Ruijie Reyee RG-NBR-E Series Routers

Cookbook

Document Version: V1.0
Date: November 1, 2022

Copyright

Disclaimer

The products, services, or features you purchase are subject to commercial contracts and terms. Some or all of the products, services or features described in this document may not be within the scope of your purchase or use. Unless otherwise agreed in the contract, Ruijie Networks does not make any express or implied statement or guarantee for the content of this document.

Due to product version upgrades or other reasons, the content of this document will be updated from time to time. Ruijie Networks reserves the right to modify the content of the document without any notice or prompt.

This manual is for reference only. 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.

Preface

Intended Audience

This document is intended for:

- Network engineers
- Technical support and service engineers
- Network administrators

Technical Support

- Official website of Ruijie Reyee: https://www.ruijienetworks.com/products/reyee
- Technical Support Website: https://ruijienetworks.com/support
- Case Portal: https://caseportal.ruijienetworks.com
- Community: https://community.ruijienetworks.com
- Technical Support Email: service_rj@ruijienetworks.com

Conventions

1. GUI Symbols

Interface symbol	Description	Example
Boldface	1. Button names 2. Window names, tab name, field name and menu items 3. Link	1. Click **OK**. 2. Select **Config Wizard**. 3. Click the **Download File** link.
>	Multi-level menus items	Select **System** > **Time**.

2. Signs

The signs used in this document are described as follows:

Warning

An alert that calls attention to important rules and information that if not understood or followed can result in data loss or equipment damage.

Caution

An alert that calls attention to essential information that if not understood or followed can result in function failure or performance degradation.

Note

An alert that contains additional or supplementary information that if not understood or followed will not lead to serious consequences.

Specification

An alert that contains a description of product or version support.

3. Note

This manual is used to guide users to understand the product, install the product, and complete the configuration.

- The example of the port type may be different from the actual situation. Proceed with the configuration according to the port type supported by the product.
- The example of display information may contain the content of other product series (such as model and description). Refer to the actual display information.
- The router and router product icons involved in this manual represent common routers and Layer 3 switches running routing protocols.

Contents

1 Overview

1.1 Introduction

RG-NBR-E series enterprise-class routers are multi-service integrated routers tailored by Ruijie Reyee for integrated scenarios such as office, hotel, restaurant, entertainment, and scenic spot. RG-NBR-E series enterprise-class routers support many functions such as service acceleration channel, precise flow control, network access behavior management, VPN total-division interconnection, and intelligent routing, and support connection to Ruijie cloud platform (MACC free cloud platform) for remote cloud O&M and central management, which can well meet the integrated network needs of scenarios such as office, hotel, restaurant, entertainment, and scenic spot.

RG-NBR-E series enterprise-class routers support the web management GUI. The web management system can be used to configure and manage the common functions of the devices.

1.2 Specifications of Ruijie RG-NBR-E Series Routers

1.2.1 Ruijie RG-NBR6120-E Router

1. Appearance of Ruijie RG-NBR6120-E Router

Figure 1-1 Front Panel of Ruijie RG-NBR6120-E Router

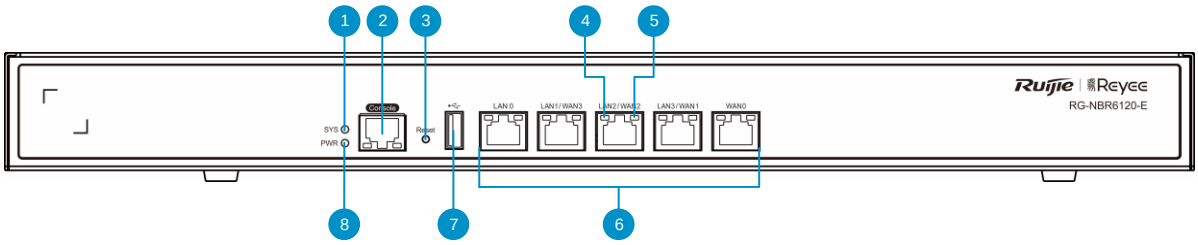


Table 1-1 Description of the Front Panel of Ruijie RG-NBR6210-E Router

No.	Indicator/Port	Description
1	SYS	System indicator: ● If it blinks green, the system is being initialized. ● If it is steady green, system initialization is completed.
2	Console	Console port. It connects to the console cable. After connecting to the serial port of the management PC, the device can be managed through the console port.
3	Reset	Restarts the device. Press and hold this button for more than 5s to reset the device to factory defaults.

No.	Indicator/Port	Description
4	LAN2	● If it is steady orange, the port is connected at a rate of 1000 Mbit/s. ● If it is off, the port is connected at a rate of 10 Mbit/s or 100 Mbit/s.
5	WAN2	● If it is steady green, the port is connected. ● If it blinks green, the port is receiving or transmitting traffic.
6	10/100/1000M self-adaptive Ethernet ports	Five 10/100/1000M self-adaptive fast Ethernet ports: support automatic recognition of network cables and cross-over cables. ● LAN0 (GE 0/0) is a LAN port and WAN0 (GE 0/4) is a WAN port, and they do not support the WAN/LAN switchover. ● LAN3/WAN1 (GE 0/3) is a WAN port by default and supports the WAN/LAN switchover. ● LAN1/WAN3 (GE 0/1) and LAN2/WAN2 (GE 0/2) are LAN ports by default and support the WAN/LAN switchover.
7	USB	USB2.0 port that connects to USB-compliant peripheral devices, such as USB flash drives.
8	PWR	Power supply indicator: ● If it is steady green, the device is receiving power properly. ● If it is off, the power module is faulty or not powered on.

Figure 1-2 Back Panel of Ruijie RG-NBR6210-E Router

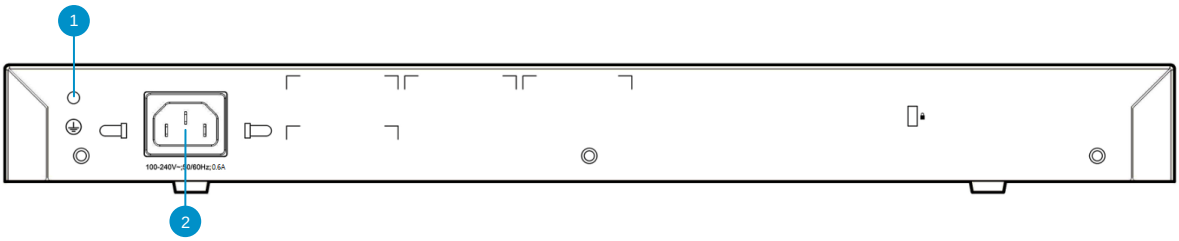


Table 1-2 Description of the Back Panel of Ruijie RG-NBR6210-E Router

No.	Button/Port	Description
1	Grounding screw	Connects to the grounding system of the installation site through the grounding wire to provide grounding protection.
2	Power port	Connects to an AC power cord.

2. Specifications of Ruijie RG-NBR6210-E Router

Table 1-3 Specifications of Ruijie RG-NBR6210-E Router

Item	Description
Model	RG-NBR6120-E
Storage	DDR3 SDRAM: 512 MB
	eMMC: 4 GB
	BOOTROM: 2 MB
I/O setup	Five 10/100/1000M self-adaptive fast Ethernet ports: support automatic recognition of network cables and crossover cables. ● WAN ports: Two WAN ports by default. WAN0 (GE 0/4) port is a WAN port and does not support the WAN/LAN switchover. LAN3/WAN1 (GE 0/3) port is a WAN port by default and supports the WAN/LAN switchover. ● LAN ports: Three LAN ports by default. LAN0 (GE 0/0) port is a LAN port and does not support the WAN/LAN switchover. LAN1/WAN3 (GE 0/1) and LAN2/WAN2 (GE 0/2) ports are LAN ports by default and support the WAN/LAN switchover.
	One console port
	One USB port
Interface standard	Ethernet: 10Base-T/100Base-TX/1000Base-TX
	Console port: RS-232
Dimension (W x H x D)	440 mm x 43.6 mm x 200 mm (excluding the foot pad)
Voltage	100-240 V, 50/60 Hz
Power consumption	Less than 20 W
Working environment	Temperature: 0°C to 45°C (32°F to 113°F)
	Humidity: 10% to 90% RH (non-condensing)

Note

Not all USB disks are supported. The Kingston USB disk with FAT 32 is recommended.

1.2.2 Ruijie RG-NBR6205-E Router

1. Appearance of Ruijie RG-NBR6205-E Router

Figure 1-3 Front Panel of Ruijie RG-NBR6205-E Router

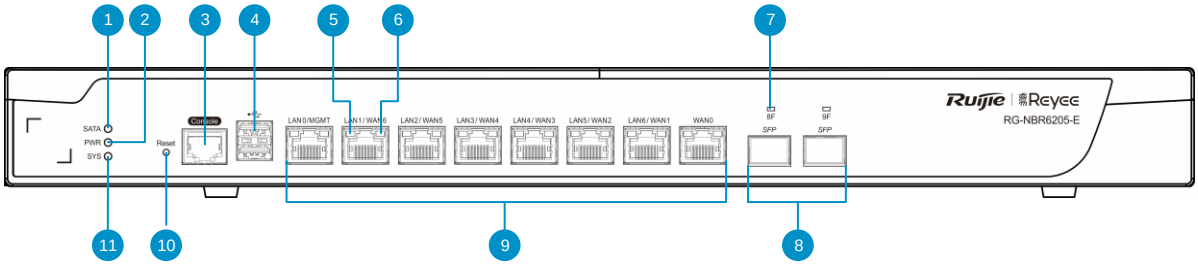


Table 1-4 Description of the Front Panel of Ruijie RG-NBR6205-E Router

No.	Indicator/Port	Description
1	SATA	SATA hard disk indicator: ● If it is steady green, the SATA hard disk is in place. ● If it blinks green, the SATA hard disk is reading or writing data.
2	PWR	Power indicator: ● If it is steady green, the router is receiving power properly. ● If it is off, the power module is faulty or not powered on.
3	Console	Console port. It connects to the console cable. After connecting to the serial port of the management PC, the device can be managed through the console port.
4	USB	Two USB ports They are USB2.0 ports that connect to USB-compliant peripheral devices, such as USB flash drives.
5	LAN1	● If it is steady orange, the port is connected at a rate of 1000 Mbit/s. ● If it is off, the port is connected at are rate of 10 Mbit/s or 100 Mbit/s.
6	WAN6	● If it is steady green, the port is connected at a rate of 10 Mbit/s, 100 Mbit/s or 1000 Mbit/s. ● If it blinks green, the port is receiving or transmitting traffic.
7	8F	● If it is steady green, the port is connected. ● If it blinks green, the port is receiving or transmitting traffic.
8	GE fiber ports	Two SFP ports (8F, 9F): ● WAN ports by default that support the WAN/LAN switchover. ● Support 1000BASE-SX/LX/ZX mini GBIC and GE-SFP-LX20/LH40-BIDI SPF modules.

No.	Indicator/Port	Description
9	GE copper ports	Eight 10/100/1000M self-adaptive fast Ethernet ports (copper ports 0-7) that support automatic recognition of network cables and crossover cables: ● LAN0 (GE 0/0) port is a LAN port and WAN0 (GE 0/7) port is a WAN port, and they do not support the WAN/LAN switchover. ● LAN6/WAN1 (GE 0/6) is WAN port by default and supports the WAN/LAN switchover. ● LAN1/WAN6 (GE 0/1), LAN2/WAN5 (GE 0/2), LAN3/WAN4 (GE 0/3), LAN4/WAN3 (GE 0/4), LAN5/WAN2 (GE 0/5) are LAN ports by default and support the WAN/LAN switchover. ● In bridge mode, LAN0 (GE 0/0) port is also the MGMT port.
10	Reset	Restarts the router. Press and hold this button for more than 5 s to reset the router to factory defaults.
11	SYS	System indicator: ● If it blinks green, the system is being initialized. ● If it is steady green, system initialization is completed. ● If it is steady red, the system is in abnormal state.

Figure 1-4 Back Panel of Ruijie RG-NBR6205-E Router

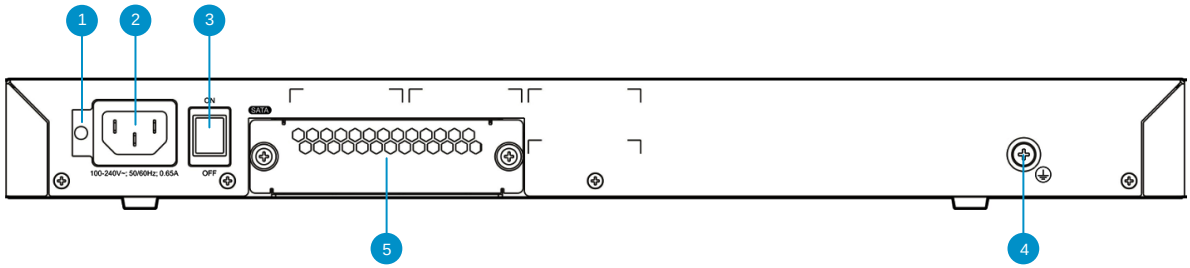


Table 1-5 Description of the Back Panel of Ruijie RG-NBR6205-E Router

No.	Indicator/Port	Description
1	Retainer holder	Holds the power cord retainer to secure the power cord.
2	Power port	Connects to an AC power cord.
3	Power switch	Controls power supply.
4	Grounding screw	Connects to the grounding system of the installation site through the grounding wire to provide grounding protection.
5	Hard disk expansion card slot	Fits the hard disk module. The supported hard disk module model is RG-NBR-HDD-1T.

2. Specifications of Ruijie RG-NBR6205-E Router

Table 1-6 Specifications of Ruijie RG-NBR6205-E Router

Item	Description
Model	RG-NBR6205-E
Storage	DDR4 SDRAM: 2 GB
	BOOTROM: 8 MB
	eMMC: 8 GB
	SATA: 1 TB (optional)
I/O setup	● Eight 10/100/1000M self-adaptive fast Ethernet ports: support automatic recognition of network cables and cross-over cables. ○ By default, LAN0 (GE 0/0), LAN1/WAN6 (GE 0/1), LAN2/WAN5 (GE 0/2), LAN3/WAN4 (GE 0/3), LAN4/WAN3 (GE 0/4) and LAN5/WAN2 (GE 0/5) are LAN ports, while WAN0 and LAN6/WAN1 (GE 0/6) are WAN ports. ○ LAN1/WAN6 (GE 0/1), LAN2/WAN5 (GE 0/2), LAN3/WAN4 (GE 0/3), LAN4/WAN3 (GE 0/4), LAN5/WAN2 (GE 0/5) and LAN6/WAN1 (GE 0/6) support the WAN/LAN switchover. ● Two SFP ports: ○ Support 1000BASE-SX/LX/ZX mini GBIC and GE-SFP-LX20/LH40-BIDI SPF modules. ○ By default, the SFP ports are WAN ports, and support the WAN/LAN switchover.
	One management port (in bridge mode)
	One console port
	Two USB ports
Hardware disk module	One hardware disk module (optional)
Hot swapping	Not supported
Interface standard	Ethernet: 10Base-T/100Base-TX/1000Base-TX, 1000BASE-SX/LX/ZX, 10GBASE-SR/LR/ZR
	Console port: RS-232
Dimension (W x H x D)	440 mm x 43.6 mm x 200 mm (excluding the foot pad)
Voltage	100-240 V; 50/60 Hz
Power	Less than 25 W
Working environment	Temperature: 0°C to 45°C (32°F to 113°F)
	Humidity: 10% to 90% RH (non-condensing)

Note

Not all USB disks are supported. The Kingston USB disk with FAT 32 is recommended.

Caution

- Avoid vibration and collision during device moving and usage.
- To power off the device with the hard disk module installed, turn off the power button. Do not remove the power cord until the PWR LED turns off; otherwise, the hardware disk will be damaged.

1.2.3 Ruijie RG-NBR6210-E Router

1. Appearance of Ruijie RG-NBR6210-E Router

Figure 1-5 Front Panel of Ruijie RG-NBR6210-E Router

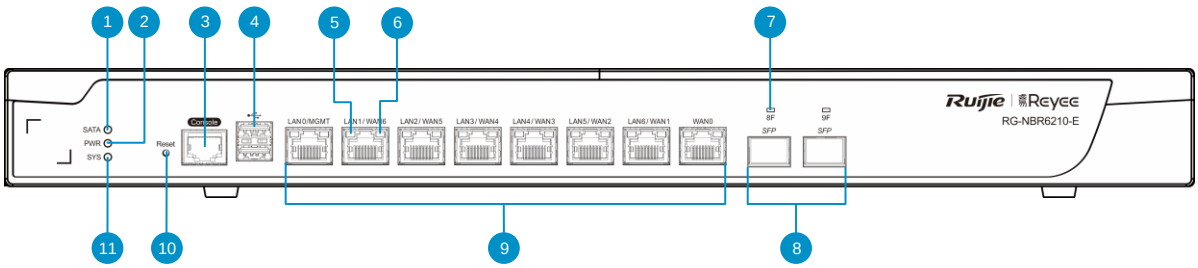


Table 1-7 Description of the Front Panel of Ruijie RG-NBR6210-E Router

No.	Indicator/Port	Description
1	SATA	SATA hard disk indicator: ● If it is steady green, the SATA hard disk is in place. ● If it blinks green, the SATA hard disk is reading or writing data.
2	PWR	Power indicator: ● If it is steady green, the device is receiving power properly. ● If it is off, the power module is faulty or not powered on.
3	Console	Console port. It connects to the console cable. After connecting to the serial port of the management PC, the device can be managed through the console port.
4	USB	2 USB ports They are USB2.0 ports that connect to USB-compliant peripheral devices, such as USB flash drives.
5	LAN1	● If it is steady orange, the port is connected at a rate of 1000 Mbit/s. ● If it is off, the port is connected at a rate of 10 Mbit/s or 100 Mbit/s.
6	WAN6	● If it is steady green, the port is connected at a rate of 10 Mbit/s, 100 Mbit/s, or 1000 Mbit/s. ● If it blinks green, the port is receiving or transmitting traffic.
7	8F	● If it is steady green, the port is connected. ● If it blinks green, the port is receiving or transmitting traffic.

No.	Indicator/Port	Description
8	GE fiber ports	Two SFP ports (8F, 9F): ● WAN ports by default and support WAN/LAN switchover. ● Support 1000BASE-SX/LX/ZX mini GBIC and GE-SFP-LX20/LH40-BIDI SPF modules.
9	GE copper ports	Eight 10/100/1000M self-adaptive fast Ethernet ports (0~7 copper ports): ● 10/100/1000M self-adaptive and support automatic recognition of network cables and cross-over cables. ● LAN0 (GE 0/0) is a LAN port and WAN0 (GE 0/7) is a WAN port. Both do not support WAN/LAN switchover. ● By default, LAN6/WAN1 (GE 0/6) is a WAN port and supports WAN/LAN switchover. ● By default, LAN1/WAN6 (GE 0/1), LAN2/WAN5 (GE 0/2), LAN3/WAN4 (GE 0/3), LAN4/WAN3 (GE 0/4) and LAN5/WAN2 (GE 0/5) are LAN ports and support WAN/LAN switchover. ● In bridge mode, LAN0 (GE 0/0) is also the MGMT port.
10	Reset	Restarts the router. Press and hold this button for more than 5 s to reset the router to factory defaults.
11	SYS	System indicator: ● If it blinks green, the system is being initialized. ● If it is steady green, system initialization is completed. ● If it is steady red, the system is in abnormal state.

Figure 1-6 Back Panel of Ruijie RG-NBR6210-E Router

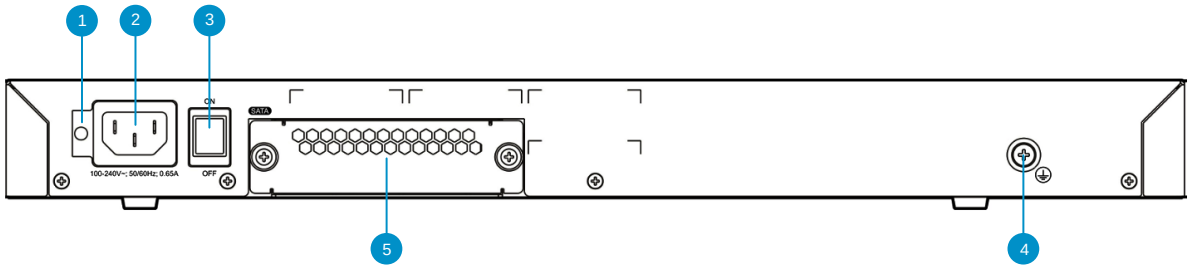


Table 1-8 Description of the Back Panel of Ruijie RG-NBR6210-E Router

No.	Indicator/Port	Description
1	Retainer holder	Holds the power cord retainer to secure the power cord.
2	Power port	Connects to an AC power cord.
3	Power switch	Controls power supply.
4	Grounding screw	Connects to the grounding system of the installation site through the grounding wire to provide grounding protection.

No.	Indicator/Port	Description
5	Hard disk expansion card slot	Fits the hard disk module. The supported hard disk module model is RG-NBR-HDD-1T.

2. Specifications of Ruijie RG-NBR6210-E Router

Table 1-9 Specifications of Ruijie RG-NBR6210-E Router

Item	Description
Model	RG-NBR6210-E
Storage	DDR4 SDRAM: 2 GB
	BOOTROM: 8 MB
	eMMC: 8 GB
	SATA: 1 TB (optional)
I/O setup	● Eight 10/100/1000M self-adaptive fast Ethernet ports: support automatic recognition of network cables and cross-over cables. ○ By default, LAN0 (GE 0/0), LAN1/WAN6 (GE 0/1), LAN2/WAN5 (GE 0/2), LAN3/WAN4 (GE 0/3), LAN4/WAN3 (GE 0/4) and LAN5/WAN2 (GE 0/5) are LAN ports, while WAN0 and LAN6/WAN1 (GE 0/6) are WAN ports. ○ LAN1/WAN6 (GE 0/1), LAN2/WAN5 (GE 0/2), LAN3/WAN4 (GE 0/3), LAN4/WAN3 (GE 0/4), LAN5/WAN2 (GE 0/5) and LAN6/WAN1 (GE 0/6) support the WAN/LAN switchover. ● Two SFP ports: ○ Support 1000BASE-SX/LX/ZX mini GBIC and GE-SFP-LX20/LH40-BIDI SPF modules. ○ By default, these two SFP ports are WAN ports, and support the WAN/LAN switchover.
	One management port (in bridge mode)
	One console port
	Two USB ports
Hardware disk module	One hardware disk module (optional)
Hot swapping	Not supported
Interface standard	Ethernet: 10Base-T/100Base-TX/1000Base-TX, 1000BASE-SX/LX/ZX, 10GBASE-SR/LR/ZR
	Console port: RS-232
Dimension (W x H x D)	440 mm x 43.6 mm x 200 mm (excluding the foot pad)
Voltage	100-240 V; 50/60 Hz
Power	Less than 25 W

Item	Description
Working environment	Temperature: 0°C to 45°C (32°F to 113°F)
	Humidity: 10% to 90% RH (non-condensing)

Note

Not all USB disks are supported. The Kingston USB disk with FAT 32 is recommended.

Caution

- Avoid vibration and collision during device moving and usage when the device has the hard disk module installed.
- To power off the device equipped with the hard disk module, turn off the power button. Do not remove the power cord until the PWR LED turns off; otherwise, the hardware disk will be damaged.

1.2.4 Ruijie RG-NBR6215-E Router

1. Appearance of Ruijie RG-NBR6215-E Router

Figure 1-7 Front Panel of Ruijie RG-NBR6215-E Router

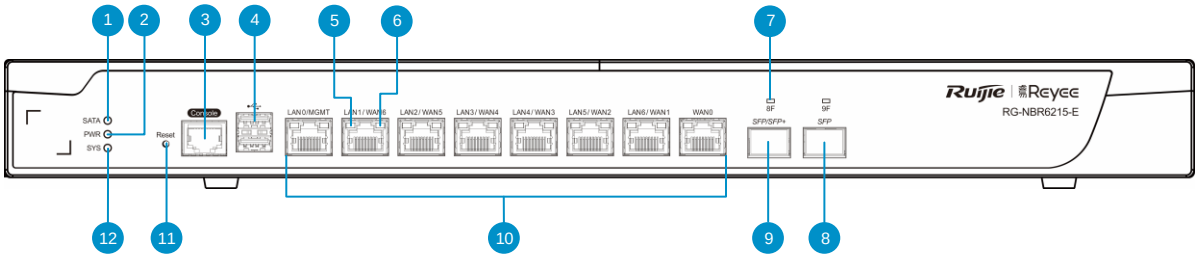


Table 1-10 Description of the Front Panel of Ruijie RG-NBR6215-E Router

No.	Indicator/Port	Description
1	SATA	SATA hard disk indicator: ● If it is steady green, the SATA hard disk is in place. ● If it blinks green, the SATA hard disk is reading or writing data.
2	PWR	Power indicator: ● If it is steady green, the device is receiving power properly. ● If it is off, the power module is faulty or not powered on.
3	Console	Console port. It connects to the console cable. After connecting to the serial port of the management PC, the device can be managed through the console port.

No.	Indicator/Port	Description
4	USB	Two USB ports They are USB2.0 ports that connect to USB-compliant peripheral devices, such as USB flash drives.
5	LAN1	● If it is steady orange, the port is connected at a rate of 1000 Mbit/s. ● If it is off, the port is connected at a rate of 10 Mbit/s or 100 Mbit/s.
6	WAN6	● If it is steady green, the port is connected at a rate of 10 Mbit/s, 100 Mbit/s, or 1000 Mbit/s. ● If it blinks green, the port is receiving or transmitting traffic.
7	8F	● If it is steady green, the port is connected. ● If it blinks green, the port is receiving or transmitting traffic.
8	SFP	One SFP port (9F): ● A WAN port by default and supports the WAN/LAN switchover. ● Supports 1000BASE-SX/LX/ZX mini GBIC and GE-SFP-LX20/LH40-BIDI SPF modules.
9	SFP/SFP+	One SFP+/SFP port (8F): ● An SFP+ port by default and supports XG-SFP-SR-MM850, XG-SFP-LR-SM1310 and XG-SFP-ER-SM1550 modules and BIDI modules. ● Can be configured as an SFP port and supports 1000BASE-SX/LX/ZX mini GBIC and GE-SFP-LX20/LH40-BIDI SPF modules. ● A LAN port by default and supports the WAN/LAN switchover.
10	GE copper ports	Eight 10/100/1000M self-adaptive fast Ethernet ports (copper ports 0-7) that support automatic recognition of network cables and cross-over cables: ● LAN0 (GE 0/0) is a LAN port and WAN0 (GE 0/7) is a WAN port, and they do not support the WAN/LAN switchover. ● By default, LAN6/WAN1 (GE 0/6) is a WAN port and supports the WAN/LAN switchover. ● By default, LAN1/WAN6 (GE 0/1), LAN2/WAN5 (GE 0/2), LAN3/WAN4 (GE 0/3), LAN4/WAN3 (GE 0/4) and LAN5/WAN2 (GE 0/5) are LAN ports and support the WAN/LAN switchover. ● In bridge mode, LAN0 (GE 0/0) port is also the MGMT port.
11	Reset	Restarts the router. Press and hold this button for more than 5 s to reset the router to factory defaults.
12	SYS	System indicator: ● If it blinks green, the system is being initialized. ● If it is steady green, system initialization is completed. ● If it is steady red, the system is in abnormal state.

Figure 1-8 Back Panel of Ruijie RG-NBR6215-E Router

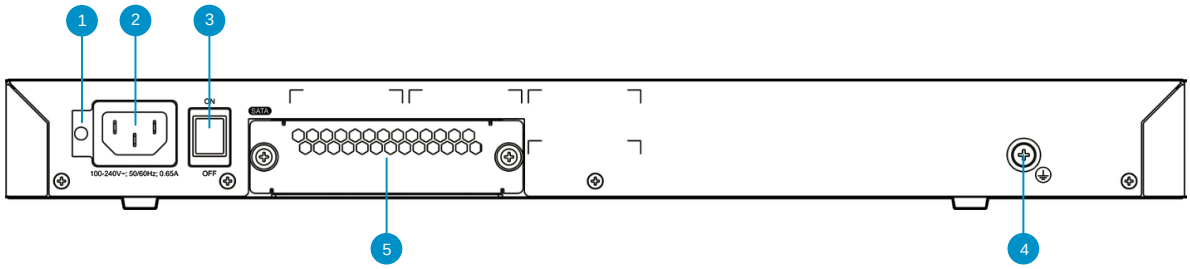


Table 1-11 Description of the Back Panel of Ruijie RG-NBR6215-E Router

No.	Indicator/Port	Description
1	Retainer holder	Holds the power cord retainer to secure the power cord.
2	Power port	Connects to an AC power cord.
3	Power switch	Controls power supply.
4	Grounding screw	Connects to the grounding system of the installation site through the grounding wire to provide grounding protection.
5	Hard Disk expansion card slot	Fits the hard disk module. The supported hard disk module model is RG-NBR-HDD-1T.

2. Specifications of Ruijie RG-NBR6215-E Router

Table 1-12 Specifications of Ruijie RG-NBR6215-E Router

Item	Description
Model	RG-NBR6215-E
Storage	DDR4 SDRAM: 2 GB
	BOOTROM: 8 MB
	eMMC: 8 GB
	SATA: 1 TB (OPTIONAL)

Item	Description
I/O setup	● Eight 10/100/1000M self-adaptive fast Ethernet ports that support automatic recognition of network cables and cross-over cables: ○ By default, LAN0 (GE 0/0), LAN1/WAN6 (GE 0/1), LAN2/WAN5 (GE 0/2), LAN3/WAN4 (GE 0/3), LAN4/WAN3 (GE 0/4) and LAN5/WAN2 (GE 0/5) are LAN ports, while WAN0 and LAN6/WAN1 (GE 0/6) are WAN ports. ○ LAN1/WAN6 (GE 0/1), LAN2/WAN5 (GE 0/2), LAN3/WAN4 (GE 0/3), LAN4/WAN3 (GE 0/4), LAN5/WAN2 (GE 0/5) and LAN6/WAN1 (GE 0/6) support the WAN/LAN switchover. ● One SFP+/SFP port: ○ An SFP+ port by default and supports XG-SFP-SR-MM850, XG-SFP-LR-SM1310 and XG-SFP-ER-SM1550 modules and BIDI modules. ○ Can be configured as an SFP port and supports 1000BASE-SX/LX/ZX mini GBIC and GE-SFP-LX20/LH40-BIDI SPF modules. ○ A LAN port by default and supports the WAN/LAN switchover. ● One SFP port: ○ Supports 1000BASE-SX/LX/ZX mini GBIC and GE-SFP-LX20/LH40-BIDI SPF modules. ○ A WAN port by default and supports the WAN/LAN switchover.
	One management port (in bridge mode)
	One console port
	Two USB ports
Hardware disk module	One hardware disk module (optional)
Hot swapping	Not supported
Interface standard	Ethernet: 10Base-T/100Base-TX/1000Base-TX, 1000BASE-SX/LX/ZX, 10GBASE-SR/LR/ZR
	Console port: RS-232
Dimension (W x H x D)	440 mm x 43.6 mm x 200 mm(excluding the foot pad)
Voltage	100-240 V; 50/60 Hz
Power	Less than 25 W
Working environment	Temperature: 0°C to 45°C (32°F to 113°F)
	Humidity: 10% to 90% RH (non-condensing)

Note

Not all USB disks are supported. The Kingston USB disk with FAT 32 is recommended.

Caution

- Avoid vibration and collision during device moving and usage when the device has the hard disk module installed.

- To power off the device equipped with the hard disk module, turn off the power button. Do not remove the power cord until the PWR LED turns off; otherwise, the hardware disk will be damaged.
- The SFP+ port does not support the direct connection between two RG-EG3200 series or RG-NBR6200-E series devices through the SFP module or fiber cables.

1.3 Specifications of the Hard Disk Module

RG-NBR-HDD-1T hard disk module is applicable to RG-NBR6205-E, RG-NBR6210-E, and RG-NBR6215-Erouters.

Note

The hard disk module must be separately purchased.

Figure 1-9 Appearance of the RG-NBR-HDD-1T Hard Disk

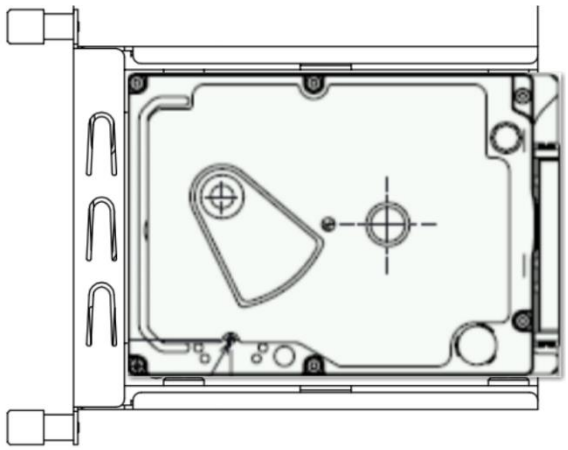


Table 1-13 Specifications of the RG-NBR-HDD-1T Hard Disk

Model	RG-NBR-HDD-1T
Applicable models	RG-NBR6205-E, RG-NBR6210-E and RG-NBR6215-E
Dimensions (L x W x H)	130 mm x 102 mm x 27 mm
Type	HDD
Memory	1 TB
Operational altitude	0 m to 3000 m
Hot swapping	Not supported

Note

- The software has been installed in the hard disk with the format "*.EXT3*", so the hard disk is plug and play.
- The hardware disk module does not support hot swapping. You have to reset the device after installing the hard disk.

Caution

- Avoid vibration and collision during device moving and usage.
- Products should be transported in original packages.
- Errors may occur if a RG-NBR-HDD-1T hard disk is used at an altitude over 3,000 m.
- When using the hard disk, do not drop, press on the surface or cover the air hole of the hard disk.

2 Getting Started

2.1 Preparing for Installation

2.1.1 Safety Precautions

The Router acts as the critical transfer station of network connections, and its normal service is crucial to the normal operation of the entire network. The following safety suggestions are applicable to the installation and use of the Router:

- Do not place the device in a watery place and prevent any liquid from entering into it.
- Keep the device away from heat sources.
- Wear an ESD wrist strap to install and maintain the device.
- Do not wear loose clothes to avoid hooking any parts. Before operation, tighten your band, shawl, and sleeves.
- Keep tools and parts away from the walkway to avoid damage.
- Use the uninterruptible power supply (UPS) to avoid power failures and other interferences.

2.1.2 Requirements on the Installation Environment

Ruijie RG-NBR-E series Routers are for indoor use only. To ensure normal operation and prolong their service life, the installation site must meet the following requirements.

1. Temperature/Humidity Requirements

The Ruijie RG-NBR-E series Routers will be damaged when being exposed to an environment that does not meet temperature/humidity requirements for a long time. To ensure normal operation and prolong the service life of the router, the equipment room must maintain constant temperature and humidity.

- If the relative humidity of the equipment room is above 90%, the insulation materials may result in defective insulation and even electric leakage.
- If the relative humidity of the equipment room is below 10%, the insulation spacer may shrink, which will make screws looser.
- Static electricity may occur in the dry environment, causing damage to the interior circuits of the router.

- A high temperature will accelerate the aging of insulation materials and compromise the reliability and even service life of the router.
- Table 2-1 lists temperature/humidity requirements. For more information about differences between products, see "Product Overview".

Table 2-1 Temperature and Humidity Requirements of Ruijie RG-NBR-E Series Routers

Temperature		Relative Humidity	
Long-term working condition	Short-term working condition	Long-term working condition	Short-term working condition
15°C to 30°C (59°F to 86°F)	0°C to 45°C (32°F to 113°F)	40% to 65%	10% to 90%

Note

- The working temperature or humidity indicates the value measured at 1.5 m above the floor and 0.4 m ahead of the equipment frame when there is no protection plate on the front and rear side of the equipment frame.
- The short-term working condition indicates the situation where the router has been working continuously within 48 hours or the accumulative device operation period does not exceed 15 days in a year.

2. Cleanliness Requirements

Dust is also a major threat to the safe operation of the router. If dust falls on the device body, it will cause electrostatic adsorption and poor contact of metal contacts. In particular, when the indoor relative humidity is low, electrostatic adsorption may easily occur. This affects the service life and easily result in communication failures. Table 1-15 lists the dust content and particle size requirements in the equipment room.

Table 2-2 Equipment Room Dust Content and Particle Size Requirements of Ruijie RG-NBR-E Series Routers

Dust	Unit	Content
Dust particles (particle diameter ≤ 0.5 μm)	particles/m³	≤ 1.4×10^7
Dust particles (0.5 μm < particle diameter ≤ 1 μm)	particles/m³	≤ 7×10^5
Dust particles (1 μm < particle diameter ≤ 3 μm)	particles/m³	≤ 2.4×10^5
Dust particles (3 μm < particle diameter ≤ 5 μm)	particles/m³	≤ 1.3×10^5

Apart from the dust, the device is also sensitive to the hydrochloric acid sulfide contained in the air. These noxious gases will accelerate metal wastage and the aging of certain parts. Table 1-16 lists the upper limits of noxious gases (sulfur dioxide, sulfured hydrogen, nitrogen dioxide, ammonia, and chlorine) in the equipment room.

Table 2-3 Upper Limits of Noxious Gases of Ruijie RG-NBR-E Series Routers

Gas	Average (mg/m^3)	Maximum (mg/m^3)
Sulfur dioxide	0.2	1.5
Sulfured hydrogen	0.006	0.03
Nitrogen dioxide	0.04	0.15
Ammonia	0.05	0.15
Chlorine	0.01	0.3

Note

The average value is measured by week. The maximum value is the extreme value within a week, which does not exceed 30 minutes per day.

3. ESD Requirements

ESD measures have been taken during circuit design, but strong static electricity will still damage the printed circuit card (PCB). Static electricity on the communication network connected to the router is mainly originated from the following sources:

- Outdoor high-voltage transmission line, lightning, and other exterior electric fields
- Indoor environment, flooring material, complete appliance structure, and other in-house systems

To avoid the damage caused by static electricity, take the following measures:

- Properly ground the router and floor.
- Apply indoor dust control.
- Maintain proper temperature and humidity.
- Before touching the circuit board, wear an ESD wrist strap and an ESD uniform.
- Place the PCB disassembled face up on the antistatic workbench or in the electromagnetic shielded bag.
- When observing or transferring the circuit board of Router, touch the outer edge of the PCB and avoid direct contact with the components on the PCB.

4. Anti-Interference Requirements

- Take effective power grid interference control measures against the power supply system.
- Keep the working ground of the Router far away from the grounding device or lightning grounding device of the power device instead of sharing.
- Keep the router far away from the high-power radio-transmitting station, radar-transmitting station, and other high-frequency and heavy-current devices.
- Take electromagnetic shielding measures when necessary.

5. Checking the Installation Location

Regardless of whether the Router is installed in the cabinet or on the workbench, comply with the following requirements:

- Ensure that sufficient room has been reserved for the air intake and air vent of Router to facilitate cooling of the router chassis.
- Install the Router in the 19-inch standard cabinet. Alternatively, install it on a clean and flat surface. In heated areas, the air conditioning system should be properly installed.
- Ensure that the cabinet and workbench are equipped with a good ventilation and cooling system.
- Ensure that the cabinet and workbench are steady enough and capable of withstanding the weight of the Router and its accessories.
- Ensure that the cabinet and workbench are properly grounded.

2.1.3 Installation Tools

To enable smooth installation, prepare the following items.

Table 2-4 Tool List

Installation tools	Phillips screwdriver, and ESD wrist strap or gloves
Connection cables	Power cords, configuration cables, Ethernet cables, and grounding wires
Related devices	Hub or switch, configuration terminal (PC equipped with the HyperTerminal program), and electric outlet

Note

The device delivered does not have the tool kit, so users need to prepare tools on the tool list.

2.2 Installing a Router

2.2.1 Installation Procedure

Install the router as follows:

(1) (Optional) Installing the hard disk

(2) Installing the Router in a specific location

(3) Performing EMG grounding

(4) Installing power cords

(5) Checking after installation

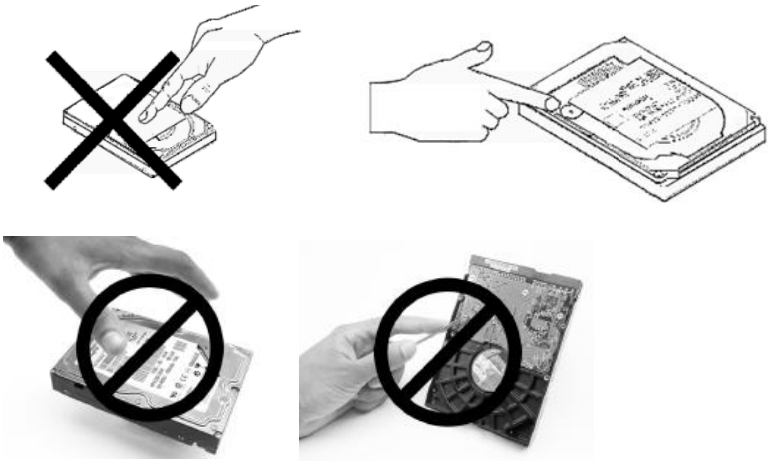
2.2.2 (Optional) Installing the Hard Disk for the RG-NBR6200-E Series Routers

RG-NBR6205-E, RG-NBR6210-E, and RG-NBR6215-E routers can be equipped with a hard disk module and the applicable model is RG-NBR-HDD-1T. The hard disk module does not come with the router and needs to be purchased as required.

1. Precautions

- Do not install the hard disk when the router is powered off; otherwise, the hard disk will be damaged.

- Do not cover the air hole of the hard disk.
- Do not press the cover of the hard disk.
- Do not toss, jolt, or shake the hard disk. Hold the side of the hard disk when removing it.
- Do not touch the PCB.

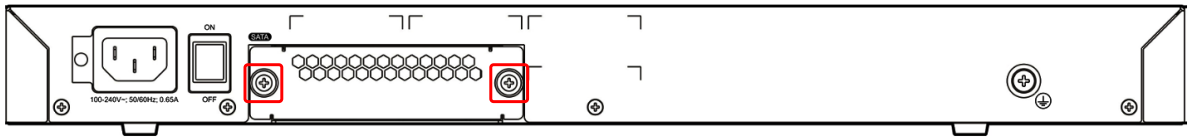


2. Installing the hard disk module

The hard disk module can only be installed in the expansion slot on the back panel of the router. The installation steps are as follows.

(1) Facing the back panel of the device, unscrew the two fixing screws on the hard disk slot cover to remove the cover.

Figure 1-1 Two Fixing Screws on the Hard Disk Slot Cover



(2) Gently insert the hard disk module into the slot.

(3) Tighten the screws.

2.2.3 Installing the Device in a Specific Location

RG-NBR-E series Routers can be mounted on a cabinet or a workbench.

1. Mounting into a cabinet

Ruijie RG-NBR-E series Routers are designed based on the dimension of a standard cabinet. You can install the router with the enclosed fixing accessories.

2. Mounting on a workbench

If a standard cabinet is unavailable, you can place the router on a clean workbench. Pay attention to the following points:

- Ensure that the workbench is steady and properly grounded.
- Stick the attached plastic pads onto the small holes at the bottom of the Router, and reserve a heat elimination

room of at least 10 cm around the router.

- Do not place any heavy things on the router.

2.2.4 Performing EMC Grounding

The grounding required for EMC design includes the shielding ground, filter ground, noise and interference suppression, and level reference, which constitute the comprehensive grounding requirements. The grounding resistance should be less than 1 ohm. The RG-NBR-E series routers are equipped with a grounding pole at the rear panel, as shown in Figure 2-1 and Figure 2-2.

Figure 2-1 Grounding of the RG-NBR-E Series Routers

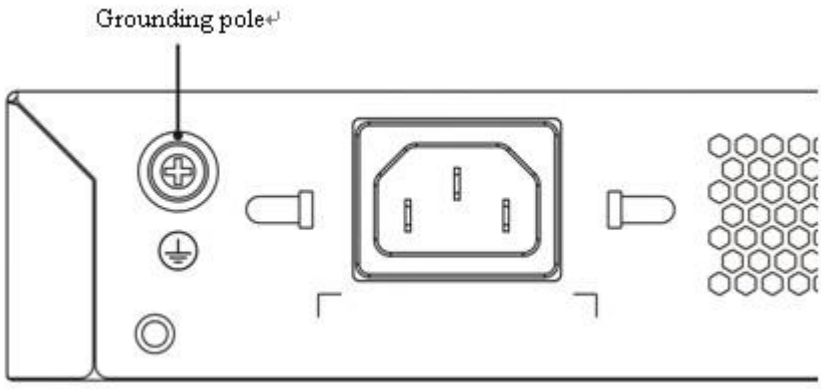
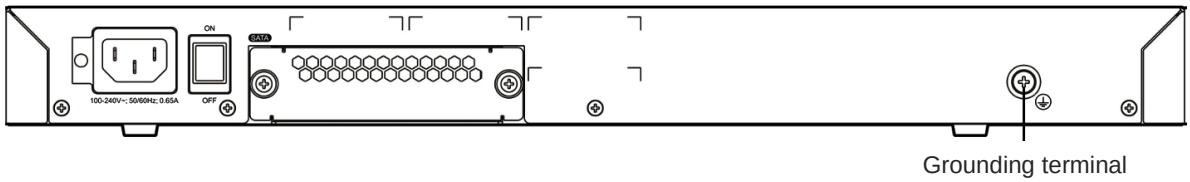


Figure 2-2 Grounding of RG-NBR6205-E, RG-NBR6210-E, and RG-NBR6215-E Series Routers



Grounding steps are as follows:

(1) Connect the grounding screw of the device to the grounding terminal of the cabinet or workbench using the grounding wire.

(2) Connect the grounding terminal of the cabinet or workbench to the grounding bar of the equipment room.

2.2.5 Installing the Power Cord

The requirements of Ruijie RG-NBR-E series Routers on AC power supply are 100–240 V and 50/60 Hz.

The Router uses 3-conductor power cords. You are advised to use a single-phase 3-conductor outlet or a multifunction microcomputer outlet with the neutral connector. The neutral point of the power supply should be securely grounded in the building. In most buildings, the neutral point of a power supply has been grounded during the construction. Ensure that the power supply is properly grounded.

Plug one end of the power cord into the power port on the back panel of the Router, and the other end into the AC power supply outlet.

Caution

Make sure that the main power supply is off before inserting the power plug.

2.2.6 Checking After the Installation

After completing the mechanical installation of THE Router, perform the following checks before powering on the router:

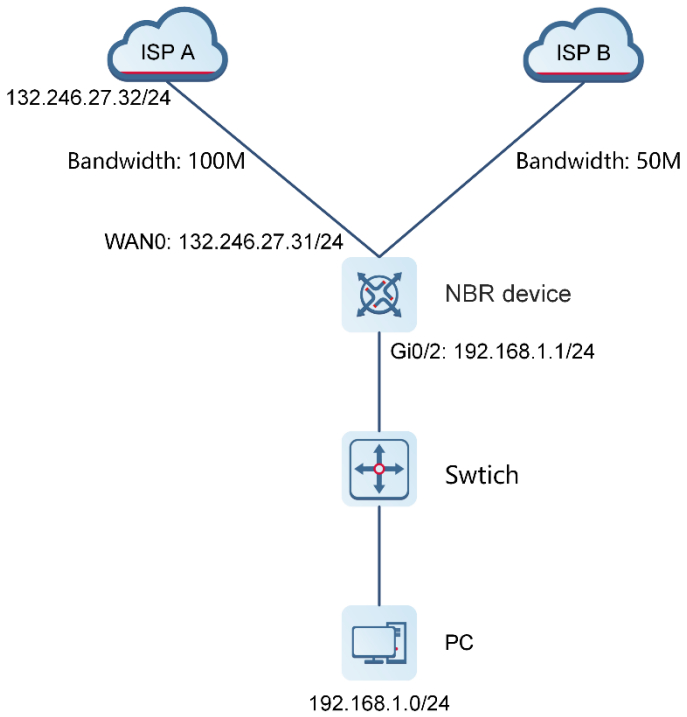
- If the router is installed in a cabinet, check whether the angle bar is steady. If the router is installed on the workbench, check whether sufficient room is reserved around the router to ensure cooling and check whether the workbench is steady.
- Check whether the power supply meets requirements.
- Check whether the earth wire of the router is properly connected.
- Check whether the router is connected correctly to other devices such as the configuration terminal.

3 Configuration

3.1 WAN Load Balance

Application Scenario

The Load Balancing function enables packets to be forwarded by multiple WAN ports in a balanced manner to avoid traffic congestion and to provide redundancy.



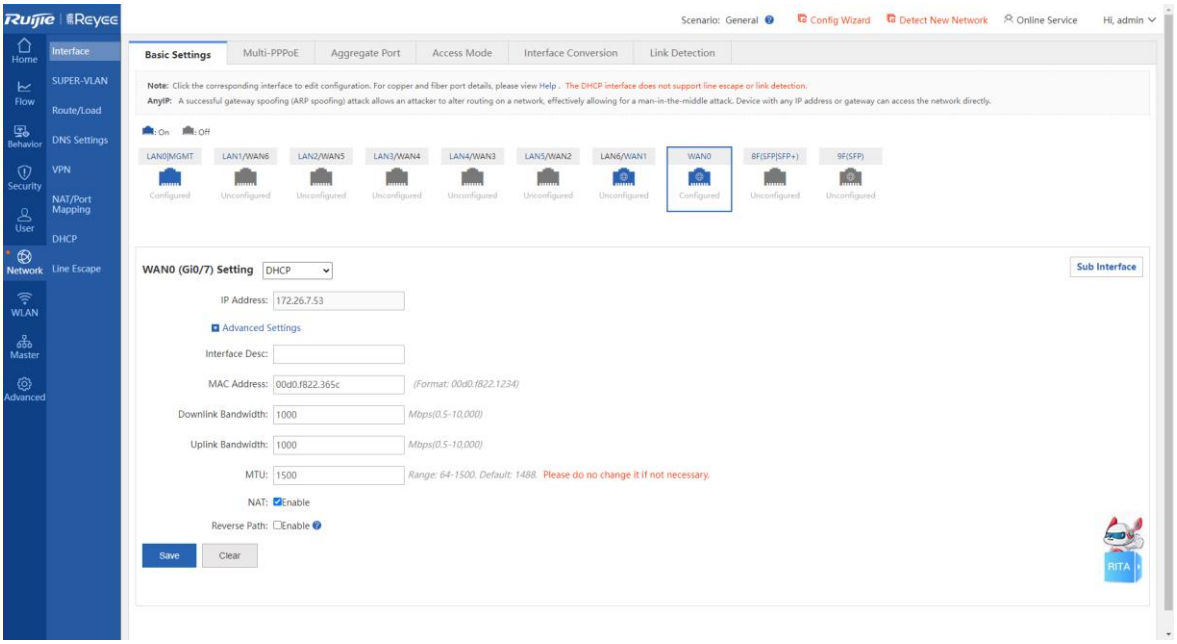
Prerequisites

- Configure IP addresses for WAN ports and default routes.
- Configure a load balancing policy.

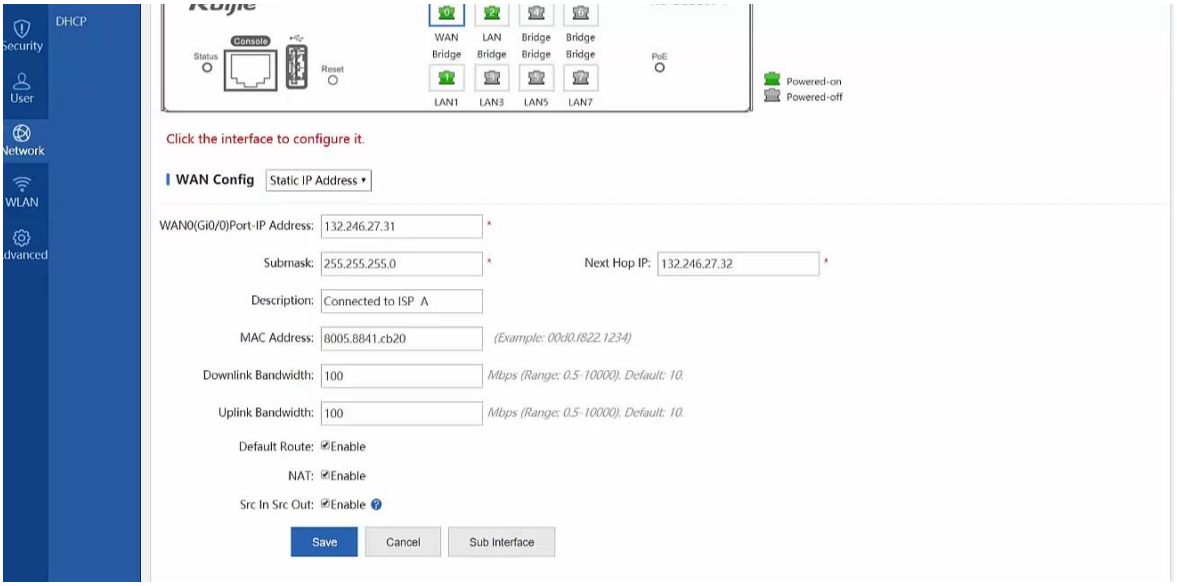
- Customize the interface weight to ensure that traffic goes through different egresses according to the weight.

Procedure

(1) Choose **Network** > **Interface** > **Basic Settings** and configure WAN0.

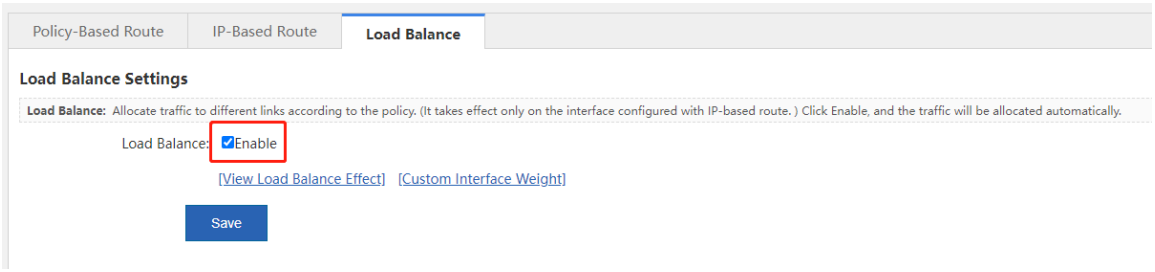


(2) Choose **Network** > **Interface** > **Basic Settings** and configure WAN1.

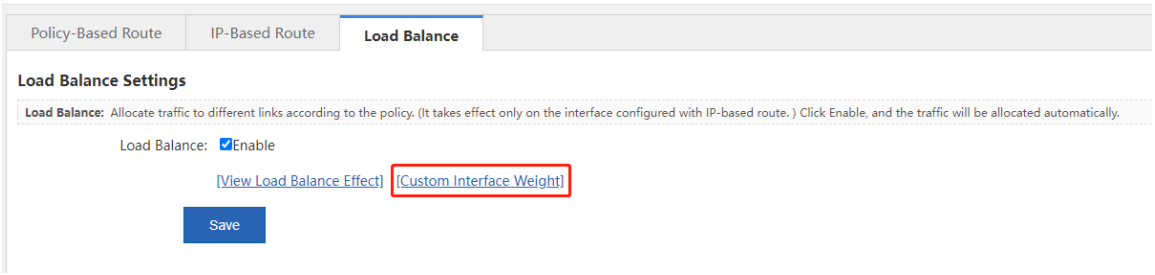


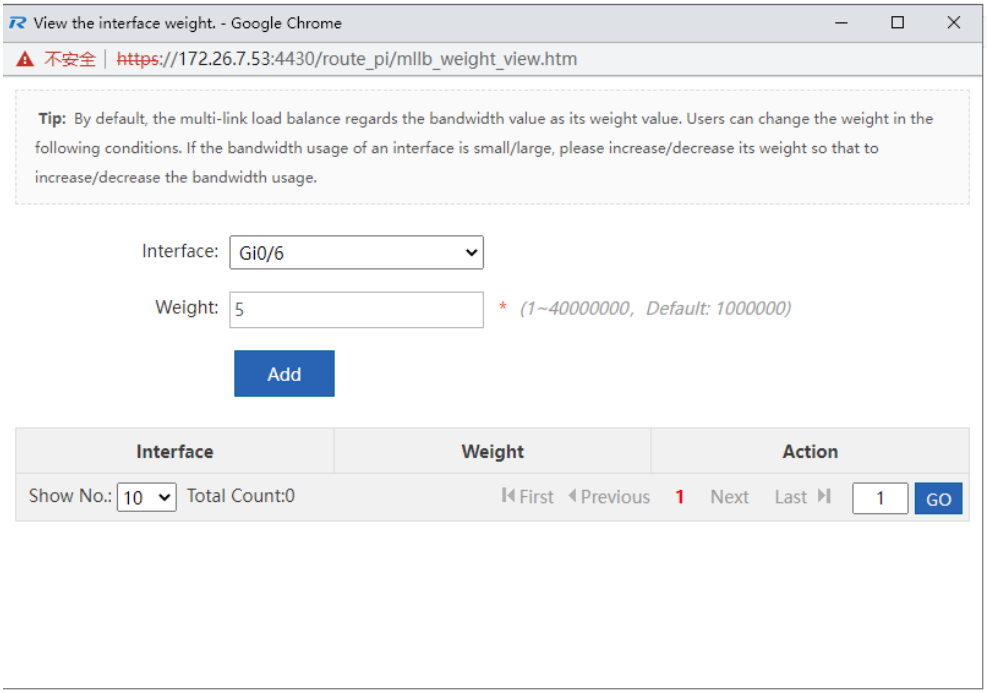
(3) Choose **Network** > **Route/Load** > **Load Balance** and enable **Load Balance**.

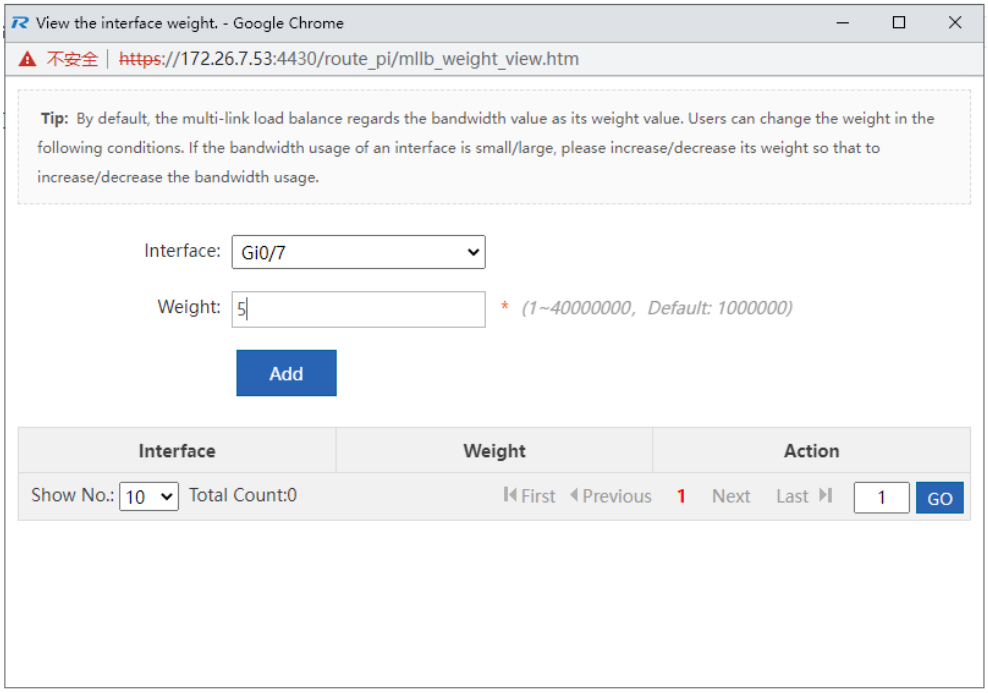
a Select **Enable**.



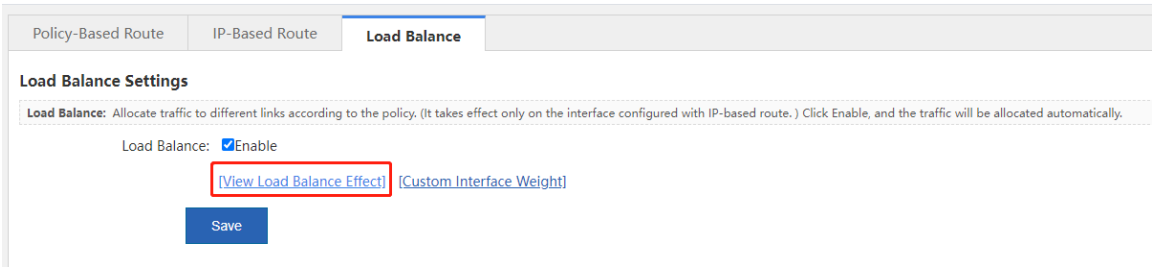
b Configure the interface weight.







c Verify the configuration.



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: Select an interface

Weight: * (1~40000000)

Add

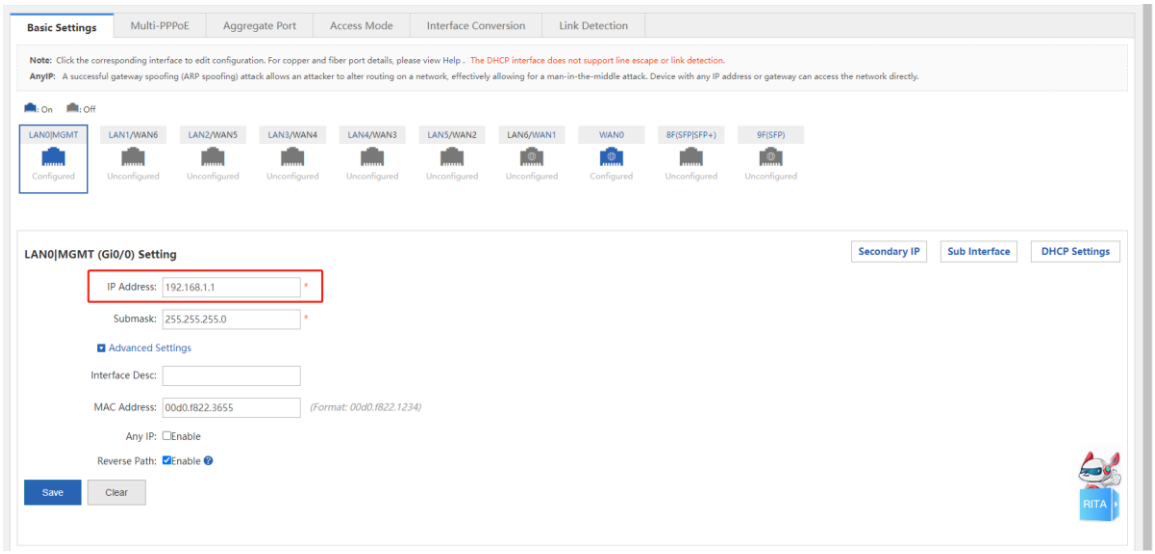
Interface	Weight	Action
GigabitEthernet 0/6	5 (Default: 1000000)	Edit Delete
GigabitEthernet 0/7	5 (Default: 1000000)	Edit Delete

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

3.2 DHCP Configuration

3.2.1 Configuring DHCP Through the Web Page

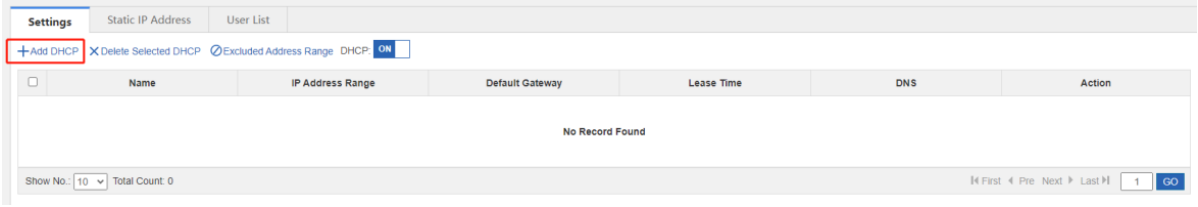
(1) Choose **Network** > **Interface** > **Basic Settings** and configure an interface's IP address.



