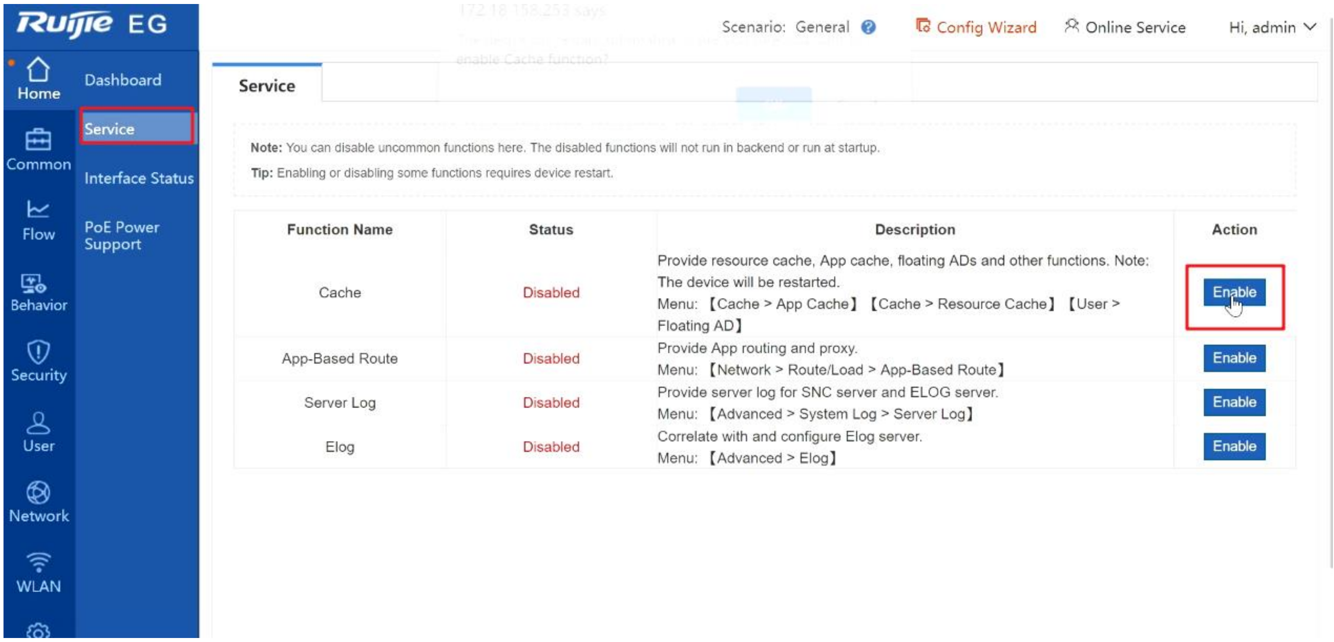
Resource cache can reduce bandwidth usage and save users from waiting for access.

Network Topology



Configuration Steps:

Step 1: Enable the cache function, the device will be restarted:



