RG-WALL 1600-Z-S Series

Cloud-Managed Firewall

Cookbook

Document Version: V1.0

Date: 2023-08-11

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.

The content of this document will be updated from time to time due to product version upgrades or other reasons. 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 servicing 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	Choose **System** > **Time**.

2. Signs

The signs used in this document are described as follows:

Danger

An alert that calls attention to safety operation instructions that if not understood or followed when operating the device can result in physical injury.

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 introduces the features of the product and offers guidance on configuration and testing.

Contents

1 Product Overview

1.1 Overview

With the emergence of new hot spots such as social networking, cloud computing, and big data, the Internet has entered a stage of prosperity never experienced in history. However, the information security problems accompanied have become increasingly complex, bringing huge challenges to the traditional security construction model. With years of technology accumulation and considering the development trend of next-generation firewalls, Ruijie Networks promotes the RG-WALL 1600-Z3200-S series cloud management firewalls (hereinafter referred to as Z-S series firewalls) to meet the actual needs of the market.

The RG-WALL 1600-Z-S series cloud management firewalls use DPDK-based high-performance network forwarding service platform to provide active asset discovery, intelligent policy manager, and one-click fault analysis functions, simplifying product launch and operation and maintenance (O&M). This series of firewalls have rich security functions, including intrusion prevention, port scan, traffic learning, application control, and defense against DoS/DDoS attacks. These firewalls also support unified management on the cloud platform, data synchronization to the cloud for analysis and reporting, and remote monitoring and O&M.

The Z-S series firewalls have performance expansion capabilities, and a single hardware platform supports 3–10 G performance expansion, which can be realized through a performance license.

The Z-S series firewalls are suitable for network egress, area boundary, and other scenarios of general education, higher education, government, and enterprise customers.

1.2 Product Characteristics

- Easy configuration

  The Z-S series firewall provides a quick onboarding wizard to help users quickly complete basic configurations for network access. Users only need to select interfaces and a mode and configure the basic connection type and IP address to bring a device online. The configuration wizard also provides optional functions such as connectivity test, license import, and policy configuration to help users complete basic operations related to testing, authorization, and policies.

- Intelligent policy manager

Affected by factors such as service accumulation and change of O&M personnel, the configuration complexity of security policies becomes increasingly high during routine security policy O&M. Major problems are as follows: Policies are not refined enough. Services are interrupted due to conflicts between new and existing policies. O&M personnel are concerned about the overall policy health and whether policies are optimal. When a fault occurs, O&M personnel usually need to trace and analyze the policies that are changed. Complex policies make O&M even more difficult.

The Z-S series firewall provides functions including port scan, traffic learning, policy simulation space, intelligent policy sorting, and policy lifecycle management to help users resolve the preceding problems.

- App identification and control

  The Z-S series firewall can identify over 2000 applications of 36 categories. It can identify more applications after the rule base is upgraded. App identification and control can implement traffic control and management.

- Diversified security defense

  The Z-S series firewall provides rich security defense functions to defend against various types of traffic flood attacks including SYN flood, UDP flood, ICMP flood, and IP flood, and large-traffic DDoS attacks. With the built-in comprehensive IPS signature library, the firewall can perform real-time deep scan on the traffic passing through it to identify malicious information hidden in the traffic and generate alarms and block the traffic in real time, protecting users against threats from malicious traffic.

- High stability and reliability

  The Z-S series firewall uses a stable and reliable hardware design to provide the following functions: Provides dual-boot instruction to reduce the probability of device start failures caused by boot problems. Actively monitors the voltage of each circuit on the device motherboard, prompts for voltage exceptions, and applies power-off protection in case of grid exceptions to protect storage components against damage in case of abnormal grid fluctuations and abrupt power-off. Uses dual-power supply and area-based power design to avoid whole device restart caused by short circuit of the optical module.

- Flexible expansion

  The Z-S series firewall can expand the device performance based on licenses. It also has high hardware expansion capability, with one expansion slot and an optional hard disk of 1 TB.

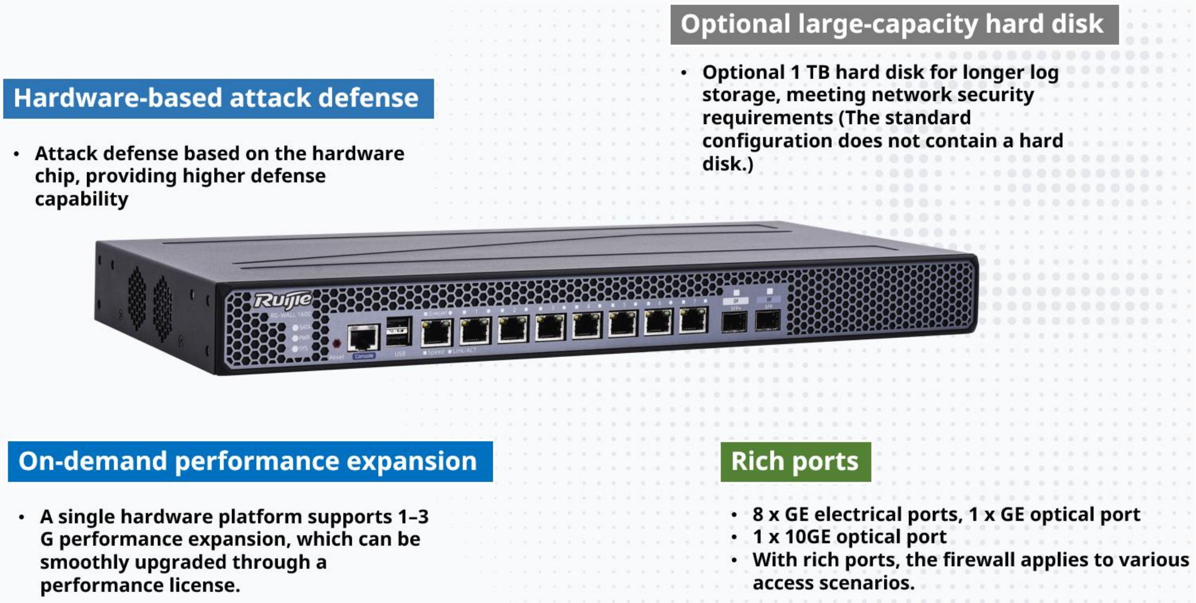
- Easy cloud-based O&M

  The Z-S series firewall supports configuration delivery, upgrade, status monitoring, and hot patch installation on the cloud to lower the O&M difficulty.

1.3 Hardware Description

The RG-WALL 1600-Z3200-S cloud management firewall uses the brand-new NTOS platform and has the following characteristics:

- Rich ports: The firewall has fixed ports including eight GE electrical ports, one GE optical port, and one 10GE optical port. With rich ports, the firewall applies to various access scenarios.
- Optional large-capacity hard disk: 1 TB high-performance hard disk can be configured for longer log storage. (The standard configuration does not contain a hard disk.)
- Hardware-based attack defense: Attack defense based on the hardware chip provides higher defense capability.
- Scalable performance: A single hardware platform supports 1–3 G performance expansion, which can be smoothly upgraded through a performance license.



Optional large-capacity hard disk

- Optional 1 TB hard disk for longer log storage, meeting network security requirements (The standard configuration does not contain a hard disk.)

Hardware-based attack defense

- Attack defense based on the hardware chip, providing higher defense capability

On-demand performance expansion

- A single hardware platform supports 1–3 G performance expansion, which can be smoothly upgraded through a performance license.

Rich ports

- 8 x GE electrical ports, 1 x GE optical port
- 1 x 10GE optical port
- With rich ports, the firewall applies to various access scenarios.

1.3.1 RG-WALL 1600-Z3200-S Panels

1. Front Panel

Figure 1-1 Front Panel

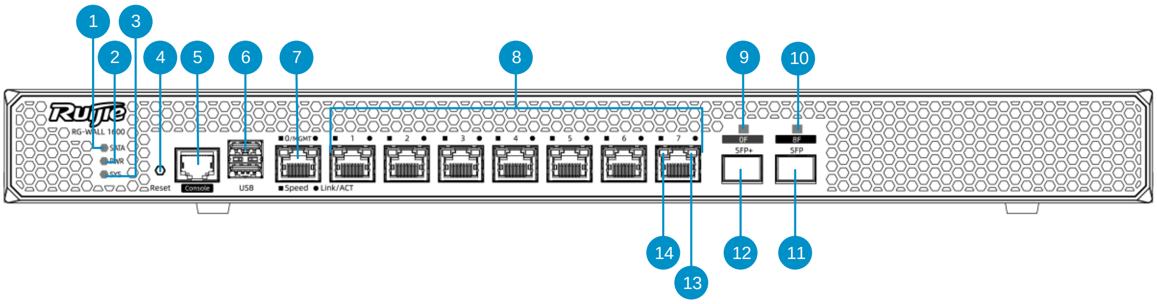


Table 1-1 Components on the Front Panel

No.	Component	Description
1	SATA hard disk indicator	- Steady green: A hard disk is connected. - Blinking green: Data is being read or written.
2	PWR indicator	- Steady green: The power supply is normal. - Off: The power supply is cut off or fails.
3	SYS indicator	- Blinking green: The device is powered on and being initialized. - Steady green: Initialization is complete. - Steady red: An alarm is generated.
4	Reset button	- Restarting the device: Press the button for less than 3 seconds. - Restoring factory settings: Press the button for more than 5 seconds. When you perform either of the preceding operations, device status information is collected. After the device restarts, you can access the web UI of the firewall, choose **System** > **One-Click Collection**, and download

No.	Component	Description
		the information.
5	Console port	It is used to connect to the console for device maintenance and diagnosis. Note: The console port is used only in special scenarios. For details, contact technical support personnel.
6	USB port	Two USB 2.0 ports can be used to connect USB drives.
7	Electrical port 0 (port 0/MGMT)	It is used to access the device management page upon first login.
8	Electrical ports 1 to 7	They are used to connect network cables.
9	Optical port 0F indicator	● Steady green: The port is connected. ● Blinking green: The port is receiving or sending data. ● Off: The optical port is incorrectly connected.
10	Optical port 8F indicator	● Steady green: The port is connected. ● Blinking green: The port is receiving or sending data. ● Off: The optical port is incorrectly connected.
11	Optical port 8F	Gigabit optical port. For details about optical modules that support this port, see Table 1-3.
12	Optical port 0F	10 Gigabit optical port. For details about optical modules that support this port, see Table 1-3.
13	Link/ACT status indicators (round) of electrical ports 0 to 7	● Steady green: The port is connected. ● Blinking green: The port is receiving or sending data.

No.	Component	Description
		● Off: The port is incorrectly connected.
14	Speed indicators (square) of electrical ports 0 to 7	● Steady orange: Gbit/s port speed ● Off: 100/10 Mbit/s port speed

2. Rear Panel

Figure 1-2 Rear Panel

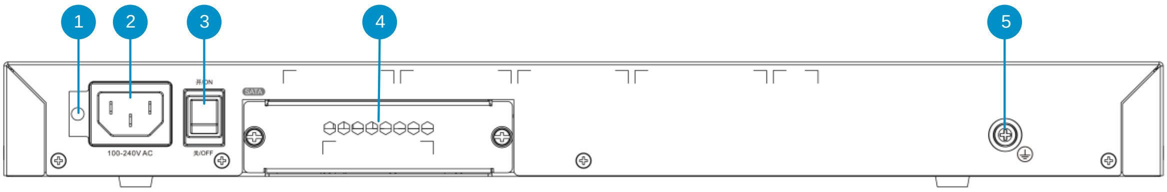


Table 1-2 Components on the Rear Panel

No.	Component	Description
1	Installation position of a power cord retention clip	Used to install a power cord retention clip.
2	Power socket	Used to connect an AC power cord.
3	Power switch	Used to power on or power off the device.
4	Expansion slot for a hard disk	Used to install a hard disk.
5	Grounding terminal	Used to ground the device to ensure electrical safety.

1.4 Specifications

1.4.1 RG-WALL 1600-Z3200-S Specifications

Table 1-3 Specifications

Model	RG-WALL 1600-Z3200-S
Storage	DDR4 SDRAM: 4 GB
	Boot ROM: 8 MB
	eMMC: 8 GB
	SATA hard disk: 1 TB
Port	The firewall supports eight Gigabit electrical ports and two optical ports. ● Electrical port: works at a rate of 10 Mbit/s, 100 Mbit/s, or 1000 Mbit/s in auto-negotiation mode and automatically identifies network cables and crossover cables. ● Gigabit optical port: supports 1000BASE-SX/LX/ZX mini GBIC and GE-SFP-LX20/LH40-BIDI optical modules. ● 10 Gigabit optical port: supports XG-SFP-SR-MM850, XG-SFP-LR-SM1310, and XG-SFP-ER-SM1550 optical modules, as well as BIDI optical modules.
	MGMT port Used as GE 0/0 port. It works at a rate of 10 Mbit/s, 100 Mbit/s, or 1000 Mbit/s in auto-negotiation mode and automatically identifies network cables and crossover cables.
	Console port: 1
	USB port: two USB 2.0 ports
Bypass	Not supported

Expansion Slot for Hard Disk	(Optional) One 1 TB hard disk can be configured.
Expansion Card	Not supported
Hot Swapping	Hard disk: not supported
Port Standards	Ethernet port: 10Base-T/100Base-TX/1000Base-TX, 1000BASE-SX/LX/ZX, and 10GBASE-SR/LR/ZR
	Console port: RS-232
Dimensions (H x W x D)	43.6 mm x 440 mm x 200 mm (1.72 in. x 17.32 in. x 7.87 in.; without rubber pads)
Power Supply	100–240 V AC, 50–60 Hz; 0.65 A
Max. Power Consumption	Less than 25 W
Temperature	0°C to 45°C (32°F to 113°F)
Humidity	10% to 90% RH (non-condensing)

2 Device Management

2.1 Logging In to the Device

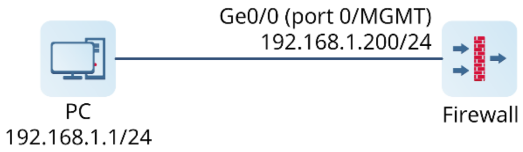
2.1.1 Logging In to the Device from the Web

Application Scenario

The web management page provides a visualized graphical management page for efficient configuration and management.

You can configure and manage the firewall on the visualized web UI and configure the management functions of Ge0/1.

Network Topology



Prerequisites

- The Z-S series firewall provides the default web configurations as listed in Table 2-1. You can log in to the management page with the default values through HTTPS.

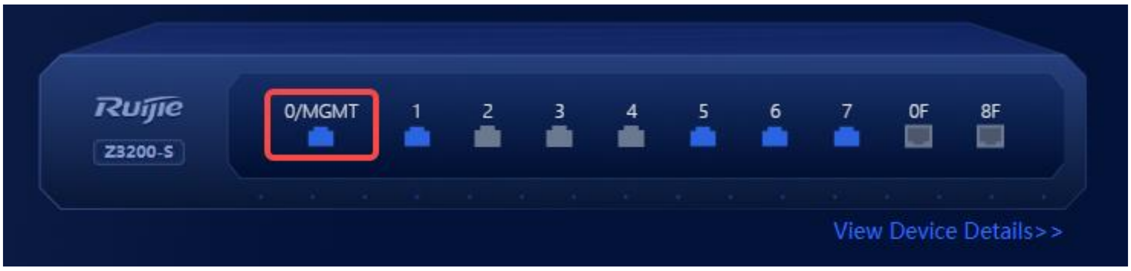
Table 2-1 Default Web Configurations

Function Item	Default Value
Web service	Enabled
Device IP	192.168.1.200 (port 0/MGMT)
Username/Password	admin/firewall
Default user permission	Super Admin (with all the permissions)

Note

- If the address of port 0/MGMT on the firewall is modified but you forget the address, you can can access the Command Line Interface (CLI) to view the current configuration. For details, see 0
- Logging In to the Device from the Console.
- If you change the password and forget it, restore the initial password. For details, see 2.6 Password Restoration.

- The management PC and firewall have been connected and can communicate with each other.
  - Port 0/MGMT on the firewall is connected to the management PC through a network cable.



  - The default IP address of port 0/MGMT is 192.168.1.200. To ensure that the management PC can communicate with the firewall, the IP address of the local NIC on the management PC must be changed to one in the same network segment as that of port 0/MGMT, for example, 192.168.1.100/24.
- The management PC meets relevant requirements on the browser and resolution.
  - Browsers: Internet Explorer 11.0, Google Chrome, Firefox, and some Internet Explorer kernel-based browsers 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 is 1440 x 900. In case of other resolution, scroll bars may appear on the UI, affecting the use experience.

Configuration Points

(1) Set the IP address of the management PC to one in the same network segment as the IP address of port 0/MGMT.

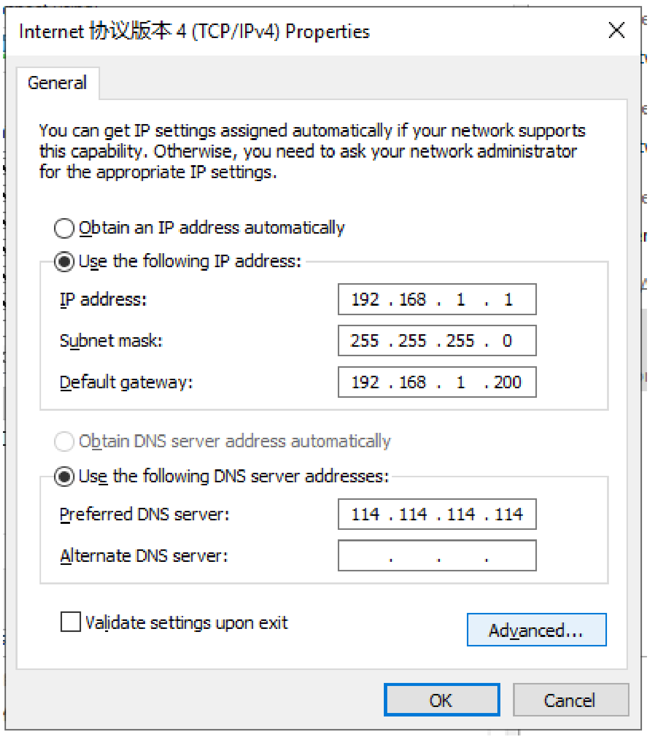
(2) Log in to the web management page.

(3) Configure the Ge0/1 port and enable the management functions on the port. By default, IP addresses or access management functions such as HTTPS are not configured for other ports except 0/MGMT.

Procedure

(1) Configure an IP address for the management PC.

The default IP address of port 0/MGMT on the firewall is 192.168.1.200. On the management PC, set **IP address** to 192.168.1.1 and **Default gateway** to 192.168.1.200.



Internet 协议版本 4 (TCP/IPv4) Properties

General

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

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 1

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 200

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 114 . 114 . 114 . 114

Alternate DNS server: . . .

□ Validate settings upon exit

(2) Log in to the web management page.

Note

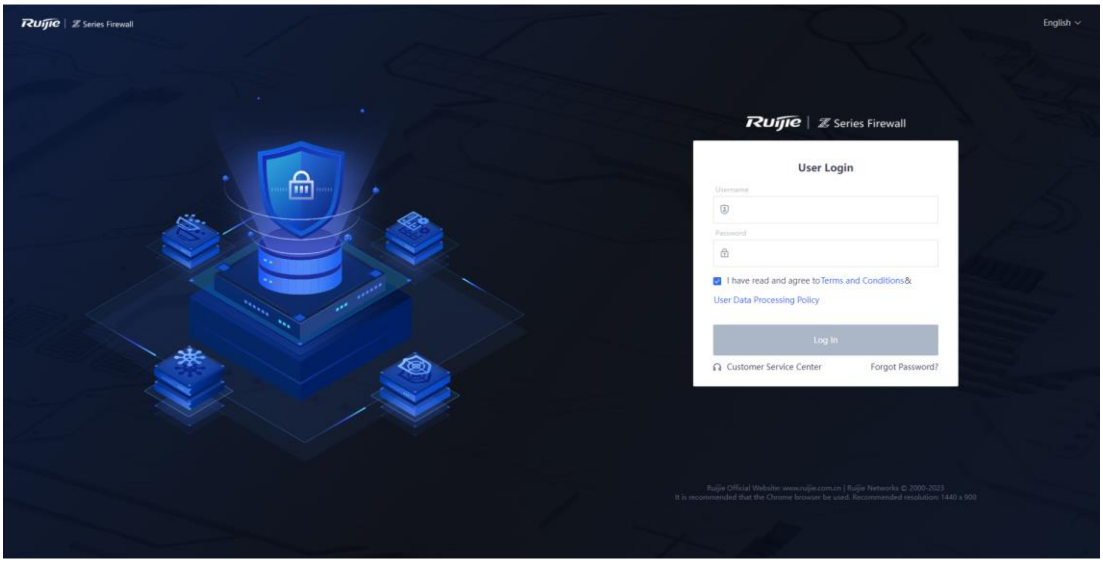
It takes a certain period of time to complete system initialization after the device is powered on and started. You are advised to wait for 5 to 6 minutes before accessing the web page.

a Open a browser on the management PC.

b Enter **https://192.168.1.200** in the address bar and press **Enter**.

The login page is displayed.

c Enter the username (**admin**), password (default: **firewall**), and verification code. Read the statement, select **I have read and agree to Terms and Condition & User Data Processing Policy**, and click **Log In**.



User Login

Username

Password

☑ I have read and agree to Terms and Conditions& User Data Processing Policy

Log In

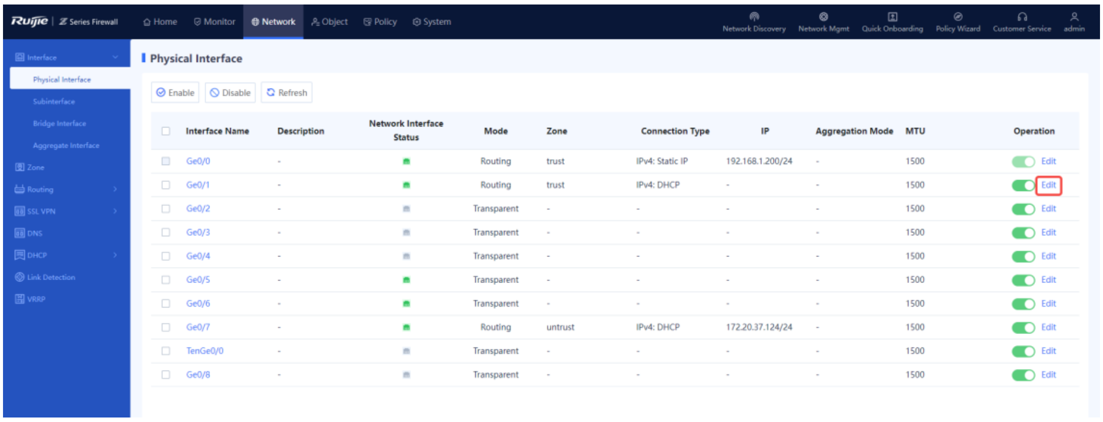
Customer Service Center Forgot Password?

Ruijie Official Website: www.ruijie.com.cn | Ruijie Networks © 2000-2023
It is recommended that the Chrome browser be used. Recommended resolution: 1440 x 900

(4) (Optional) If you log in to the web management page for the first time, the system forces you to change the default password of the Super Admin.

(5) Set the IP address of the Ge0/1 port to 192.168.0.200/24 and enable the management functions on the Ge0/1.

a Choose **Network** > **Interface** > **Physical Interface**.

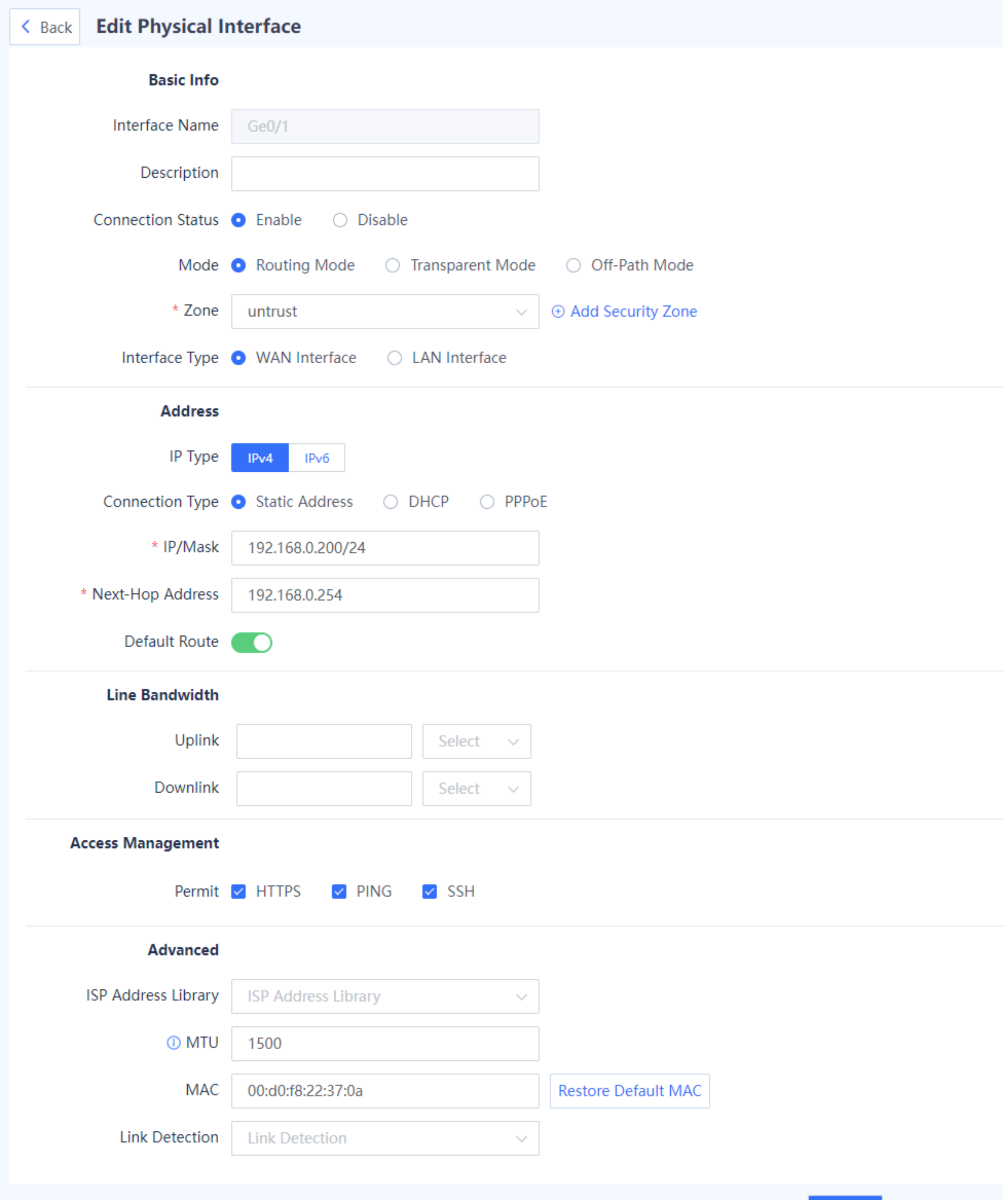


Physical Interface

□	Interface Name	Description	Network Interface Status	Mode	Zone	Connection Type	IP	Aggregation Mode	MTU	Operation
□	Ge0/0	-	🟩	Routing	trust	IPv4: Static IP	192.168.1.200/24	-	1500	Edit
□	Ge0/1	-	🟩	Routing	trust	IPv4: DHCP	-	-	1500	Edit
□	Ge0/2	-	▨	Transparent	-	-	-	-	1500	Edit
□	Ge0/3	-	▨	Transparent	-	-	-	-	1500	Edit
□	Ge0/4	-	▨	Transparent	-	-	-	-	1500	Edit
□	Ge0/5	-	🟩	Transparent	-	-	-	-	1500	Edit
□	Ge0/6	-	🟩	Transparent	-	-	-	-	1500	Edit
□	Ge0/7	-	🟩	Routing	untrust	IPv4: DHCP	172.20.37.124/24	-	1500	Edit
□	TenGe0/0	-	▨	Transparent	-	-	-	-	1500	Edit
□	Ge0/8	-	▨	Transparent	-	-	-	-	1500	Edit

b Select **Ge0/1** and click **Edit**.

c Configure attributes of Ge0/1.



Back **Edit Physical Interface**

Basic Info

Interface Name: Ge0/1

Description:

Connection Status: ● Enable ○ Disable

Mode: ● Routing Mode ○ Transparent Mode ○ Off-Path Mode

* Zone: untrust | Add Security Zone

Interface Type: ● WAN Interface ○ LAN Interface

Address

IP Type: IPv4 | IPv6

Connection Type: ● Static Address ○ DHCP ○ PPPoE

* IP/Mask: 192.168.0.200/24

* Next-Hop Address: 192.168.0.254

Default Route: on

Line Bandwidth

Uplink: Select

Downlink: Select

Access Management

Permit: ☑ HTTPS ☑ PING ☑ SSH

Advanced

ISP Address Library: ISP Address Library

MTU: 1500

MAC: 00:d0:f8:22:37:0a | Restore Default MAC

Link Detection: Link Detection

Item	**Description**	**Remarks**
IP/Mask	IP address of the physical interface.	[Example] 192.168.0.200/24
Access Manageme	Whether the interface supports HTTPS, ping, and SSH.	The configuration takes effect when local defense is

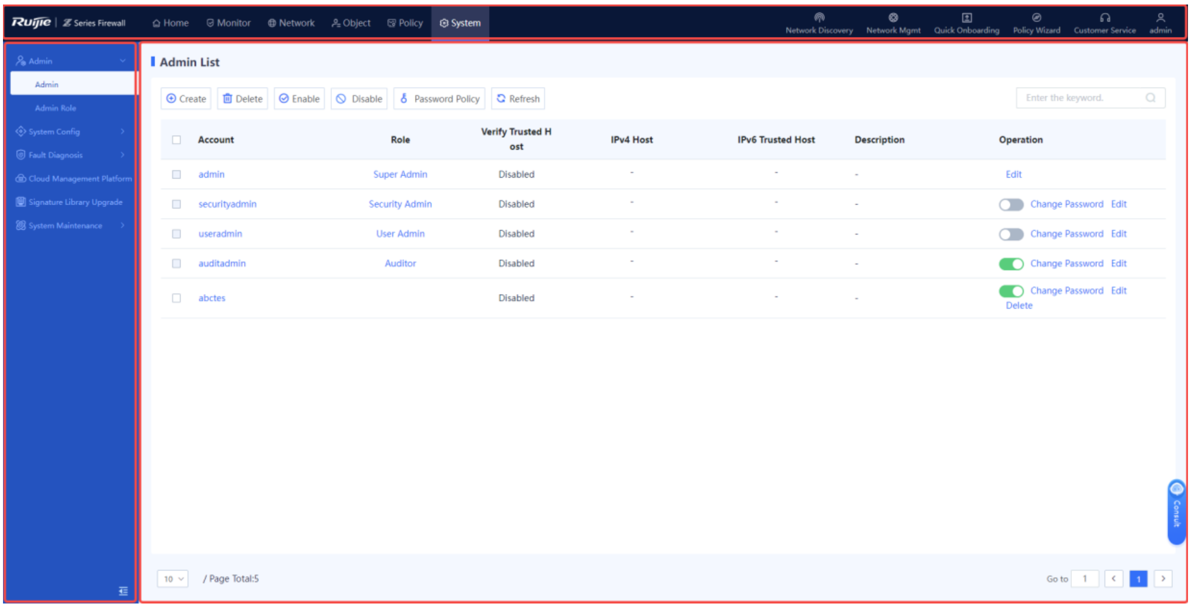
Item	Description	Remarks
nt	● **HTTPS:** Allows users to access the device using https://*Interface IP address*, such as https://192.168.0.200. ● **PING:** Allows users to ping the interface address. If this option is not selected, ping fails even if there is a reachable route. ● **SSH:** Allows users to access the device by creating an SSH connection with the interface IP address that is used as the destination address, such as **ssh 192.168.0.200**.	enabled on the device. [Example] Select **HTTPS**.

d Click **Save**.

Follow-up Procedure

- Enter **https://192.168.0.200** in the browser and log in to the system for management.
- Figure 2-1 shows the web management page layout of the firewall Figure 2-1.

Figure 2-1 Web Management Page Layout



Admin List

Account	Role	Verify Trusted Host	IPv4 Host	IPv6 Trusted Host	Description	Operation
admin	Super Admin	Disabled	-	-	-	Edit
securityadmin	Security Admin	Disabled	-	-	-	Change Password Edit
useradmin	User Admin	Disabled	-	-	-	Change Password Edit
auditadmin	Auditor	Disabled	-	-	-	Change Password Edit
abctes		Disabled	-	-	-	Change Password Edit Delete

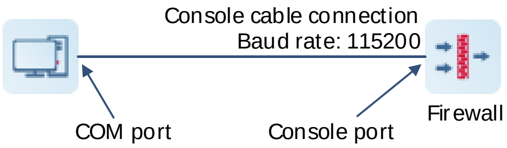
Area	Description
Mark and panel area	● This area displays the company logo, device name, and function panel. ● This area supports new network discovery, network-wide management, quick onboarding, policy configuration wizard, and customer service, helping users quickly complete deployment operations. ● This area displays the current login user and allows you to change the password and log out.
Navigation pane	This area displays the web function menus of the device in the tree structure. You can click a function menu in the navigation bar to access the corresponding function configuration page. The configured items are displayed in the operation area.
Operation area	In this area, you can perform configuration operations and view information and the operation results.

2.1.2 Logging In to the Device from the Console

Application Scenario

To access the CLI for configuration management, connect a console cable to the console port of the device and start the terminal simulation software such as Super Terminal or SecureCRT. By default, the firewall supports console management.

Network Topology



Tool Preparation

- Console cable
  - Model 1: Connect one end of the cable to the 9-hole DB9 connector and the other end to the RJ45 connector.

- Model 2: Connect one end of the cable to the RJ45 connector and the other end to the USB connector.

- PC with a COM port: The COM port of the PC is usually located near the display interface on the rear panel of the chassis. The COM port has nine pins, as shown in Figure 2-2.

  If your PC does not have a COM port (such as the laptop), the USB-to-COM cable (as shown in Figure 2-3) must be connected to the USB port to convert it into the COM port. You can also use the USB-to-console (RJ45) cable of Model 2 directly.

Figure 2-2 COM port

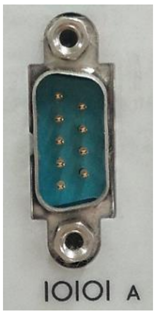
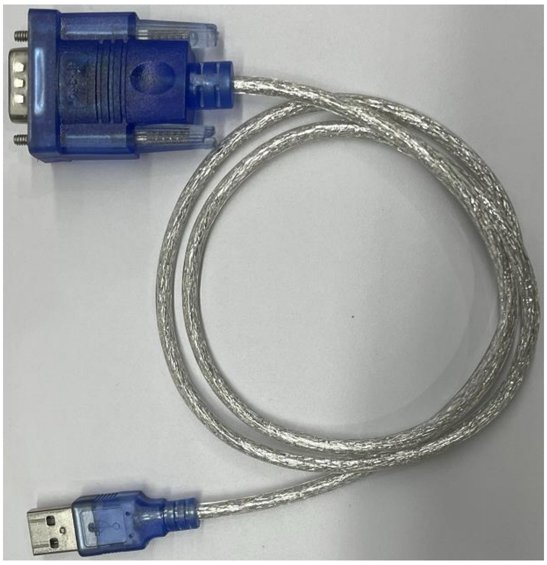


Figure 2-3 USB-to-COM Cable



- Install SecureCRT, Super Terminal, or another terminal simulation software on the PC.
    - A PC running the Windows XP operating system is usually delivered with Super Terminal in the accessories. For a PC running Windows 7 or a later version, you need to download Super Terminal independently.
    - Super Terminal is not installed in Windows Server 2003 by default. To install Super Terminal, choose **Control Panel** > **Add/Remove Programs**.

Configuration Points

(1) Prepare a configuration cable and a PC that can be connected to a configuration cable. (For details, see **Tool Preparation**.)

(2) Connect the configuration cable.

Connect the RJ45 connector of the configuration cable to the console port of the device and the other end to the COM port of the PC.

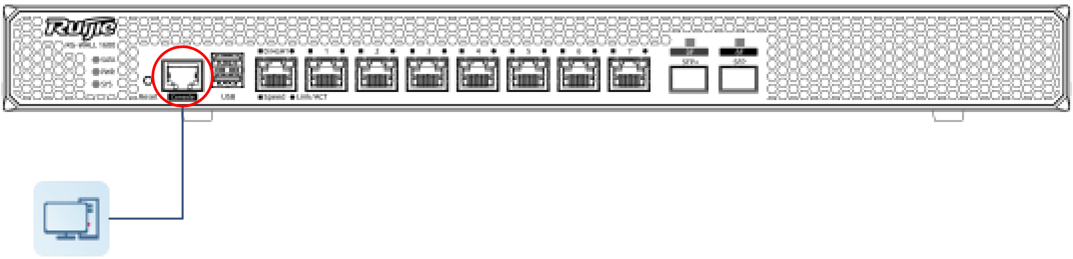
(3) Run the terminal simulation software to log in to the device.

Procedure

(1) Connect the configuration cable.

a Insert the RJ45 connector of the console cable to the console port of the device (as shown in the following figure).

b Insert the DB9 connector on the other end of the console cable to the 9-pin COM port of the PC.



(2) Run the terminal simulation software after the configuration cable is connected.

Note

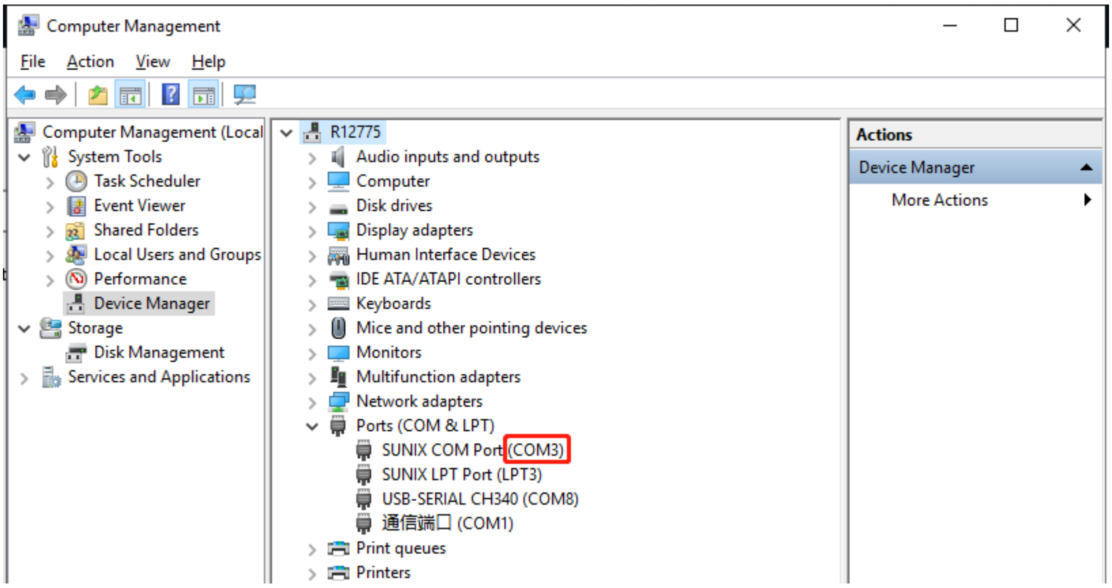
This section uses SecureCRT as an example. For details about other programs, see the corresponding operation manual.

a View identified COM ports on the PC.

Note

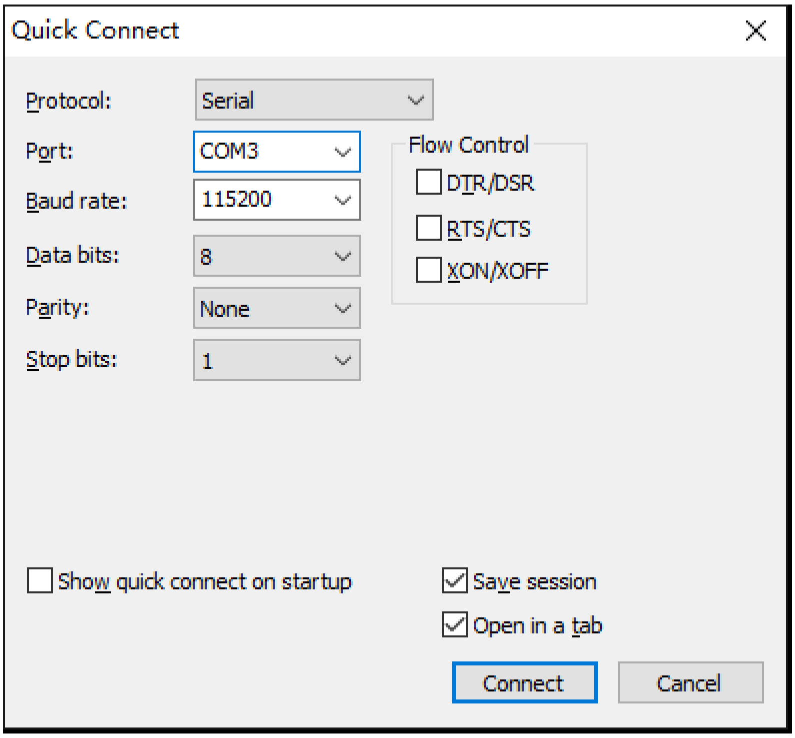
If a PC has only one COM port, it is displayed as COM1 by default. In this case, skip this step.

Right-click **This PC**, choose **Manage** > **Device Manager**, and view COM ports under **Ports (COM & LPT)**.



b Run the SecureCRT software. The **Quick Connect** dialog box is displayed automatically. (If the dialog box is not displayed, click in the menu bar.) In the dialog box, set the connection parameters and click **Connect**. The following table describes the connection parameters that you need to set.

Parameter	**Value**
Protocol	Serial
Port	COM port of the PC identified in the previous step
Baud rate	115200
RTC/CTS	Deselect



Quick Connect

Protocol: Serial

Port: COM3

Baud rate: 115200

Data bits: 8

Parity: None

Stop bits: 1

Flow Control

□ DTR/DSR

□ RTS/CTS

□ XON/XOFF

□ Show quick connect on startup

☑ Save session

☑ Open in a tab

Configuration Verification

Press **Enter** and enter the username **admin** and password **firewall** as prompted. (If you change the password and forget it, restore the initial password. For details, see 2.6 Password Restoration.)

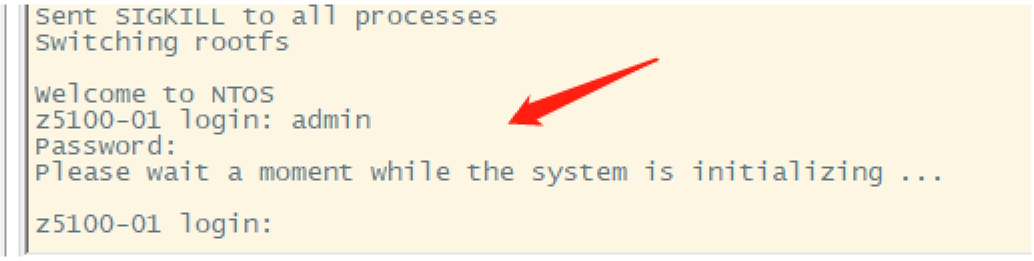
Note

It takes a certain period of time to complete system initialization after the device is powered on and started. You are advised to wait until the system is ready before running CLI commands.