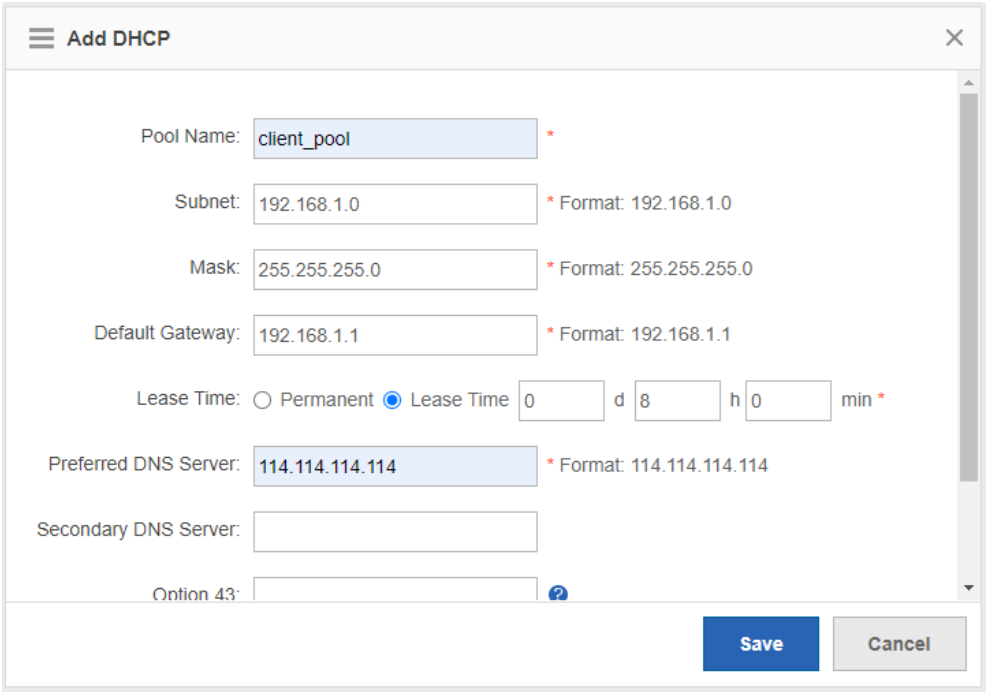
(2) Choose **Network** > **DHCP** > **Settings** and perform the following configurations.

a Enable DHCP.

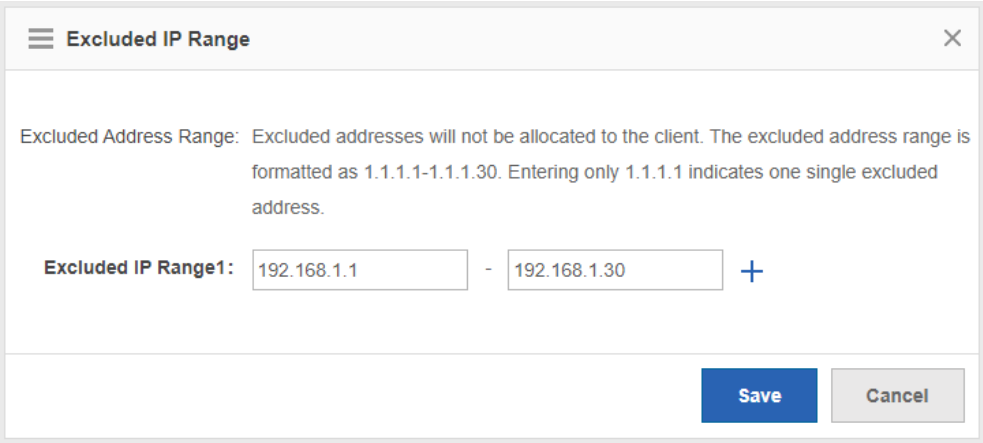
(3) Click **Add DHCP** to add a DHCP pool.



(4) Configure the DHCP pool, including the subnet, router, lease, and DNS server addresses.

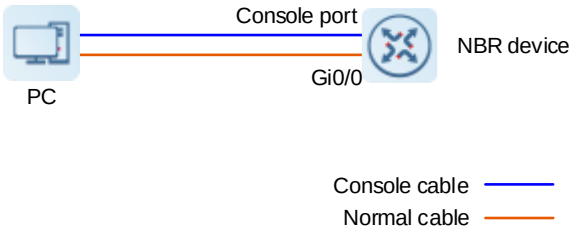


(5) Click **Excluded Address Range** and configure the excluded IP address range in the DHCP pool.



3.2.2 Configuring DHCP in CLI Mode

(1) Connect to the NBE router as shown in the following figure.



(2) Run the following commands in turn.

```
Ruijie>enable
Ruijie#configure terminal
Ruijie(config)#service dhcp       //Enable DHCP.
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. The default lease time is 24     hours.
Ruijie(dhcp-config)#network 192.168.1.0 255.255.255.0       //Configure an IP address range for the DHCP pool.
*The following is static IP distribution in DHCP.
Ruijie(dhcp-config)# hardware-address 0026.b90b.a48a       //Set the terminal MAC address to 0026.b90b.a48a.
Ruijie(dhcp-config)# host 192.168.1.150    255.255.255.0       //Configure a static IP address and mask.
*The above is static IP distribution in DHCP.

Ruijie(dhcp-config)#dns-server 192.168.58.110    8.8.8.8       //The primary DNS server address is 192.168.58.110 and the secondary IP address is 8.8.8.8.
Ruijie(dhcp-config)#default-router 192.168.1.1       //Set the router IP address.
Ruijie(dhcp-config)#end
Ruijie#write       //Save the configuration.
```

3.3 DNS Configuration

3.3.1 Working Principle

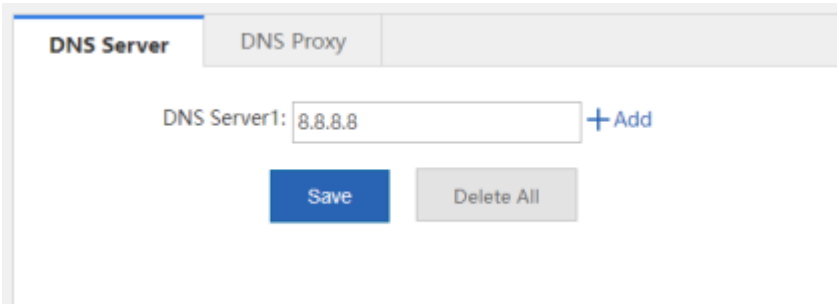
If DNS proxy is enabled, the NBR LAN port will intercept DNS traffic. Replace destination DNS server IP address with others which have been configured in WAN port, and then send the message to that new DNS server to associate the client to the new DNS server.

3.3.2 Effect

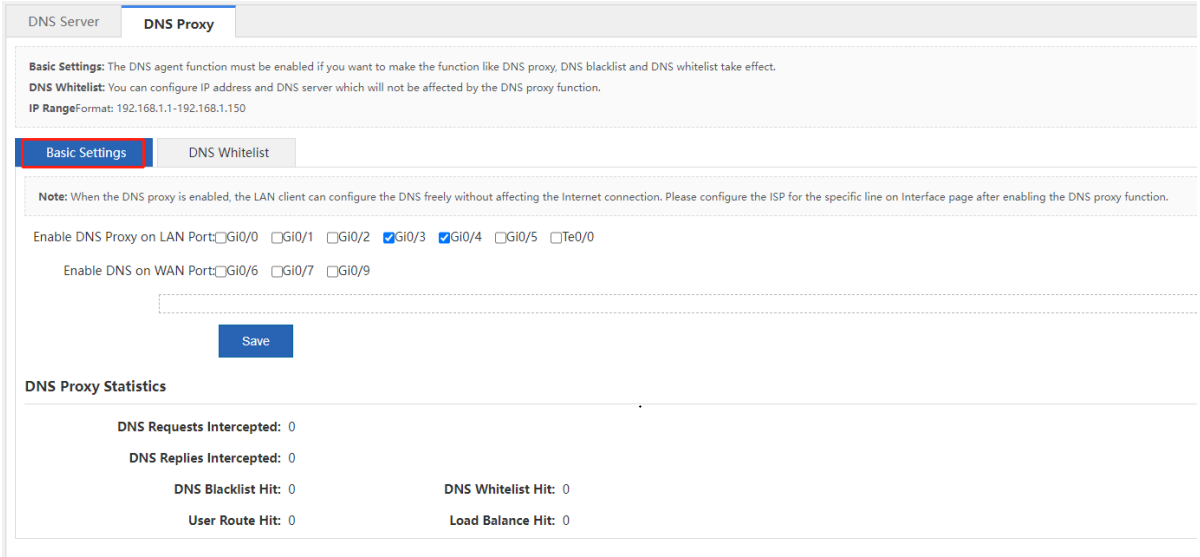
- Realize load balance. When a link is loaded heavily, the LAN port can intercept traffic of which the destination DNS server is in that link. And then replace destination with other DNS server not in that link.
- The DNS server can be configured on your PC freely. If an incorrect DHCP server address is configured, the LAN port can intercept the traffic and replace it with the correct one.
- Detect faulty link actively and switch to a new available DNS sever.

3.3.3 Procedure

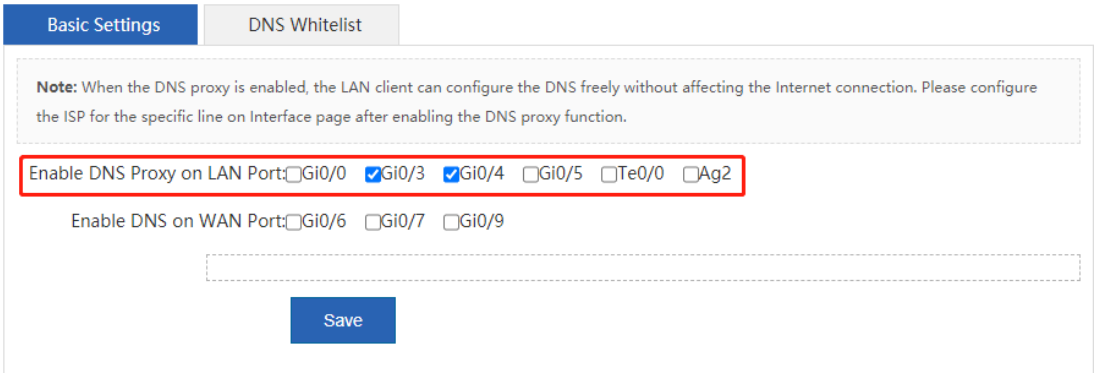
(1) Choose **Network** > **DNS Settings** > **DNS Server**, configure the DNS server address, and save the configuration.



(2) Choose **Network** > **DNS Settings** > **DNS Proxy** and click **Basic Settings**.



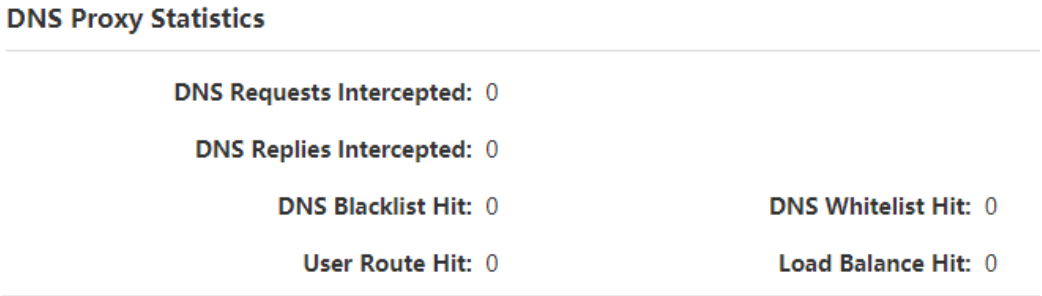
a Check the LAN ports where the DNS proxy will be enabled.



b Check the WAN ports connected to the DNS server, and configure the DNS server address of the corresponding line.

c Click **Save**.

d Check DNS proxy statistics.

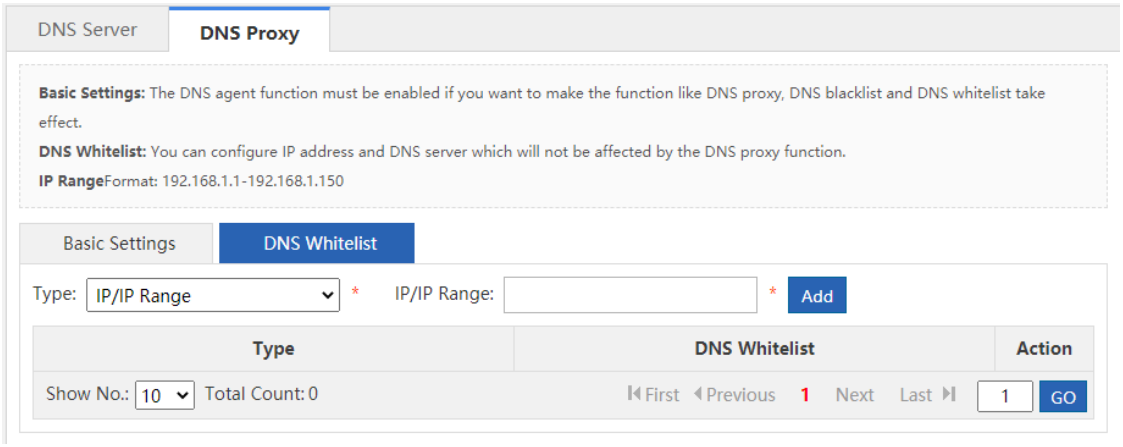


(3) Check the **DNS Whitelist** tab and set the configuration items.

The DNS Whitelist function is used to set special resources (including IP addresses and DNS servers) that are not affected by the DNS proxy function.

Select **IP/IP Range** or **DNS Server**, enter the corresponding IP address in the **IP/IP range** text box, and click **Add**.

The configuration will be displayed.



3.4 Behavior Policies

3.4.1 Basic Settings

1. Enabling of All Audit Functions

Application Scenario

1. The Router serves as an egress and can access the Internet by using a static IP address. The LAN user router is configured on the LAN port of the router to provide Internet access.

2. The WAN bandwidth is 10 Mbit/s, the WAN port address is 192.168.33.56/24, the WAN router address is 192.168.33.1, and the LAN is in the 192.168.1.0/24 network segment.

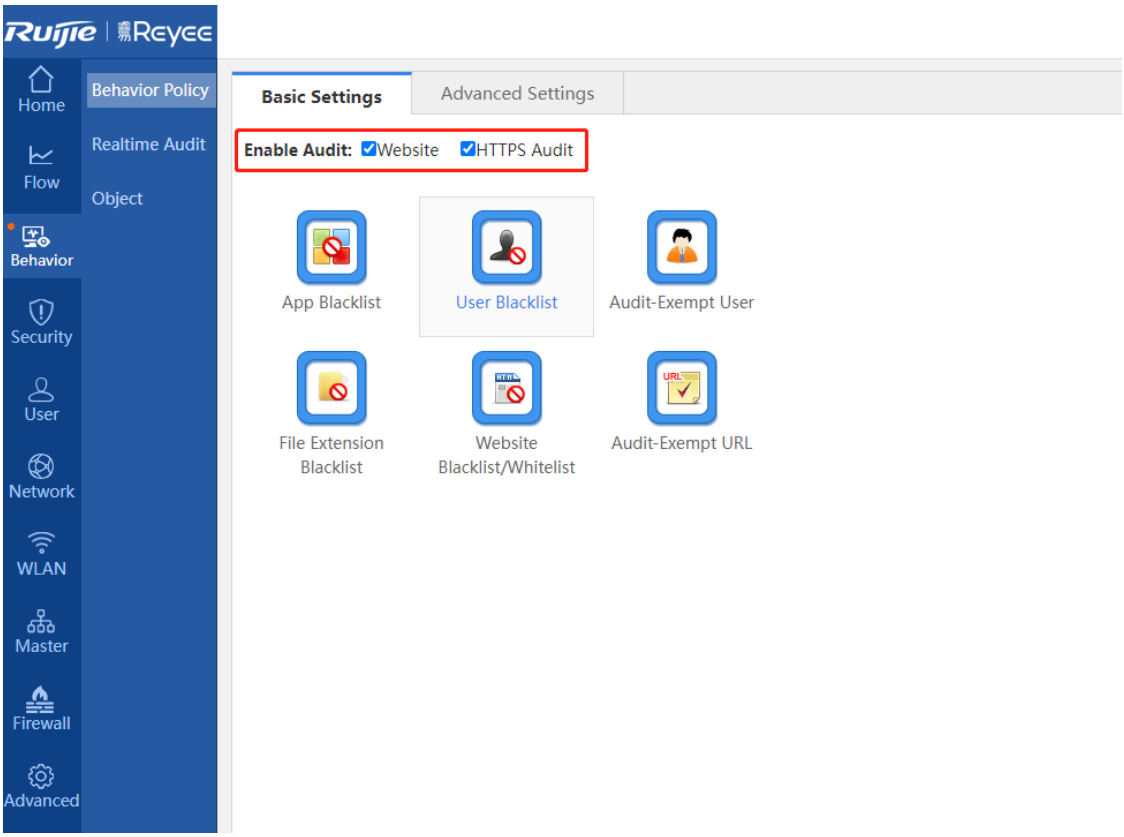
3. Users in the LAN business security group (192.168.1.2 to 192.168.1.100) are prohibited from accessing the Internet.

Prerequisites

All audit functions have been enabled on the **Basic Settings** page.

Procedure

Choose **Behavior** > **Behavior Policy** > **Basic Settings**, and check all audit functions.



Verification

View audit records of services in behavior reports.

2. User Blacklist

Application Scenario

1. The router serves as an egress and can access the Internet by using a static IP address. The LAN user router is configured on the LAN port of the router to provide Internet access.

2. The WAN bandwidth is 10 Mbit/s, the WAN port address is 192.168.33.56/24, the WAN router 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.

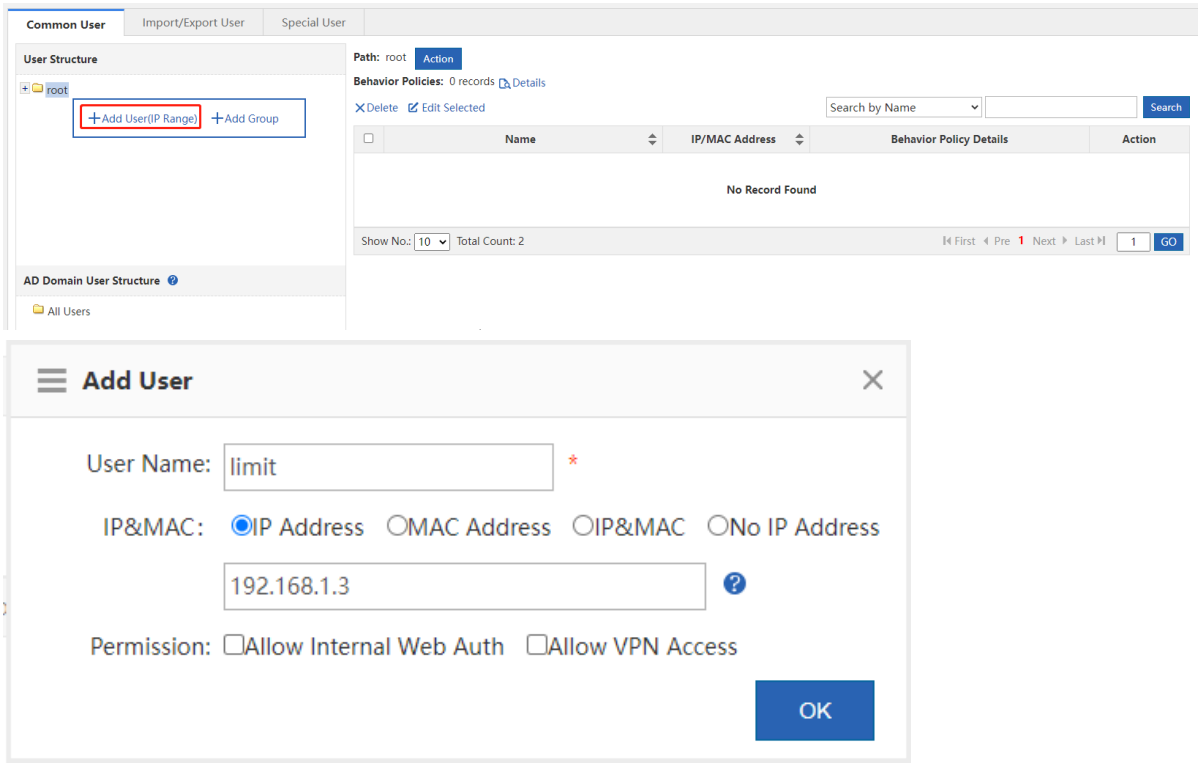
Prerequisite

1. Choose **User** > **User** to add the users that are prohibited from accessing the Internet.

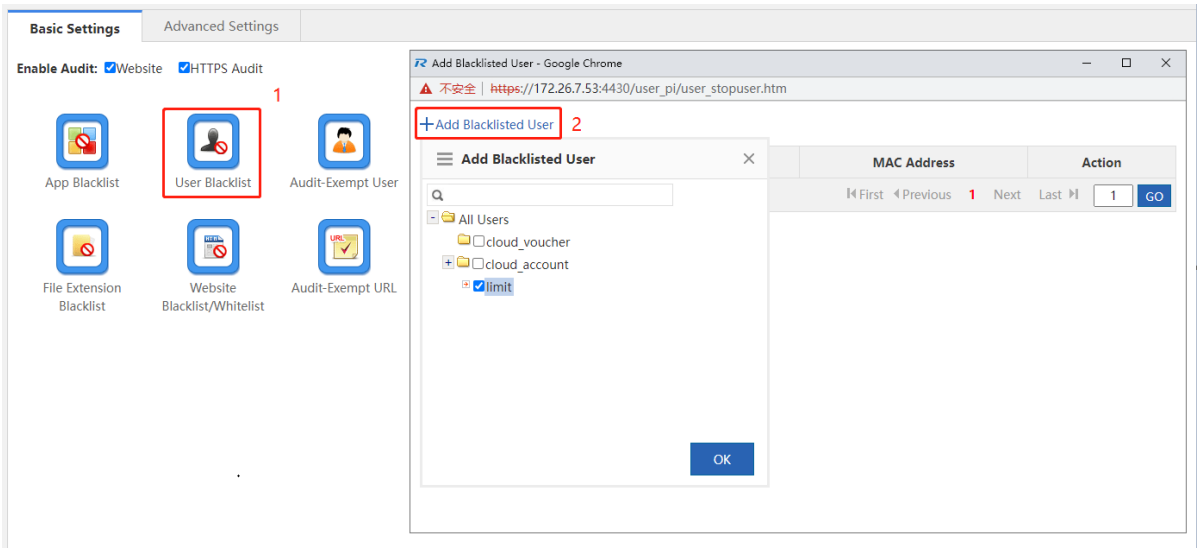
2. Choose **Flow** > **Behavior Policy** > **Basic Settings** and click **User Blacklist**.

Procedure

(1) Choose **User** > **User** > **Common User** and enter the IP addresses of the users that are prohibited from accessing the Internet.



(2) Choose **Behavior** > **Behavior Policy** > **Basic Settings**, and click **User Blacklist**.



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.

3. Website Blacklist

Application Scenario

1. The router serves as an egress and can access the Internet by using a static IP address. The LAN user router is configured on the LAN port of the router to provide basic Internet access.

2. The WAN bandwidth is 10 Mbit/s, the WAN port IP address is 192.168.33.56/24, the WAN router 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 www.baidu.com.

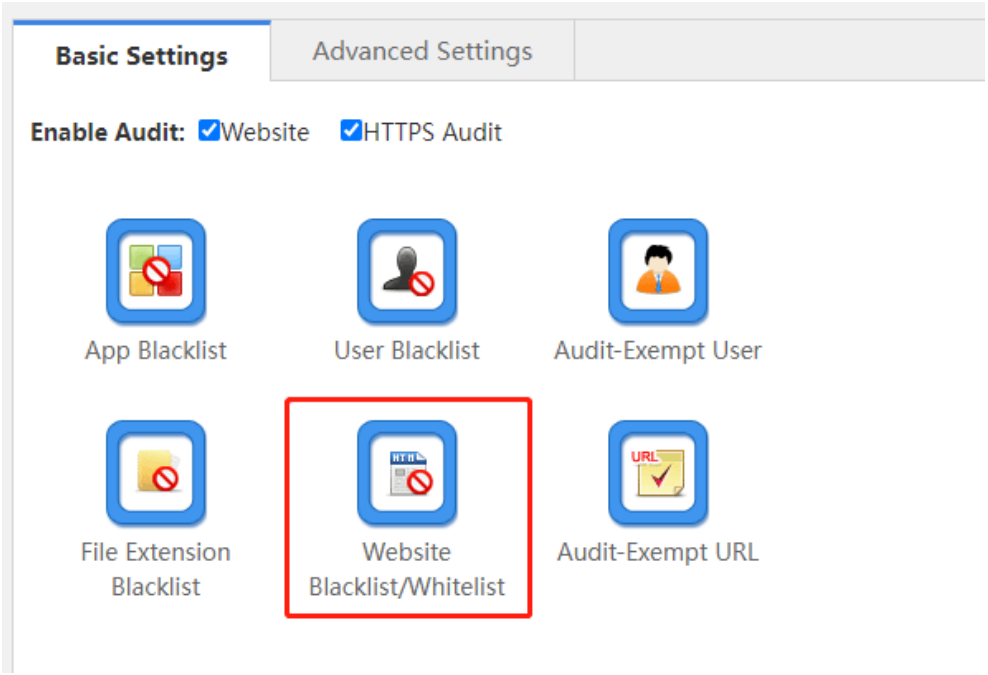
Prerequisites

1. Choose **User** > **User** > **Common User** and add users to be prevented from accessing the website www.baidu.com.

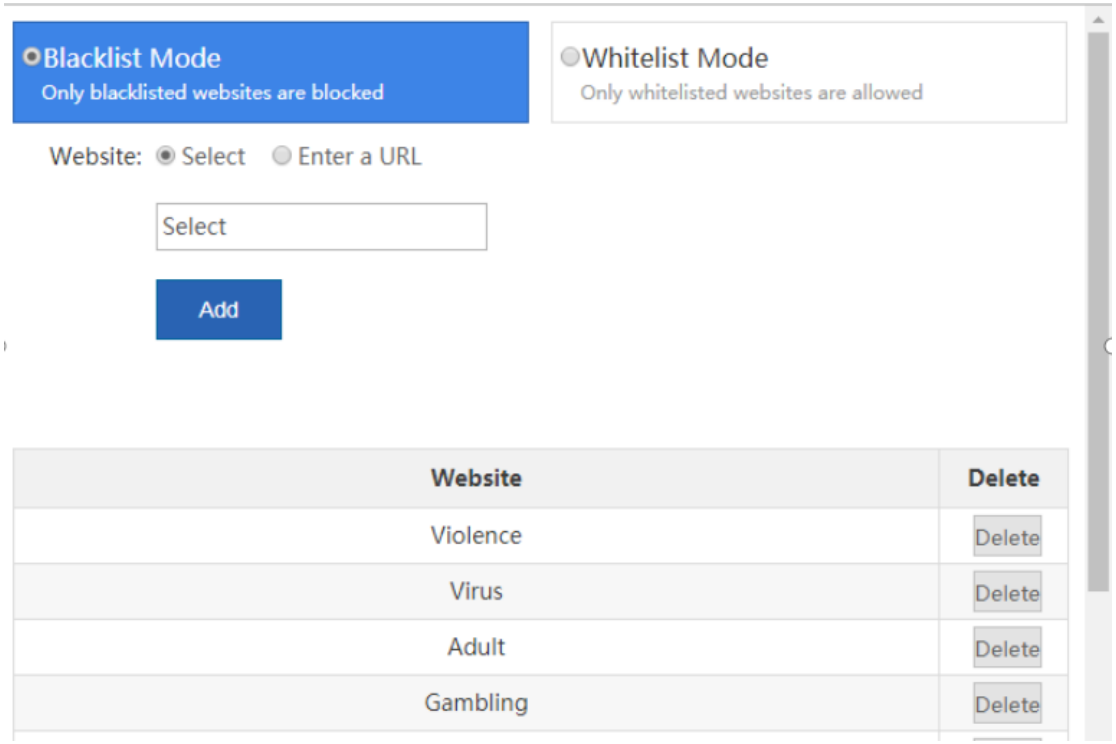
2. Choose **Flow** > **Behavior Policy** > **Basic Settings**, click **Website Blacklist/Whitelist**, and click **Blacklist Mode**.

Procedure

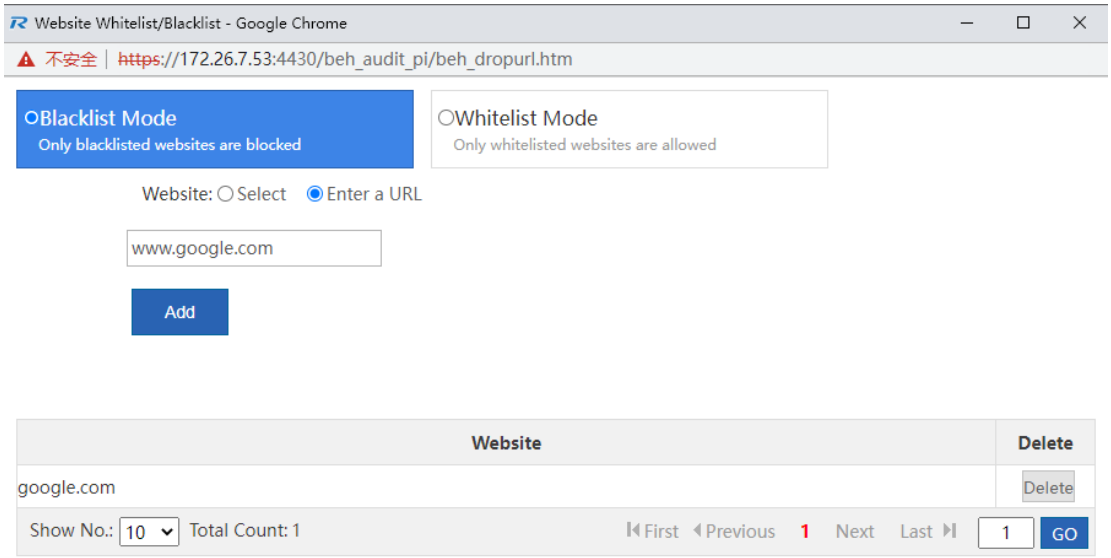
(1) Choose **Behavior** > **Behavior Policy** > **Basic Settings** and click **Website Blacklist/Whitelist**.



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



The URL categories displayed after you click **Select** are default website classifications. You can also click **Enter a URL** to enter a URL.



Keyword matching is also supported. 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.

Verification

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

4. Website Whitelist

Application Scenario

1. The router serves as an egress and can access the Internet by using a static IP address. The LAN user router is configured on the LAN port of the NBR router to provide basic Internet access.

2. The WAN bandwidth is 10 Mbit/s, the WAN port address is 192.168.33.56/24, the WAN router 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.

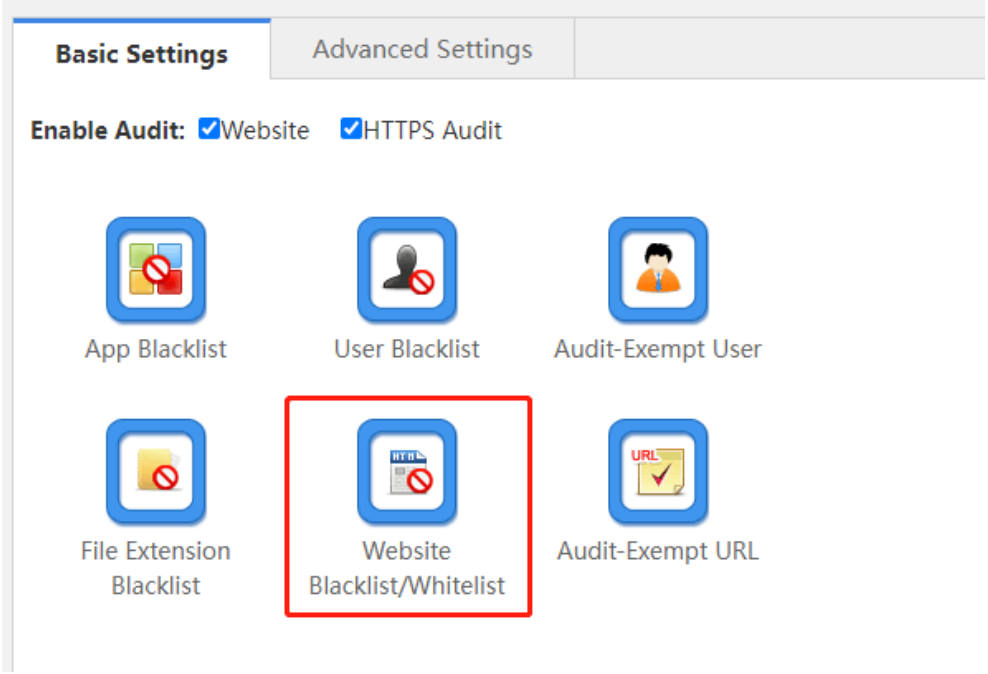
Prerequisites

1. Choose **User** > **User** and add user IP addresses.

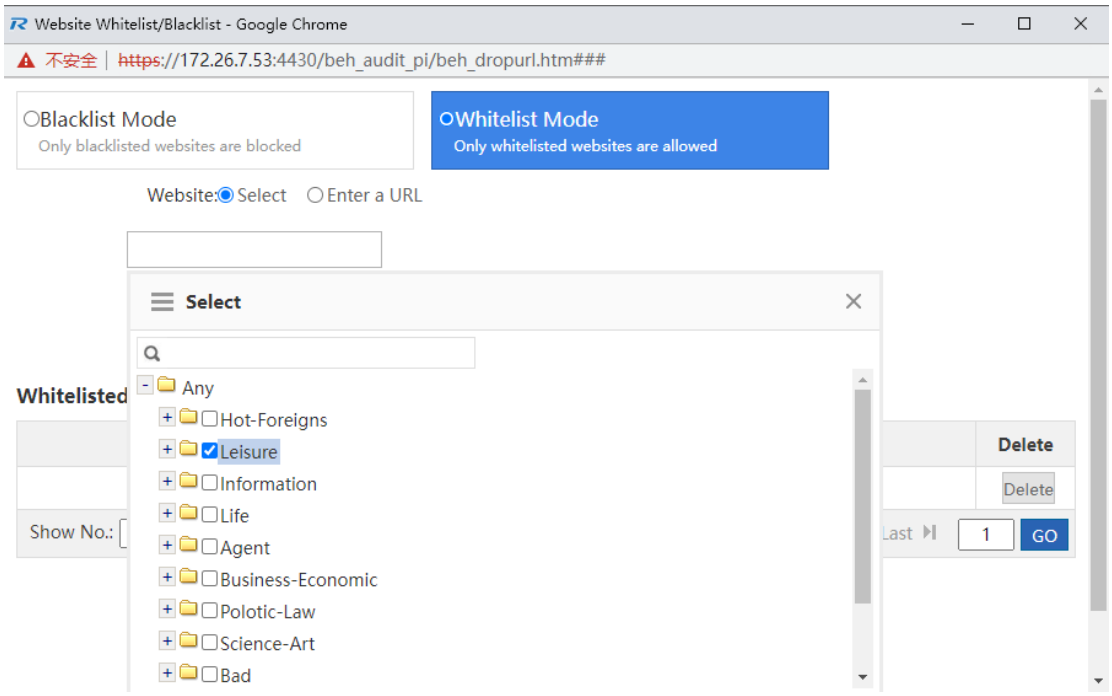
2. Choose **Flow** > **Behavior Policy** > **Basic Settings**, click **Website Blacklist/Whitelist**, and click **Whitelist Mode**.

Procedure

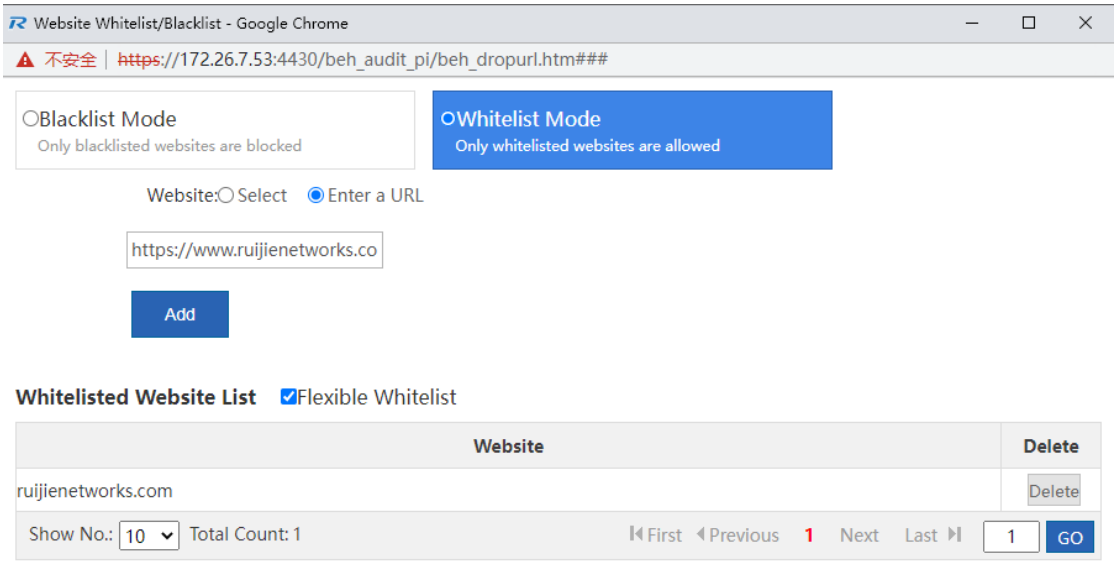
(1) Choose **Behavior** > **Behavior Policy** > **Basic Settings** and click **Website Blacklist/Whitelist**.



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



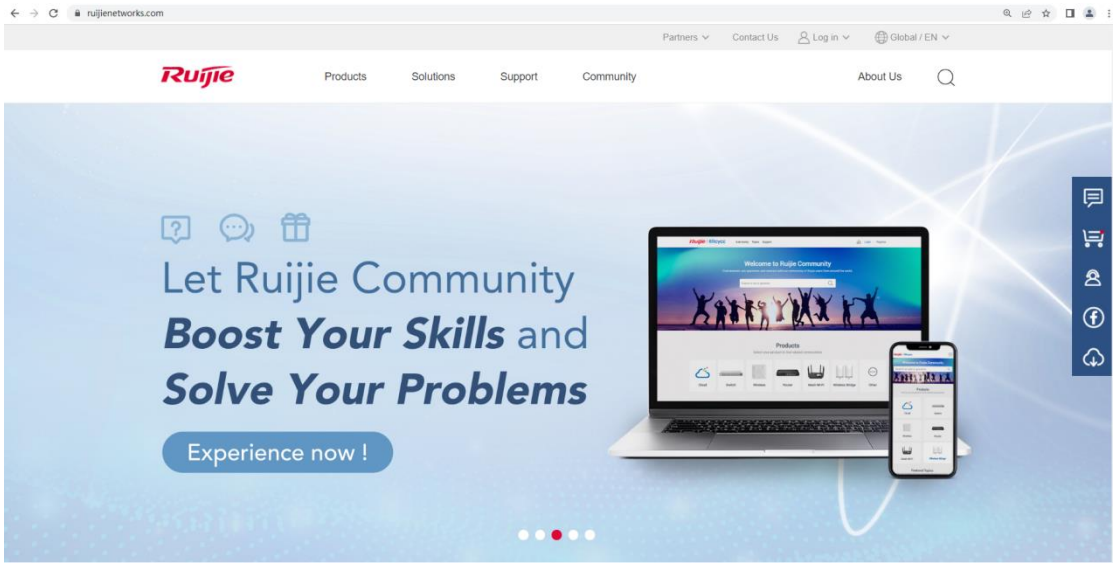
The URL categories displayed after selecting **Select** are default ones of the device. Alternatively, you can click **Enter a URL** to enter a URL.



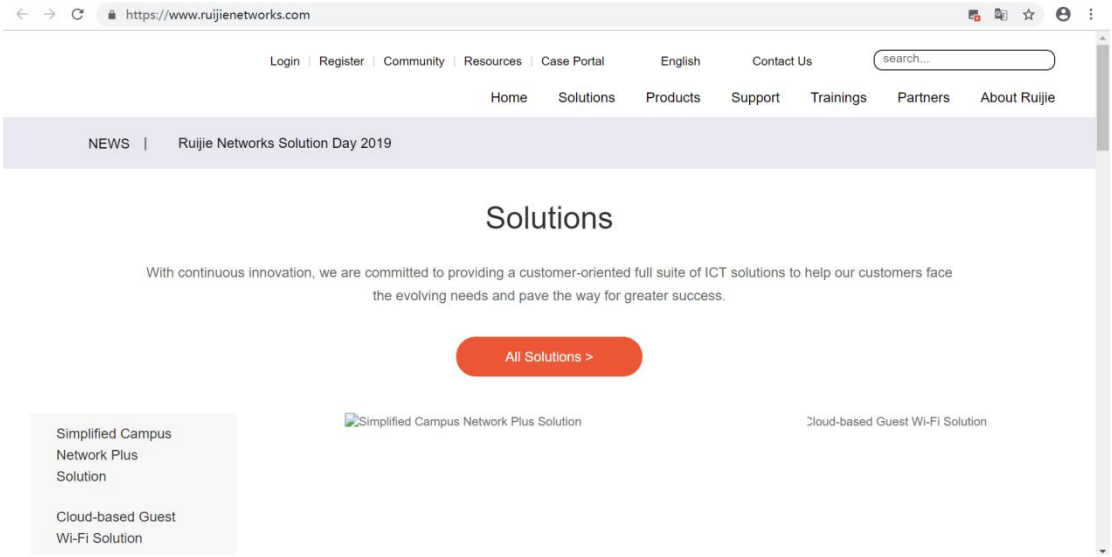
Flexible Whitelist: After **Flexible Whitelist** is selected, some pictures not belonging to a whitelisted website can be displayed when the whitelisted website is accessed. For details, see "Verification".

Verification

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



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



Accessing other websites is prohibited.

5. Audit-Exempt URL

Application Scenario

1. The router serves as an egress and can access the Internet by using a static IP address. The LAN user router is configured on the LAN port of the NBR router to provide basic Internet access.

2. The WAN bandwidth is 10 Mbit/s, the WAN port address is 192.168.33.56/24, the WAN router 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.

Prerequisites

1. Choose **User** > **User** > **Common User** and add users who can access the audit-exempt website www.google.com.

2. Choose **Behavior** > **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 website audit exemption policy has a high priority. If you block the websites of the preceding two categories in **Behavior Policy** > **Advanced Settings**, the websites may fail to be blocked.

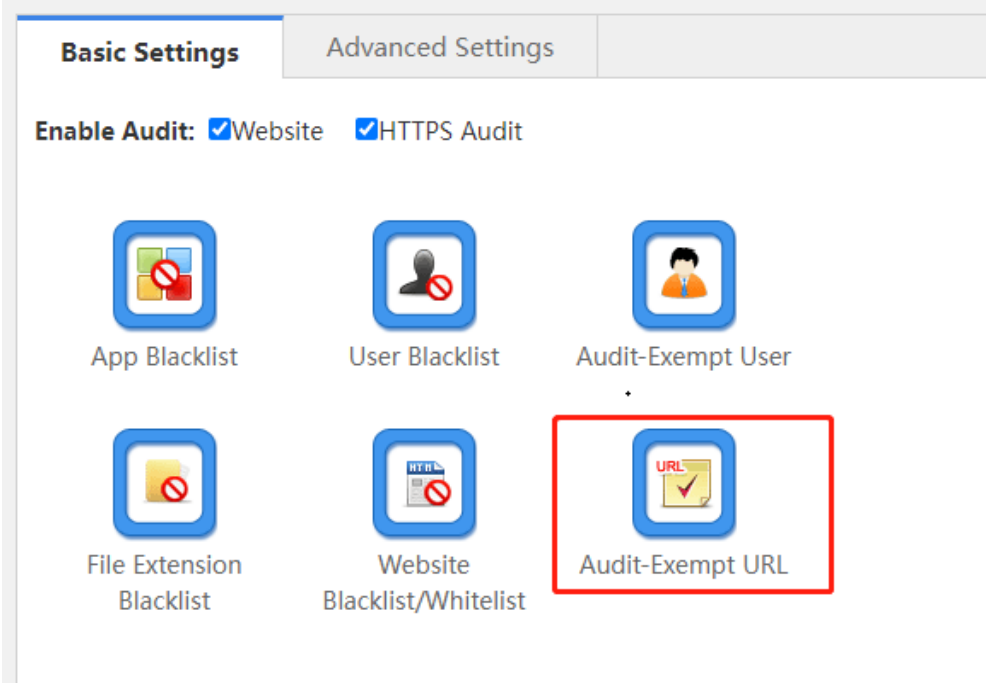
For example, a user configures a behavior policy to block www.360safe.com, which belongs to the system upgrade category by default. The website audit exemption policy has a higher priority and users can still access www.360safe.com even if this website is configured in a different category. To avoid such a case, perform the following operations:

(1) Check whether the category of the website www.360safe.com is correct. If not, contact R&D engineers.

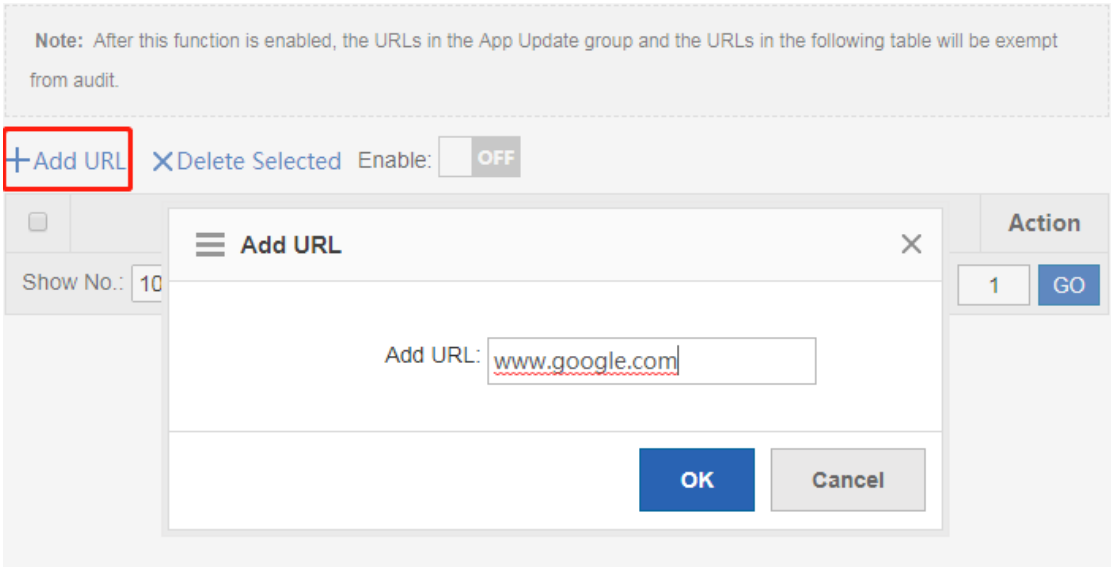
(2) Run commands on the CLI to delete the system upgrade category from the website audit exemption policy. If you still want to exempt other websites of the system upgrade category from audit, configure websites with priorities lower than that of the policy for blocking www.360safe.com on **Advanced Settings**.

Procedure

(1) Choose **Behavior** > **Behavior Policy** > **Basic Settings** and click **Audit-Exempt URL**.



(2) Click **Add URL** to add a URL.



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.

3.4.2 Advanced Settings

1. Website Access Policy

Application Scenario

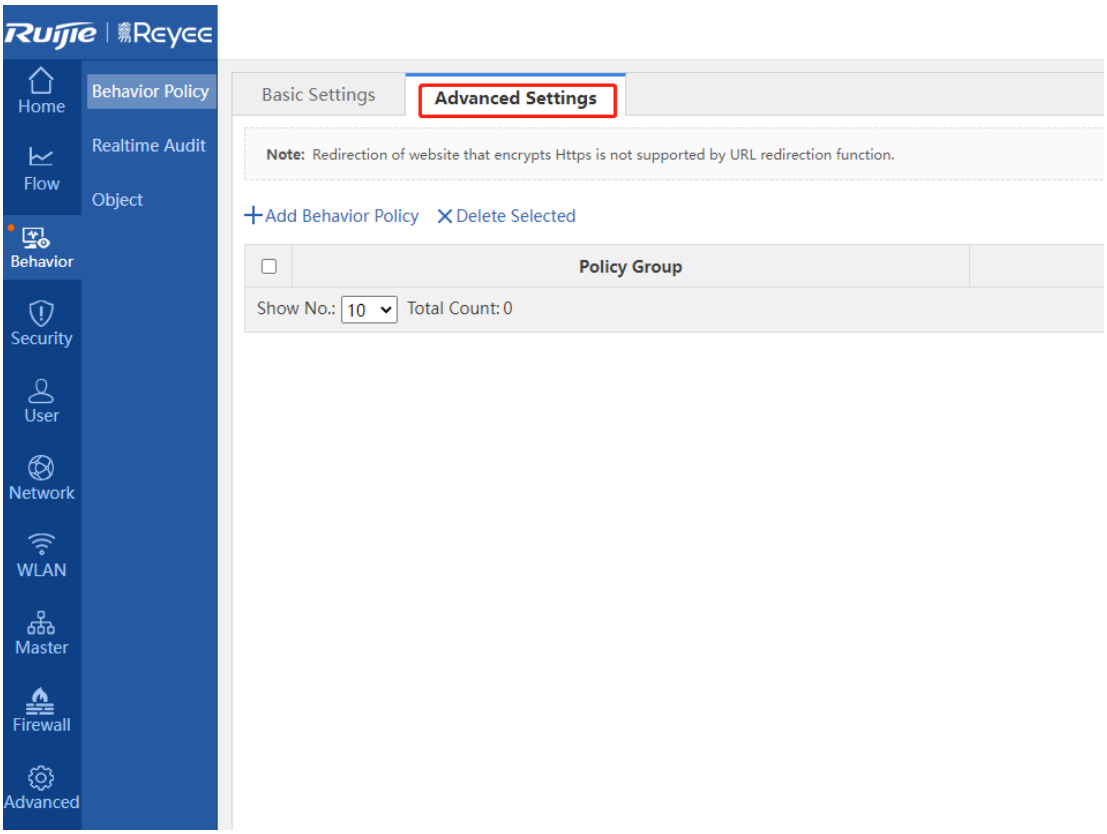
1. The router serves as an egress and can access the Internet by using a static IP address. The LAN user router is configured on the LAN port of the NBR router to provide basic Internet access.

2. The WAN bandwidth is 10 Mbit/s, the WAN port address is 192.168.33.56/24, the WAN router address is 192.168.33.1, and the LAN is in the 192.168.1.0/24 network segment.

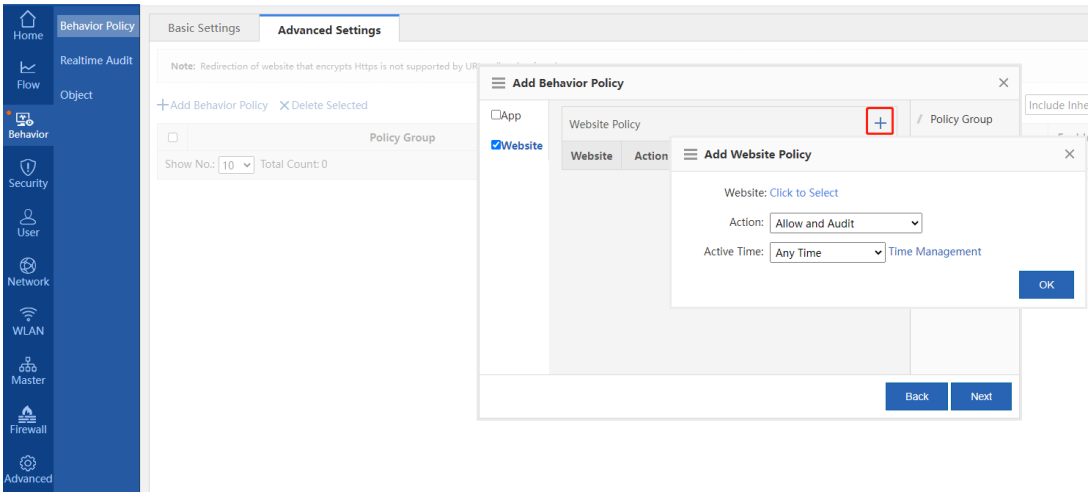
3. All LAN users are prohibited from accessing online shopping websites such as www.taobao.com.

Prerequisites

(1) Choose **Behavior** > **Behavior Policy** > **Advanced Settings**.



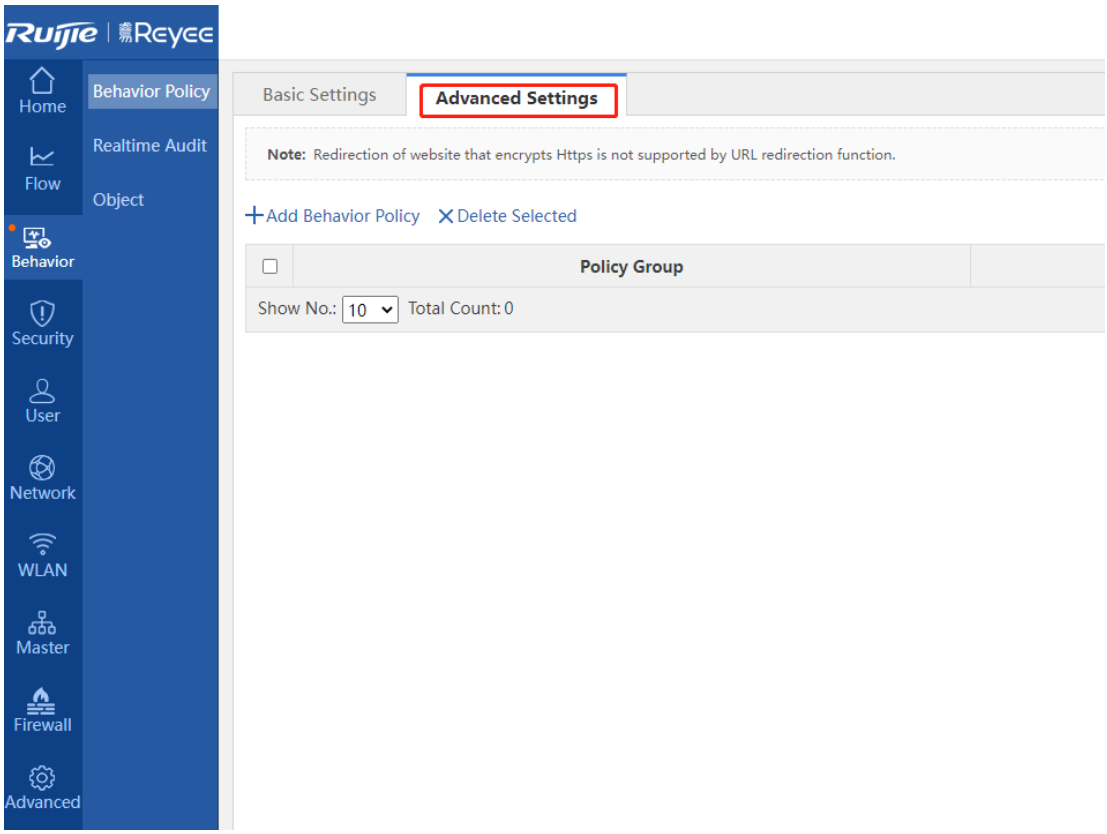
(2) Configure a website access policy during policy creation.



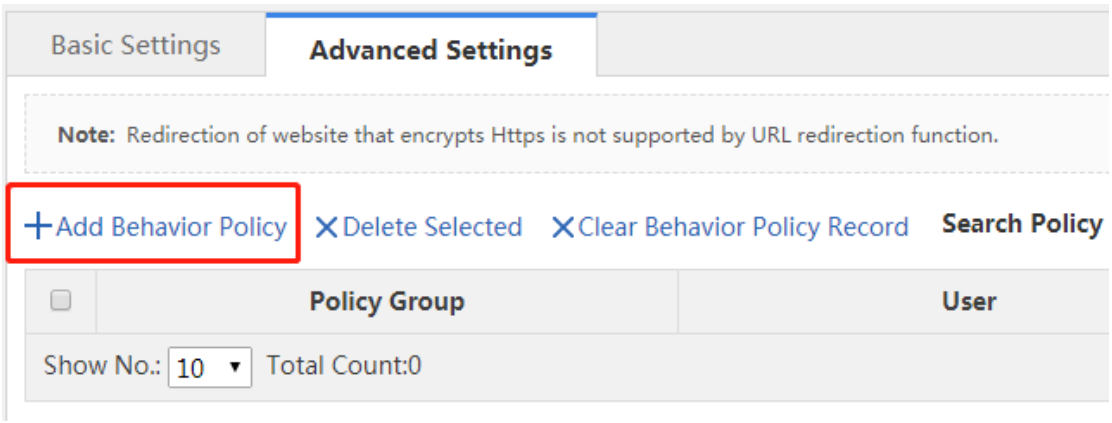
(3) If the policy does not take effect after the configuration is complete, check whether the user objects, application time, and selected applications are correct in policy configuration.

Procedure

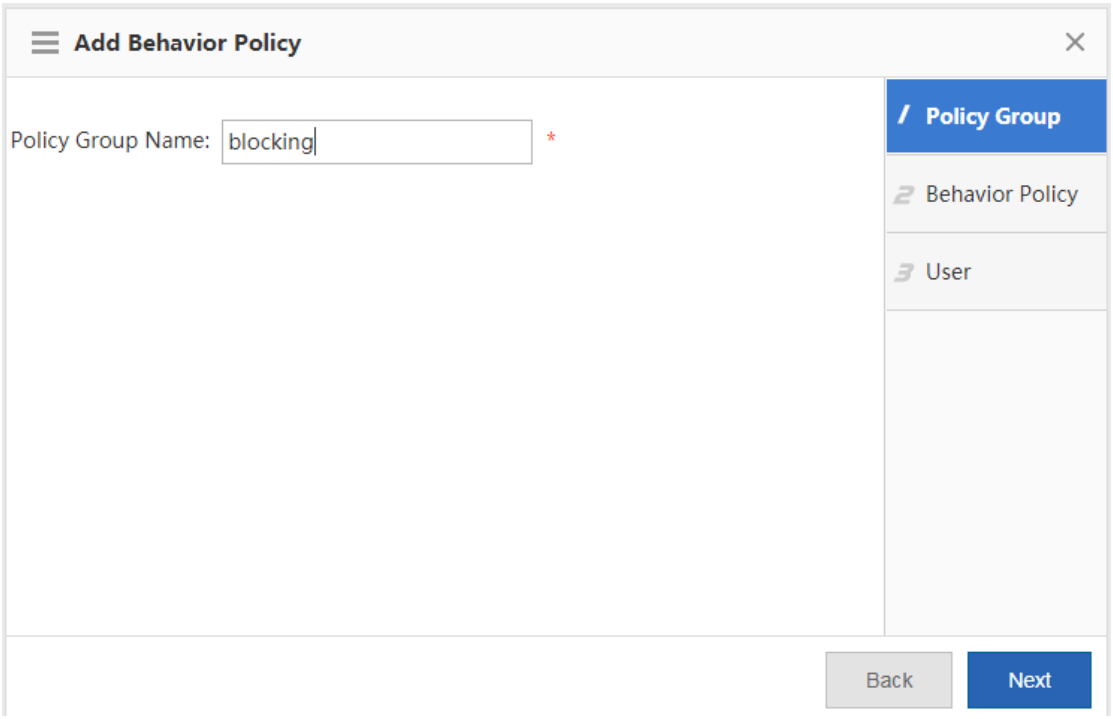
(1) Choose **Behavior** > **Behavior Policy** > **Advanced Settings**.



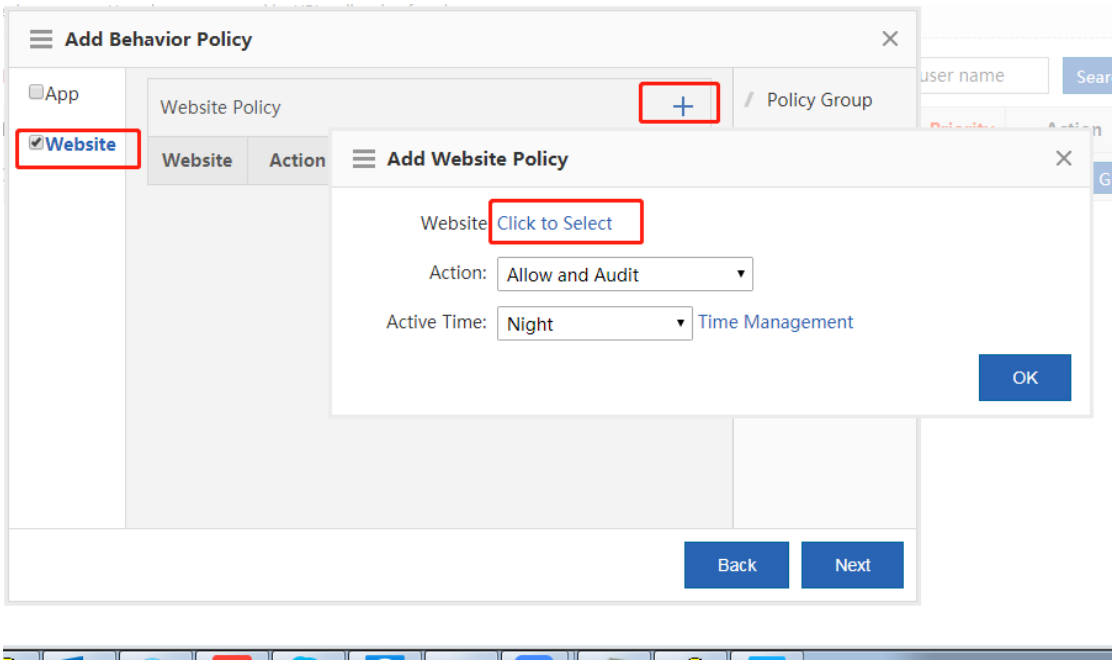
(4) Click **Add Behavior Policy**.



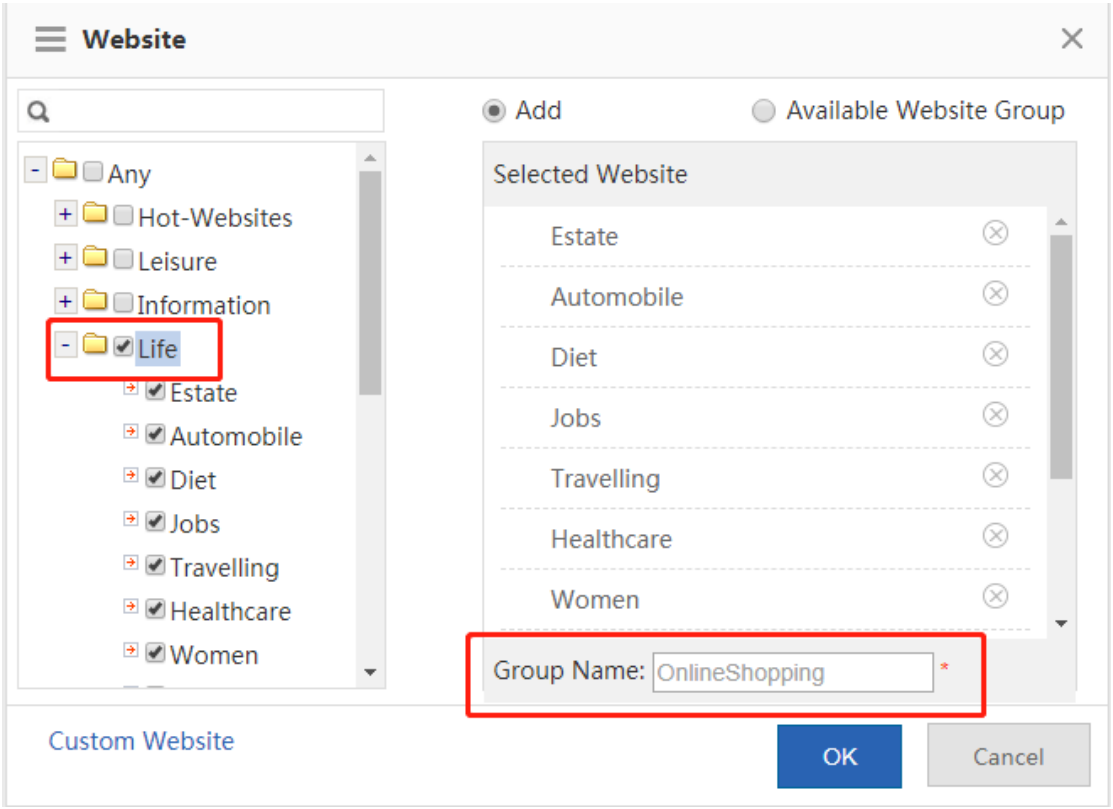
a Enter the name of a policy.