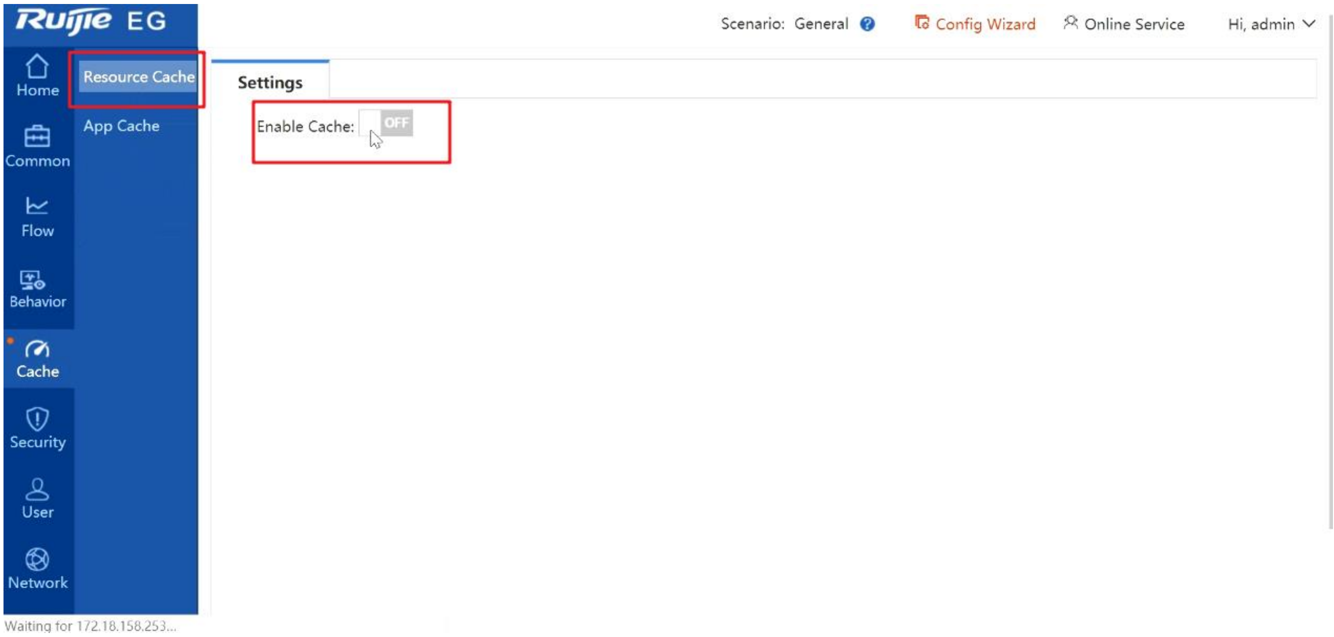
Service

Note: You can disable uncommon functions here. The disabled functions will not run in backend or run at startup.

Tip: Enabling or disabling some functions requires device restart.

Function Name	Status	Description	Action
Cache	Disabled	Provide resource cache, App cache, floating ADs and other functions. Note: The device will be restarted. Menu: 【Cache > App Cache】【Cache > Resource Cache】【User > Floating AD】	Enable
App-Based Route	Disabled	Provide App routing and proxy. Menu: 【Network > Route/Load > App-Based Route】	Enable
Server Log	Disabled	Provide server log for SNC server and ELOG server. Menu: 【Advanced > System Log > Server Log】	Enable
Elog	Disabled	Correlate with and configure Elog server. Menu: 【Advanced > Elog】	Enable

Step 2: Enable resource cache:

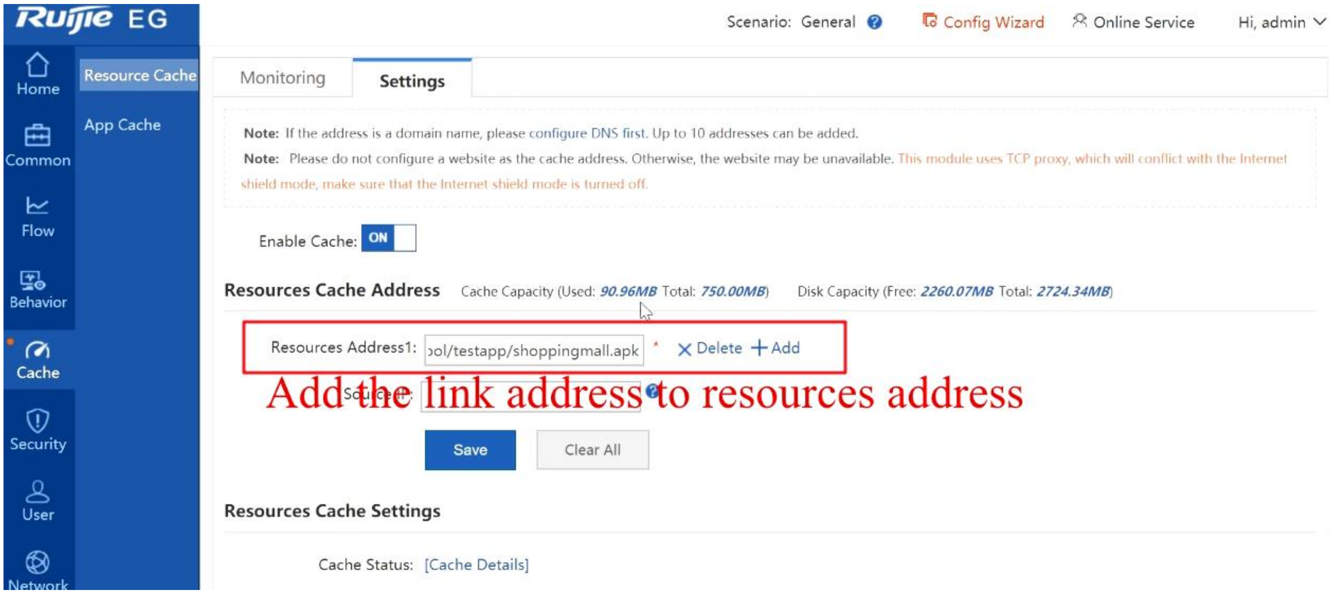


Settings

Enable Cache: OFF

Waiting for 172.18.158.253...

Step 3: Paste the download link of the resource to the “Resources Address1”:



Note: If the address is a domain name, please configure DNS first. Up to 10 addresses can be added.

Note: Please do not configure a website as the cache address. Otherwise, the website may be unavailable. This module uses TCP proxy, which will conflict with the Internet shield mode, make sure that the Internet shield mode is turned off.