Caution

If you fail to access the CLI, check the configurations as follows:

- Check whether the configuration cable is connected to the console port.
- Check whether the baud rate is set to 115200 for the terminal simulation connection.
- If the preceding configurations are correct, replace the PC, configuration cable, and terminal login software.



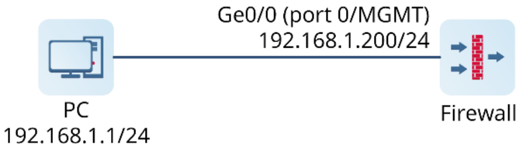
```
Sent SIGKILL to all processes
Switching rootfs

Welcome to NTOS
z5100-01 login: admin
Password:
Please wait a moment while the system is initializing ...

z5100-01 login:
```

2.1.3 Logging In to the Device Using SSH

Application Scenario

When you want to configure the device or collect information in CLI management mode, but you do not have a configuration cable or you are far away from the device, you can remotely log in to the device using SSH.

Network Topology



Configuration Points

To use the SSH login method, the connectivity between the management PC and the management interface address of the device must be ensured. After the ping function is enabled on the interface, the management PC must be able to ping the management interface.

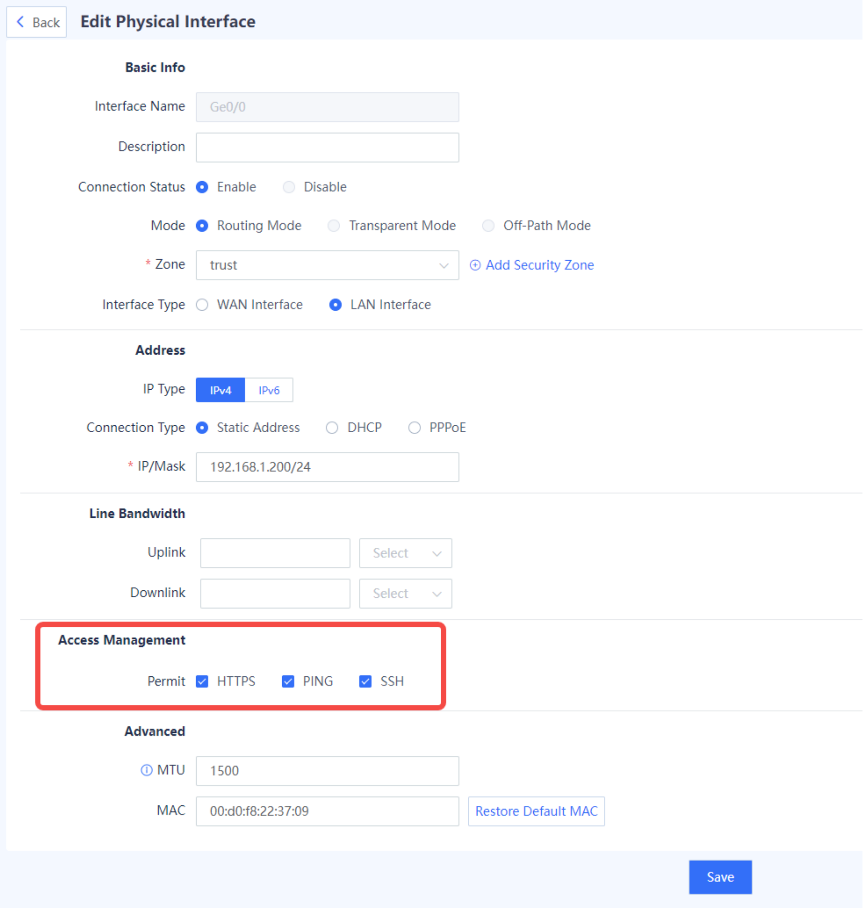
(1) Enable the SSH function on the interface.

(2) Manage the device using SSH.

Procedure

(1) Enable the SSH management function on the interface.

a Choose **Network** > **Interface** > **Physical Interface** and edit **Ge0/0** (port 0/MGMT), as shown in the following figure.



< Back **Edit Physical Interface**

Basic Info

Interface Name: Ge0/0

Description:

Connection Status: ● Enable ○ Disable

Mode: ● Routing Mode ○ Transparent Mode ○ Off-Path Mode

* Zone: trust ⊕ Add Security Zone

Interface Type: ○ WAN Interface ● LAN Interface

Address

IP Type: IPv4 IPv6

Connection Type: ● Static Address ○ DHCP ○ PPPoE

* IP/Mask: 192.168.1.200/24

Line Bandwidth

Uplink: Select

Downlink: Select

Access Management

Permit: ☑ HTTPS ☑ PING ☑ SSH

Advanced

MTU: 1500

MAC: 00:d0:f8:22:37:09 Restore Default MAC

Save

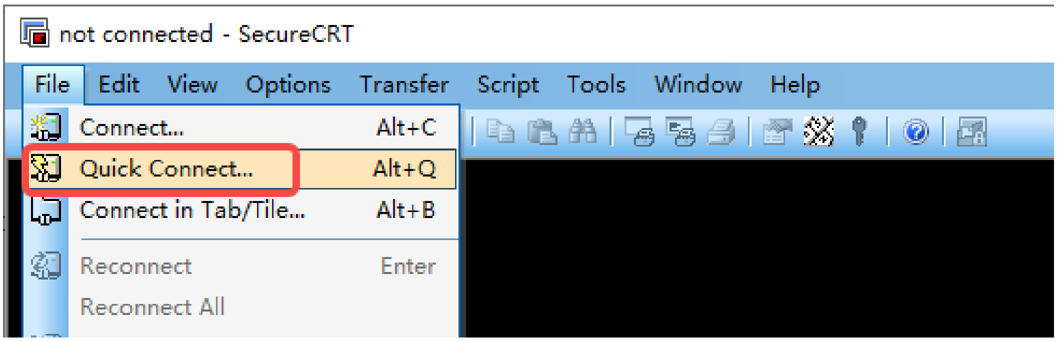
b In the **Access Management** area, select **SSH** (ping function disabled on the interface by default) and click **Save**.

(2) Manage the device using SSH.

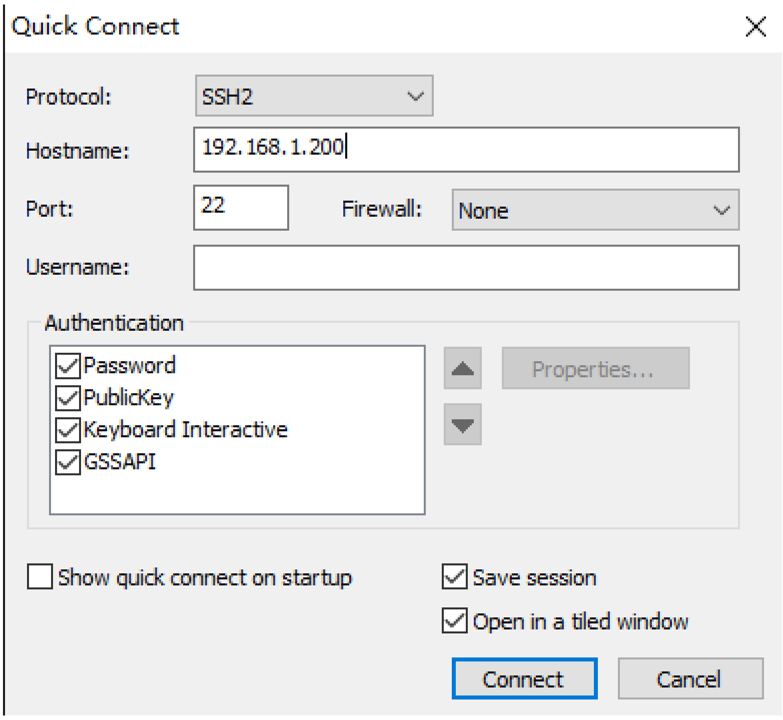
Create an SSH connection using the terminal simulation software (such as SecureCRT), and enter the username and password (for login to the web management page) to manage the device.

The following uses the SecureCRT software as an example.

a Start the SecureCRT software and choose **File** > **Quick Connect**.



b In the **Quick Connect** dialog box, set **Protocol** to **SSH2**, **Hostname** to the management address 192.168.1.200 of the device (that is, IP address of Ge0/0), and **Port** to **22**, retain the default values for other parameters, and click **Connect**.



Quick Connect

Protocol: SSH2

Hostname: 192.168.1.200

Port: 22

Firewall: None

Username:

Authentication

☑ Password

☑ PublicKey

☑ Keyboard Interactive

☑ GSSAPI

□ Show quick connect on startup

☑ Save session

☑ Open in a tiled window

c Enter the username and password (**admin** and **firewall** by default) as prompted to log in to the CLI for configuration management.

2.2 Modifying the Web Login Configuration

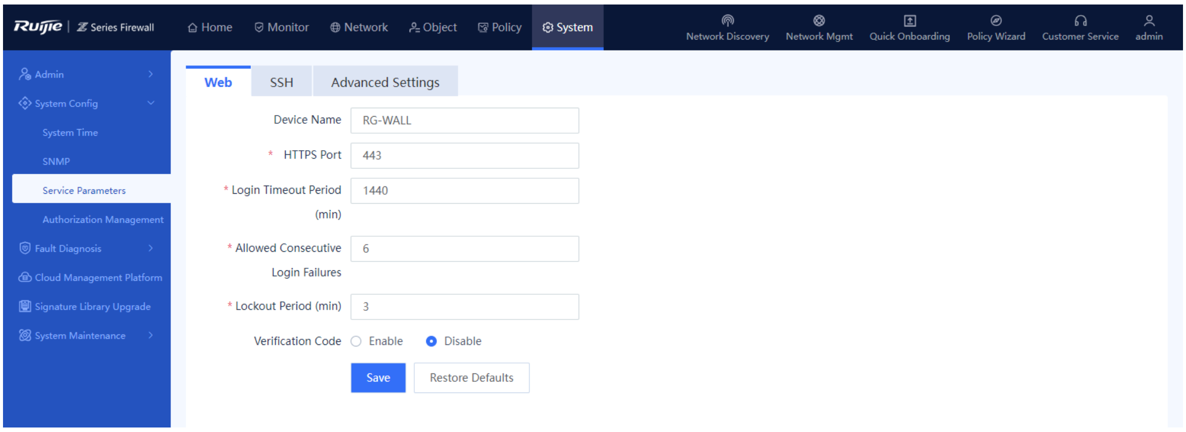
Application Scenario

To improve the login security, the administrator can set web login parameters, for example, locking the administrator account if the number of incorrect password attempts exceeds the specified number. These parameters improve the login security and reduce the data leakage risks caused by password leakage.

Procedure

(1) Choose **System** > **System Config** > **Service Parameters** and click the **Web** tab.

(2) Customize the web service configuration.



Device Name: RG-WALL

* HTTPS Port: 443

* Login Timeout Period (min): 1440

* Allowed Consecutive Login Failures: 6

* Lockout Period (min): 3

Verification Code: ○ Enable ● Disable

Save | Restore Defaults

Item	Description	Remarks
Device Name	Name of the device. In integrated deployment on Ruijie Cloud, you can view the modified device name on the Ruijie Cloud platform and master device. For details about integrated deployment on Ruijie Cloud, see 6.1 Integrated Deployment on Ruijie Cloud.	[Example] RG-WALL
HTTPS Port	Port number used by the web service.	The default value is 443. [Example] 443
Login Timeout Period	Period of time within which if no operation is performed after login to the web management page. The system displays a prompt of login timeout when the administrator tries to log in to the web management page again.	● Enter an integer in the range of 0 to 1440, in minutes. ● The default value is 30 minutes. [Example] 30
Allowed Consecutive Login Failures	Number of consecutive incorrect password attempts. If a user enters an incorrect password for a number of times exceeding the value specified by this parameter, the system automatically locks the user.	● Enter an integer in the range of 0 to 10. ● The default value is 6. [Example] 3
Lockout Period	Period of time within which the automatically locked user is not allowed to log in to the web management page.	● Enter an integer in the range of 0 to 30, in minutes. ● The default value is 3. [Example] 30

Verification Code	Whether a verification code is required for login to the web management page.	By default, the value is **Enable**. [Example] **Enable**

(3) Click **Save**.

2.3 Account Permission Settings

2.3.1 Administrator Permission Overview

Upon factory delivery, the system provides the following default administrator roles: Super Admin, Security Admin, Auditor, and User Admin. The permissions of the default roles are described in Table 2-2.

Table 2-2 Permissions of the Default Roles

Role Type	Permission	Default Account
Super Admin	Read-write permissions on all menus of the web page	admin
Security Admin	No permission on **Admin** menus under **System** Read-write permissions on other menus	securityadmin
Auditor	Read permission on **Home** menus Read permission on **Monitor** menus No permissions on other menus	auditadmin
User Admin	Read permission on **Home** menus Read-write permissions on **Admin** menus under **System** No permissions on other menus	useradmin

2.3.2 Enabling Default Accounts

Application Scenario

The system default administrator accounts **securityadmin**, **auditadmin**, and **useradmin** take effect after they are enabled and passwords are set for them.

Note

The account **admin** can be used immediately after factory delivery, without the need for the following operations.

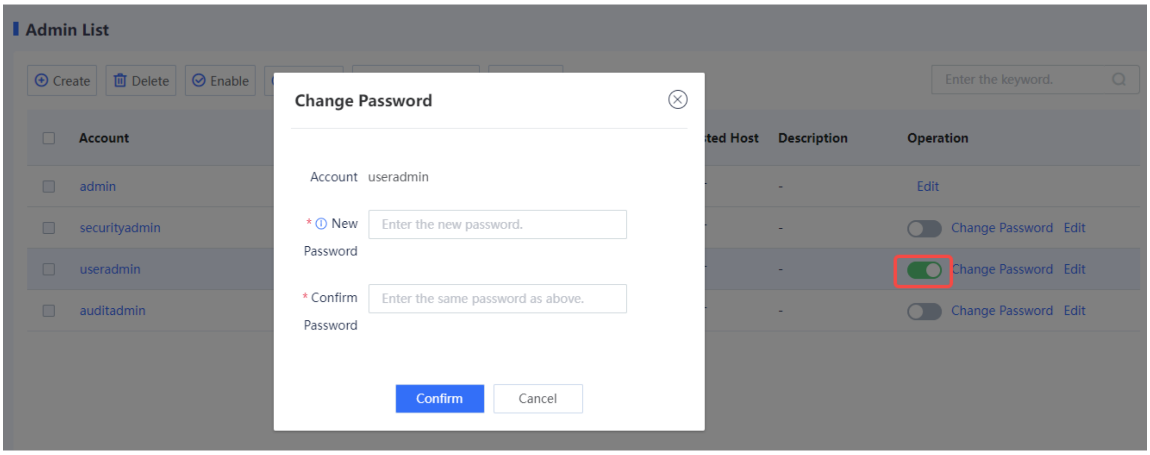
Procedure

(1) Choose **System** > **Admin**.

The system displays the default accounts.

(2) Select a default account to be enabled and set its status to **Enable**.

The **Change Password** dialog box is displayed.



Account	ted Host	Description	Operation
admin	-	-	Edit
securityadmin	-	-	Change Password Edit
useradmin	-	-	Change Password Edit
auditadmin	-	-	Change Password Edit

Account useradmin

(3) Set a new password for the account and enter the password again for confirmation.

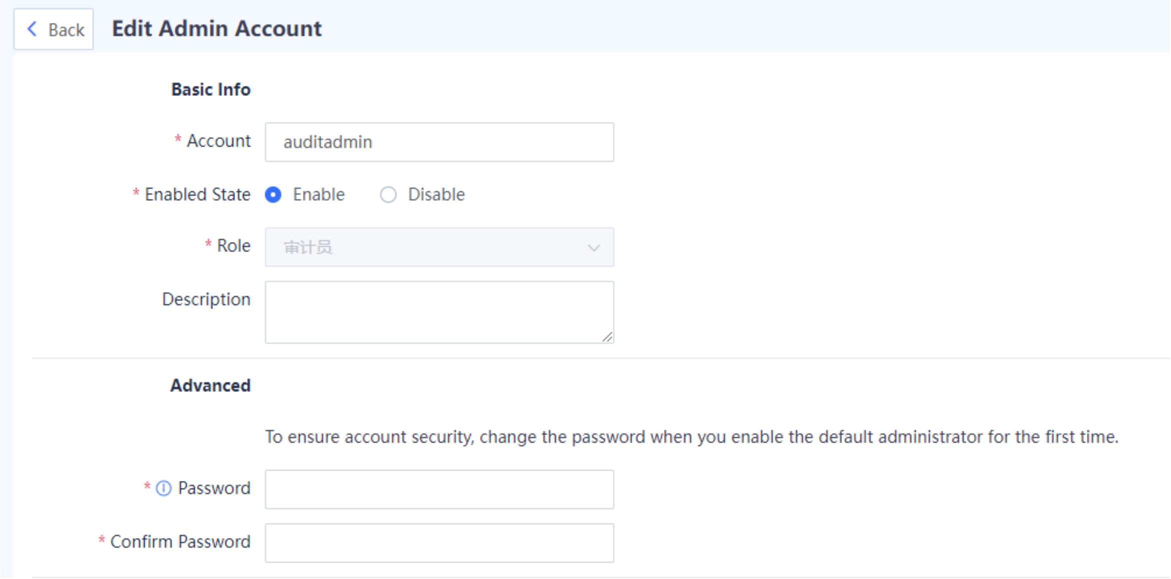
Password description:

- A password must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters.
- A password cannot contain any Chinese character, space, or full-width character.
- Password length range: 8–15 characters
- A password cannot be the same as the username or the username in reverse order.

(4) Click **Confirm**.

Follow-up Procedure

- In the administrator list, find the target account and click **Edit**. On the **Edit Admin Account** page, modify the default account and description to that can be easily identified.



< Back **Edit Admin Account**

Basic Info

* Account: auditadmin

* Enabled State: ● Enable ○ Disable

* Role: 审计员

Description:

Advanced

To ensure account security, change the password when you enable the default administrator for the first time.

* Password:

* Confirm Password:

- The default administrator account cannot be deleted.

2.3.3 Creating an Administrator

1. Creating an Administrator Role

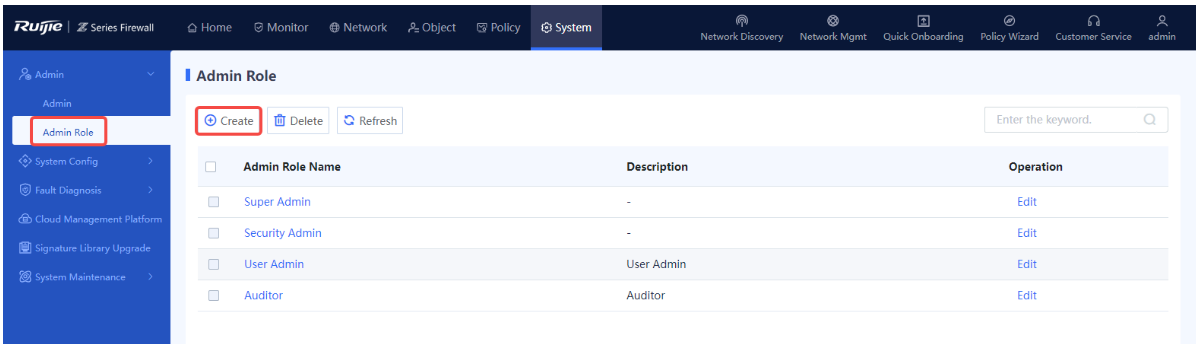
Application Scenario

The user scenario grants different permissions to different roles to implement level- and rights-based management. You can customize administrator roles and grant permissions to the roles as required.

Procedure

(1) Choose **System** > **Admin Role**.

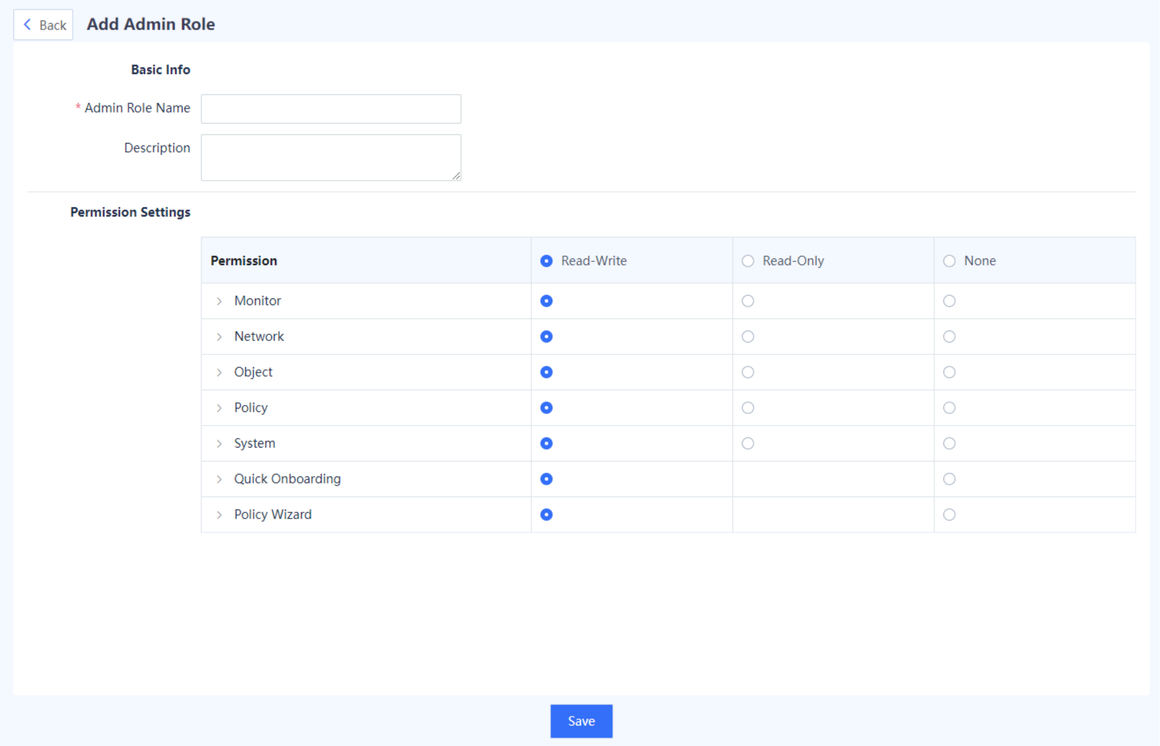
(2) In the operation area, click **Create**.



Admin Role

□	Admin Role Name	Description	Operation
□	Super Admin	-	Edit
□	Security Admin	-	Edit
□	User Admin	User Admin	Edit
□	Auditor	Auditor	Edit

(3) Set a new role and grant permissions to the role.



Basic Info

* Admin Role Name

Description

Permission Settings

Permission	● Read-Write	○ Read-Only	○ None
› Monitor	●	○	○
› Network	●	○	○
› Object	●	○	○
› Policy	●	○	○
› System	●	○	○
› Quick Onboarding	●		○
› Policy Wizard	●		○

Item	Description	Remarks
Admin Role Name	Name of the role, which is used to identify the role.	[Example] Security Admin
Description	Description of the role, which distinguishes role permissions.	[Example] New
Permission Settings		
Permission	Web page functions that can be operated by the new administrator role.	[Example] Monitor
Permission Settings	Different modules have different permissions, including: **Read-Write**: View, add, delete, and edit permissions **Read-Only**: View permission only	[Example] Read-Only

Item	Description	Remarks
	None: No permission at all	

(4) Click **Save**. A role is created.

2. Creating an Administrator Account

Application Scenario

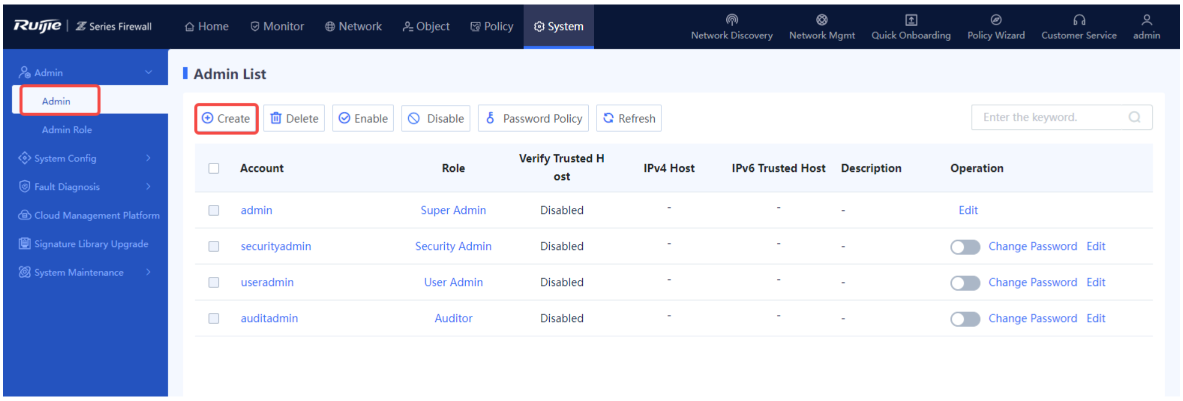
With the increase of device administrators, the Super Admin can create a new administrator account and specify a role for the account.

After the new administrator logs in to the device, the administrator can only view or manage modules of the corresponding role.

Procedure

(1) Choose **System** > **Admin**.

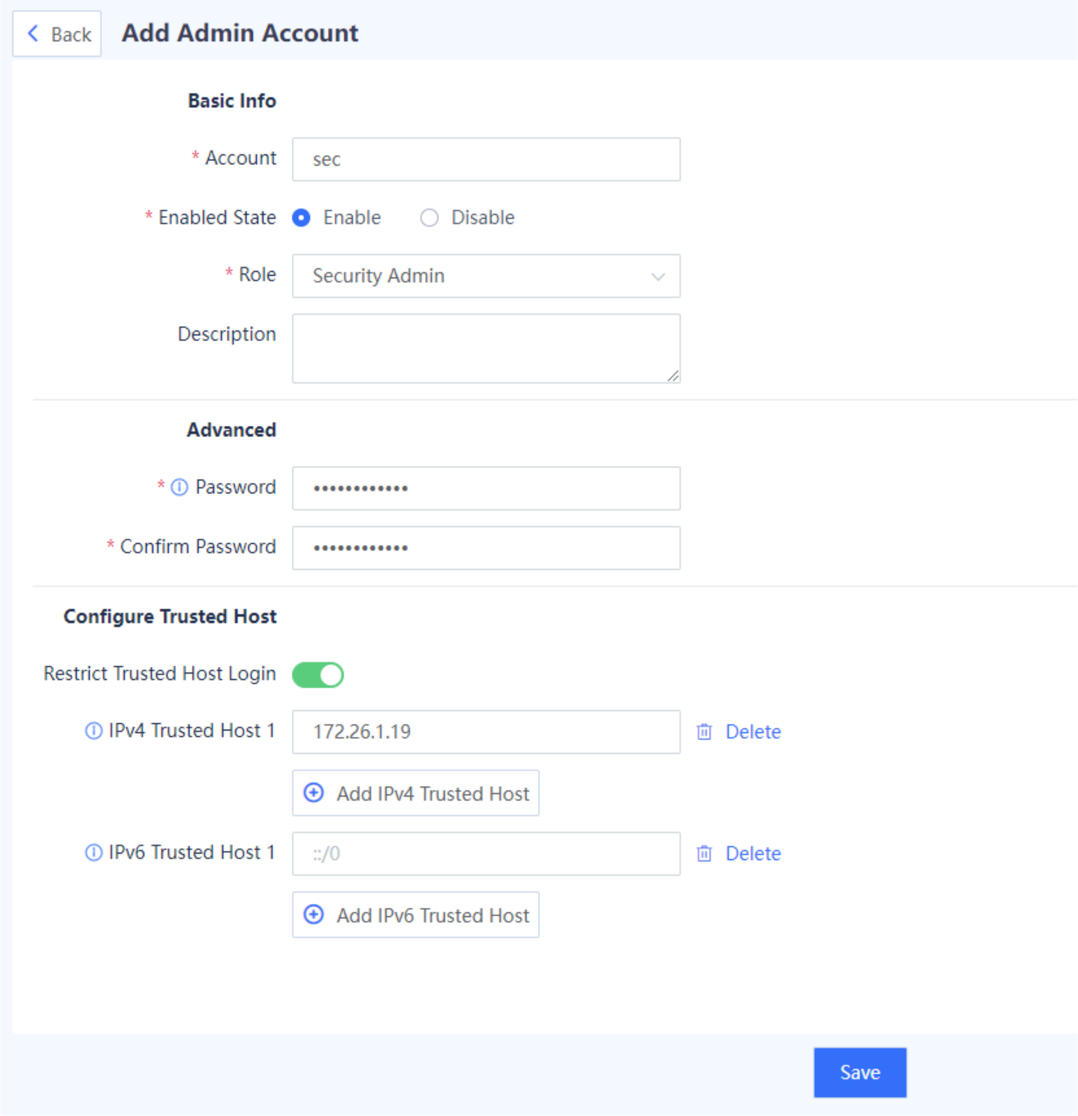
(2) Above the operation area, click **Create**.



Admin List

□	Account	Role	Verify Trusted Host	IPv4 Host	IPv6 Trusted Host	Description	Operation
□	admin	Super Admin	Disabled	-	-	-	Edit
□	securityadmin	Security Admin	Disabled	-	-	-	Change Password Edit
□	useradmin	User Admin	Disabled	-	-	-	Change Password Edit
□	auditadmin	Auditor	Disabled	-	-	-	Change Password Edit

(3) Enter the basic information and select a role.



Back Add Admin Account

Basic Info

* Account: sec

* Enabled State: ● Enable ○ Disable

* Role: Security Admin

Description:

Advanced

* Password: ••••••••••••

* Confirm Password: ••••••••••••

Configure Trusted Host

Restrict Trusted Host Login: ●

IPv4 Trusted Host 1: 172.26.1.19 Delete

Add IPv4 Trusted Host

IPv6 Trusted Host 1: ::/0 Delete

Add IPv6 Trusted Host

Save

Item	Description	Remarks
Basic Info		
Account	Username of the created administrator.	● The username can contain letters, digits, and underscores (_), and must start with a letter. ● The value cannot be the same as an existing administrator username. [Example]

Item	Description	Remarks
		Admin_security
Enabled State	Whether to enable the new administrator account.	[Example] Enable
Role	Role of the new administrator, which specifies the operation permissions of the administrator.	[Example] Security Admin
Description	Description of the new administrator.	Any character is supported. [Example] With the security monitor permission
Advanced		
Password	Password used by the new administrator to log in to the web UI.	The password is a string of 8 to 15 characters. Any character is supported. [Example] admin@123
Confirm Password	Enter the login password again.	The value of Confirm Password must be the same as that of Password. [Example] admin@123
Configure Trusted Host		
Restrict Trusted Host Login	If this function is enabled, the account can only log in to the firewall using a specified IP address (trusted host).	[Example] Enable
IPv4 Trusted	Enter the IPv4 address of a trusted	[Example]

Item	Description	Remarks
Host 1	host.	192.168.1.1
IPv6 Trusted Host 1	Enter the IPv6 address of a trusted host.	[Example] 333:444:0:1::1

(4) Click **Save**. An administrator account is created.

2.3.4 Changing the Password

1. Modifying the Administrator Password Security Policy

Application Scenario

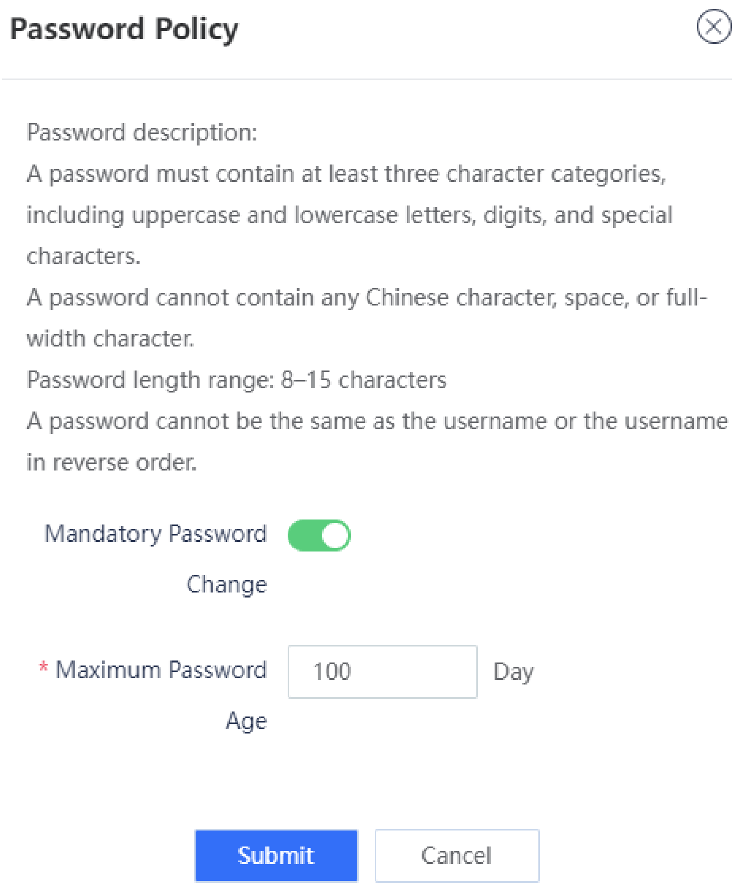
To ensure the security of an administrator password, the account and password must be modified periodically. You can set a validity period for a password. After a password expires, the system forces the user to change the password.

Procedure

(1) Access the **Password Policy** page.

a Choose **System** > **Admin**.

b Above the operation area, click **Password Policy**.



Password Policy

Password description:
A password must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters.
A password cannot contain any Chinese character, space, or full-width character.
Password length range: 8–15 characters
A password cannot be the same as the username or the username in reverse order.

Mandatory Password Change: On

* Maximum Password Age: 100 Day

(2) Enable **Mandatory Password Change**.

(3) Set **Maximum Password Age**.

(4) Click **Submit**.

Follow-up Procedure

When a password is used for a period of time longer than that limited by the system, the system forces you to change the administrator password.

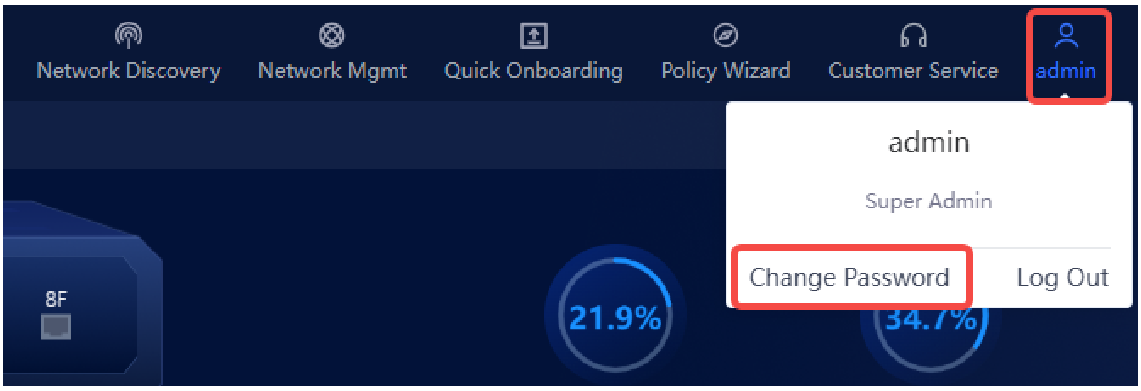
2. Changing the Default User Password of the Super Admin

Application Scenario

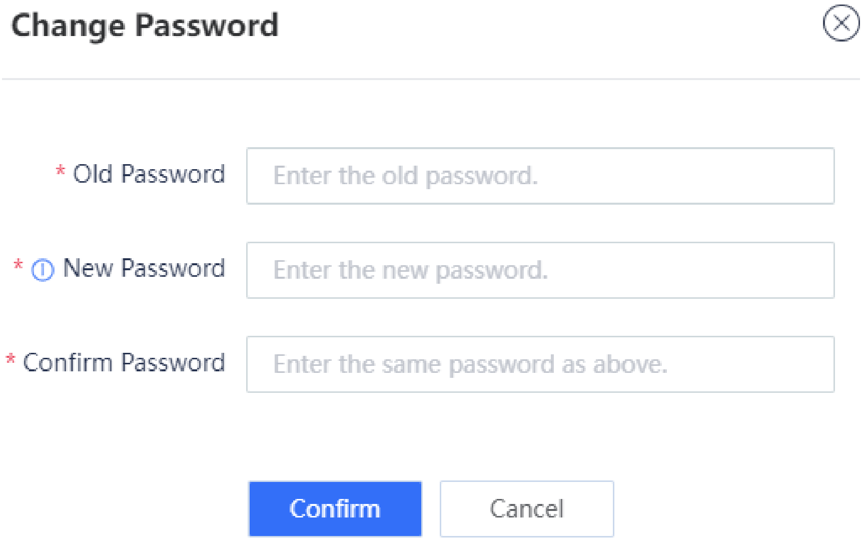
Upon factory delivery, the default password of the Super Admin account **admin** is **firewall**. To ensure the account security, you must change the default password of the account **admin** in time.

Procedure

(5) In the title and panel area, click the name of the login user and choose **Change Password** from the short-cut menu.



(6) In the **Change Password** dialog box, enter the old password, new password, and confirm password.



Item	Description	Remarks
Old Password	Password used by the login user.	You need to obtain the password of the login user in advance.
New Password	Password after change.	The new password must meet the following requirements: ● Contain 8 to 15 characters. ● Contain at least three types of the following: uppercase letters, lowercase letters, digits, and special characters, and

		cannot contain Chinese characters, spaces, or full-width characters. ● Cannot be the same as the username or the username in reverse order.
Confirm Password	Password after change that is entered again.	The value of **Confirm Password** must be the same as that of **New Password**.

(7) Click **Confirm**.

3. Changing the Password of Administrators Except the Super Admin

Application Scenario

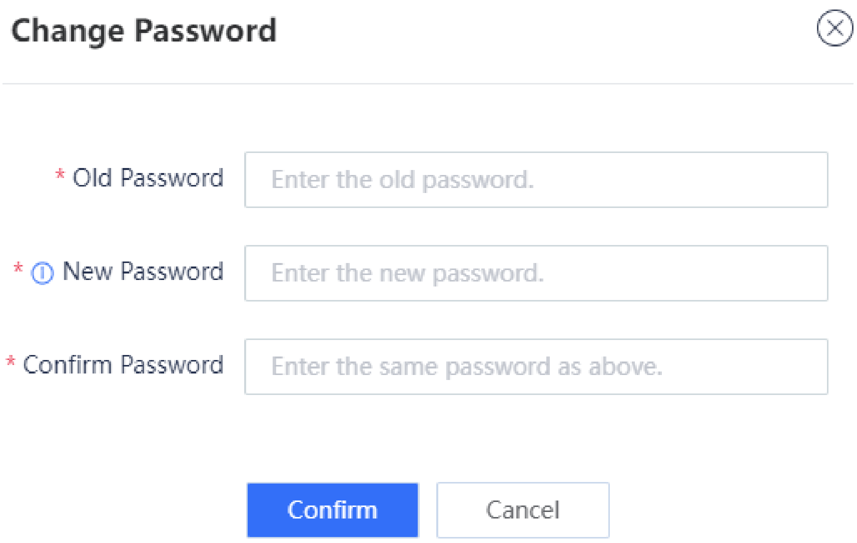
When other administrators forget their passwords or want to change their passwords to improve the security, the Super Admin can change the password for them.

Procedure

(1) Choose **System** > **Admin**.

(2) Select the administrator whose password needs to be changed and click **Change Password** in the **Operation** column.

The **Change Password** dialog box is displayed.



Change Password

* Old Password: Enter the old password.

* New Password: Enter the new password.

* Confirm Password: Enter the same password as above.

(3) Set a new password for the administrator.

The new password must meet the following requirements:

- Contain 8 to 15 characters.
- Contain at least three types of the following: uppercase letters, lowercase letters, digits, and special characters, and cannot contain Chinese characters, spaces, or full-width characters.
- Cannot be the same as the username or the username in reverse order.

(4) Click **Confirm**.

2.4 Configuration Backup and Restoration

2.4.1 Exporting the Configuration

Application Scenario

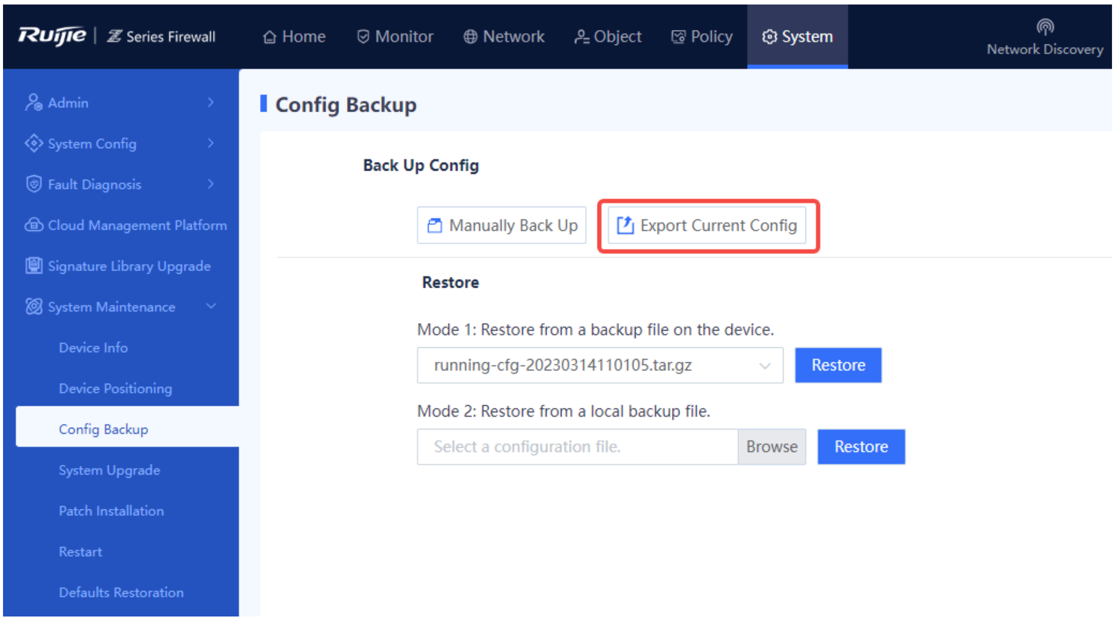
An administrator can use the configuration backup function to manually back up the current configuration or export the current system configuration file to facilitate subsequent restoration or batch configuration.