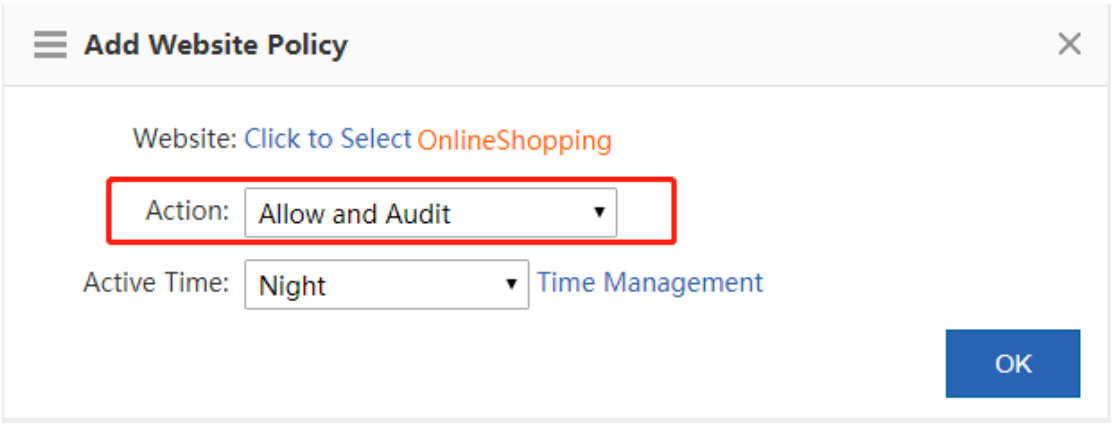
b Configure a behavior control policy.



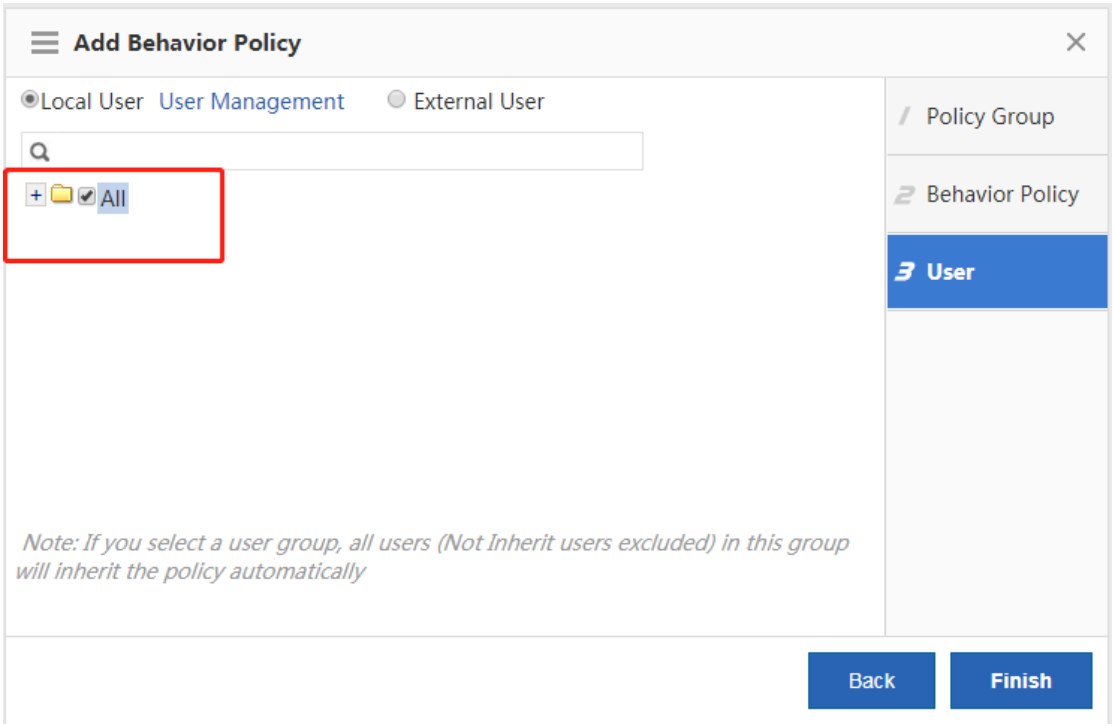
c Select the online shopping website defined previously.



d Select **Deny and Audit** from the **Action** drop-down list box.



e Associate users.

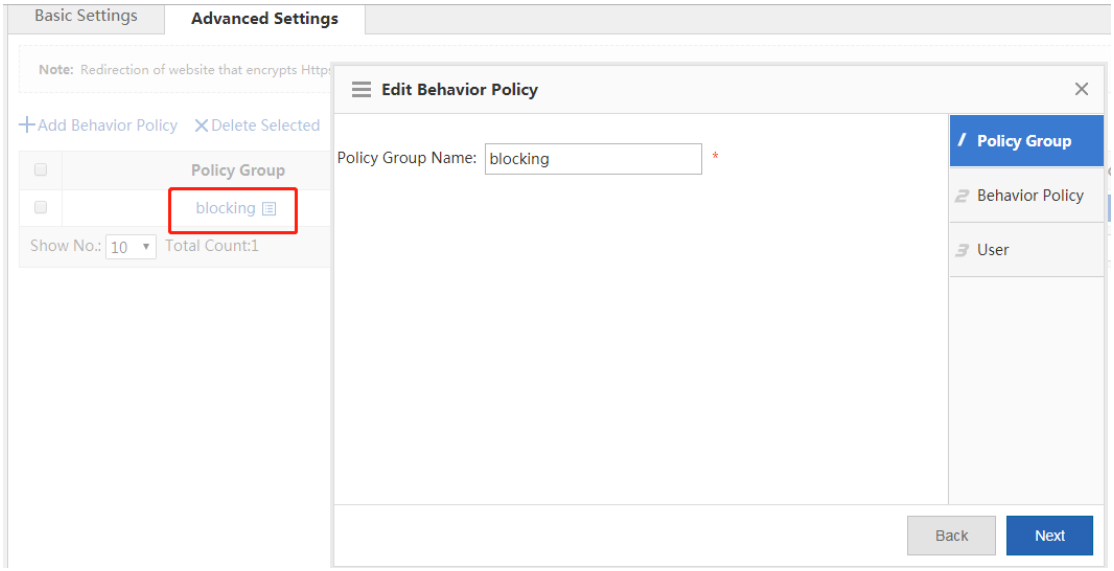


f Click **Finish** to generate the policy.

Note

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

(5) View the configured policy on **Advanced Settings**.



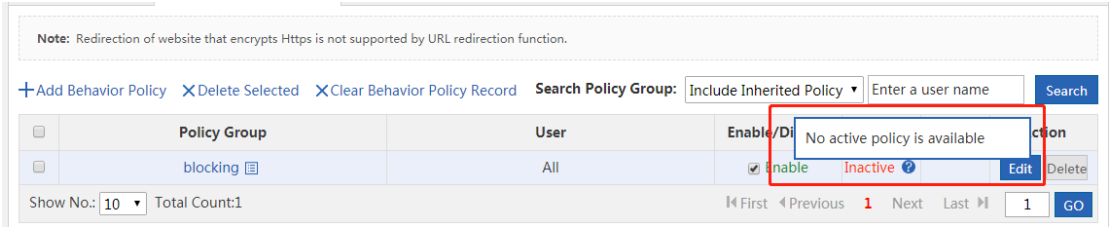
Note

A policy configured later takes effect. This is because policies are matched from top down.

Verification

When a user accesses www.taobao.com, a message 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.

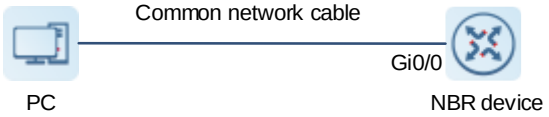


2. HTTPS Domain Name Filtering and Audit

Application Scenario

1. The router serves as an egress and can access the Internet by using a static IP address. The LAN user router is configured on the LAN port of the NBR router to provide basic Internet access.
2. LAN users' access to HTTPS websites can be audited and blocked.

Figure 3-1 Network Topology

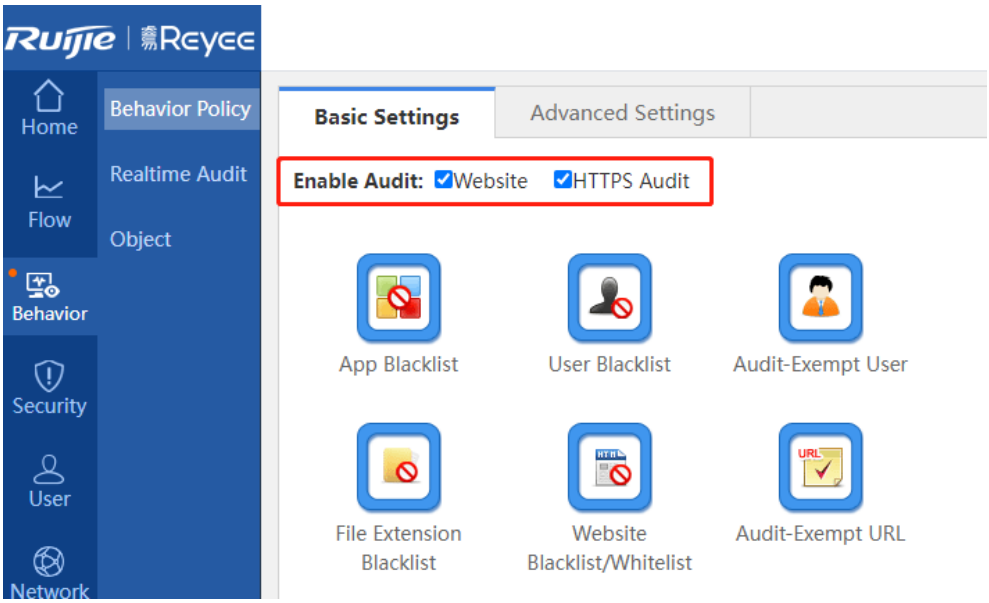


Prerequisites

1. On **Basic Settings**, use the default audit policy to audit 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.

Procedure

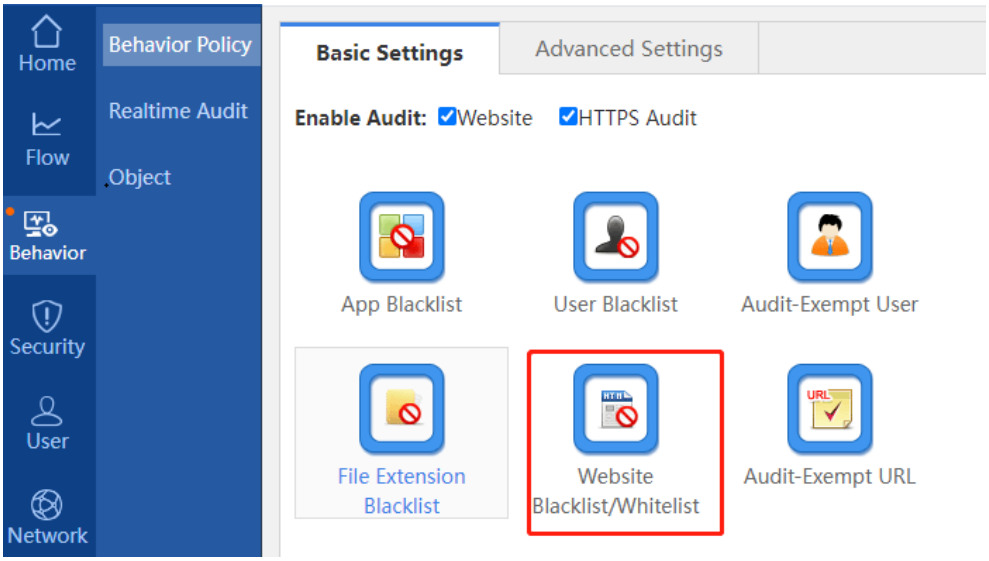
Method 1: Enable the HTTPS domain name audit on **Basic Settings**.
Choose **Behavior** > **Behavior Policy** > **Basic Settings** and select **Website** and **HTTPS Audit** in **Enable Audit** to enable HTTPS domain name audit.

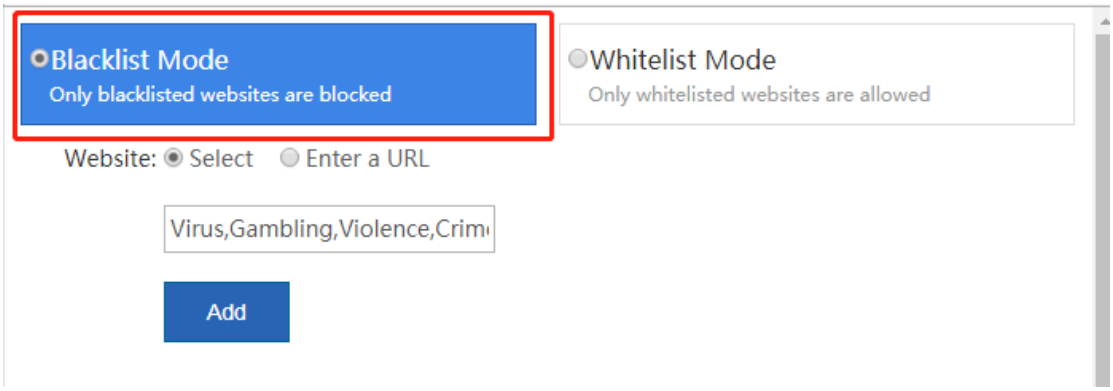


Method 2: Add websites to a blacklist on **Basic Settings**.

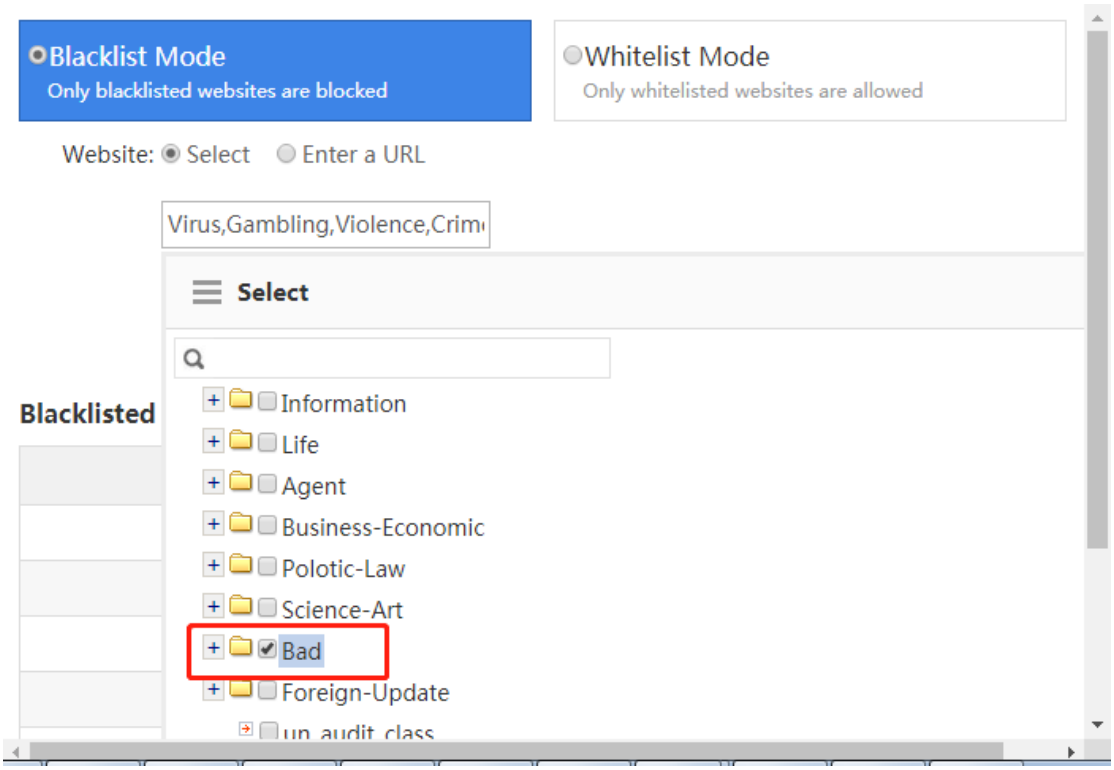
(1) Choose **Behavior** > **Behavior Policy** > **Basic Settings** and select **HTTPS Audit** in **Enable Audit** to enable HTTPS website audit.

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

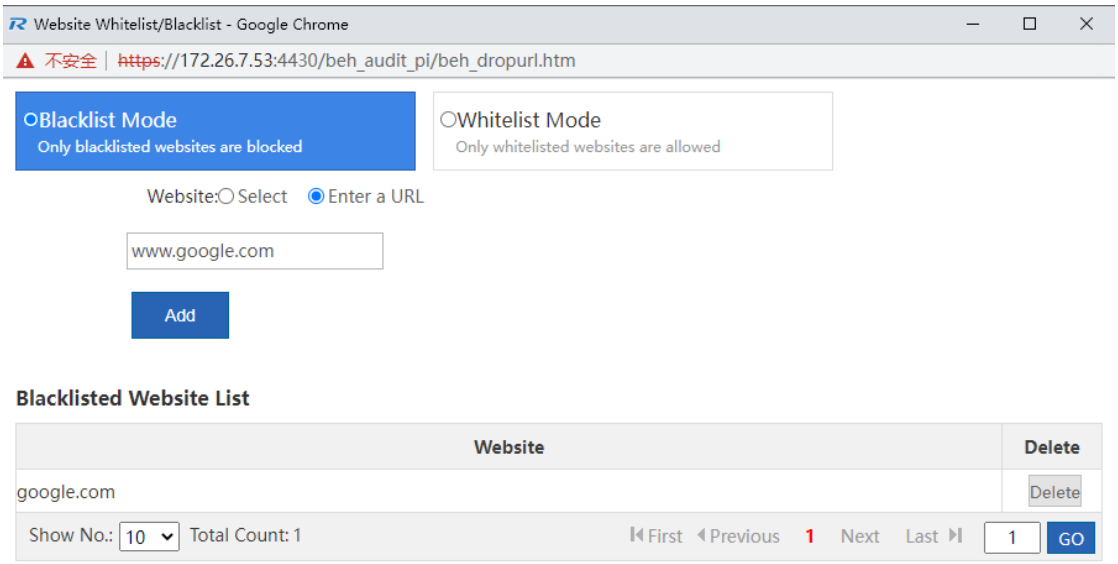




(3) Click **Select**, click the text box, and select websites to be blocked.

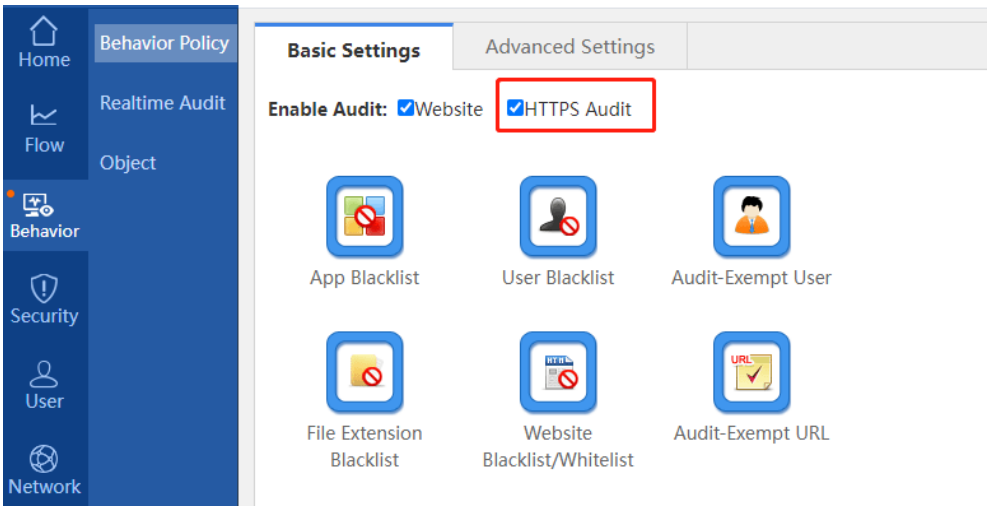


(4) Click **Enter a URL** and enter the website to be blocked in the text box.

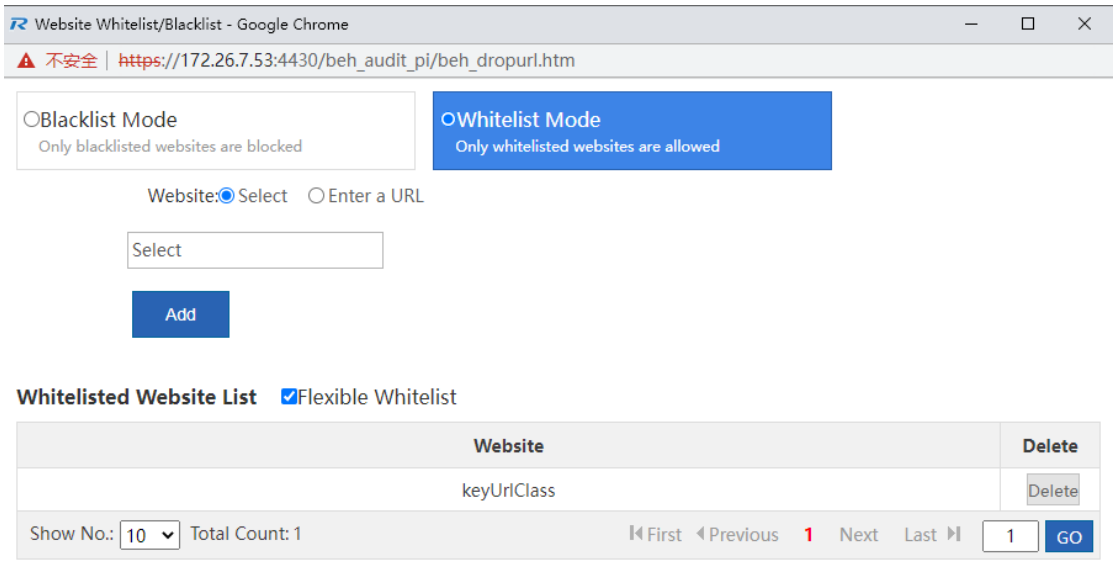


Method 3: Add websites to a whitelist on **Basic Settings**.

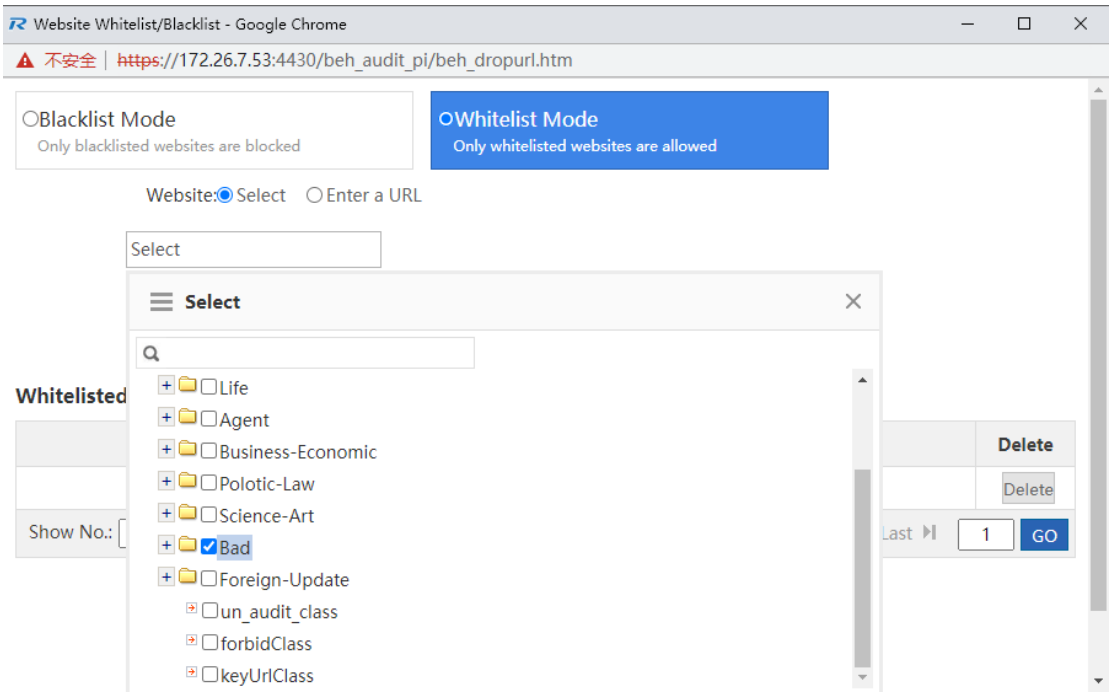
(1) Choose **Behavior** > **Behavior Policy** > **Basic Settings** and select **HTTPS Audit** in **Enable Audit** to enable HTTPS website audit.



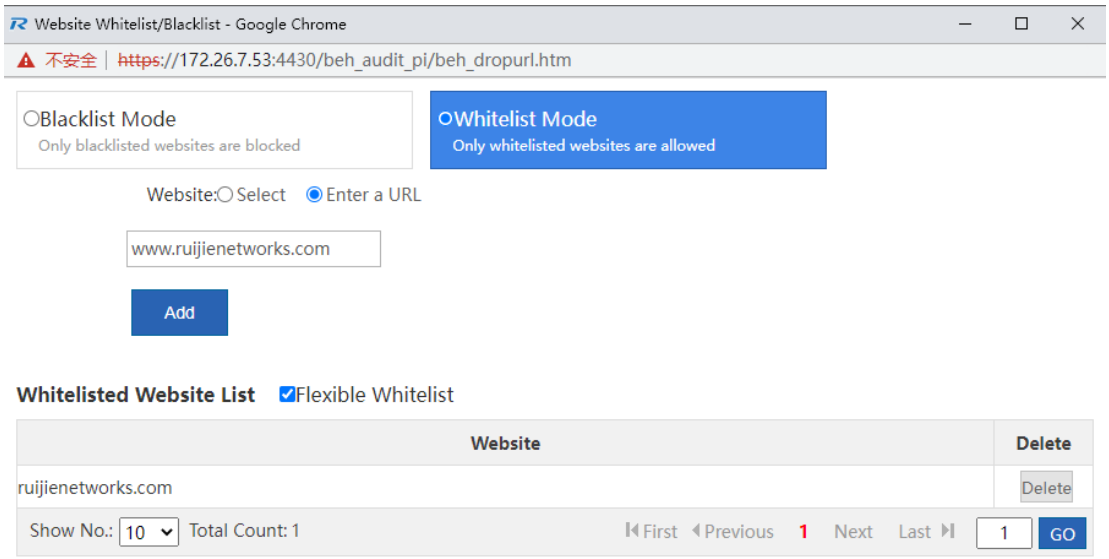
(2) Choose **Behavior** > **Behavior Policy** > **Basic Settings,** click **Website Blacklist/Whitelist**, and click **Whitelist Mode**.



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



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

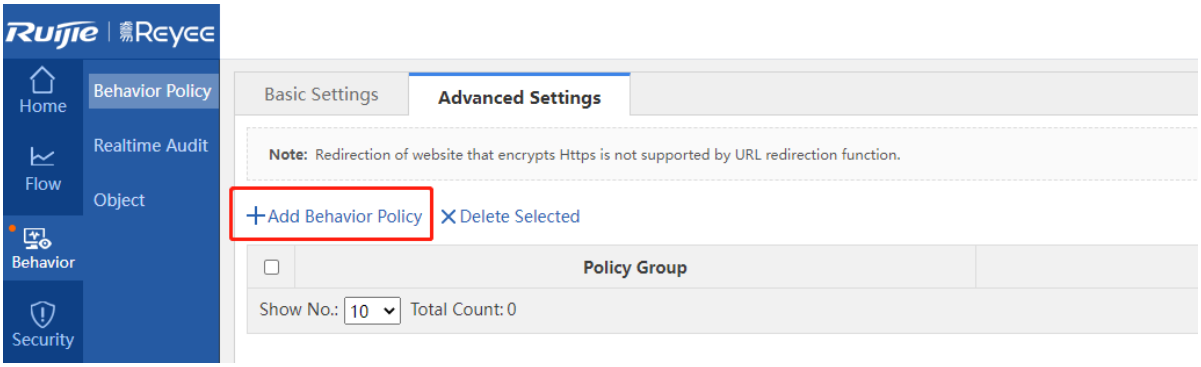


Method 4: Configure the HTTPS website blocking/allowing and audit/audit exemption functions on **Advanced Settings**.

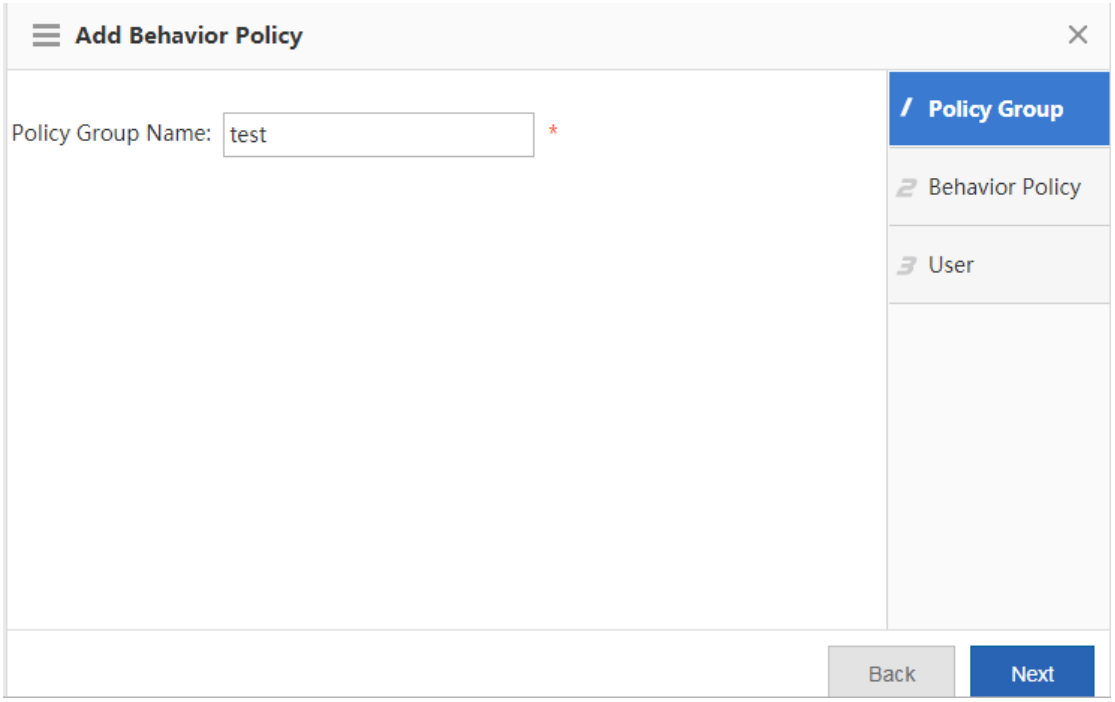
(1) Choose **Behavior** > **Behavior Policy** > **Basic Settings** and select **HTTPS Audit** in **Enable Audit** to enable HTTPS website audit.

(2) Choose Behavior > Behavior Policy > Advanced Settings and click Add Behavior Policy to create a behavior policy.

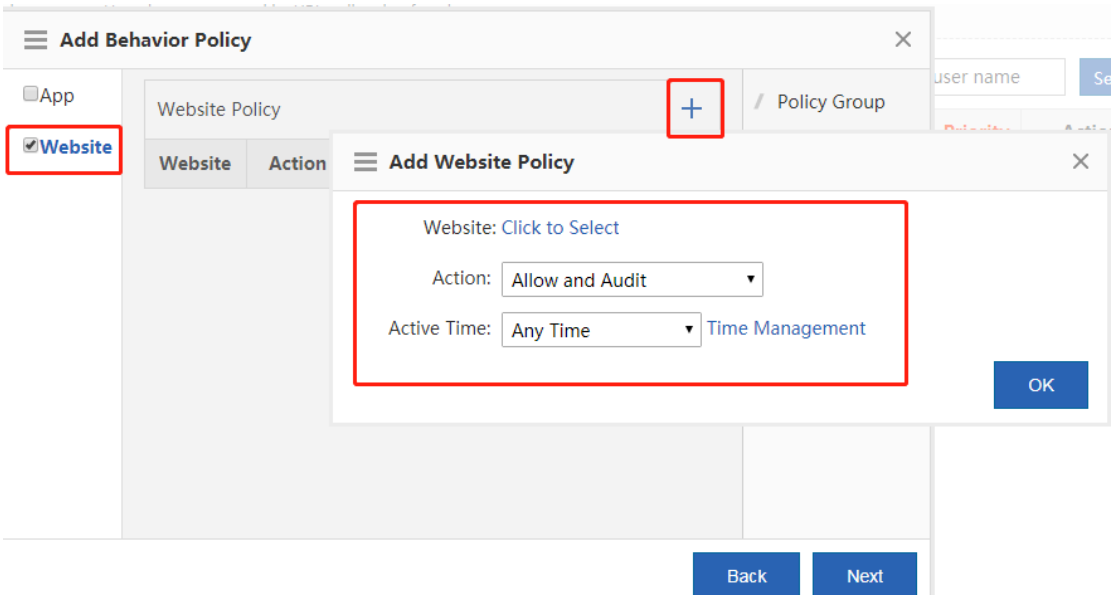
Alternatively, click an existing behavior policy to be modified in the list.



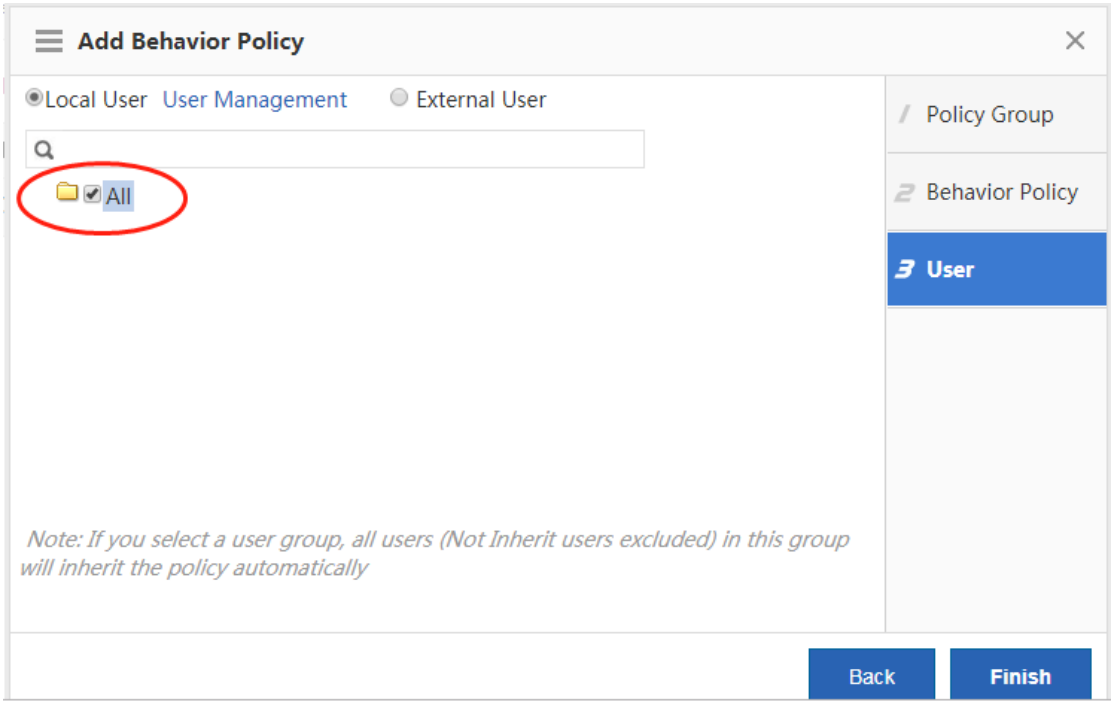
(3) Click **Policy Group** to set the name of a policy group.



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

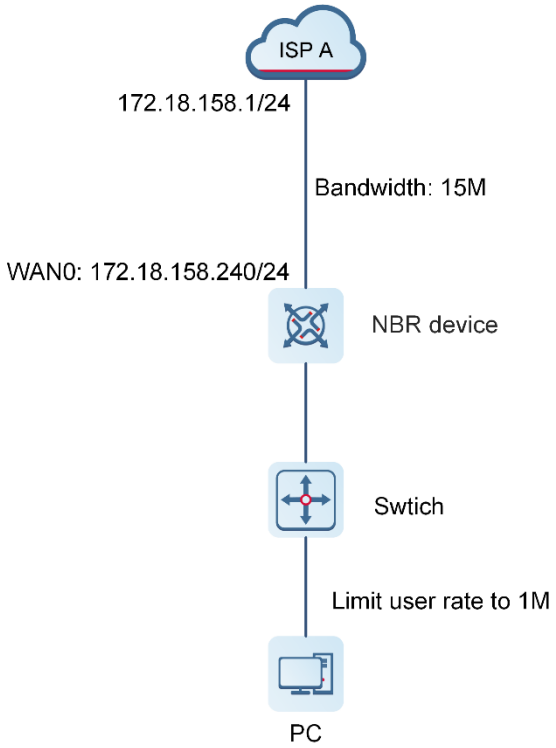


(5) Click **User** to apply the policy group to users or a user group.



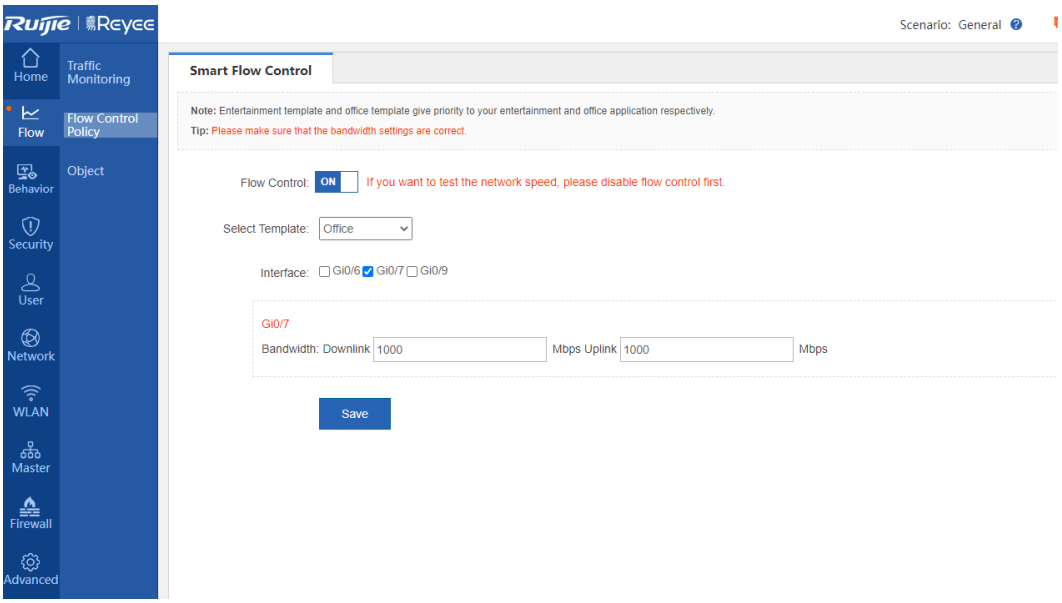
3.5 Rate Limit

Application Scenario

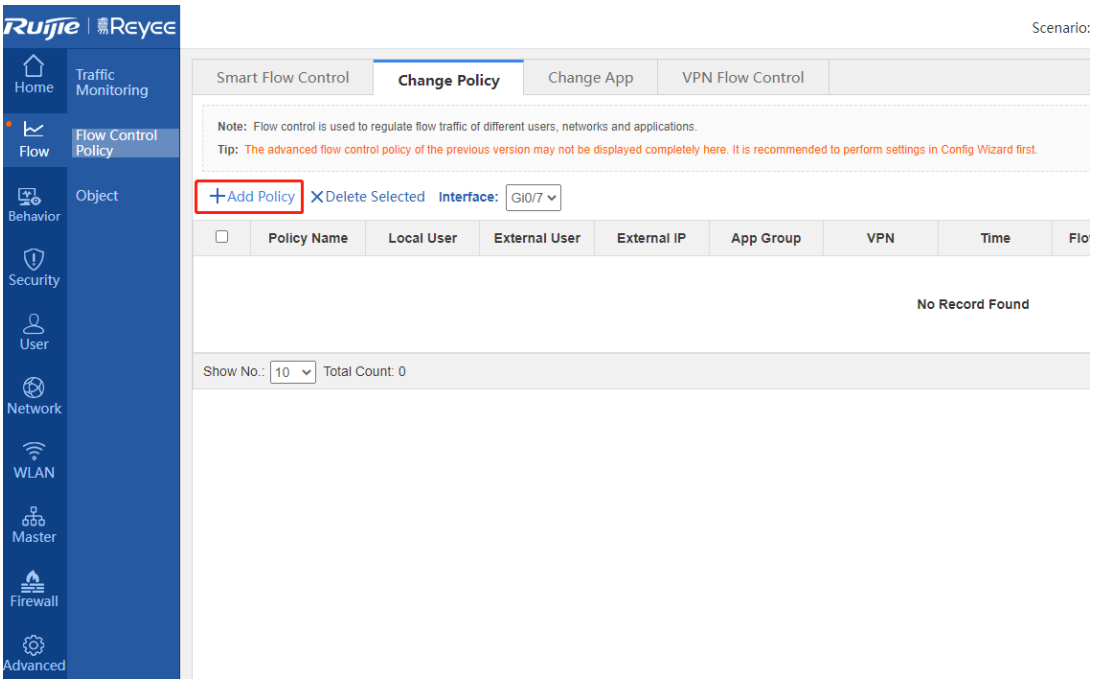


Procedure

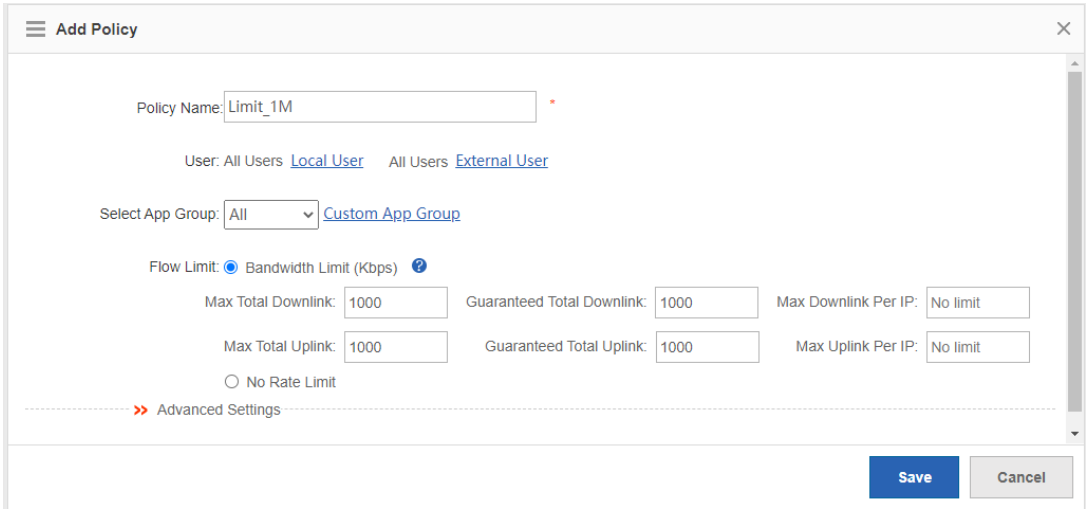
(1) Choose **Flow** > **Flow Control Policy** > **Smart Flow Control** and enable **Flow Control**.



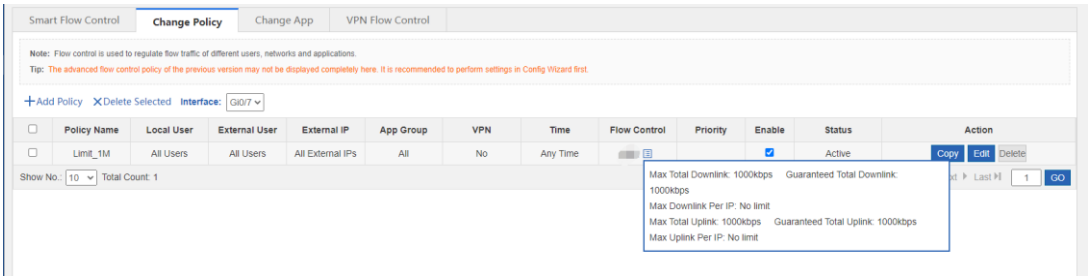
(2) Choose **Flow** > **Flow Control Policy** > **Change Policy** and add a flow control policy.



(3) Add a policy and click **Save**.



(4) Confirm whether the policy is configured correctly.



(5) Use Speedtest tool to verify the rate limit setting

3.6 Port Mapping

Application Scenario

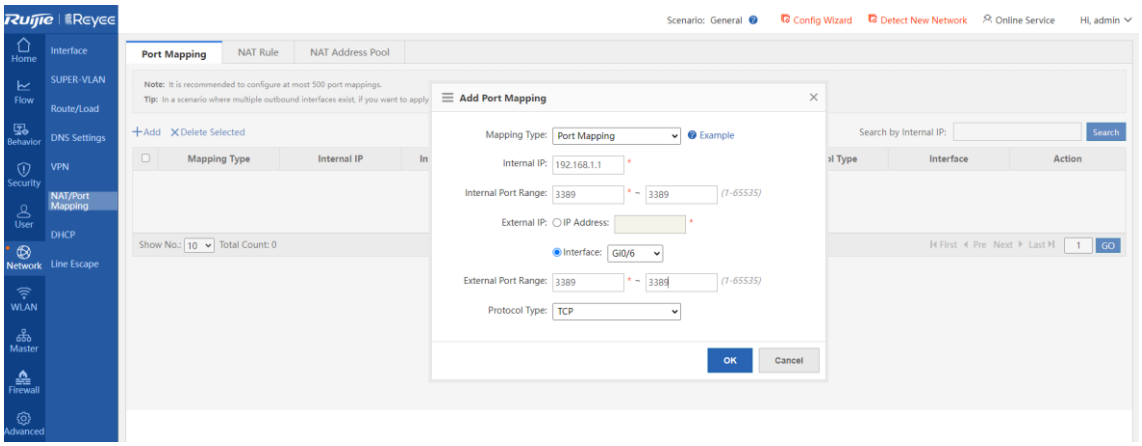
A server is deployed on the LAN and HTTP, FTP or other services are enabled. The server address is a private address. WAN users cannot access this address directly or services provided by the server. In this case, you can enable the port mapping function to allow WAN users to access the LAN server.

For example, the server address is 192.168.1.20 and HTTP is enabled. The server address is a private address, so WAN users cannot directly access the HTTP service provided by the server. You can map the server address and server ports to a public network address on the router so that WAN users can access the HTTP service provided by the server.

Procedure

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

Choose **Network** > **NAT/Port Mapping** > **Port Mapping** and add a port mapping entry.



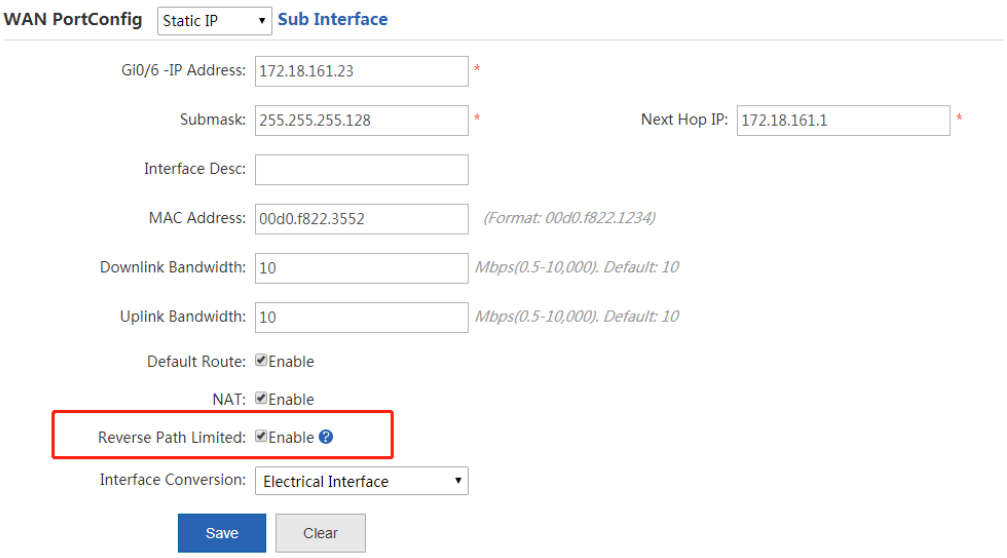
- **Mapping Type**: Select **Port Mapping** from the **Mapping Type** drop-down list box, indicating that a port of the LAN server needs to be mapped.
- **Internal IP**: indicates the IP address of the server.
- **Internal Port Range**: indicates the port for the server to provide external services.
- **External IP**: indicates the IP address of a WAN port (**IP Address** is selected when the IP address of a WAN port is dynamic).
- **External Port Range**: indicates the target WAN service port for port mapping.
- **Protocol Type**: indicates the protocol used by the server to provide services.

(2) Command generated on the CLI:

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

(3) In multi-egress network environments, you are advised to enable the RPL function on the WAN interface.

Select **Reverse Path Limited**.