Enable Cache: ON

Resources Cache Address Cache Capacity (Used: 90.96MB Total: 750.00MB) Disk Capacity (Free: 2260.07MB Total: 2724.34MB)

Resources Address1: ›ol/testapp/shoppingmall.apk * × Delete + Add

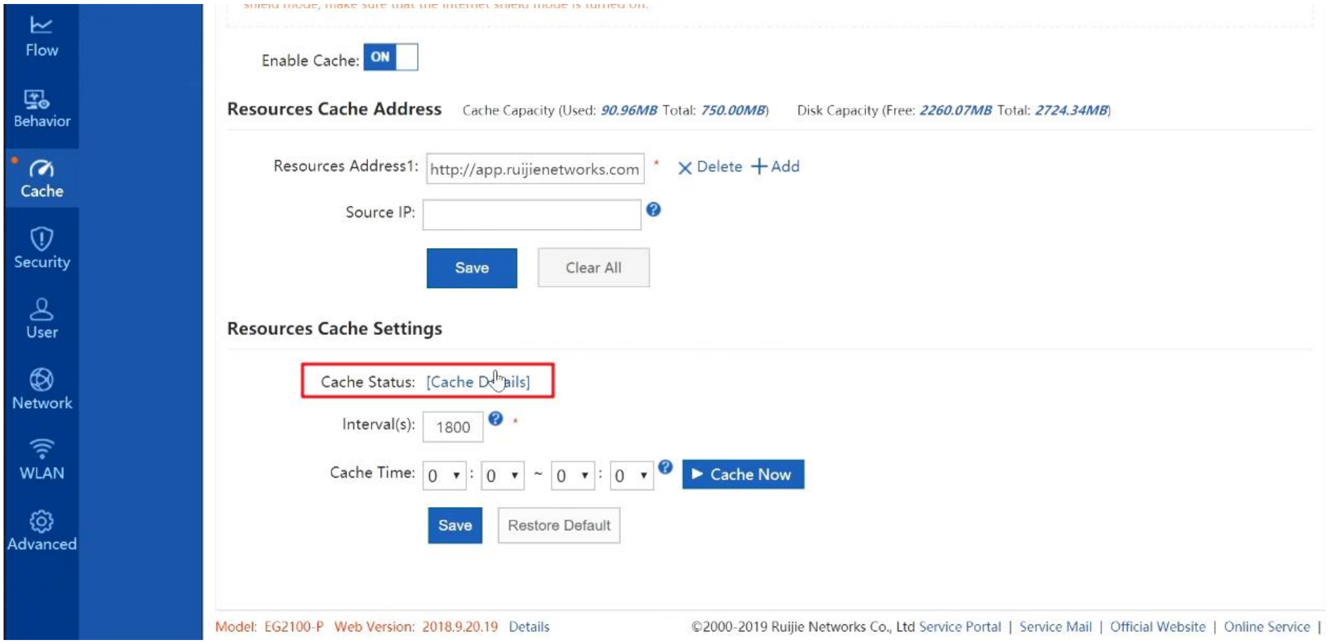
Add the link address to resources address

Save Clear All

Resources Cache Settings

Cache Status: [Cache Details]

Step 4: Check the cache file:



Enable Cache: ON

Resources Cache Address Cache Capacity (Used: 90.96MB Total: 750.00MB) Disk Capacity (Free: 2260.07MB Total: 2724.34MB)

Resources Address1: http://app.ruijienetworks.com * × Delete + Add

Source IP:

Save Clear All

Resources Cache Settings

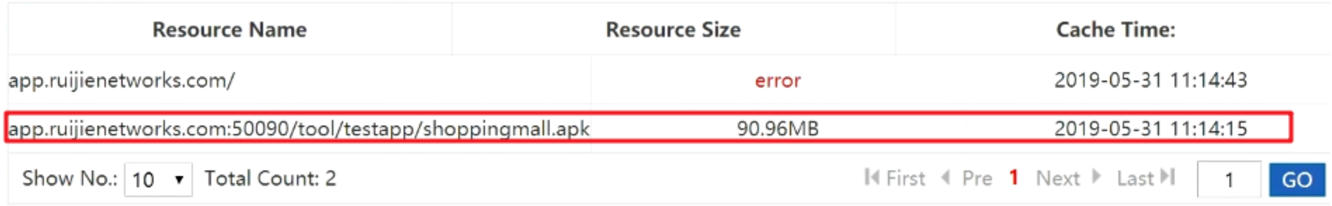
Cache Status: [Cache Details]

Interval(s): 1800 *

Cache Time: 0 : 0 ~ 0 : 0 ▶ Cache Now

Save Restore Default

Model: EG2100-P Web Version: 2018.9.20.19 Details ©2000-2019 Ruijie Networks Co., Ltd Service Portal | Service Mail | Official Website | Online Service |