Procedure

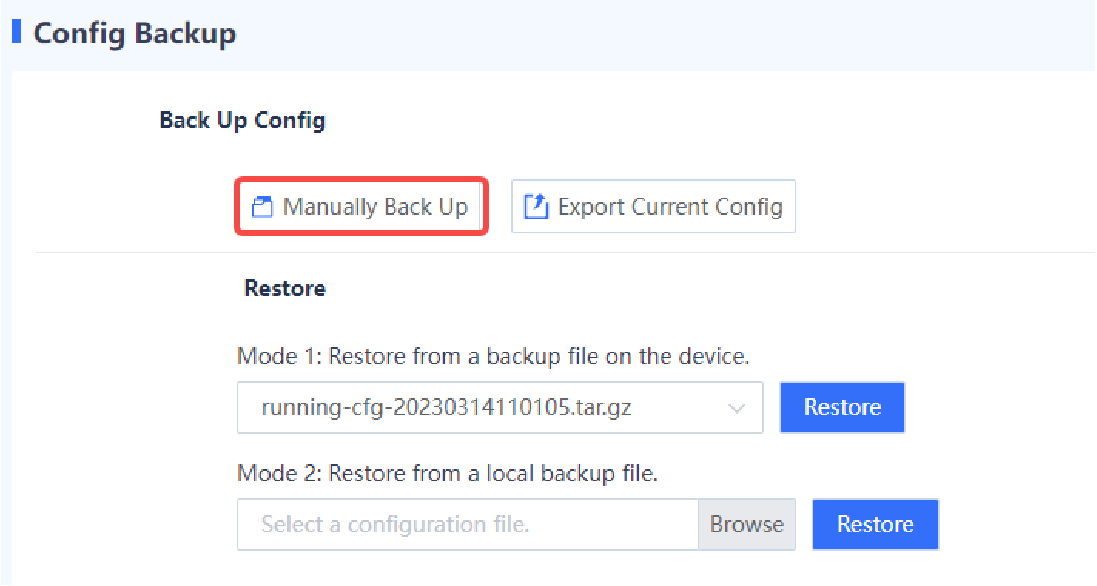
(1) Choose **System** > **System Maintenance** > **Config Backup**.

(2) Back up the configuration using either of the following methods:

- Click **Export Current Config** to download the configuration file.



- Click **Manually Back Up** to save the current configuration file to the firewall.



Config Backup

Back Up Config

Restore

Mode 1: Restore from a backup file on the device.

running-cfg-20230314110105.tar.gz

Mode 2: Restore from a local backup file.

Select a configuration file.

2.4.2 Importing the Configuration

Application Scenario

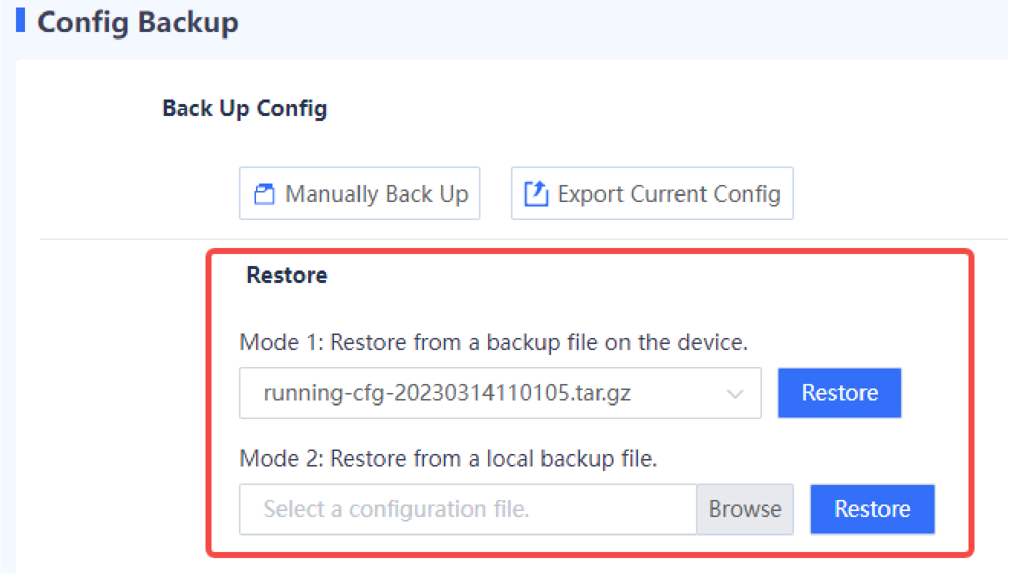
You can import the backup configuration file in the following scenarios to implement quick restoration and deployment.

- After a device restores from a fault, import the backup configuration file to facilitate quick restoration and deployment.
- When you deploy a new device in the same network environment, import the configuration file of another device to implement quick deployment.

Procedure

(1) Choose **System** > **System Maintenance** > **Config Backup**.

(2) In the **Restore** area, you can restore from a backup file on the device or click **Browse** to select a local backup file.



Config Backup

Back Up Config

Restore

Mode 1: Restore from a backup file on the device.

running-cfg-20230314110105.tar.gz

Mode 2: Restore from a local backup file.

Select a configuration file.

(3) Click **Restore** to import the backup configuration to the current device.

Follow-up Procedure

After a configuration file is imported, the device automatically restarts to make the configuration take effect.

2.5 Defaults Restoration

You can perform the defaults restoration operation when you want to delete all configurations of the device. The Z-S series firewall supports web-based one-click restoration and restoration by pressing the Reset button.

⚠ **Caution**

The defaults restoration operation clears all the configurations. Before you perform this operation, back up the configurations in time.

2.5.1 Web-based One-Click Restoration

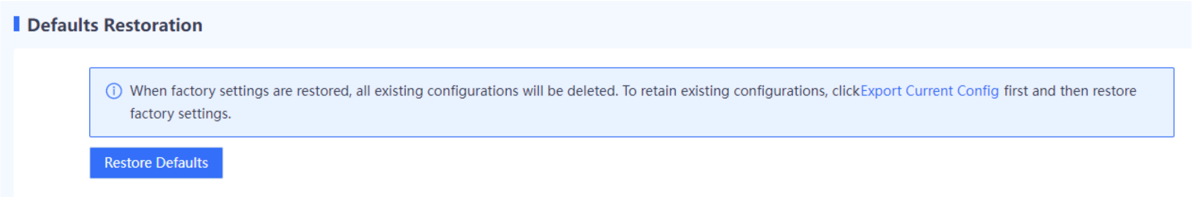
Application Scenario

When you are unable to operate the hardware directly in the equipment room, you can perform the defaults restoration operation on the web management page.

Procedure

(4) Choose **System** > **System Maintenance** > **Defaults Restoration**.

(5) Click **Restore Defaults**.



Defaults Restoration

ⓘ When factory settings are restored, all existing configurations will be deleted. To retain existing configurations, clickExport Current Config first and then restore factory settings.

Follow-up Procedure

The device automatically restarts. After the restart, all configurations of the device are restored to factory defaults.

2.5.2 Restoration by Pressing the Reset Button

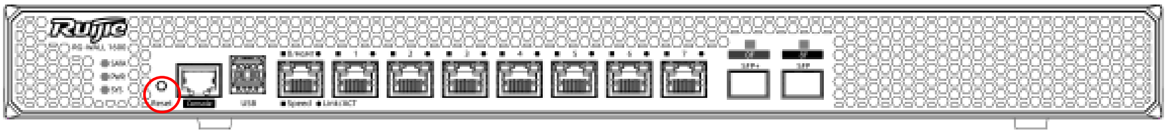
Application Scenario

When you can maintain the device in the equipment room, press the Reset button on the device to restore factory defaults.

Procedure

Press and hold the Reset button on the device (for over 5s). The Reset button is located on the front panel of the device, as shown in Figure 2-4.

Figure 2-4 Reset Button on the Front Panel



Follow-up Procedure

The device automatically restarts. After the restart, all configurations of the device are restored to factory defaults.

Note

The Reset button provides the following functions:

- Device restart: Press and hold for less than 3s.
- Defaults restoration: Press and hold for over 5s.

Both of the preceding two operations will initiate one-click collection. After the restart, you can log in to the web management page and choose **System** > **Fault Diagnosis** > **One-Click Collection** to download the device status information.

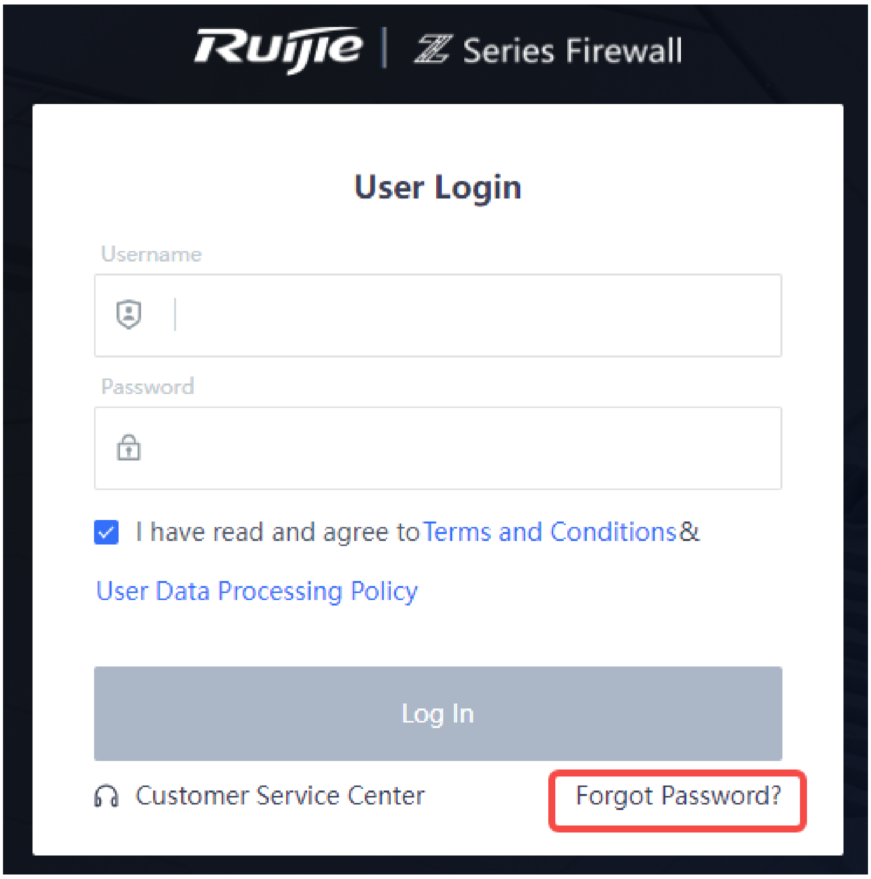
2.6 Password Restoration

Application Scenario

When the administrator forgets the login password, you can restore the current password to the default password.

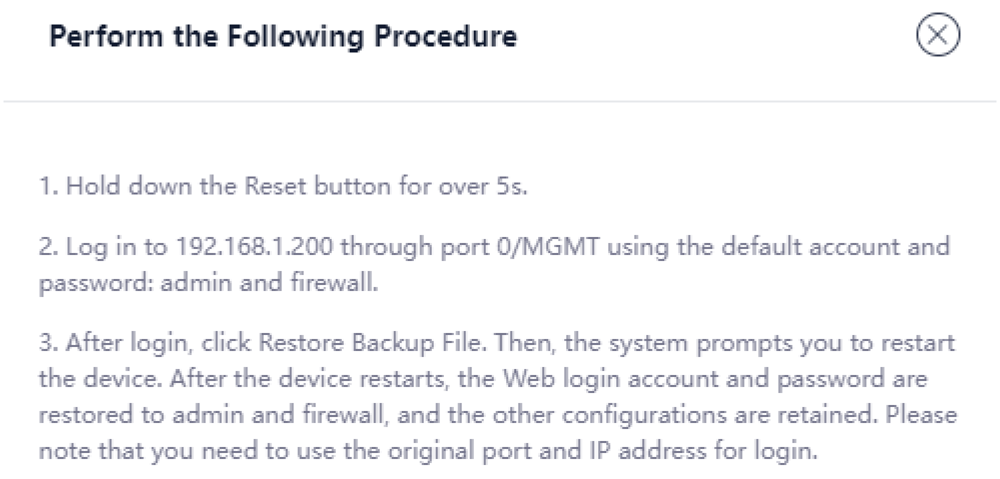
Procedure

(1) Access the **User Login** page of the web management platform.


Ruijie | Z Series Firewall
User Login
Username
Password
☑ I have read and agree to Terms and Conditions &
User Data Processing Policy
Log In
Customer Service Center
Forgot Password?

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

(3) Perform the operation as instructed on the page.



Perform the Following Procedure

1. Hold down the Reset button for over 5s.

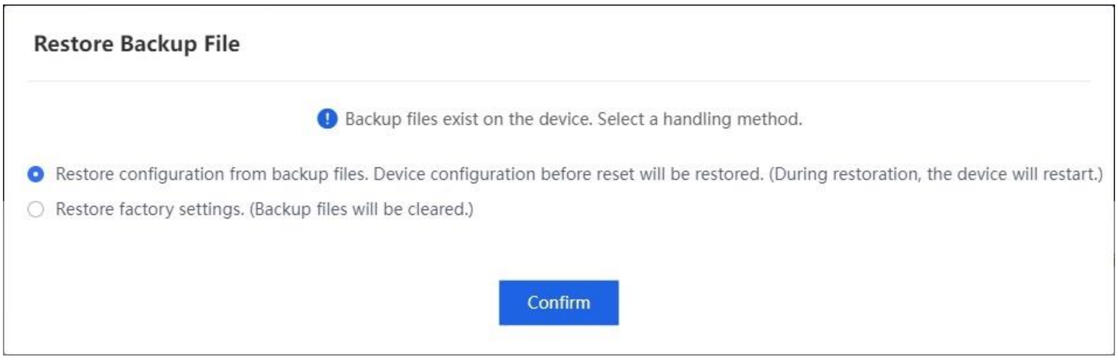
2. Log in to 192.168.1.200 through port 0/MGMT using the default account and password: admin and firewall.

3. After login, click Restore Backup File. Then, the system prompts you to restart the device. After the device restarts, the Web login account and password are restored to admin and firewall, and the other configurations are retained. Please note that you need to use the original port and IP address for login.

a Hold down the Reset button for over 5s until the device is restored to the factory mode.

b Connect the management PC to port 0/MGMT on the device panel through a network cable and set the IP address of the PC to one in the same network segment as that of port 0/MGMT (default address: 192.168.1.200), such as 192.168.1.201. Log in to https://192.168.1.200 and enter the default username and password (**admin** and **firewall**).

c After login, click **Restore Backup File**. Then, the system prompts you to restart the device. After the device restarts, the web login account and password are restored to **admin** and **firewall**, and the other configurations are retained.

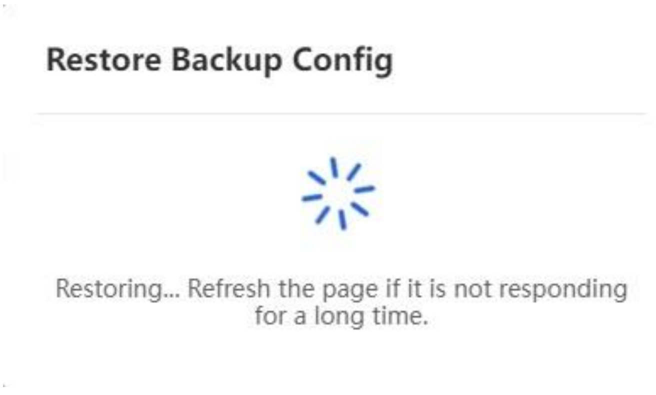


Restore Backup File

Backup files exist on the device. Select a handling method.

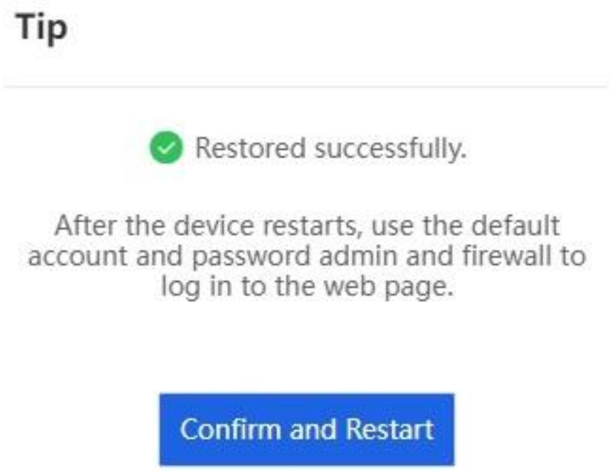
● Restore configuration from backup files. Device configuration before reset will be restored. (During restoration, the device will restart.)

○ Restore factory settings. (Backup files will be cleared.)



Restore Backup Config

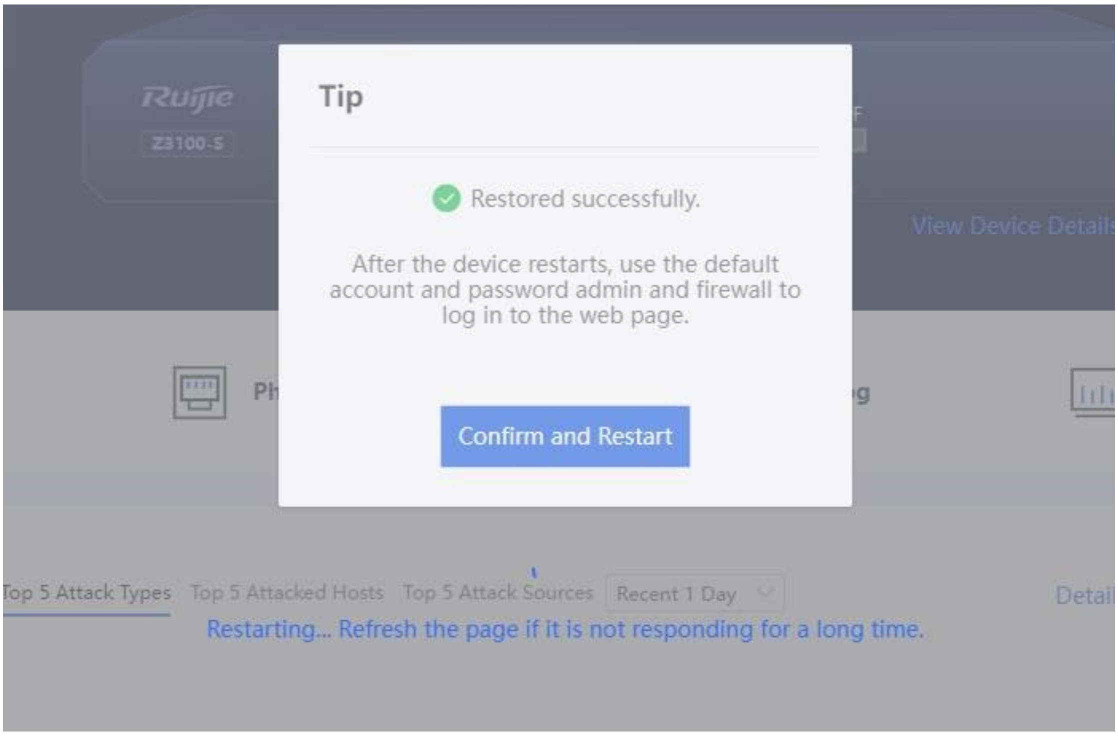
Restoring... Refresh the page if it is not responding for a long time.



Tip

Restored successfully.

After the device restarts, use the default account and password admin and firewall to log in to the web page.

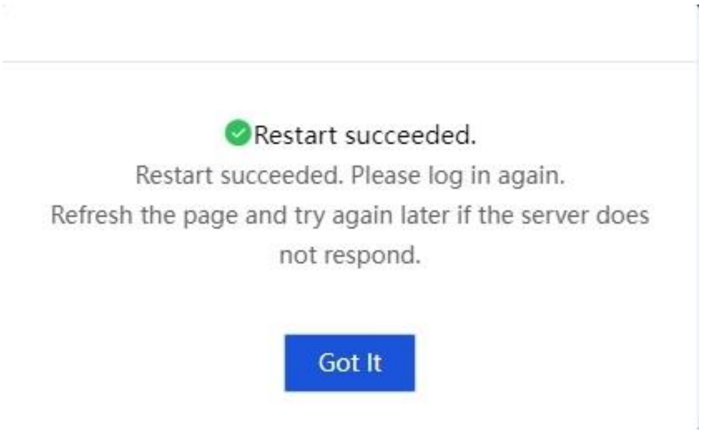


Tip

Restored successfully.

After the device restarts, use the default account and password admin and firewall to log in to the web page.

Restarting... Refresh the page if it is not responding for a long time.

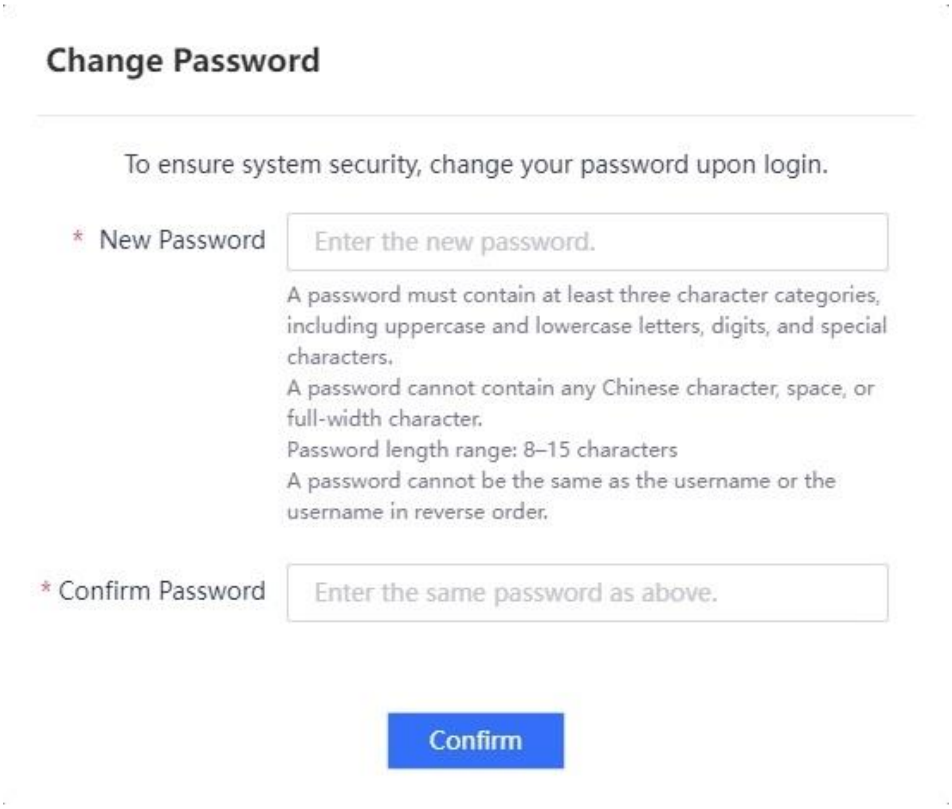


Restart succeeded.

Restart succeeded. Please log in again.

Refresh the page and try again later if the server does not respond.

d Log in to the device using the default account and password (**admin** and **firewall**) and change the password as required.



Change Password

To ensure system security, change your password upon login.

* New Password: Enter the new password.

A password must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters.

A password cannot contain any Chinese character, space, or full-width character.

Password length range: 8–15 characters

A password cannot be the same as the username or the username in reverse order.

* Confirm Password: Enter the same password as above.

2.7 SNMP Management

2.7.1 Overview

Simple Network Management Protocol (SNMP) is a protocol used for network monitoring and management. SNMP allows the network administrators to perform information query, network configuration, fault locating, and capacity planning for nodes on the network for efficient and batch management of network devices.

The firewall supports basic SNMP functions, allows administrators to manage devices on the third-party platform using SNMP, and enables devices to actively report alarms to the network management system (NMS) server.

The firewall supports the following SNMP versions:

- SNMPv1

  SNMPv1 is the first officially released SNMP version, which is defined in RFC 1157. SNMPv1 performs authentication based on the community name. The serial management interface (SMI) and Management Information Base (MIB) of SNMPv1 are simple, with low security.

- SNMPv2c

  SNMPv2c is a community-based management architecture, which is defined in RFC 1901. SNMPv2c is compatible with SNMPv1 and provides two more protocol operations (GetBulk and Inform) to support more data types and error codes.

- SNMPv3

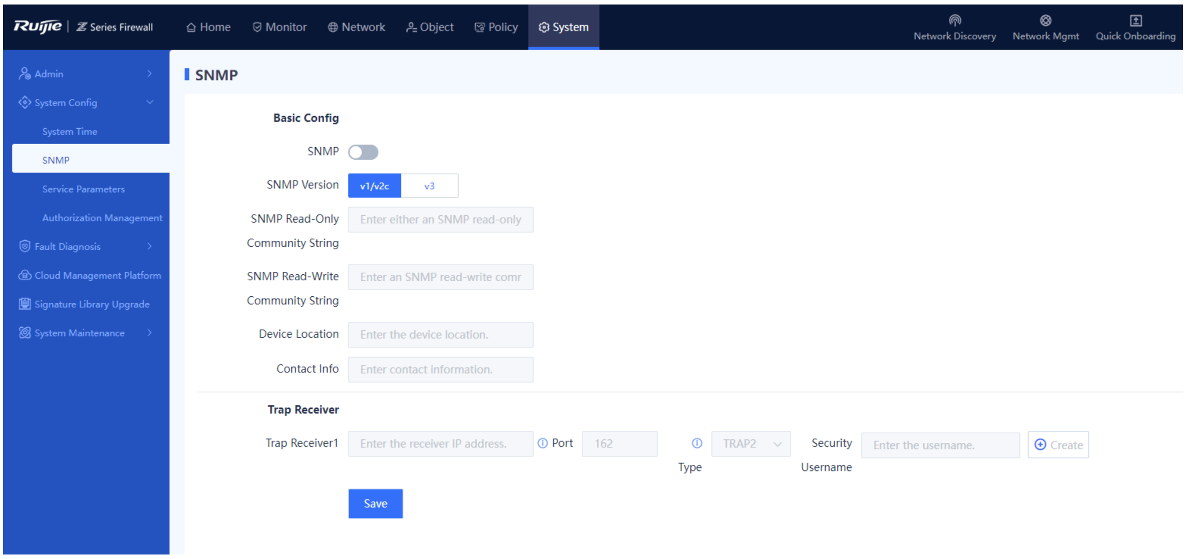
  SNMPv3 defines extended security capabilities and provides the following security features through data identification and encryption:

  - Ensures that data is not tampered during the transmission.
  - Ensures that data is sent by a valid data source.
  - Encrypts packets to ensure data confidentiality.

2.7.2 Configuring SNMP

(1) Access the **SNMP** configuration page.

Choose **System** > **System Config** > **SNMP**.



SNMP

Basic Config

SNMP

SNMP Version: v1/v2c | v3

SNMP Read-Only Community String: Enter either an SNMP read-only

SNMP Read-Write Community String: Enter an SNMP read-write comr

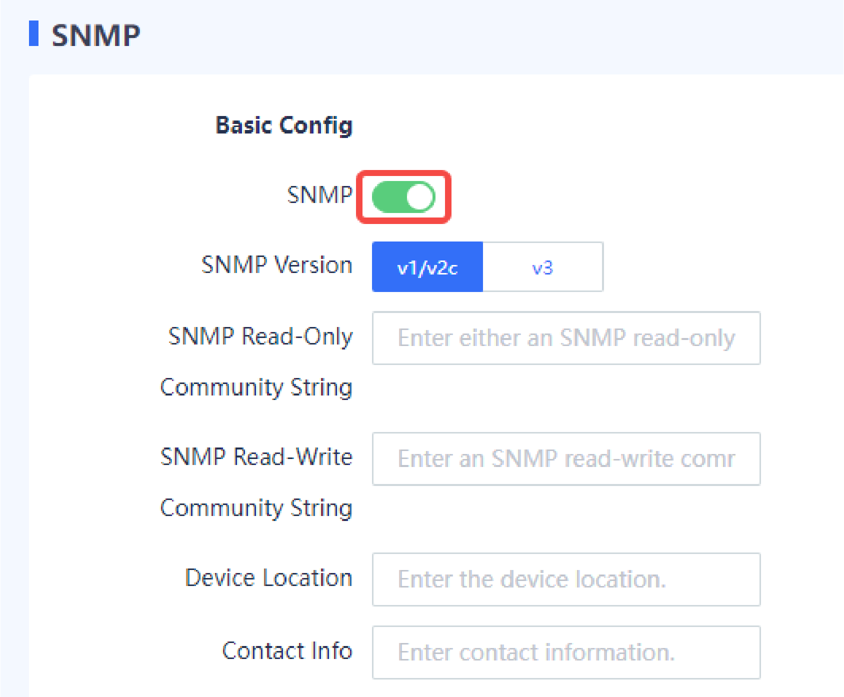
Device Location: Enter the device location.

Contact Info: Enter contact information.

Trap Receiver

Trap Receiver1: Enter the receiver IP address. Port: 162 Type: TRAP2 Security Username: Enter the username.

(2) Enable **SNMP**.



SNMP

Basic Config

SNMP

SNMP Version: v1/v2c | v3

SNMP Read-Only Community String: Enter either an SNMP read-only

SNMP Read-Write Community String: Enter an SNMP read-write comr

Device Location: Enter the device location.

Contact Info: Enter contact information.

(3) Configure parameters for interconnecting the firewall and NMS server.

Item	Description	Remarks
SNMP Version	Version number of SNMP. The options are **v1/v2c** and **v3**.	The selected version must match that of the NMS server. [Example]

<table>
<tr><th>Item</th><th>Description</th><th>Remarks</th></tr>
<tr><td></td><td></td><td>v3</td></tr>
<tr><td colspan="3">SNMP Version: v1/v2c</td></tr>
<tr><td>SNMP Read-Only Community String</td><td>Community name used for authentication between the managed device and NMS server.
If the NMS user uses a read-only community name for authentication, the user possesses the read-only permission to query device information.</td><td>The value must be the same as the read-only community name on the NMS. Otherwise, access from the NMS to the device may fail.
Characters such as `~!#%^&*+\|{};:'"/<>? and spaces are not allowed.
[Example]
public</td></tr>
<tr><td>SNMP Read-Write Community String</td><td>Community name used for authentication between the managed device and NMS server.
If the NMS user uses a read-write community name for authentication, the user possesses the read-write permission on device configuration.</td><td>The value must be the same as the read-write community name on the NMS. Otherwise, access from the NMS to the device may fail.
Characters such as `~!#%^&*+\|{};:'"/<>? and spaces are not allowed.
[Example]
private</td></tr>
<tr><td colspan="3">SNMP Version: v3</td></tr>
<tr><td>Security Username</td><td>Username used by the NMS user to access the managed device.</td><td>The value must be the same as that on the NMS.
Characters such as `~!#%^&*+\|{};:'"/<>? and spaces are not allowed.
[Example]</td></tr>
</table>

Item	Description	Remarks
		user1
Authentication Algorithm	Authentication algorithm used to verify the user identity. MD5 and SHA algorithms are supported.	The value must be the same as that on the NMS. [Example] MD5
Authentication Key	Password used to verify whether the NMS user is valid.	The value must be the same as the authentication password configured on the NMS. [Example] authkey
Encryption Algorithm	Encryption algorithm used to encrypt the transmitted data. AES and DES algorithms are supported.	The value must be the same as that on the NMS. [Example] AES
Encryption Key	Password used to encrypt the transmitted data.	The value must be the same as the encryption password configured on the NMS. [Example] prikey
Device Location	Physical location of the managed device. This information allows the administrator to quickly locate a faulty device.	-
Contact Info	Contact information of the maintenance engineer of the managed device. This information allows the administrator to easily	-

Item	Description	Remarks
	get in touch with the device-related personnel.	
Trap Receiver Click **Create** to add a trap receiver.		
Trap Receiver	Destination host address that receives the Trap message.	[Example] 1.1.1.2
Port	Number of the port used by the managed device to send a Trap message to the destination host. The default value is 162.	[Example] 162
Type	Trap type. The options are **TRAP**, **TRAP2**, and **INFORM**.	The type is **TRAP2** in most cases. [Example] TRAP2
Security Username	Credential used by the device to report alarm information to the NMS server.	The value must be the same as that on the NMS server. [Example] user1

(4) Click **Save**.

3 License Activation

3.1 Authorization Service Overview

After purchasing a device, you can use basic functions of the device. To use value-added functions or expand device resources due to service expansion, you can purchase the corresponding function or resource licenses. License-based authorization can effectively lower costs. You can import licenses based on actual needs to obtain custom functions.

The device supports four types of licenses: function license, performance license, signature library license, and testing license. The following table compares the licenses of different types.

Category	**Industry Attribute**	**Effective Time**	**License Type**	**Description**
Performance license	Yes	Permanent	1 GB capacity per license	The basic forwarding performance is 3 GB, and forwarding capacity can be expanded to 10 GB by importing multiple licenses.
Security license	No	With a validity period	Intrusion Prevention (IPS)	● This license upgrades the IPS signature library of the firewall to identify and protect against various types of in-depth attacks, including vulnerability attack, overflow attack, database attack, advanced threat attack, and brute-force attack. ● Each license provides the upgrade service of the IPS signature library of one year.

Category	Industry Attribute	Effective Time	License Type	Description
			App identification (app/URL)	● This license upgrades the app identification signature library to identify Internet applications and limit and control the Internet application access of users. ● Each license provides the upgrade service of the app identification signature library of one year.
			Antivirus (AV)	● This license provides the virus scan function and upgrades the AV signature library to detect viruses in various types of files transmitted using HTTPS, HTTP, FTP, SMTP, and POP3. ● Each license provides the upgrade service of the AV signature library of one year.
			Threat Intelligence (TI)	● This license upgrades the TI signature library to import instant and global threat intelligence information to the firewall, so that the firewall can identify and defend against advanced threats such as Advanced Persistent Threat (APT) and mining. ● Each license provides the upgrade service of the TI

Category	Industry Attribute	Effective Time	License Type	Description
				signature library of one year.

3.2 Secure Cloud Platform

3.2.1 Overview

As the supporting platform for the Z-S series firewall, the Secure Cloud Platform provides the following functions: license activation, license change, version upgrade, patch upgrade, and security signature library upgrade.

3.2.2 Secure Cloud Platform Operations

1. User Registration and Login

(1) Register a user.

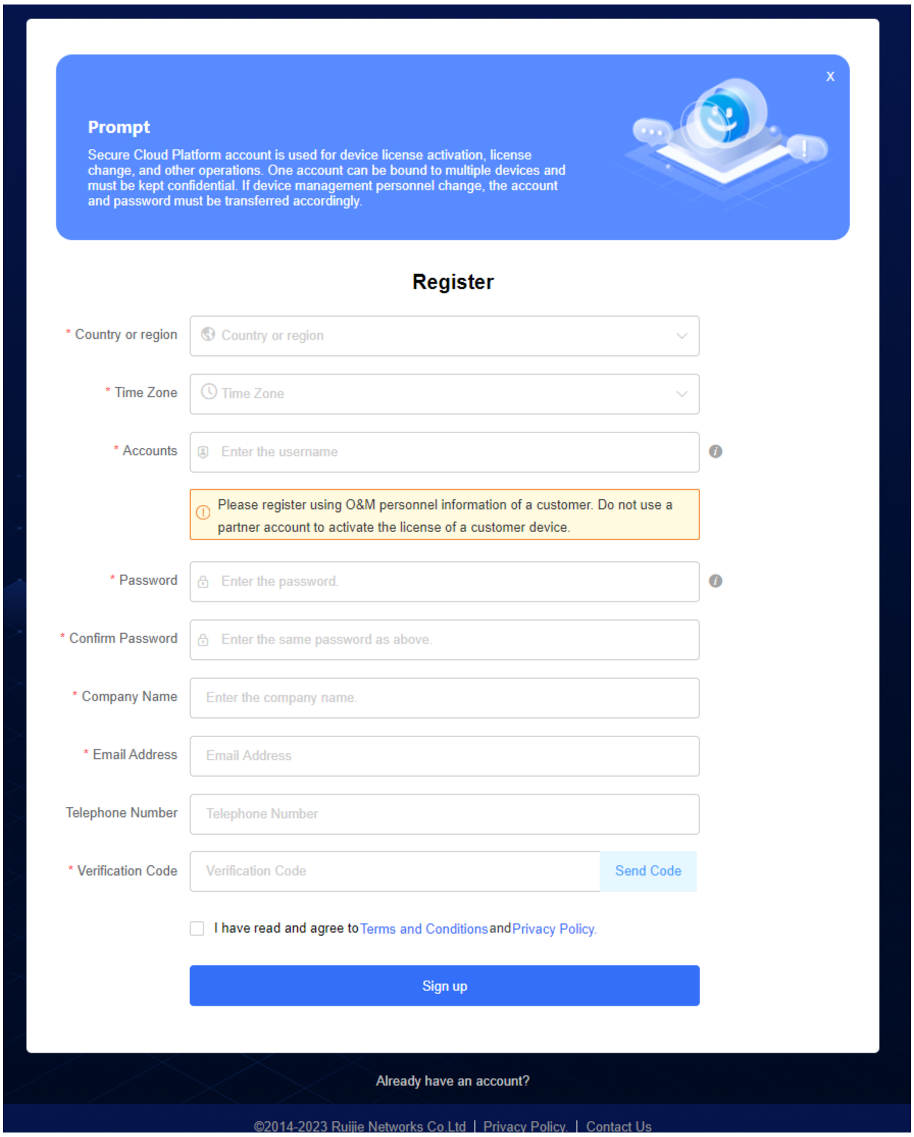
Note

When you register a user, you need to bind the user to a device SN. Ensure that the device SN exists in the order system (device is normally delivered).

a Enter https://secloud-en.ruijienetworks.com/ in the browser and press **Enter**.

b Click **Sign up** to access the registration page.

c Enter the required user information to complete registration.



Prompt

Secure Cloud Platform account is used for device license activation, license change, and other operations. One account can be bound to multiple devices and must be kept confidential. If device management personnel change, the account and password must be transferred accordingly.

Register

* Country or region	Country or region
* Time Zone	Time Zone
* Accounts	Enter the username
	Please register using O&M personnel information of a customer. Do not use a partner account to activate the license of a customer device.
* Password	Enter the password.
* Confirm Password	Enter the same password as above.
* Company Name	Enter the company name.
* Email Address	Email Address
Telephone Number	Telephone Number
* Verification Code	Verification Code Send Code

□ I have read and agree to Terms and Conditions and Privacy Policy.

Sign up

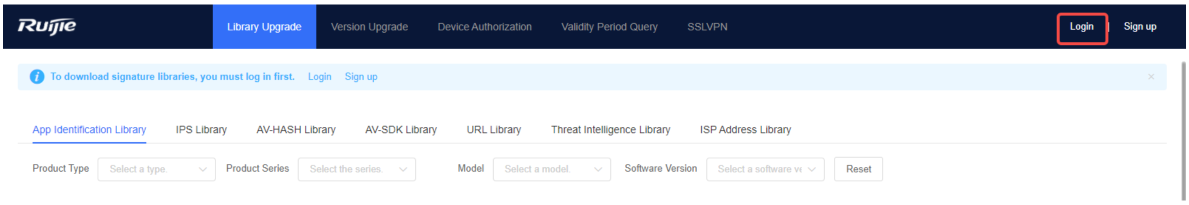
Already have an account?

©2014-2023 Ruijie Networks Co.Ltd | Privacy Policy | Contact Us

(2) Log in to the platform.

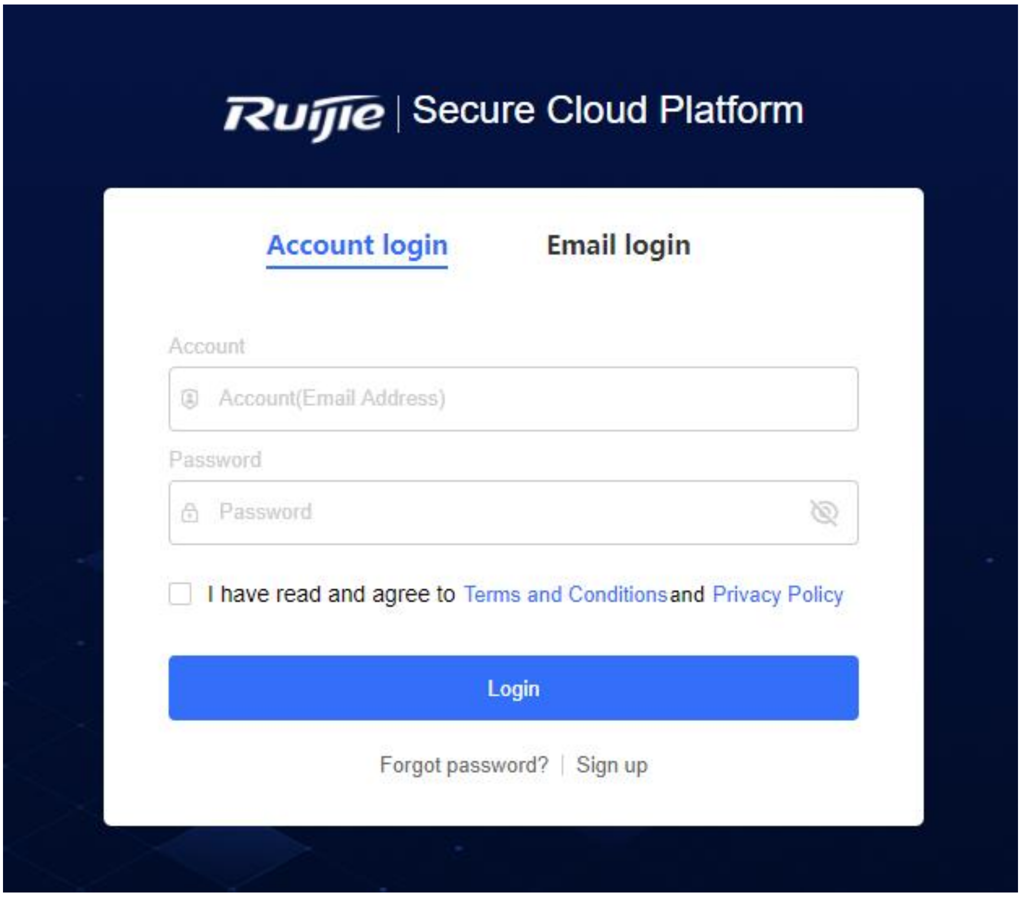
Visit https://secloud-en.ruijienetworks.com/ to access the login page.

If the login page is not displayed, click **Login** in the upper right corner of the home page.