(4) 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
```

Verification

(1) Click **Start** and choose **Remote Desktop Connection**. The **Remote Desktop Connection** dialog box is displayed. Enter the IP address of the WAN port.

(5) Click **Connect**. The server login page is displayed.

3.7 DMZ Host Mapping

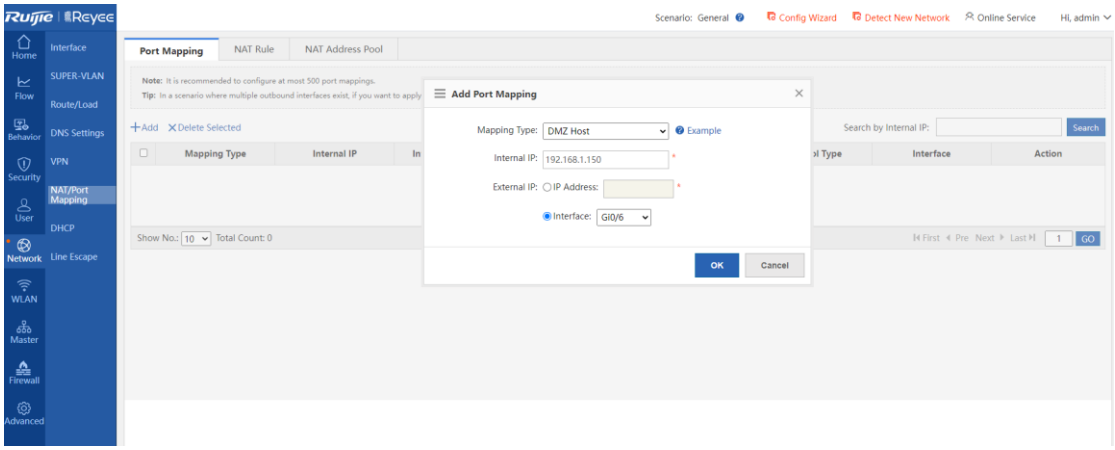
Application Scenario

A server is configured on the LAN and multiples services are enabled. 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.

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 router, so WAN users can access the server.

Procedure

(1) Choose **Network** > **NAT/Port Mapping** > **Port Mapping**, add an entry, and select **DMZ Host**.



- **Mapping Type**: Select **DMZ Host** from the **Mapping Type** drop-down list box, indicating that all ports of the LAN server need to be mapped.
- **Internal IP**: indicates the IP address of the server.
- **External IP**: indicates the IP address of a WAN port (**IP Address** is selected when the IP address of a WAN port is dynamic).

(2) Command generated on the CLI:

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

Verification

(1) Click **Start** and choose **Remote Desktop Connection**. The **Remote Desktop Connection** dialog box is displayed. Enter the IP address of the WAN port.

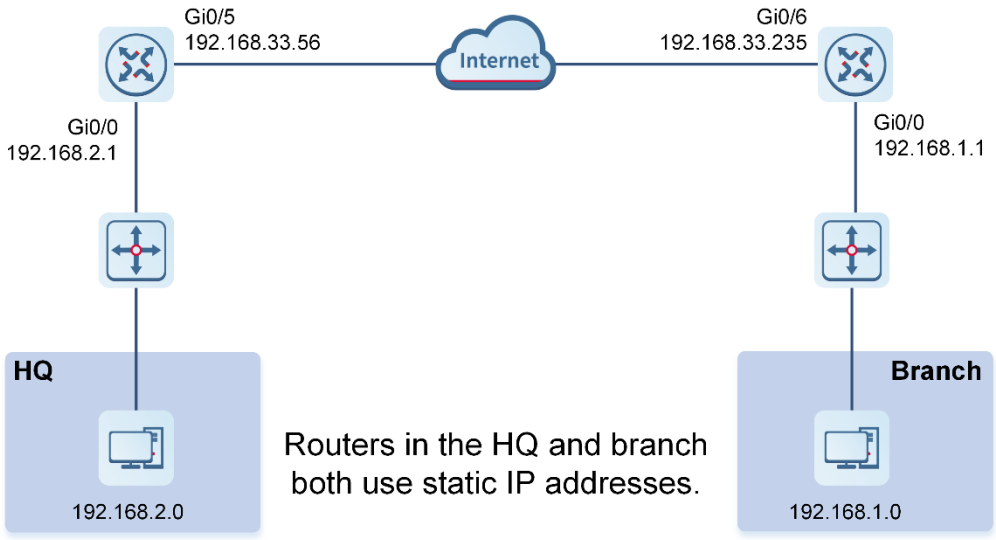
(3) Click **Connect**. The server login page is displayed.

3.8 IPsec VPN

3.8.1 A Branch Router Accesses the HQ Router Using a Static IP Address in Dialup Mode

Application Scenario

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



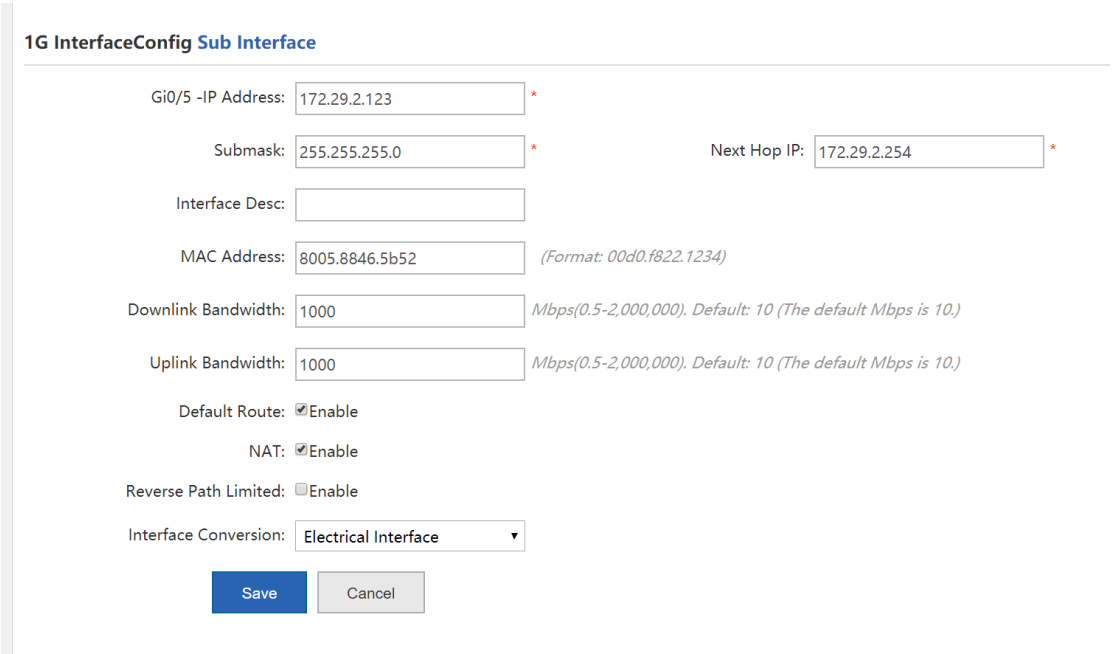
Prerequisites

- Configure router A in the HQ as the IPsec server.
- Configure router B in the branch as the IPsec client.
- Keep consistent parameter settings at both ends:
  - Authentication mode: pre-shared key, with the key set to **ruijie**
  - IKE algorithm: 3DES-MD5, DH2
  - IPsec negotiation scheme: ESP (3DES-MD5)

Procedure

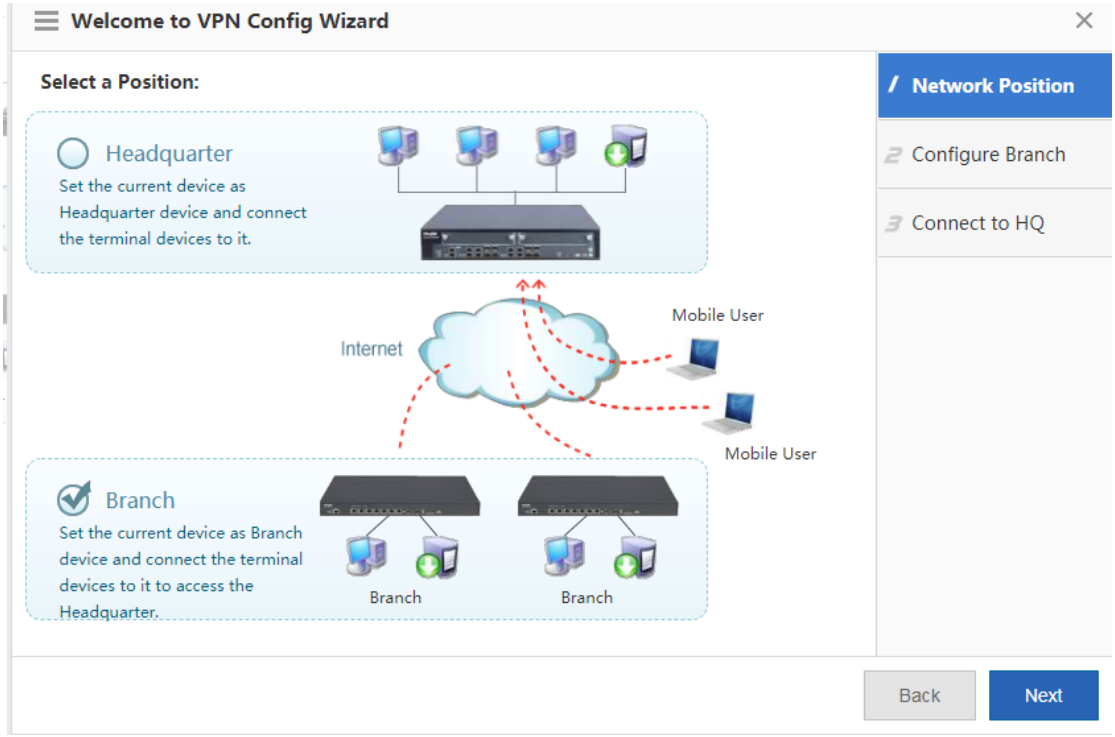
(1) Configure router B in the branch.

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.

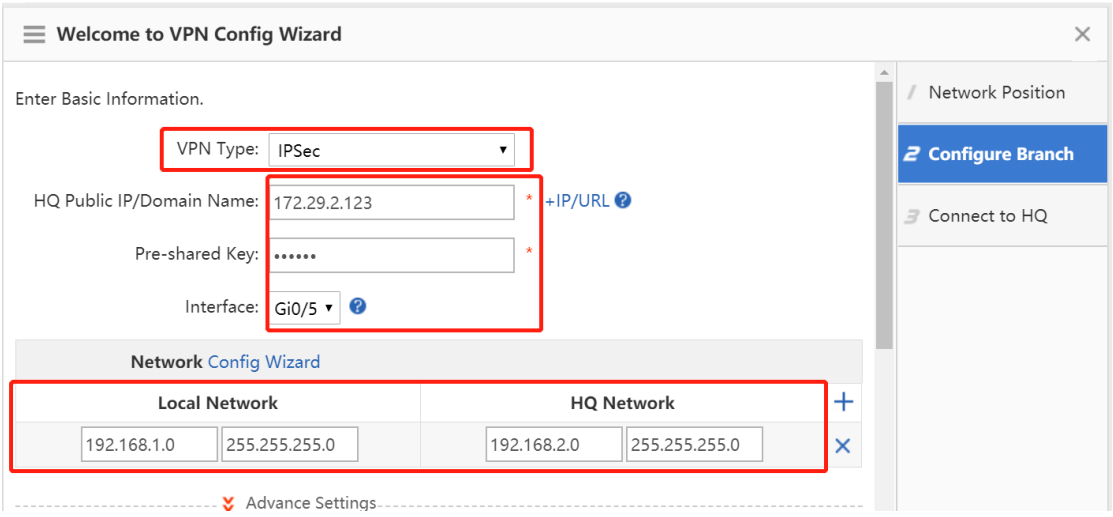


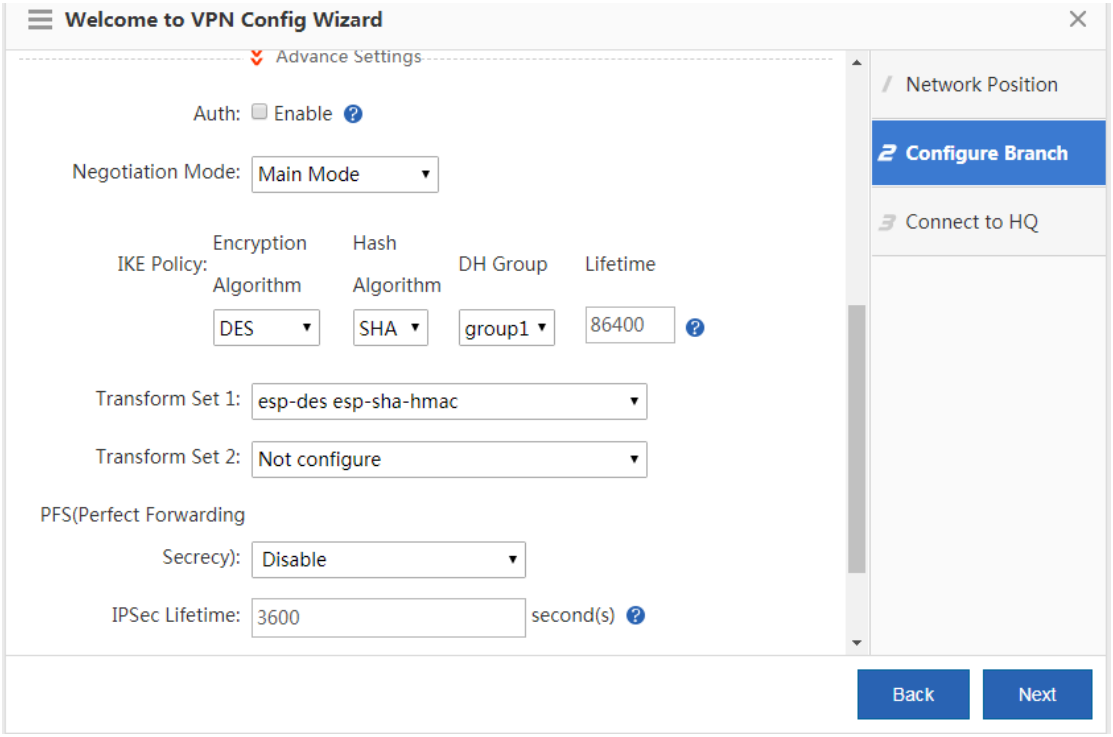
(2) Configure IPsec for router B in the branch.

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



Configure basic branch information.





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 dialler interface can be configured on the web page:

IKE algorithm: 3DES-MD5 and DH2

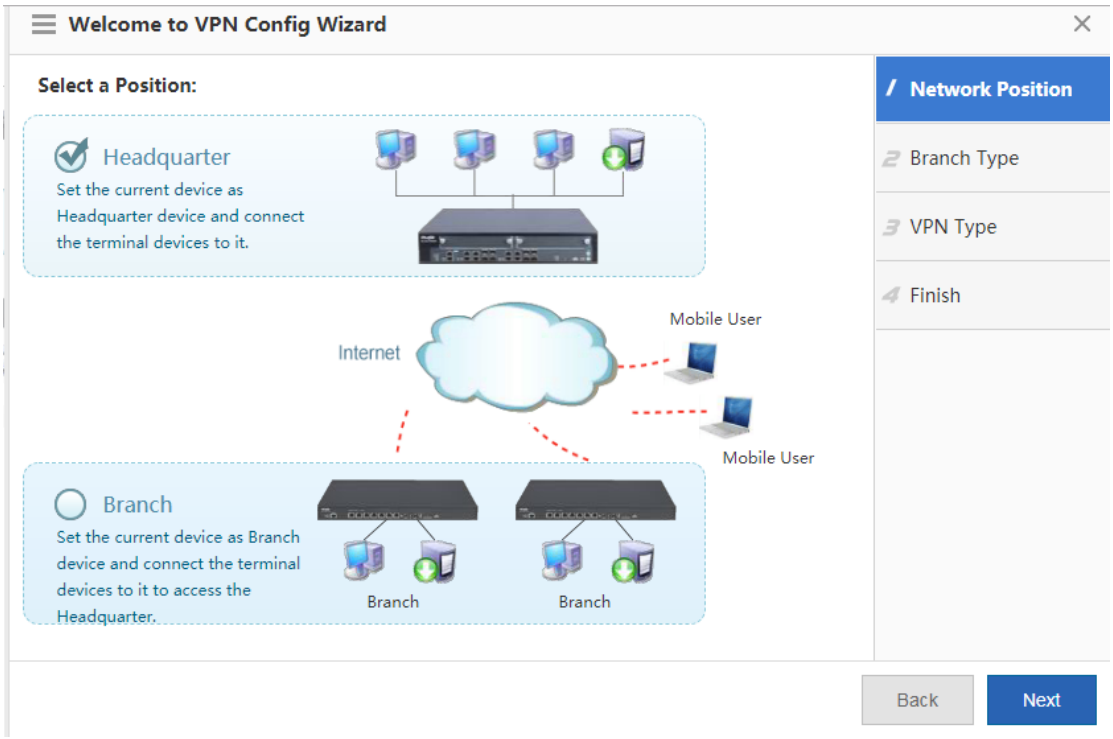
IPsec negotiation scheme: ESP (3DES-MD5)

(3) Configure router A in the HQ.

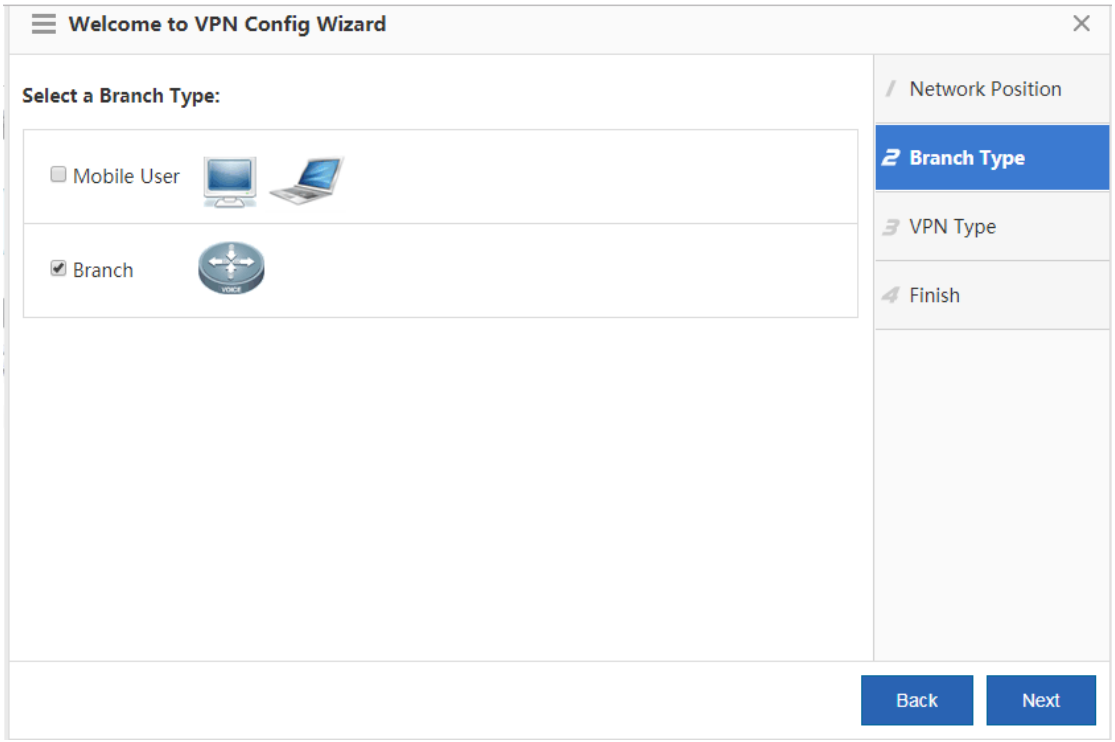
a Complete wizard-based setup to implement Internet access of the HQ router.

b Configure IPsec for router A in the HQ.

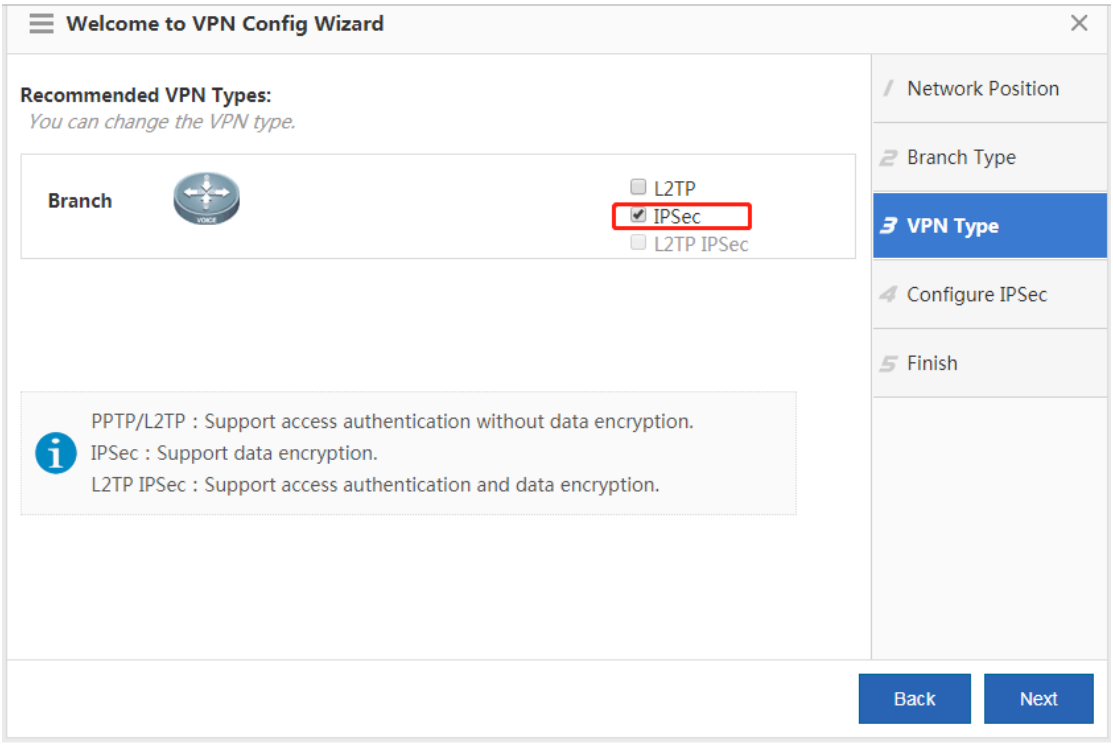
Choose **Network** > **VPN** and click **Configure**. Select **Headquarter** and click **Next**.



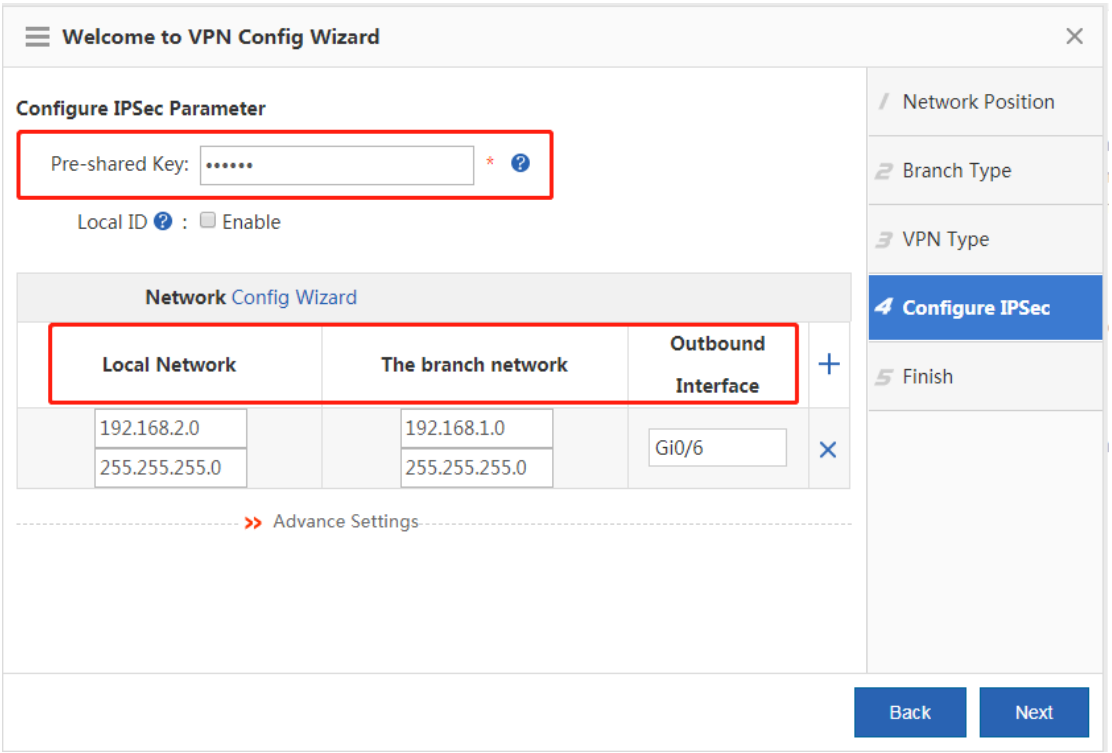
Select **Branch** and click **Next**.

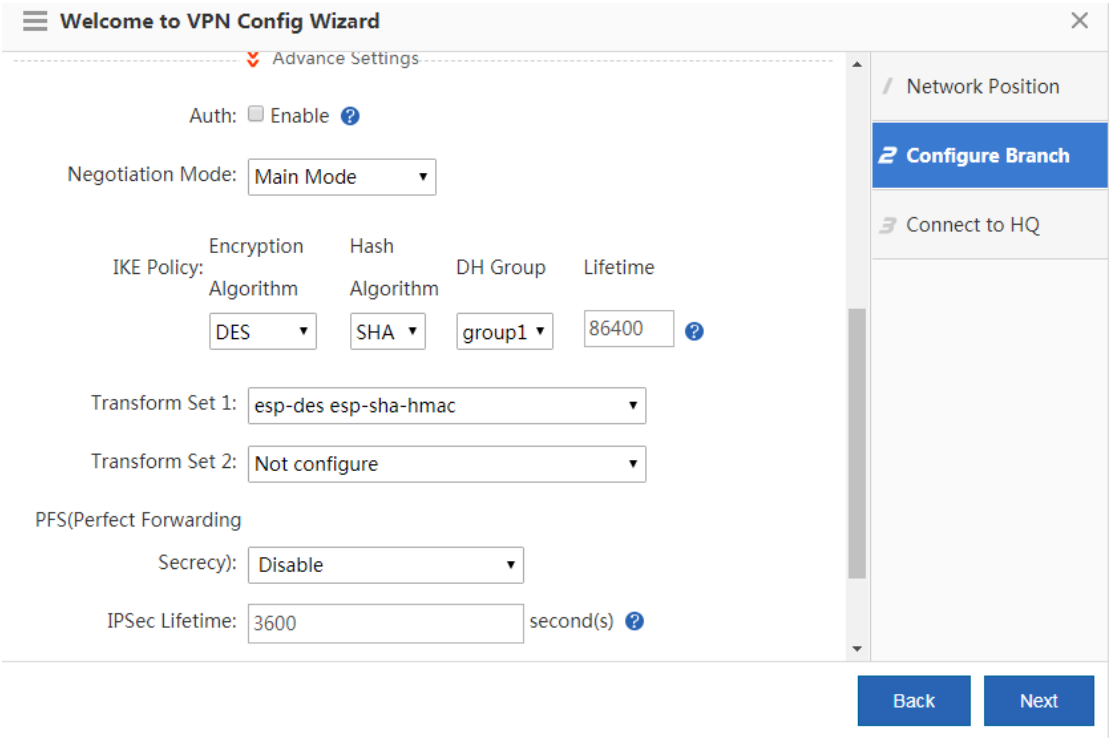


Select IPsec and click **Next**.

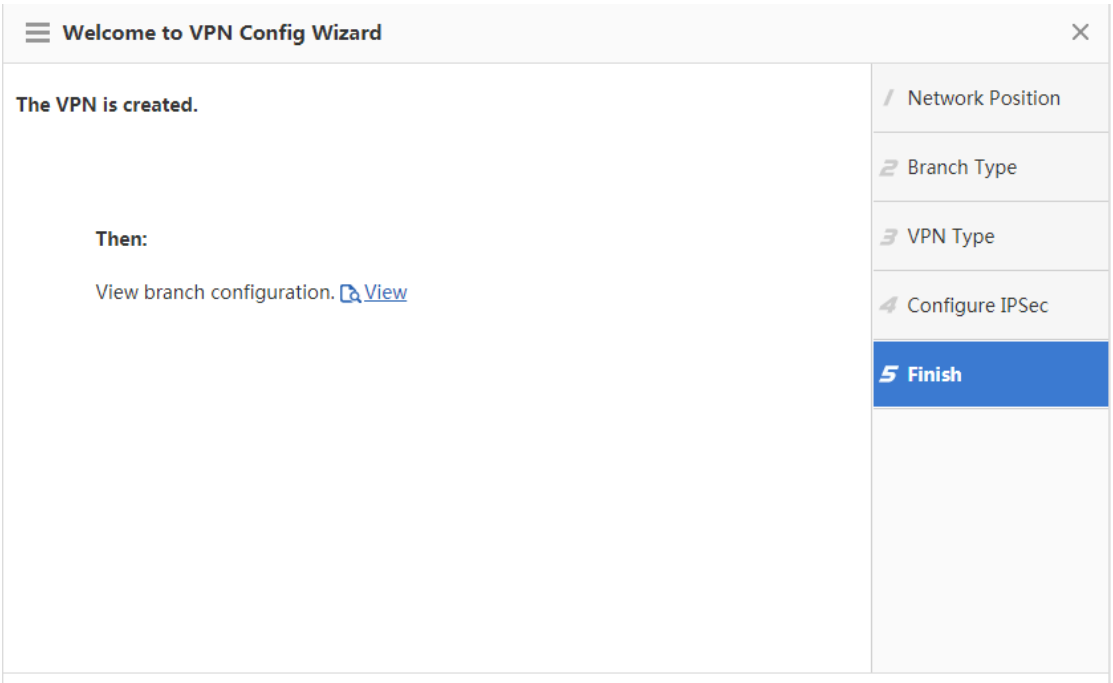


Configure IPsec VPN and click **Next**.





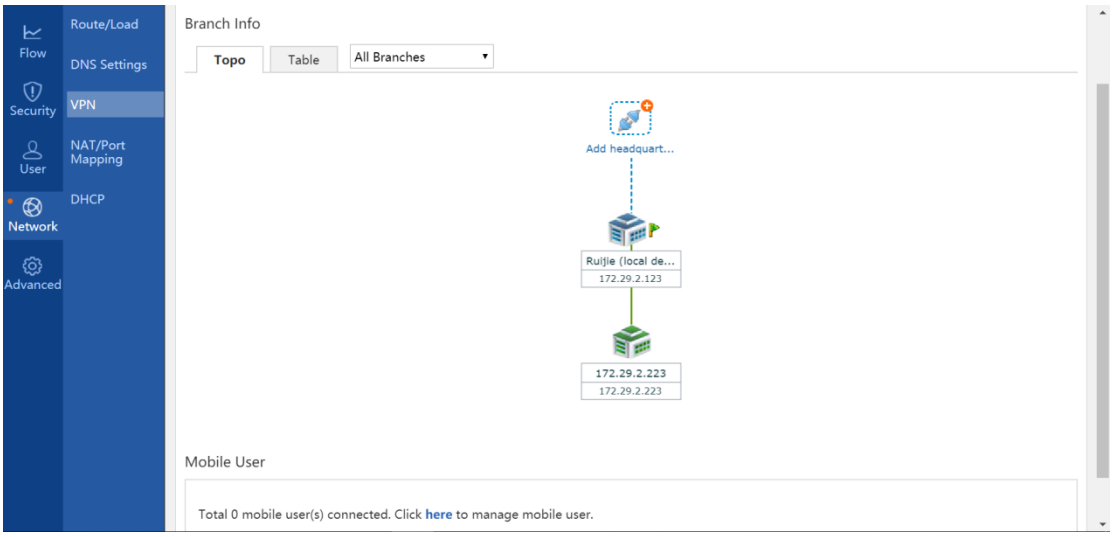
The IPsec VPN configuration is complete.



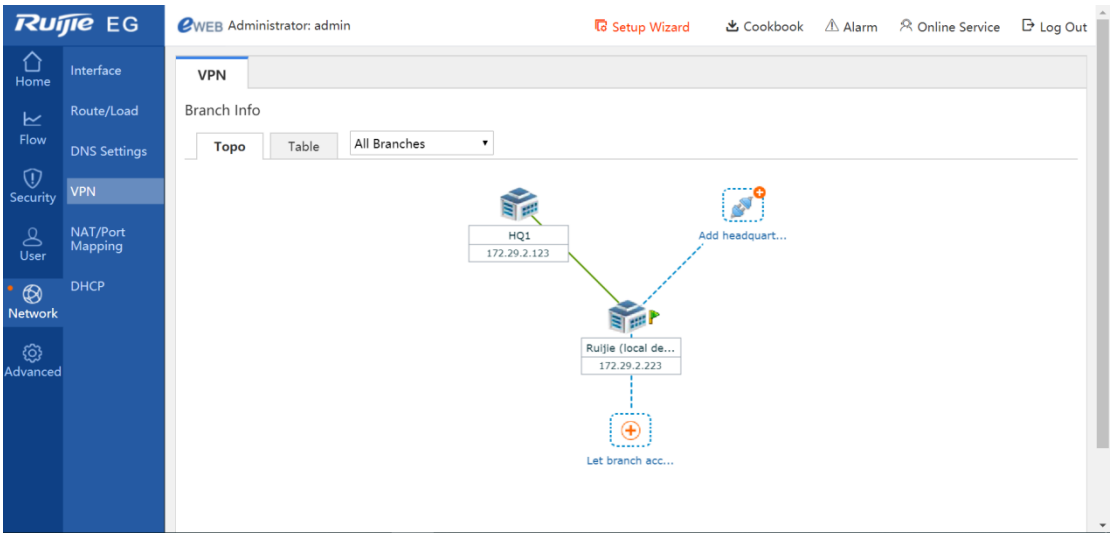
Verification

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 routers in the HQ and branch can access each other.

Note

- When the Internet access service is configured through wizard-based setup on the web of the router, IPsec VPN can be configured only after the next-hop address is configured on the interface configuration page in wizard-based setup. If no next-hop address is configured for an interface, the interface cannot be selected during VPN configuration.
- After VPN is configured, the router automatically delivers AAA configuration (the system asks you to enter the user name and password during device login, and the telnet password needs to be reconfigured).
- After deleting the VPN configuration, close the browser to make the deletion take effect. Otherwise, the system retains the previous VPN configuration.
- When a WAN port receives an IPsec request but no traffic 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. However,

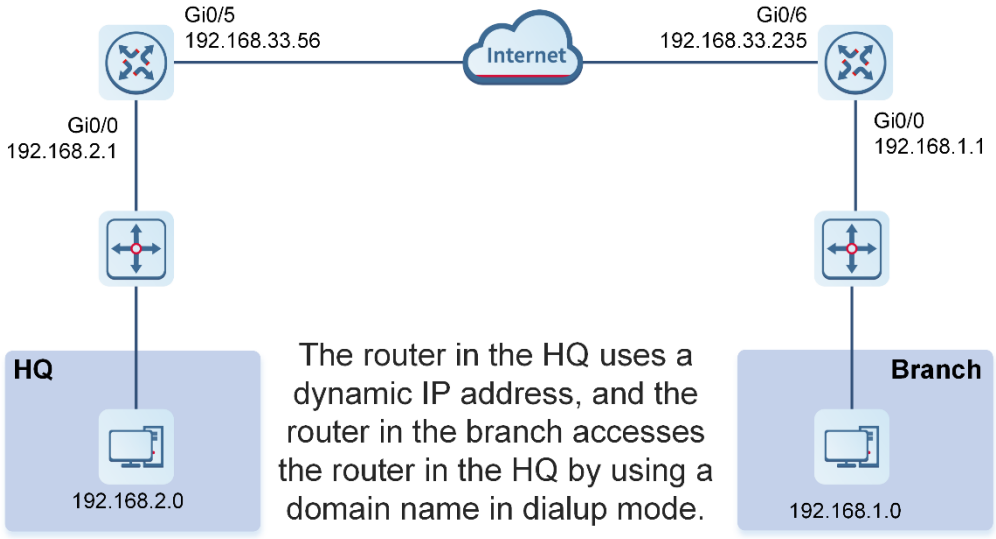
this is beneficial to network management. An ACL can be configured to filter out requests from undesired IPsec-compliant device that is connected to the router.

- 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.

3.8.2 The Branch Router Accesses the HQ Router Using a Dynamic IP Address in Dialup Mode

Application Scenario

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



Prerequisites

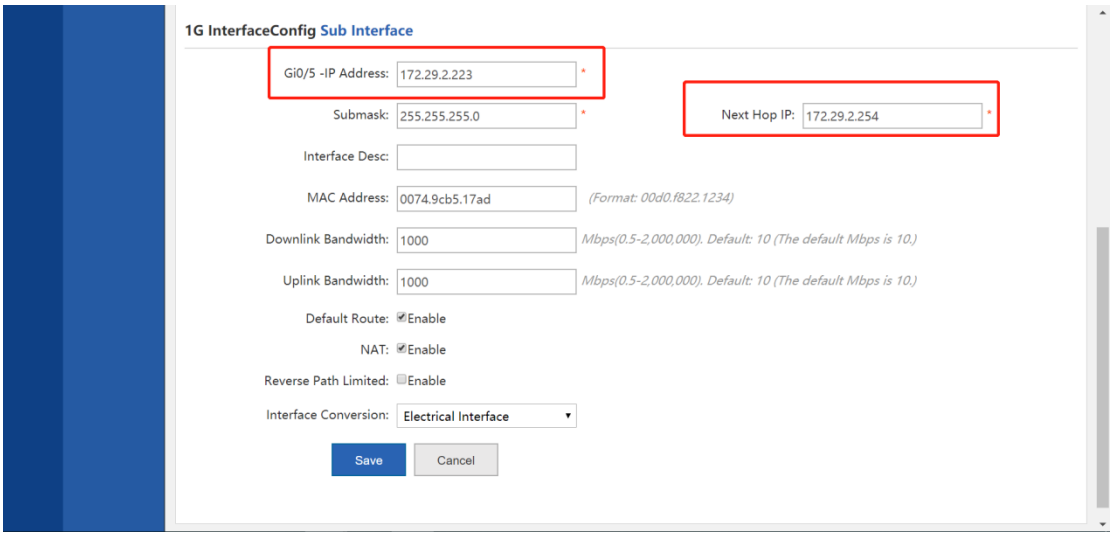
1. Configure router A in the HQ as the IPsec server.
2. Configure router B in the branch as the IPsec client.
3. Keep consistent parameter settings at both ends:
   - Authentication mode: pre-shared key, with the key set to **ruijie**
   - IKE algorithm: 3DES-MD5 and DH2
   - IPsec negotiation scheme: ESP (3DES-MD5)

Procedure

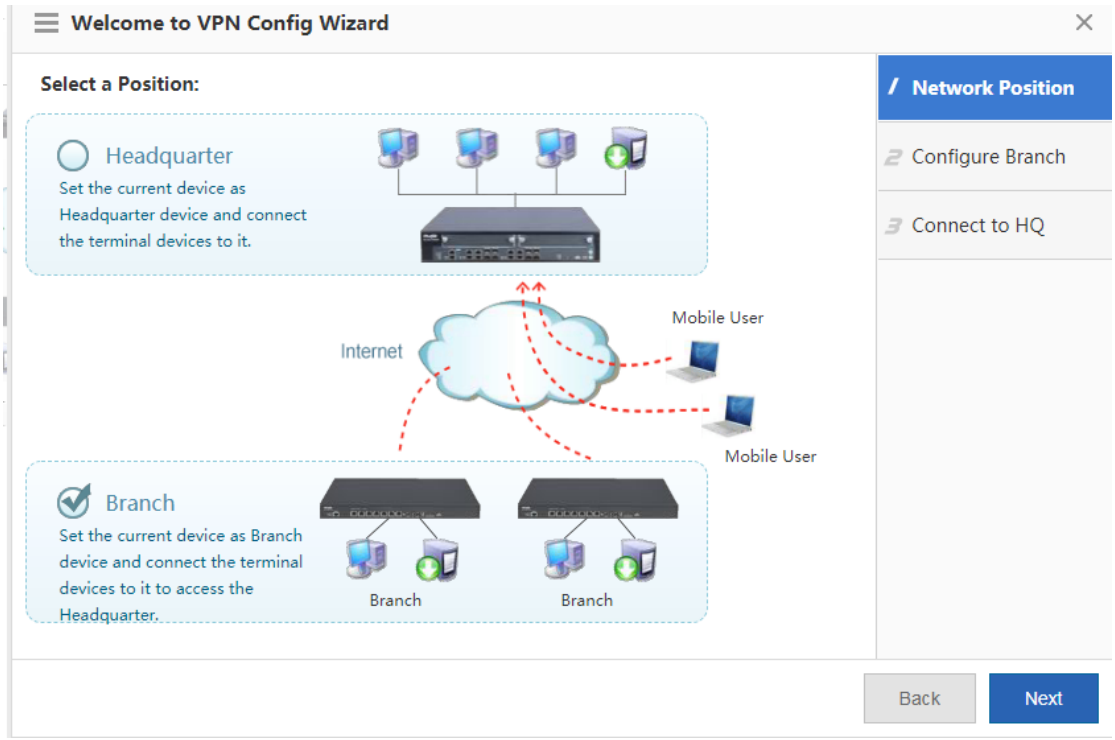
(1) Configure router B in the branch.

The web page does not support dynamic domain names. Therefore, complete configuration on the web page and modify the configuration on the CLI.

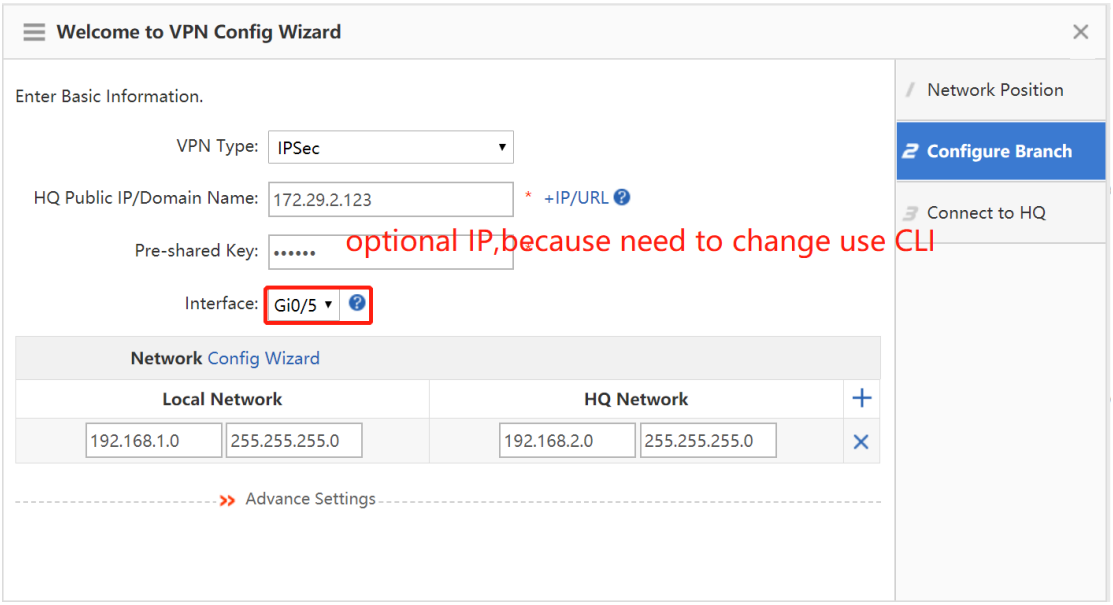
a Complete wizard-based setup to meet Internet access requirements of users in the HQ and branch. If the users can access the Internet, check whether the next-hop address is configured for the WAN interface.

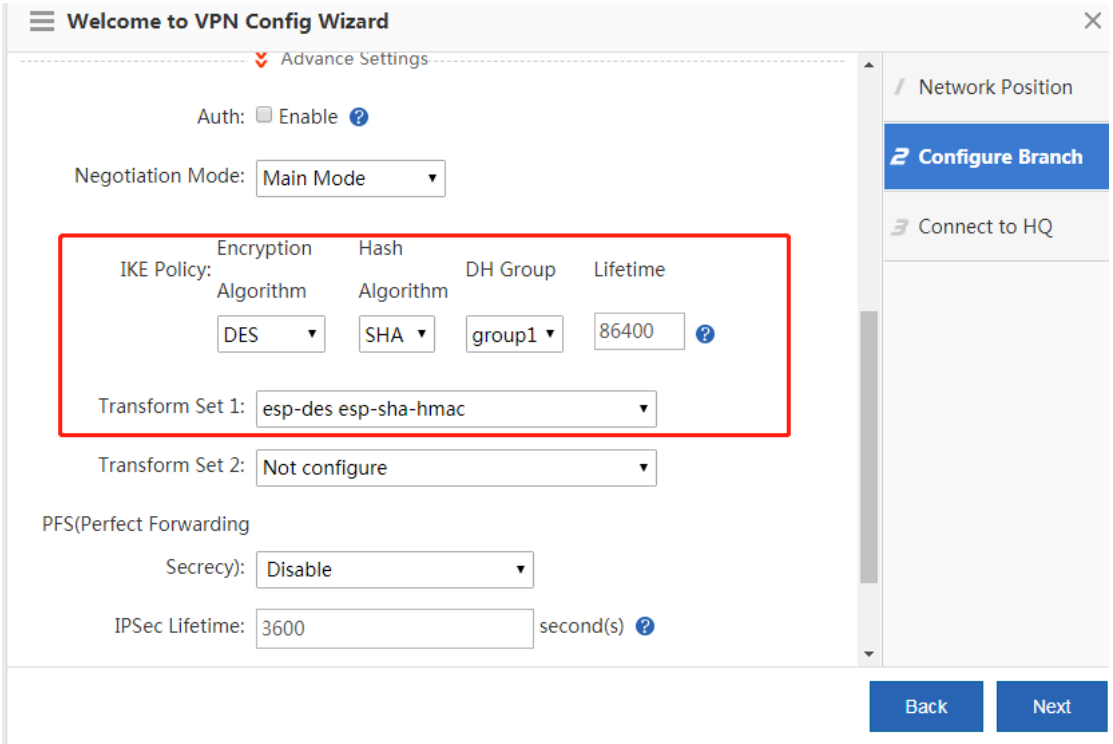


b Choose **Network** > **VPN** and click **Configure**. Select **Branch** and click **Next**.

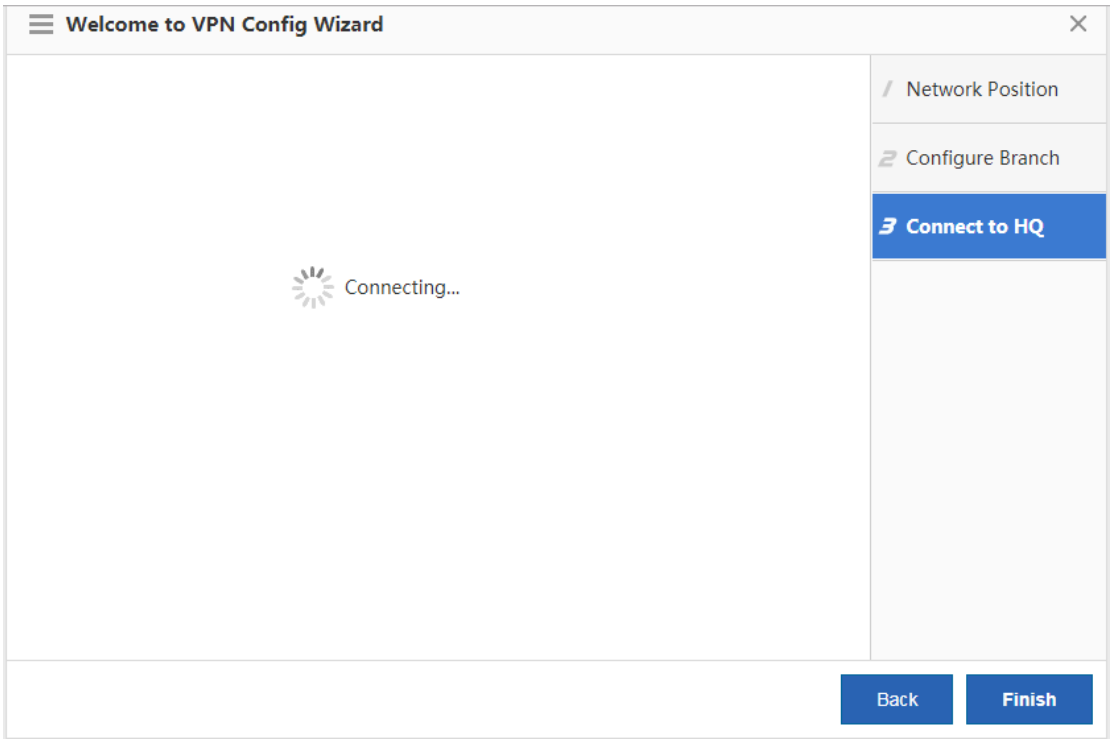


c Configure basic IPsec information and click **Next**.





d Click **Finish**.

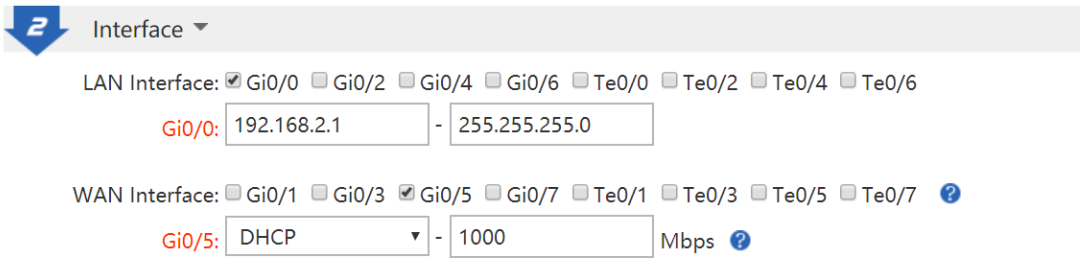


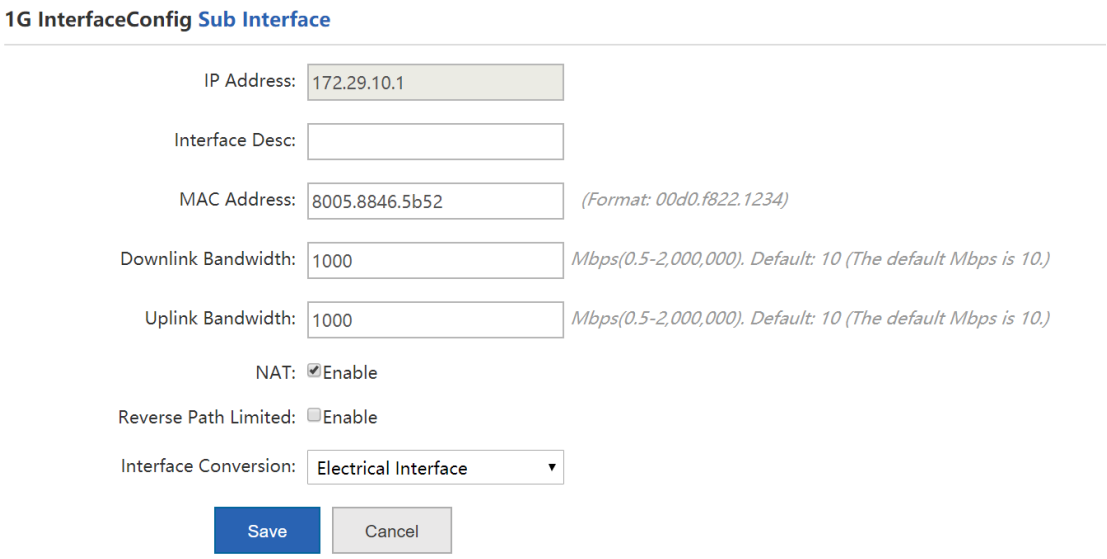
On the CLI, change the public IP address of the HQ router to a dynamic domain name.