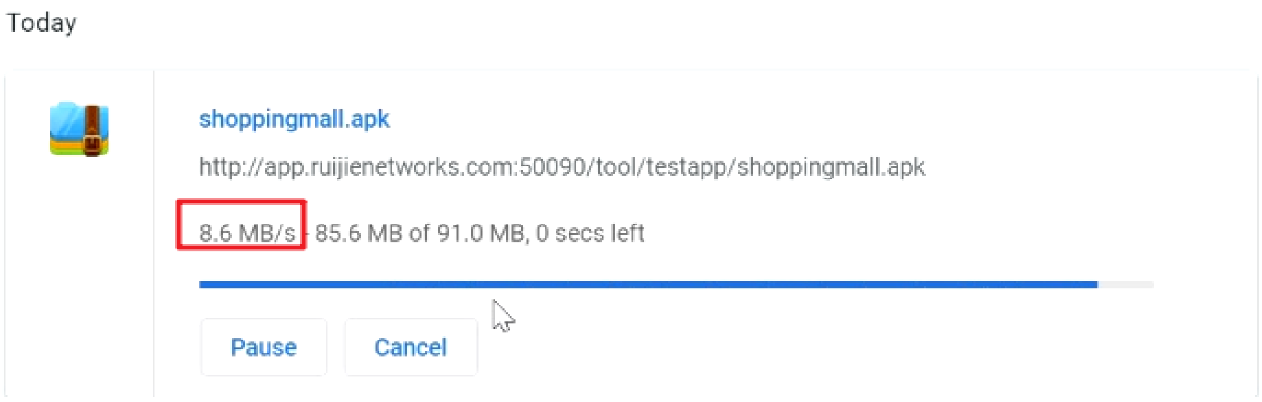


Resource Name	Resource Size	Cache Time:
app.ruijienetworks.com/	error	2019-05-31 11:14:43
app.ruijienetworks.com:50090/tool/testapp/shoppingmall.apk	90.96MB	2019-05-31 11:14:15

Show No.: 10 ▾ Total Count: 2 First Pre 1 Next Last 1 GO

Configuration Verification

Download the file via browser:



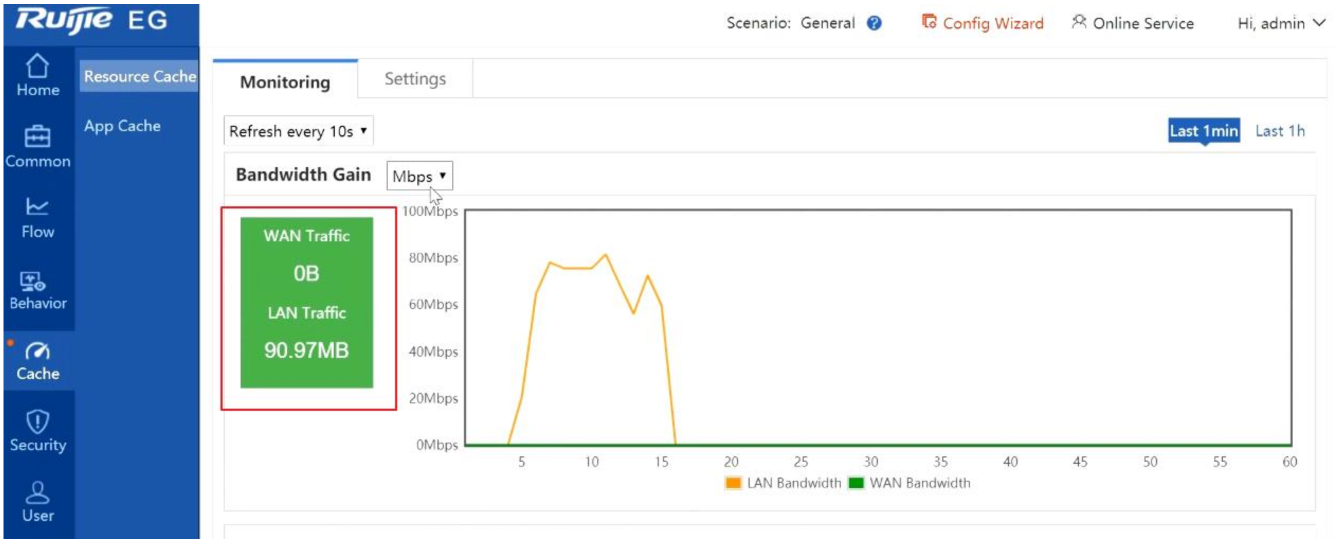
Today

shoppingmall.apk

http://app.ruijienetworks.com:50090/tool/testapp/shoppingmall.apk

8.6 MB/s - 85.6 MB of 91.0 MB, 0 secs left

The file is downloaded within the LAN.



WAN Traffic: 0B

LAN Traffic: 90.97MB