To download signature libraries, you must log in first. Login Sign up

Product Type: Select a type Product Series: Select the series. Model: Select a model. Software Version: Select a software ve Reset



Ruijie | Secure Cloud Platform

Account

Account(Email Address)

Password

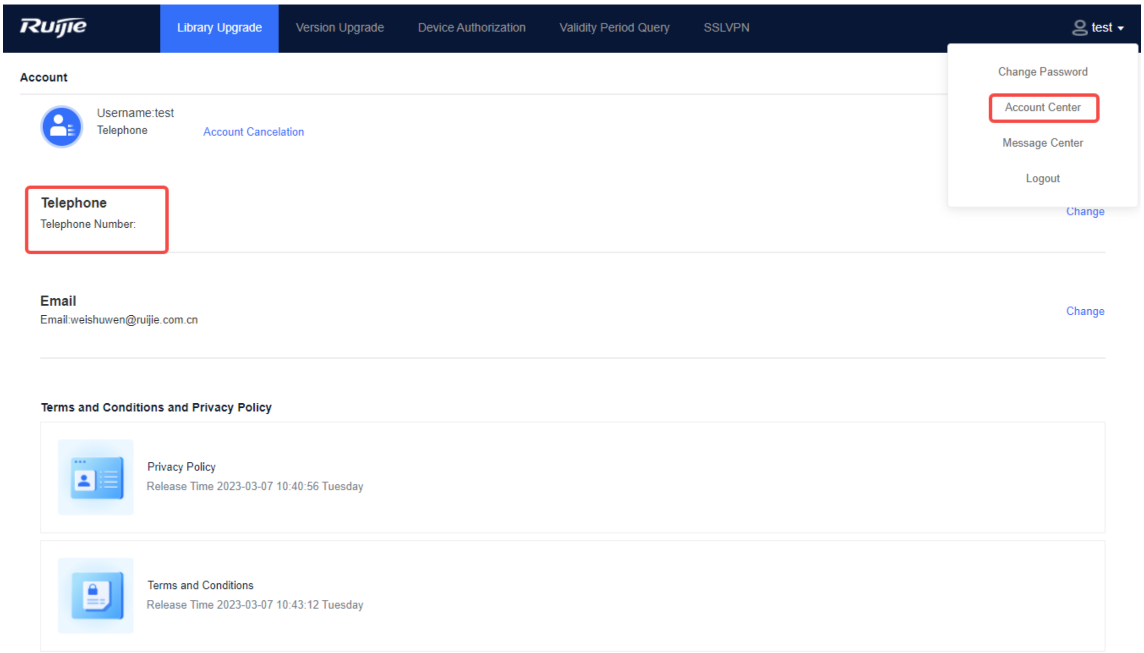
Password

□ I have read and agree to Terms and Conditions and Privacy Policy

(3) Modify personal information.

a Modify the mobile number.

Click the drop-down list box of the login username in the upper right corner of the page and then click **Account Center** to view the bound mobile number. Click **Change** to modify the mobile number bound to the current user.



Account

Username:test
Telephone

Account Cancelation

Telephone
Telephone Number:

Change

Email
Email:weishuwen@ruijie.com.cn

Change

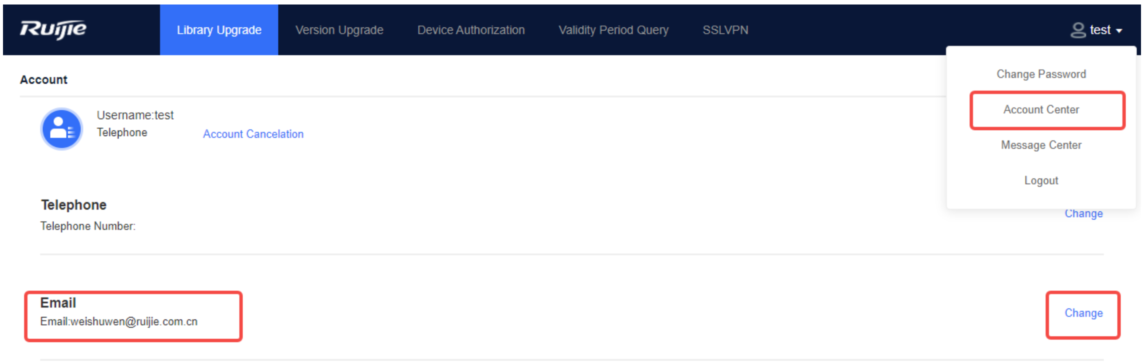
Terms and Conditions and Privacy Policy

Privacy Policy
Release Time 2023-03-07 10:40:56 Tuesday

Terms and Conditions
Release Time 2023-03-07 10:43:12 Tuesday

b Modify the email address.

Click the drop-down list box of the login username in the upper right corner of the page and then click **Account Center** to view the bound email address. Click **Change** to modify the email address bound to the current user.



Account

Username:test
Telephone

Account Cancelation

Telephone
Telephone Number:

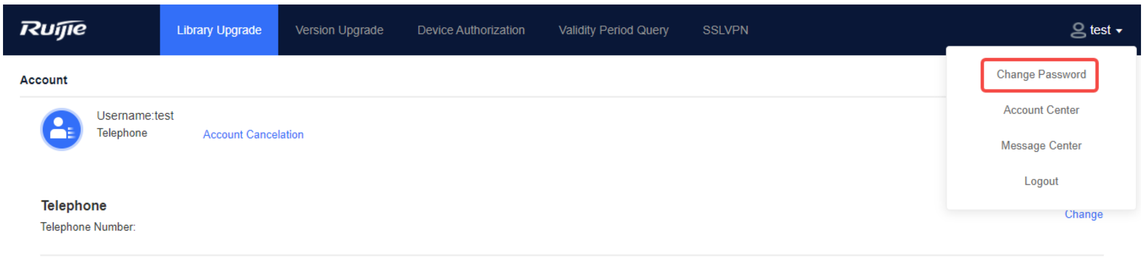
Change

Email
Email:weishuwen@ruijie.com.cn

Change

c Change the password.

Click the drop-down list box of the login username in the upper right corner of the page and then click **Change Password** to change the login password of the current user.



Account

Username:test

Telephone

Telephone

Telephone Number:

2. App Identification Signature Library Upgrade

Prerequisites

The App Identification license has been activated for the firewall and the license is within the validity period.

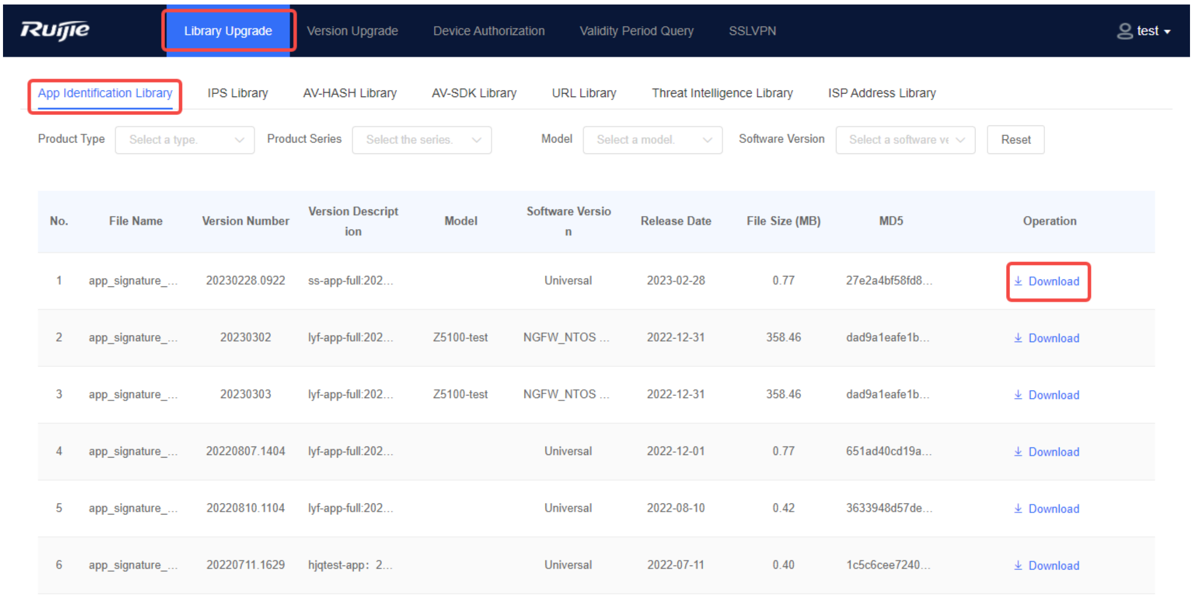
Procedure

- Offline upgrade

(1) Download a version file for the app identification signature library.

a Log in to the Secure Cloud Platform using an account with permission on the **Signature Library Upgrade** menu.

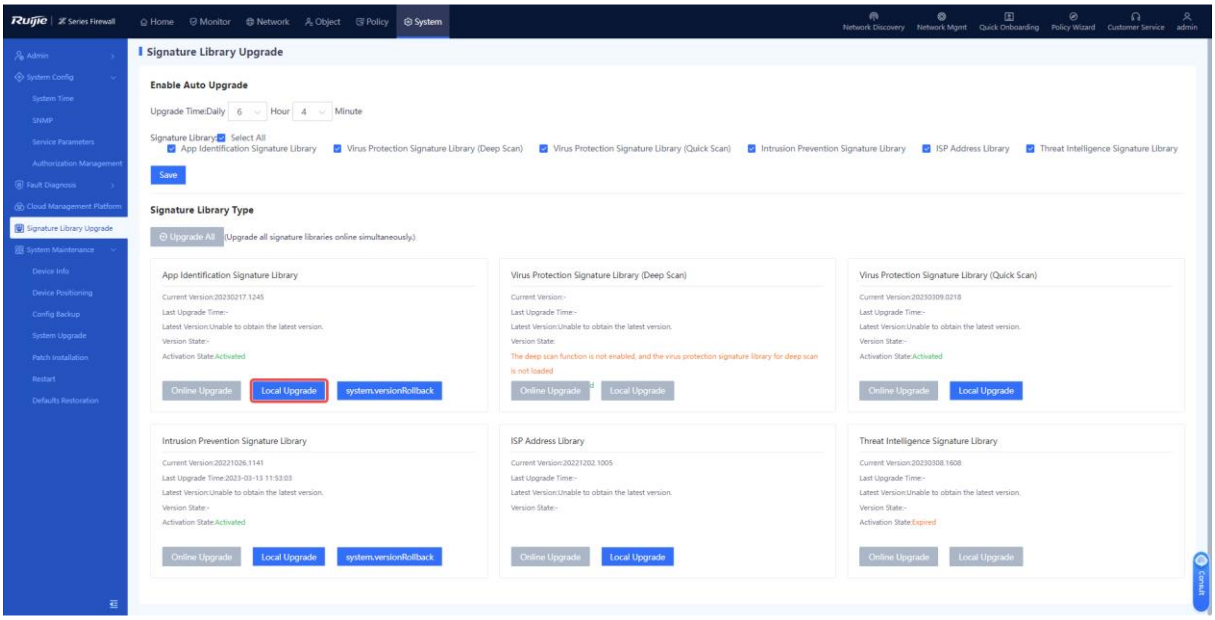
b Choose **Signature Library Upgrade** > **App Identification Library**, find the applicable version, and click **Download** in the **Operation** column to download the upgrade file to the local device.



Product Type: Select a type.
Product Series: Select the series.
Model: Select a model.
Software Version: Select a software ve

No.	File Name	Version Number	Version Description	Model	Software Version	Release Date	File Size (MB)	MD5	Operation
1	app_signature_...	20230228.0922	ss-app-full:202...		Universal	2023-02-28	0.77	27e2a4bf58fd8...	⤓ Download
2	app_signature_...	20230302	lyf-app-full:202...	Z5100-test	NGFW_NTOS ...	2022-12-31	358.46	dad9a1eafe1b...	⤓ Download
3	app_signature_...	20230303	lyf-app-full:202...	Z5100-test	NGFW_NTOS ...	2022-12-31	358.46	dad9a1eafe1b...	⤓ Download
4	app_signature_...	20220807.1404	lyf-app-full:202...		Universal	2022-12-01	0.77	651ad40cd19a...	⤓ Download
5	app_signature_...	20220810.1104	lyf-app-full:202...		Universal	2022-08-10	0.42	3633948d57de...	⤓ Download
6	app_signature_...	20220711.1629	hjqtest-app: 2...		Universal	2022-07-11	0.40	1c5c6cee7240...	⤓ Download

(2) After the version file is downloaded, choose **System** > **Signature Library Upgrade** on the firewall to upgrade the app identification signature library in offline mode (local upgrade).



Signature Library Upgrade

Enable Auto Upgrade

Upgrade Time:Daily 6 Hour 4 Minute

Signature Library: ☑ Select All
☑ App Identification Signature Library ☑ Virus Protection Signature Library (Deep Scan) ☑ Virus Protection Signature Library (Quick Scan) ☑ Intrusion Prevention Signature Library ☑ ISP Address Library ☑ Threat Intelligence Signature Library

Save

Signature Library Type

Upgrade All (Upgrade all signature libraries online simultaneously.)

App Identification Signature Library
Current Version:20230217.1245
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated
Online Upgrade | Local Upgrade | system.versionRollback

Virus Protection Signature Library (Deep Scan)
Current Version:-
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:
The deep scan function is not enabled, and the virus protection signature library for deep scan is not loaded
Online Upgrade | Local Upgrade

Virus Protection Signature Library (Quick Scan)
Current Version:20230309.0218
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated
Online Upgrade | Local Upgrade

Intrusion Prevention Signature Library
Current Version:20221026.1141
Last Upgrade Time:2023-03-13 11:53:03
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated
Online Upgrade | Local Upgrade | system.versionRollback

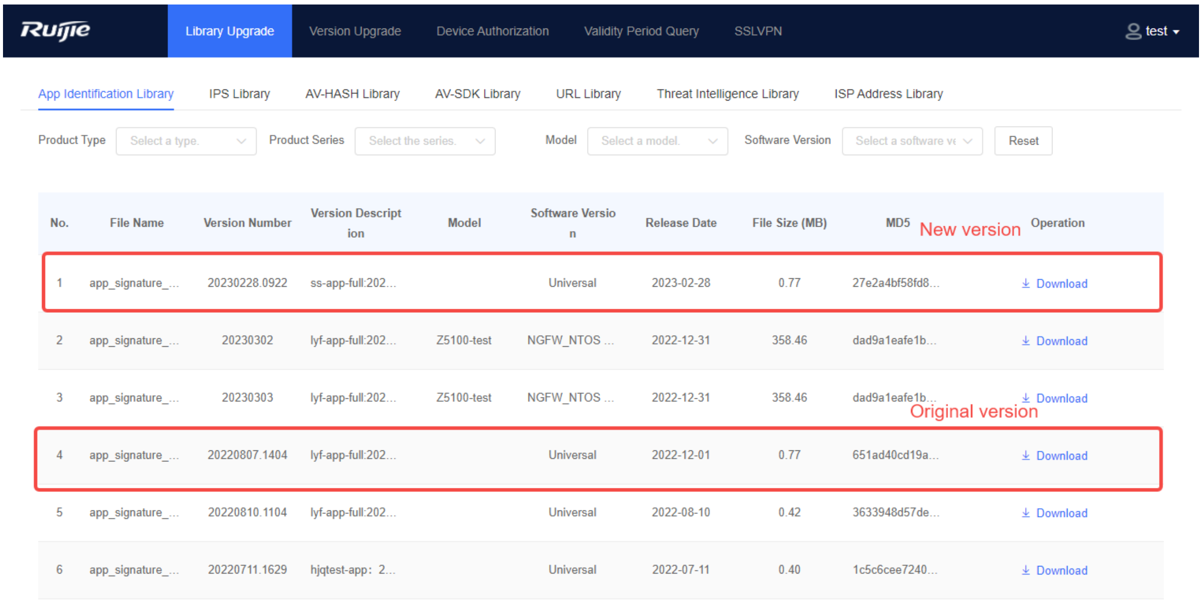
ISP Address Library
Current Version:20221202.1005
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Online Upgrade | Local Upgrade

Threat Intelligence Signature Library
Current Version:20230308.1608
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Expired
Online Upgrade | Local Upgrade

- Online upgrade

Note

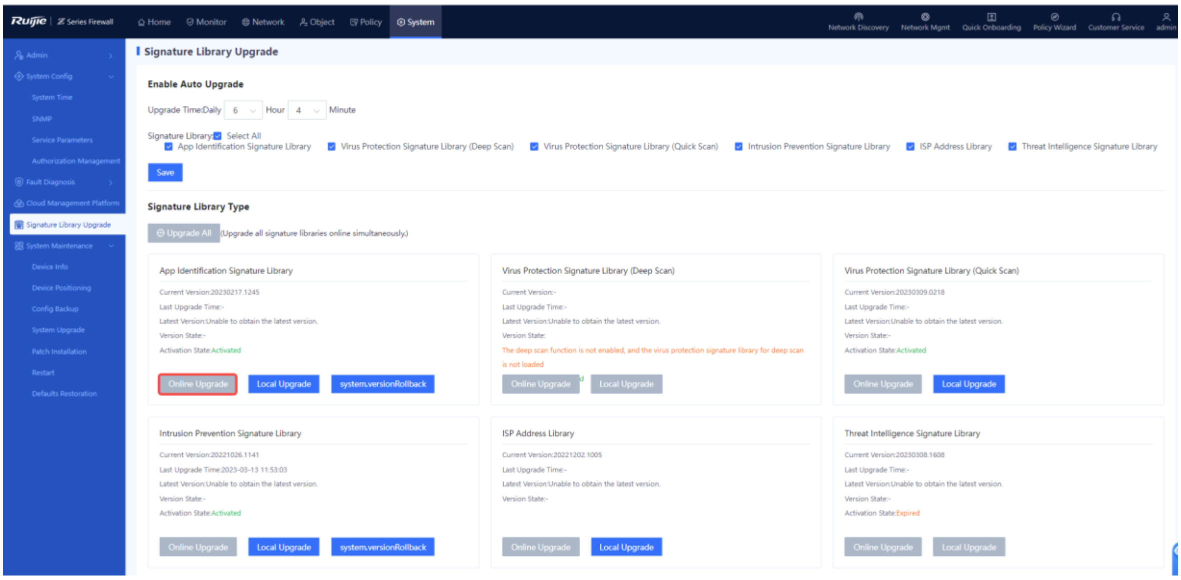
- The firewall must be connected to the Internet.
- When the current version information about the app identification signature library of the firewall exists on the cloud platform and a new version is available, online upgrade of the app identification signature library can be performed on the firewall.



Product Type Select a type. | Product Series Select the series. | Model Select a model. | Software Version Select a software ve | Reset

No.	File Name	Version Number	Version Description	Model	Software Version	Release Date	File Size (MB)	MD5	Operation
1	app_signature_...	20230228.0922	ss-app-full:202...		Universal	2023-02-28	0.77	27e2a4bf58fd8...	Download
2	app_signature_...	20230302	lyf-app-full:202...	Z5100-test	NGFW_NTOS ...	2022-12-31	358.46	dad9a1eafe1b...	Download
3	app_signature_...	20230303	lyf-app-full:202...	Z5100-test	NGFW_NTOS ...	2022-12-31	358.46	dad9a1eafe1b...	Download
4	app_signature_...	20220807.1404	lyf-app-full:202...		Universal	2022-12-01	0.77	651ad40cd19a...	Download
5	app_signature_...	20220810.1104	lyf-app-full:202...		Universal	2022-08-10	0.42	3633948d57de...	Download
6	app_signature_...	20220711.1629	hjqtest-app：2...		Universal	2022-07-11	0.40	1c5c6cee7240...	Download

Choose **System** > **Signature Library Upgrade** on the firewall, find **App Identification Signature Library**, and upgrade the app identification signature library in online mode.



Signature Library Upgrade

Enable Auto Upgrade

Upgrade Time:Daily 6 Hour 4 Minute

Signature Library:☑ Select All
☑ App Identification Signature Library ☑ Virus Protection Signature Library (Deep Scan) ☑ Virus Protection Signature Library (Quick Scan) ☑ Intrusion Prevention Signature Library ☑ ISP Address Library ☑ Threat Intelligence Signature Library

Signature Library Type

(Upgrade all signature libraries online simultaneously.)

App Identification Signature Library
Current Version:20230217.1245
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated

Virus Protection Signature Library (Deep Scan)
Current Version:-
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:
The deep scan function is not enabled, and the virus protection signature library for deep scan is not loaded

Virus Protection Signature Library (Quick Scan)
Current Version:20230309.0218
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated

Intrusion Prevention Signature Library
Current Version:20221026.1141
Last Upgrade Time:2023-03-13 11:53:03
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated

ISP Address Library
Current Version:20221202.1005
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-

Threat Intelligence Signature Library
Current Version:20230308.1608
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Expired

3. IPS Signature Library Upgrade

Prerequisites

The Intrusion Prevention (IPS) license has been activated for the firewall and the license is within the validity period.

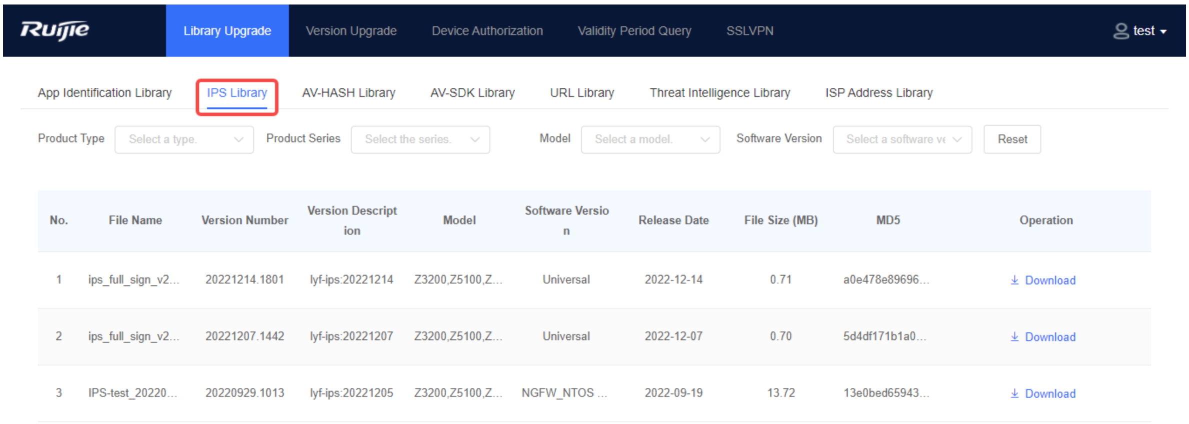
Procedure

- Offline upgrade

(1) Download a version file for the IPS signature library.

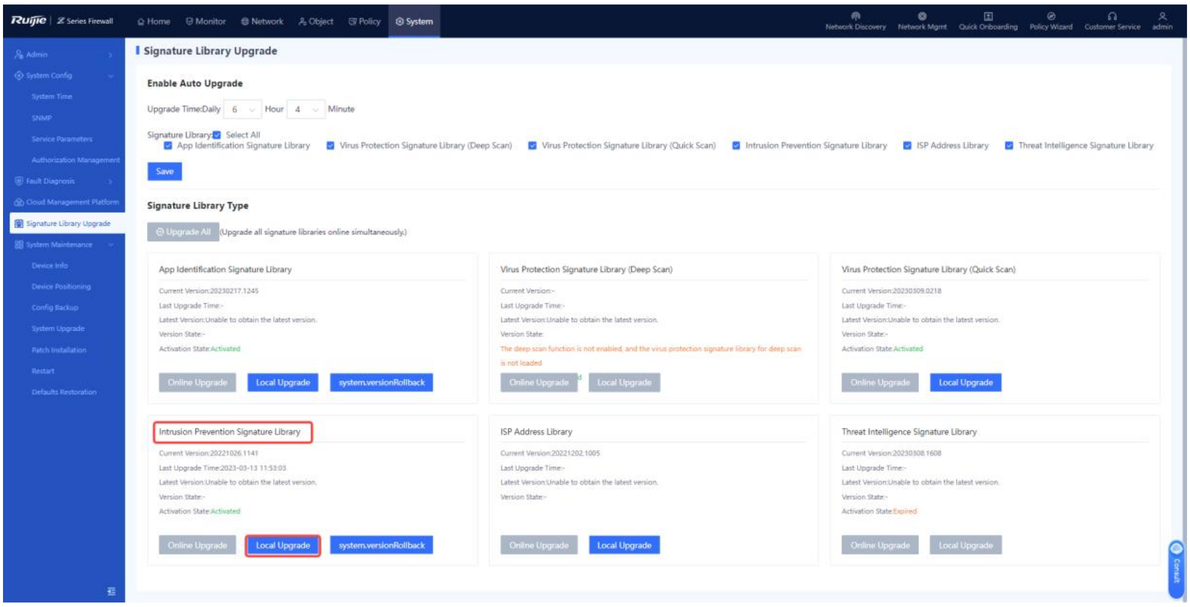
a Log in to the Secure Cloud Platform using an account with permission on the **Signature Library Upgrade** menu.

b Choose **Signature Library Upgrade** > **IPS Library**, find the applicable version, and click **Download** in the **Operation** column to download the upgrade file to the local device.



No.	File Name	Version Number	Version Description	Model	Software Version	Release Date	File Size (MB)	MD5	Operation
1	ips_full_sign_v2...	20221214.1801	lyf-ips:20221214	Z3200,Z5100,Z...	Universal	2022-12-14	0.71	a0e478e89696...	Download
2	ips_full_sign_v2...	20221207.1442	lyf-ips:20221207	Z3200,Z5100,Z...	Universal	2022-12-07	0.70	5d4df171b1a0...	Download
3	IPS-test_20220...	20220929.1013	lyf-ips:20221205	Z3200,Z5100,Z...	NGFW_NTOS ...	2022-09-19	13.72	13e0bed65943...	Download

(2) After the version file is downloaded, choose **System** > **Signature Library Upgrade** on the firewall to upgrade the IPS signature library in offline mode (local upgrade).



Signature Library Upgrade

Enable Auto Upgrade

Upgrade Time:Daily 6 Hour 4 Minute

Signature Library:☑ Select All
☑ App Identification Signature Library ☑ Virus Protection Signature Library (Deep Scan) ☑ Virus Protection Signature Library (Quick Scan) ☑ Intrusion Prevention Signature Library ☑ ISP Address Library ☑ Threat Intelligence Signature Library

Signature Library Type

(Upgrade all signature libraries online simultaneously.)

App Identification Signature Library
Current Version:20230217.1245
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated

Virus Protection Signature Library (Deep Scan)
Current Version:-
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:
The deep scan function is not enabled, and the virus protection signature library for deep scan is not loaded

Virus Protection Signature Library (Quick Scan)
Current Version:20230309.0218
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated

Intrusion Prevention Signature Library
Current Version:20221026.1141
Last Upgrade Time:2023-03-13 11:53:03
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated

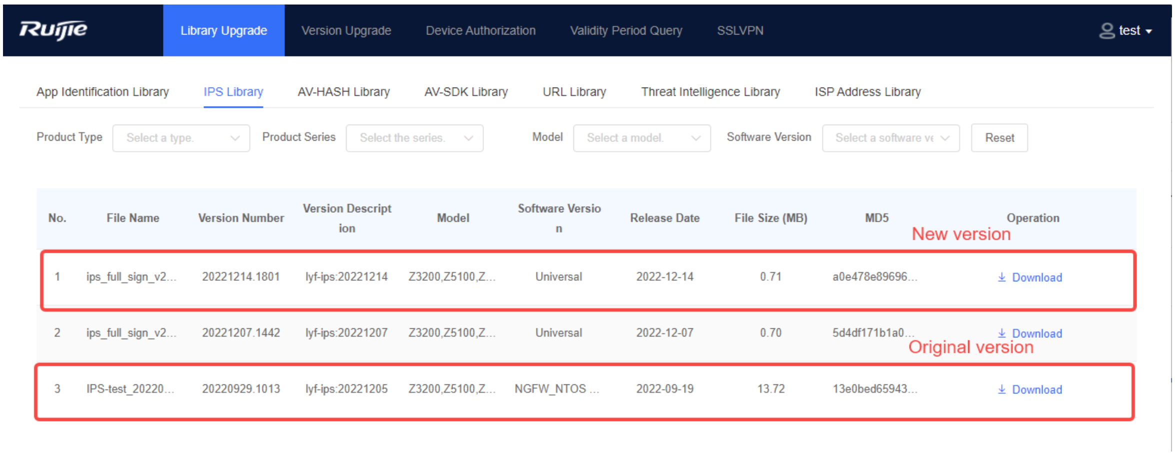
ISP Address Library
Current Version:20221202.1005
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-

Threat Intelligence Signature Library
Current Version:20230308.1608
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Expired

- Online upgrade

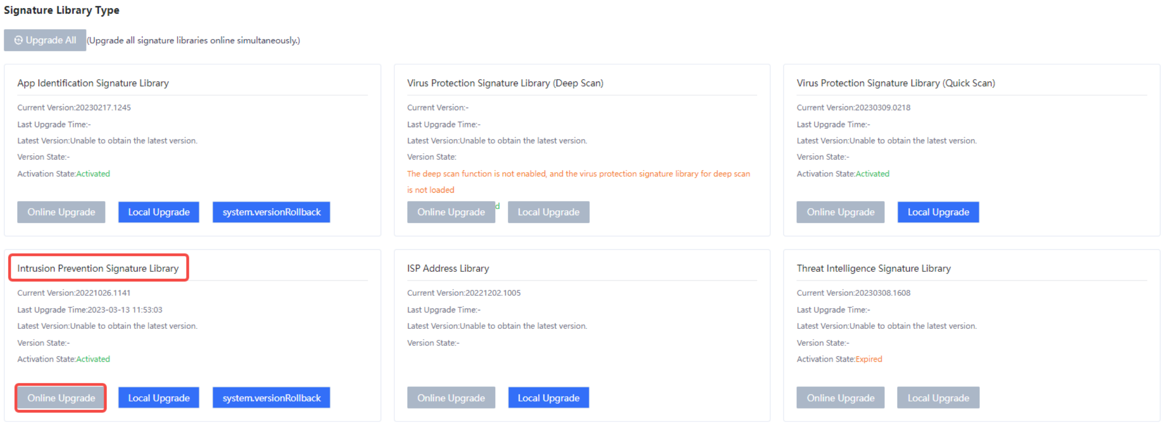
Note

- The firewall must be connected to the Internet.
- When the current version information about the signature library of the firewall exists on the cloud platform and a new version is available, online upgrade of the IPS signature library can be performed on the firewall.



No.	File Name	Version Number	Version Description	Model	Software Version	Release Date	File Size (MB)	MD5	Operation
1	ips_full_sign_v2...	20221214.1801	lyf-ips:20221214	Z3200,Z5100,Z...	Universal	2022-12-14	0.71	a0e478e89696...	Download
2	ips_full_sign_v2...	20221207.1442	lyf-ips:20221207	Z3200,Z5100,Z...	Universal	2022-12-07	0.70	5d4df171b1a0...	Download
3	IPS-test_20220...	20220929.1013	lyf-ips:20221205	Z3200,Z5100,Z...	NGFW_NTOS ...	2022-09-19	13.72	13e0bed65943...	Download

Choose **System** > **Signature Library Upgrade** on the firewall, find **Intrusion Prevention Signature Library**, and upgrade the IPS signature library in online mode.



App Identification Signature Library

Current Version:20230217.1245
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated

Virus Protection Signature Library (Deep Scan)

Current Version:-
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:
The deep scan function is not enabled, and the virus protection signature library for deep scan is not loaded

Virus Protection Signature Library (Quick Scan)

Current Version:20230309.0218
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated

Intrusion Prevention Signature Library

Current Version:20221026.1141
Last Upgrade Time:2023-03-13 11:53:03
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated

ISP Address Library

Current Version:20221202.1005
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-

Threat Intelligence Signature Library

Current Version:20230308.1608
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Expired

4. Virus Protection (Quick Scan) Signature Library Upgrade

Prerequisites

The Antivirus (AV) license has been activated for the firewall and the license is within the validity period.

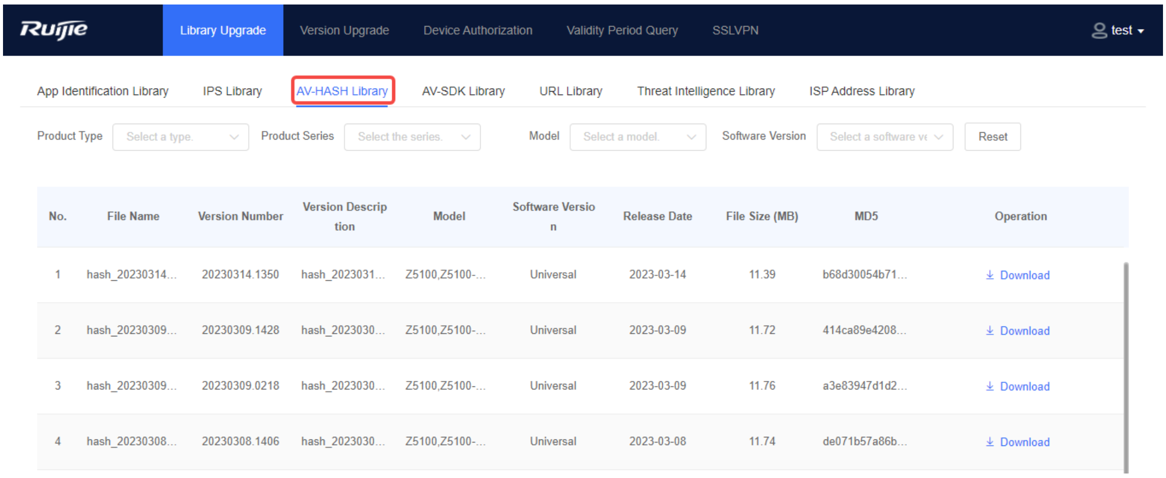
Procedure

- Offline upgrade

(1) Download the version file for the AV-HASH library.

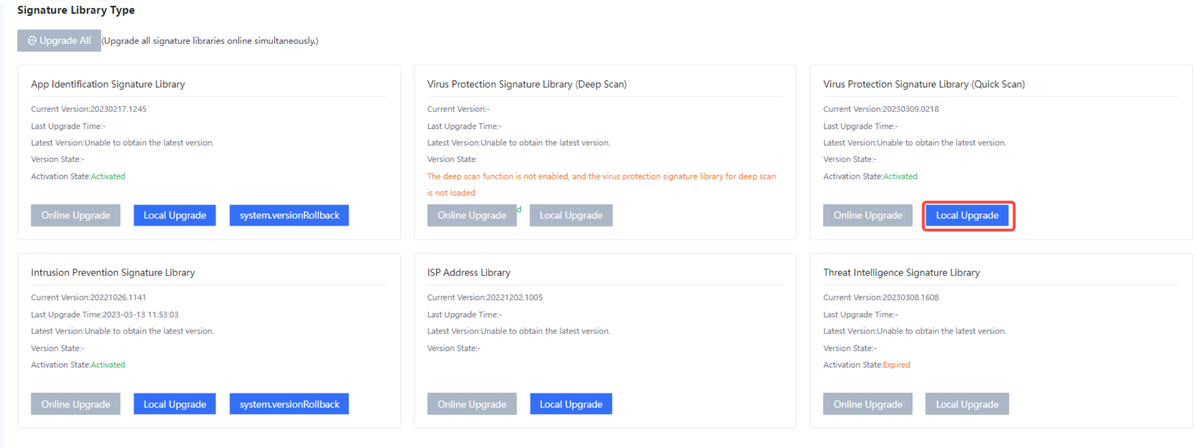
a Log in to the Secure Cloud Platform using an account with permission on the **Signature Library Upgrade** menu.

b Choose **Signature Library Upgrade** > **AV-HASH Library**, find the applicable version, and click **Download** in the **Operation** column to download the upgrade file to the local device.



No.	File Name	Version Number	Version Description	Model	Software Version	Release Date	File Size (MB)	MD5	Operation
1	hash_20230314...	20230314.1350	hash_2023031...	Z5100,Z5100-...	Universal	2023-03-14	11.39	b68d30054b71...	⤓ Download
2	hash_20230309...	20230309.1428	hash_2023030...	Z5100,Z5100-...	Universal	2023-03-09	11.72	414ca89e4208...	⤓ Download
3	hash_20230309...	20230309.0218	hash_2023030...	Z5100,Z5100-...	Universal	2023-03-09	11.76	a3e83947d1d2...	⤓ Download
4	hash_20230308...	20230308.1406	hash_2023030...	Z5100,Z5100-...	Universal	2023-03-08	11.74	de071b57a86b...	⤓ Download

(2) After the version file is downloaded, choose **System** > **Signature Library Upgrade** on the firewall, find **Virus Protection Signature Library (Quick Scan)**, and click **Local Upgrade** to perform offline upgrade.


Signature Library Type

(Upgrade all signature libraries online simultaneously.)

App Identification Signature Library
Current Version:20230217.1245
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated

Virus Protection Signature Library (Deep Scan)
Current Version:-
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:
The deep scan function is not enabled, and the virus protection signature library for deep scan is not loaded

Virus Protection Signature Library (Quick Scan)
Current Version:20230309.0218
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated

Intrusion Prevention Signature Library
Current Version:20221026.1141
Last Upgrade Time:2023-03-13 11:53:03
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated

ISP Address Library
Current Version:20221202.1005
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-

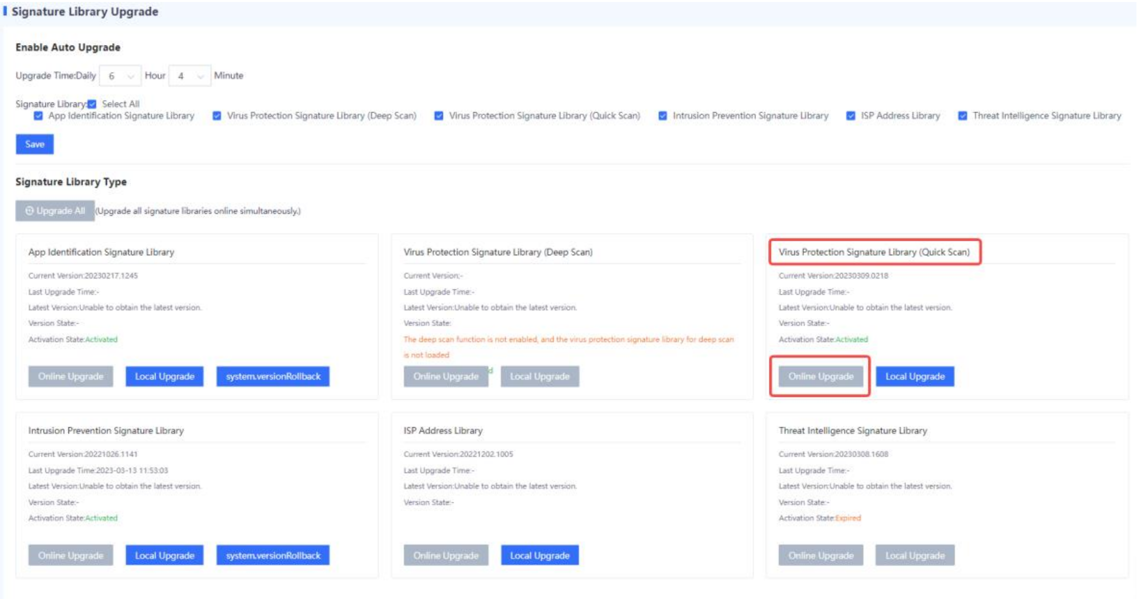
Threat Intelligence Signature Library
Current Version:20230308.1608
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Expired

- Online upgrade

Note

- The firewall must be connected to the Internet.
- When the current version information about the signature library of the firewall exists on the cloud platform and a new version is available, online upgrade of the AV-HASH library can be performed on the firewall.

Choose **System** > **Signature Library Upgrade** on the firewall, find **Virus Protection Signature Library (Quick Scan)**, and click **Online Upgrade** to perform online upgrade.



Signature Library Upgrade

Enable Auto Upgrade

Upgrade Time:Daily 6 Hour 4 Minute

Signature Library: ☑ Select All
☑ App Identification Signature Library ☑ Virus Protection Signature Library (Deep Scan) ☑ Virus Protection Signature Library (Quick Scan) ☑ Intrusion Prevention Signature Library ☑ ISP Address Library ☑ Threat Intelligence Signature Library

Signature Library Type

(Upgrade all signature libraries online simultaneously.)

App Identification Signature Library
Current Version:20230217.1245
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated

Virus Protection Signature Library (Deep Scan)
Current Version:-
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:
The deep scan function is not enabled, and the virus protection signature library for deep scan is not loaded

Virus Protection Signature Library (Quick Scan)
Current Version:20230309.0218
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated

Intrusion Prevention Signature Library
Current Version:20221026.1141
Last Upgrade Time:2023-03-13 11:53:03
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated

ISP Address Library
Current Version:20221202.1005
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-

Threat Intelligence Signature Library
Current Version:20230308.1608
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Expired

5. Virus Protection (Deep Scan) Signature Library Upgrade

Prerequisites

The Antivirus (AV) license has been activated for the firewall and the license is within the validity period.

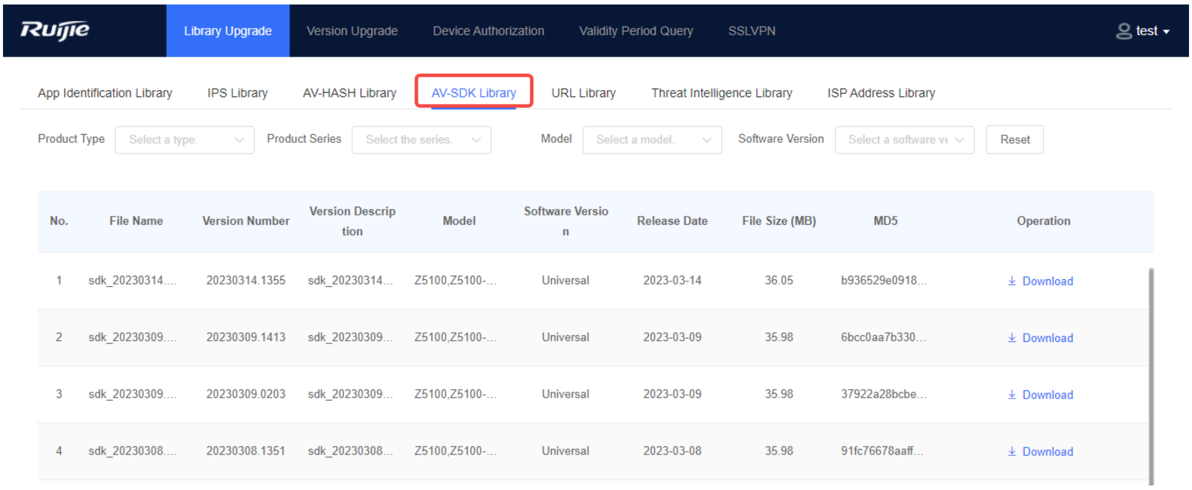
Procedure

- Offline upgrade

(1) Download the version file for the AV-SDK library.