```
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
```

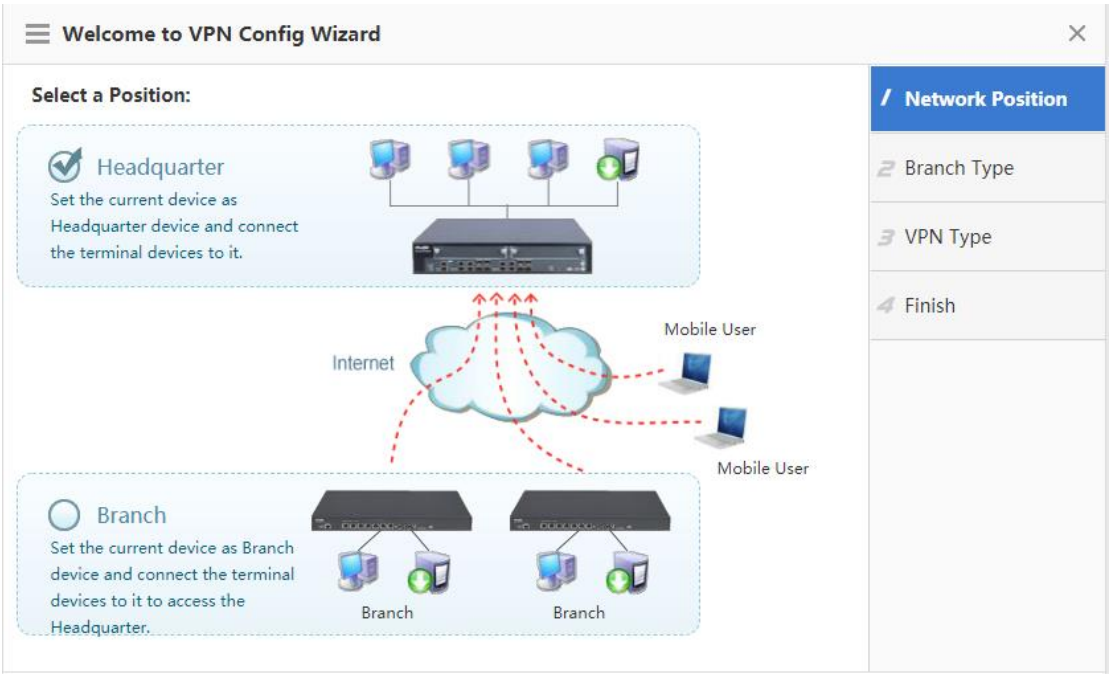
(2) Configure router A in the HQ.

a 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.

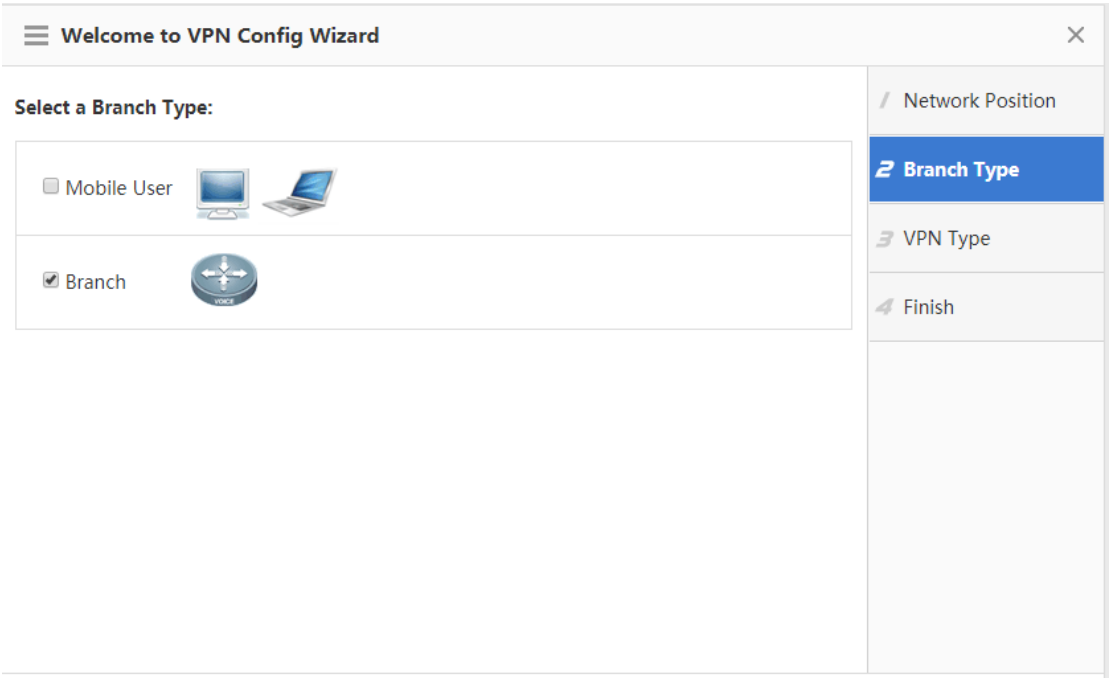




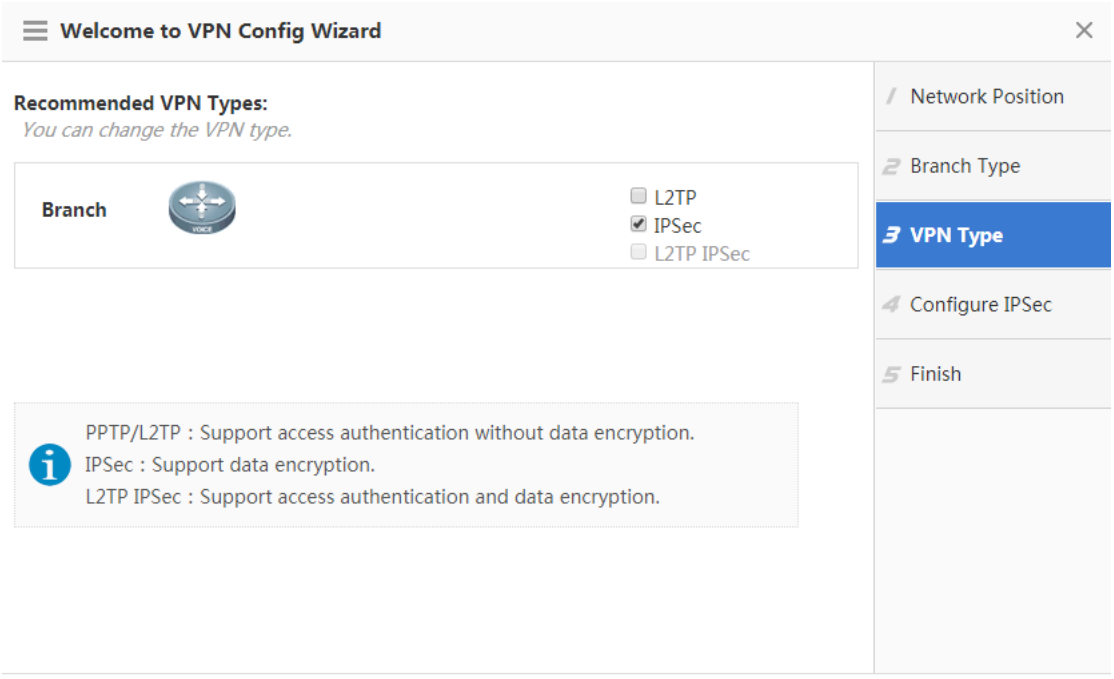
b Choose **Network** > **VPN** and click **Configure**. Select **Headquarter** and click **Next**.



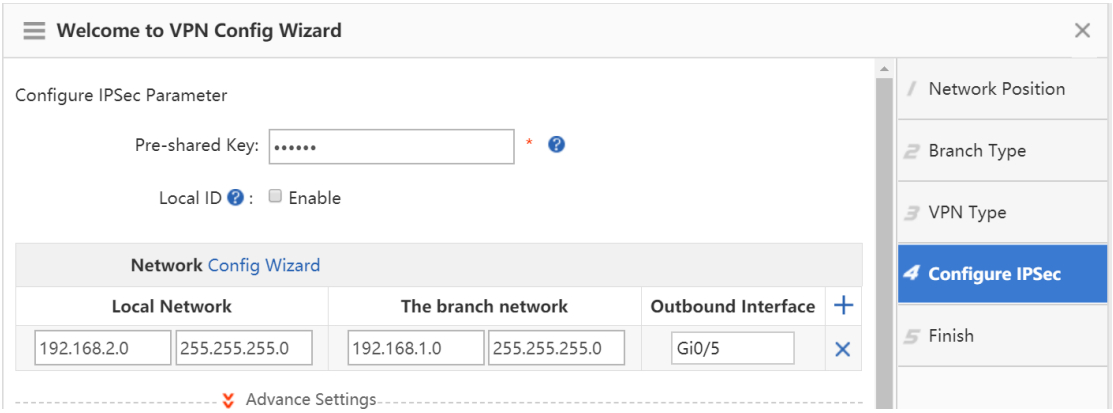
c Select **Branch** and click **Next**.

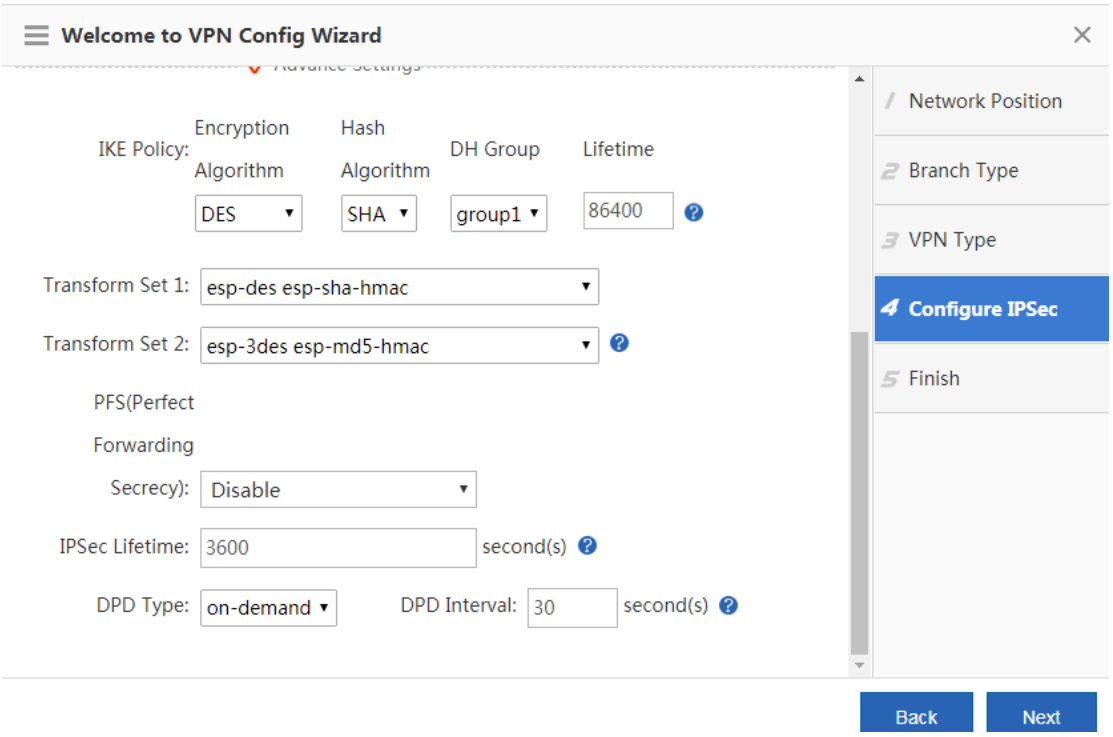


d Select IPsec and click **Next**.

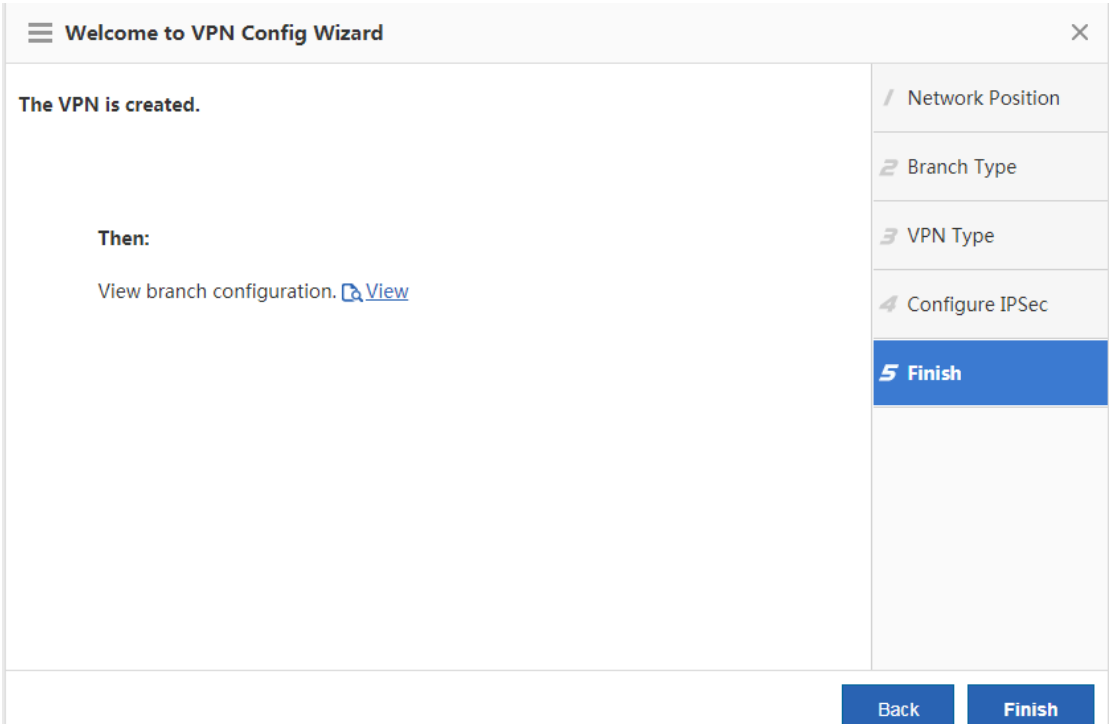


e Configure IPsec basic information and click **Next**.





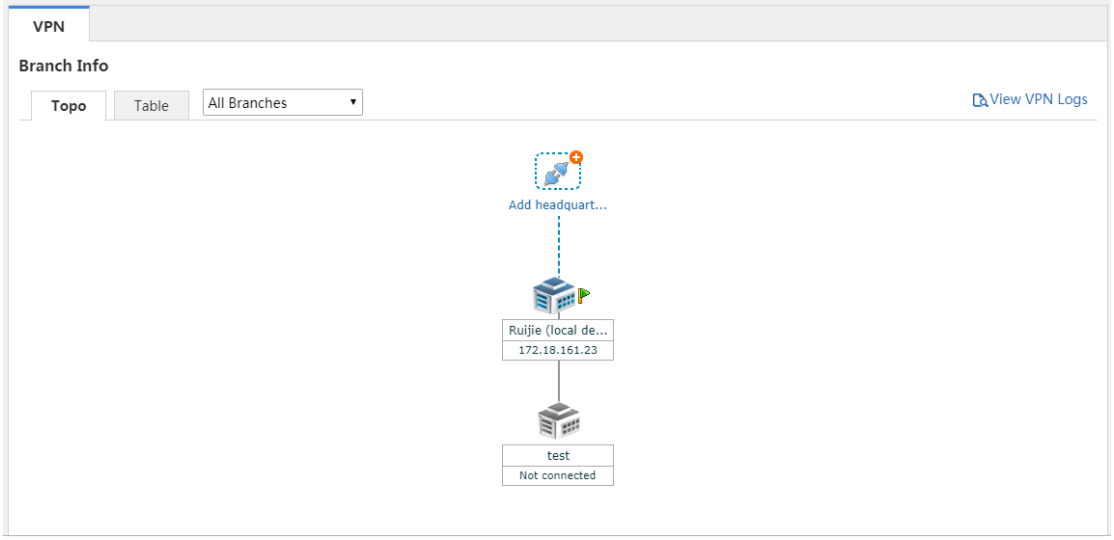
f Click **Finish**.



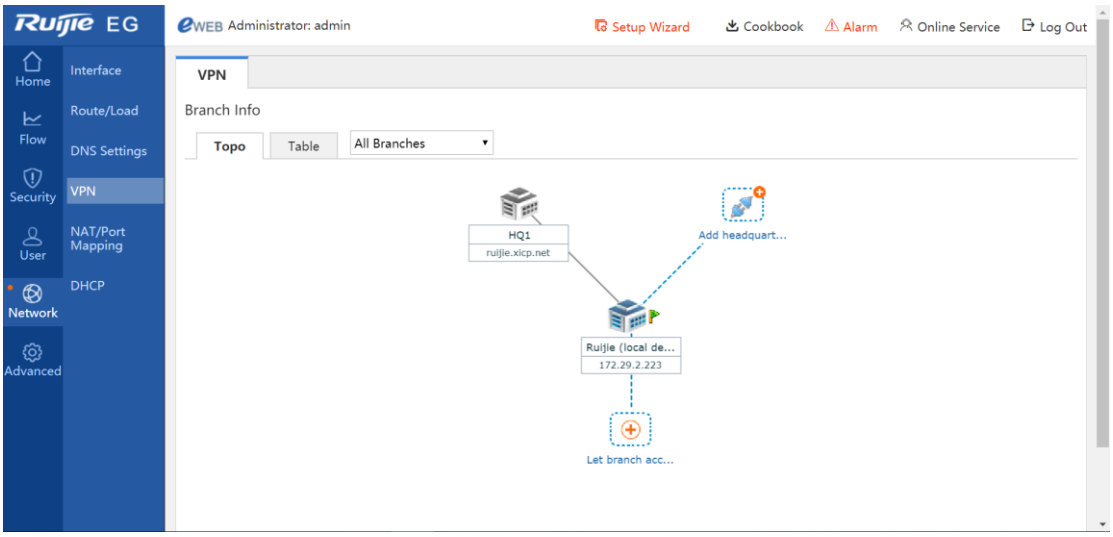
Verification

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.

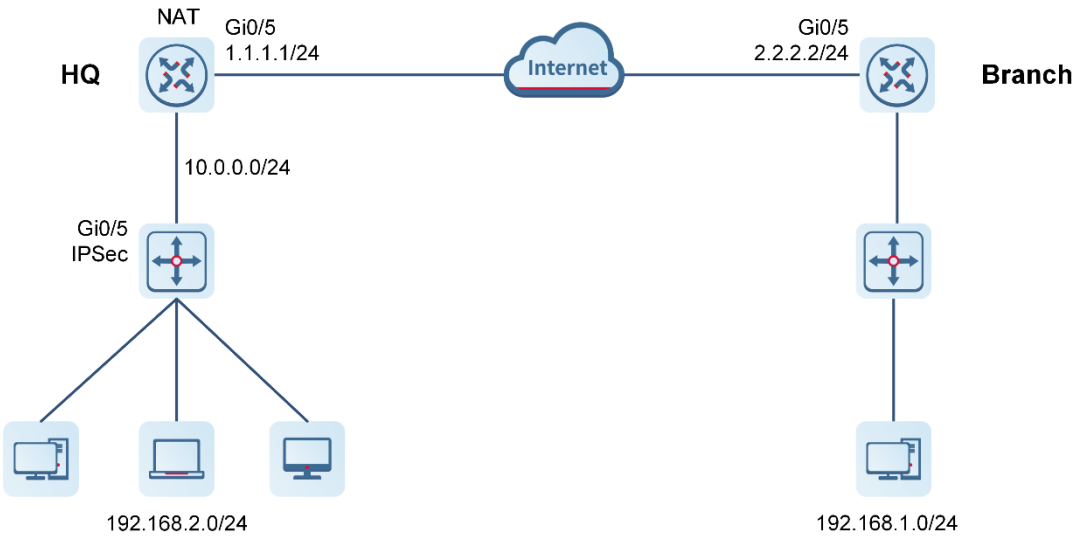
Note

- 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.
- When a WAN port receives an IPsec request but no traffic 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. Instead, this is beneficial to network management. An ACL can be configured to filter out requests from the undesired IPsec-compliant device that is connected to the router.
- 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.

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

Application Scenario

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.



Prerequisite

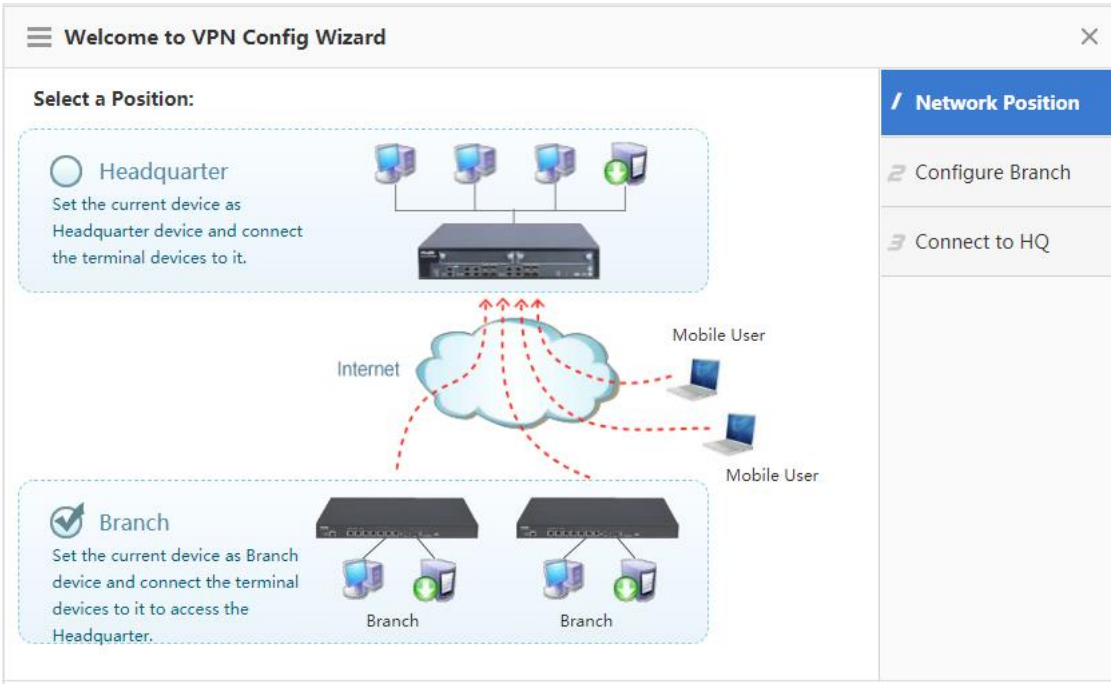
- Configure router A in the HQ as the IPsec server.
- Configure router B in the branch as the IPsec client.
- Keep consistent parameter settings at both ends:
  - Authentication mode: pre-shared key, with the key set to **ruijie**
  - IKE algorithm: 3DES-MD5 and DH2
  - IPsec negotiation scheme: ESP (3DES-MD5)
- Configure NAT mapping on the outermost egress of the HQ and establish an IPsec connection on the LAN router.

Procedure

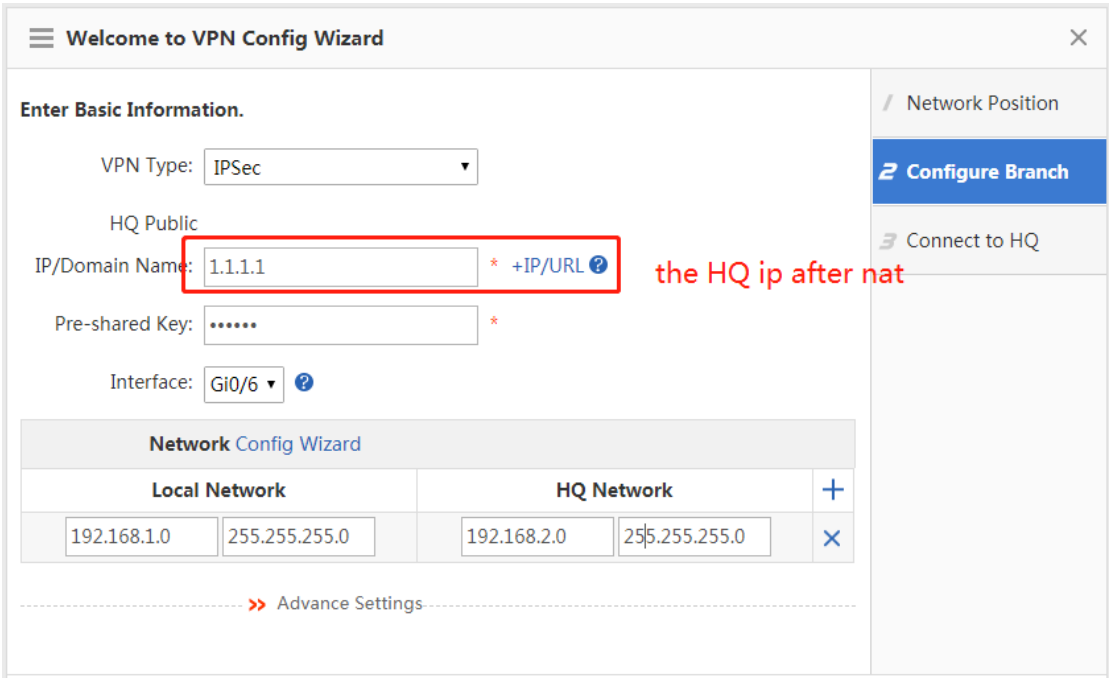
(1) Ensure that basic configuration on the device and routers in both the HQ and branch are normal, and LANs users at both ends can access the WAN.

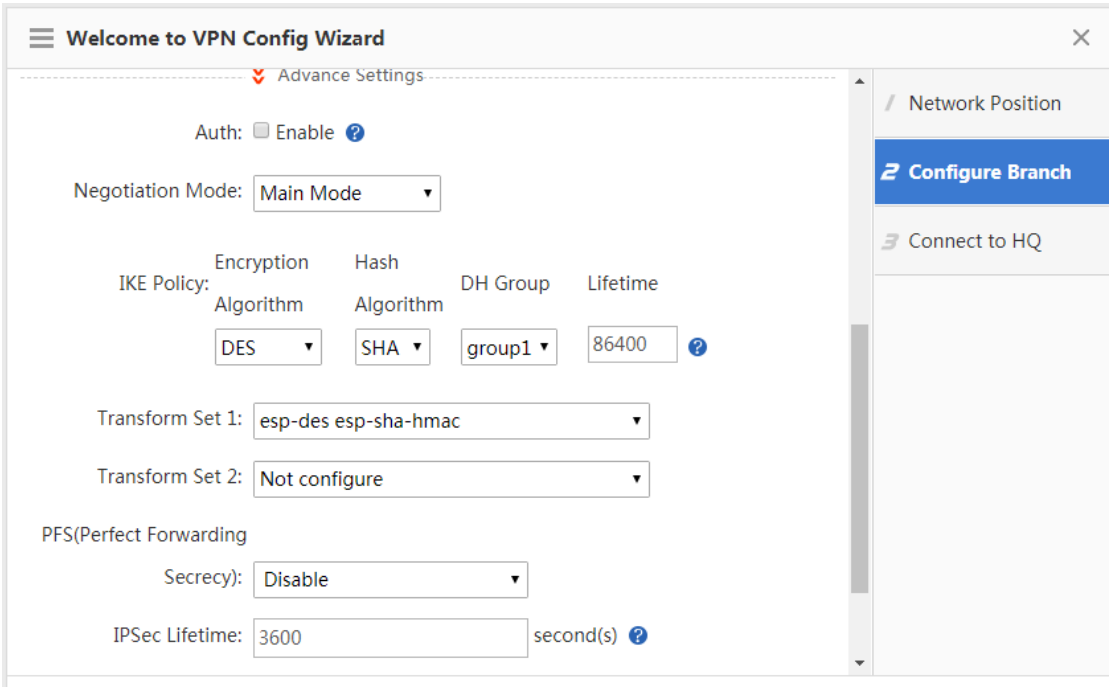
(2) Configure router B in the branch.

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

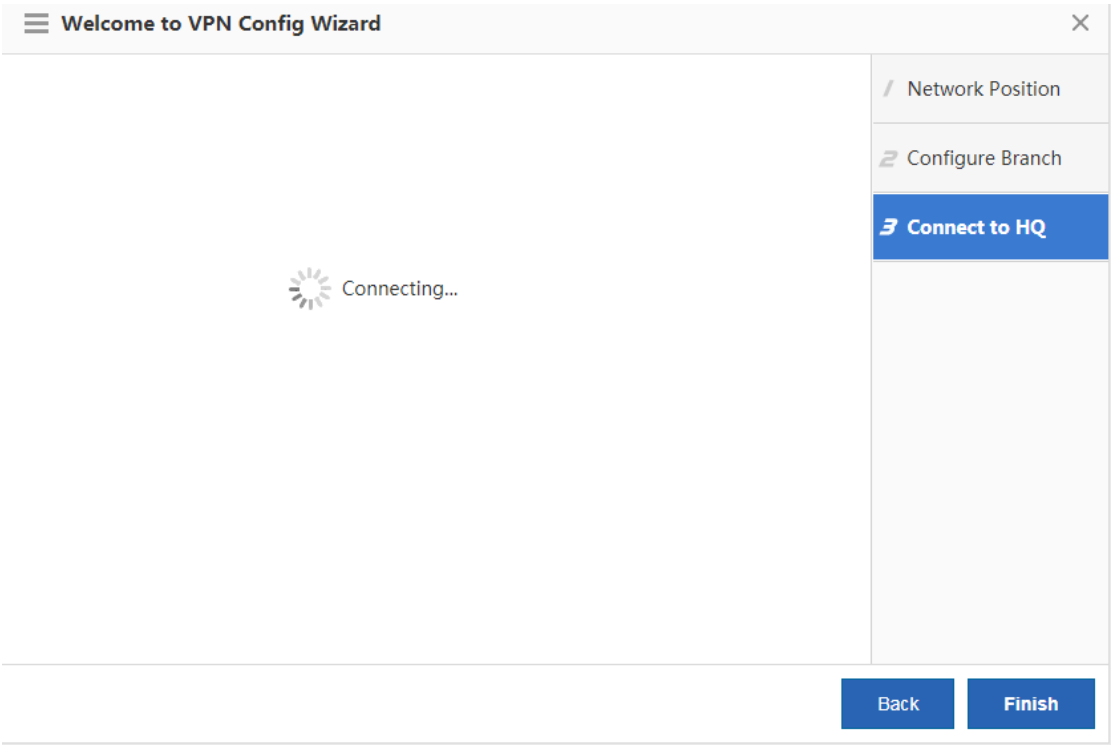


Configure an IPsec policy, set the public IP address of the HQ router to the IP address obtained after NAT, and click **Next**.





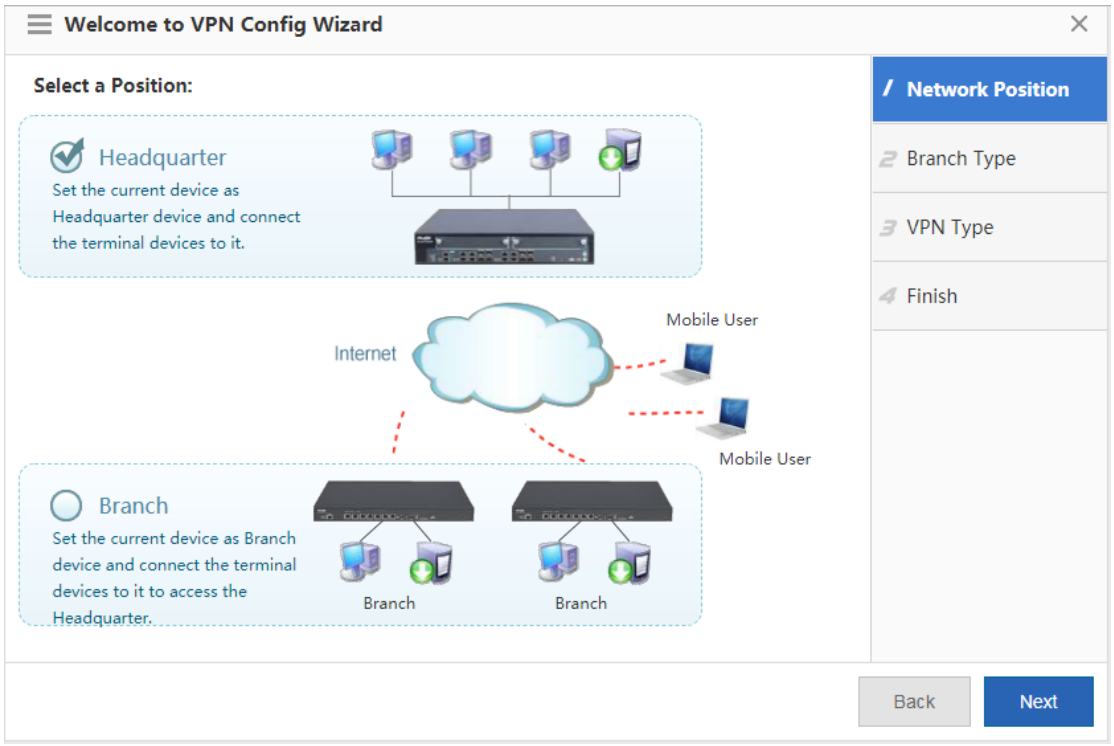
Click **Finish**.



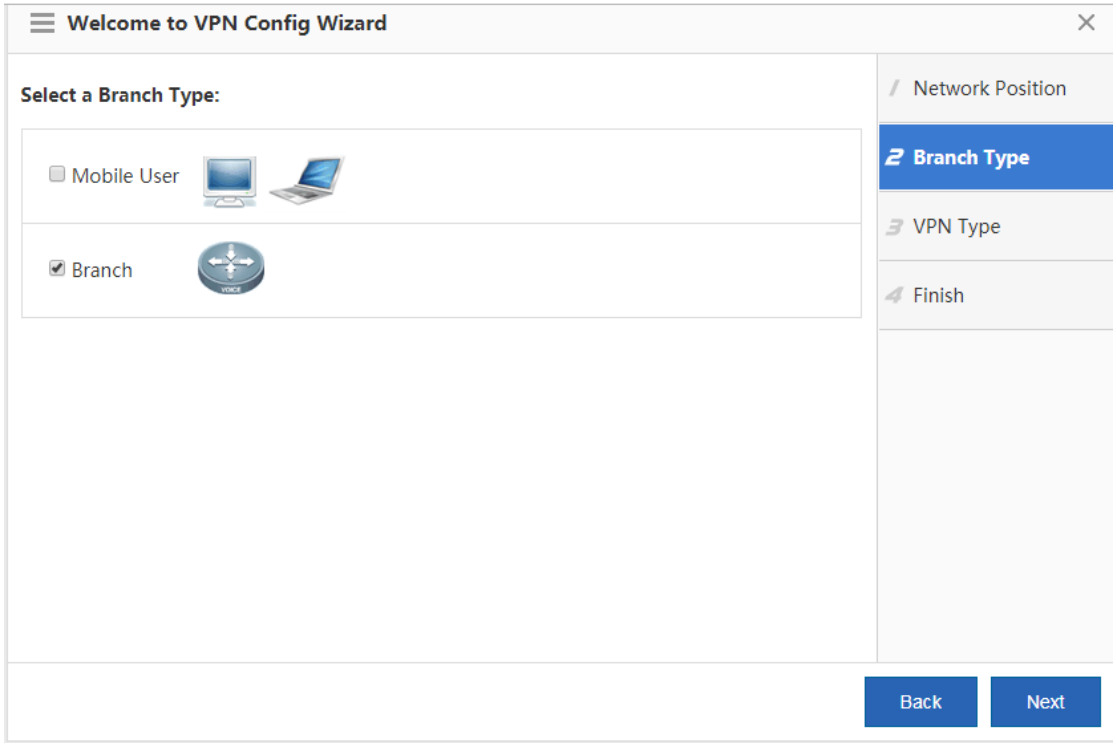
(3) Configure router A in the HQ.

Configure IPsec on the LAN router.

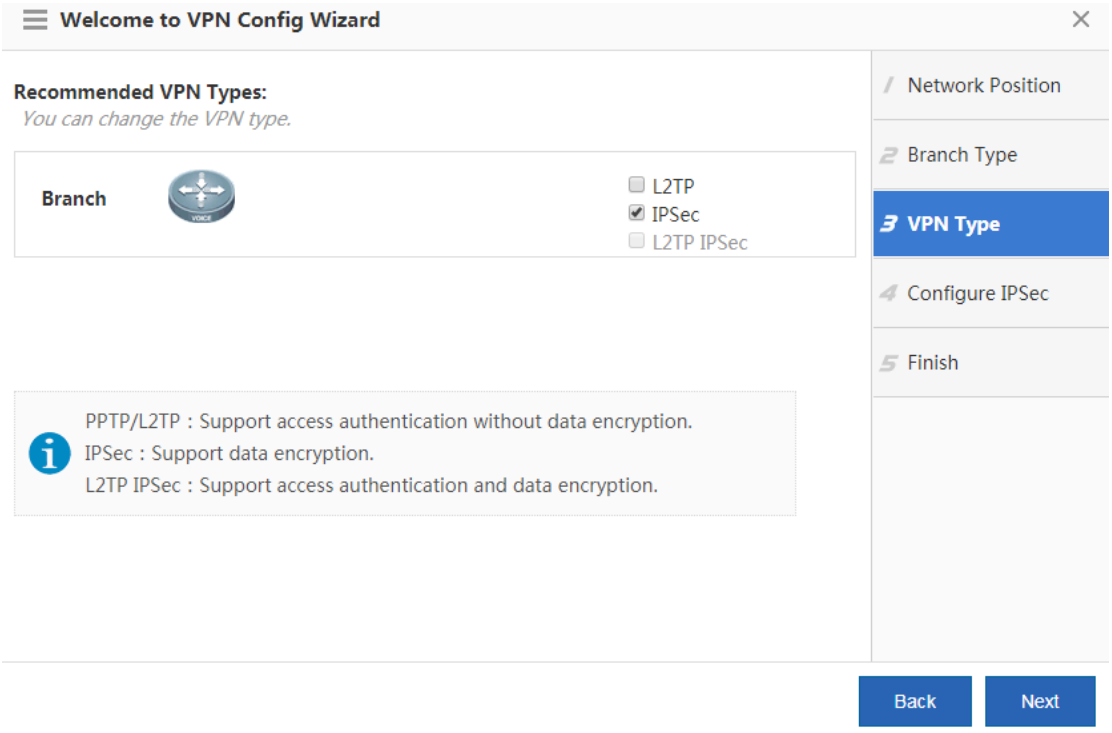
a Choose **Network** > **VPN** and click **Configure**. Select **Headquarter** and click **Next**.



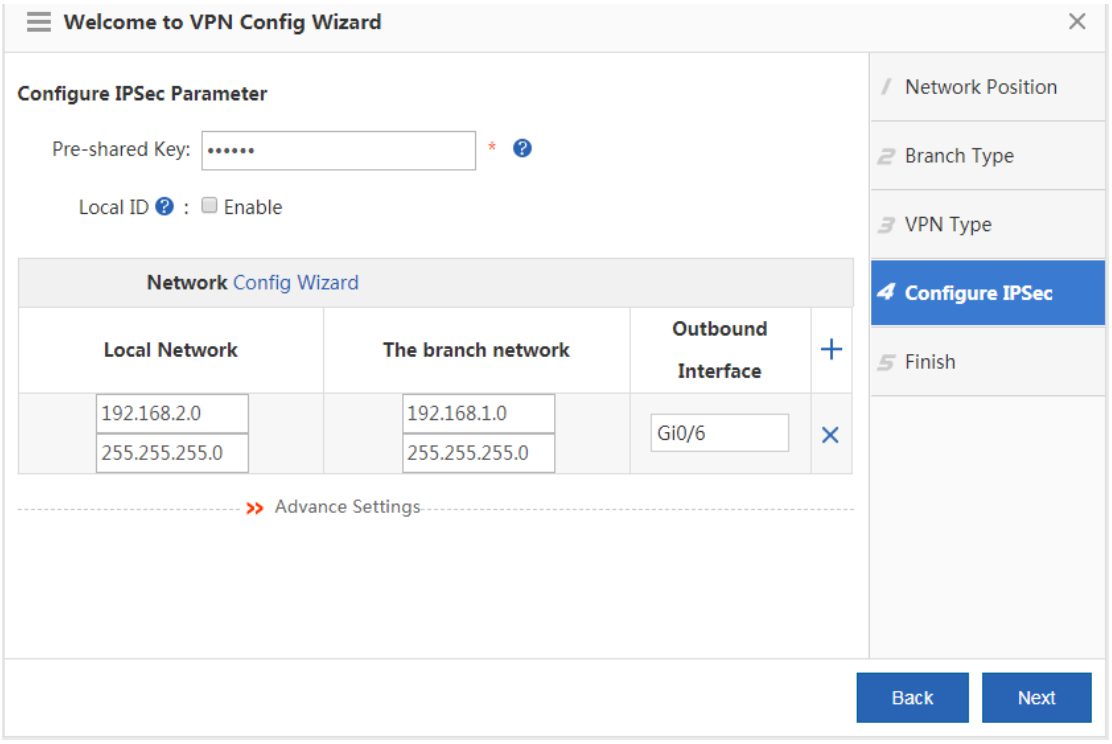
b Select **Branch** and click **Next**.

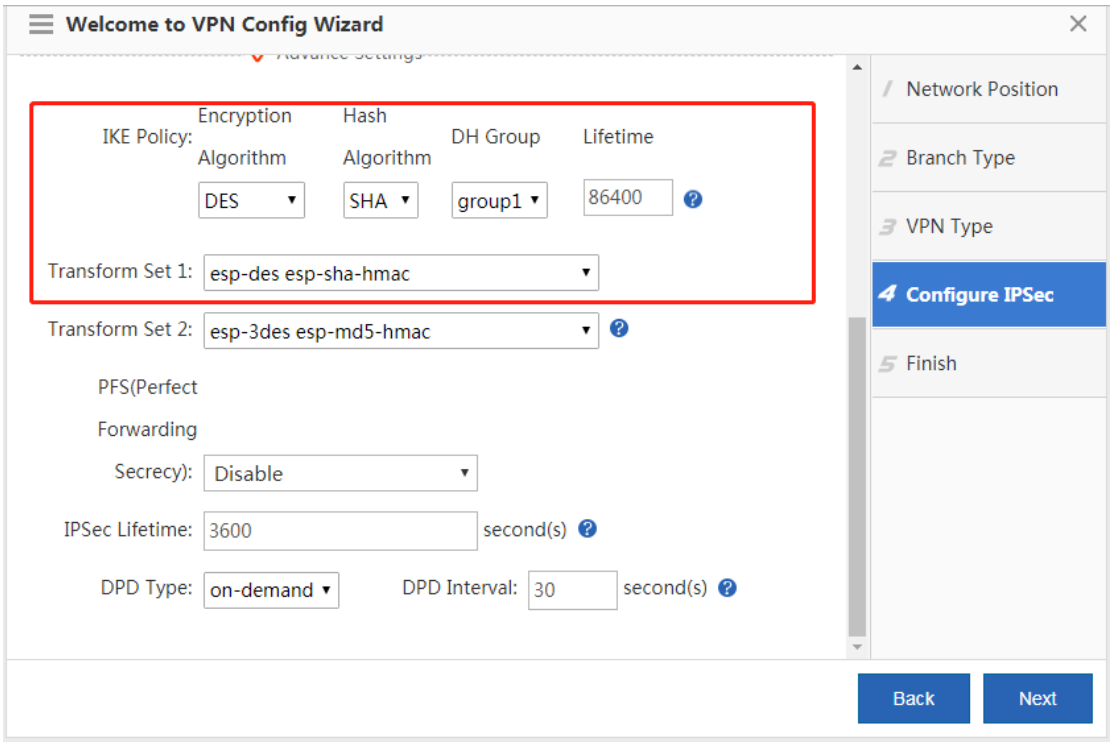


c Select IPsec and click **Next**.

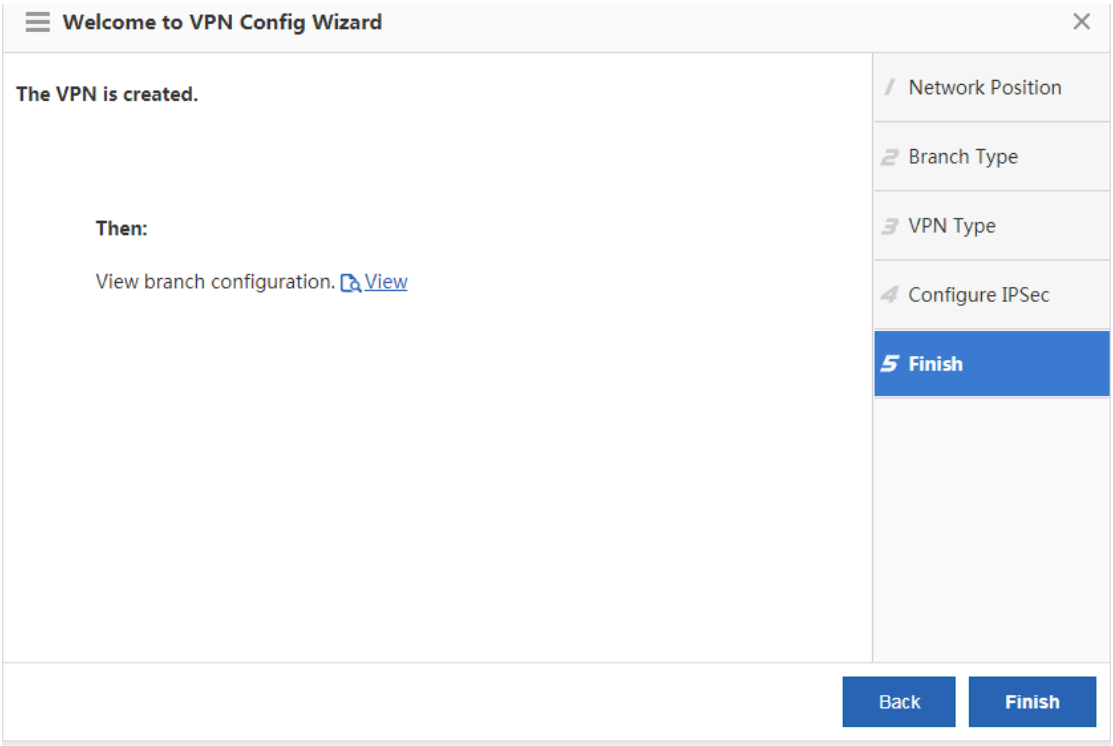


d Configure IPsec basic information and click **Next**.





e Click **Finish**.



(4) IPsec uses UDP ports 500 and 4500. Map UDP ports 500 and 4500 on the egress of the HQ to UDP ports 500 and 4500 of the LAN router respectively.

Map UDP port 500.

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

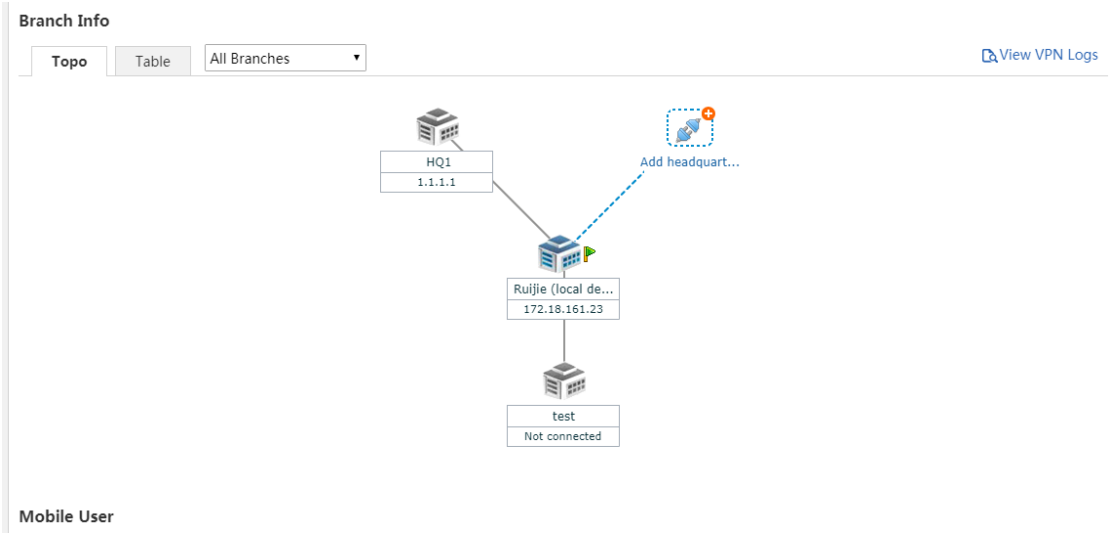
Map UDP port 4500.

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

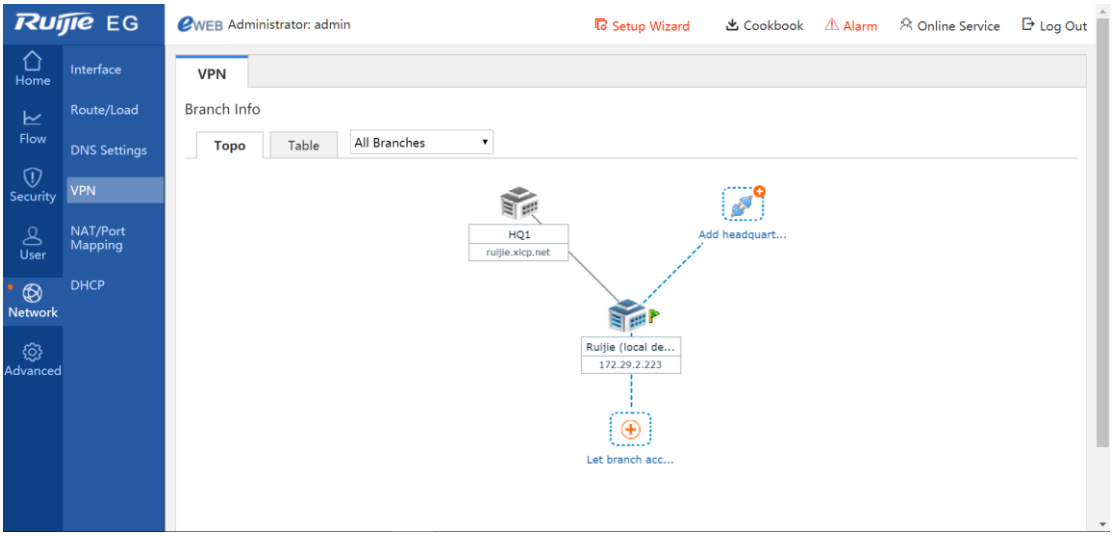
Verification

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.

3.9 Integrating the NBR Device with Ruijie Cloud

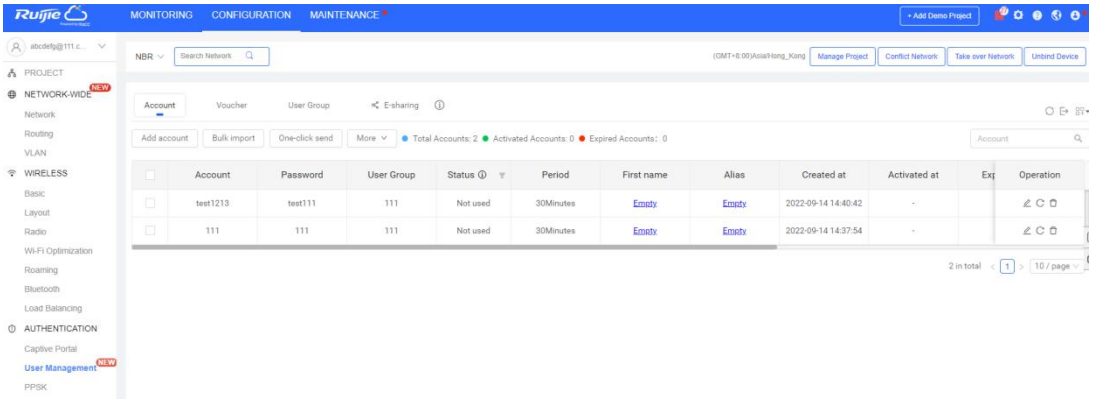
Application Scenario

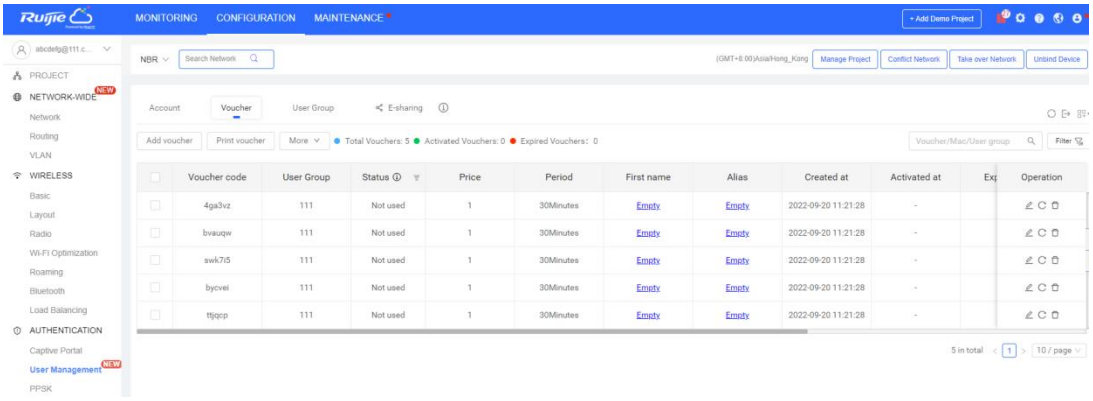
By integrating Ruijie Cloud and the router, the portal template, voucher, account, one-click and SMS authentication method can be synchronized to the router, which can enhance local authentication performance.

3.9.1 Synchronizing Voucher/Account Login to a Router

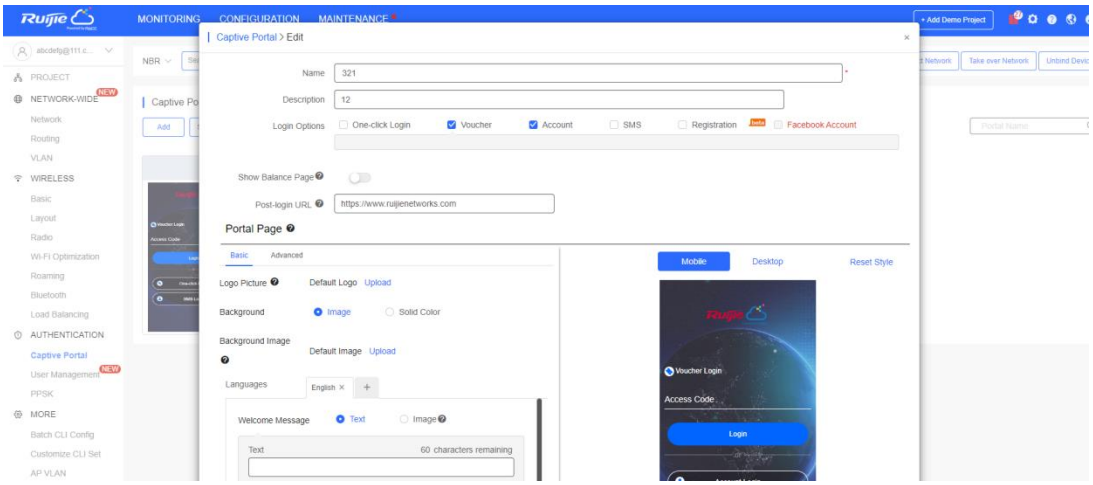
Procedure

(1) Connect the router to Ruijie Cloud, and create a voucher and an account on Ruijie Cloud.

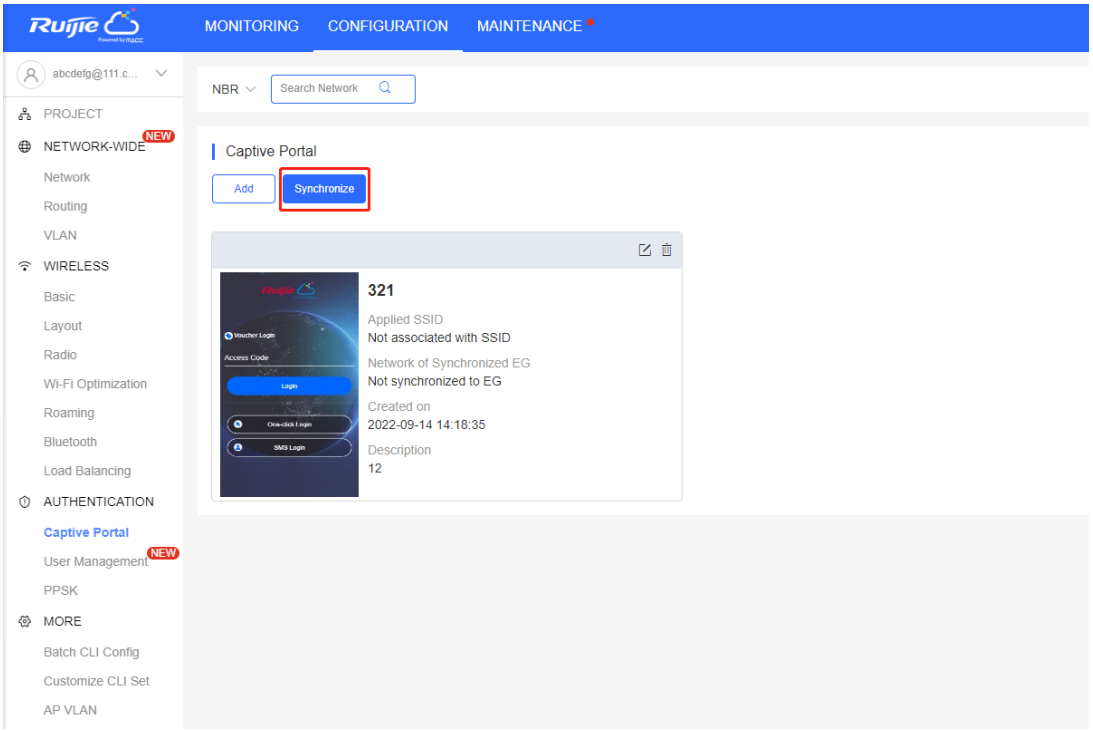


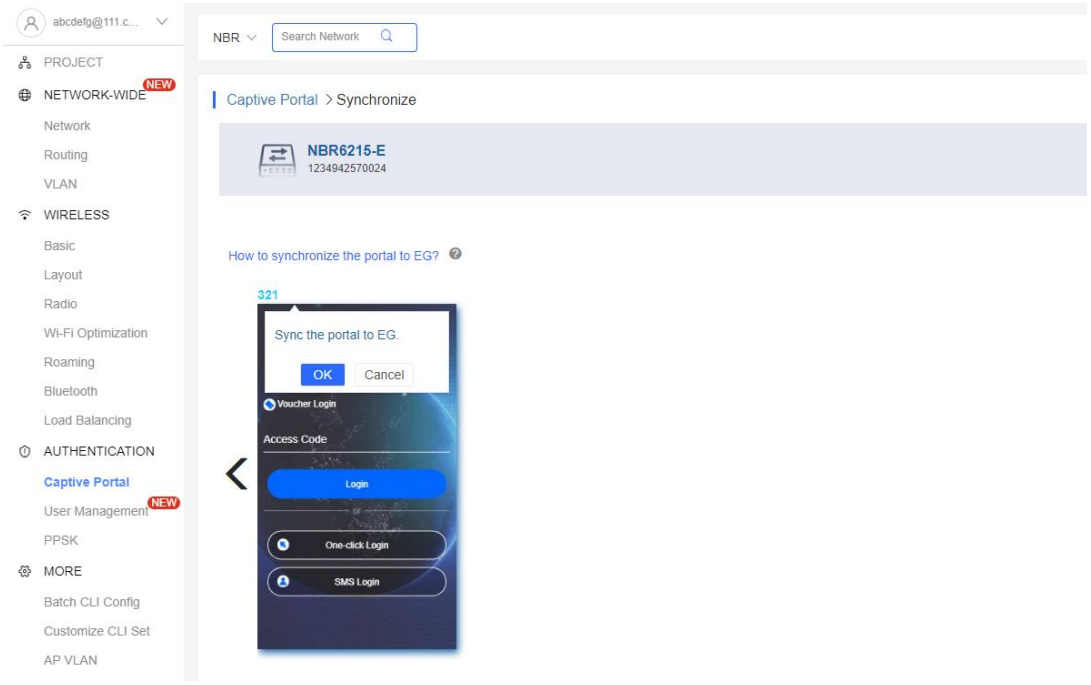


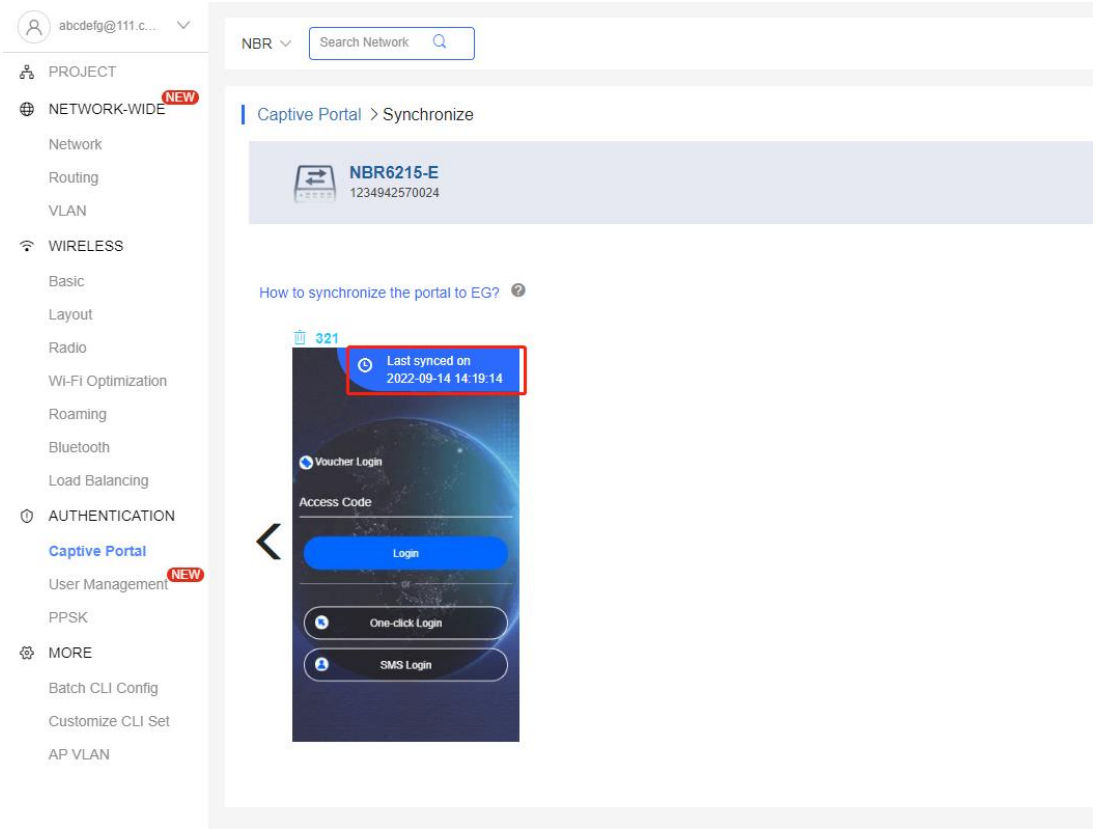
(2) Access Ruijie Cloud, choose **Configuration** > **Authentication** > **Captive Portal**, select the group and add the captive portal template, and set **Login Option** to **Voucher** and **Account**.



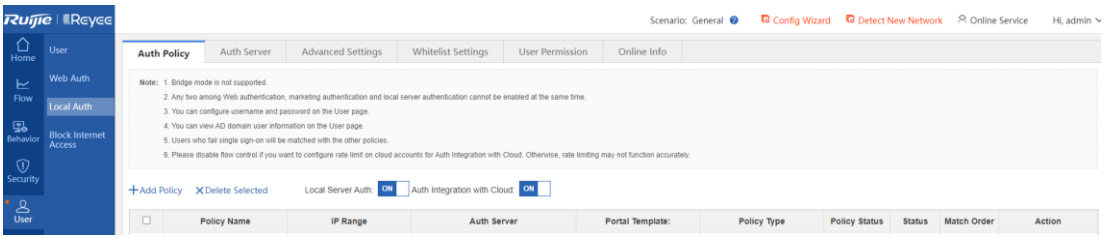
(3) Click **Synchronize** to synchronize the captive portal from Ruijie Cloud to the router.



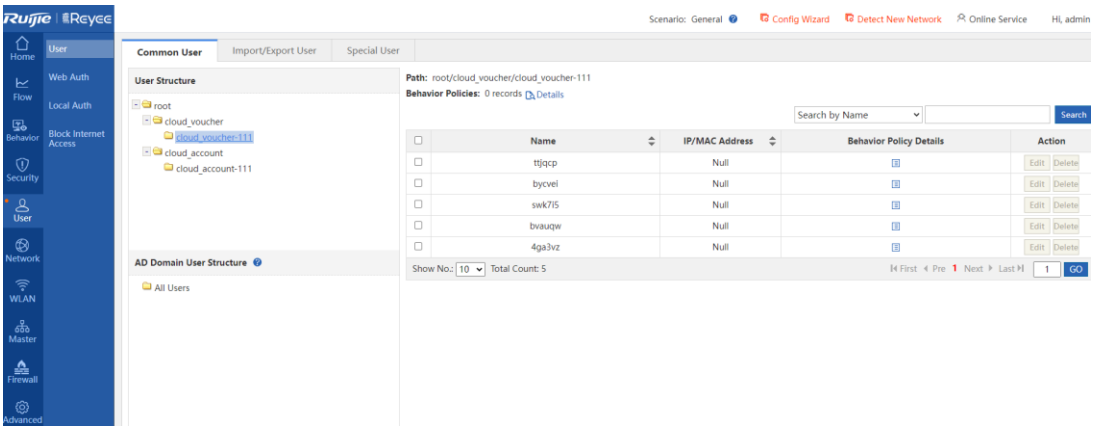




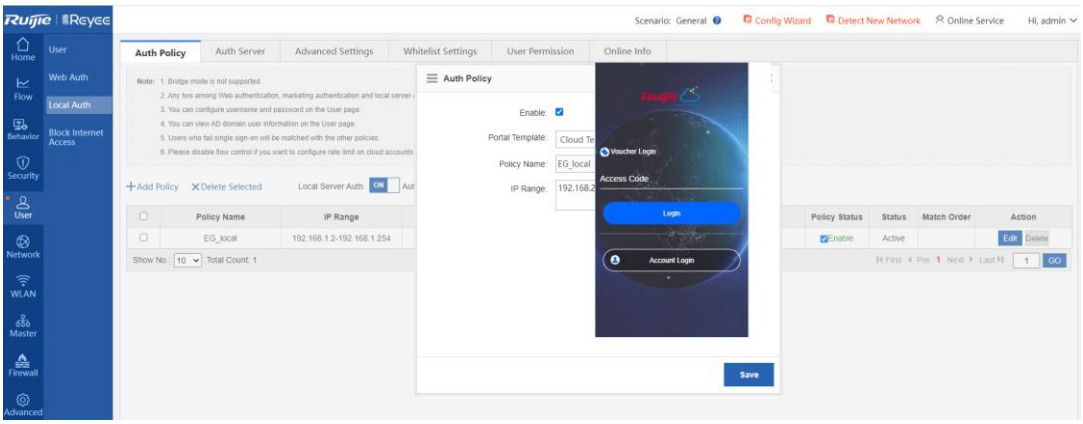
(4) Log in to the router, choose **User** > **Local Auth**, and enable **Auth integration with Cloud**.

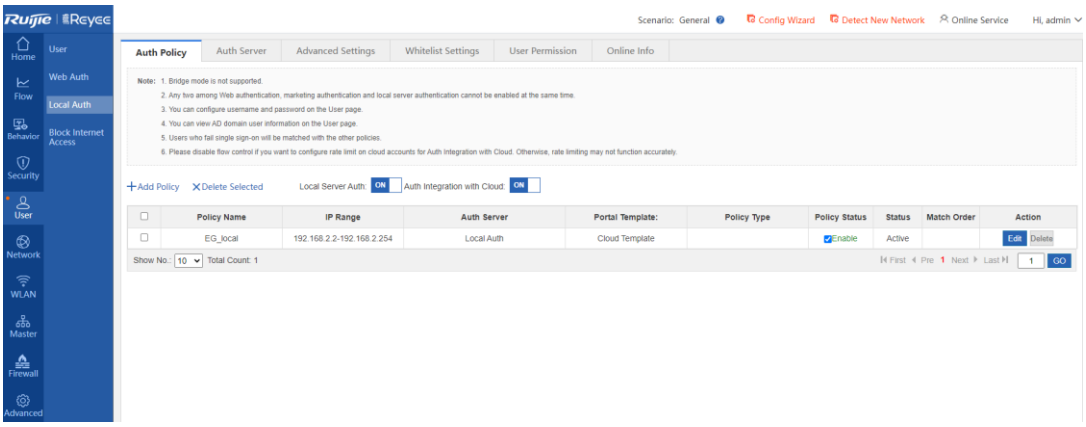


(5) Log in to the router and choose **User** > **User**. Users synchronized from Ruijie Cloud (voucher and account) will be displayed.



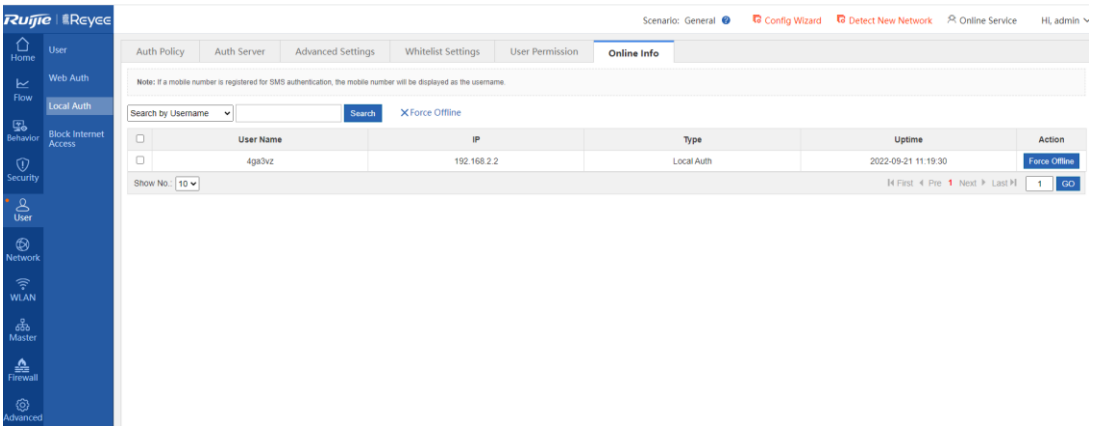
(6) Log in to the router, choose **User** > **Local Auth** > **Auth Policy** > **Add Policy**, and set the portal template and IP range.

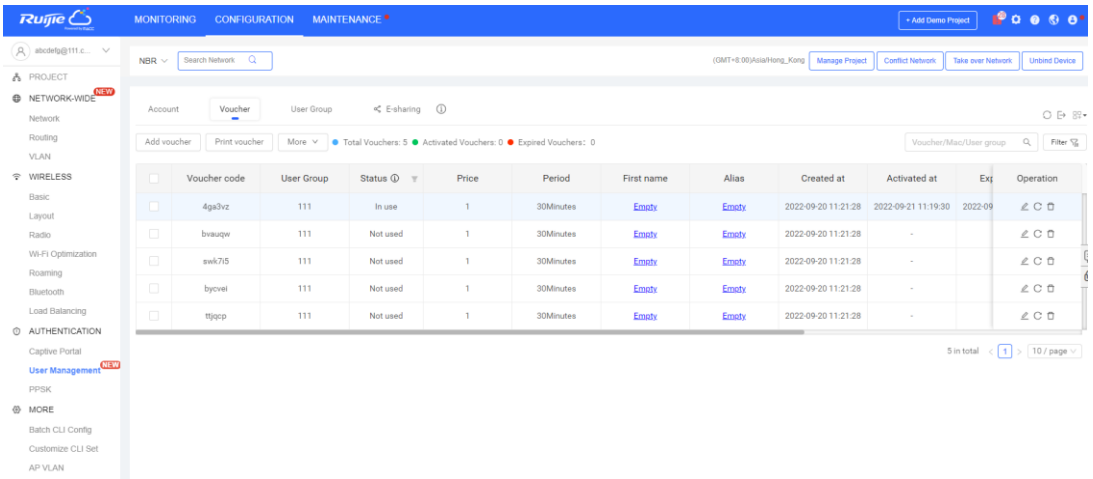




(7) Verification

Connect to the network with the account login. This account status is activated on Ruijie Cloud after login.



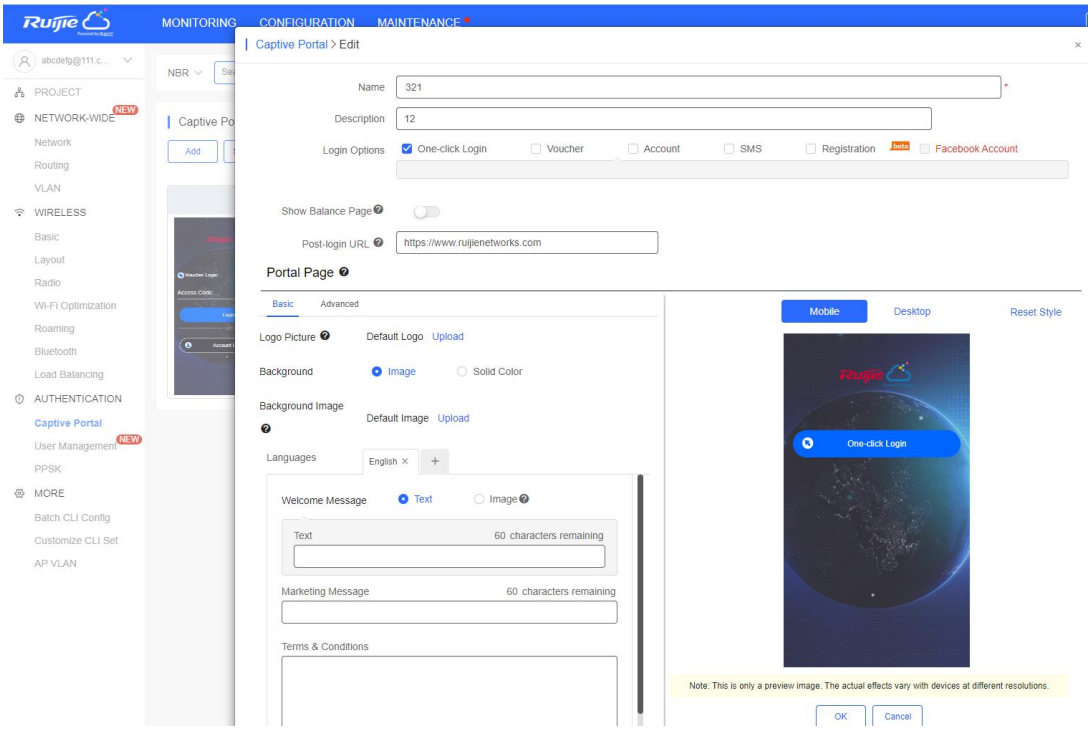


3.9.2 Synchronizing Voucher/Account Login to a Router

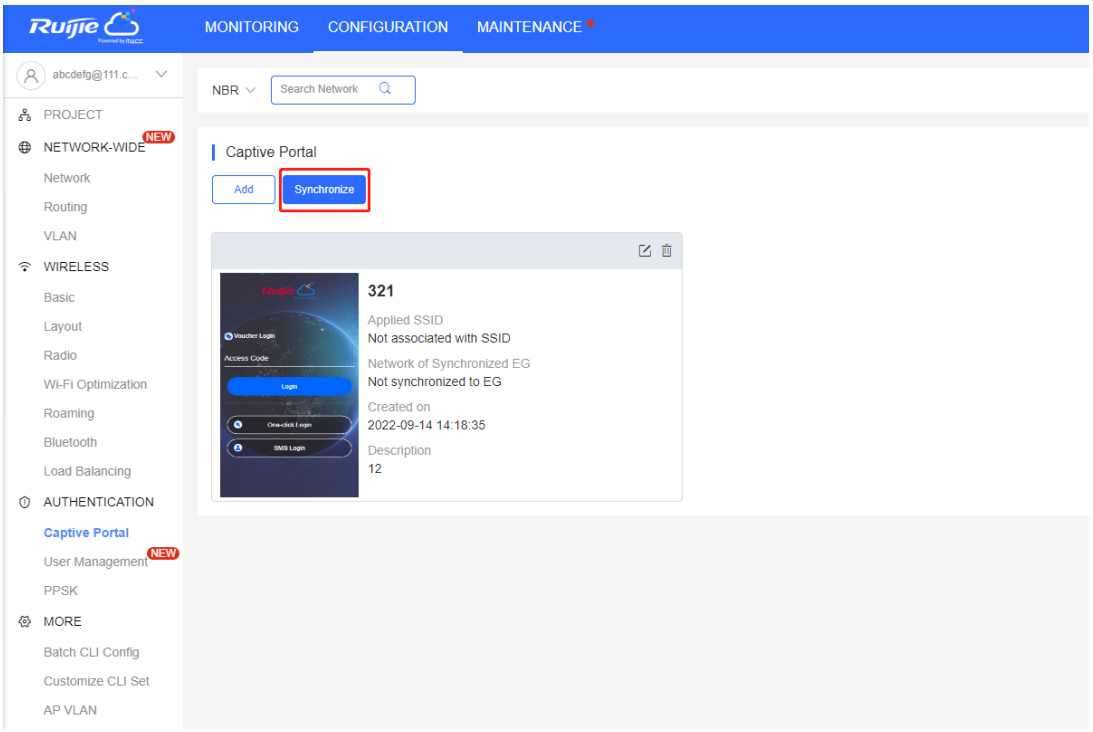
Procedure

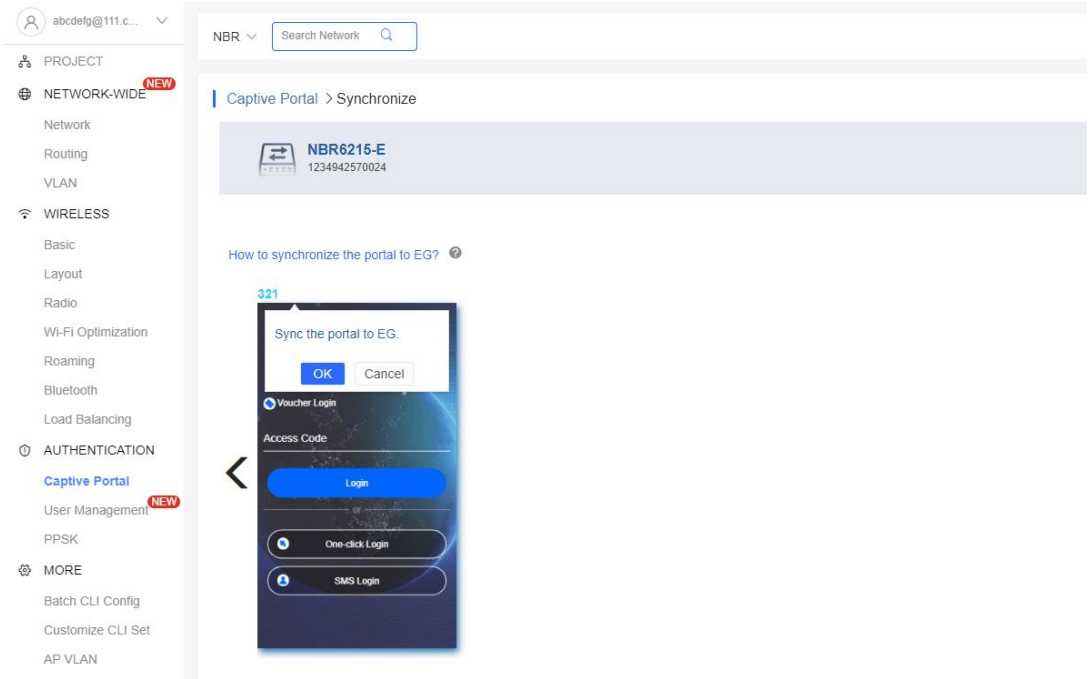
(1) Connect the router to Ruijie Cloud.

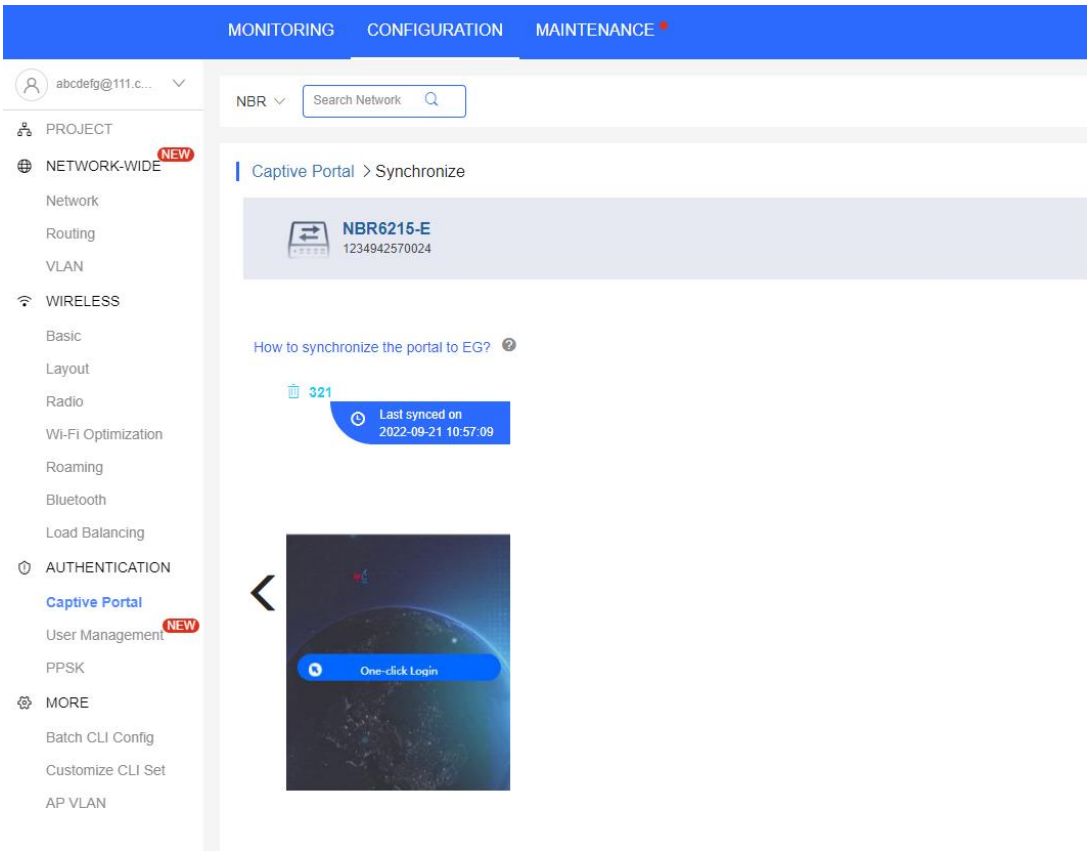
(2) Access Ruijie Cloud, choose **Configuration** > **Authentication** > **Captive Portal**, select the group and add the captive portal template, and set **Login Option** to **One-click**.



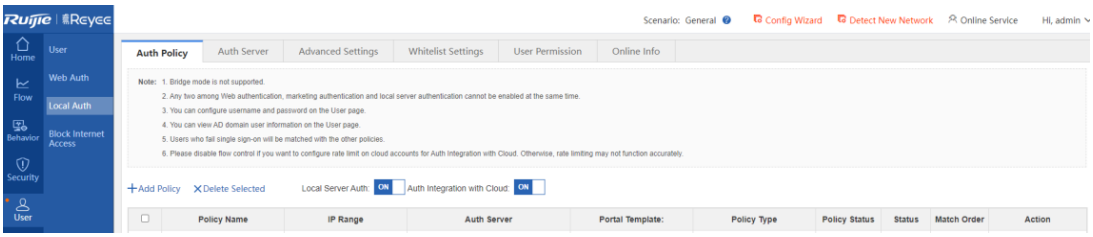
(3) Click **Synchronize** to synchronize the captive portal from Ruijie Cloud to the router.


MONITORING
CONFIGURATION
MAINTENANCE
abcdefg@111.c...
PROJECT
NETWORK-WIDE
NEW
Network
Routing
VLAN
WIRELESS
Basic
Layout
Radio
Wi-Fi Optimization
Roaming
Bluetooth
Load Balancing
AUTHENTICATION
Captive Portal
User Management
NEW
PPSK
MORE
Batch CLI Config
Customize CLI Set
AP VLAN
NBR
Search Network
Captive Portal
Add
Synchronize
321
Applied SSID
Not associated with SSID
Network of Synchronized EG
Not synchronized to EG
Created on
2022-09-14 14:18:35
Description
12

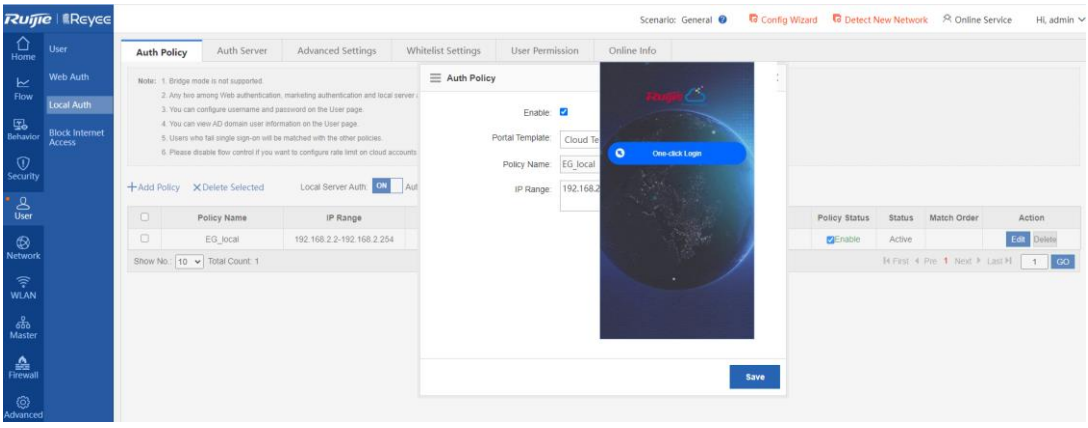

abcdefg@111.c...
PROJECT
NETWORK-WIDE
NEW
Network
Routing
VLAN
WIRELESS
Basic
Layout
Radio
Wi-Fi Optimization
Roaming
Bluetooth
Load Balancing
AUTHENTICATION
Captive Portal
User Management
NEW
PPSK
MORE
Batch CLI Config
Customize CLI Set
AP VLAN
NBR
Search Network
Captive Portal > Synchronize
NBR6215-E
1234942570024
How to synchronize the portal to EG?
321
Sync the portal to EG.
OK
Cancel
Voucher Login
Access Code
Login
One-click Login
SMS Login

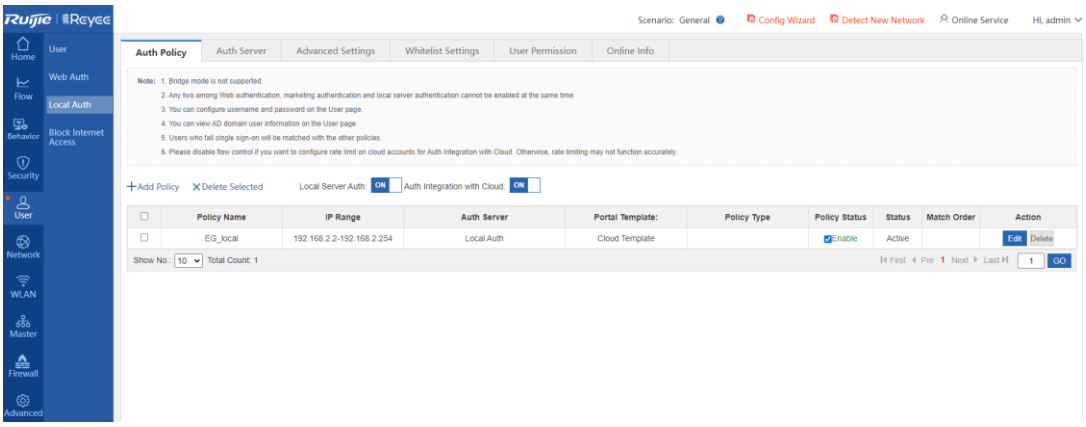


(4) Log in to the router, click **User** > **Local Auth,** and enable **Auth integration with Cloud**



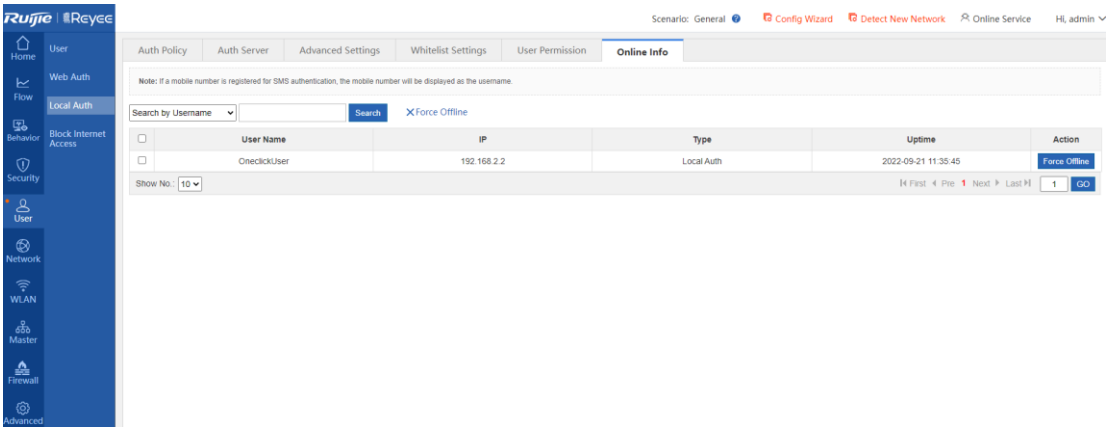
(5) Log in to the router, choose **User** > **Local Auth** > **Auth Policy** > **Add Policy**, and set the portal template and IP range.





(6) Verification

Connect a client to the network. The one-click login portal page will be displayed. The user can access the Internet after login.



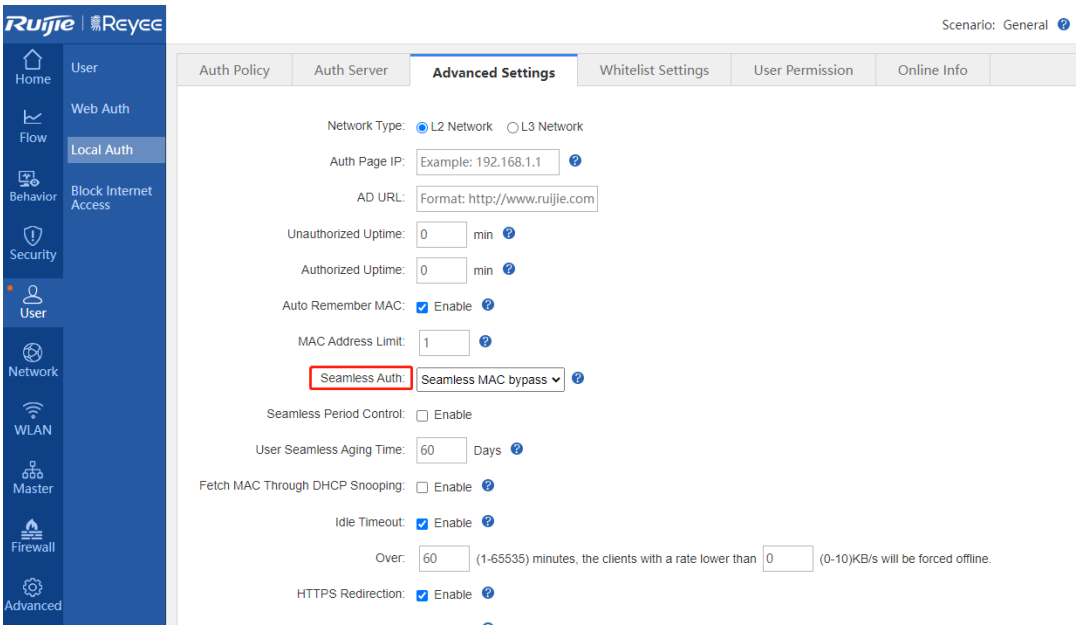
3.9.3 Synchronizing Voucher/Account Login to the NBR Device

Procedure

(1) Connect the router to Ruijie Cloud, and add/delete the voucher/account, which should be synchronized to the router.

(2) Enable or disable seamless authentication on the router.

There are three seamless authentication options, which are **Disable**, **Seamless MAC bypass** and **Browser-based authentication bypass.**



(3) Verification

After a user goes online for the first time, it will connect to the network automatically next time without authentication.

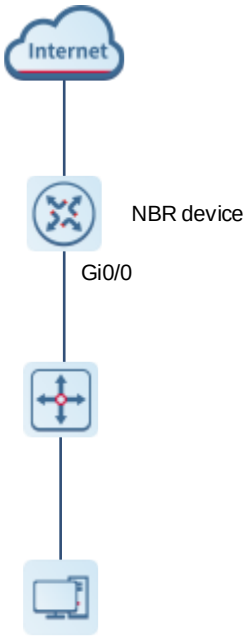
3.10 Local Web Authentication

Application Scenario

- LAN users access the Internet through the NBR router.
- The WAN bandwidth is 10 Mbit/s, the IP address of the WAN port is 192.168.33.56/24, the IP address of the WAN router is 192.168.33.1, and the addresses of LAN ports are in the 192.168.1.1/24 network segment.
- LAN users can access the WAN only after passing identity authentication.
- The router supports web authentication on sub-interfaces. The configuration method is the same as that of common web authentication.
- Internal web authentication allows users to proactively add go-offline pages to favorites and modify passwords. With this function enabled, the router forbids users from accessing the Internet (blocking user accounts) and disconnects users.

Note

The preceding IP addresses are used in a simulated environment and are not provided by an IPS device.



Prerequisites

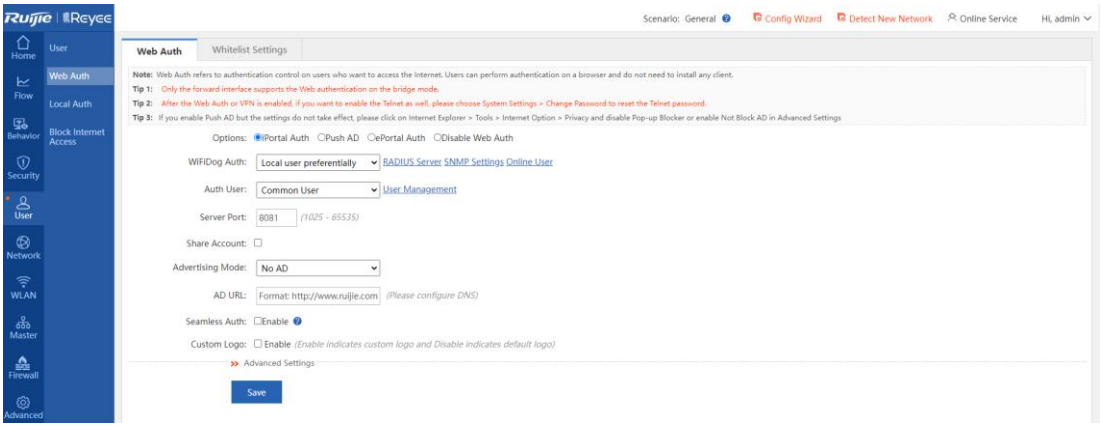
- Perform wizard-based setup to ensure that LAN users can successfully access the WAN.
- Select the internal Web authentication server function in the real-name Internet access policy.

Note

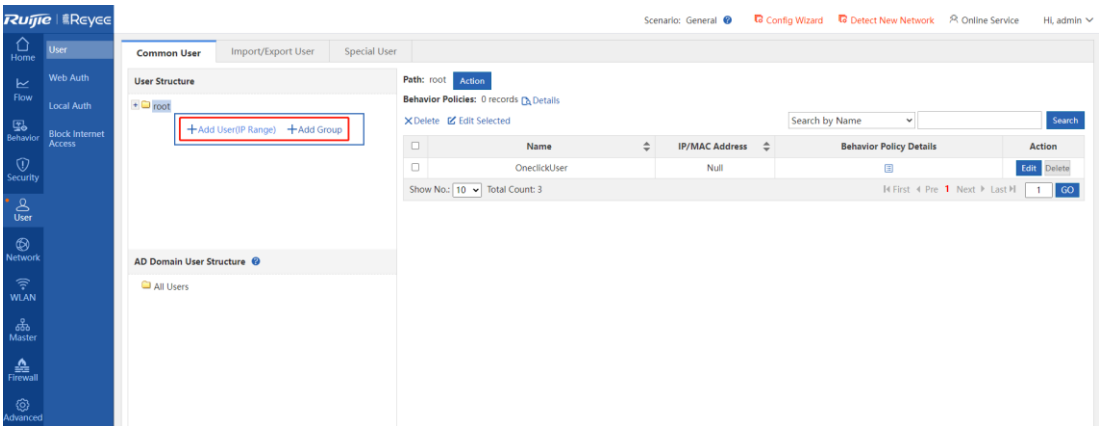
- If advertisement push is enabled, the entered advertisement address cannot contain the character "?".
- If web authentication is enabled and port mapping is configured, the LAN server IP address used for port mapping needs to be added to the authentication-exempt IP address list. Otherwise, port mapping may fail.
- After web authentication is enabled, the remote login password (that is, Telnet password) needs to be changed. If advertisement push is enabled, the entered advertisement address cannot contain the character "?".

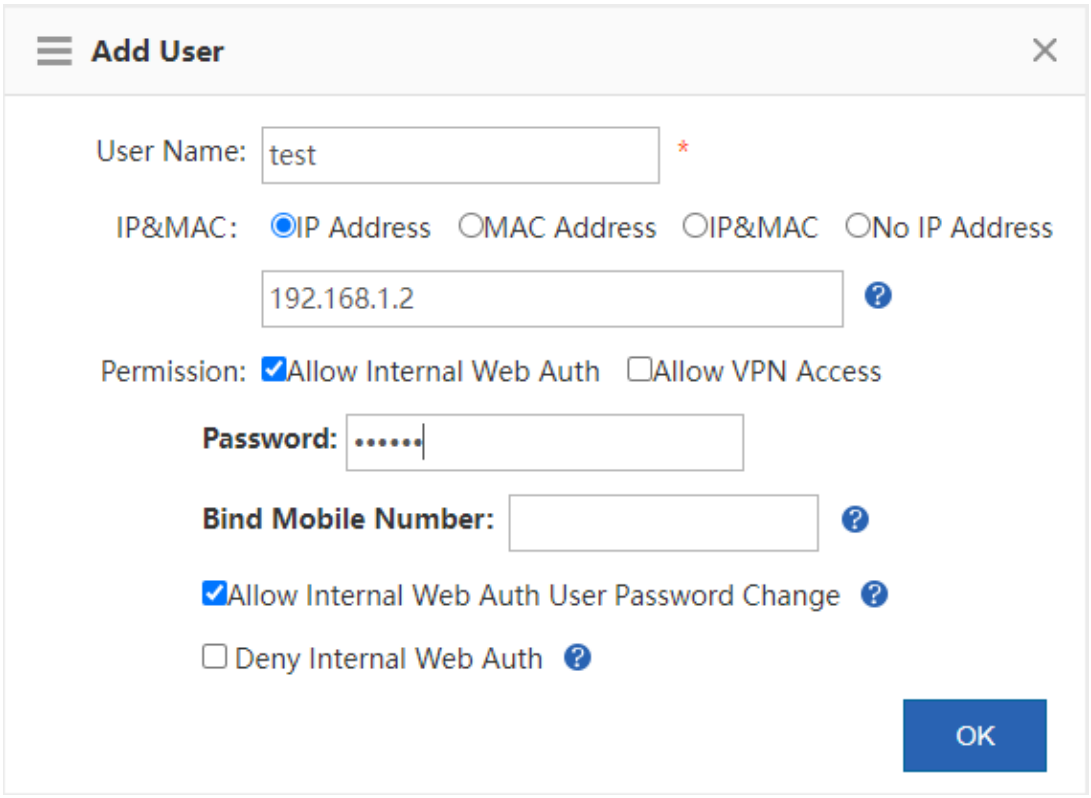
Procedure

(1) Choose **User** > **Web Auth** and click **iPortal Auth** on the **Web Auth** tab page to enable the internal authentication function, as shown in the following figure.

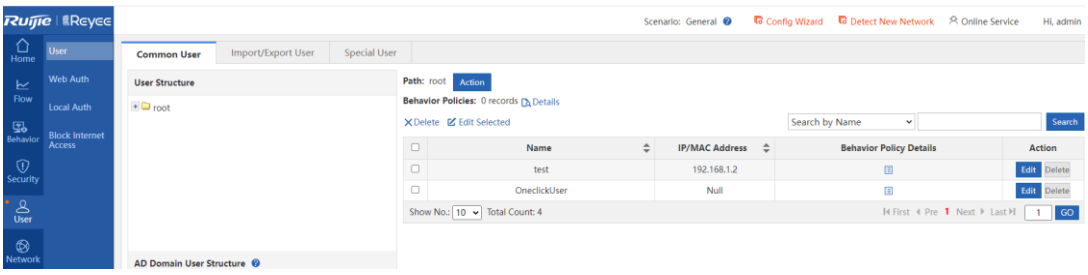


(2) Add a user to be authenticated: Click a user group in the user organization on the left, add a user (IP range) to the user group, and configure the username and password, as shown in the following figure.





(3) A user added successfully is displayed in the user list, as shown in the following figure.



(4) 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 only web authentication for the account.

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

(5) 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.

(6) **Verification**

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

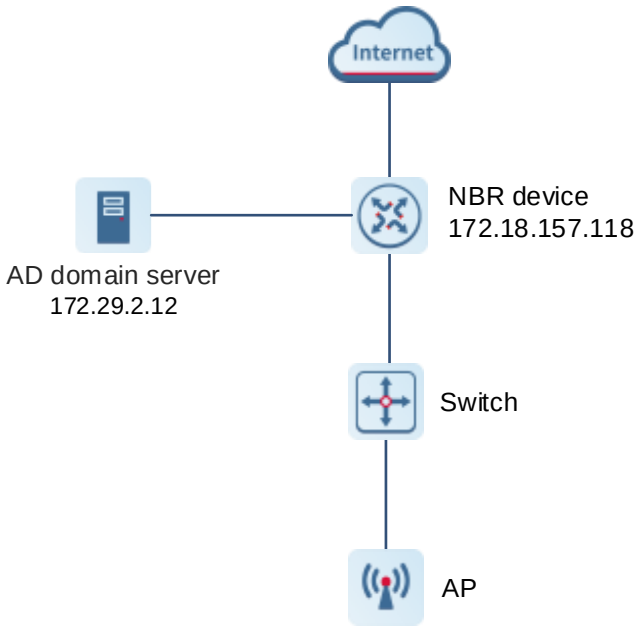
Enter the correct username and password and click **Log in**. The authentication success page is displayed.

3.11 AD Domain Integration

Application Scenario

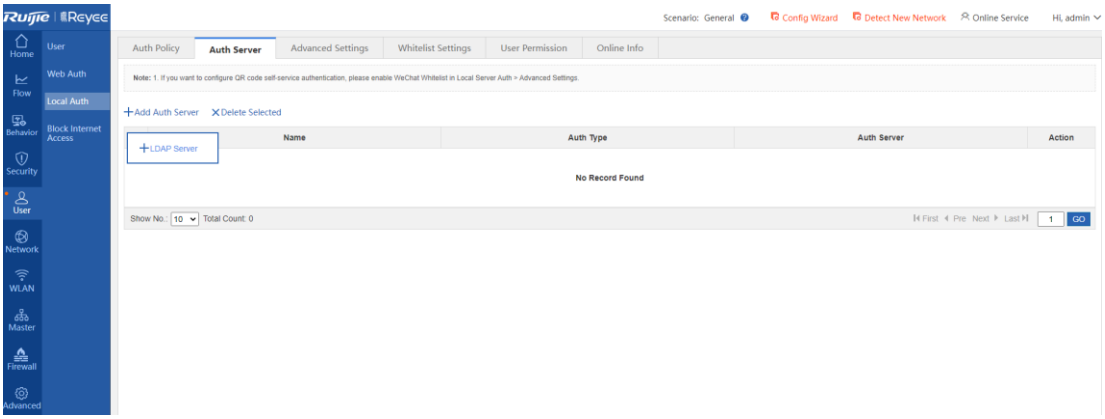
A server running Active Directory Domain Service (AD DS) is called a domain controller. It authenticates and authorizes all users and computers in a Windows domain network. That is, it assigns and enforces security policies for all computers and installing or updating software.

Active Directory Domain Services (AD DS) is the cornerstone of every Windows domain network. It stores information about members of the domain, including devices and users, verifies their credentials, and defines their access rights.

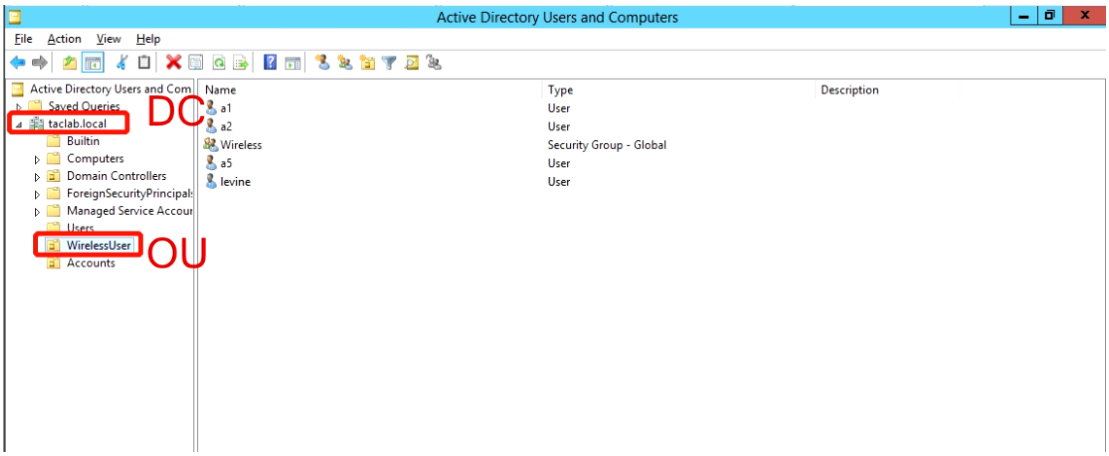


Procedure

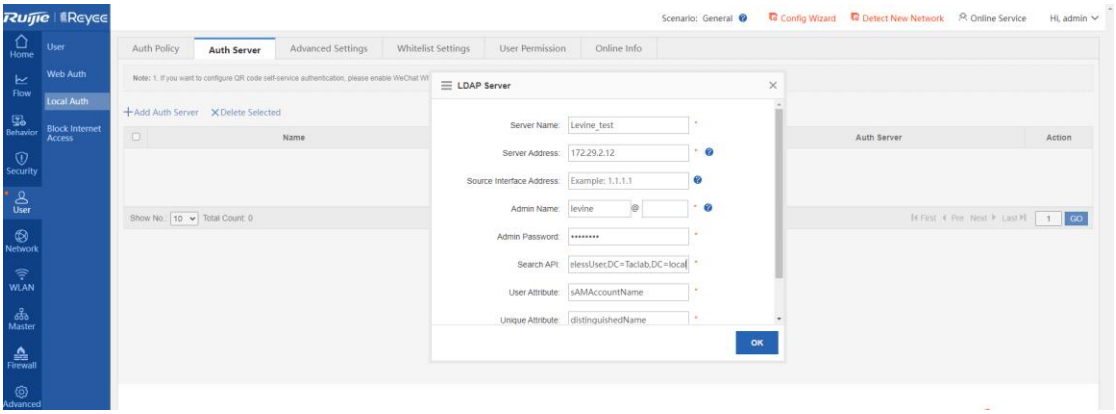
(1) Choose **User** > **Local Auth** > **Auth Server** and add an AD domain server on the router.



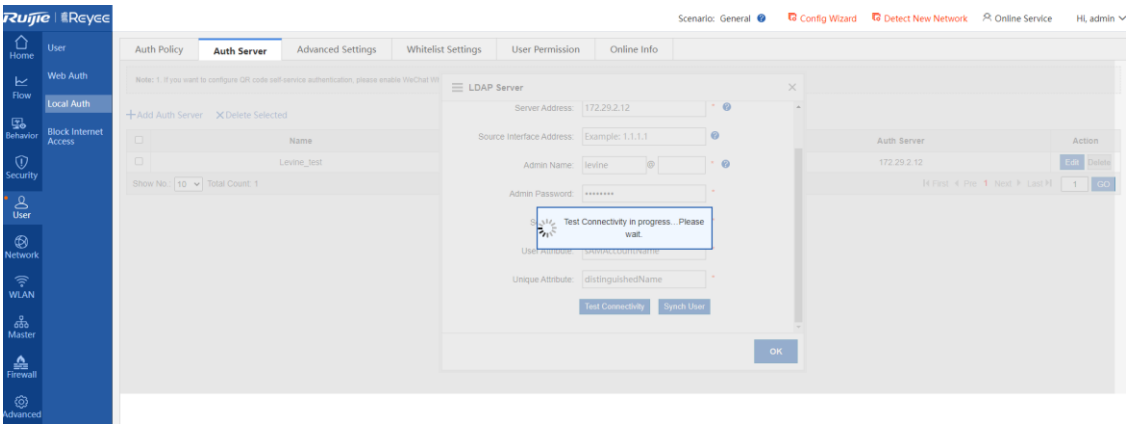
(2) Edit the LDAP server.



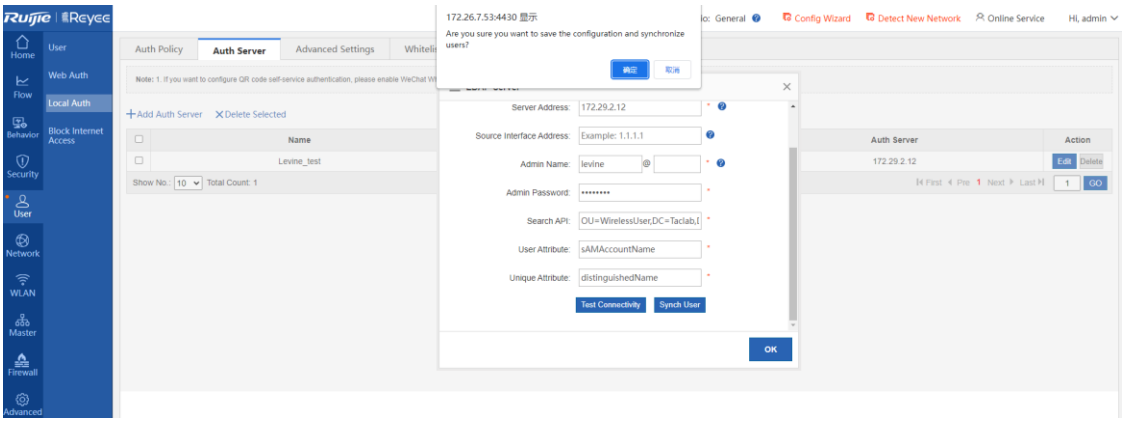
In this case, the Search API is: OU=WirelessUser,DC=taclab,DC=local.

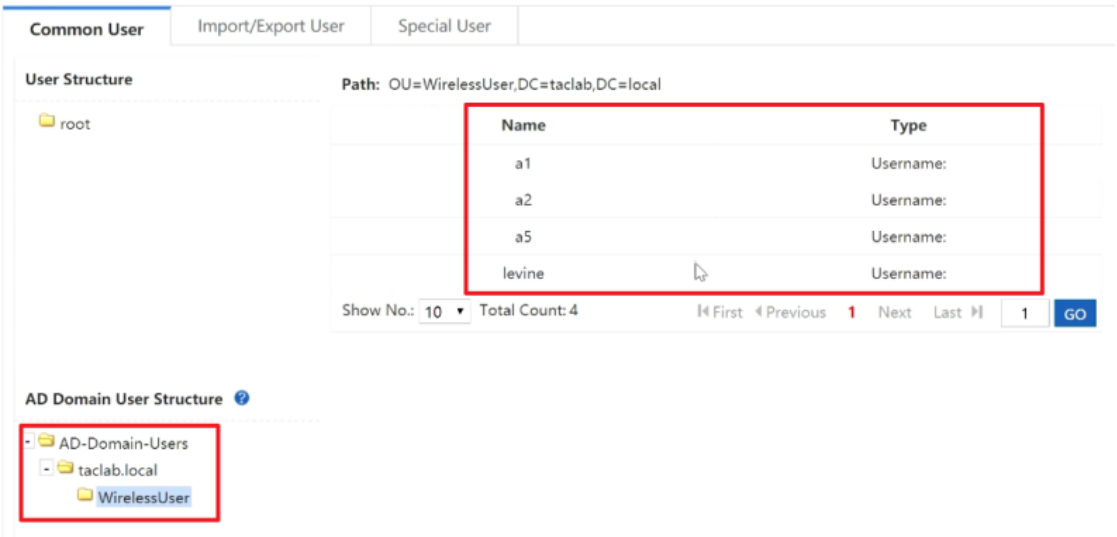


(3) Check the connectivity between the router and LDAP server.

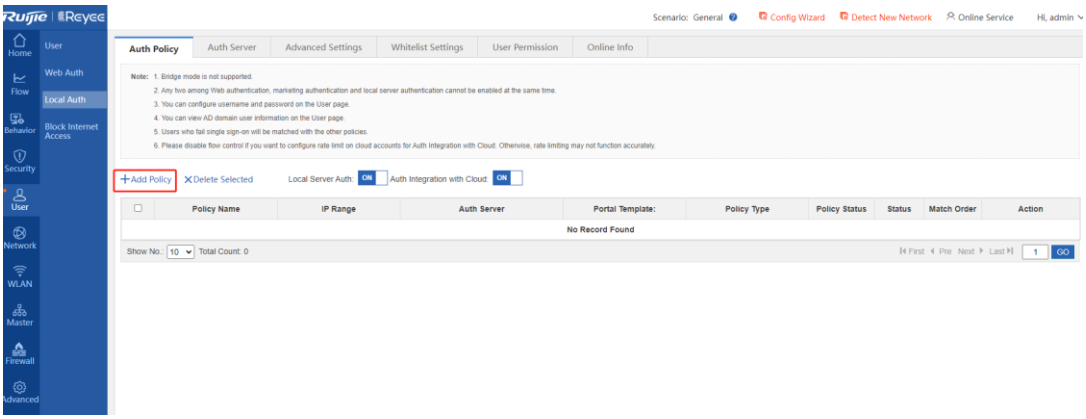


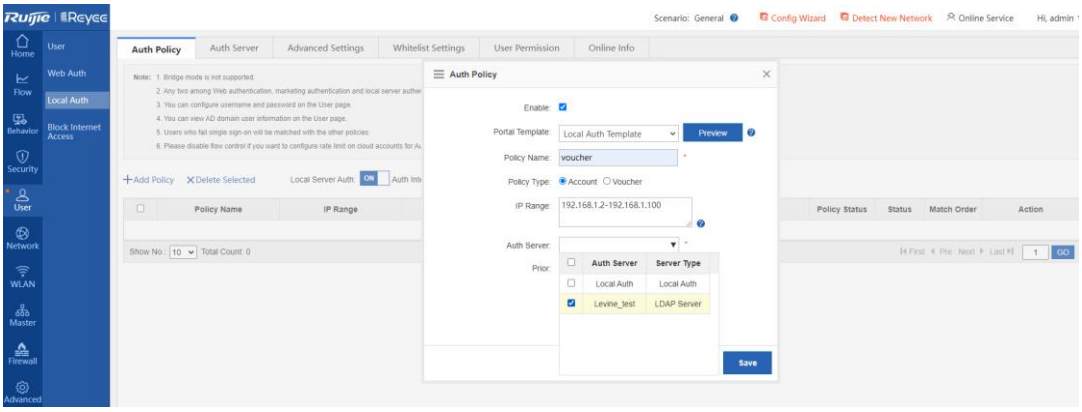
(4) Synchronize the account to the router.





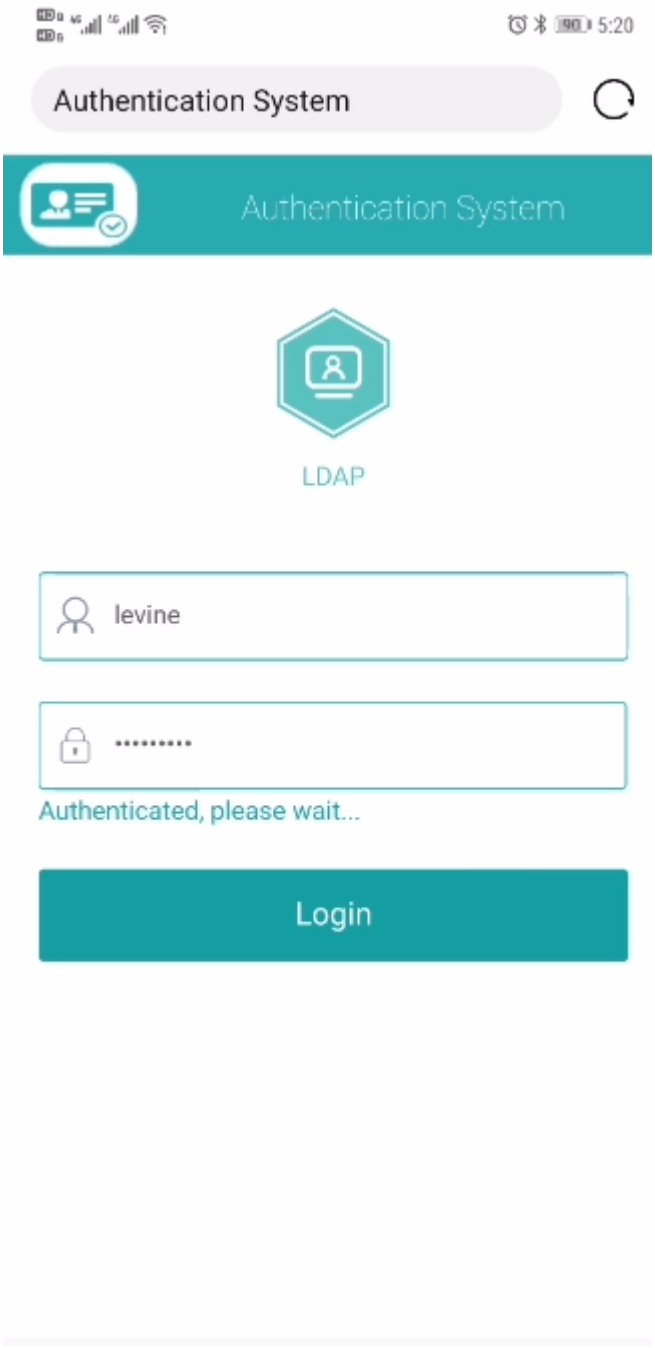
(5) Configure an authentication policy on the router.





(6) **Verification**

Connect a device to the network. The authentication page will be displayed. A user can log in with the AD account.


5:20
Authentication System
Authentication System
LDAP
levine
Authenticated, please wait...
Login

3.12 Firewall

The firewall feature can detect multiple types of network-layer attacks and take measures based on the configured policy to protect the internal network from malicious attacks, thereby ensuring the normal operation of the internal network.

Note

- The NBR6205-E, NBR6210-E and NBR6215-E enterprise-class routers support the firewall feature.
- The NBR6120-E enterprise-class router does not support the firewall feature.

3.12.1 Attack Defense Configuration

The router is usually deployed on the intranet egress. Both normal service traffic and malicious attack traffic pass through the router. You can enable the attack defense function and configure corresponding policies to detect and block the attack traffic passing through the router, ensuring the safety of the internal network.

Attack defense configuration supports the protocol policy, zone policy, and global defense policy, which are prioritized in a decreasing order.

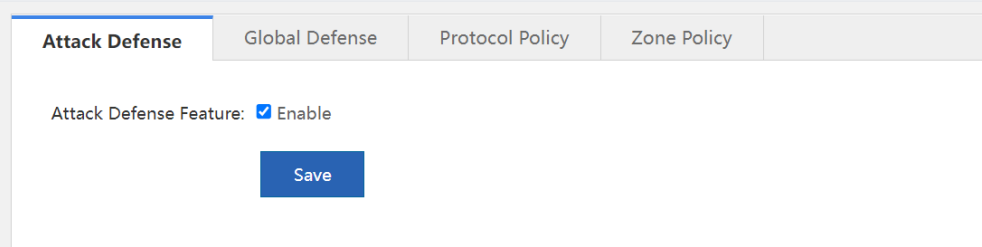
1. Attack Defense Feature

The attack defense feature is used to display the menu and configure the attack defense. Only when you enable the feature can you view and configure the attack defense feature. If the attack defense is enabled, the device and the internal network will be defended according to the predefined policies. You can add new defense policies as required.

Procedure

(1) Choose **Firewall** > **Attack Defense Config** > **Attack Defense**.

(2) Select **Enable** to enable the attack defense feature and click **Save**.



2. Global Defense

Global defense is designed to defend the router. The global defense limits the establishment speed of sessions to ensure efficient utilization of router resources. You can enable global defense to prevent resource exhaustion attacks or DoS attacks.