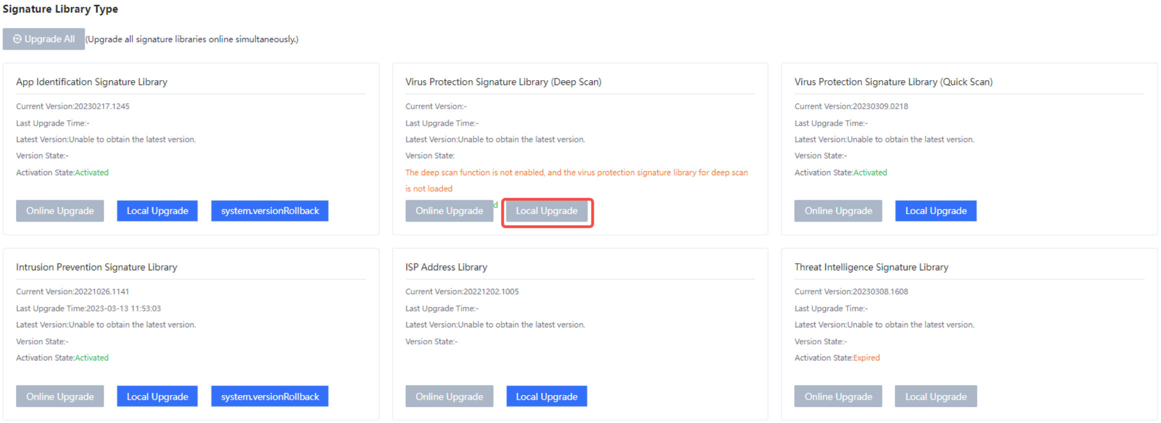
a Log in to the Secure Cloud Platform using an account with permission on the **Signature Library Upgrade** menu.

b Choose **Signature Library Upgrade** > **AV-SDK Library**, find the applicable version, and click **Download** in the **Operation** column to download the upgrade file to the local device.



No.	File Name	Version Number	Version Description	Model	Software Version	Release Date	File Size (MB)	MD5	Operation
1	sdk_20230314....	20230314.1355	sdk_20230314...	Z5100,Z5100-...	Universal	2023-03-14	36.05	b936529e0918...	⤓ Download
2	sdk_20230309....	20230309.1413	sdk_20230309...	Z5100,Z5100-...	Universal	2023-03-09	35.98	6bcc0aa7b330...	⤓ Download
3	sdk_20230309....	20230309.0203	sdk_20230309...	Z5100,Z5100-...	Universal	2023-03-09	35.98	37922a28bcbe...	⤓ Download
4	sdk_20230308....	20230308.1351	sdk_20230308...	Z5100,Z5100-...	Universal	2023-03-08	35.98	91fc76678aaff...	⤓ Download

(2) After the version file is downloaded, choose **System** > **Signature Library Upgrade** on the firewall, find **Virus Protection Signature Library (Deep Scan)**, and click **Local Upgrade** to perform offline upgrade.



(Upgrade all signature libraries online simultaneously.)

App Identification Signature Library
Current Version:20230217.1245
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated

Virus Protection Signature Library (Deep Scan)
Current Version:-
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:
The deep scan function is not enabled, and the virus protection signature library for deep scan is not loaded

Virus Protection Signature Library (Quick Scan)
Current Version:20230309.0218
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated

Intrusion Prevention Signature Library
Current Version:20221026.1141
Last Upgrade Time:2023-03-13 11:53:03
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated

ISP Address Library
Current Version:20221202.1005
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-

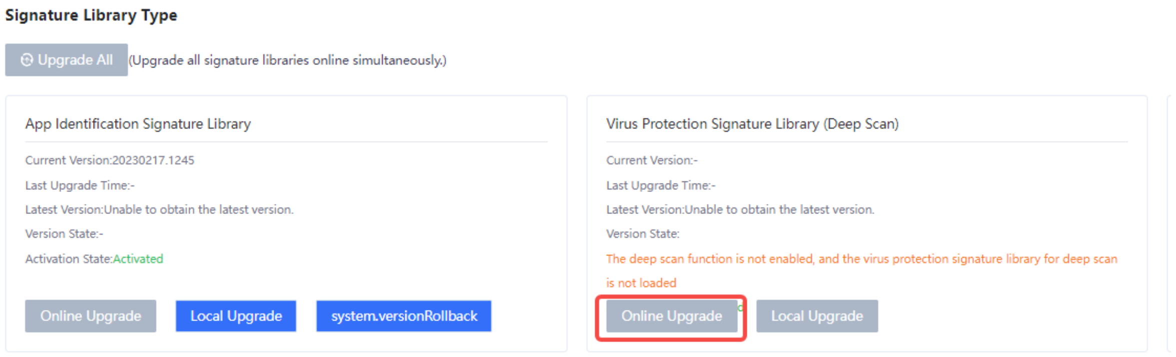
Threat Intelligence Signature Library
Current Version:20230308.1608
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Expired

- Online upgrade

Note

- The firewall must be connected to the Internet.
- When the current version information about the signature library of the firewall exists on the cloud platform and a new version is available, online upgrade of the AV-SDK library can be performed on the firewall.

Choose **System** > **Signature Library Upgrade** on the firewall, find **Virus Protection Signature Library (Deep Scan)**, and click **Online Upgrade** to perform online upgrade.



Signature Library Type

Upgrade All (Upgrade all signature libraries online simultaneously.)

App Identification Signature Library

Current Version:20230217.1245

Last Upgrade Time:-

Latest Version:Unable to obtain the latest version.

Version State:-

Activation State:Activated

Virus Protection Signature Library (Deep Scan)

Current Version:-

Last Upgrade Time:-

Latest Version:Unable to obtain the latest version.

Version State:

The deep scan function is not enabled, and the virus protection signature library for deep scan is not loaded

6. ISP Address Library Upgrade

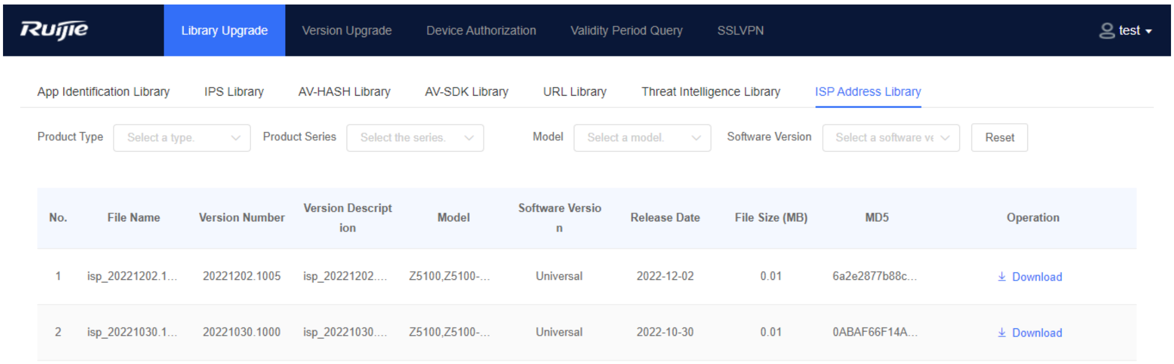
Procedure

- Offline upgrade

(1) Download a version file for the ISP address library.

a Log in to the Secure Cloud Platform using an account with permission on the **Signature Library Upgrade** menu.

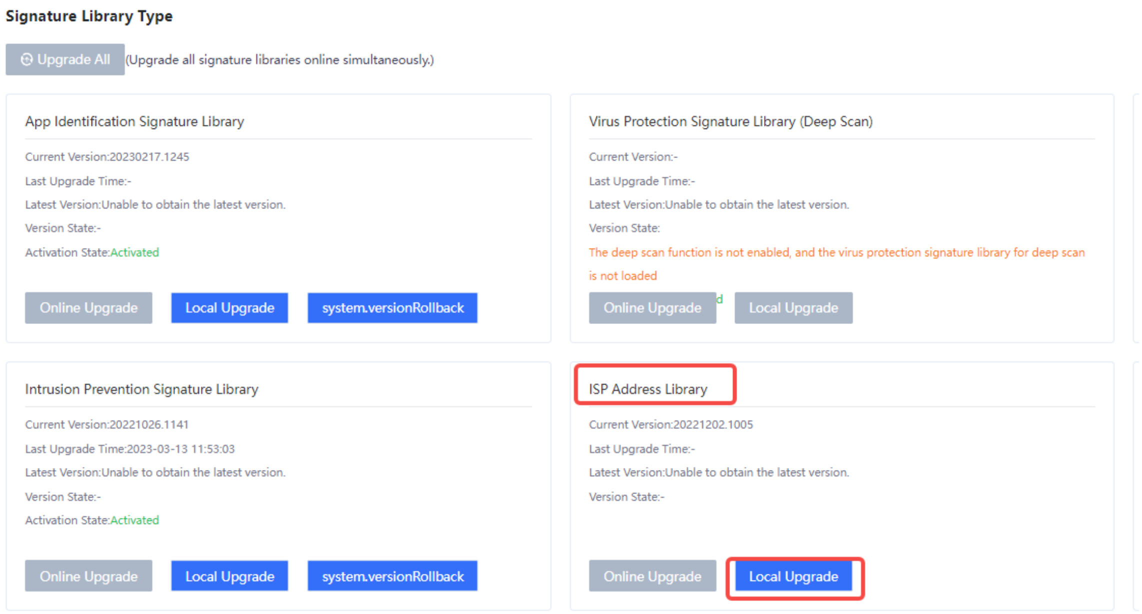
b Choose **Signature Library Upgrade** > **ISP Address Library**, find the applicable version, and click **Download** in the **Operation** column to download the upgrade file to the local device.



Product Type: Select a type. Product Series: Select the series. Model: Select a model. Software Version: Select a software ve Reset

No.	File Name	Version Number	Version Description	Model	Software Version	Release Date	File Size (MB)	MD5	Operation
1	isp_20221202.1...	20221202.1005	isp_20221202....	Z5100,Z5100-...	Universal	2022-12-02	0.01	6a2e2877b88c...	Download
2	isp_20221030.1...	20221030.1000	isp_20221030....	Z5100,Z5100-...	Universal	2022-10-30	0.01	0ABAF66F14A...	Download

(2) After the version file is downloaded, choose **System** > **Signature Library Upgrade** on the firewall, find **ISP Address Library**, and click **Local Upgrade** to upload the upgrade file for the upgrade.



Signature Library Type

(Upgrade all signature libraries online simultaneously.)

App Identification Signature Library

Current Version:20230217.1245
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated

Virus Protection Signature Library (Deep Scan)

Current Version:-
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:
The deep scan function is not enabled, and the virus protection signature library for deep scan is not loaded

Intrusion Prevention Signature Library

Current Version:20221026.1141
Last Upgrade Time:2023-03-13 11:53:03
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated

ISP Address Library

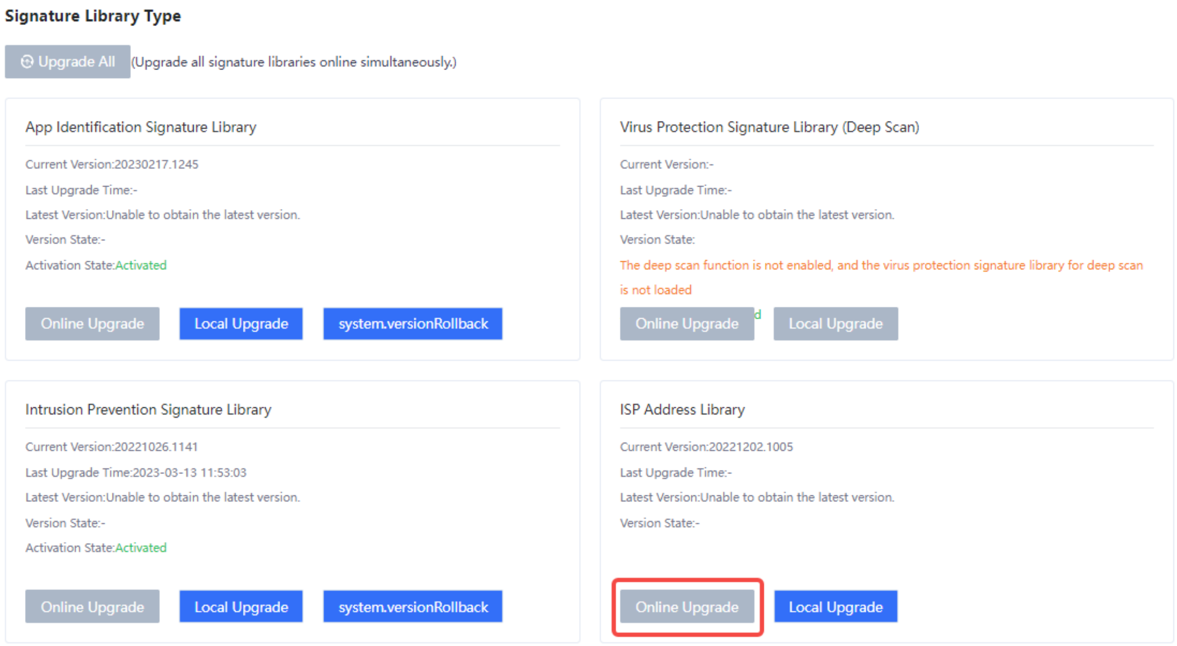
Current Version:20221202.1005
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-

- Online upgrade

Note

- The firewall must be connected to the Internet.
- When the current version information about the signature library of the firewall exists on the cloud platform and a new version is available, online upgrade of the ISP address library can be performed on the firewall.

Choose **System** > **Signature Library Upgrade** on the firewall, find **ISP Address Library**, and click **Online Upgrade** to perform online upgrade.



Signature Library Type

(Upgrade all signature libraries online simultaneously.)

App Identification Signature Library

Current Version:20230217.1245
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated

Virus Protection Signature Library (Deep Scan)

Current Version:-
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:
The deep scan function is not enabled, and the virus protection signature library for deep scan is not loaded

Intrusion Prevention Signature Library

Current Version:20221026.1141
Last Upgrade Time:2023-03-13 11:53:03
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated

ISP Address Library

Current Version:20221202.1005
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-

7. Threat Intelligence Library Upgrade

Prerequisites

The Threat Intelligence (TI) license has been activated for the firewall and the license is within the validity period.

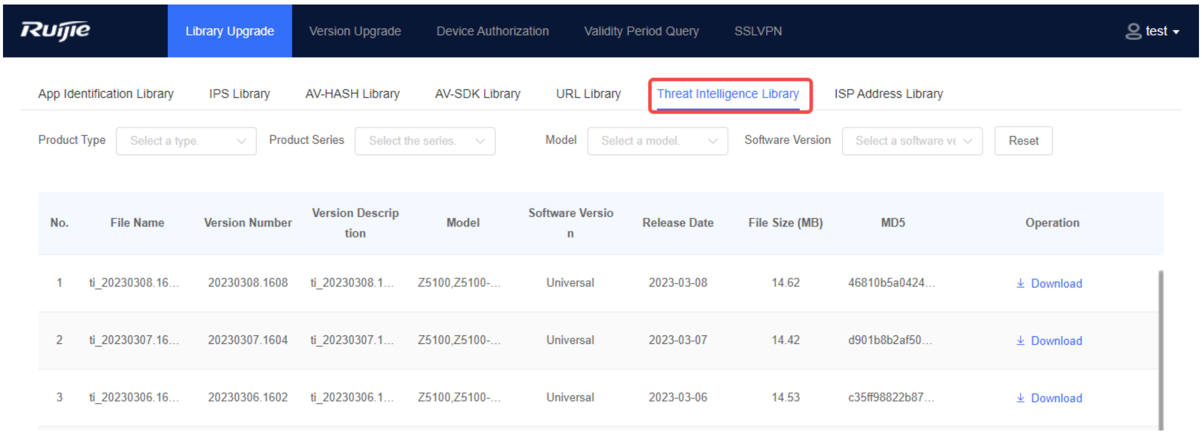
Procedure

- Offline upgrade

(1) Download a version file for the threat intelligence library.

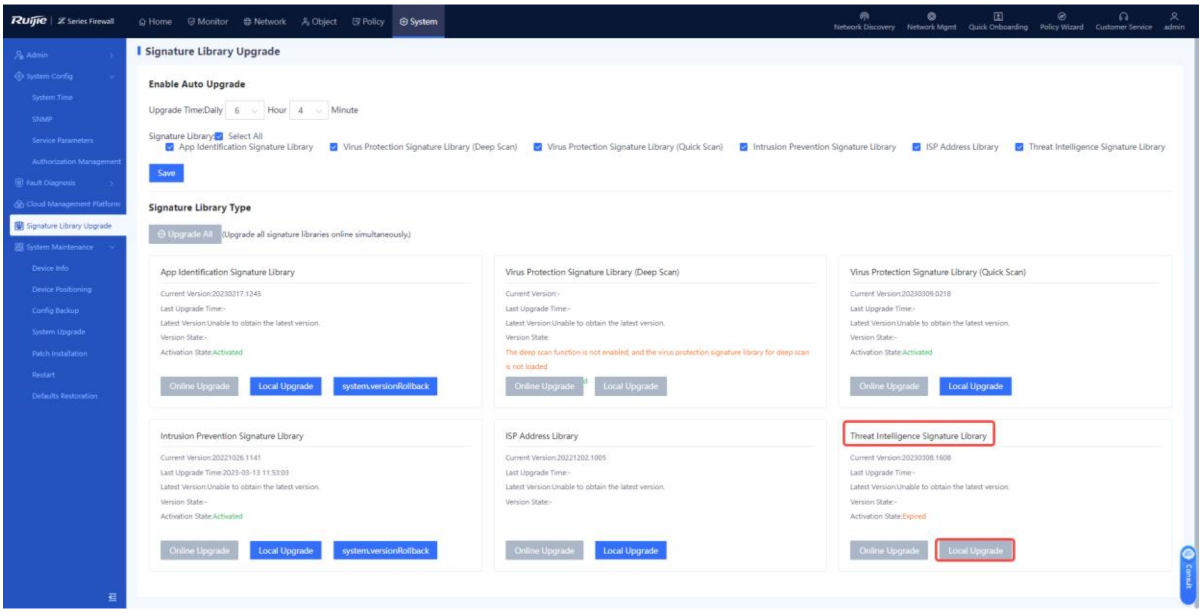
a Log in to the Secure Cloud Platform using an account with permission on the **Signature Library Upgrade** menu.

b Choose **Signature Library Upgrade** > **Threat Intelligence Library**, find the applicable version, and click **Download** in the **Operation** column to download the upgrade file to the local device.



No.	File Name	Version Number	Version Description	Model	Software Version	Release Date	File Size (MB)	MD5	Operation
1	ti_20230308.16...	20230308.1608	ti_20230308.1...	Z5100,Z5100-...	Universal	2023-03-08	14.62	46810b5a0424...	⤓ Download
2	ti_20230307.16...	20230307.1604	ti_20230307.1...	Z5100,Z5100-...	Universal	2023-03-07	14.42	d901b8b2af50...	⤓ Download
3	ti_20230306.16...	20230306.1602	ti_20230306.1...	Z5100,Z5100-...	Universal	2023-03-06	14.53	c35ff98822b87...	⤓ Download

(2) After the version file is downloaded, choose **System** > **Signature Library Upgrade** on the firewall, find **Threat Intelligence Signature Library**, and click **Local Upgrade** to upload the upgrade file for the upgrade.



Signature Library Upgrade

Enable Auto Upgrade

Upgrade Time:Daily 6 Hour 4 Minute

Signature Library: ☑ Select All
☑ App Identification Signature Library ☑ Virus Protection Signature Library (Deep Scan) ☑ Virus Protection Signature Library (Quick Scan) ☑ Intrusion Prevention Signature Library ☑ ISP Address Library ☑ Threat Intelligence Signature Library

Save

Signature Library Type

Upgrade All (Upgrade all signature libraries online simultaneously.)

App Identification Signature Library
Current Version:20230217.1245
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated
Online Upgrade | Local Upgrade | system.versionRollback

Virus Protection Signature Library (Deep Scan)
Current Version:-
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:
The deep scan function is not enabled, and the virus protection signature library for deep scan is not loaded
Online Upgrade | Local Upgrade

Virus Protection Signature Library (Quick Scan)
Current Version:20230309.0218
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated
Online Upgrade | Local Upgrade

Intrusion Prevention Signature Library
Current Version:20221026.1141
Last Upgrade Time:2023-03-13 11:53:03
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated
Online Upgrade | Local Upgrade | system.versionRollback

ISP Address Library
Current Version:20221202.1005
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Online Upgrade | Local Upgrade

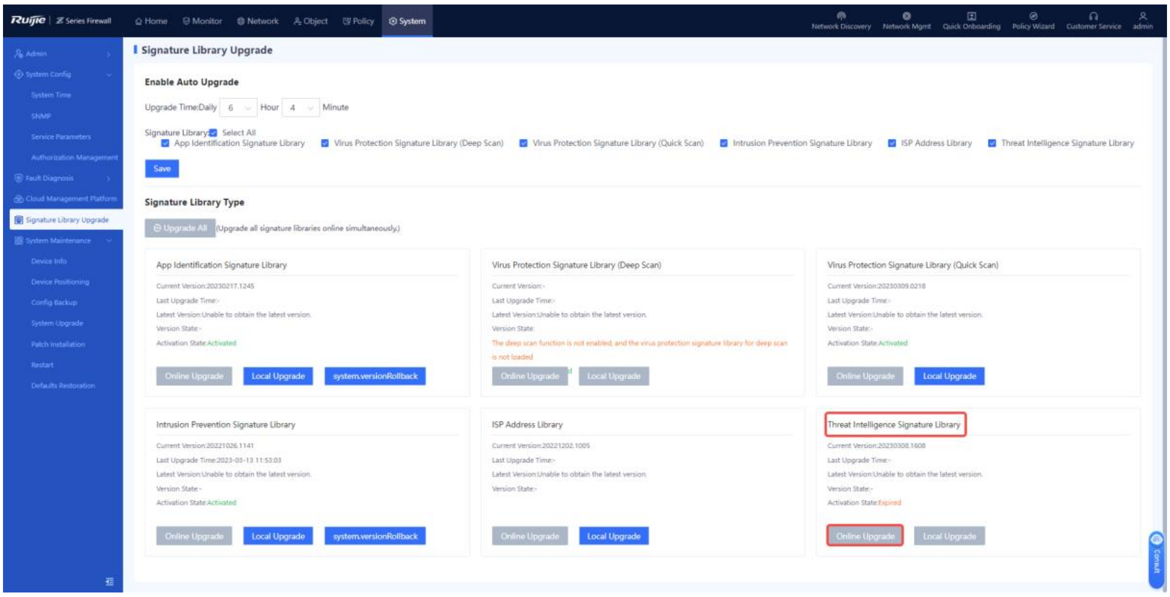
Threat Intelligence Signature Library
Current Version:20230308.1608
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Expired
Online Upgrade | Local Upgrade

- Online upgrade

Note

- The firewall must be connected to the Internet.
- When the current version information about the signature library of the firewall exists on the cloud platform and a new version is available, online upgrade of the threat intelligence library can be performed on the firewall.

Choose **System** > **Signature Library Upgrade** on the firewall, find **Threat Intelligence Signature Library**, and click **Online Upgrade** to perform online upgrade.



Signature Library Upgrade

Enable Auto Upgrade

Upgrade Time:Daily 6 Hour 4 Minute

Signature Library: ☑ Select All
☑ App Identification Signature Library ☑ Virus Protection Signature Library (Deep Scan) ☑ Virus Protection Signature Library (Quick Scan) ☑ Intrusion Prevention Signature Library ☑ ISP Address Library ☑ Threat Intelligence Signature Library

Save

Signature Library Type

Upgrade All (Upgrade all signature libraries online simultaneously.)

App Identification Signature Library
Current Version:20230217.1245
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated
Online Upgrade | Local Upgrade | system.versionRollback

Virus Protection Signature Library (Deep Scan)
Current Version:-
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:
The deep scan function is not enabled, and the virus protection signature library for deep scan is not loaded
Online Upgrade | Local Upgrade

Virus Protection Signature Library (Quick Scan)
Current Version:20230309.0218
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated
Online Upgrade | Local Upgrade

Intrusion Prevention Signature Library
Current Version:20221026.1141
Last Upgrade Time:2023-03-13 11:53:03
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated
Online Upgrade | Local Upgrade | system.versionRollback

ISP Address Library
Current Version:20221202.1005
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Online Upgrade | Local Upgrade

Threat Intelligence Signature Library
Current Version:20230308.1608
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Expired
Online Upgrade | Local Upgrade

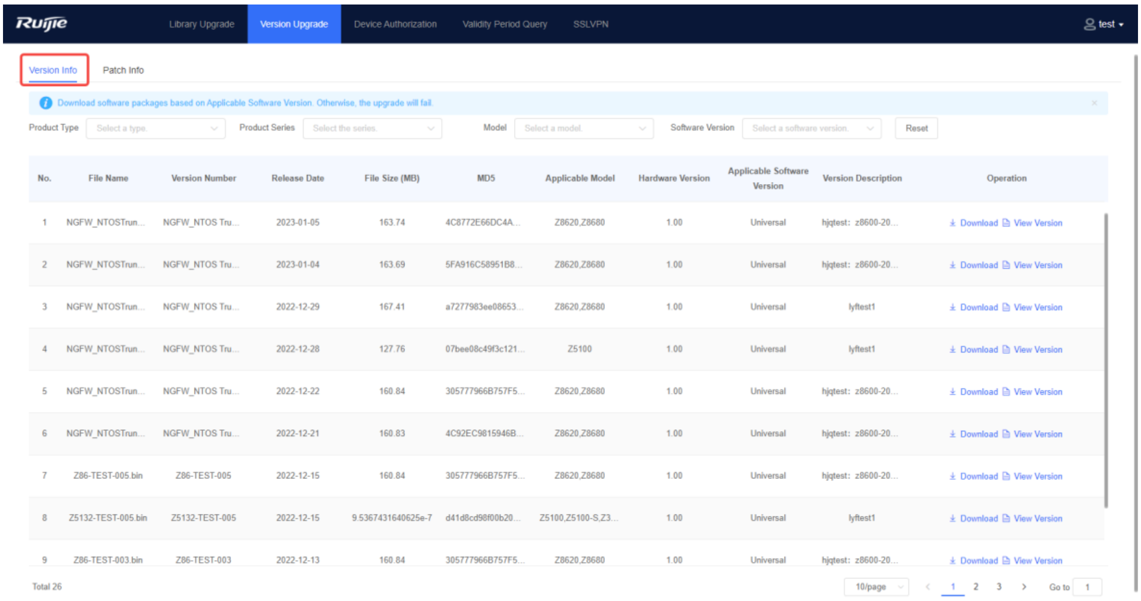
8. System Upgrade

- Offline upgrade

(1) Download a device version.

a Confirm that the user possesses permission on the **Version Upgrade** menu.

b Log in to the platform using an account with the desired permission, choose **Version Upgrade** > **Version Info**, find the applicable version, and download the version file.



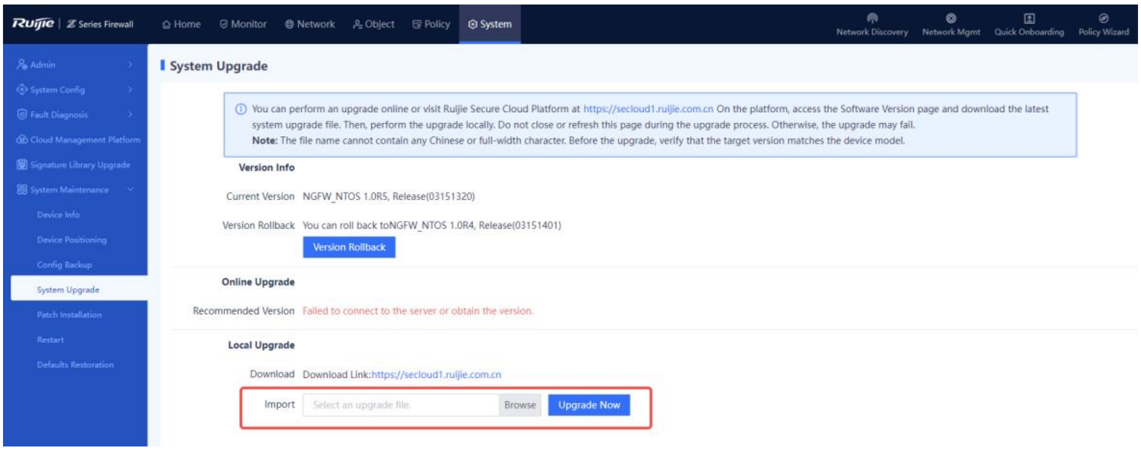
Download software packages based on Applicable Software Version. Otherwise, the upgrade will fail.

Product Type: Select a type. Product Series: Select the series. Model: Select a model. Software Version: Select a software version. Reset

No.	File Name	Version Number	Release Date	File Size (MB)	MD5	Applicable Model	Hardware Version	Applicable Software Version	Version Description	Operation
1	NGFW_NTOSTrun...	NGFW_NTOS Tru...	2023-01-05	163.74	4C8772E66DC4A...	Z8620,Z8680	1.00	Universal	hjqtest: z8600-20...	Download View Version
2	NGFW_NTOSTrun...	NGFW_NTOS Tru...	2023-01-04	163.69	5FA916C58951B8...	Z8620,Z8680	1.00	Universal	hjqtest: z8600-20...	Download View Version
3	NGFW_NTOSTrun...	NGFW_NTOS Tru...	2022-12-29	167.41	a7277983ee08653...	Z8620,Z8680	1.00	Universal	lyftest1	Download View Version
4	NGFW_NTOSTrun...	NGFW_NTOS Tru...	2022-12-28	127.76	07bee08c49f3c121...	Z5100	1.00	Universal	lyftest1	Download View Version
5	NGFW_NTOSTrun...	NGFW_NTOS Tru...	2022-12-22	160.84	305777966B757F5...	Z8620,Z8680	1.00	Universal	hjqtest: z8600-20...	Download View Version
6	NGFW_NTOSTrun...	NGFW_NTOS Tru...	2022-12-21	160.83	4C92EC9815946B...	Z8620,Z8680	1.00	Universal	hjqtest: z8600-20...	Download View Version
7	Z86-TEST-005.bin	Z86-TEST-005	2022-12-15	160.84	305777966B757F5...	Z8620,Z8680	1.00	Universal	hjqtest: z8600-20...	Download View Version
8	Z5132-TEST-005.bin	Z5132-TEST-005	2022-12-15	9.5367431640625e-7	d41d8cd98f00b20...	Z5100,Z5100-S,Z3...	1.00	Universal	lyftest1	Download View Version
9	Z86-TEST-003.bin	Z86-TEST-003	2022-12-13	160.84	305777966B757F5...	Z8620,Z8680	1.00	Universal	hjqtest: z8600-20...	Download View Version

Total 26 10/page < 1 2 3 > Go to 1

(2) After the version upgrade file is downloaded, choose **System** > **System Maintenance** > **System Upgrade** on the firewall, upload the upgrade file, and perform offline upgrade (local upgrade) of the device system version.



System Upgrade

You can perform an upgrade online or visit Ruijie Secure Cloud Platform at https://secloud1.ruijie.com.cn On the platform, access the Software Version page and download the latest system upgrade file. Then, perform the upgrade locally. Do not close or refresh this page during the upgrade process. Otherwise, the upgrade may fail.
Note: The file name cannot contain any Chinese or full-width character. Before the upgrade, verify that the target version matches the device model.

Version Info

Current Version NGFW_NTOS 1.0R5, Release(03151320)

Version Rollback You can roll back toNGFW_NTOS 1.0R4, Release(03151401)

Version Rollback

Online Upgrade

Recommended Version Failed to connect to the server or obtain the version.

Local Upgrade

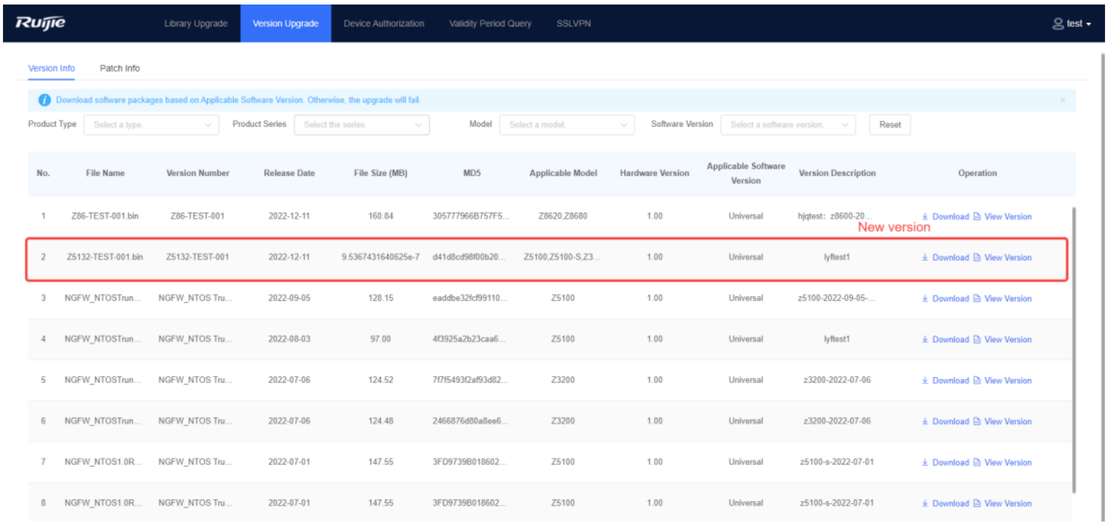
Download Download Link:https://secloud1.ruijie.com.cn

Import Select an upgrade file. Browse Upgrade Now

- Online upgrade

Note

- The firewall must be connected to the Internet.
- When the current version information about the firewall exists on the cloud platform and a new version is available, online upgrade of the device system can be performed on the firewall.



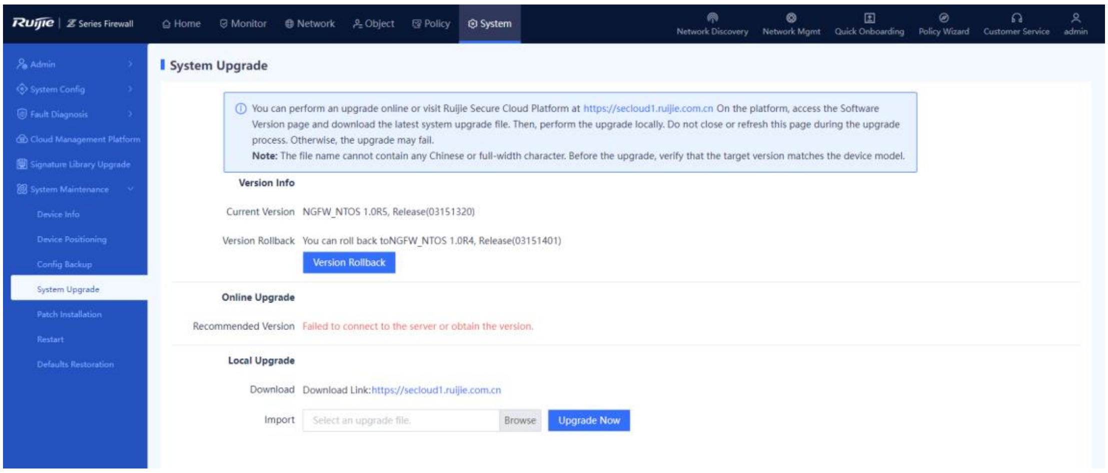
Download software packages based on Applicable Software Version. Otherwise, the upgrade will fail.

Product Type: Select a type. Product Series: Select the series. Model: Select a model. Software Version: Select a software version. Reset

No.	File Name	Version Number	Release Date	File Size (MB)	MD5	Applicable Model	Hardware Version	Applicable Software Version	Version Description	Operation
1	Z86-TEST-001.bin	Z86-TEST-001	2022-12-11	160.84	305777966B757F5...	Z8620,Z8680	1.00	Universal	hjqtest：z8600-20...	Download View Version
2	Z5132-TEST-001.bin	Z5132-TEST-001	2022-12-11	9.5367431640625e-7	d41d8cd98f00b20...	Z5100,Z5100-S,Z3...	1.00	Universal	lyftest1	Download View Version
3	NGFW_NTOSTrun...	NGFW_NTOS Tru...	2022-09-05	128.15	eaddbe32fcf99110...	Z5100	1.00	Universal	z5100-2022-09-05-...	Download View Version
4	NGFW_NTOSTrun...	NGFW_NTOS Tru...	2022-08-03	97.00	4f3925a2b23caa6...	Z5100	1.00	Universal	lyftest1	Download View Version
5	NGFW_NTOSTrun...	NGFW_NTOS Tru...	2022-07-06	124.52	7f7f5493f2af93d82...	Z3200	1.00	Universal	z3200-2022-07-06	Download View Version
6	NGFW_NTOSTrun...	NGFW_NTOS Tru...	2022-07-06	124.48	2466876d80a8ee6...	Z3200	1.00	Universal	z3200-2022-07-06	Download View Version
7	NGFW_NTOS1.0R...	NGFW_NTOS Tru...	2022-07-01	147.55	3FD9739B018602...	Z5100	1.00	Universal	z5100-s-2022-07-01	Download View Version
8	NGFW_NTOS1.0R...	NGFW_NTOS Tru...	2022-07-01	147.55	3FD9739B018602...	Z5100	1.00	Universal	z5100-s-2022-07-01	Download View Version

New version

Choose **System** > **System Maintenance** > **System Upgrade** and click **Upgrade Now** to perform online upgrade.



System Upgrade

You can perform an upgrade online or visit Ruijie Secure Cloud Platform at https://secloud1.ruijie.com.cn On the platform, access the Software Version page and download the latest system upgrade file. Then, perform the upgrade locally. Do not close or refresh this page during the upgrade process. Otherwise, the upgrade may fail.
Note: The file name cannot contain any Chinese or full-width character. Before the upgrade, verify that the target version matches the device model.

Version Info

Current Version NGFW_NTOS 1.0R5, Release(03151320)

Version Rollback You can roll back toNGFW_NTOS 1.0R4, Release(03151401)

Version Rollback

Online Upgrade

Recommended Version Failed to connect to the server or obtain the version.

Local Upgrade

Download Download Link:https://secloud1.ruijie.com.cn

Import Select an upgrade file. Browse Upgrade Now

9. Patch Installation

When a patch in the system is not installed, an alarm is displayed on the home page. When more than 20 patch packages need to be installed, you are advised to upgrade the software version.

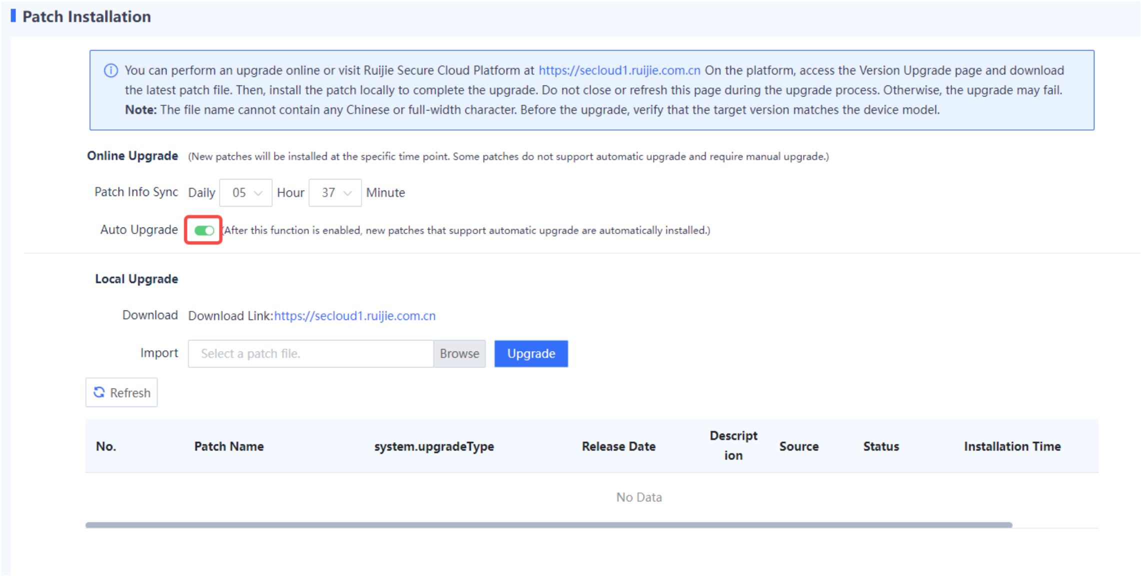
- Online patch installation

a Log in to the firewall and choose **System** > **System Maintenance** > **Patch Installation**.

b Enable **Online Upgrade**. The system automatically installs the patch packages.

Caution

Online upgrade is successful only when the firewall can properly communicate with the Ruijie cloud platform.



ⓘ You can perform an upgrade online or visit Ruijie Secure Cloud Platform at https://secloud1.ruijie.com.cn On the platform, access the Version Upgrade page and download the latest patch file. Then, install the patch locally to complete the upgrade. Do not close or refresh this page during the upgrade process. Otherwise, the upgrade may fail.
Note: The file name cannot contain any Chinese or full-width character. Before the upgrade, verify that the target version matches the device model.

Online Upgrade (New patches will be installed at the specific time point. Some patches do not support automatic upgrade and require manual upgrade.)

Patch Info Sync: Daily 05 Hour 37 Minute

Auto Upgrade: enabled (After this function is enabled, new patches that support automatic upgrade are automatically installed.)

Local Upgrade

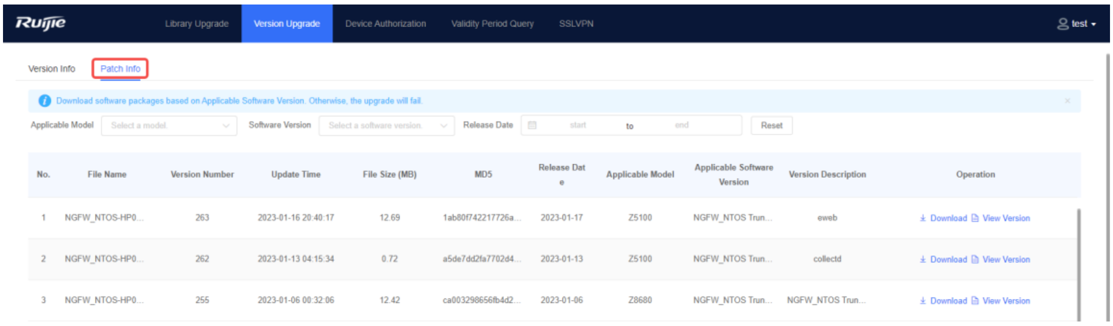
Download: Download Link:https://secloud1.ruijie.com.cn

Import: Select a patch file. Browse Upgrade

No.	Patch Name	system.upgradeType	Release Date	Description	Source	Status	Installation Time
No Data							

- Offline patch installation

a Log in to the Ruijie Secure Cloud Platform, choose **Version Upgrade** > **Patch Info**, and download the latest patch upgrade file to the local device.



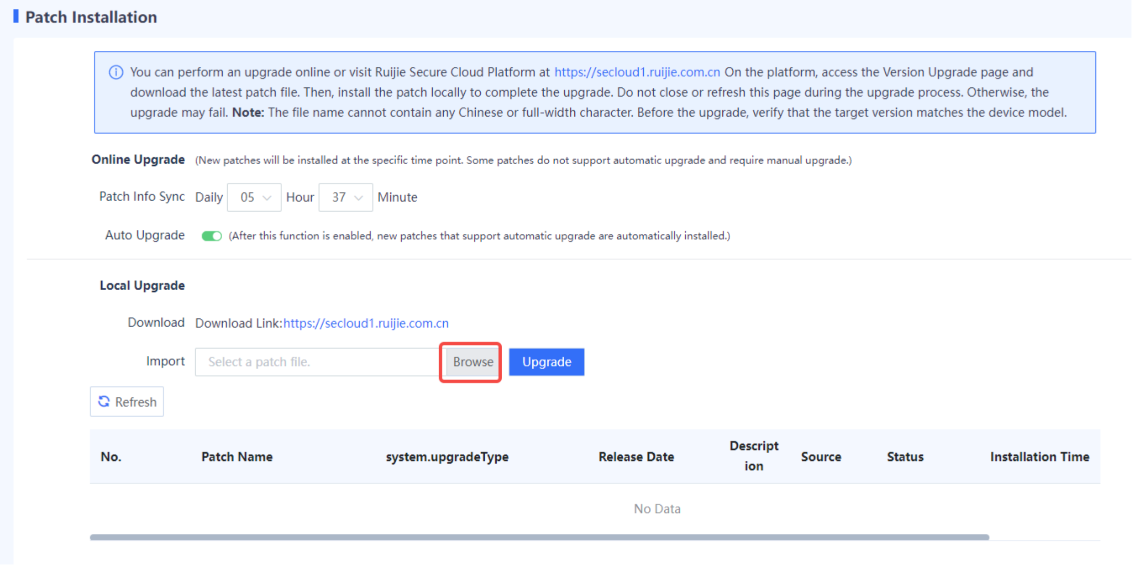
ⓘ Download software packages based on Applicable Software Version. Otherwise, the upgrade will fail.

Applicable Model: Select a model. Software Version: Select a software version. Release Date: start to end Reset

No.	File Name	Version Number	Update Time	File Size (MB)	MD5	Release Date	Applicable Model	Applicable Software Version	Version Description	Operation
1	NGFW_NTOS-HP0...	263	2023-01-16 20:40:17	12.69	1ab80f742217726a...	2023-01-17	Z5100	NGFW_NTOS Trun...	eweb	Download View Version
2	NGFW_NTOS-HP0...	262	2023-01-13 04:15:34	0.72	a5de7dd2fa7702d4...	2023-01-13	Z5100	NGFW_NTOS Trun...	collectd	Download View Version
3	NGFW_NTOS-HP0...	255	2023-01-06 00:32:06	12.42	ca003298656fb4d2...	2023-01-06	Z8680	NGFW_NTOS Trun...	NGFW_NTOS Trun...	Download View Version

c Log in to the firewall and choose **System** > **System Maintenance** > **Patch Installation**.

d In the **Local Upgrade** area, click **Browse** and select a patch file.



Patch Installation

You can perform an upgrade online or visit Ruijie Secure Cloud Platform at https://secloud1.ruijie.com.cn On the platform, access the Version Upgrade page and download the latest patch file. Then, install the patch locally to complete the upgrade. Do not close or refresh this page during the upgrade process. Otherwise, the upgrade may fail. **Note:** The file name cannot contain any Chinese or full-width character. Before the upgrade, verify that the target version matches the device model.

Online Upgrade (New patches will be installed at the specific time point. Some patches do not support automatic upgrade and require manual upgrade.)

Patch Info Sync: Daily 05 Hour 37 Minute

Auto Upgrade: (After this function is enabled, new patches that support automatic upgrade are automatically installed.)

Local Upgrade

Download: Download Link:https://secloud1.ruijie.com.cn

Import: Select a patch file.

No.	Patch Name	system.upgradeType	Release Date	Description	Source	Status	Installation Time

No Data

e Click **Upgrade** to start system upgrade.

Note

Device restart is not required after successful hot patch installation, but is required for successful cold patch installation. You need to select whether to restart the device based on actual needs.

10. License Activation

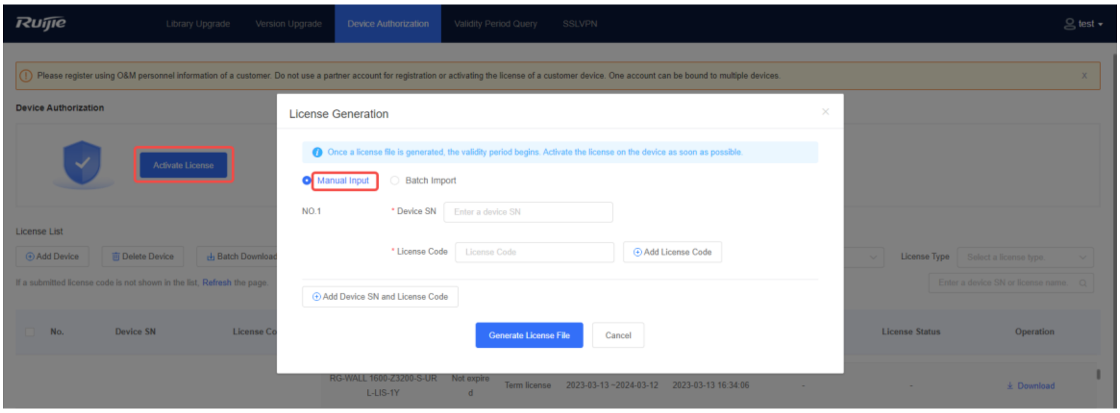
- License binding

(1) Confirm that the user possesses permission on the **Device Authorization** menu.

(2) Log in to the platform using an account with the desired permission, and choose **Device Authorization** > **Activate License**. In the **License Generation** dialog box, bind licenses using one of the following methods:

  o Manually add the device SN and license code.

  Select **Manual Input**, enter the device SN and license code, and click **Generate License File**.



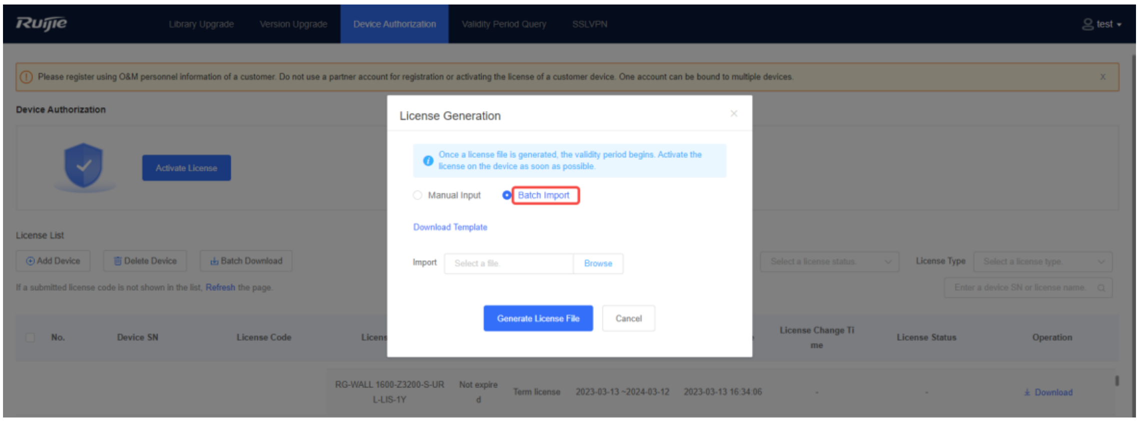
Please register using O&M personnel information of a customer. Do not use a partner account for registration or activating the license of a customer device. One account can be bound to multiple devices.

Once a license file is generated, the validity period begins. Activate the license on the device as soon as possible.

If a submitted license code is not shown in the list, Refresh the page.

- ○ Batch import device SNs and license codes.

  Select **Batch Import**, download a template, enter the device SNs and license codes in the template in the correct format, upload the file, and click **Generate License File**.



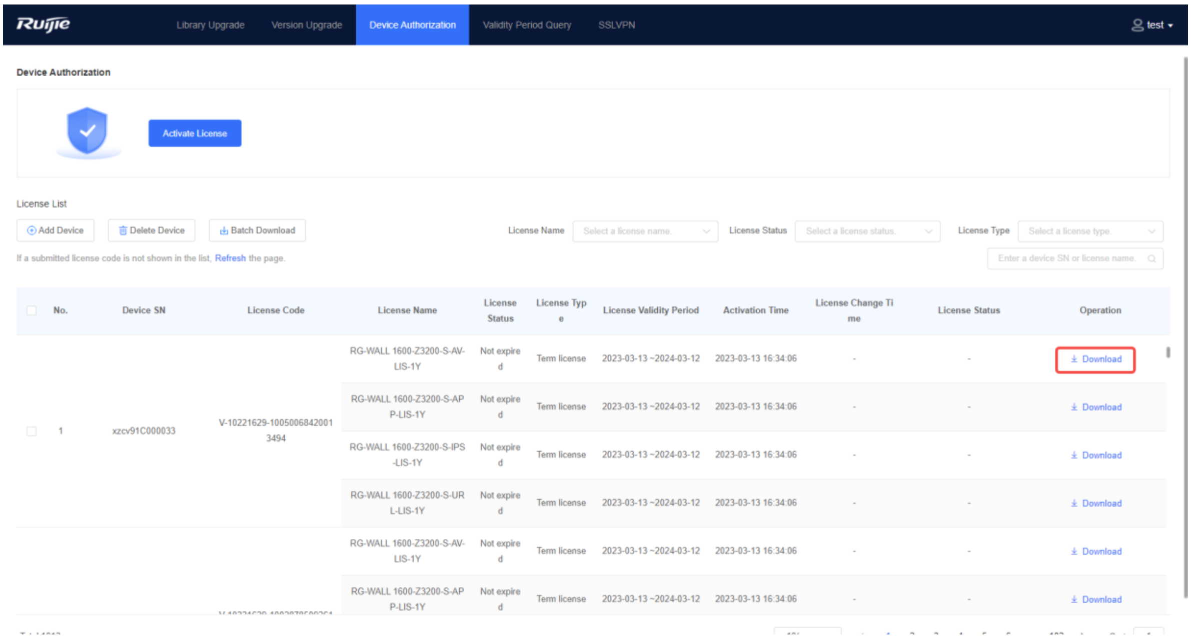
Please register using O&M personnel information of a customer. Do not use a partner account for registration or activating the license of a customer device. One account can be bound to multiple devices.

Once a license file is generated, the validity period begins. Activate the license on the device as soon as possible.

If a submitted license code is not shown in the list, Refresh the page.

- Offline activation

(1) Log in to the Secure Cloud Platform, bind the device SN to the license code, find the desired item in the license list on the **Device Authorization**, and click **Download** to download the license file.



Device Authorization

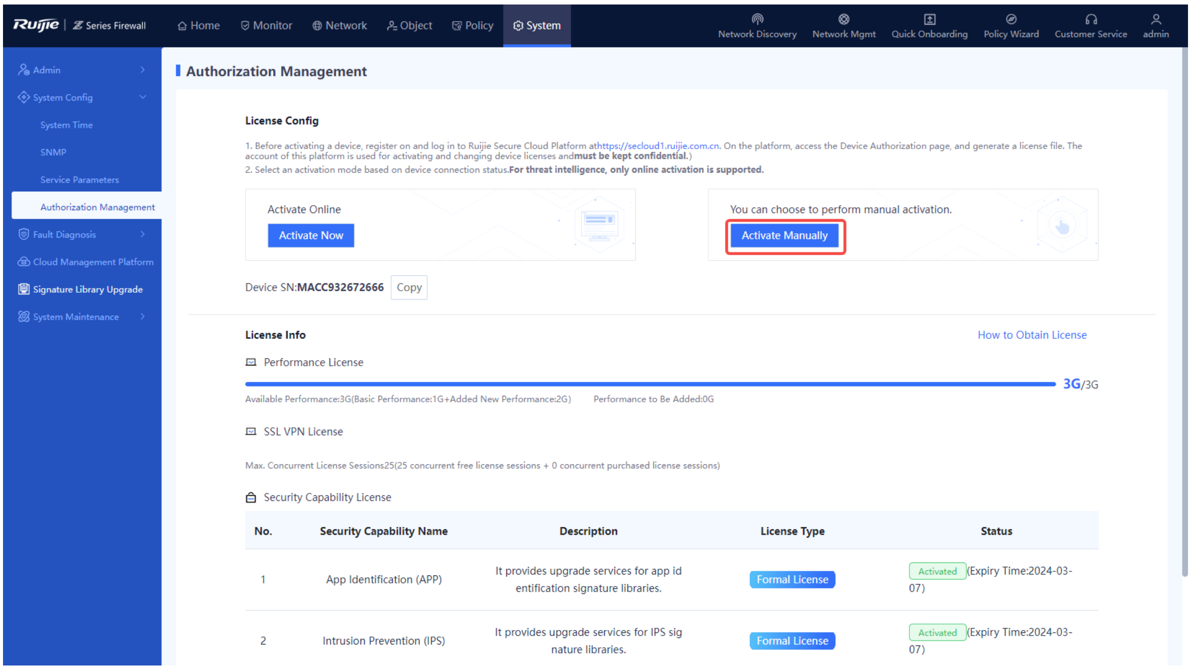
License List

License Name License Status License Type

If a submitted license code is not shown in the list, Refresh the page.

No.	Device SN	License Code	License Name	License Status	License Type	License Validity Period	Activation Time	License Change Time	License Status	Operation
1	xzcv91C000033	V-10221629-10050068420013494	RG-WALL 1600-Z3200-S-AV-LIS-1Y	Not expired	Term license	2023-03-13 ~2024-03-12	2023-03-13 16:34:06	-	-	Download
			RG-WALL 1600-Z3200-S-APP-LIS-1Y	Not expired	Term license	2023-03-13 ~2024-03-12	2023-03-13 16:34:06	-	-	Download
			RG-WALL 1600-Z3200-S-IPS-LIS-1Y	Not expired	Term license	2023-03-13 ~2024-03-12	2023-03-13 16:34:06	-	-	Download
			RG-WALL 1600-Z3200-S-URL-LIS-1Y	Not expired	Term license	2023-03-13 ~2024-03-12	2023-03-13 16:34:06	-	-	Download
			RG-WALL 1600-Z3200-S-AV-LIS-1Y	Not expired	Term license	2023-03-13 ~2024-03-12	2023-03-13 16:34:06	-	-	Download
			RG-WALL 1600-Z3200-S-APP-LIS-1Y	Not expired	Term license	2023-03-13 ~2024-03-12	2023-03-13 16:34:06	-	-	Download

(2) On the firewall, choose **System** > **System Config** > **Authorization Management** and click **Activate Manually** to upload the license file for offline license activation. For details, see 3.2.3 2. Manual Activation.



Authorization Management

License Config

1. Before activating a device, register on and log in to Ruijie Secure Cloud Platform athttps://secloud1.ruijie.com.cn. On the platform, access the Device Authorization page, and generate a license file. The account of this platform is used for activating and changing device licenses and**must be kept confidential.**)

2. Select an activation mode based on device connection status.**For threat intelligence, only online activation is supported.**

Activate Online

You can choose to perform manual activation.

Device SN:**MACC932672666**

License Info

Performance License

3G/3G

Available Performance:3G(Basic Performance:1G+Added New Performance:2G) Performance to Be Added:0G

SSL VPN License

Max. Concurrent License Sessions25(25 concurrent free license sessions + 0 concurrent purchased license sessions)

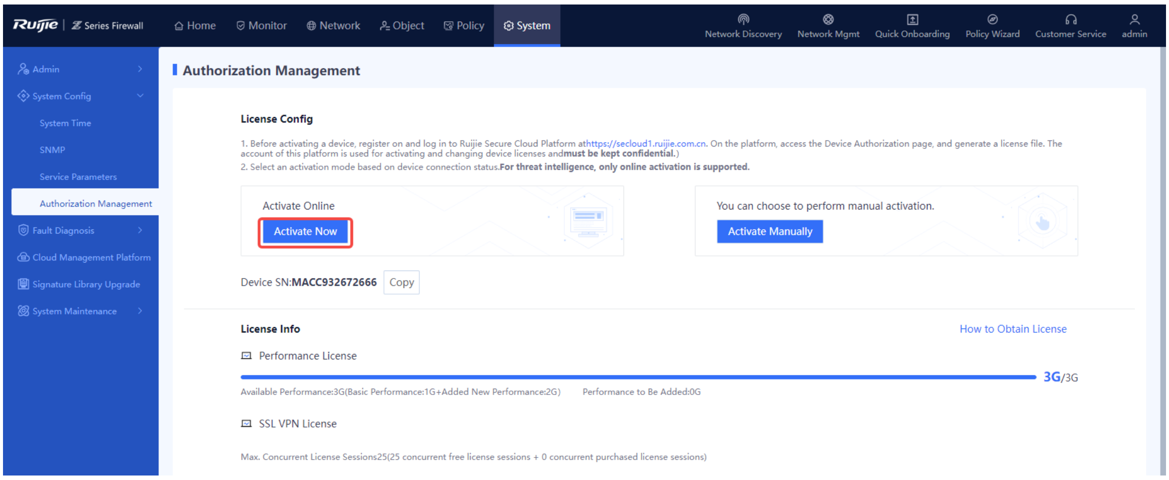
Security Capability License

No.	Security Capability Name	Description	License Type	Status
1	App Identification (APP)	It provides upgrade services for app identification signature libraries.	Formal License	Activated (Expiry Time:2024-03-07)
2	Intrusion Prevention (IPS)	It provides upgrade services for IPS signature libraries.	Formal License	Activated (Expiry Time:2024-03-07)

- Online activation

After the firewall is connected to the Internet, choose **System** > **System Config** > **Authorization Management** on the firewall to perform online activation directly. For details, see 3.2.3 1. Automatic Activation.

.



Authorization Management

License Config

1. Before activating a device, register on and log in to Ruijie Secure Cloud Platform athttps://secloud1.ruijie.com.cn. On the platform, access the Device Authorization page, and generate a license file. The account of this platform is used for activating and changing device licenses and**must be kept confidential.**)

2. Select an activation mode based on device connection status.**For threat intelligence, only online activation is supported.**

Activate Online

Activate Now

You can choose to perform manual activation.

Activate Manually

Device SN:**MACC932672666** Copy

License Info

How to Obtain License

Performance License

3G/3G

Available Performance:3G(Basic Performance:1G+Added New Performance:2G) Performance to Be Added:0G

SSL VPN License

Max. Concurrent License Sessions25(25 concurrent free license sessions + 0 concurrent purchased license sessions)

3.2.3 License Activation Methods

Two license activation methods are available: automatic activation and manual activation.

Caution

The threat intelligence function supports online activation only.

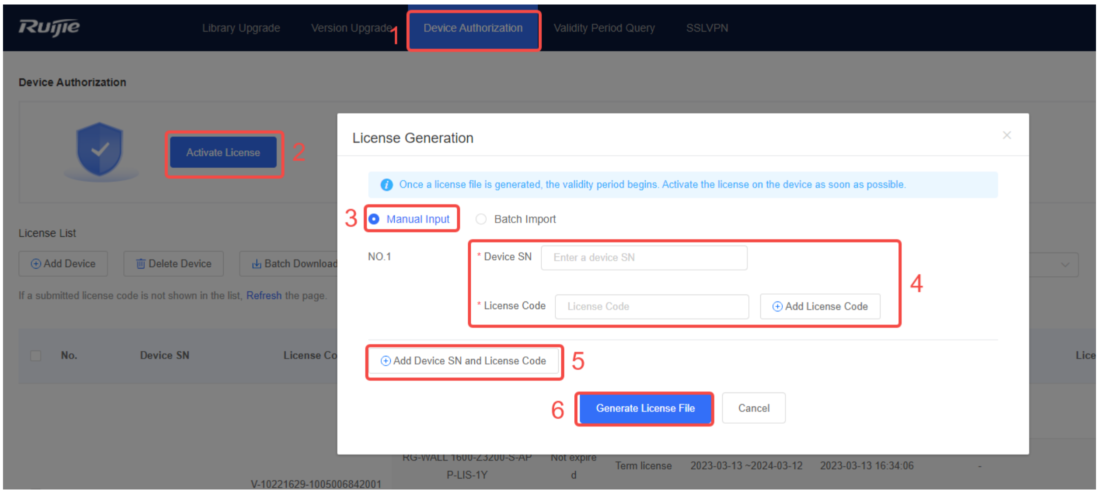
1. Automatic Activation

Application Scenario

When the device is connected to the Internet, you can use the automatic activation method to perform online activation in real time.

Prerequisites

- Automatic activation is supported only when the license code is within the validity period. If the license code has expired (obtaining the validity period in the license file), contact the technical support personnel.
- Before license activation, log in to the Secure Cloud Platform (https://secloud-en.ruijienetworks.com/), choose **Device Authorization** > **Activate License**, and generate a license file.



Once a license file is generated, the validity period begins. Activate the license on the device as soon as possible.

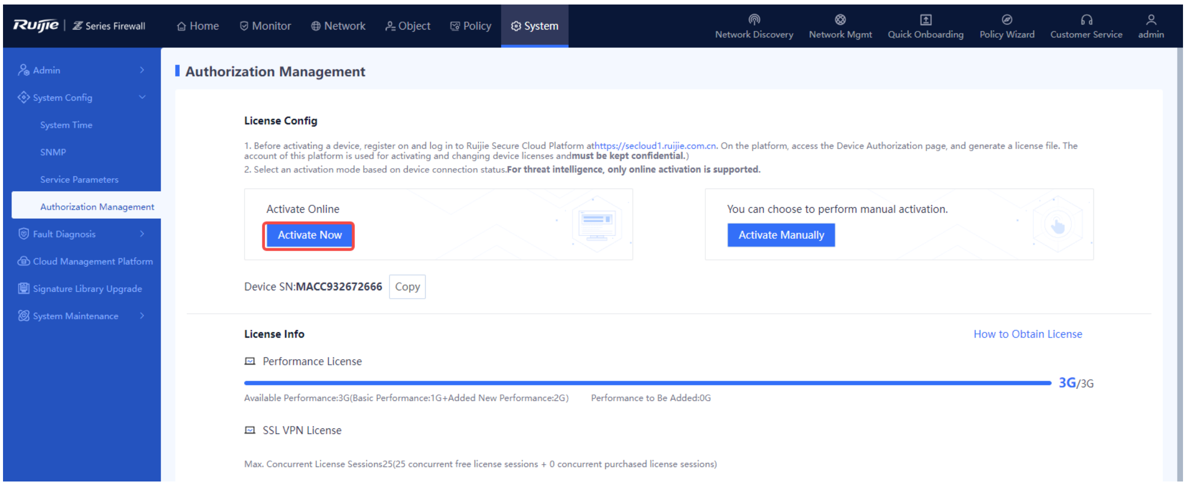
If a submitted license code is not shown in the list, Refresh the page.

V-10221629-1005006842001 RG-WALL 1600-Z3200-S-AP P-LIS-1Y Not expired Term license 2023-03-13 ~2024-03-12 2023-03-13 16:34:06 -

Procedure

(1) Choose **System** > **System Config** > **Authorization Management**.

(2) Click **Activate Now**.



1. Before activating a device, register on and log in to Ruijie Secure Cloud Platform athttps://secloud1.ruijie.com.cn. On the platform, access the Device Authorization page, and generate a license file. The account of this platform is used for activating and changing device licenses and**must be kept confidential.**)

2. Select an activation mode based on device connection status.**For threat intelligence, only online activation is supported.**

You can choose to perform manual activation.

Device SN:**MACC932672666**

Available Performance:3G(Basic Performance:1G+Added New Performance:2G) Performance to Be Added:0G

Max. Concurrent License Sessions25(25 concurrent free license sessions + 0 concurrent purchased license sessions)

Note

NTOS1.0R1P1 and later versions support automatic license activation after the device is connected to the Internet. After the device SN and license code are bound on the cloud platform, you do not need to click **Activate Now** on the device.

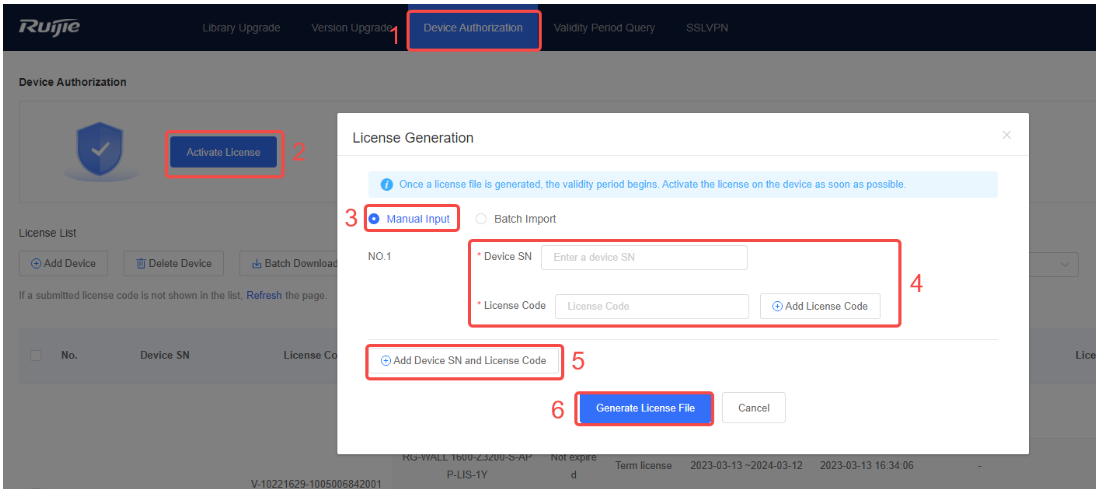
2. Manual Activation

Application Scenario

When the device is not connected to the Internet, you can use the manual activation method to manually upload a license file for activation.

Prerequisites

You have performed the following operations: Log in to the Secure Cloud Platform, and choose **Device Authorization** from the main menu. On the page that is displayed, click **Activate License**, and generate a license file.



Device Authorization

License Generation

Once a license file is generated, the validity period begins. Activate the license on the device as soon as possible.

● Manual Input ○ Batch Import

NO.1

* Device SN: Enter a device SN

* License Code: License Code

If a submitted license code is not shown in the list, Refresh the page.

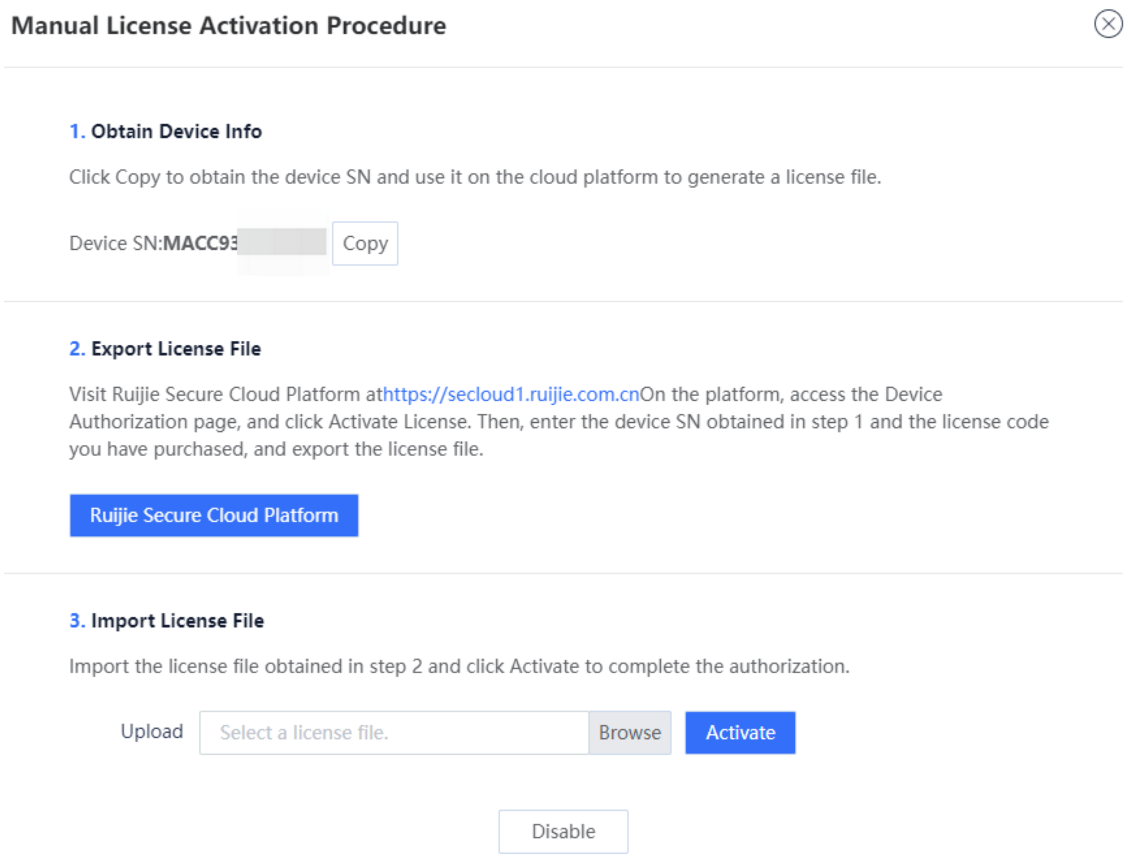
No.	Device SN	License Co					
	V-10221629-1005006842001	RG-WALL 1600-Z3200-S-AP P-LIS-1Y	Not expired	Term license	2023-03-13 ~2024-03-12	2023-03-13 16:34:06	-

Procedure

(1) Choose **System** > **System Config** > **Authorization Management**.

(2) Click **Activate Manually**.

The **Manual License Activation Procedure** page is displayed.



Manual License Activation Procedure

1. Obtain Device Info

Click Copy to obtain the device SN and use it on the cloud platform to generate a license file.

Device SN:MACC93[redacted] Copy

2. Export License File

Visit Ruijie Secure Cloud Platform athttps://secloud1.ruijie.com.cnOn the platform, access the Device Authorization page, and click Activate License. Then, enter the device SN obtained in step 1 and the license code you have purchased, and export the license file.

Ruijie Secure Cloud Platform

3. Import License File

Import the license file obtained in step 2 and click Activate to complete the authorization.

Upload Select a license file. Browse Activate

Disable

(3) Copy the device SN and log in to the Ruijie Secure Cloud Platform to export the license file.

(4) Click **Browse** to upload the license file.

(5) Click **Activate** to activate the license.

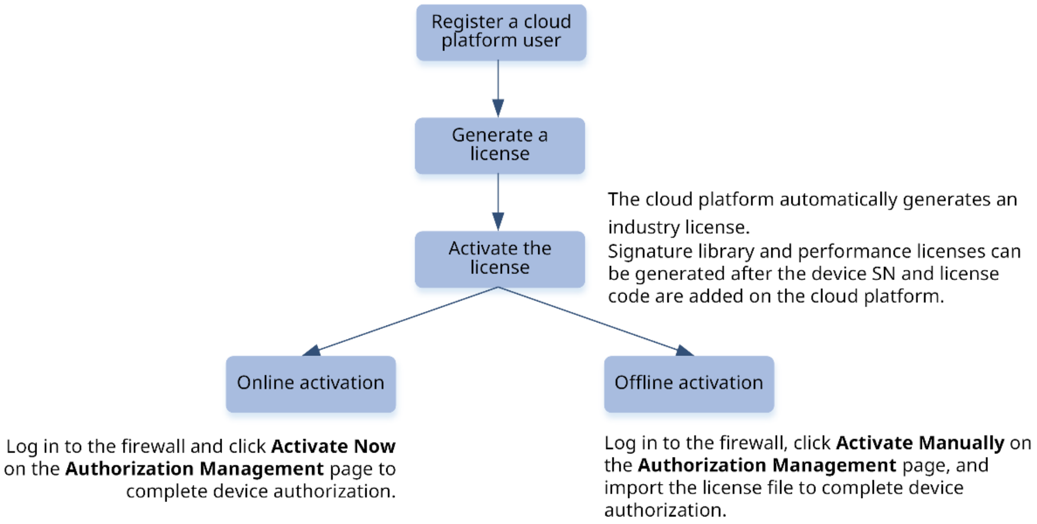
Follow-up Procedure

After license activation, the page displays the activation status of the license.

3.3 Precautions for License Activation

Before using the license activation function, pay attention to the following points:

- After license activation, ensure that DNS is correctly configured for the firewall and the firewall is connected to the Internet all the time.
- Before license activation, log in to the Ruijie Secure Cloud Platform (https://secloud-en.ruijienetworks.com), choose **Device Authorization** > **Activate License**, and generate a license file. (The account of the Secure Cloud Platform is used to activate and change the license. Keep the account safe.)



The cloud platform automatically generates an industry license.
Signature library and performance licenses can be generated after the device SN and license code are added on the cloud platform.

Log in to the firewall and click **Activate Now** on the **Authorization Management** page to complete device authorization.

Log in to the firewall, click **Activate Manually** on the **Authorization Management** page, and import the license file to complete device authorization.

- Automatic activation is supported only when the license code is within the validity period. If the license code has expired (obtaining the validity period in the license file), contact the technical support personnel.

4 Signature Library Upgrade

Some security defense functions of the firewall need to filter data packets based on the signatures contained in the signature libraries. Periodical signature library upgrade enables the firewall to classify and detect data flows based on the latest features of programs and threats that are updated continuously, so that the firewall can identify and defend against various types of attacks to protect internal networks. You are advised to upgrade signature libraries periodically. An upgraded signature library takes effect in security policies immediately, without the need for software upgrade or firewall configuration modification.

All signature library versions become valid only after they are released on the cloud platform. The cloud platform is associated with the order shipping system for you to add device SNs.

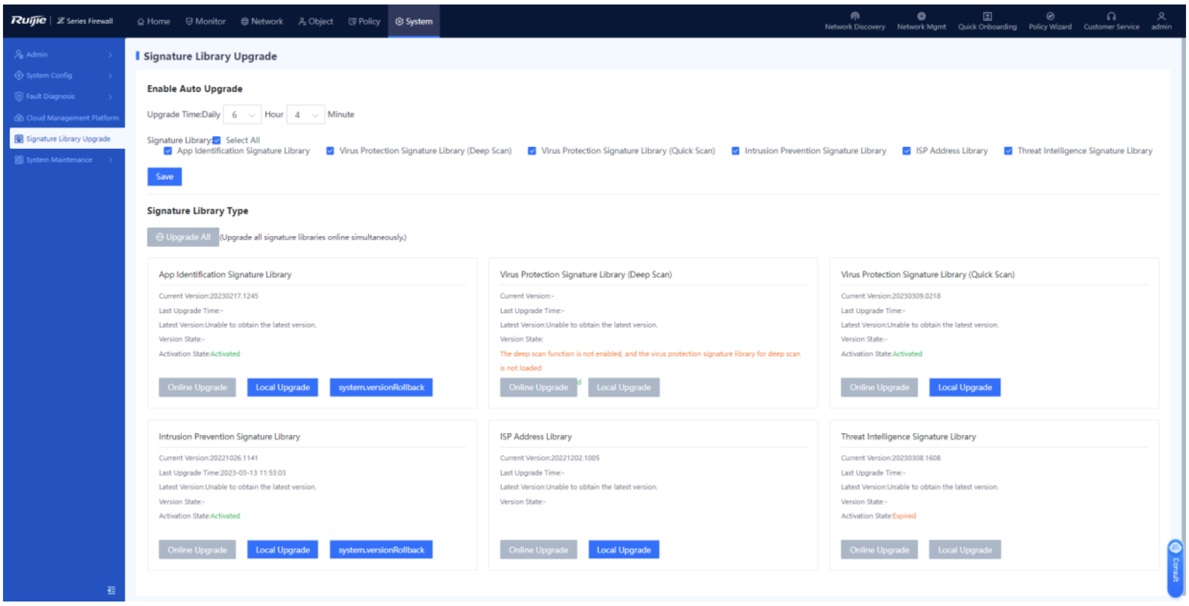
4.1 Configuring Automatic Upgrade

Application Scenario

The system automatically downloads or updates the latest signature library versions from the cloud based on the specified schedule. Automatic upgrade eliminates the need for human intervention and improves the operation efficiency.

Procedure

(1) Choose **System** > **Signature Library Upgrade**.



Signature Library Upgrade

Enable Auto Upgrade

Upgrade Time:Daily 6 Hour 4 Minute

Signature Library: ☑ Select All
☑ App Identification Signature Library ☑ Virus Protection Signature Library (Deep Scan) ☑ Virus Protection Signature Library (Quick Scan) ☑ Intrusion Prevention Signature Library ☑ ISP Address Library ☑ Threat Intelligence Signature Library

Signature Library Type

(Upgrade all signature libraries online simultaneously.)

App Identification Signature Library
Current Version:20230217.1245
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated

Virus Protection Signature Library (Deep Scan)
Current Version:-
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:
The deep scan function is not enabled, and the virus protection signature library for deep scan is not loaded

Virus Protection Signature Library (Quick Scan)
Current Version:20230309.0218
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated

Intrusion Prevention Signature Library
Current Version:20221026.1141
Last Upgrade Time:2023-03-13 11:53:03
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated

ISP Address Library
Current Version:20221202.1005
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-

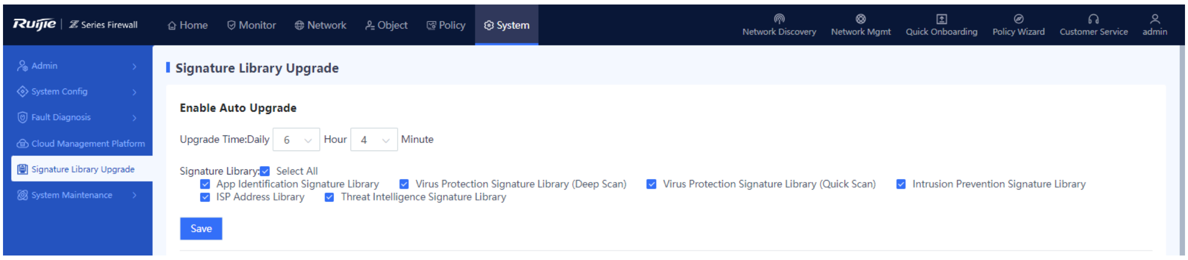
Threat Intelligence Signature Library
Current Version:20230308.1608
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Expired

The system displays information about the current signature libraries:

- **Last Upgrade Time**: displays the last time when a signature library is upgraded.
- **Latest Version**: displays the latest version information and functions and instructs you to upgrade a signature library.

(2) In the **Enable Auto Upgrade** area, configure an automatic upgrade policy for signature libraries.

The system automatically downloads or updates the latest signature library versions from the cloud based on the specified schedule.



Signature Library Upgrade

Enable Auto Upgrade

Upgrade Time:Daily 6 Hour 4 Minute

Signature Library: ☑ Select All
☑ App Identification Signature Library ☑ Virus Protection Signature Library (Deep Scan) ☑ Virus Protection Signature Library (Quick Scan) ☑ Intrusion Prevention Signature Library
☑ ISP Address Library ☑ Threat Intelligence Signature Library

a Set the time for automatic upgrade.

You are advised to configure an off-peak period.

b Select the type of signature library to be upgraded.

(3) Click **Save**.

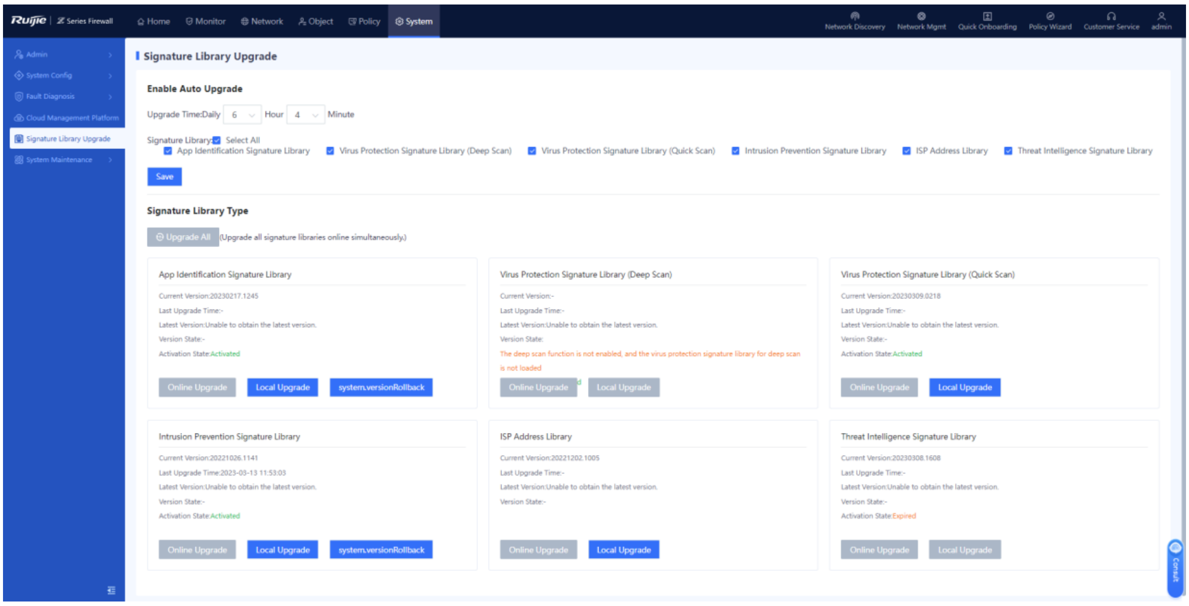
4.2 Local Manual Upgrade

Application Scenario

When the device cannot connect to the Internet or the version server, the system cannot automatically detect whether latest signature library versions are available. In this case, you can complete upgrade in offline manual mode.

Procedure

(1) Choose **System** > **Signature Library Upgrade**.



Signature Library Upgrade

Enable Auto Upgrade

Upgrade Time:Daily 6 Hour 4 Minute

Signature Library: ☑ Select All
☑ App Identification Signature Library ☑ Virus Protection Signature Library (Deep Scan) ☑ Virus Protection Signature Library (Quick Scan) ☑ Intrusion Prevention Signature Library ☑ ISP Address Library ☑ Threat Intelligence Signature Library

Signature Library Type

Upgrade All (Upgrade all signature libraries online simultaneously.)

App Identification Signature Library
Current Version:20230217.1245
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated

Virus Protection Signature Library (Deep Scan)
Current Version:-
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:
The deep scan function is not enabled, and the virus protection signature library for deep scan is not loaded

Virus Protection Signature Library (Quick Scan)
Current Version:20230309.0218
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated

Intrusion Prevention Signature Library
Current Version:20221026.1141
Last Upgrade Time:2023-03-13 11:53:03
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated

ISP Address Library
Current Version:20221202.1005
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-

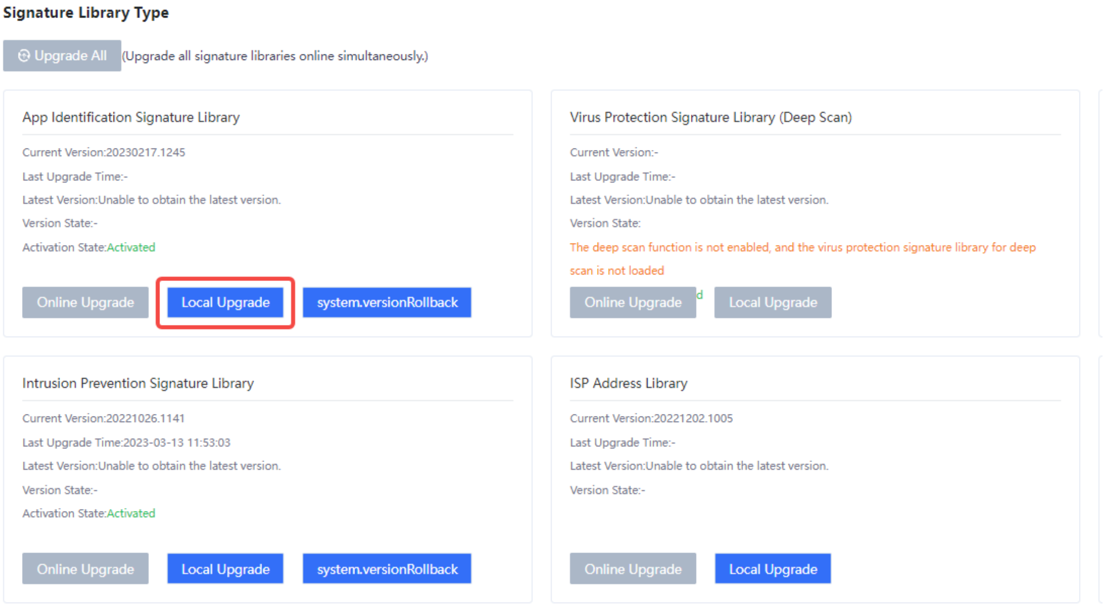
Threat Intelligence Signature Library
Current Version:20230308.1608
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Expired

The system displays information about the current signature libraries:

- **Last Upgrade Time**: displays the last time when a signature library is upgraded.
- **Latest Version**: displays the latest version information and functions and instructs you to upgrade a signature library.