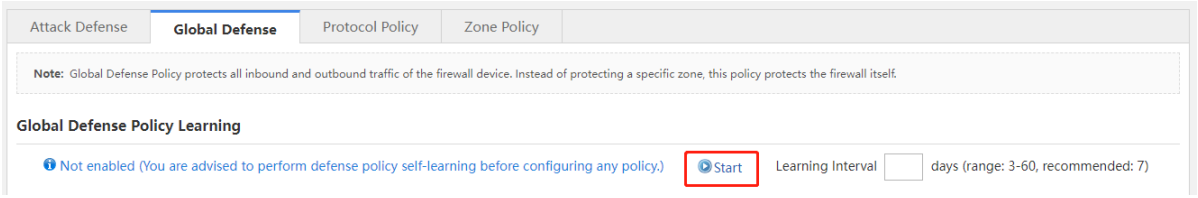
Procedure

(1) Choose **Firewall** > **Attack Defense Config** > **Global Defense**.

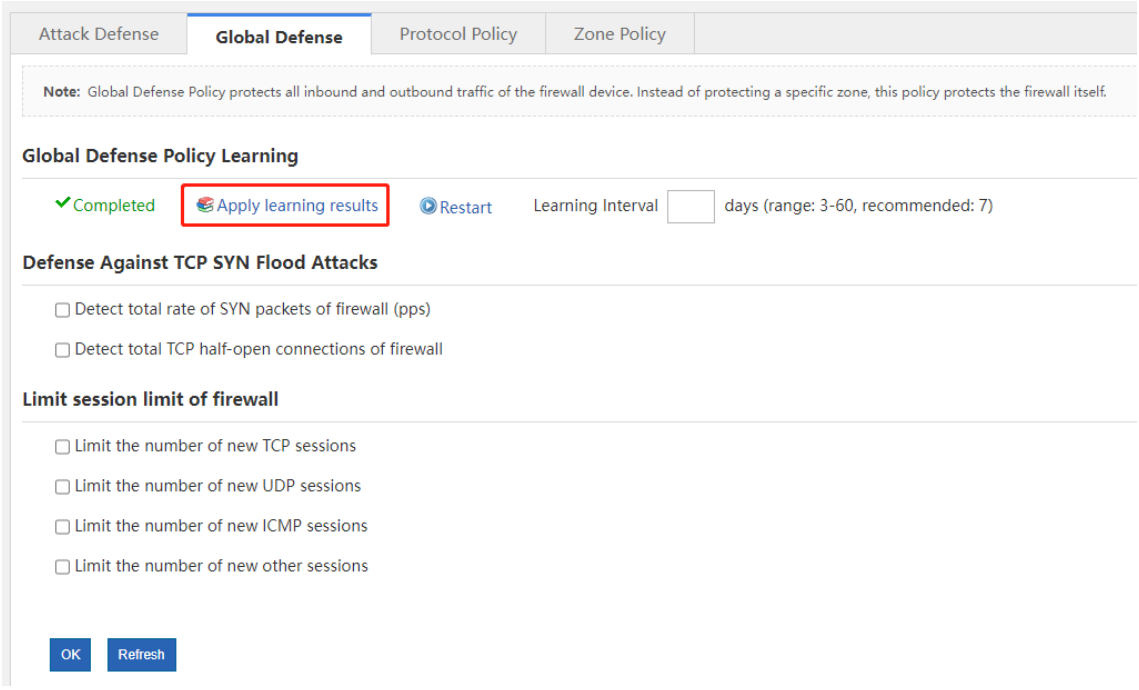
(2) Click **Start** and the device will obtain an optimal protection threshold that fits the current network through automatic learning.

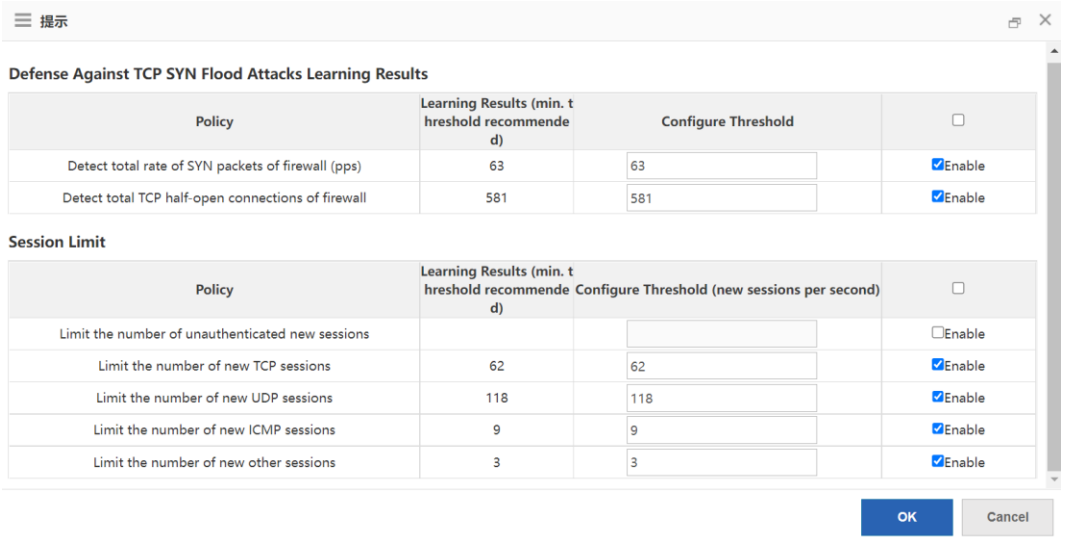
Caution

- To guarantee better effects of the learned policy, please ensure that the automatic learning period includes the traffic peak period.
- The default learning period is seven days. You can suspend the learning period or set a new period as required.
- You are advised to make the device relearn and apply new learning results after the network is changed.



(3) After global defense policy learning is completed, click **Apply learning results**. Adjust the threshold based on the network conditions and learning results.





(4) Click **OK** after the configuration is completed.

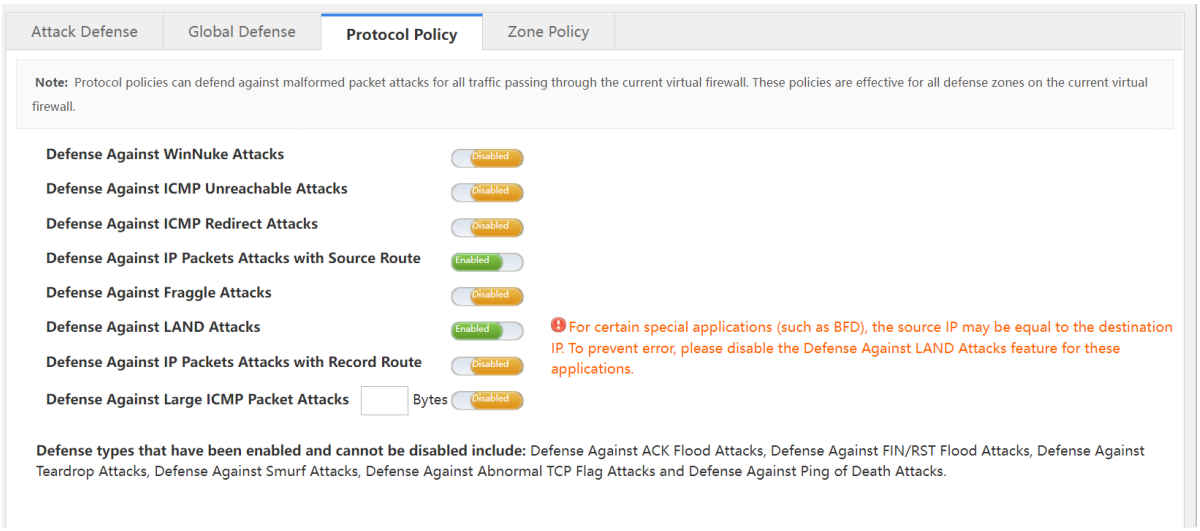
3. Protocol Policy

Protocol policies can defend against attacks for vulnerabilities of the protocol operating mechanism. The device will filter protocol packets with attack characteristics if the corresponding protocol is enabled.

Procedure

(1) Choose **Firewall** > **Attack Defense Config** > **Protocol Policy**.

(2) Click to enable the defense policy as required to make the specified policy take effect.



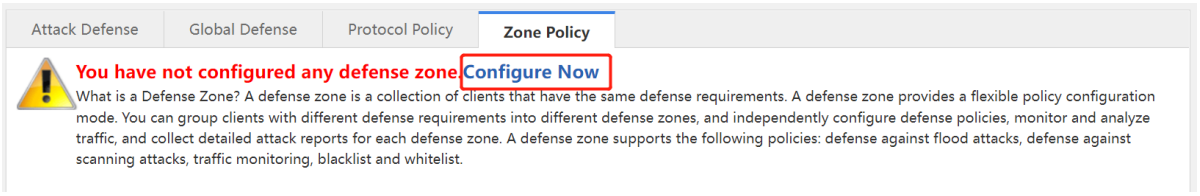
4. Zone Policy

A defense zone is a collection of clients that have the same defense requirements. You can group clients with different defense requirements into corresponding defense zones to defend the clients based on groups and manage them separately. You can configure defense policies for specified zones respectively to defend the client precisely.

Procedure

(1) Choose **Firewall** > **Attack Defense Config** > **Zone Policy**.

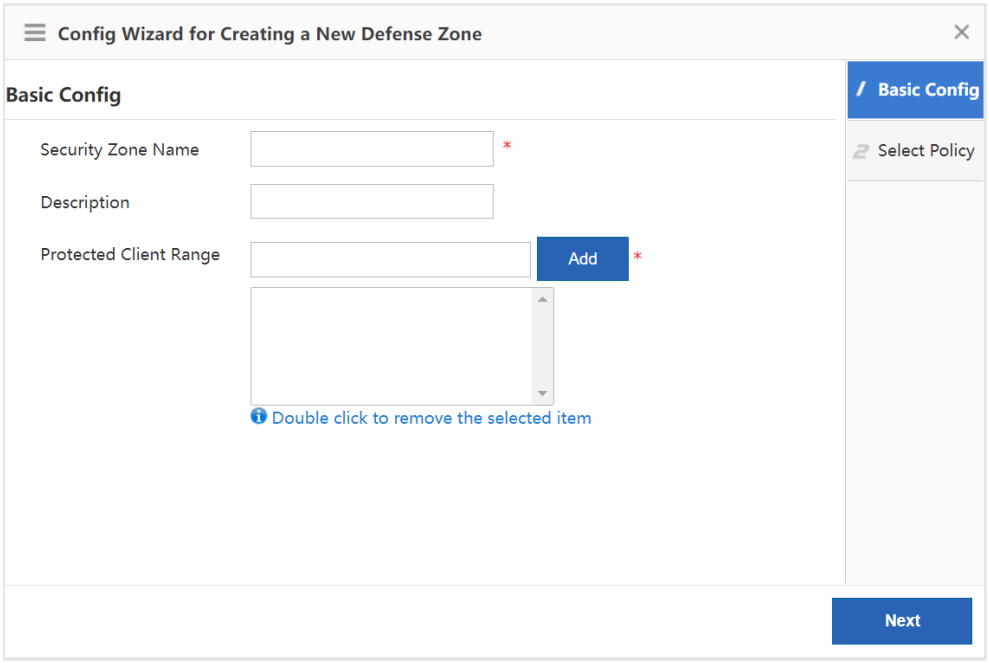
(2) Click **Configure Now** to enter the **Config Wizard for Creating a New Defense Zone** page.



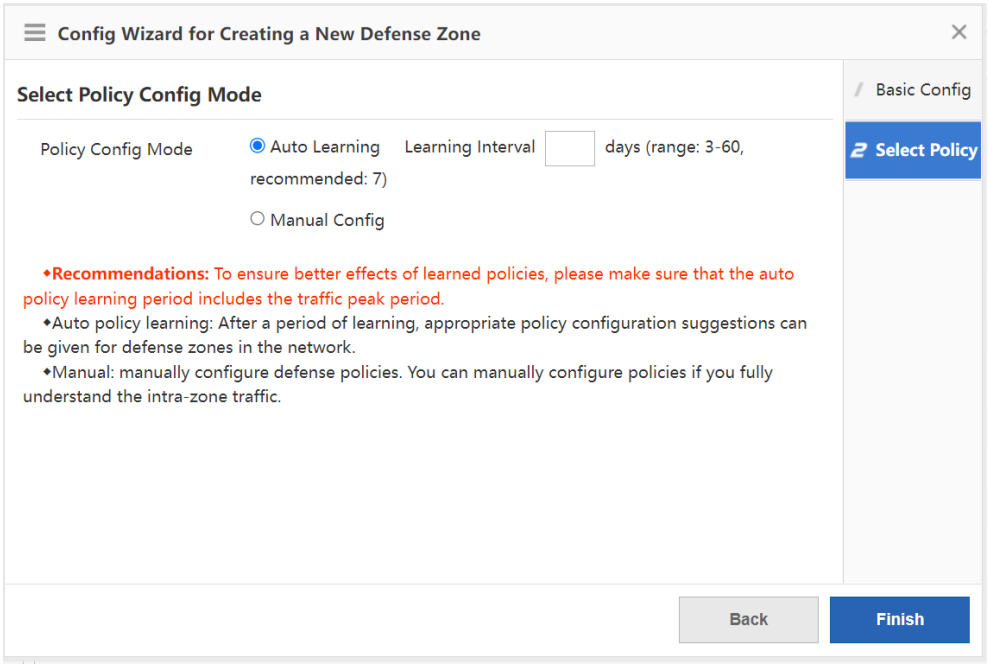
(3) Enter the security zone name, description and the protected client range, and click **Next**.

Note

The protected client range supports a single IP address (example: 1.1.1.1), subnet bit length (example: 1.1.1.0/24), or subnet mask (example: 1.1.1.0/255.255.255.0). Enter the protected client range and click **Add** to enter another range.

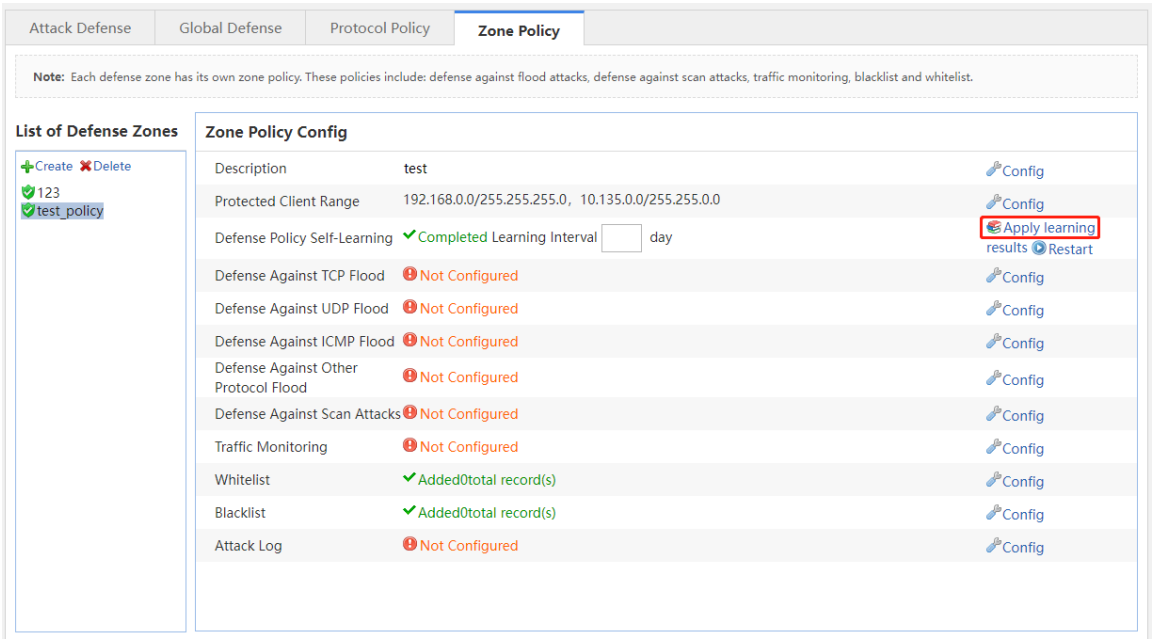


(4) Select policy configuration mode as required and click **Finish**.



(5) If you select **Auto Learning** for the policy configuration mode, follow the procedure to configure the policy. If you select **Manual Config**, you can skip the procedure.

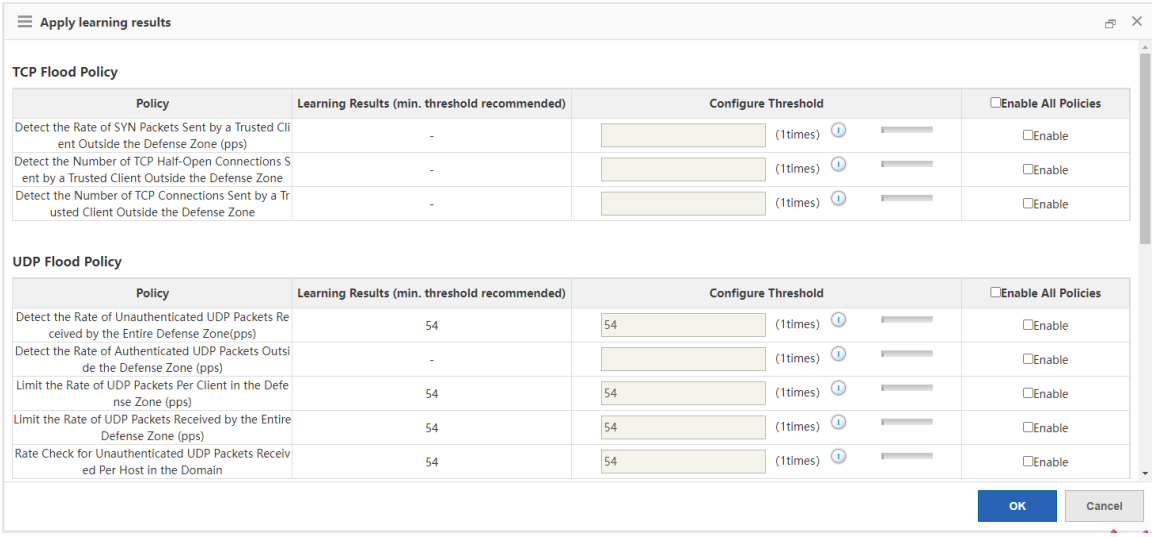
a Click Apply learning results after leaning to enter the Apply learning results page.



b Configure the threshold based on the learning results and the actual conditions of the defense zone.

Note

As the traffic monitoring function consumes some of device performance. You are advised to disable the traffic monitoring function after the defense zone policy works smoothly to ensure that the device can achieve the maximum service processing capacity.

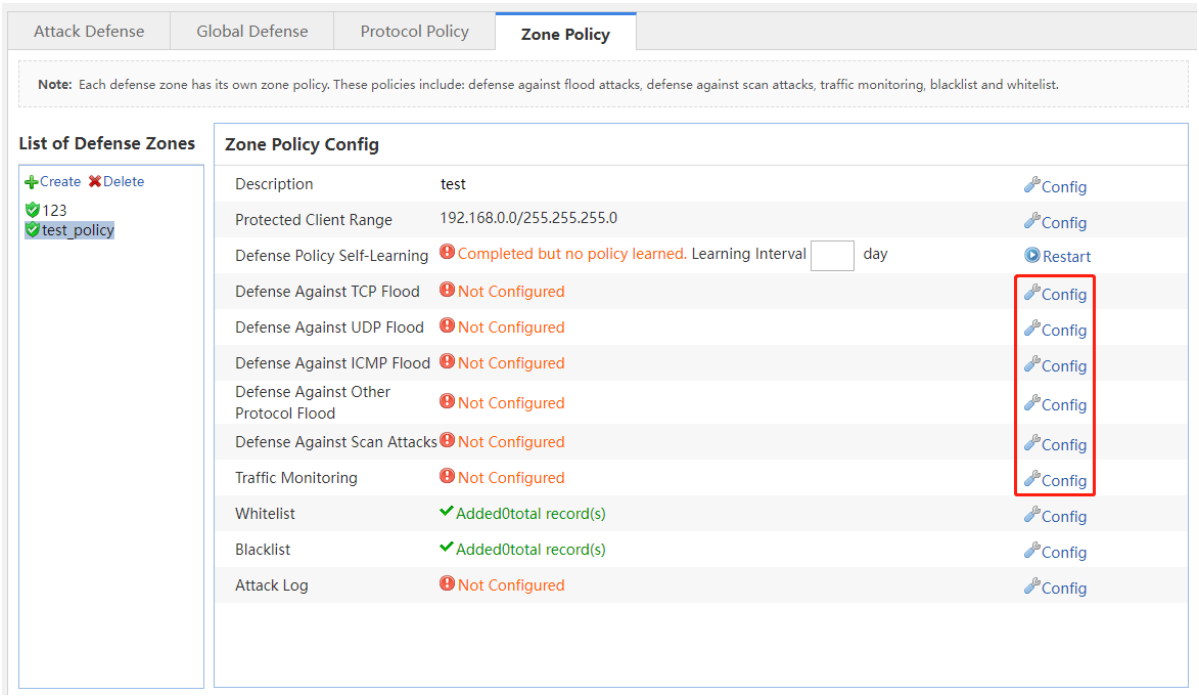


c Click **OK** after the configuration is completed.

(6) If you select **Manual Config** for the policy configuration mode, follow the procedure to configure the policy. If you select **Auto Learning**, you can skip the procedure.

Note

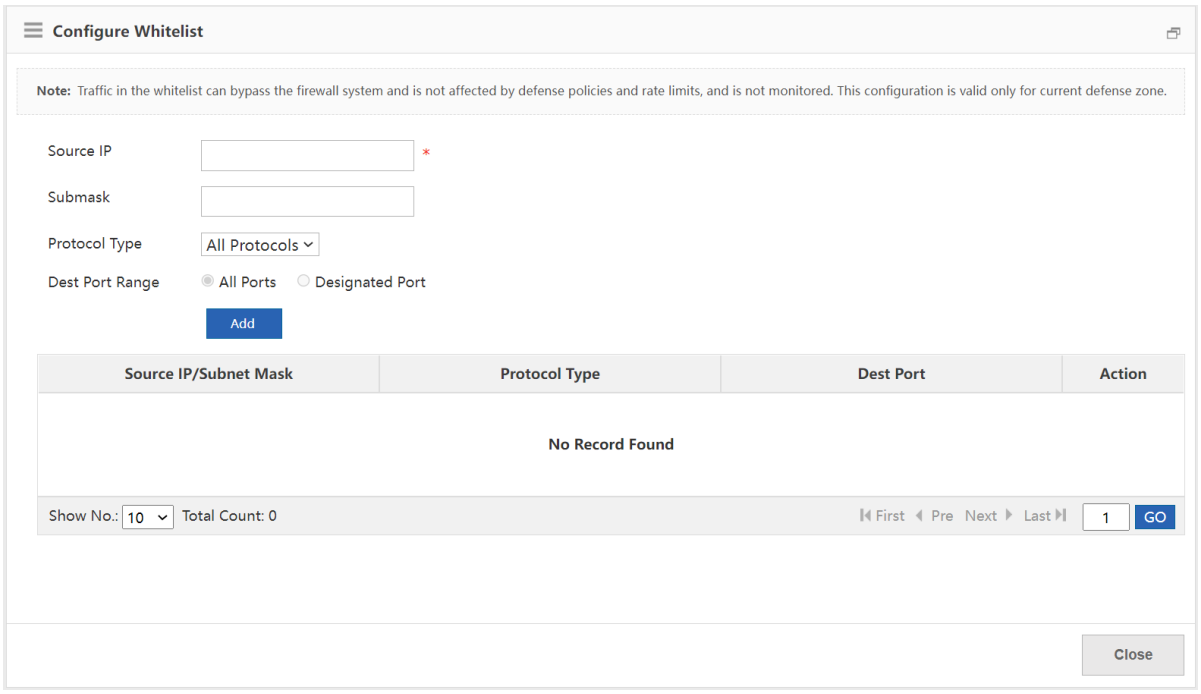
As the traffic monitoring function consumes some of device performance. You are advised to disable the traffic monitoring function after the defense zone policy works smoothly to ensure that the device can achieve the maximum service processing capacity.



(7) (Optional) For a trusted source IP address, you can add it to the whitelist to bypass the detection of the device and the traffic of this source IP will not be affected. Click **Config** of the whitelist to access the **Configure Whitelist** page, enter the source IP address, the subnet mask, select the protocol type and the designation port range, and click **Add**.

Note

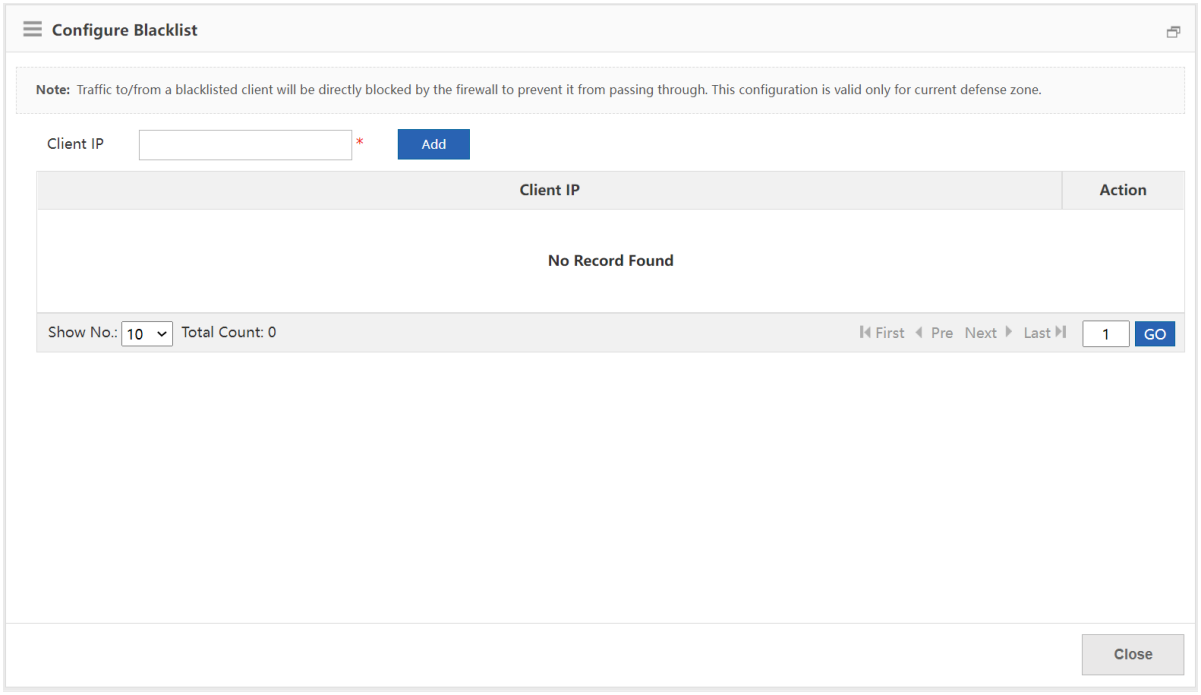
- The whitelist is valid only for this defense zone.
- The whitelist overrides the blacklist. If an IP address is added to a whitelist and a blacklist simultaneously, the whitelist is valid.



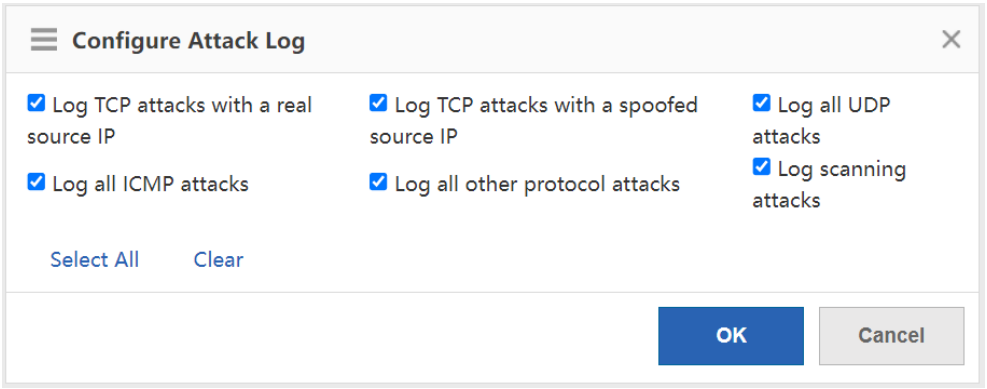
(8) (Optional) For an untrusted source IP address, you can add it to the blacklist. The traffic to or from the blacklisted client will be blocked by the device. Click **Config** of the blacklist to access the **Configure Blacklist** page, enter the client IP address, and click **Add**.

Note

- The blacklist is valid only for this defense zone.
- The whitelist overrides the blacklist. If an IP address is added to a whitelist and a blacklist simultaneously, the whitelist is valid.



(9) (Optional) Click **Config** of the attack log to enable logging and printing of the specified type of policy. Select the log types as required, and click **OK**.



3.12.2 Security Zone Configuration

A security zone is a logical concept that the objects in a security zone have same security requirements, security access control, and border control policies. You can group multiple interfaces or IP addresses with the same security requirements on the device into the same security zone to implement hierarchical management of policies and precise protection. For example, the subnet A is connected to the interface 1 of the router device which belongs to the security zone 1, and the subnet B is connected to the interface 2 of the router device which belongs to the security zone 2. You can only configure the access policy between the security zone 1 and the security zone 2 to perform the access control on the subnet A and the subnet B.

1. Enabling the Security Zone Feature

The security zone feature is used to display and configure the security zone menu. You can enable this feature to view and configure the security zone and related policies.

Procedure

(1) Choose **Firewall** > **Security Zone Config** > **Security Zone Feature**.

(2) Select the security zone feature and click **Save**.

2. Security Zone

The device supports creating a security zone based on the IP address (IPv4 only) or the device interface. You cannot use the two types of security zones simultaneously. The existing security zone and zone policies will be cleared if you switch the creating mode. An interface-based security zone is created by default.

The default access rules between different security zones are as follows.

- The clients or interfaces in the same security zone cannot access each other.
- The security zone of higher priority can access the security zone of lower priority, but not vice versa.

- The security zones of the same priority cannot access each other.

If the zone policy and the global policy are configured, the device will process the packets based on the access control rule of the zone policy and the global policy. Otherwise, the device will process the packets based on the default access policy.

- **Interface-based Security Zone**

After the interfaces are grouped into a security zone, when a packet reaches the device, the device will identify the source interface and the destination interface of the packet, match the interface of the packet with the interface associated with the security zone to determine the source security zone and the destination security zone to which the packet belongs, and then forward or block the packet according to the access policy between security zones or the default access policy.

The default security zone is predefined by the device and cannot be deleted. Interfaces that are not grouped into specified security zones will be assigned to the default security zone.

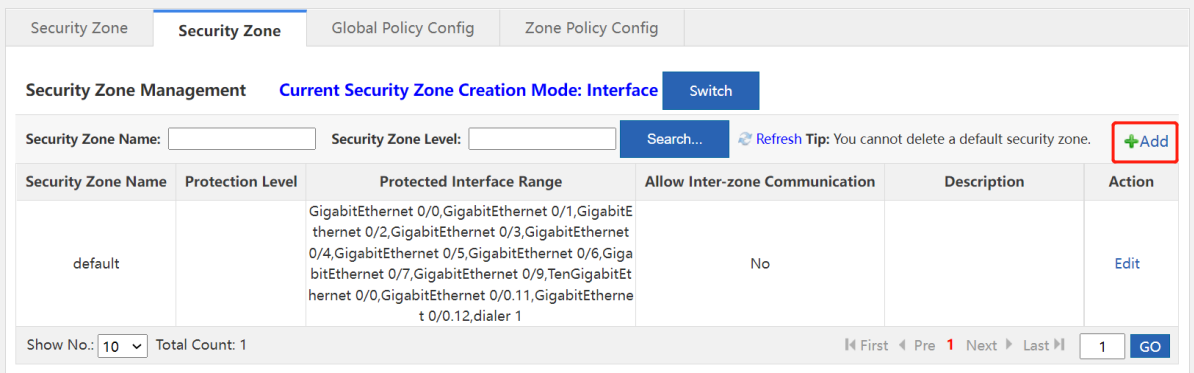
Procedure

(1) Choose **Firewall** > **Security Zone Config** > **Security Zone**.

(2) Click **Add** to access the **Create Interface-based Security Zone** page.

Note

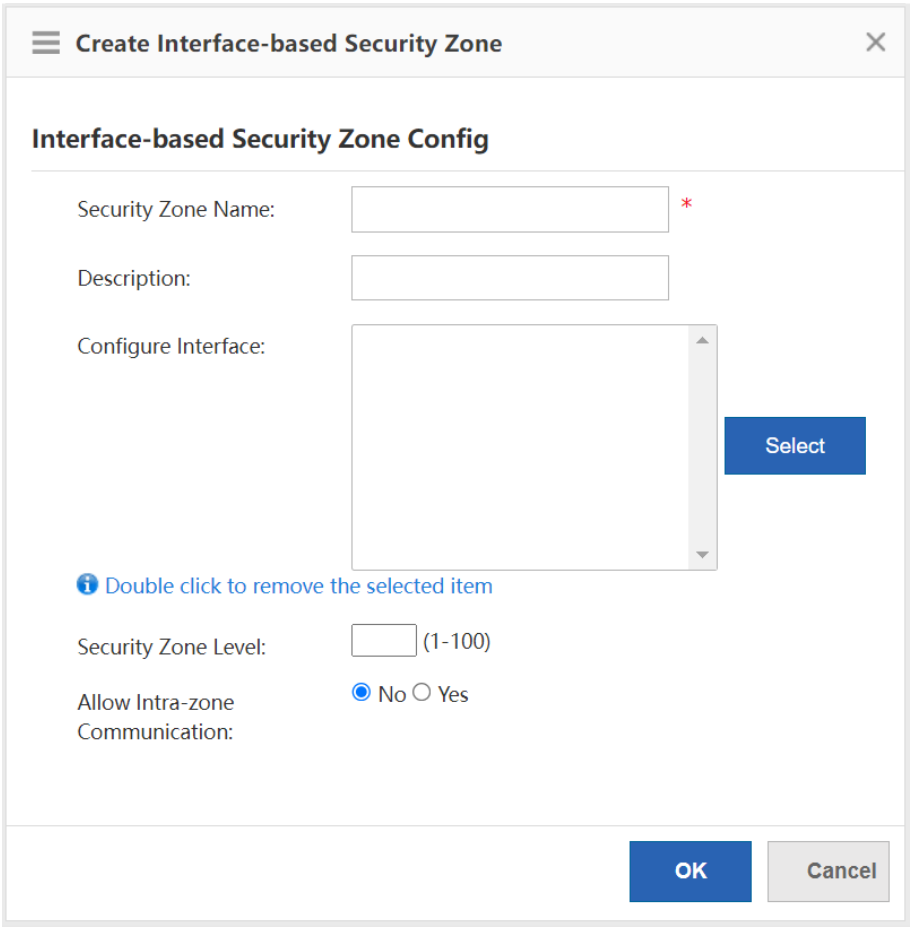
The device will display the page of the interface-based security zone by default. If not, you can click **Switch** to enter the page of the interface-based security zone.



(3) Enter the security zone name and description. Click **Select** to select the interfaces belonging to this security zone. Enter the security zone level, select whether to allow intra-zone communication and click **OK**.

Note

The security zone level is the priority. The higher value indicates higher priority. By default, the security zone with a high priority can access the security zone with a low priority, but not vice versa. The security zones of the same priority cannot access each other.



- **IP-based Security Zone**

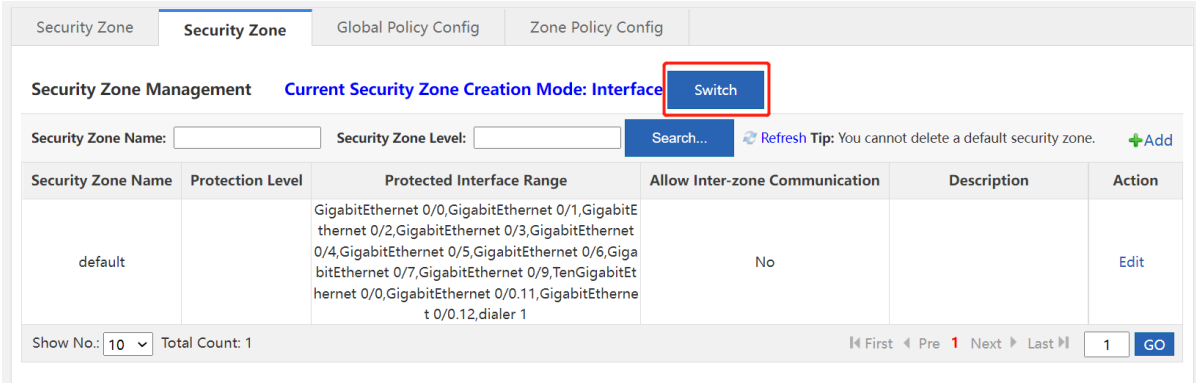
After the IP addresses are grouped into a security zone, when a packet reaches the device, the device will identify the source IP address and the destination IP address of the packet, match the IP address with the ACLs associated with the security zone to determine the source security zone and the designation security zone which the packet belongs to, and then forward or block the packet according to the policy between the security zones or the default access control rule.

The default security zone is predefined by the device and cannot be deleted. IP addresses that are not grouped into specified security zones will be assigned to the default security zone.

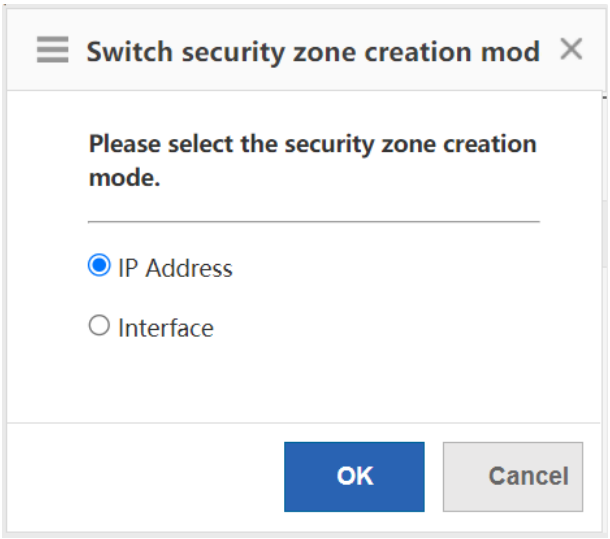
Procedure

(1) Choose **Firewall** > **Security Zone Config** > **Security Zone**.

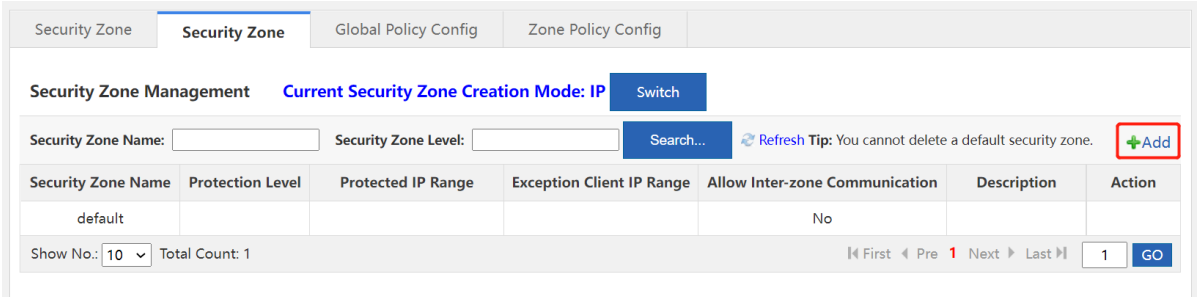
(2) Click Switch to access the Switch Security Zone Creation Mode page.



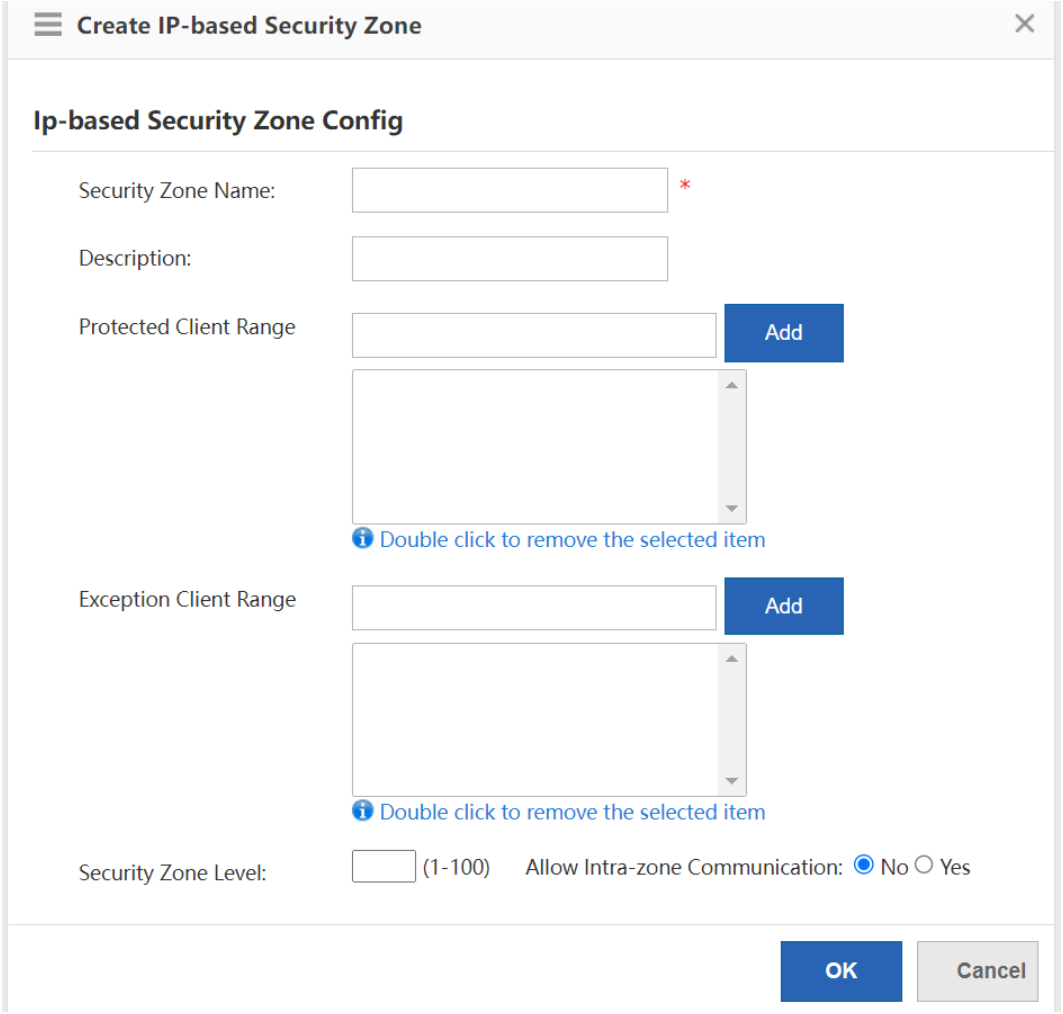
(3) Select **IP Address** and click **OK**.



(4) Click **Add** to access the **Create IP-based Security Zone** page.



(5) Enter the parameters of the IP-based security zone and click **OK**.



Parameter	Description
Security Zone Name	The unique identifier of the security zone.
Description	The description of the security zone
Protected Client Range	Indicate the client IP range of the security zone. You can enter a single IP address (example: 1.1.1.1), a subnet or mask length (example: 1.1.1.0/24), a subnet or mask (example: 1.1.1.0/255.255.255.0) or any. Enter a protected client range and click **Add** to enter another range.
Exception Client Range	Indicate the IP address that does not belong to the security zone. For example, add the subnet 1.1.1.0/24 to a security zone, except for the IP address 1.1.1.1 in this subnet. You can add it to the exception client range.
Security Zone Level	The security zone level is the priority. The higher value indicates higher priority. By default, the security zone of higher priority can access the security zone of lower priority, but not vice versa. The security zones of the same priority cannot access each other.

Parameter	Description
Allow Intra-zone Communication	Select whether the IP addresses in the security zone are allowed for intra-zone communication.

3. Global Policy Configuration

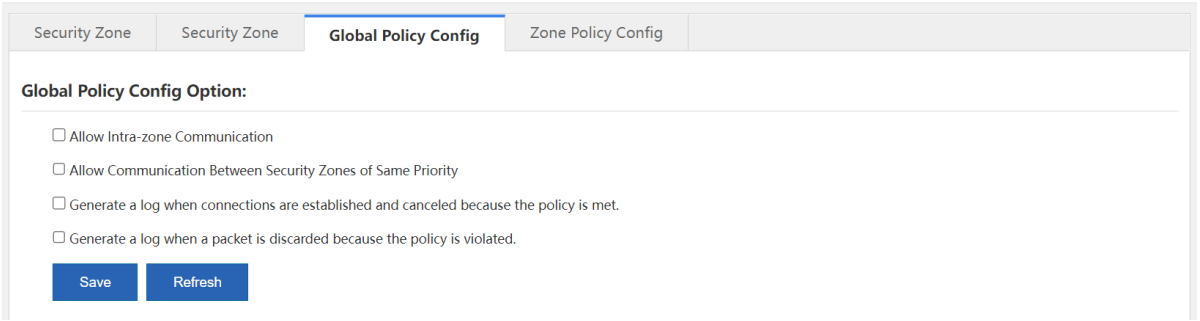
The global access policy is used to control whether to allow the intra-zone communication, whether to allow the communication between security zones of the same priority, whether to generate a log when connections are established and canceled after the security zone policy is matched, and whether to generate a log when the packet is discarded due to the violation of the security zone access policy.

The priority of the global policy is higher than the default access policy.

Procedure

(1) Choose **Firewall** > **Security Zone Config** > **Global Policy Config**.

(2) Select the configuration items as required and click **Save**.



4. Zone Policy Configuration

The zone policy function is used to control whether to allow the inter-domain communication.
After the packet reaches the device, the device will identify the source security zone and the destination security zone to which the packet belongs based on the packet characteristics. If the source security zone is not equal to the destination security zone, it is an inter-domain access, and the packet is forwarded according to the zone policy. If the zone policy is not configured, the packet will be processed according to the global policy or the default access policy. If the source security zone is equal to the destination security zone, it is an intra-domain access, and the packet will be processed according to the security zone configuration.

The zone policy varies with the security zone creation mode. That is, if the creation mode is switched from the interface-based mode to the IP-based mode, the zone policy page will also switch to the IP-based security zone policy configuration page and the existing zone policy will be invalid and deleted, and vice versa.

The priority of the zone policy, the global policy and the default access policy is in a decreasing order.

- **Creating an Interface-based security zone policy**

The interface-based security zone policy is not configured by default.

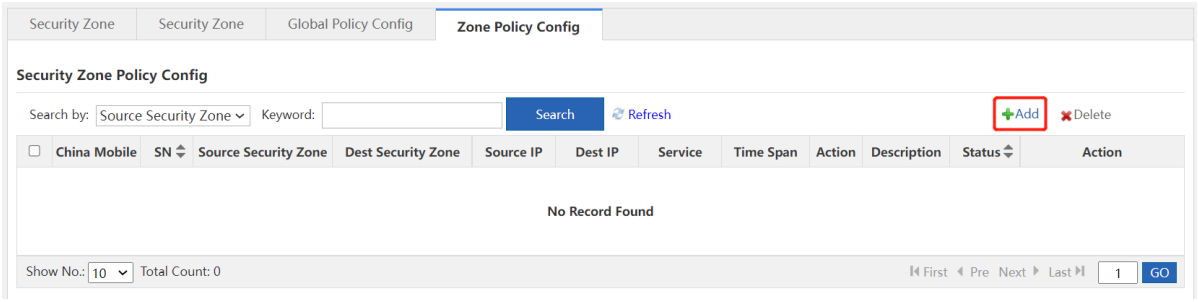
Prerequisite

Select the **Interface** mode for security zone policy configuration.

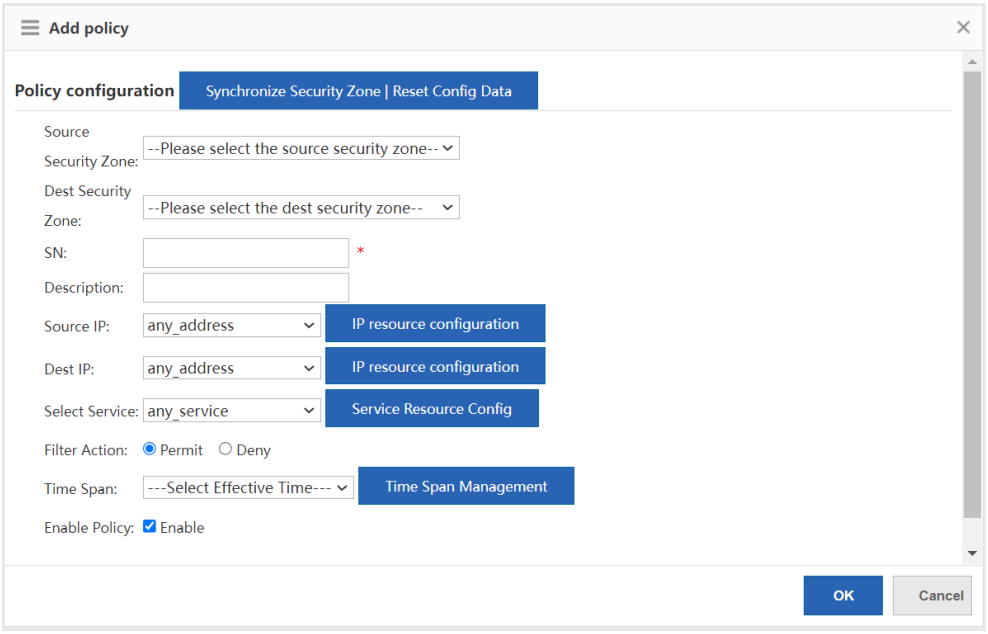
Procedure

(1) Choose **Firewall** > **Security Zone Config** > **Zone Policy Config**.

(2) Click **Add** to access the **Add Policy** page.



(3) Configure the policy parameters according to the following information and click **OK**.



Configuration Item	Parameter
Source Security Zone	Control the access between the designated source security zone and the destination security zone.