(2) Perform local manual upgrade.

a In the area of a signature library to be upgraded, click **Local Upgrade**.



Signature Library Type

Upgrade All (Upgrade all signature libraries online simultaneously.)

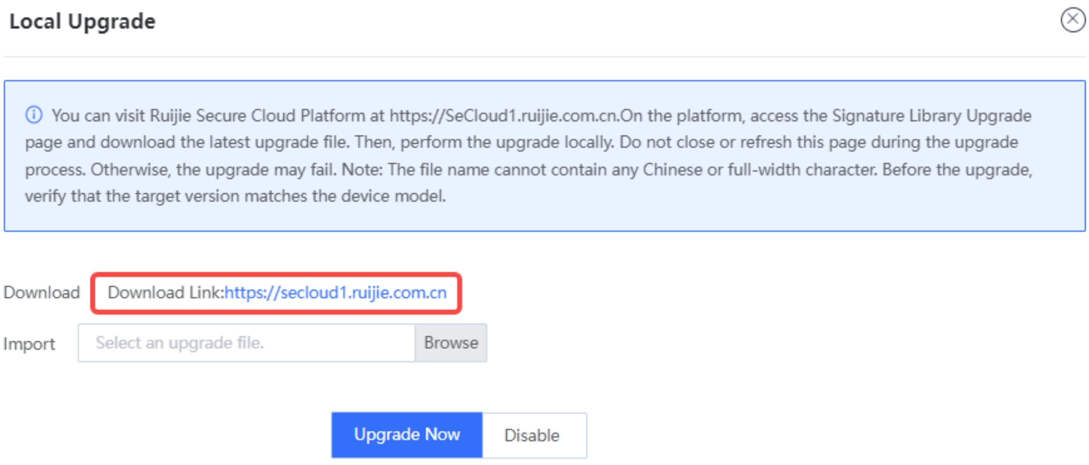
App Identification Signature Library
Current Version:20230217.1245
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated

Virus Protection Signature Library (Deep Scan)
Current Version:-
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:
The deep scan function is not enabled, and the virus protection signature library for deep scan is not loaded

Intrusion Prevention Signature Library
Current Version:20221026.1141
Last Upgrade Time:2023-03-13 11:53:03
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated

ISP Address Library
Current Version:20221202.1005
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-

b (Optional) If no upgrade file is obtained in advance, click the link next to **Download Link** to download the signature library upgrade file from the Secure Cloud Platform.



Local Upgrade

You can visit Ruijie Secure Cloud Platform at https://SeCloud1.ruijie.com.cn.On the platform, access the Signature Library Upgrade page and download the latest upgrade file. Then, perform the upgrade locally. Do not close or refresh this page during the upgrade process. Otherwise, the upgrade may fail. Note: The file name cannot contain any Chinese or full-width character. Before the upgrade, verify that the target version matches the device model.

Download: Download Link:https://secloud1.ruijie.com.cn

Import: Select an upgrade file.

c Click **Browse** to import the upgrade file.

d Click **Upgrade Now**.

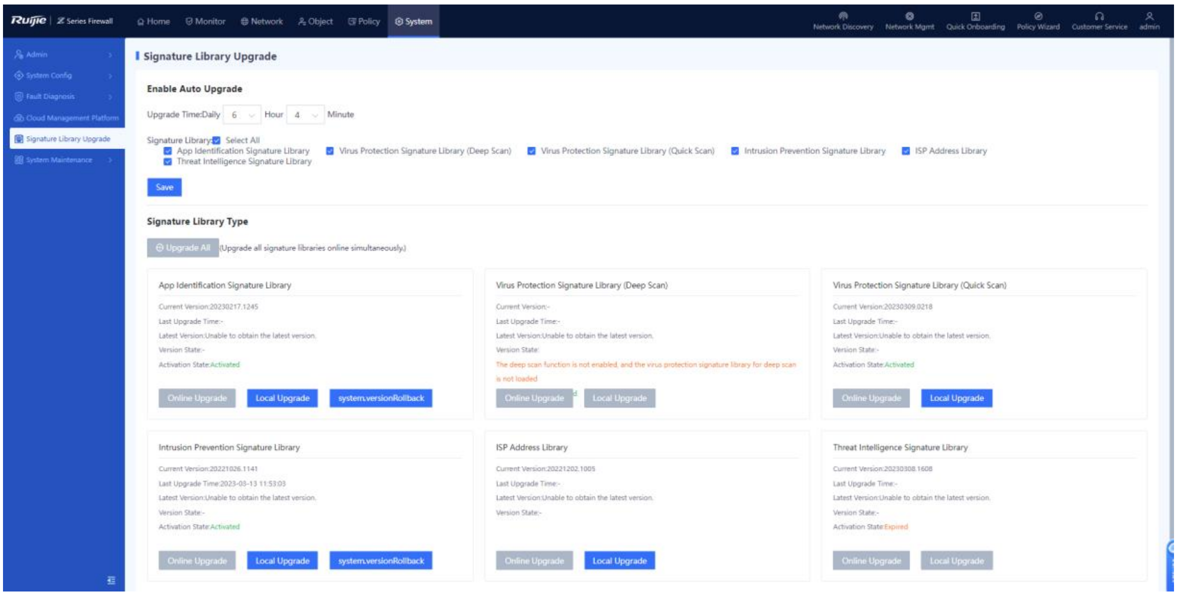
4.3 Online Automatic Upgrade

Application Scenario

When the device is connected to the network and can properly communicate with the version server, if the system automatically detects that latest signature library versions are available, you can complete the upgrade in online automatic mode.

Procedure

(1) Choose **System** > **Signature Library Upgrade**.



Signature Library Upgrade

Enable Auto Upgrade

Upgrade Time:Daily 6 Hour 4 Minute

Signature Library: ☑ Select All
☑ App Identification Signature Library ☑ Virus Protection Signature Library (Deep Scan) ☑ Virus Protection Signature Library (Quick Scan) ☑ Intrusion Prevention Signature Library ☑ ISP Address Library
☑ Threat Intelligence Signature Library

Signature Library Type

(Upgrade all signature libraries online simultaneously.)

App Identification Signature Library
Current Version:20230217.1245
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated

Virus Protection Signature Library (Deep Scan)
Current Version:-
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:
The deep scan function is not enabled, and the virus protection signature library for deep scan is not loaded

Virus Protection Signature Library (Quick Scan)
Current Version:20230309.0218
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated

Intrusion Prevention Signature Library
Current Version:20221026.1141
Last Upgrade Time:2023-03-13 11:53:03
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated

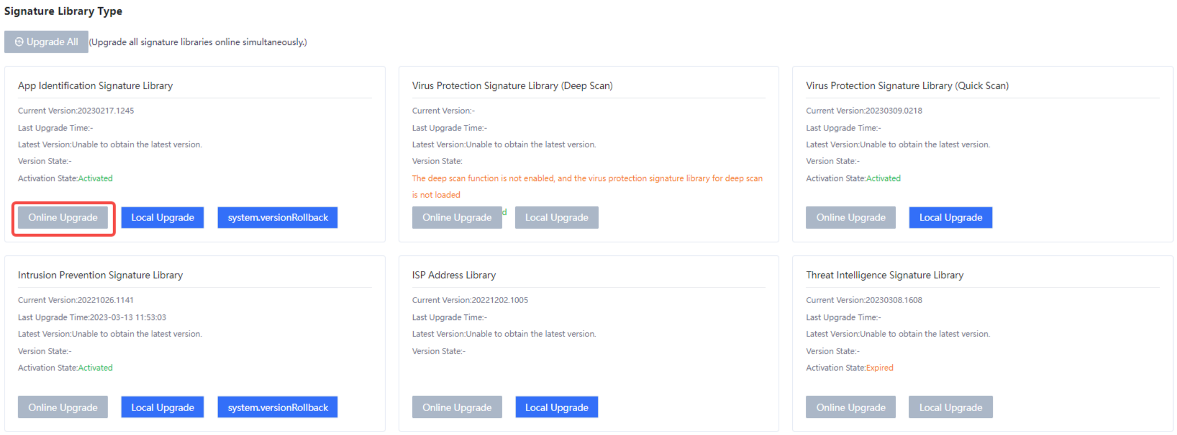
ISP Address Library
Current Version:20221202.1005
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-

Threat Intelligence Signature Library
Current Version:20230308.1608
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Expired

The system displays information about the current signature libraries:

- **Last Upgrade Time**: displays the last time when a signature library is upgraded.
- **Latest Version**: displays the latest version information and functions and instructs you to upgrade a signature library.

(2) In the area of a signature library to be upgraded, click **Online Upgrade**.



Signature Library Type

(Upgrade all signature libraries online simultaneously.)

App Identification Signature Library

Current Version:20230217.1245
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated

Virus Protection Signature Library (Deep Scan)

Current Version:-
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:
The deep scan function is not enabled, and the virus protection signature library for deep scan is not loaded

Virus Protection Signature Library (Quick Scan)

Current Version:20230309.0218
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated

Intrusion Prevention Signature Library

Current Version:20221026.1141
Last Upgrade Time:2023-03-13 11:53:03
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated

ISP Address Library

Current Version:20221202.1005
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-

Threat Intelligence Signature Library

Current Version:20230308.1608
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Expired

Note

When all signature libraries need to be upgraded, click **Upgrade All**.

5 Version Upgrade

5.1 Overview

To use the latest functions of the device, you must upgrade the device software version periodically.

Description of firewall software version:

- The software version of the Z-S series firewall is NTOS1.0RX (X ranges from 1 to 99). The first main version is named R1, and the subsequent versions are named R2, R3... in turn. If the version number contains Release, such as NGFW_NTOS1.0R2, Release(02131401), the number next to Release represents the internal version built-up number, which is used to quickly locate version information.
- The product version number remains unchanged in different development stages of a project, while the release number may change. When the product version number changes, the release version changes too. To use the latest functions of the device, you must upgrade the device software version periodically.
- The software version of the firewall is released and updated from time to time. You need to download the latest software version from the official website or based on the pushed information on the web page of the firewall.

The following describes information of a sample release version.

Note

The file name, MD5 value, and screenshots in this section are for reference only. The file name and MD5 value actually obtained prevail.

File Name	**NGFW_NTOS1.0R2P1_Z5100-S_install.bin**
File Description	System upgrade installation package, universal version
File Size	158,404,288 bytes
Applicable	RG-WALL-1600-Z5100-S

Product	
MD5 Value	415f9d28e04604418e1120ee68964618
Software Version	NGFW_NTOS1.0R2P1

⚠ **Caution**

- You can upgrade the software version on the site only after upgrade is verified in the lab environment.
- Before upgrade on the site, configurations of the customer must be backed up.
- If a prompt message for restart forbidden is displayed during the upgrade process, do not power off the firewall, reset the system, or remove and insert modules.

5.2 Upgrade Operations

ℹ **Note**

The version information in the screenshots in the procedure is for reference only. The version information obtained from the release note of the product prevails.

5.2.1 Offline Upgrade

Application Scenario

When a network exception occurs, the system cannot automatically obtain the latest software version. You can upgrade or roll back the software version in offline mode.

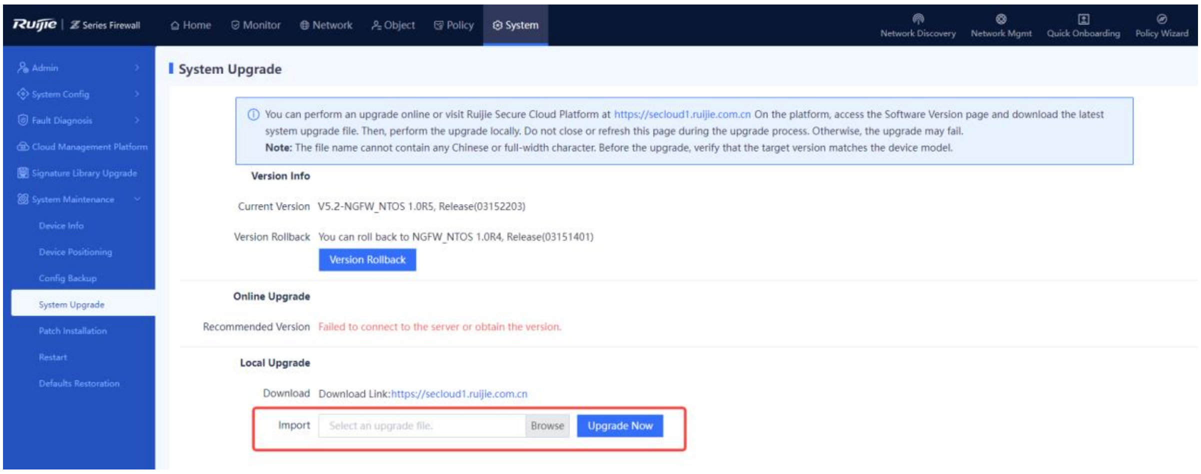
Prerequisites

An upgrade file is obtained in advance.

Procedure

(1) Choose **System** > **System Maintenance** > **System Upgrade**.

The **System Upgrade** page is displayed.



System Upgrade

You can perform an upgrade online or visit Ruijie Secure Cloud Platform at https://secloud1.ruijie.com.cn On the platform, access the Software Version page and download the latest system upgrade file. Then, perform the upgrade locally. Do not close or refresh this page during the upgrade process. Otherwise, the upgrade may fail.
Note: The file name cannot contain any Chinese or full-width character. Before the upgrade, verify that the target version matches the device model.

Version Info

Current Version V5.2-NGFW_NTOS 1.0R5, Release(03152203)

Version Rollback You can roll back to NGFW_NTOS 1.0R4, Release(03151401)

Online Upgrade

Recommended Version Failed to connect to the server or obtain the version.

Local Upgrade

Download Download Link:https://secloud1.ruijie.com.cn

Import Select an upgrade file.

(2) (Optional) If no upgrade file is obtained in advance, click the link next to **Download Link** to download the upgrade file.

(3) In the **Local Upgrade** area, click **Browse** and select an applicable upgrade file.

(4) Click **Upgrade Now** to start system upgrade.

After successful upgrade, you can choose to make the upgrade take effect immediately or upon next restart as prompted.

Follow-up Procedure

Choose **System** > **System Maintenance** > **Device Info** to view the software version information and confirm whether the upgrade is successful.

Caution

If the version information after the upgrade differs from the target upgrade version, perform the upgrade operation again. If the upgrade fails again, contact the technical support personnel.

5.2.2 Online Upgrade

Application Scenario

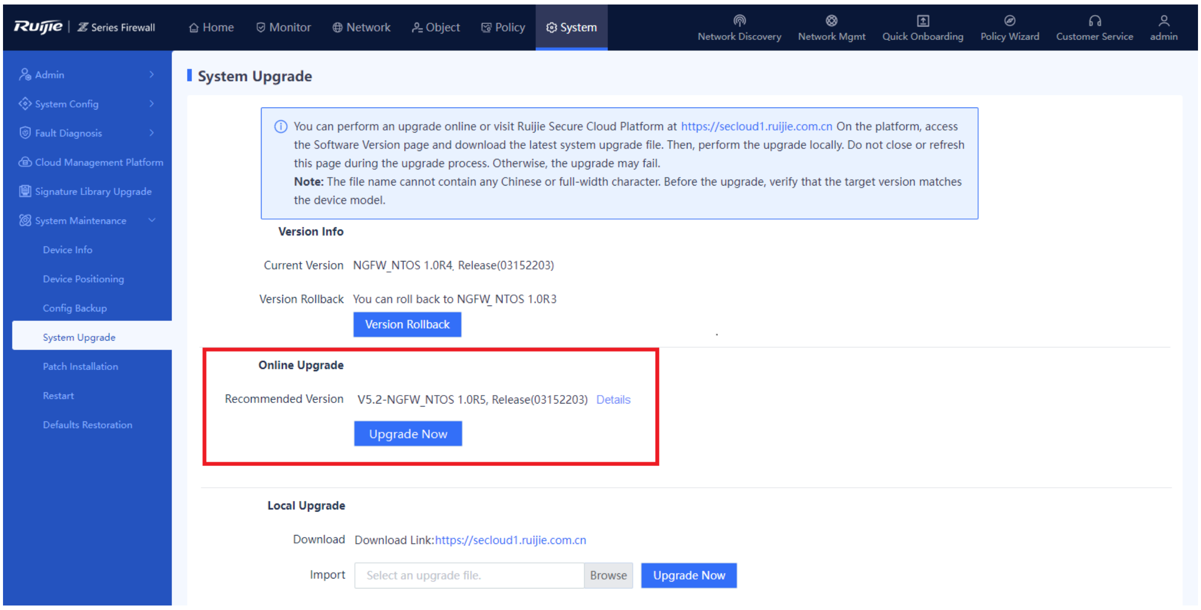
When the network communication is normal and the system displays a recommended version, you can upgrade the software version in online mode.

Procedure

(1) Choose **System** > **System Maintenance** > **System Upgrade**.

The **System Upgrade** page is displayed.

(2) In the **Online Upgrade** area, click **Upgrade Now**.



System Upgrade

You can perform an upgrade online or visit Ruijie Secure Cloud Platform at https://secloud1.ruijie.com.cn On the platform, access the Software Version page and download the latest system upgrade file. Then, perform the upgrade locally. Do not close or refresh this page during the upgrade process. Otherwise, the upgrade may fail.

Note: The file name cannot contain any Chinese or full-width character. Before the upgrade, verify that the target version matches the device model.

Version Info

Current Version NGFW_NTOS 1.0R4, Release(03152203)

Version Rollback You can roll back to NGFW_NTOS 1.0R3

Online Upgrade

Recommended Version V5.2-NGFW_NTOS 1.0R5, Release(03152203)

Local Upgrade

Download Download Link:https://secloud1.ruijie.com.cn

Import Select an upgrade file.

(3) Read the prompt information and click **Confirm**.

The system starts system upgrade automatically.

Follow-up Procedure

Choose **System** > **System Maintenance** > **Device Info** to view the software version information and confirm whether the upgrade is successful.

Caution

If the version information after the upgrade differs from the target upgrade version, perform the upgrade operation again. If the upgrade fails again, contact the technical support personnel.

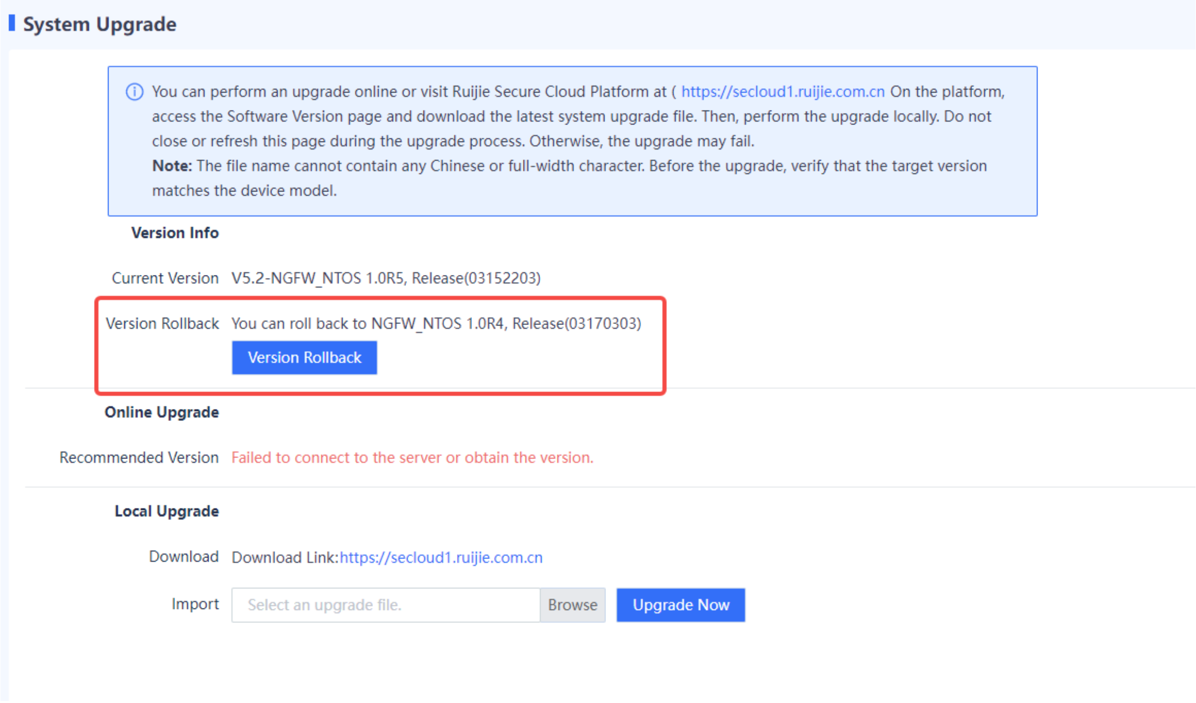
5.2.3 Version Rollback

Application Scenario

When an upgrade file of a previous version exists on the device, the system automatically displays the information about the version to which the system can be rolled back.

Procedure

(1) Choose **System** > **System Maintenance** > **System Upgrade**.



System Upgrade

ⓘ You can perform an upgrade online or visit Ruijie Secure Cloud Platform at (https://secloud1.ruijie.com.cn On the platform, access the Software Version page and download the latest system upgrade file. Then, perform the upgrade locally. Do not close or refresh this page during the upgrade process. Otherwise, the upgrade may fail.
Note: The file name cannot contain any Chinese or full-width character. Before the upgrade, verify that the target version matches the device model.

Version Info

Current Version V5.2-NGFW_NTOS 1.0R5, Release(03152203)

Version Rollback You can roll back to NGFW_NTOS 1.0R4, Release(03170303)

Online Upgrade

Recommended Version Failed to connect to the server or obtain the version.

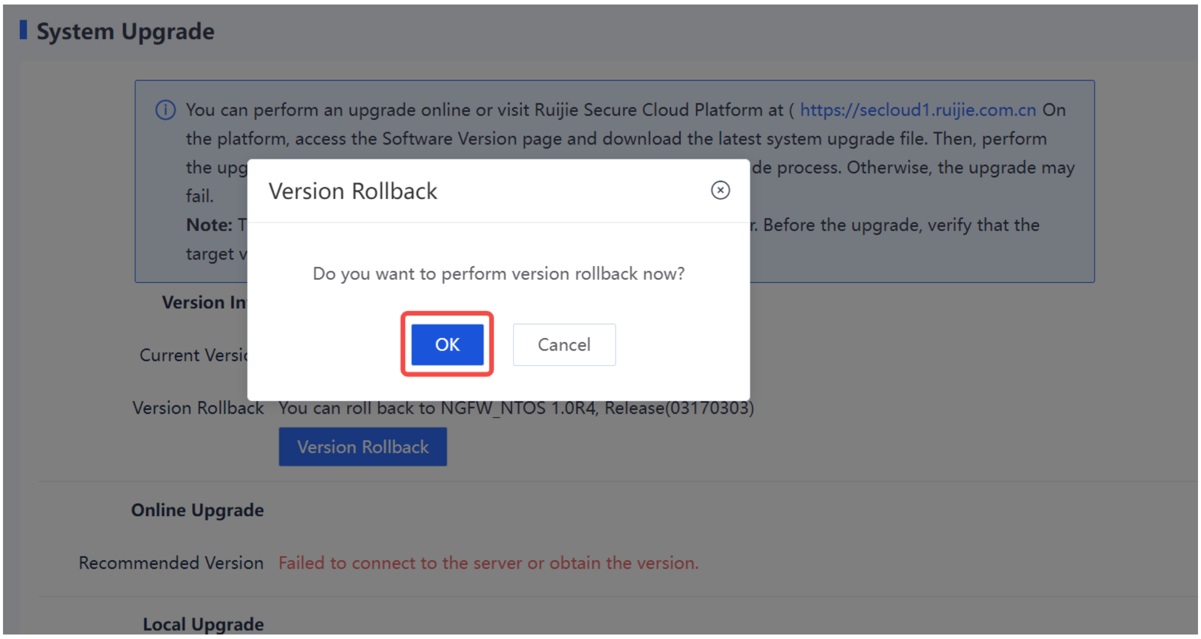
Local Upgrade

Download Download Link:https://secloud1.ruijie.com.cn

Import Select an upgrade file.

(2) In the **Version Info** area, click **Version Rollback**.

(3) In the dialog box that is displayed, click **OK**. The system is rolled back to the specified version.



System Upgrade

ⓘ You can perform an upgrade online or visit Ruijie Secure Cloud Platform at (https://secloud1.ruijie.com.cn On the platform, access the Software Version page and download the latest system upgrade file. Then, perform the upg de process. Otherwise, the upgrade may fail.
Note: T . Before the upgrade, verify that the target v

Version Rollback

Do you want to perform version rollback now?

Version In

Current Versi

Version Rollback You can roll back to NGFW_NTOS 1.0R4, Release(03170303)

Online Upgrade

Recommended Version Failed to connect to the server or obtain the version.

Local Upgrade

6 Configuration Examples for Typical Scenarios

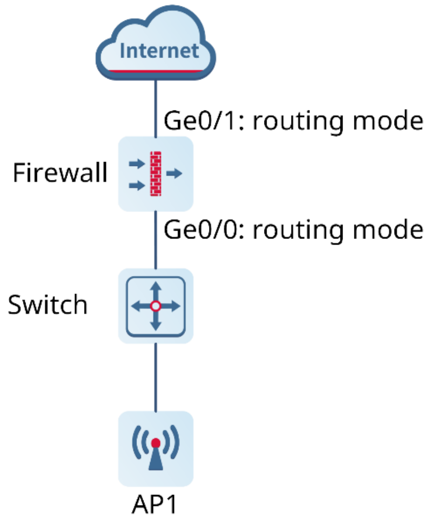
6.1 Integrated Deployment on Ruijie Cloud

As the firewall has complex functions, technical personnel may be unable to or fail to configure some functions during actual network deployment. Therefore, the firewall provides the quick deployment function (with new network discovery, network-wide management, and cloud management capabilities) to add the firewall to the current network through new network discovery, helping you quickly deploy the firewall on the site. If you cannot configure complex services, you can contact Ruijie engineers to perform remote configuration using the Ruijie Cloud platform.

6.1.1 Firewall Deployment (Routing Mode)

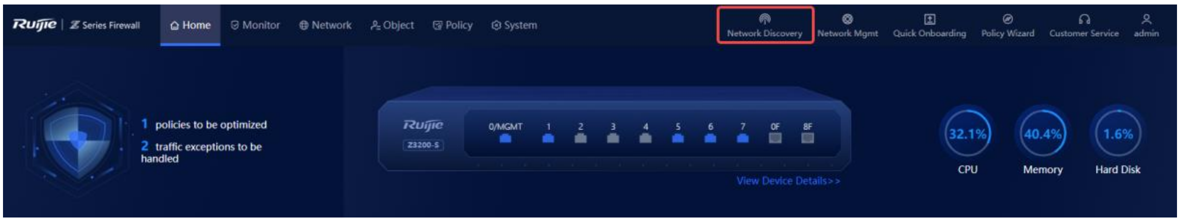
1. Application Scenario

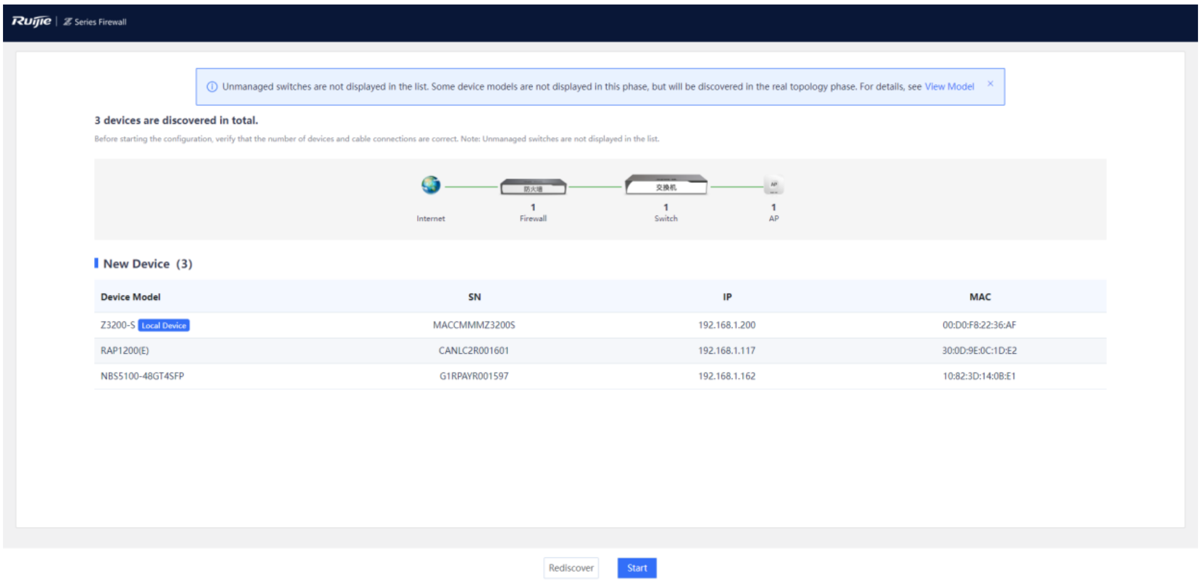
The firewall functions as an egress router and it is uplinked to the Internet and downlinked to a switch. You are advised to deploy the firewall in routing mode. The uplink interface is configured to work in routing mode to access the Internet and the downlink interface is configured to work in routing mode.



2. Procedure

(1) Click **Network Discovery**. The current networking information is displayed.





ⓘ Unmanaged switches are not displayed in the list. Some device models are not displayed in this phase, but will be discovered in the real topology phase. For details, see View Model ×

3 devices are discovered in total.

Before starting the configuration, verify that the number of devices and cable connections are correct. Note: Unmanaged switches are not displayed in the list.

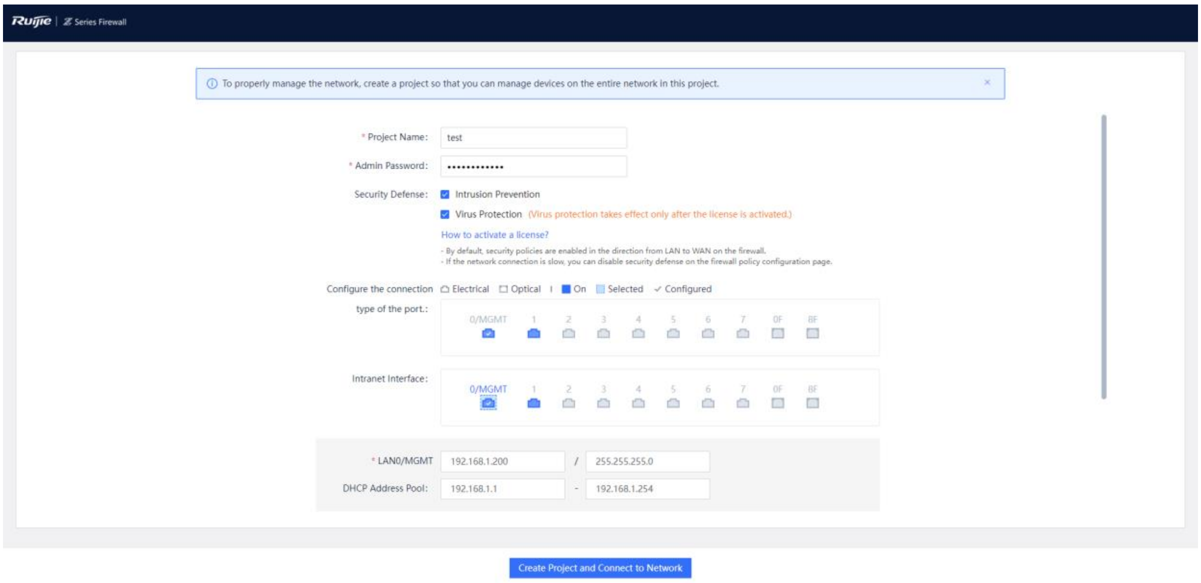
New Device (3)

Device Model	SN	IP	MAC
Z3200-S Local Device	MACCMMMZ3200S	192.168.1.200	00:D0:F8:22:36:AF
RAP1200(E)	CANLC2R001601	192.168.1.117	30:0D:9E:0C:1D:E2
NBS5100-48GT4SFP	G1RPAYR001597	192.168.1.162	10:82:3D:14:0B:E1

(2) Click **Start**. Enter the network project name and configure a port IP address as prompted.

Note

- The DHCP server function is enabled on the firewall by default, and the default DHCP address pool is configured on the management port.
- Intrusion prevention and virus protection are enabled on the firewall by default. You can choose to disable these functions based on actual needs. The virus protection function takes effect only after a license is uploaded. For details about license activation, click **How to activate a license?** and scan the QR code to view the license activation video.



Ruijie | Z Series Firewall

ⓘ To properly manage the network, create a project so that you can manage devices on the entire network in this project. ×

* Project Name: test

* Admin Password: ••••••••••••

Security Defense: ☑ Intrusion Prevention

☑ Virus Protection (Virus protection takes effect only after the license is activated.)

How to activate a license?

- By default, security policies are enabled in the direction from LAN to WAN on the firewall.
- If the network connection is slow, you can disable security defense on the firewall policy configuration page.

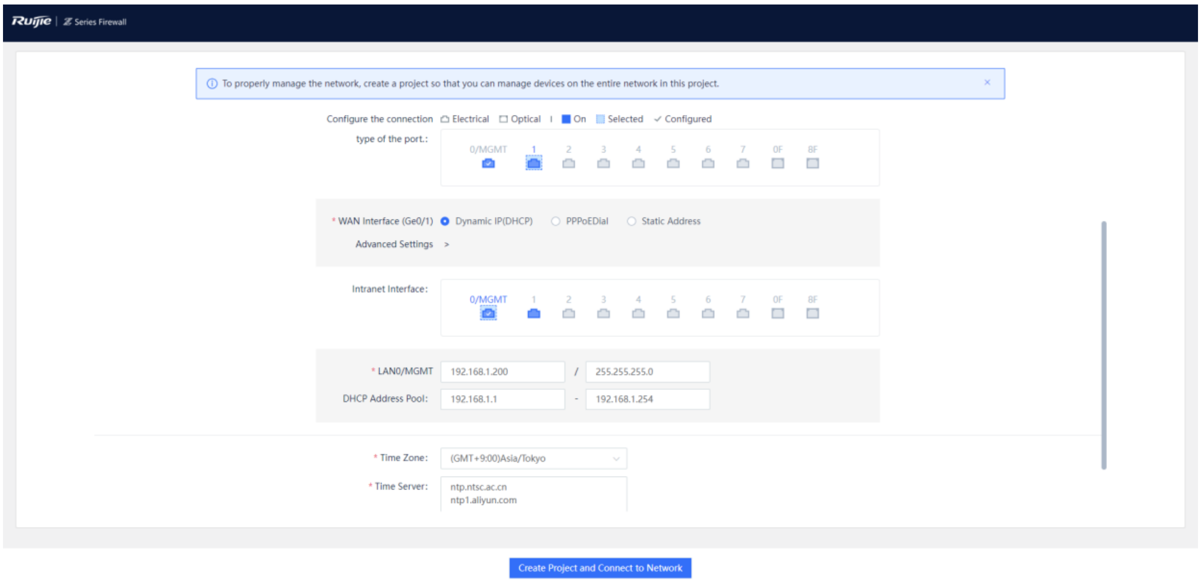
Configure the connection type of the port.: Electrical □ Optical I ■ On ▨ Selected ✓ Configured

Intranet Interface:

* LAN0/MGMT 192.168.1.200 / 255.255.255.0

DHCP Address Pool: 192.168.1.1 - 192.168.1.254

Create Project and Connect to Network



Ruijie | Z Series Firewall

ⓘ To properly manage the network, create a project so that you can manage devices on the entire network in this project. ×

Configure the connection type of the port.: Electrical □ Optical I ■ On ▨ Selected ✓ Configured

* WAN Interface (Ge0/1) ● Dynamic IP(DHCP) ○ PPPoEDial ○ Static Address

Advanced Settings >

Intranet Interface:

* LAN0/MGMT 192.168.1.200 / 255.255.255.0

DHCP Address Pool: 192.168.1.1 - 192.168.1.254

* Time Zone: (GMT+9:00)Asia/Tokyo

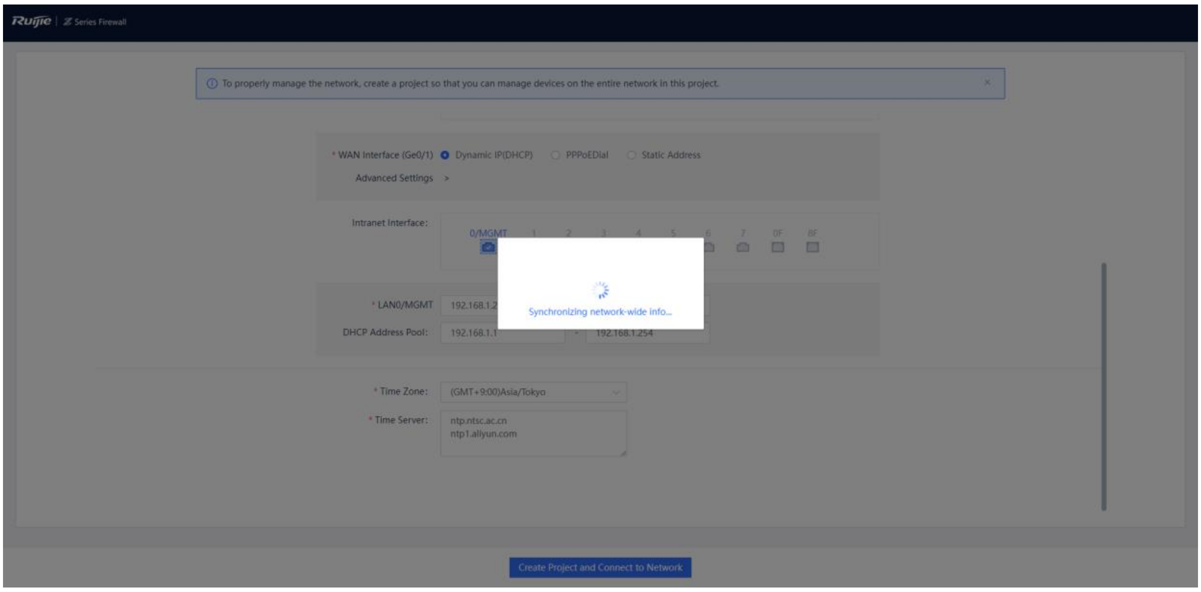
* Time Server: ntp.ntsc.ac.cn
ntp1.aliyun.com

Create Project and Connect to Network

Item	Description	Remarks
WAN Interface	Connects the firewall to the Internet. Generally, the WAN interface is directly connected to the fiber to the home (FTTH) Optical Network Unit (ONU) of the ISP. Three methods are available for a WAN interface to obtain an IP address: ● **Dynamic IP (DHCP)**: Applicable when no professional network administrator is available. The user terminal automatically obtains an IP address to access the Internet	[Example] Ge0/1 Dynamic IP (DHCP)

Item	Description	Remarks
	after the terminal is connected to the firewall. ● **PPPoE**: Applicable for dialup access to the ISP network. The username and password of the dialup user must be configured. ● **Static Address**: Applicable when the network administrator specifies an IP address for the device based on the predefined IP address planning. This connection type requires the network administrator to possess certain network knowledge. The IP address/mask and next-hop address must be configured.	
LAN Interface	Connects to the LAN. The LAN interface IP address must be configured based on the predefined IP address planning.	[Example] 192.168.1.1/24

(3) Click **Create Project and Connect to Network**. The system delivers configuration information.



To properly manage the network, create a project so that you can manage devices on the entire network in this project.

* WAN Interface (Ge0/1) ● Dynamic IP(DHCP) ○ PPPoEDial ○ Static Address

Advanced Settings >

Intranet Interface: 0/MGMT 1 2 3 4 5 6 7 0F 8F

* LAN0/MGMT 192.168.1.2

DHCP Address Pool: 192.168.1.1 - 192.168.1.254

* Time Zone: (GMT+9:00)Asia/Tokyo

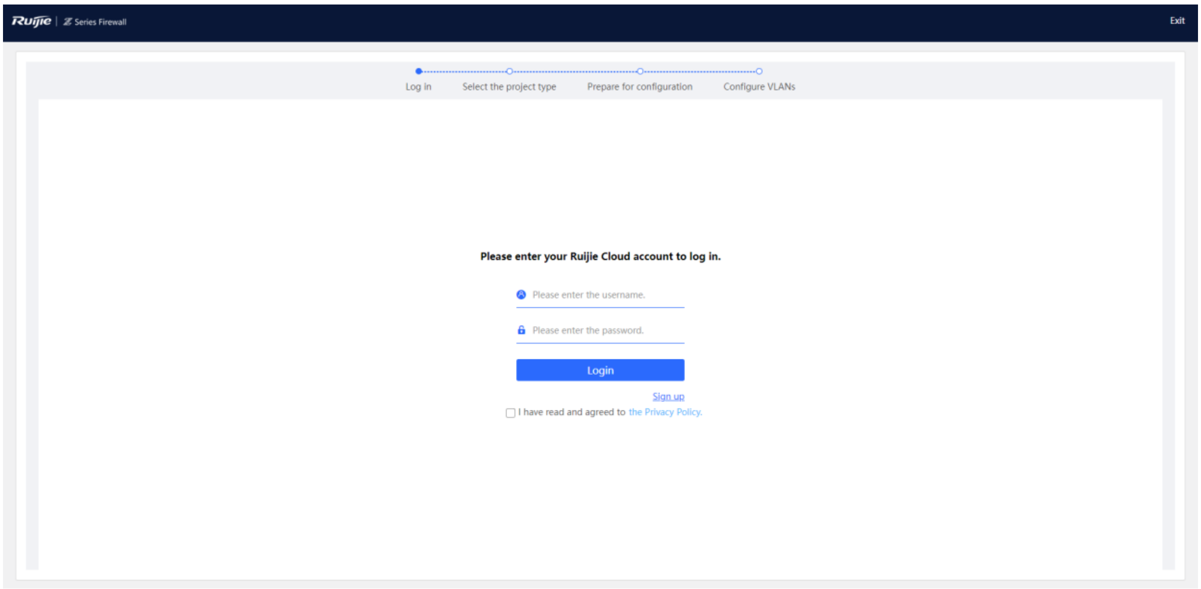
* Time Server: ntp.ntsc.ac.cn
ntp1.aliyun.com

Synchronizing network-wide info...