Dest Security Zone	Control the access between the designated source security zone and the destination security zone.
SN	Indicate the policy priority. The lower value indicates the higher priority. The policy of higher priority is matched preferentially if multiple zone policies are configured.
Description	The description of the zone policy.
Source IP	Access control for packets from the designated source IP address. Click **IP Resource Configuration** to add a new IP address object. For details, see 1.4 IP Resource Configuration.

Configuration Item	Parameter
Dest IP	Access control for the packets to the designated destination IP address. Click **IP Resource Configuration** to add a new IP address object. For details, see 1.4 IP Resource Configuration.
Select Service	Access control for the packets from the selected service type. Click **Service Resource Configuration** to add a new service object. For details, see 1.5 Service Resource Configuration.
Filter Action	The action executed on the packets matching with the zone policy.
Time Span	The time span in which the policy takes effect.
Enable Policy	Indicate whether to enable the policy. Only an enabled zone policy will match with the packet.

- **Creating an IP-based Security Zone Policy**

The interface-based security zone policy is not configured by default.

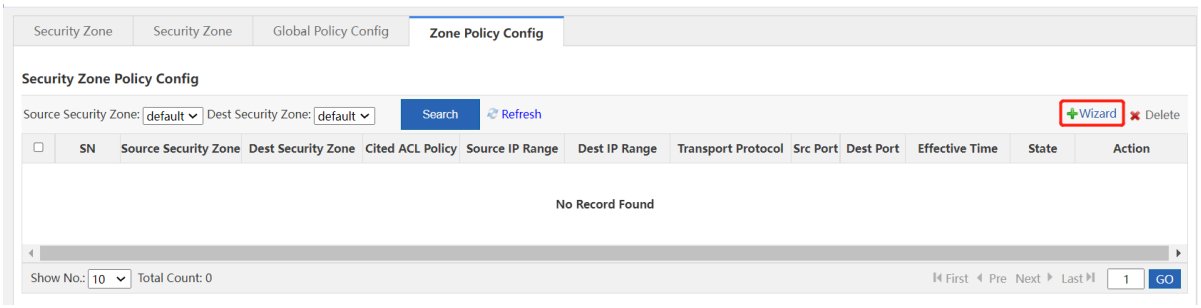
Prerequisite

Select the **IP** mode for security zone policy configuration.

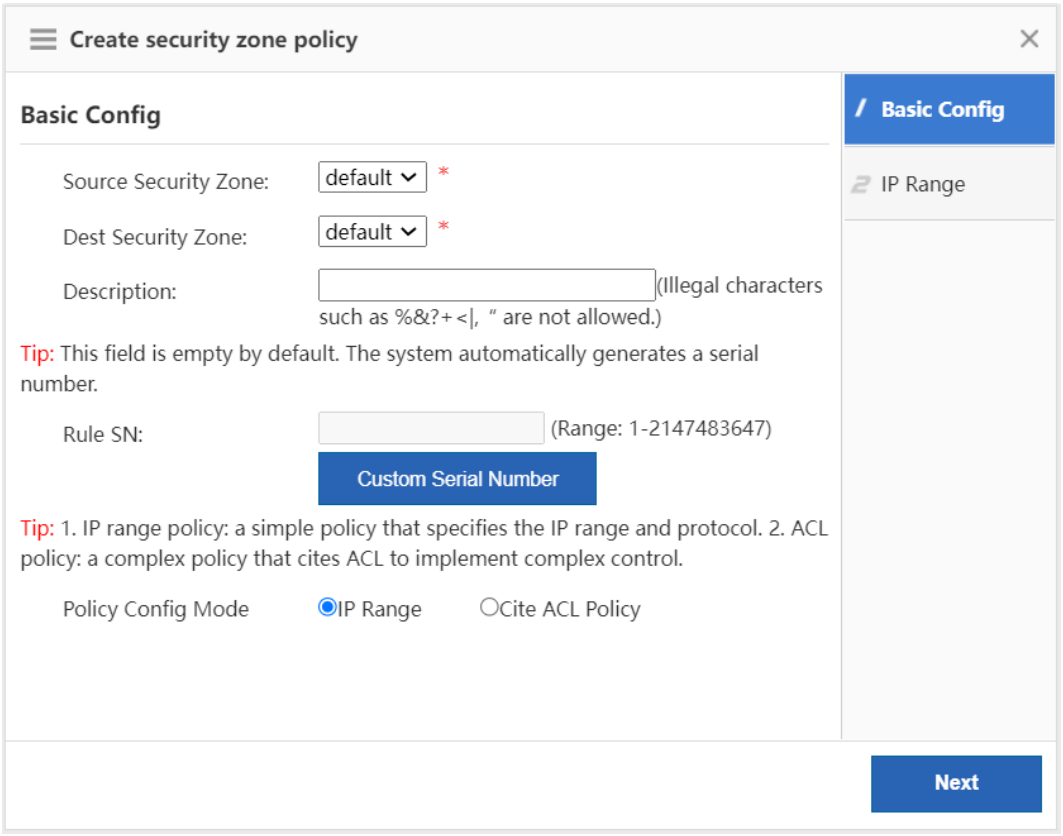
Procedure

(1) Choose **Firewall** > **Security Zone Config** > **Zone Policy Config**.

(2) Click Wizard to access the Create security zone policy page.



(3) Configure the policy parameters according to the following information and click **Next**.

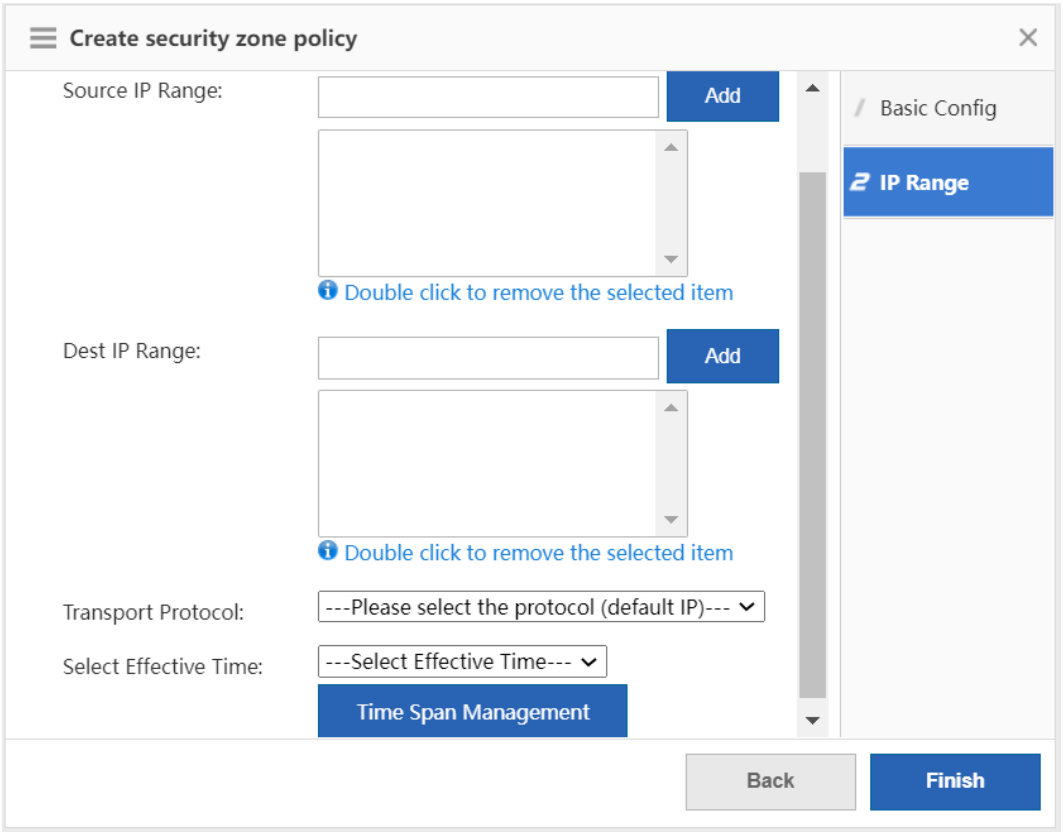


Configuration Item	Parameter
Source Security Zone	Control the access between the designated source security zone and the destination security zone.
Dest Security Zone	Control the access between the designated source security zone and the destination security zone.
Description	The description of the zone policy.
Rule SN	Indicate the policy priority. The lower value stands for the higher priority. The policy of higher priority is matched preferentially if multiple zone policies are configured.
Policy Config Mode	Indicate the mode of matching packets, which supports matching packets based on the IP range or ACL rules.

(4) Configure the IP range according to the following information and click **Finish**. If you select Cite ACL Policy for the policy configuration mode, skip this procedure and move on to next step.

Note

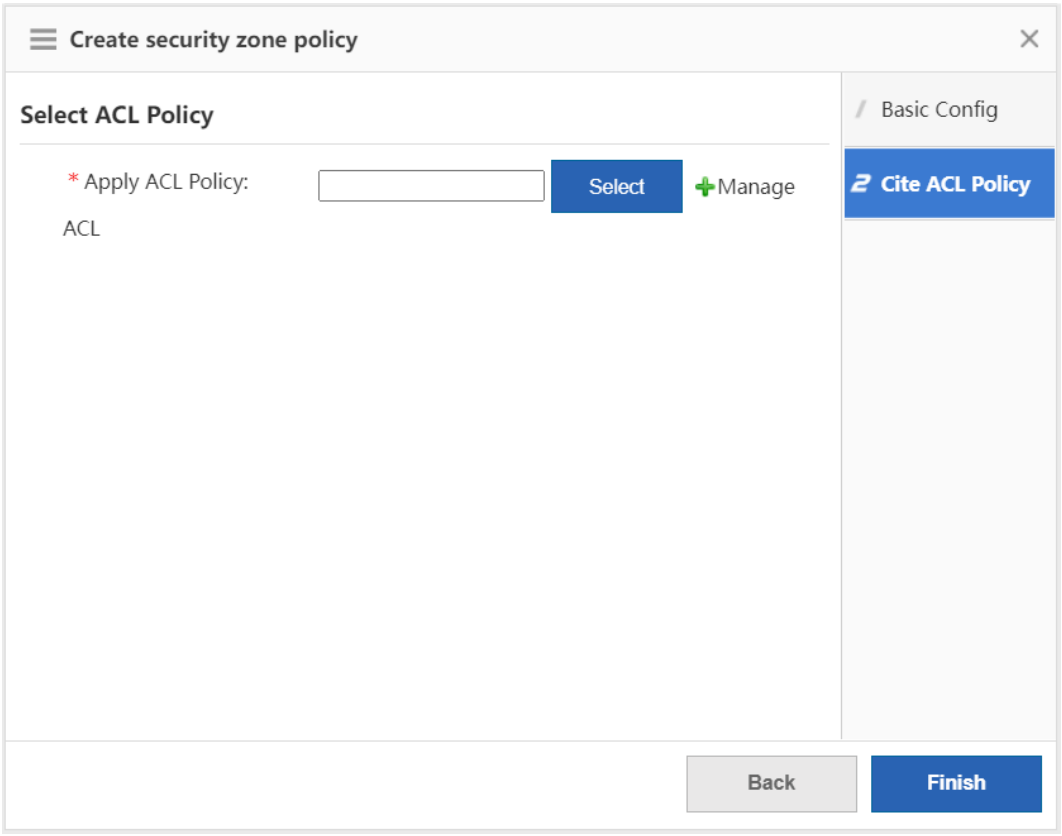
After the IP range is configured, the access is allowed or blocked according to the ACL policy with which the IP range matches.



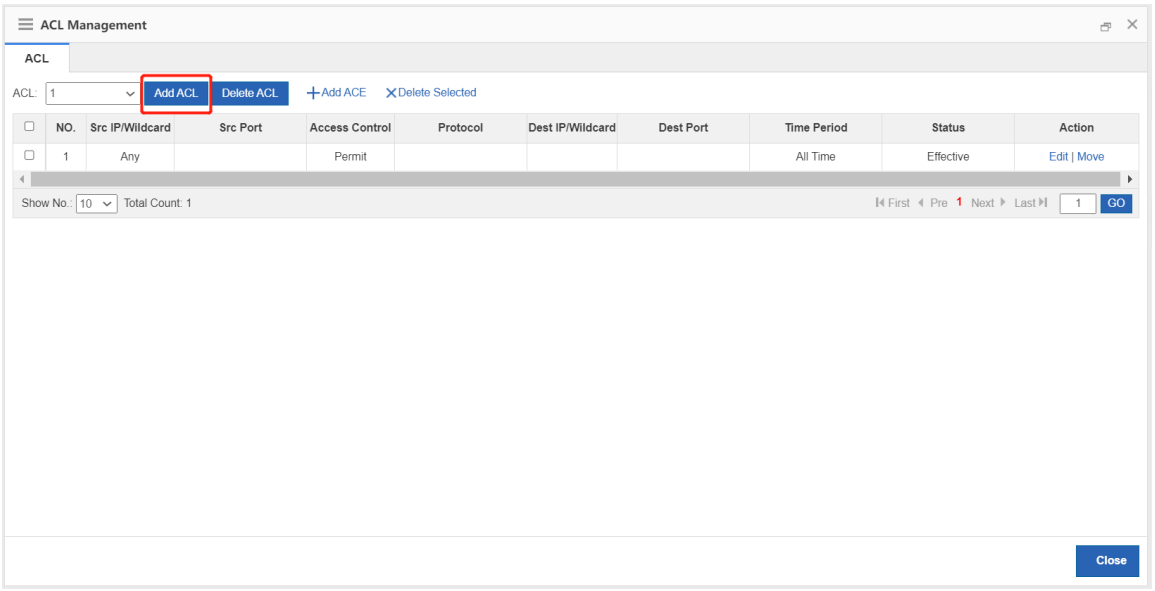
Configuration Item	Parameter
Source IP Range	Access control for the packets from the designated source IP address. You can enter a single IP address (example: 1.1.1.1), a subnet or mask length (example: 1.1.1.0/24), a subnet or mask (example: 1.1.1.0/255.255.255.0) or any. Enter a source IP range and click **Add** to enter another range.
Dest IP Range	Access control for the packets to the designated destination IP address. You can enter a single IP address (example: 1.1.1.1), a subnet or mask length (example: 1.1.1.0/24), a subnet or mask (example: 1.1.1.0/255.255.255.0) or any. Enter a source IP range and click **Add** to enter another range.
Transport Protocol	Access control for the packets of the selected protocol.
Select Effective Time	Indicate the time span in which the policy takes effect. Click **Time Span Management** to select a time span.

(5) Configure the ACL policy according to the following information and click **Finish**. If you select IP Range for the policy configuration mode, skip this procedure.

a Click **Select** to select configured ACL policy. If there is no available ACL policy, click **Manage** to create an ACL policy.

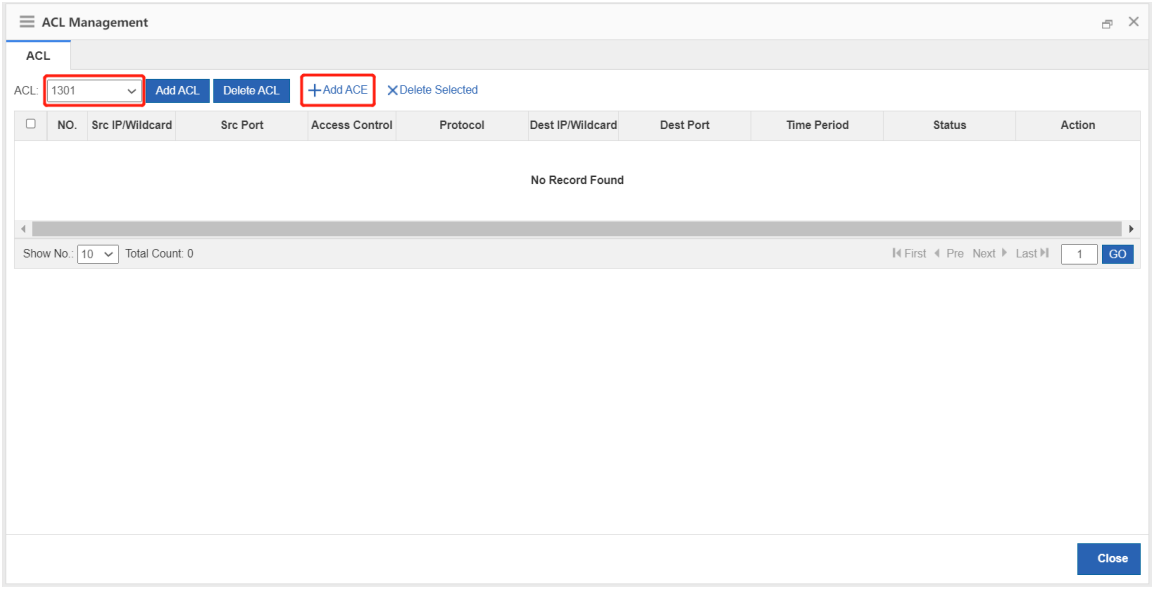


b Click **Add ACL** to access the **Add ACL** page.

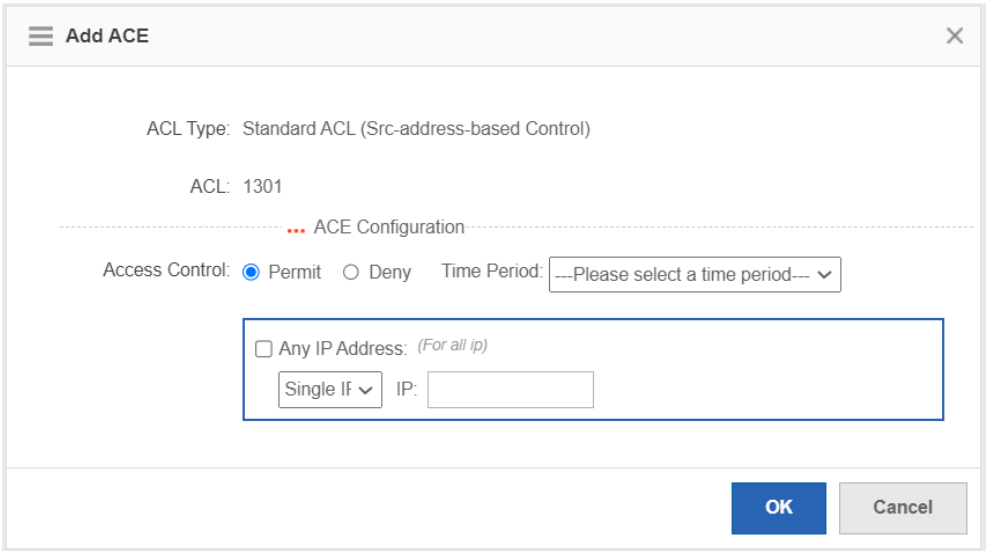


c Select the ACL type, enter the ACL name or the ACL number and click **OK**.

d Select the created ACL and click **Add ACE** to access the **Add ACE** page.

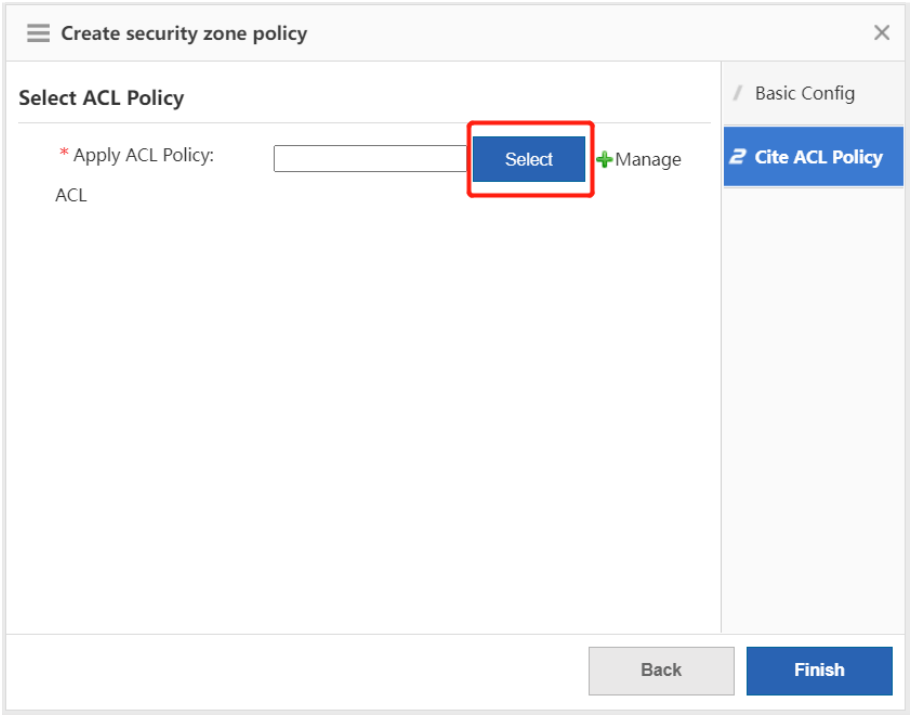


e Configure the ACE according to the following information and click **OK**.

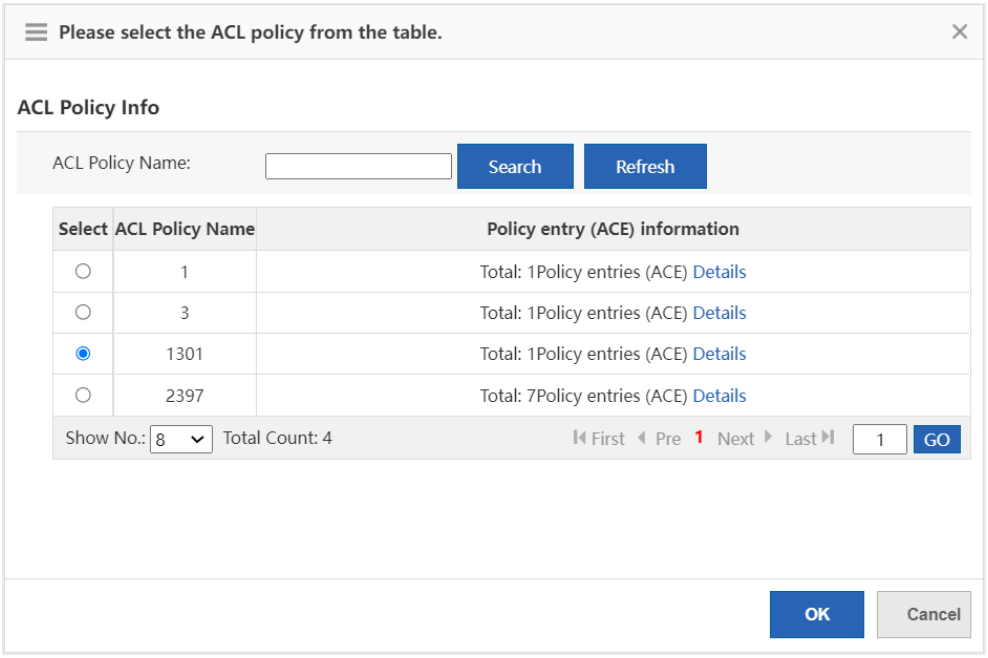


Configuration Item	Parameter
Access Control	Access control for the packets matching the ACE.
Time Period	Indicate the time period in which the ACE takes effect. Click the drop-down list box to select a time period.
IP Address	Access control for the packets from or to the designated IP address. You can enter a single IP address (example: 1.1.1.1), a subnet or mask (example: 1.1.1.0/255.255.255.0) or a wildcard (example: 1.1.1.0/0.0.0.255). If you select **Any IP Address**, the packets from all IP addresses will match the ACE.

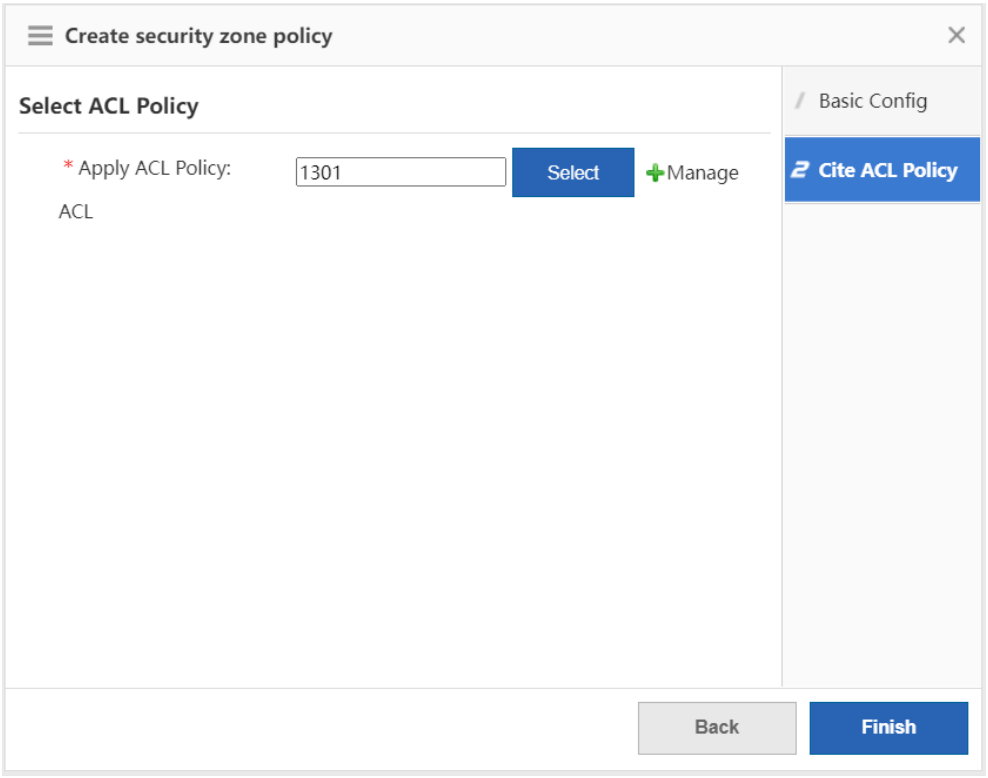
f After the ACE is configured, close the **ACL Management** page. Click **Select** on the **Create security zone policy** page to access the **Please select the ACL policy from the table** page.



g Click **Refresh**, select the created ACL policy and click **OK**.



h Click **Finish**.



3.12.3 Defense Zone Monitoring

1. Zone Running Status

The function is used to display the basic information and traffic statistics of each defense zone.

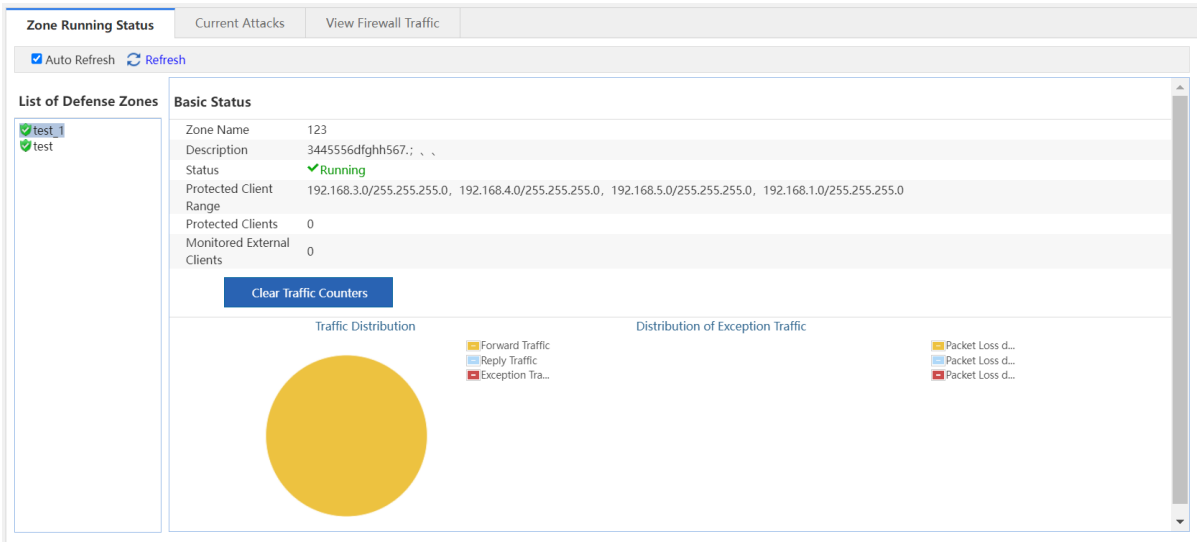
Prerequisite

The defense zone policy is configured. For details, see 1.1.4 Zone Policy.

Procedure

(1) Choose **Firewall** > **Defense Zone Status** > **Zone Running Status**.

(2) Select a defense zone, and its basic information, running status and traffic statistics will be displayed on the right of the page.



2. Current Attacks

The function is used to display the current attacks in each defense zone, and filter the attack information based on attack types or protocol types.

Prerequisite

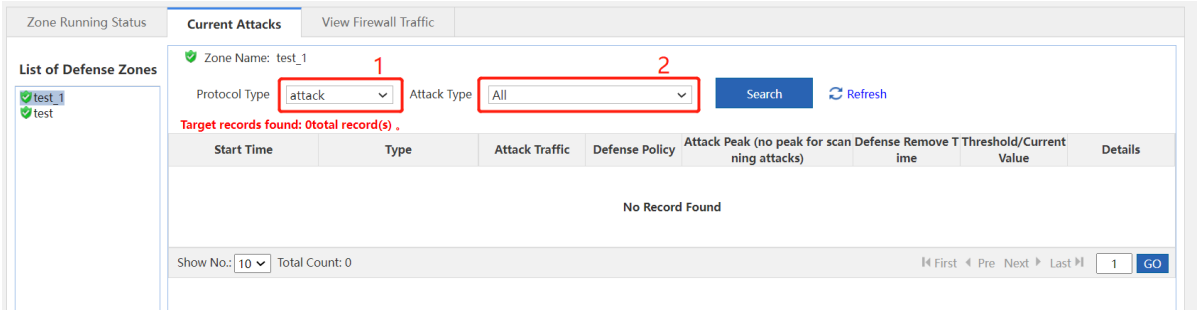
The defense zone policy is configured. For details, see 1.1.4 Zone Policy.

Procedure

(1) Choose **Firewall** > **Defense Zone Status** > **Current Attacks**.

(2) Select a defense zone. By default, the current attacks in the selected defense zone will be displayed by attack types on the right of the page.

(3) (Optional) Click the drop-down list box of **Protocol Type** and select another protocol. Click **Search** to display the attack information based on protocol types.



3. Viewing Firewall Traffic

The function is used to display global defense information.

Prerequisite

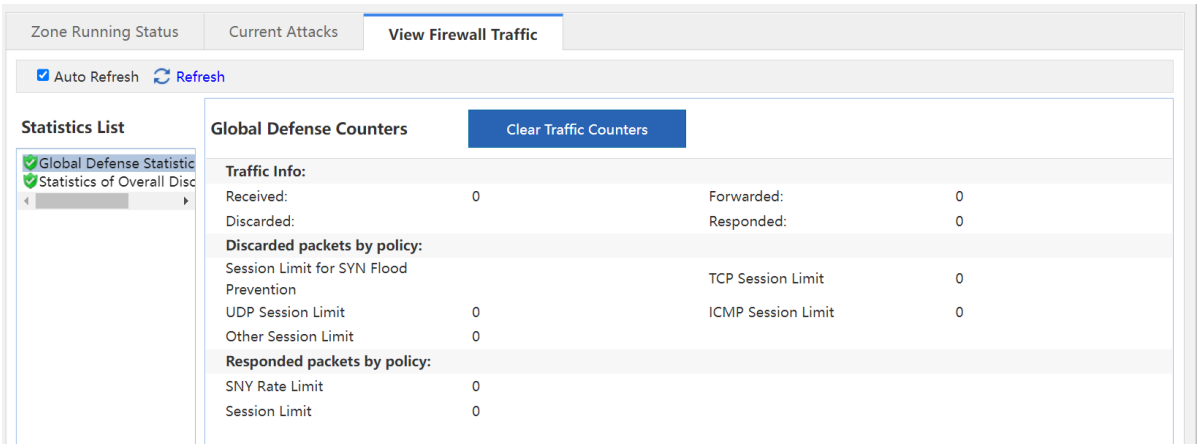
Global defense is configured. For details, see 1.1.2 Global Defense.

Procedure

(1) Choose **Firewall** > **Defense Zone Status** > **View Firewall Traffic**.

(2) Click **Global Defense Statistics** to view defense traffic statistics.

(3) Click **Statistics of Overall Discarded Packets** to view the statistics of the discarded packets based on the defense policy.



3.12.4 IP Resource Configuration

The IP resource function must work with other functions instead of working independently. For example, when configuring the inter-domain policy, you can implement access control on the packets of the designated source IP address in the source security zone.

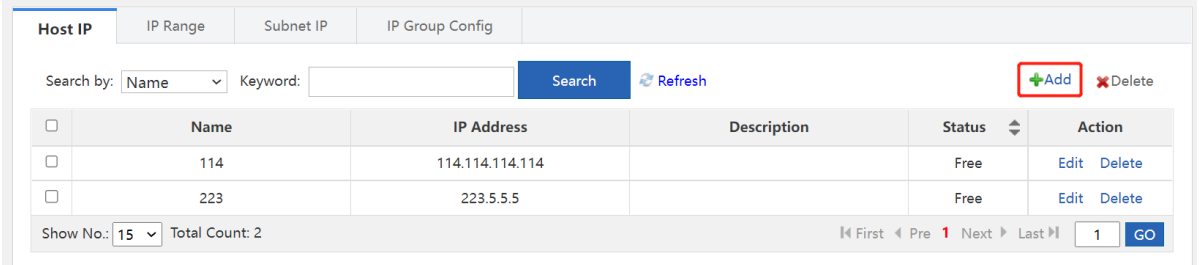
1. Host IP Address

The host IP address is a single IP address. The administrator can configure a proper name for a single IP address to identify the device with the IP address quickly.

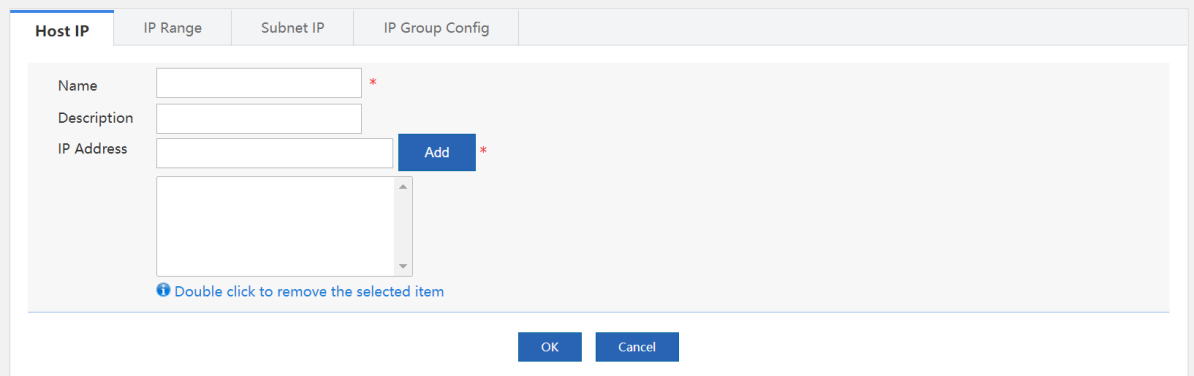
Procedure

(1) Choose **Firewall** > **IP Resource** > **Host IP**.

(2) Click **Add**.



(3) Enter the name, description and the IP address, and click **Add**. If you need multiple IP addresses, you can enter other IP addresses and click **Add**.



(4) Click **OK**.

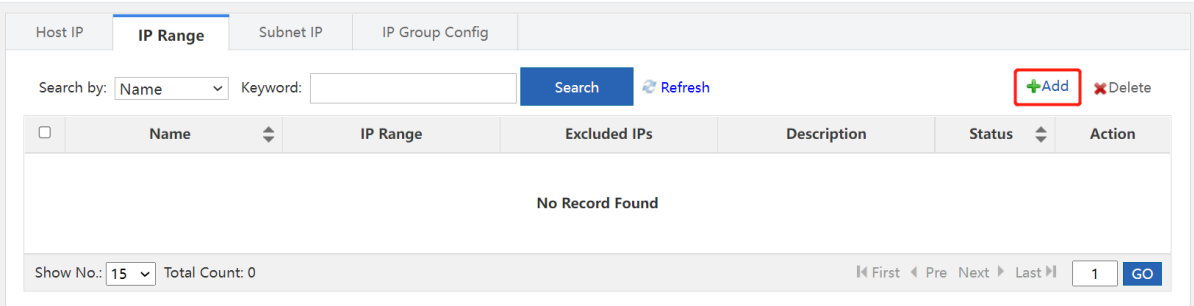
2. IP Range

IP range indicates a range of multiple IP addresses, such as 1.1.1.1 to 1.1.1.10. The administrator can configure a proper name for an IP range to identify the device with the IP address within the range quickly.

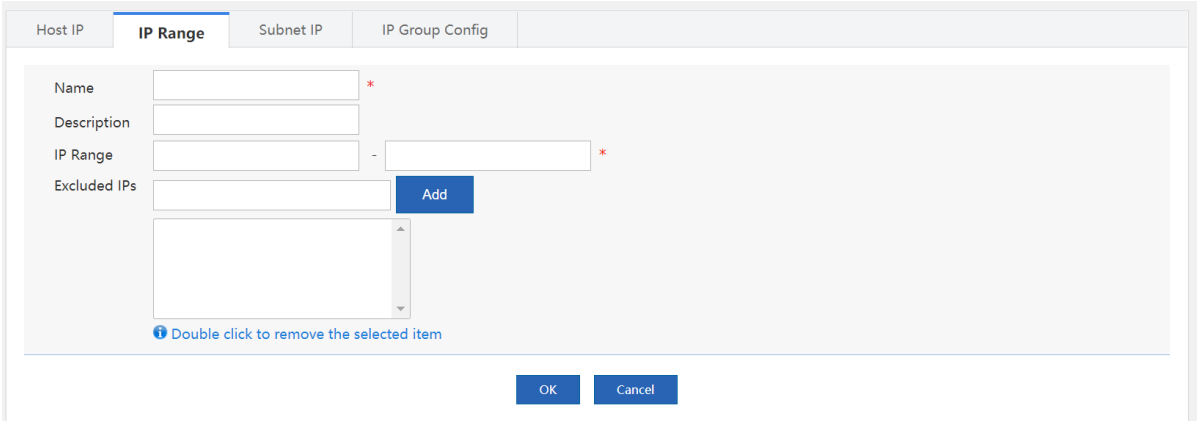
Procedure

(1) Choose **Firewall** > **IP Resource** > **IP Range**.

(2) Click **Add**.



(3) Enter the name, description and the IP range. If there is an excluded IP address, enter the excluded IP address (only a single IP address is supported.) and click **Add**. If you need to add multiple excluded IP addresses, enter other excluded IP addresses and click **Add**.



(4) Click **OK**.

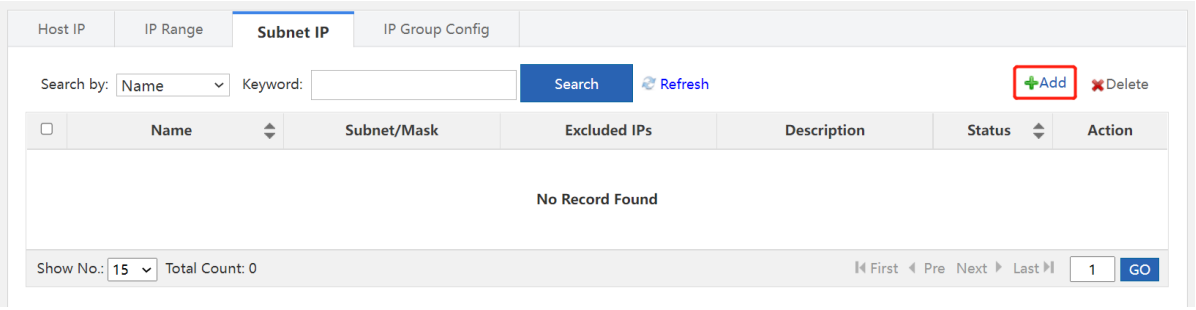
3. Subnet IP Address

For example, 1.1.1.0/255.255.255.0 is a subnet IP address. The administrator can configure a proper name for a subnet IP address to identify the subnet quickly.

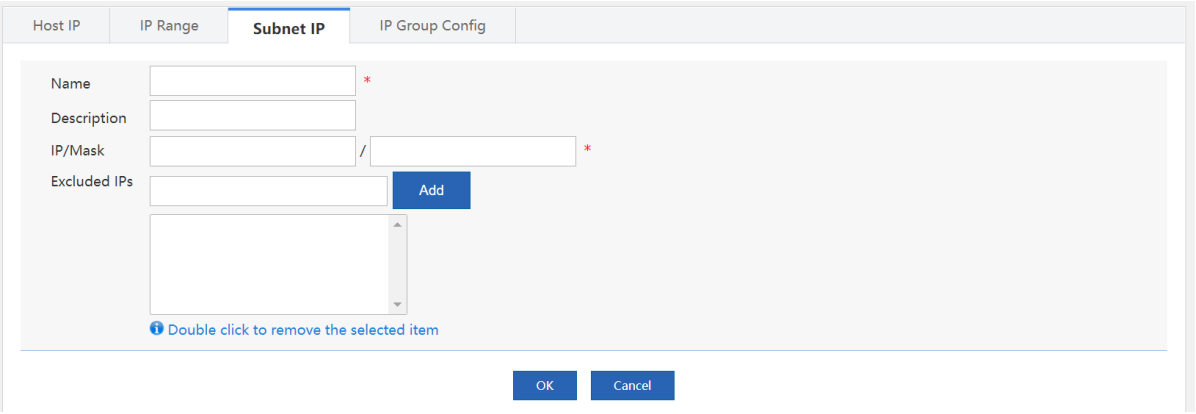
Procedure

(1) Choose **Firewall** > **IP Resource** > **Subnet IP**.

(2) Click **Add**.



(3) Enter the name, description, the IP address or the mask. If there is an excluded IP address, enter the excluded IP address (only a single IP address is supported.) and click **Add**. If you need to add multiple excluded IP addresses, enter other excluded IP addresses and click **Add**.



(4) Click **OK**.

4. IP Group Configuration

An IP group is a collection of multiple IP addresses. You can put the host IP address, the IP range or the subnet IP address with the same defense requirements into an IP group for convenient management.

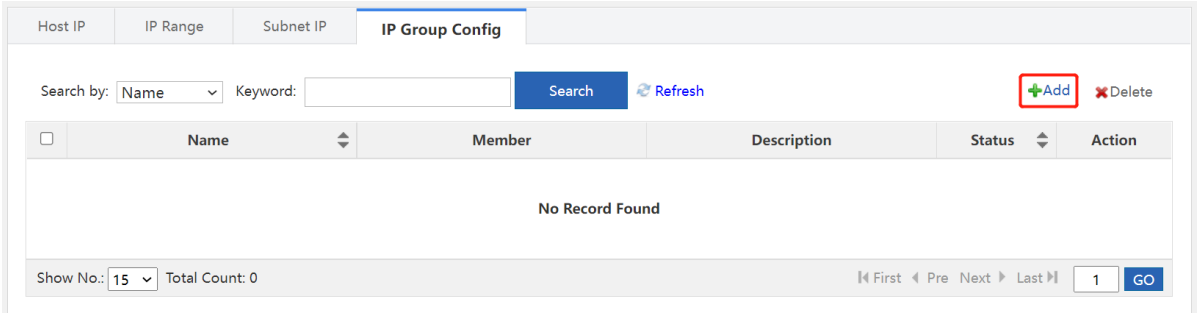
Prerequisite

The host IP address, the IP range or the subnet IP address are configured.

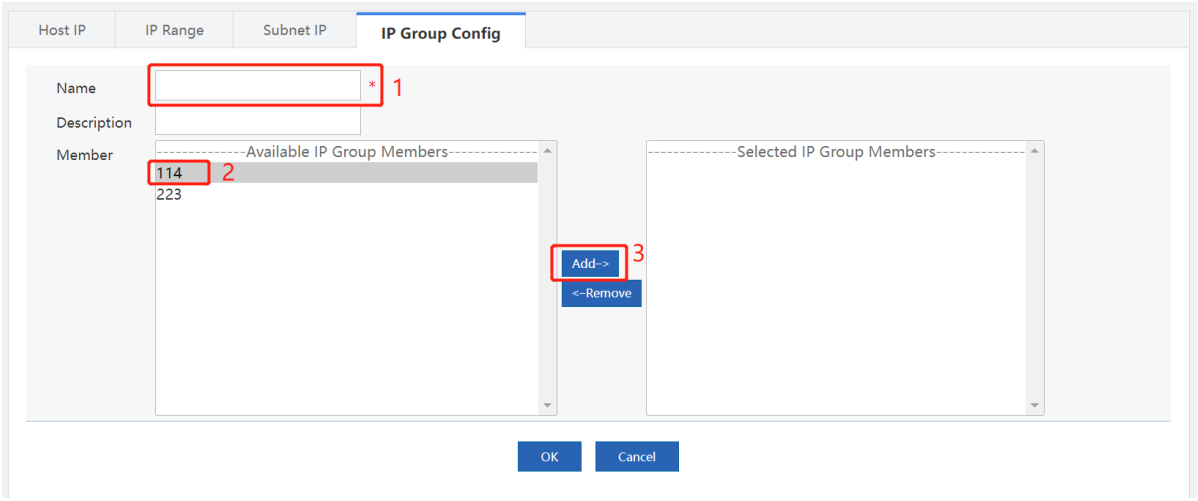
Procedure

(1) Choose **Firewall** > **IP Resource** > **IP Group Config**.

(2) Click **Add**.



(3) Enter the name and description, select the members of the IP group as required, and click **Add**.



(4) Click **OK**.

3.12.5 Service Resource Configuration

The service resource is represented by protocol types and features. Protocol features are used to match the upper layer protocols carried in the packets, such as the source port and the destination port of TCP and UDP, the ICMP message type or message authentication code.

The service resource does not work independently but works with other functions. For example, you can implement access control on the packets of a specified service when configuring the inter-security zone policies.

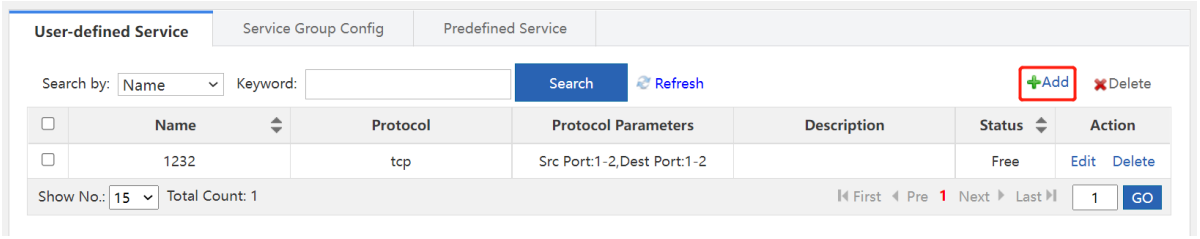
1. Customer Service

The device predefines common services. You can view the services on the **Predefined Service** page. If the predefined services do not include the required service, you can configure the service resource by yourself.

Procedure

(1) Choose **Firewall** > **Service Resource** > **User-defined Service**.

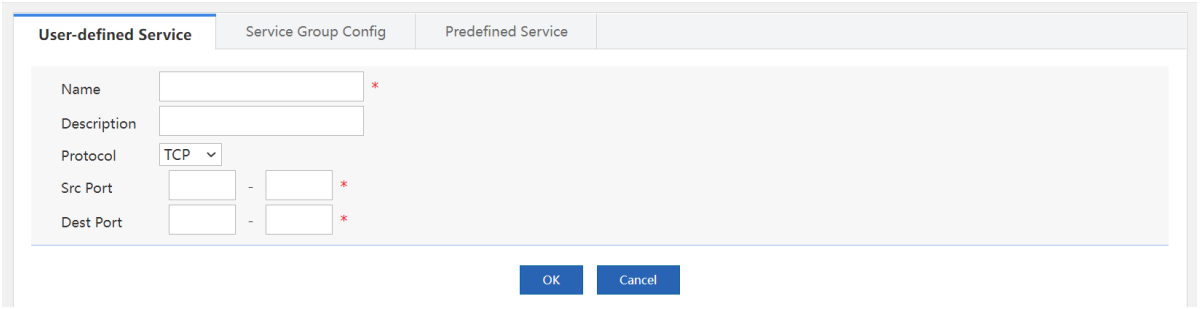
(2) Click **Add**.



(3) Enter the name and description. Select the protocol, configure the parameters of the protocol and click **OK**.

Note

The parameters may vary with the protocols. The parameters displayed on the webpage prevails.



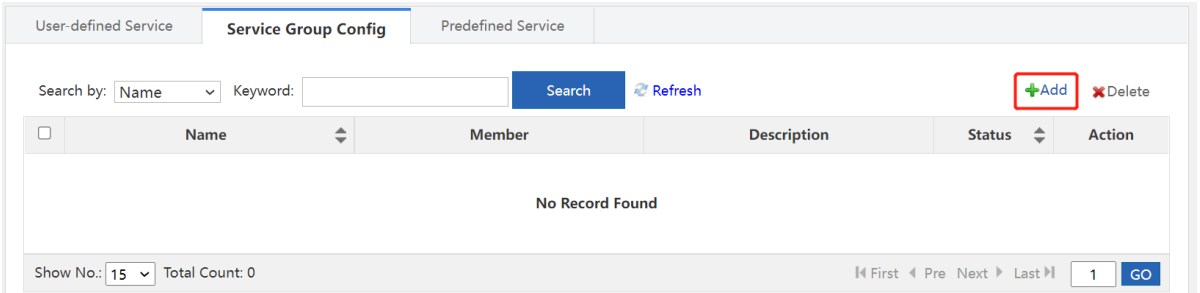
2. Service Group Configuration

A service group is a collection of multiple services. You can add the custom or predefined services with the same defense requirements to a group for convenient management.

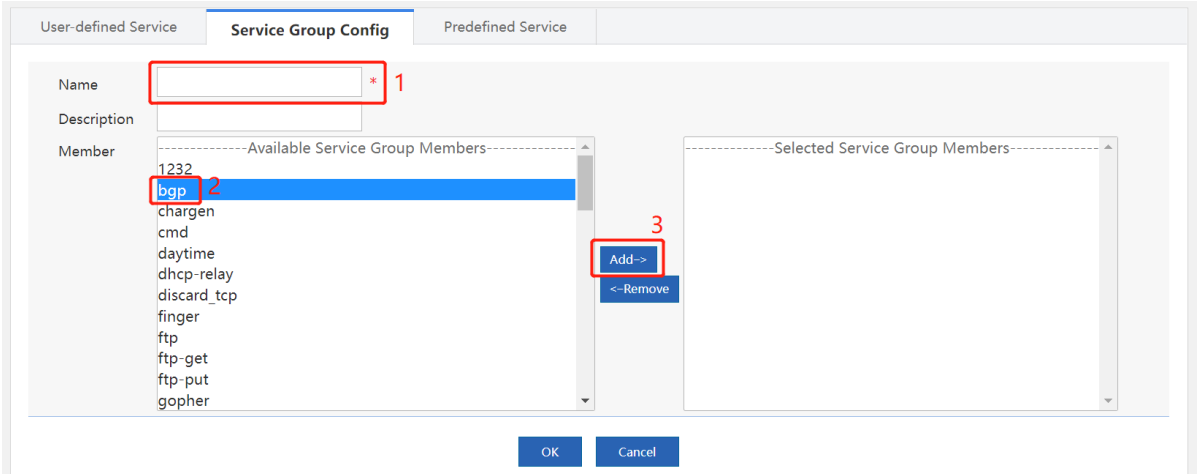
Procedure

(1) Choose **Firewall** > **Service Resource** > **Service Group Config**.

(2) Click **Add**.



(3) Enter the name and description. Select service group members as required and click **Add**.



(4) Click **OK**.

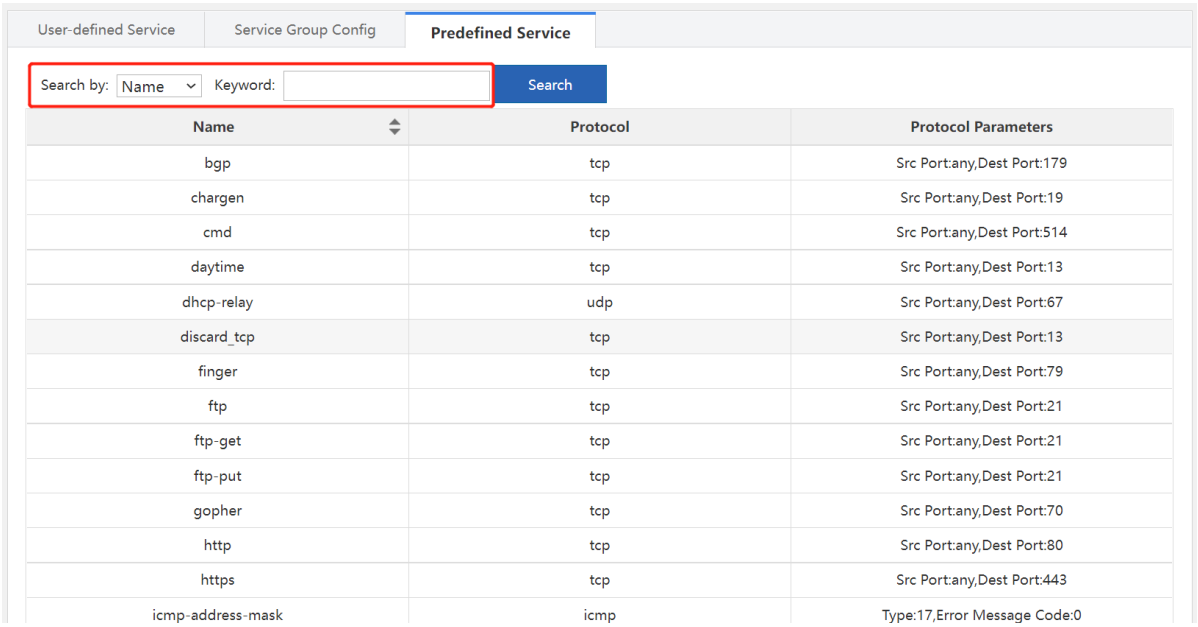
3. Predefined Service

The function is used to display predefined services.

Procedure

(1) Choose **Firewall** > **Service Resource** > **Predefined Service**.

(2) (Optional) Select a query item or enter a keyword and click **Search** to search for the service information you need.



Name	Protocol	Protocol Parameters
bgp	tcp	Src Port:any,Dest Port:179
chargen	tcp	Src Port:any,Dest Port:19
cmd	tcp	Src Port:any,Dest Port:514
daytime	tcp	Src Port:any,Dest Port:13
dhcp-relay	udp	Src Port:any,Dest Port:67
discard_tcp	tcp	Src Port:any,Dest Port:13
finger	tcp	Src Port:any,Dest Port:79
ftp	tcp	Src Port:any,Dest Port:21
ftp-get	tcp	Src Port:any,Dest Port:21
ftp-put	tcp	Src Port:any,Dest Port:21
gopher	tcp	Src Port:any,Dest Port:70
http	tcp	Src Port:any,Dest Port:80
https	tcp	Src Port:any,Dest Port:443
icmp-address-mask	icmp	Type:17,Error Message Code:0

4 Upgrade and Maintenance

4.1 Logging In

4.1.1 Logging In Through the Web Management System

The web management system provides a visualized graphical management interface, which is friendly, easy to use, and can achieve efficient configuration and management.

Configuration Environment Requirements

The client (PC or mobile terminal) used for logging in to the web management system must meet the following environmental requirements:

- Browser: Google Chrome, Internet Explorer 9.0, Internet Explorer 10.0, Internet Explorer 11.0, and some Google/Internet Explorer kernel-based browsers, for example, 360 Security Browser (recommended mode: Extreme) are supported. If you log in to the web management system using other browsers, exceptions such as garbled characters or formatting errors may occur.
- Resolution: The recommended resolution specifications are 1024 x 768, 1280 x 1024, 1440 x 960, and 1600 x 900. If other resolutions are used, the fonts and formats may be out of alignment.

Key Points

There are two ways to access the web management system depending on the access interface:

- LAN access: Access the web management system through the default IP address of the router's LAN port. In this case, the management PC must be on the same LAN as the router.
- WAN access: Access the web management system through the IP address of the router's WAN port. In this situation, ensure that the device can access the Internet and the WAN IP is a public IP address.

Note

- Both LAN access and WAN access require connectivity between the management PC and the router interfaces' IP address, that is, the management PC can ping the IP address of the router’s interface.
- If the router is configured for the first time, you are advised to access the web management system through LAN access.

1. LAN access

Prerequisites

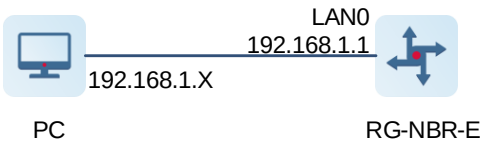
Table 4-1 lists the default web configuration of RG-NBR-E series routers. The router starts the web service by default, and you can use the default value to log in to the web management system.

Table 4-1 Default web configurations

Item	Default Setting
Device IP address (management IP address)	● The default IP address of device LAN0 (Gi0/0) port is 192.168.1.1 ● After the router is configured initially or restores to factory defaults, the default management IP address is 192.168.1.1. ● If HTTPS is enabled, the initial management IP address is 192.168.1.1:4430.

Item	Default Setting
User name/Password	admin/admin

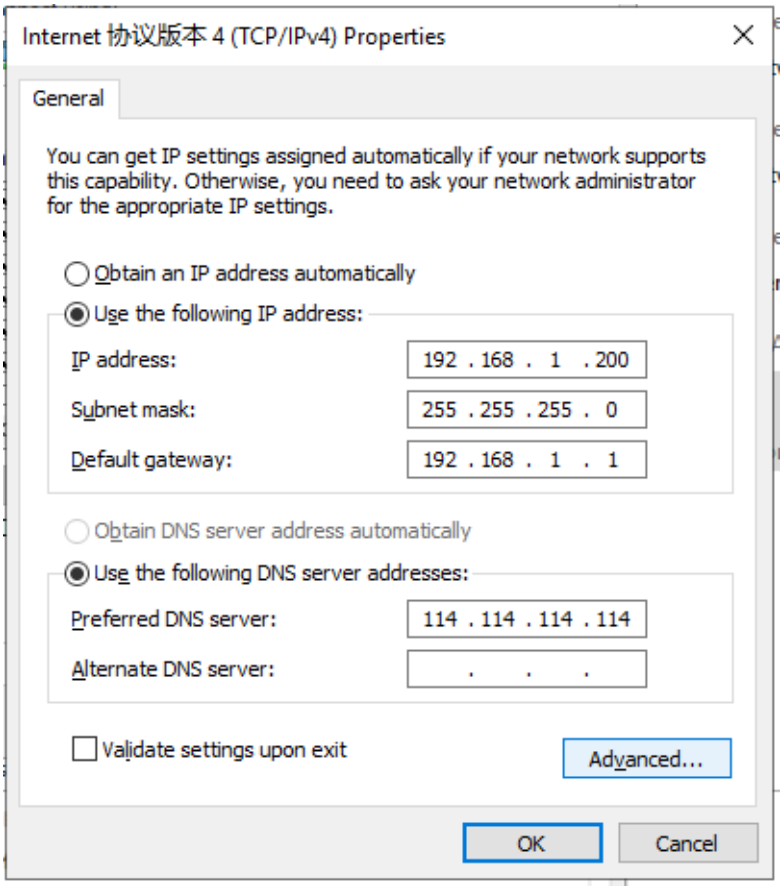
Figure 4-1 Topology through LAN access



Procedure

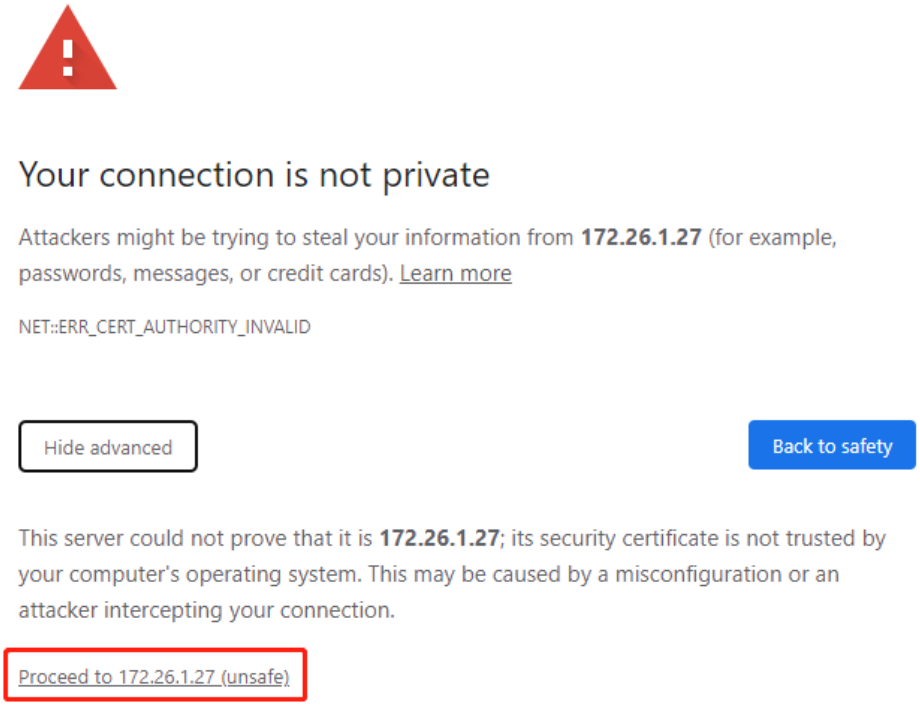
(1) Connect the LAN0 (Gi0/0) port of the router to the management PC using an Ethernet cable.

(2) Configure an IP address in the same network segment as the router's LAN0 (Gi0/0) interface IP so that the management PC can access the router. For example, set the IP address of the management PC to 192.168.1.200, the subnet mask to 255.255.255.0, and the default router to 192.168.1.1.



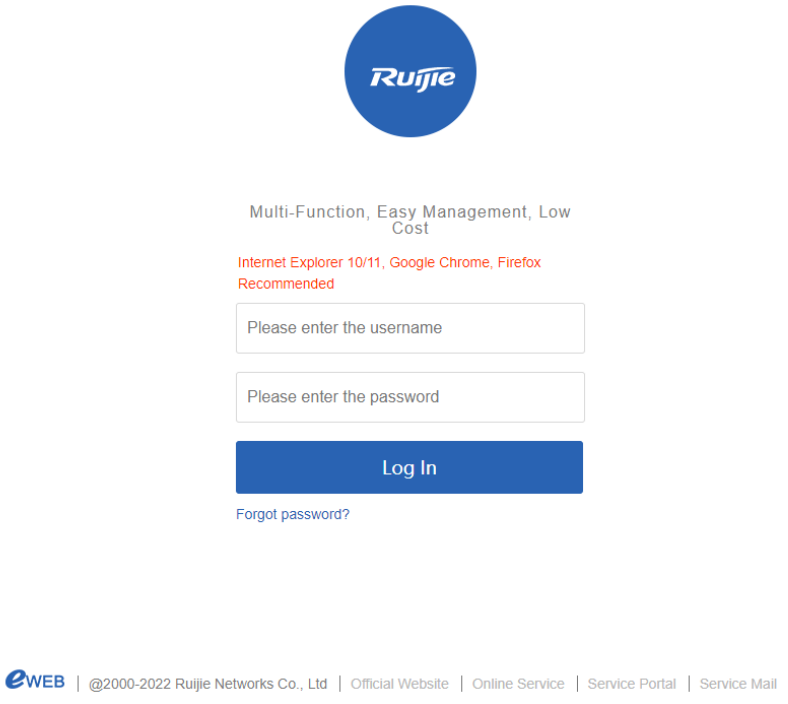
(3) Open a browser, enter **http://192.168.1.1** or **https://192.168.1.1:4430**, and press **Enter**. The login page is displayed.

A certificate security problem may be displayed when you log in through HTTPS. Ignore it and proceed.



Note

- If the IP address of LAN0 (Gi0/0) port is modified, the URL for web access will be changed to http://X.X.X.X or https://X.X.X.X:4430, where X.X.X.X is the new IP address.
- If the web access port of the device is modified to a port other than port 80, the URL for web access must be added with a port number. For example, if the port number for web access is changed to 9999, the URL for web access will be changed to http://X.X.X.X:9999, where X.X.X.X is the IP address of the port.



(4) After entering the user name and password, click **Log In** to enter the homepage of the web management system. The default user name and password are **admin**.

Note

If you forget your user name or password, handle this problem by referring to 4.2 Configuring a Password.

2. WAN access

Prerequisites

- Confirm that the router can access the Internet, and the IP address of the WAN port is a public IP address.
- The management PC can ping the IP address of the WAN port of the router.

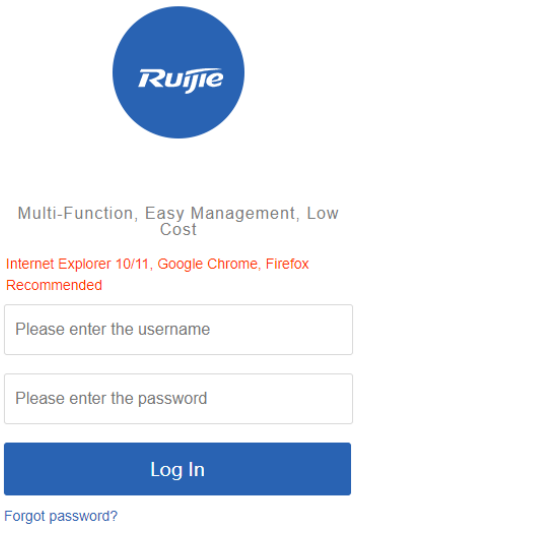
Procedure

(1) Open the browser and type in the IP address of the WAN port of the device, which is http://X.X.X.X or https://X.X.X.X:4430, where X.X.X.X is the IP address of the WAN port of the router.

Note

- If you cannot log in using HTTP, the reason is that the ISP may be attacked or port 80 may be blocked. It is recommended that HTTPS be used for WAN access. This is because HTTPS is an encryption protocol, and the ISP is unlikely to be attacked or block port 80.
- If the port for web access on the router is changed to a port other than port 80, the URL for web access must be added with a port number. For example, if you change the port number for web access to 9999, the web access address will be changed to http://X.X.X.X:9999, where X.X.X.X is the IP address of the WAN port.
- The certificate security problem may occur when you log in through HTTPS. Ignore it and proceed.

(2) On the login page, enter the user name and password and click **Login** to enter the home page of the web management system. The default user name and password are **admin**.



4.1.2 Logging In Through the Console Port

Application Scenario

To enter the CLI for configuration management, you can connect the console port (configuration port) of the router using a console cable, and enter the CLI using software such as HyperTerminal or SecureCRT. The RG-NBR-E series router allows management through the console port by default.

Tools

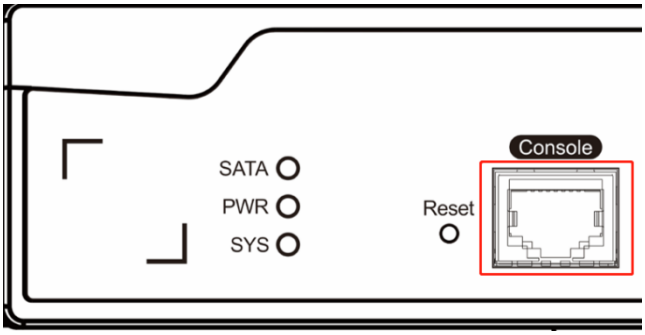
- PC with COM port: The COM port on the PC is usually behind the chassis near the monitor interface. There are nine pins on the interface, as shown in Figure 4-2. For a terminal without a COM port (such as a laptop), prepare a COM-to-USB cable or use a Type 2 console cable.

Figure 4-2 COM port

Figure 4-3 COM-to-USB cable

- Console port: a console port is an interface marked with "Console" on the front panel of the device.

Figure 4-4 Console port on the device



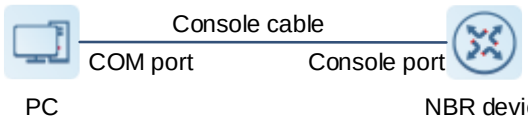
- Console cable
  - Type 1: One end of the cable is a 9-pin COM port, and the other end is an RJ45 connector.

  - Type 2: One end of the cable is an RJ45 connector, and the other end is a USB connector.

- Install SecureCRT or other terminal emulators on the management PC.

Procedure

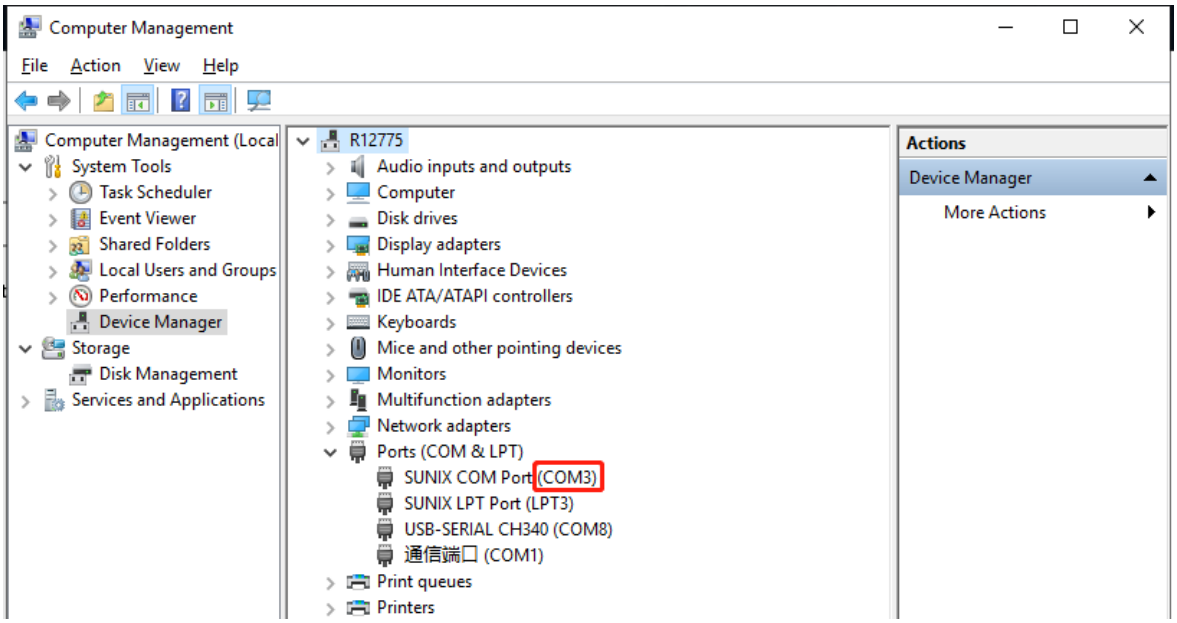
Figure 4-5 Cable connection diagram



(1) Connect the COM port of the management PC and the console port of the router with a console cable.

(2) Check the identified COM port on the management PC.

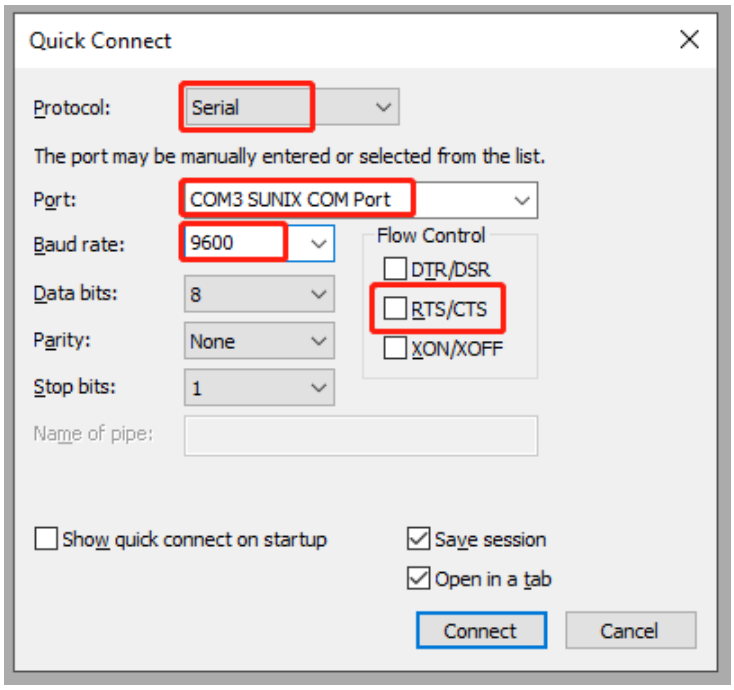
Right-click **This PC** > **Manage** > **Device Manager** to view "Ports (COM&LPT)".



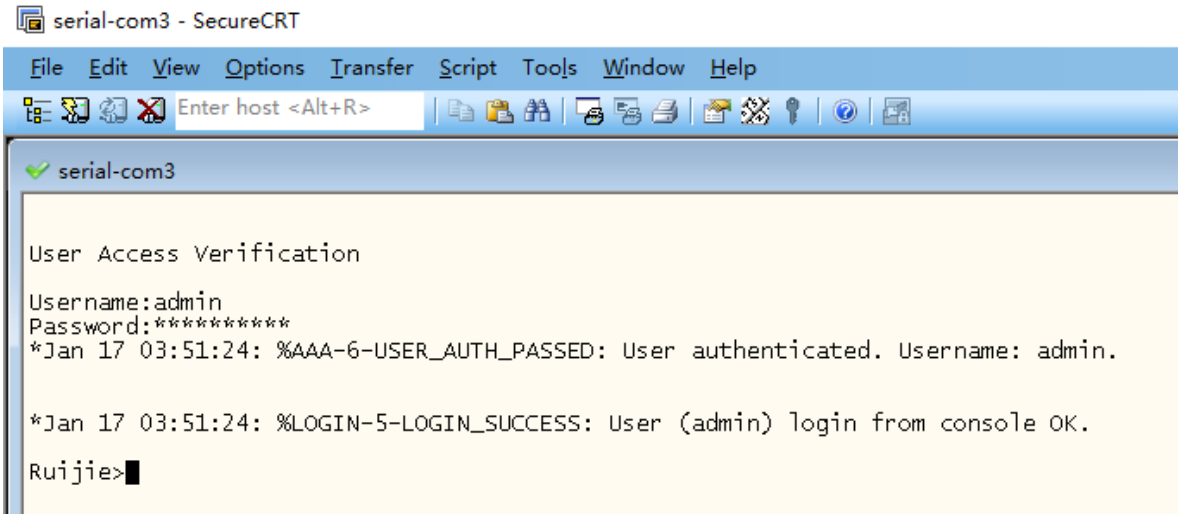
(3) Run the terminal emulator. SecureCRT is used as an example. For other programs, see corresponding instruction manuals.

Open the SecureCRT software. A quick connection window will be displayed. If the window is not displayed, click  . Set connection parameters, and click **Connect**. The following table lists connection parameters.

Connection Parameter	Parameter Value
Protocol	Serial
Port	COM port identified by the PC in the previous step
Baud rate	9600
RTC/CTS	Uncheck



(4) Enter the device CLI page. Press **Enter** and enter the user name and password (**admin/admin** by default) as prompted. If you have changed the user name and password and forget the new user name and password, recover the user name and password by referring to 4.2 Configuring a Password.



4.1.3 Logging In Through Telnet

Application Scenario

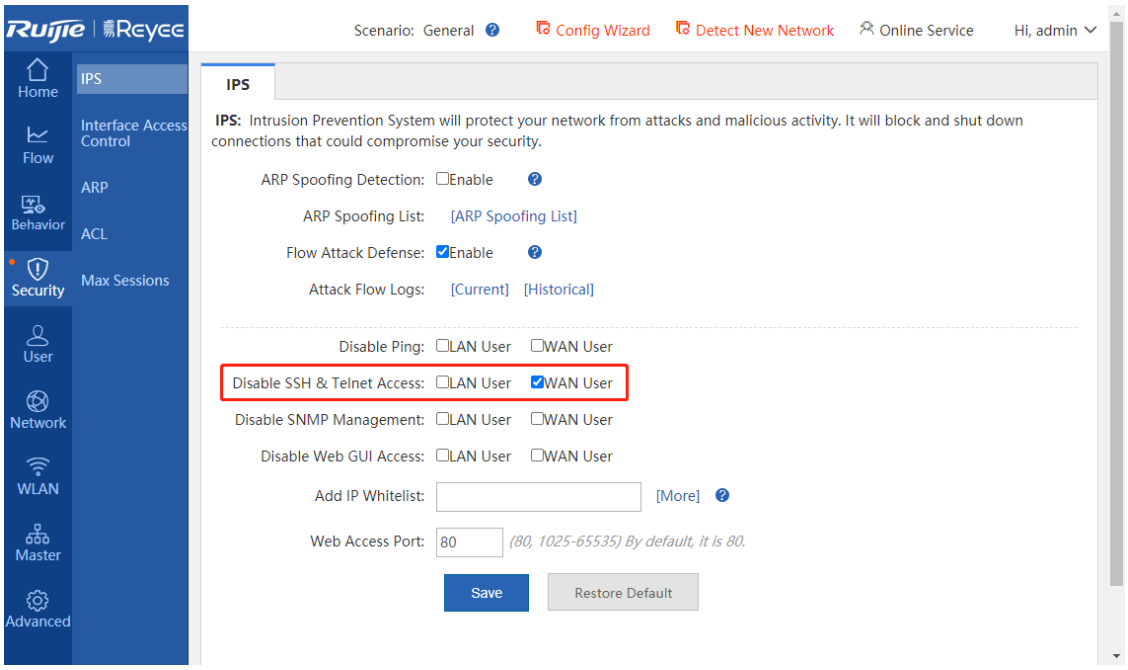
If you want to enter the CLI of the router to perform configurations or collect information, but do not have a console cable or is not around the device, you can manage the device remotely through Telnet.

Prerequisites

- Make sure that logging in through Telnet is not disabled on the router.

  a Log in to the web management system and choose **Security** > **IPS**.

b Check Telnet and SSH access restrictions. To ensure security, WAN users are not allowed to log in to the router through Telnet by default.

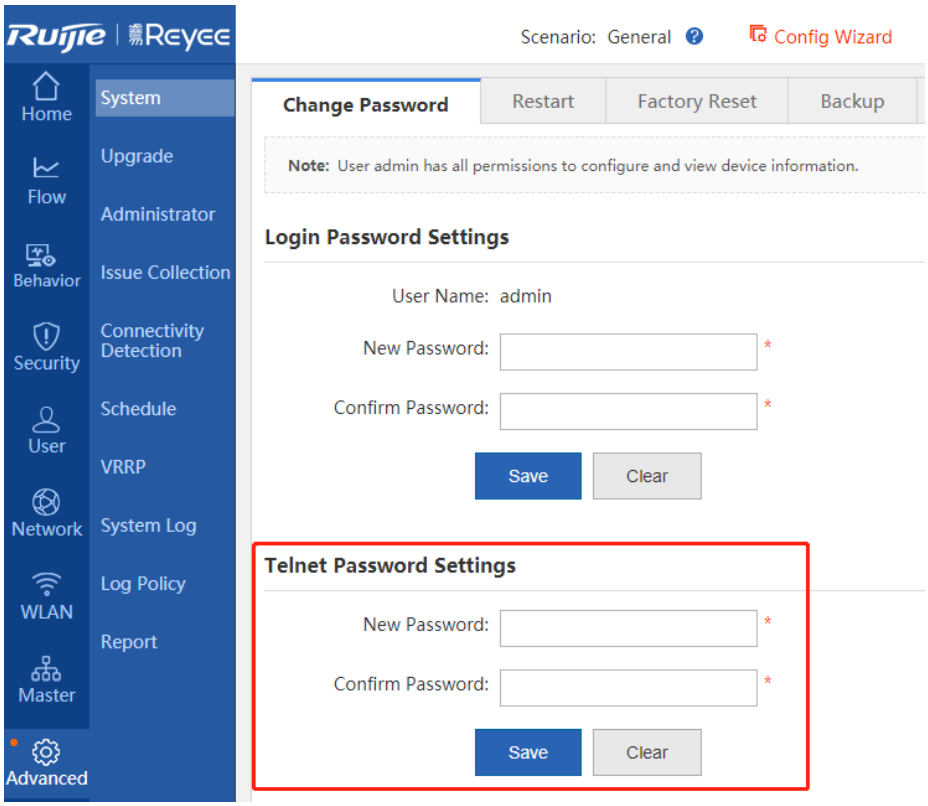


c For a WAN user to log in to the router, you can uncheck "WAN User" and click **Save** to save the change.

- Set a Telnet password for the router. The router does not have a Telnet password in the factory settings, because you cannot log in to the router through Telnet. You must log in to the web management system first to set the Telnet password.

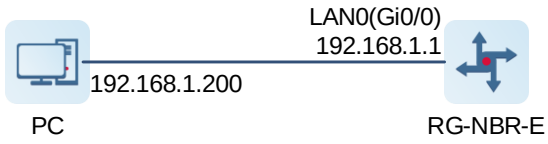
  a Log in to the web management system and choose **Advanced** > **System** > **Change Password**.

  d Enter the Telnet password and click **Save**.



- Ensure the connectivity from the management PC to the router's interface, that is, the management PC can ping the IP address of the router's interface:
  a Connect the management PC and the LAN0/MGMT (Gi0/0) port of the router with a network cable.
  e Configure an IP address for the management PC, which must be in the same network segment as the IP address of the router's interface.

Figure 4-6 Connection topology of login through Telnet

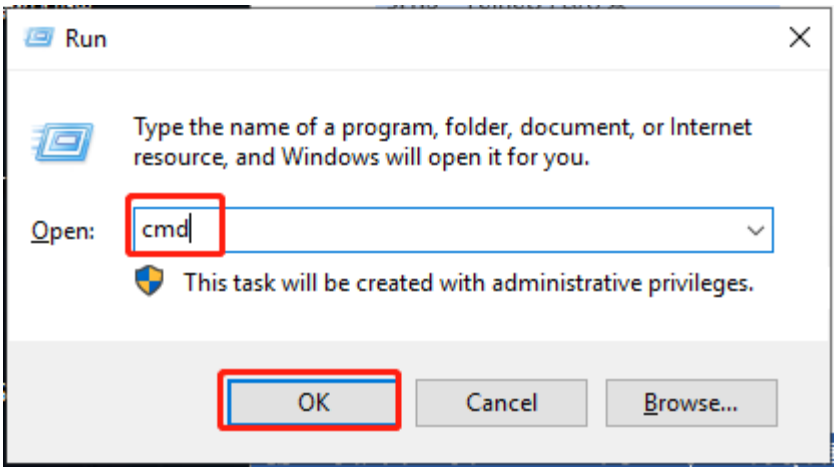


Procedure

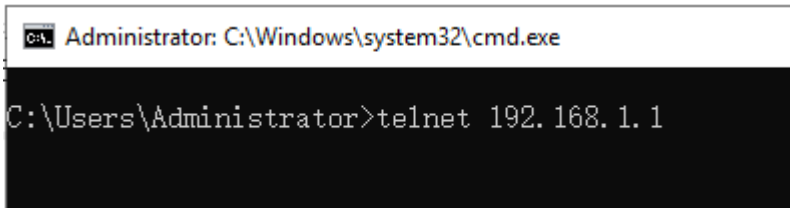
Note

- The administrator logs in to the router through Telnet using SecureCRT, the console program of Windows operating system or the software supporting Telnet connection. The following describes the steps of Telnet login by taking the console program of Windows operating system as an example.
- When establishing a Telnet connection, the host address must be the IP address of the device interface, and the port number is 23.

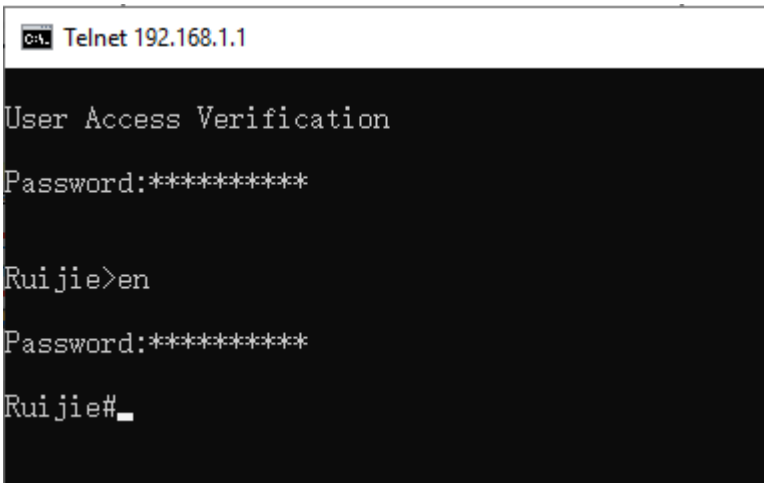
(1) On the management PC, hold down the **Win** key (with Windows logo) and press the **R** key on the keyboard to open the run dialog box. Enter **cmd** and click **OK** to enter the command prompt of the management PC.



(2) Enter the telnet *IP address of the router's interface* command and press **Enter**.



(3) Enter the password as prompted and press **Enter**. The enable password for entering privileged EXEC mode is the same as the Telnet password.

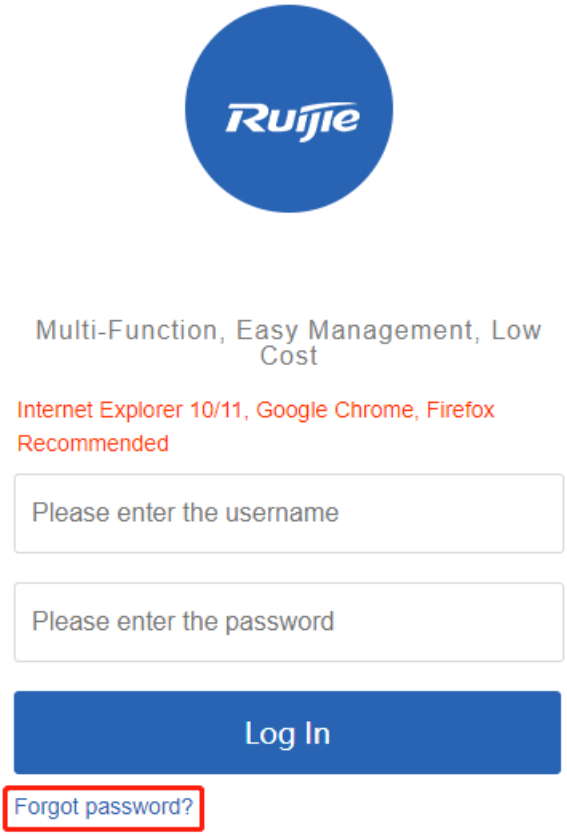


4.2 Configuring a Password

If you forget your web login password, you can restore the current password to the default password **admin**.

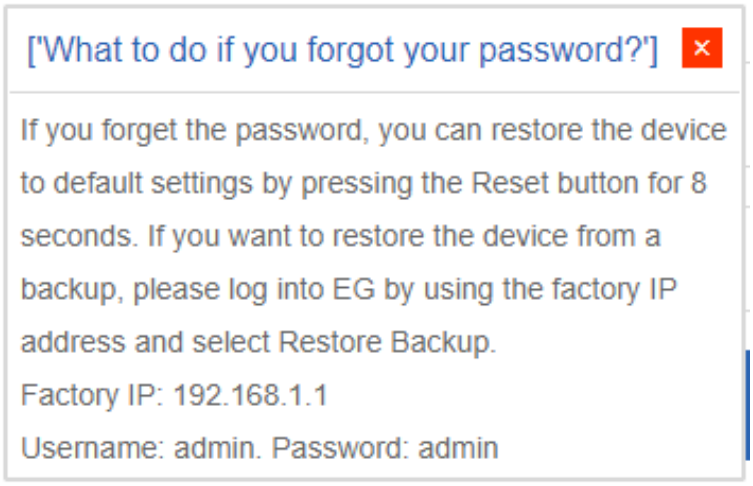
Procedure

(1) Open the web management system login page.



(2) Click **Forgot password?**.

(3) Follow the prompts on the page to restore factory settings of the router. Then log in to the web management system with the default user name and password and restore the configurations. The default username and password are **admin**.



4.3 Upgrading

4.3.1 Upgrading through Web Management System

1. Local upgrade

Application Scenario

You can upgrade the device through local upgrade if the network is abnormal and the system cannot automatically obtain the latest version, or when the upgrade rollback is performed.

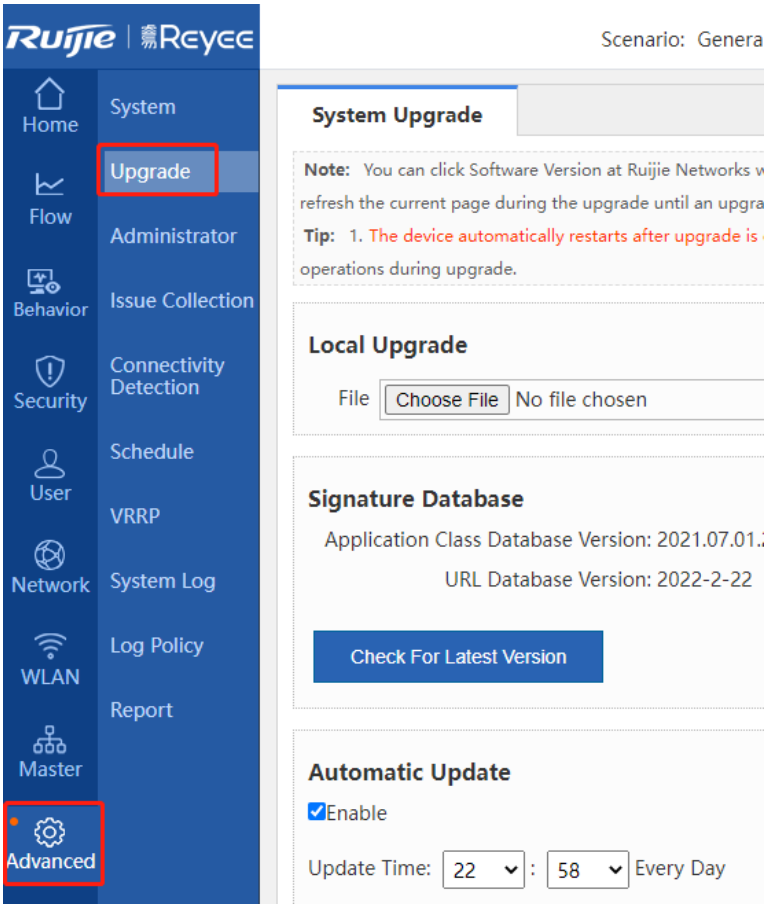
Prerequisites

Download the latest upgrade file from the official website of Ruijie Networks to a local PC.

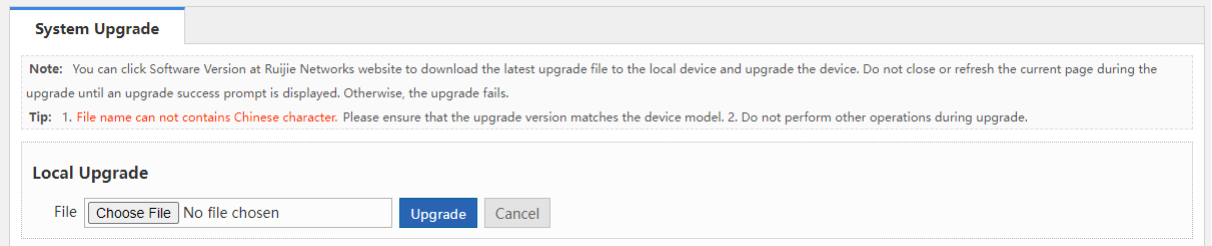
Procedure

(1) Log in to the web management system.

(2) Choose **Advanced** > **Upgrade**.



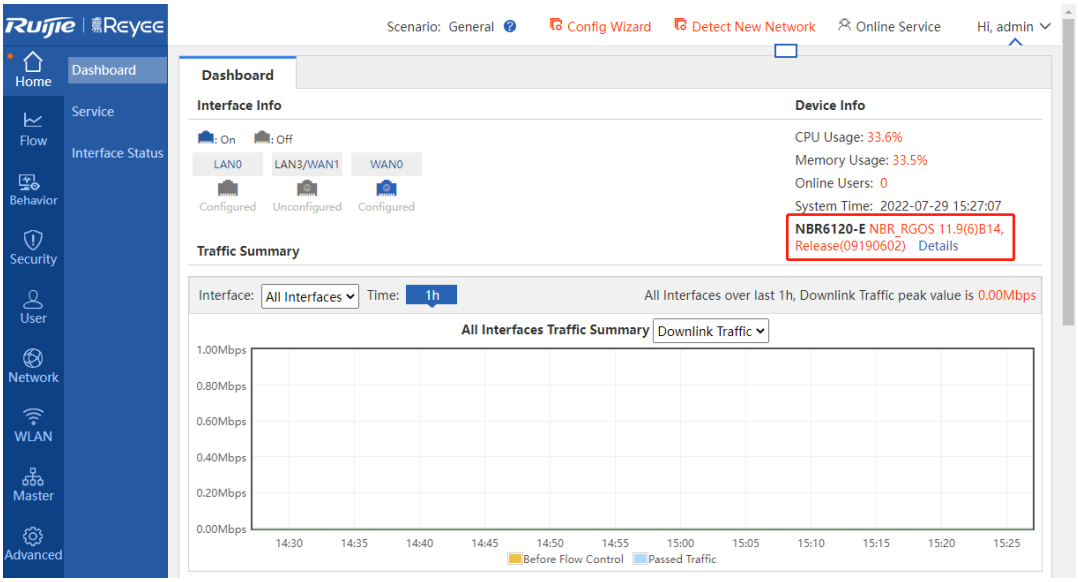
(3) Click **Choose File** to select the upgrade file, and click **Upgrade**.



(4) Click **Upgrade** to start upgrading. Do not perform any operation during upgrade. After the message indicating successful upgrade is displayed, click **OK**.

Follow-up Procedure

Check the software version and other information on the **Home** > **Dashboard** page to check whether the upgrade is successful.



2. Online upgrade

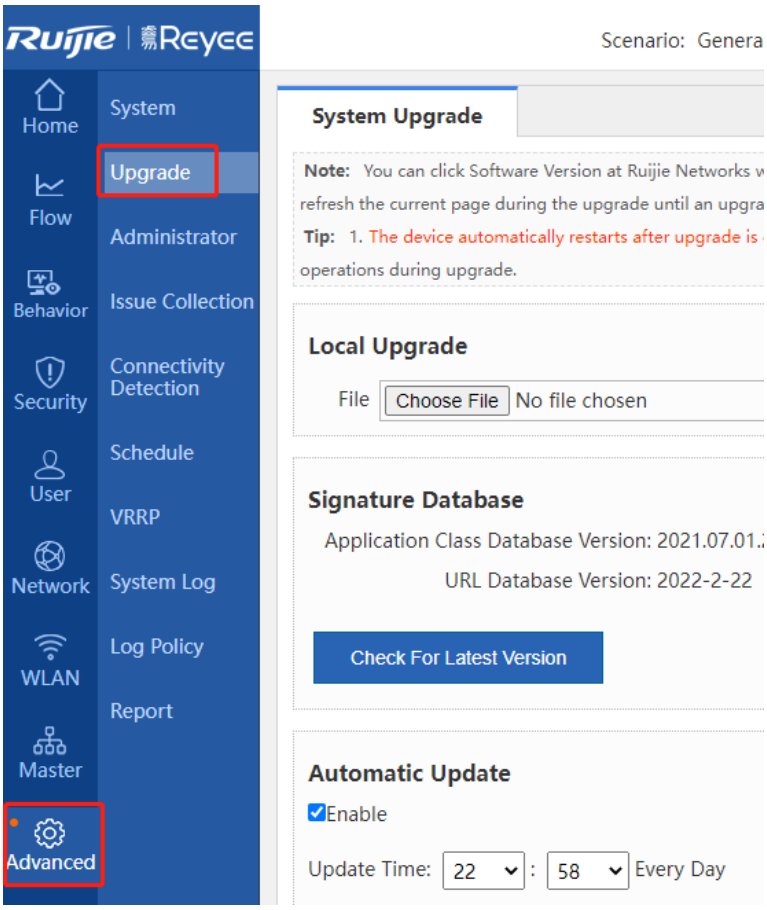
Application Scenario

You can upgrade the router online if the network communication is normal and the system prompts you with the recommended version.

Procedure

(1) Log in to the web management system.

(2) Choose **Advanced** > **Upgrade**.



(3) If the system detects a new software version, you are asked to upgrade the version. Click **Upgrade** to complete the upgrade.

4.4 Backing Up the Configuration and Resetting the NBR Device

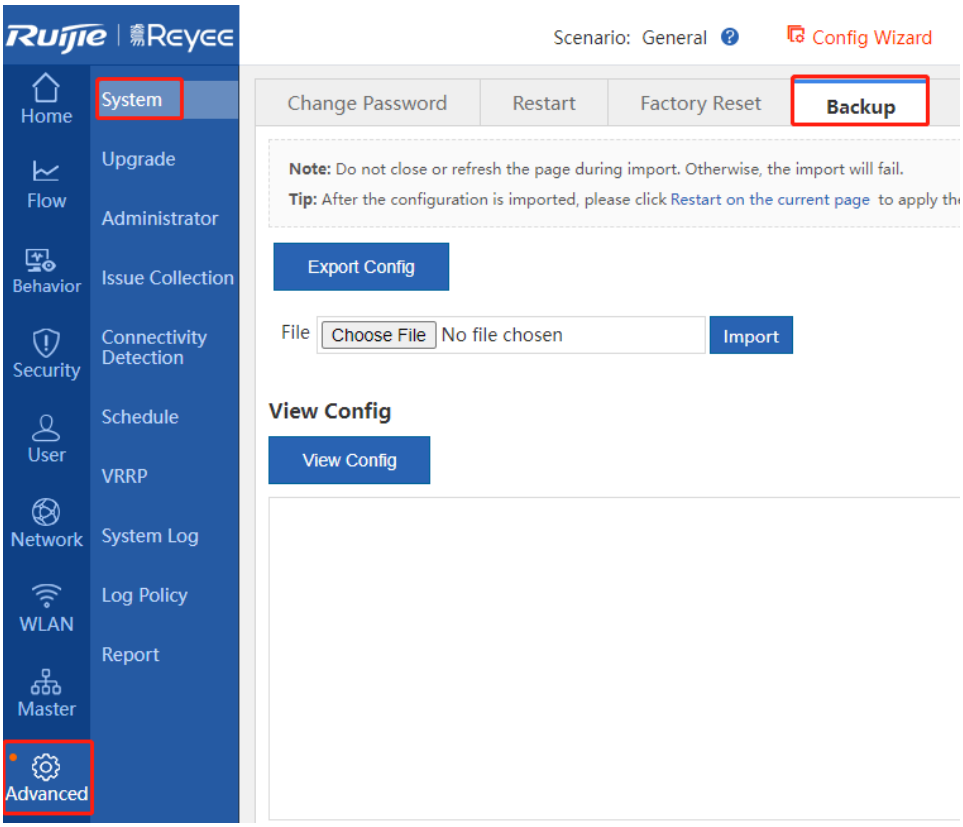
4.4.1 Exporting Configuration Files

You can export the current configurations of the router to a local PC for backup.

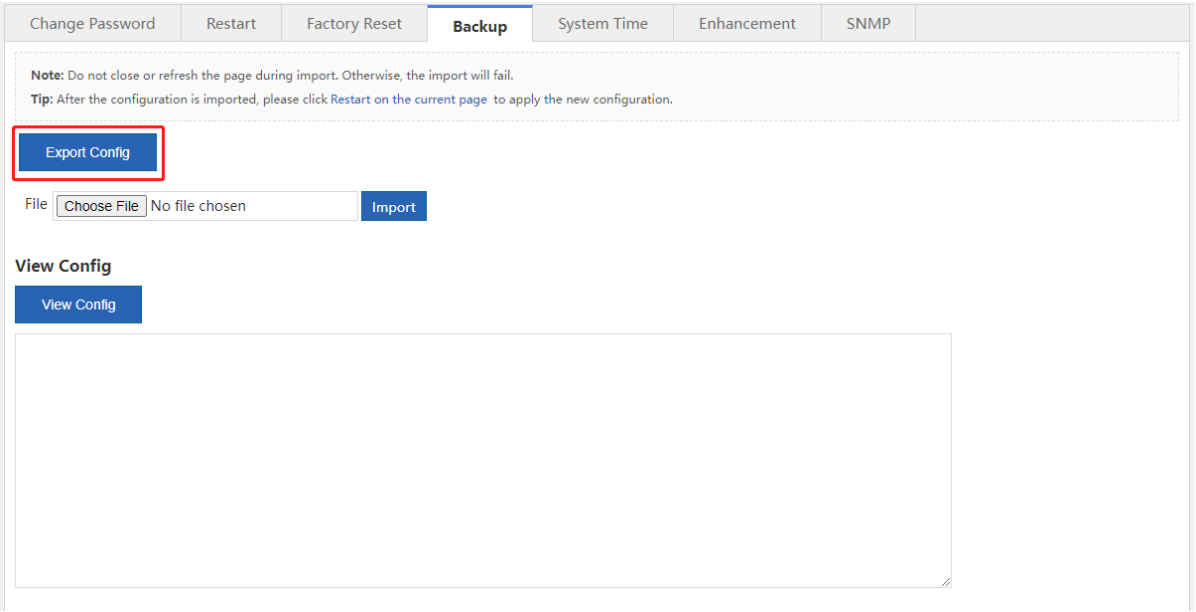
Procedure

(1) Log in to the web management system.

(2) Choose **Advanced** > **System** > **Backup**.



(3) Click **Export Config**.



(4) Select the path for storing configuration files and click **Save**.

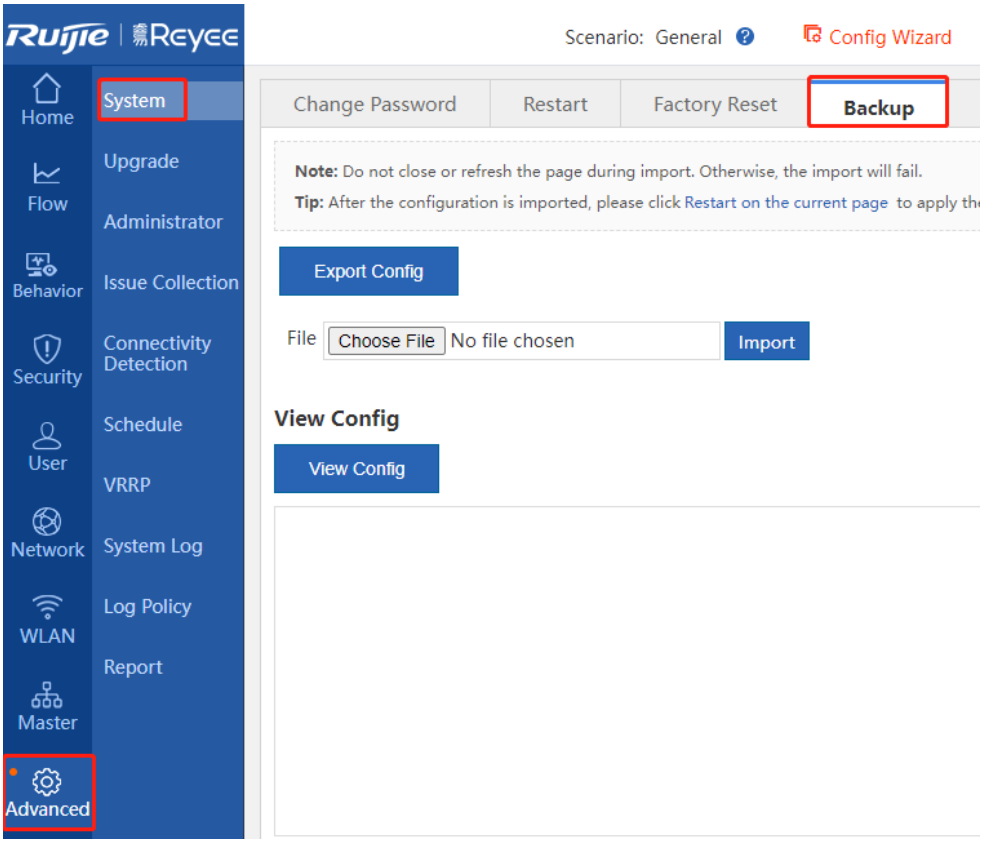
4.4.2 Importing Configuration Files

You can restore the system to the specified configuration state by importing the backup configuration files into the router.

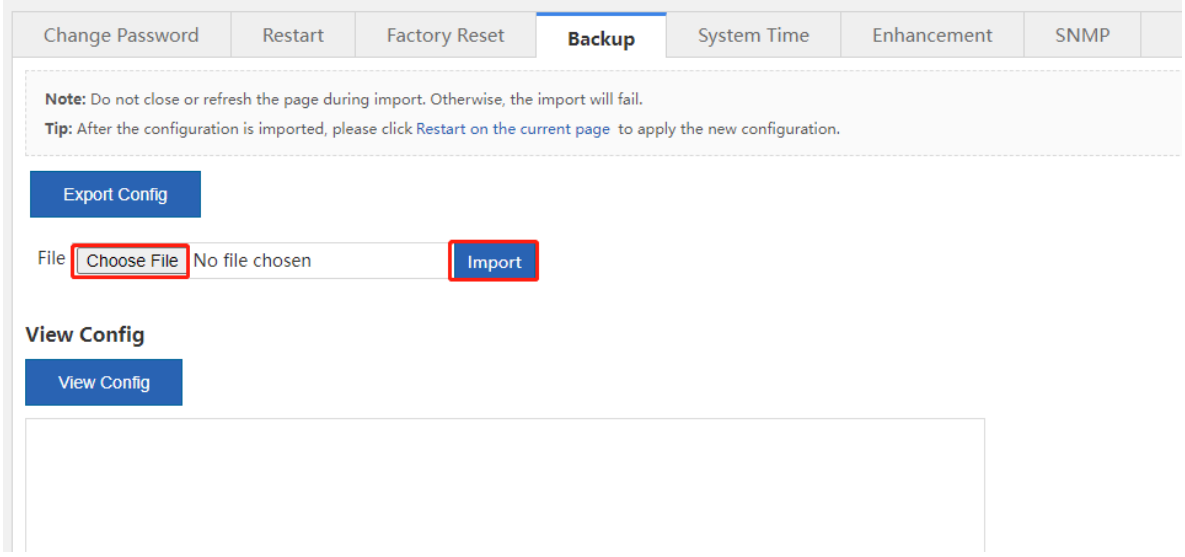
Procedure

(1) Log in to the web management system.

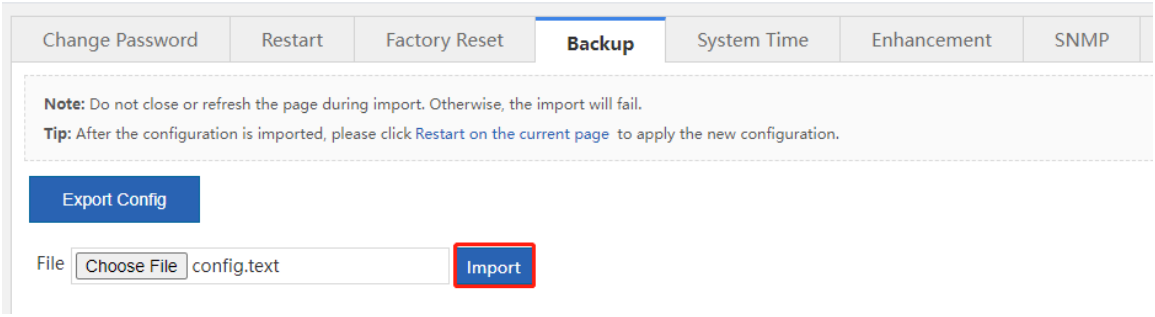
(2) Choose **Advanced** > **System** > **Backup**.



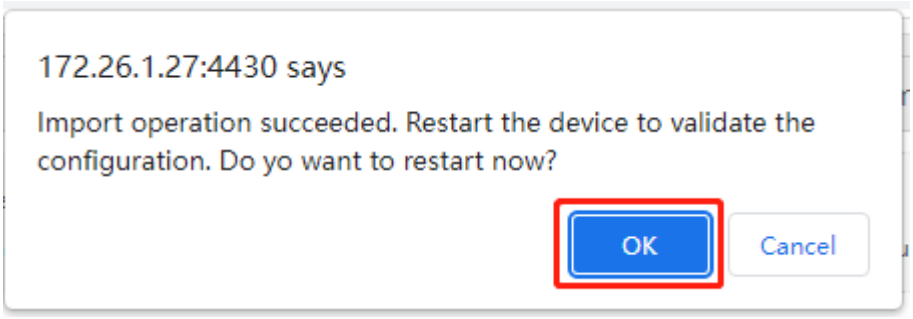
(3) Click **Choose File** and select the backup configuration files to be restored from local PC.



(4) Click **Import** to start importing. Do not close or refresh the web page until the import is complete.



(5) The imported configurations will take effect after the router is restarted. After the import is completed, you are asked whether to restart the router now. Click **OK** to restart the router.



4.5 Restoring Factory Settings

Restoring factory settings will result in deleting all the current configurations of the router.

Caution

If you restore factory settings, the existing configurations will be deleted. You need to reconfigure the router next time you log in to the router.

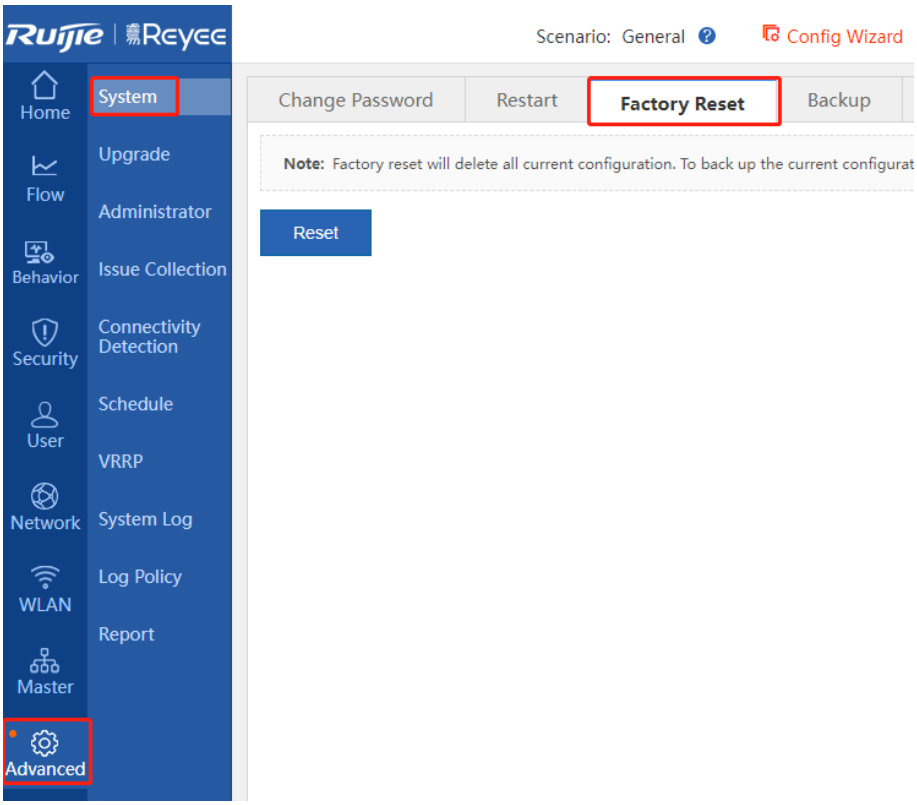
4.5.1 One-Click Reset Through Web

If you are unable to go to the equipment room and reset the router through the device panel, you can restore the router to factory settings through the factory reset function of the web management system.

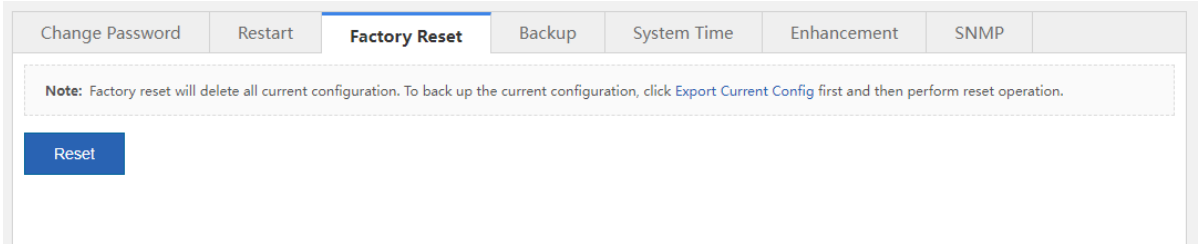
Procedure

(1) Log in to the web management system.

(2) Choose **Advanced** > **System** > **Factory Reset**.



(3) Click **Reset**.



Follow-up Procedure

The router will restart automatically. After the restart, all configurations of the router will be restored to the factory settings.

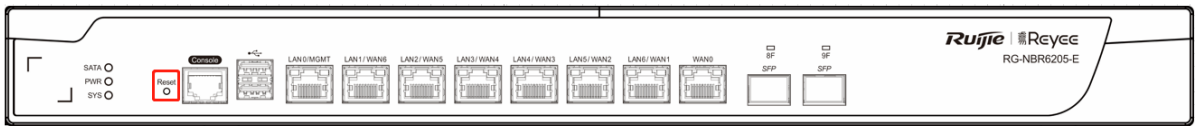
4.5.2 One-Click Reset Through Reset Button

During device maintenance in the equipment room, you can restore the router to factory settings through the Reset button on the router.

Procedure

Press and hold the Reset button on the router for more than 5s to reset it. The Reset pin is located on the front panel near the console port, as shown in Figure 4-7.

Figure 4-7 Reset Hole



Follow-up Procedure

The router will restart automatically. After the restart, all configurations of the router will be restored to the factory settings.