(4) Check the system prompt. A prompt indicating successful configuration is displayed after the configurations are completed. You can scan the username and password to log in to Ruijie Cloud and migrate the firewall to the cloud.

Note

After successful configuration, the firewall automatically adds the IP address of the DHCP server in the networking to the allowlist and generates a security policy (with the name **trust-untrust** and enabled with intrusion prevention).

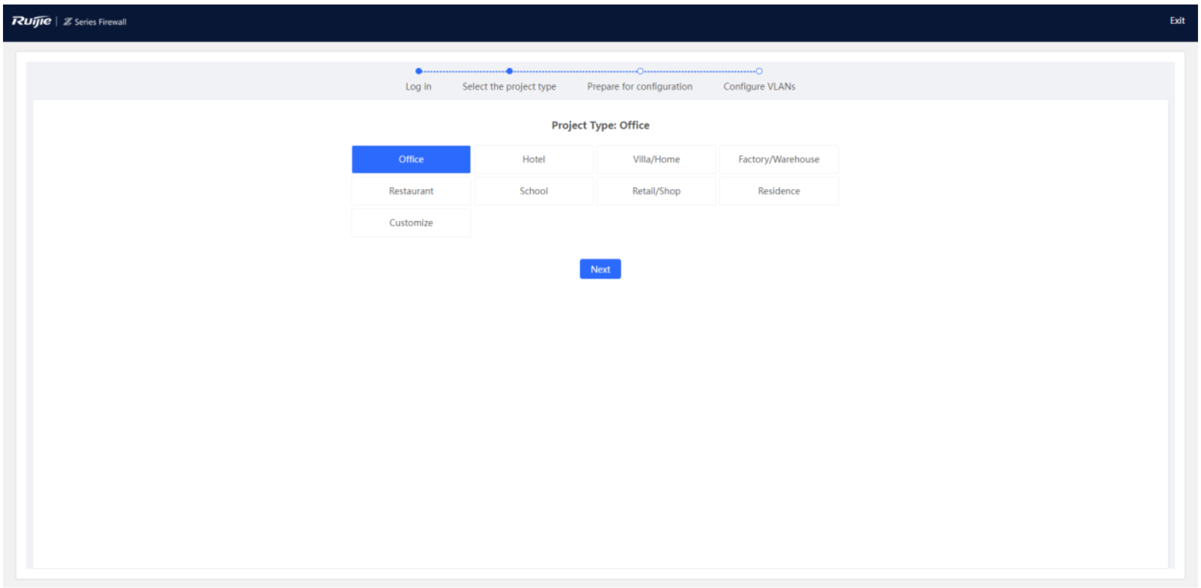

Ruijie | Z Series Firewall
Exit
Log in
Select the project type
Prepare for configuration
Configure VLANs
Please enter the username.
Please enter the password.
Login
Sign up
□ I have read and agreed to the Privacy Policy.

Please enter your Ruijie Cloud account to log in.

Note

If the firewall has been bound to the Ruijie Cloud platform, the following dialog box is displayed. Click **Go to Ruijie Cloud for Network Management** to go to the Ruijie Cloud platform and manage the device. Click **Return to EWEB Homepage** to return to the home page of the firewall.

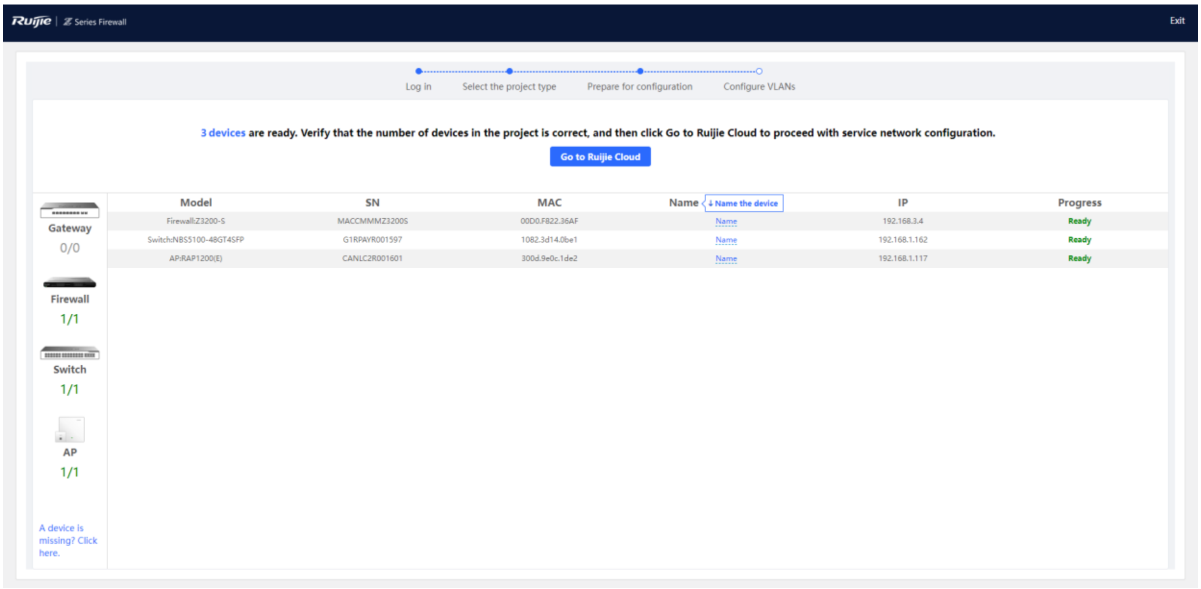
(5) After successful login, select a project type based on the actual networking scenario and click **Next**. The initial configuration delivered varies by the project type, so the project type must be set based on the actual service scenario.



Project Type: Office

(6) Wait until preparations before configuration are complete and then configure the service network.

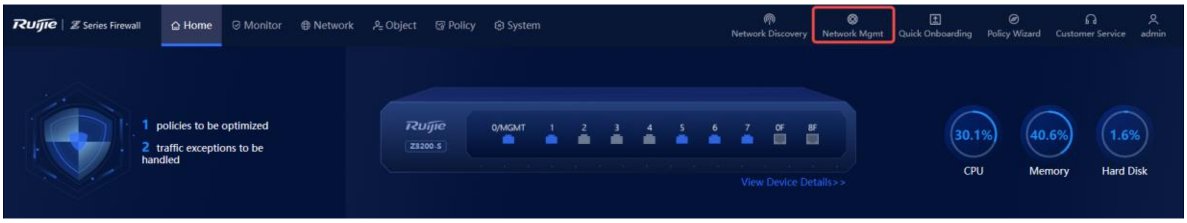
(7) After all devices go online, click **Go to the cloud platform for management** and perform service configuration on the Ruijie Cloud platform.



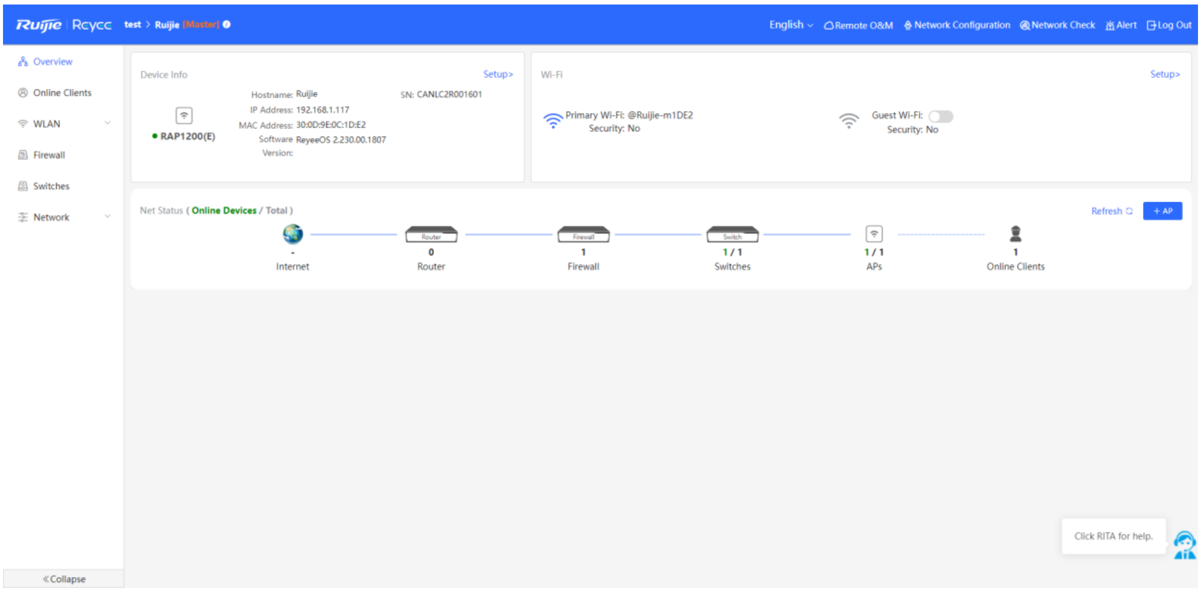
3 devices are ready. Verify that the number of devices in the project is correct, and then click Go to Ruijie Cloud to proceed with service network configuration.

Model	SN	MAC	Name ↓Name the device	IP	Progress
Firewall:Z3200-S	MACCMMMZ3200S	00D0.F822.36AF	Name	192.168.3.4	Ready
Switch:NBS5100-48GT4SFP	G1RPAYR001597	1082.3d14.0be1	Name	192.168.1.162	Ready
AP:RAP1200(E)	CANLC2R001601	300d.9e0c.1de2	Name	192.168.1.117	Ready

(8) (Optional) After service configuration is complete, click **Network Mgmt** on the firewall to switch to the web management page of the master device. You can view the current network topology and device information in the networking on the master device and manage network-wide devices.



The following figure shows the **Overview** page of the master device.



RAP1200(E)

Hostname: Ruijie
SN: CANLC2R001601
IP Address: 192.168.1.117
MAC Address: 30:0D:9E:0C:1D:E2
Software Version: ReyeeOS 2.230.00.1807

Primary Wi-Fi: @Ruijie-m1DE2
Security: No

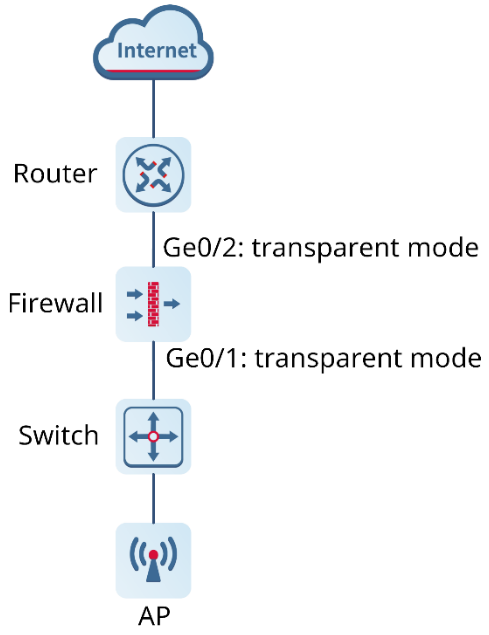
Guest Wi-Fi:
Security: No

Internet	Router	Firewall	Switches	APs	Online Clients
-	0	1	1 / 1	1 / 1	1

6.1.2 NBR Deployment (Transparent Mode)

1. Application Scenario

When the firewall is uplinked to a router and downlinked to a switch, the transparent mode is recommended. You can configure the uplink and downlink ports of the firewall to work in transparent mode. In this example, the router refers to RG-NBR6210-E (hereinafter referred to as the NBR). You can select a router of another model based on needs in the actual service scenario.



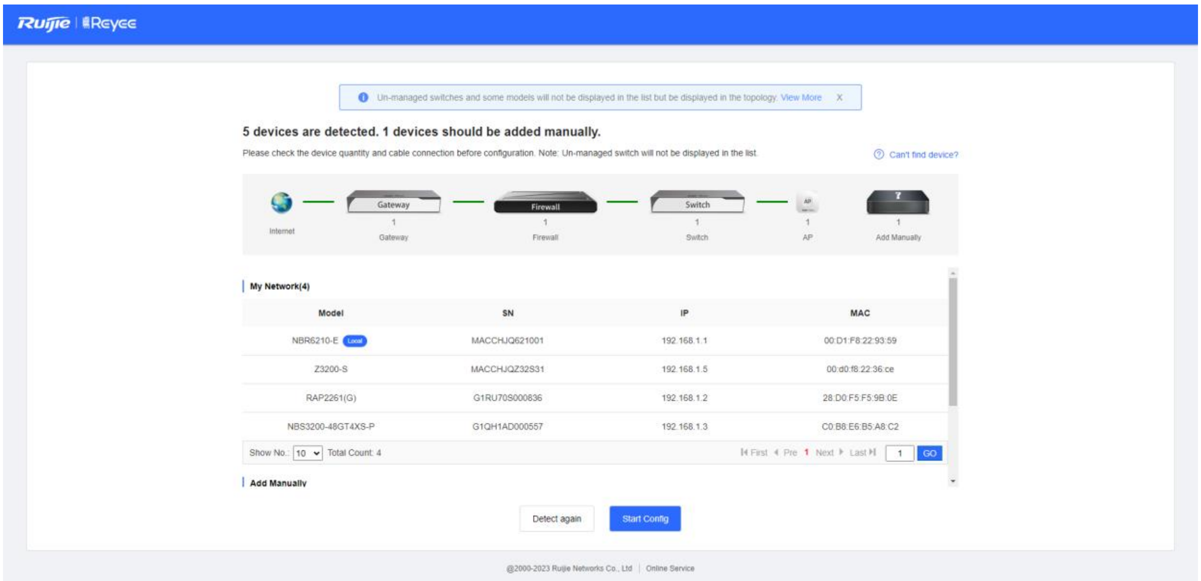
2. Procedure

(1) After a network is deployed according to the preceding figure, connect the PC to the management interface of the NBR and set the IP addresses of the PC and the management interface of the NBR to be on the same network segment to ensure that the PC can access the web page of the NBR.

Note

The IP address of the management interface Gi0/0 of RG-NBR6210-E is set to 192.168.1.1/24 upon factory delivery, and the default login username and password are **admin** and **admin**.

(2) Log in to the web page of the NBR. The following page is displayed by default. Click **Start**.



Un-managed switches and some models will not be displayed in the list but be displayed in the topology. View More X

5 devices are detected. 1 devices should be added manually.

Please check the device quantity and cable connection before configuration. Note: Un-managed switch will not be displayed in the list.

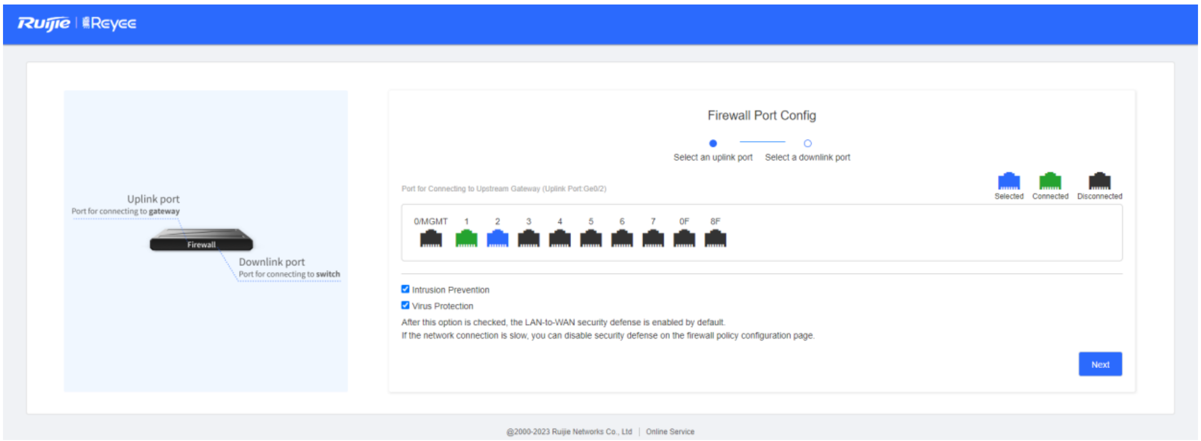
My Network(4)

Model	SN	IP	MAC
NBR6210-E Local	MACCHJQ621001	192.168.1.1	00:D1:F8:22:93:59
Z3200-S	MACCHJQZ32S31	192.168.1.5	00:d0:f8:22:36:ce
RAP2261(G)	G1RU70S000836	192.168.1.2	28:D0:F5:F5:9B:0E
NBS3200-48GT4XS-P	G1QH1AD000557	192.168.1.3	C0:B8:E6:B5:A8:C2

Show No.: 10 Total Count: 4

Add Manually

(3) Select the WAN interface (interface connected to the gateway, Ge0/2 in this example) of the firewall based on the actual networking and click **Next**.



Firewall Port Config

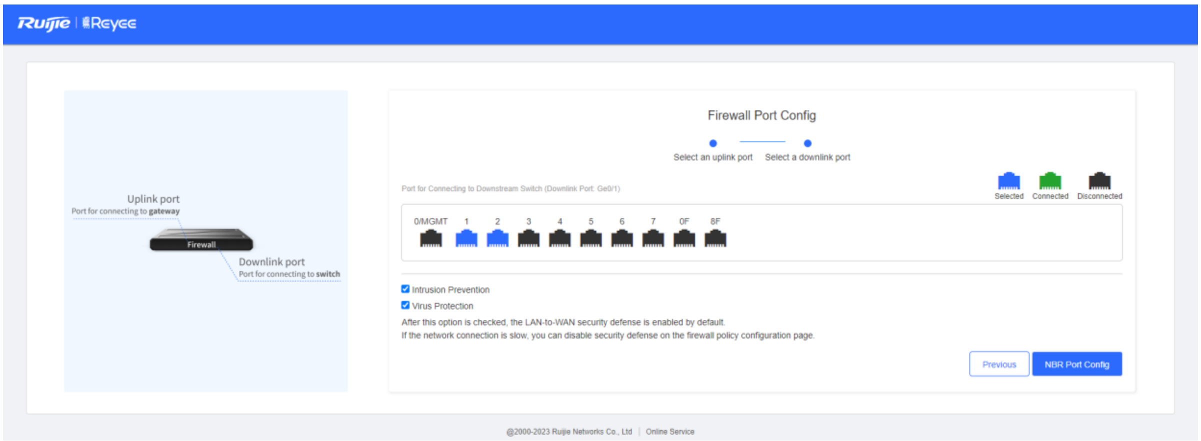
Port for Connecting to Upstream Gateway (Uplink Port Ge0/2)

☑ Intrusion Prevention

☑ Virus Protection

After this option is checked, the LAN-to-WAN security defense is enabled by default.
If the network connection is slow, you can disable security defense on the firewall policy configuration page.

(4) Select the LAN interface (interface connected to the switch, Ge0/1 in this example) of the firewall based on the actual networking and click **NBR Port Config**.



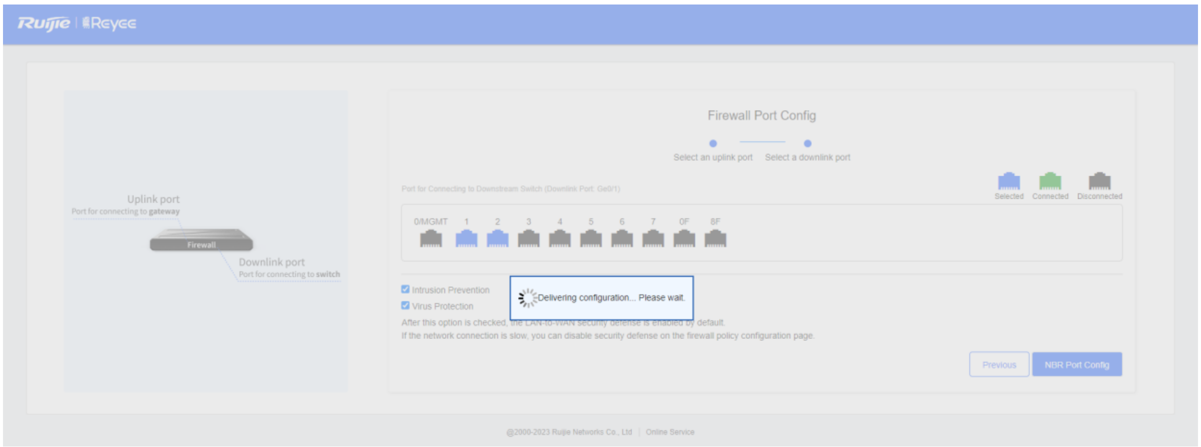
Firewall Port Config

Port for Connecting to Downstream Switch (Downlink Port: Ge0/1)

☑ Intrusion Prevention

☑ Virus Protection

After this option is checked, the LAN-to-WAN security defense is enabled by default.
If the network connection is slow, you can disable security defense on the firewall policy configuration page.



Firewall Port Config

Port for Connecting to Downstream Switch (Downlink Port: Ge0/1)

☑ Intrusion Prevention

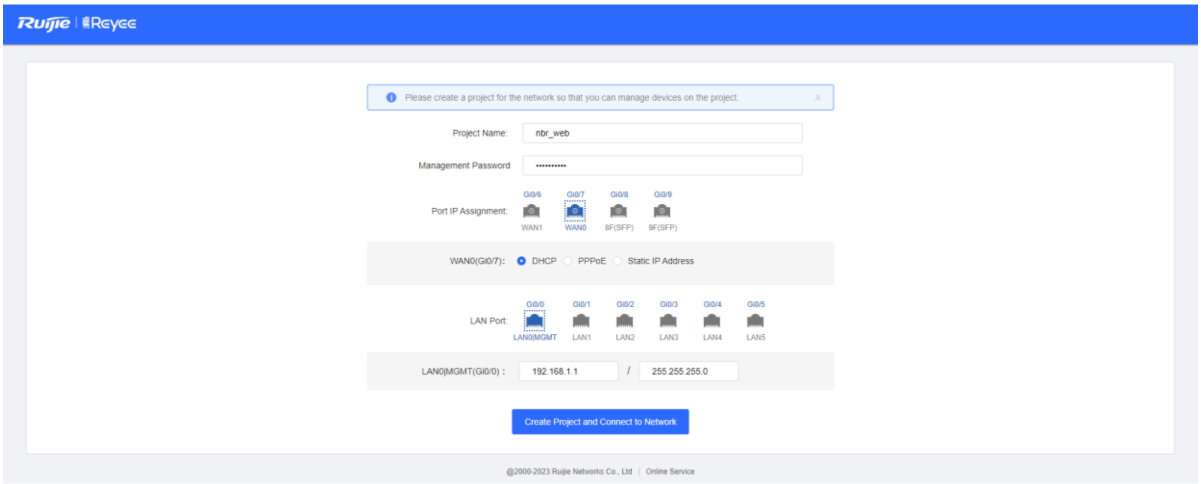
☑ Virus Protection

Delivering configuration... Please wait.

After this option is checked, the LAN-to-WAN security defense is enabled by default.

If the network connection is slow, you can disable security defense on the firewall policy configuration page.

(5) After successful configuration delivery, the following page is displayed. On this page, enter the project name and management password and click **Create Project and Connect to Network**.



Please create a project for the network so that you can manage devices on the project.

Project Name: nbr_web

Management Password ••••••••••

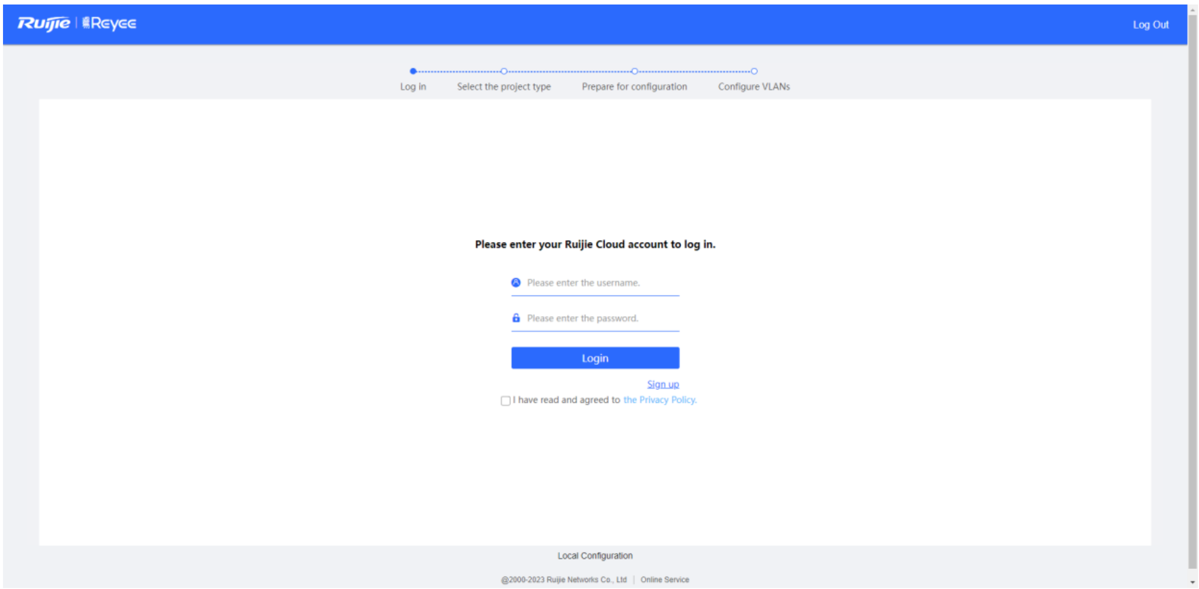
Port IP Assignment: WAN0 (Gi0/7)

WAN0(Gi0/7): ● DHCP ○ PPPoE ○ Static IP Address

LAN Port: LAN0|MGMT (Gi0/0)

LAN0|MGMT(Gi0/0) : 192.168.1.1 / 255.255.255.0

(6) Check the system prompt. A prompt indicating successful configuration is displayed after the configurations are completed. You can scan the username and password to log in to Ruijie Cloud and migrate the firewall to the cloud.



Ruijie | Reyee

Log Out

Log in — Select the project type — Prepare for configuration — Configure VLANs

Please enter your Ruijie Cloud account to log in.

Please enter the username.

Please enter the password.

Login

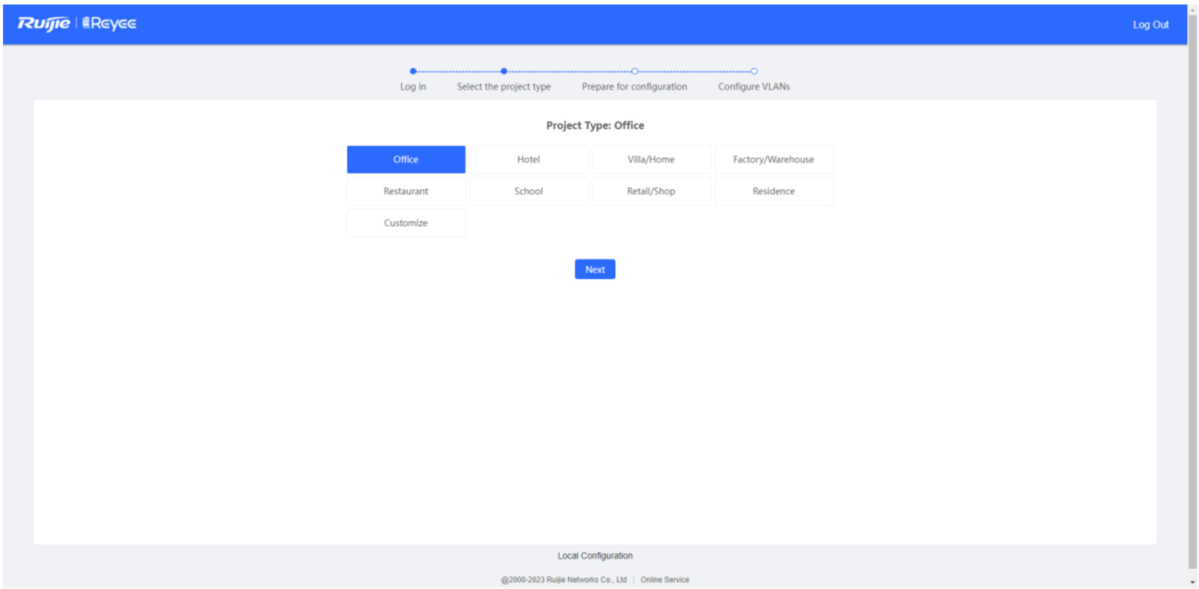
Sign up

□ I have read and agreed to the Privacy Policy.

Local Configuration

@2000-2023 Ruijie Networks Co., Ltd | Online Service

(7) After successful login, select a project type based on the actual networking scenario (**Other** in this example) and click **Next**. The initial configuration delivered varies by the project type, so the project type must be set based on the actual service scenario.



Ruijie | Reyee

Log Out

Log in — Select the project type — Prepare for configuration — Configure VLANs

Project Type: Office

Office | Hotel | Villa/Home | Factory/Warehouse

Restaurant | School | Retail/Shop | Residence

Customize

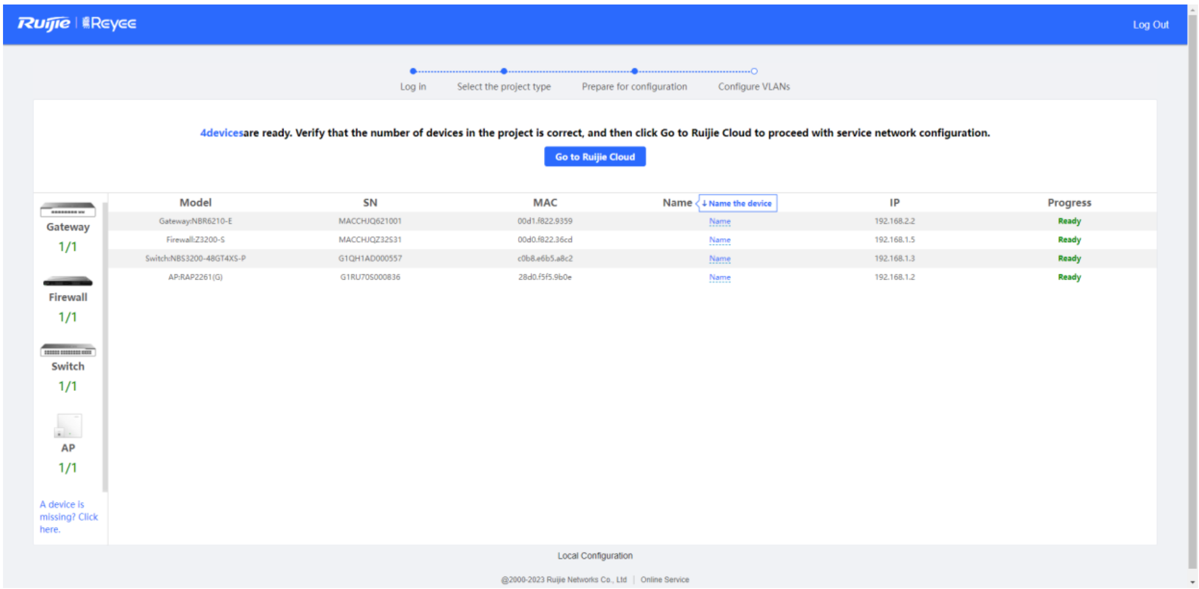
Next

Local Configuration

@2000-2023 Ruijie Networks Co., Ltd | Online Service

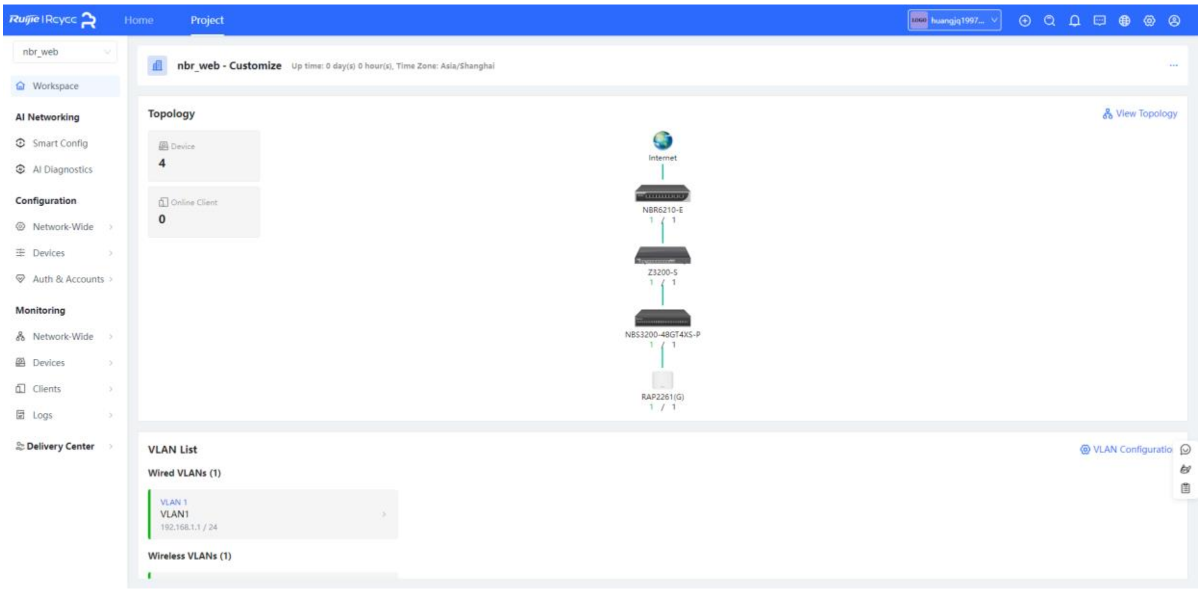
(8) Wait until preparations before configuration are complete and then configure the service network.

(9) After all devices go online, click **Go to the cloud platform for management** and perform service configuration (such as interfaces and routes) on the Ruijie Cloud platform.



4devicesare ready. Verify that the number of devices in the project is correct, and then click Go to Ruijie Cloud to proceed with service network configuration.

Model	SN	MAC	Name	IP	Progress
Gateway:NBR6210-E	MACCHJQ621001	00d1.f822.9359	Name	192.168.2.2	Ready
Firewall:Z3200-S	MACCHJQZ32S31	00d0.f822.36cd	Name	192.168.1.5	Ready
Switch:NBS3200-48GT4XS-P	G1QH1AD000557	c0b8.e6b5.a8c2	Name	192.168.1.3	Ready
AP:RAP2261(G)	G1RU70S000836	28d0.f5f5.9b0e	Name	192.168.1.2	Ready

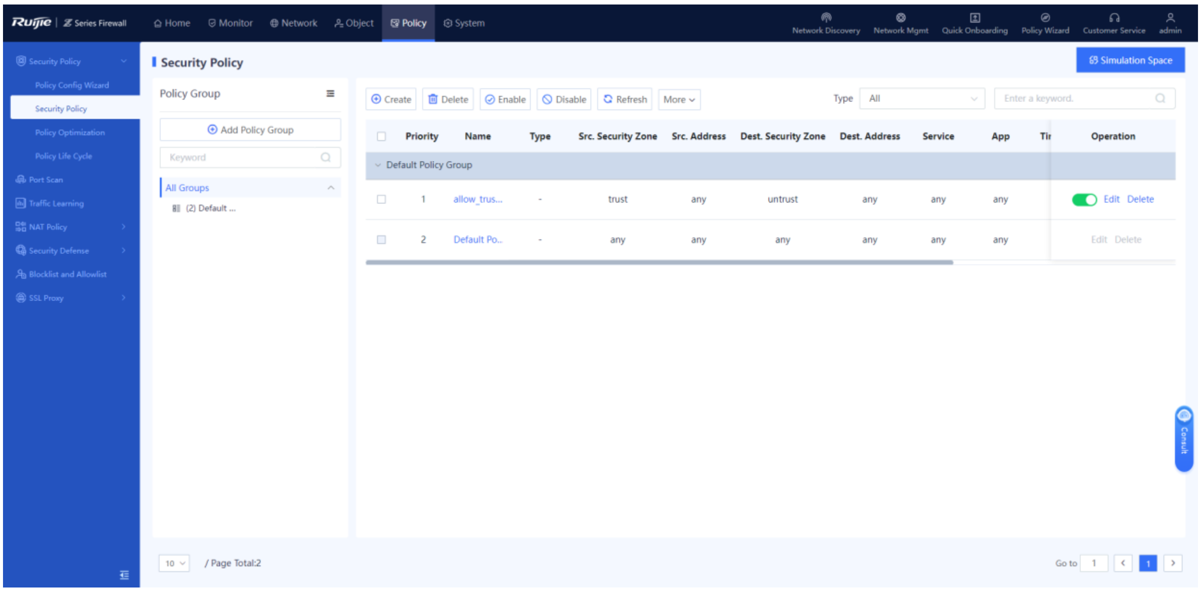


nbr_web - Customize Up time: 0 day(s) 0 hour(s), Time Zone: Asia/Shanghai

Note

Log in to the web page of the firewall from the Ruijie Cloud platform in EWEB mode and configure relevant policies.

After the firewall is migrated to the cloud, the firewall automatically adds the WAN interface and LAN interface to security zones **untrust** and **trust** respectively, generates a security policy that permits packets from the security zone **trust** to **untrust**, and enables IPS detection.



Security Policy

	Priority	Name	Type	Src. Security Zone	Src. Address	Dest. Security Zone	Dest. Address	Service	App	Ti	Operation
Default Policy Group											
□	1	allow_trus...	-	trust	any	untrust	any	any	any		Edit Delete
□	2	Default Po...	-	any	any	any	any	any	any		Edit Delete

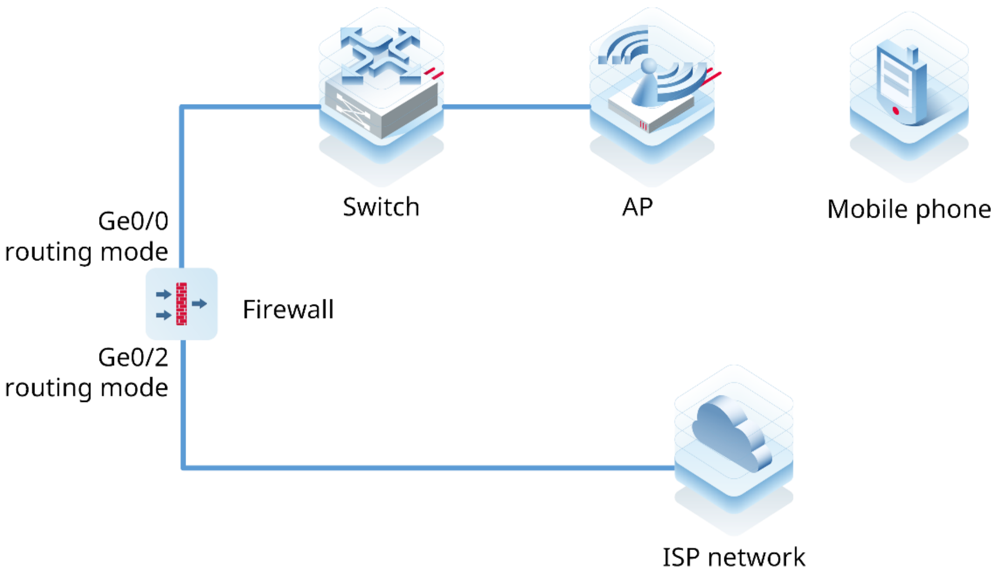
6.1.3 Deployment Using Ruijie Cloud App (Routing Mode)

1. Application Scenario

The firewall functions as a router and it is uplinked to the Internet and downlinked to a switch. You are advised to deploy the firewall in routing mode. The uplink and downlink interfaces are configured to work in routing mode.

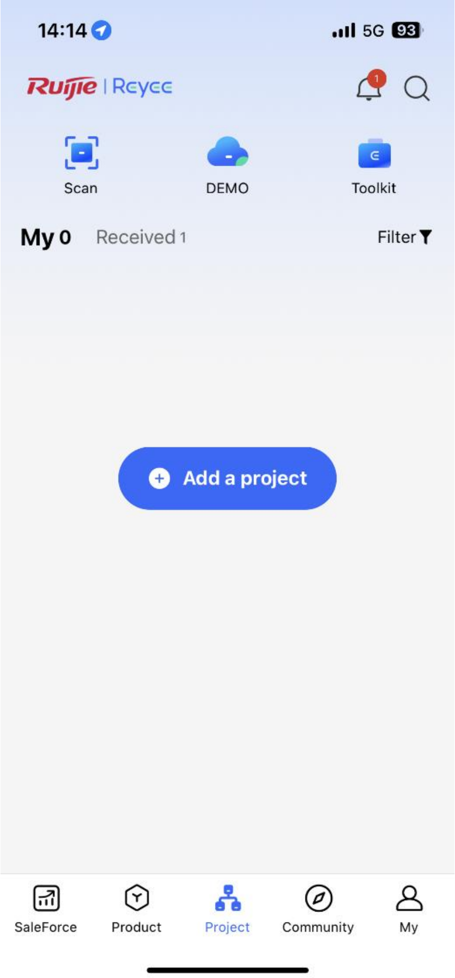
Note

You do not need to connect the firewall to the PC in Wi-Fi deployment using the Ruijie Cloud app.

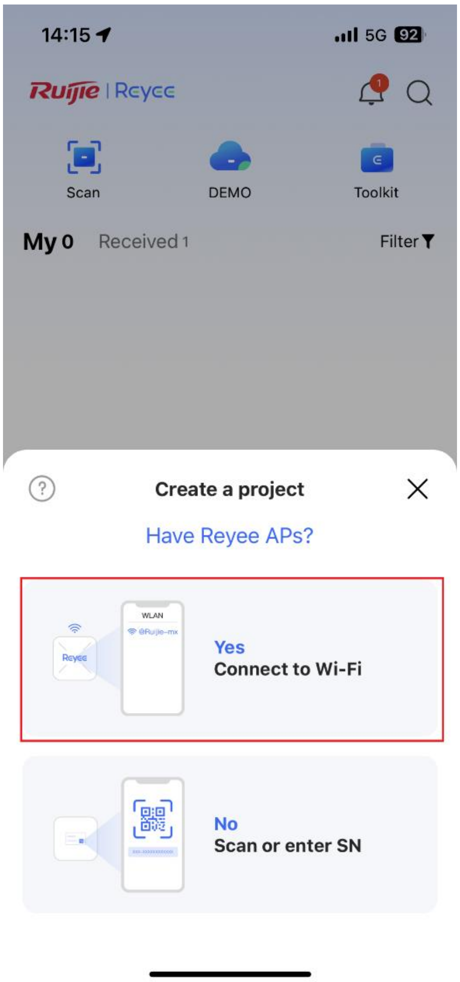


2. Procedure

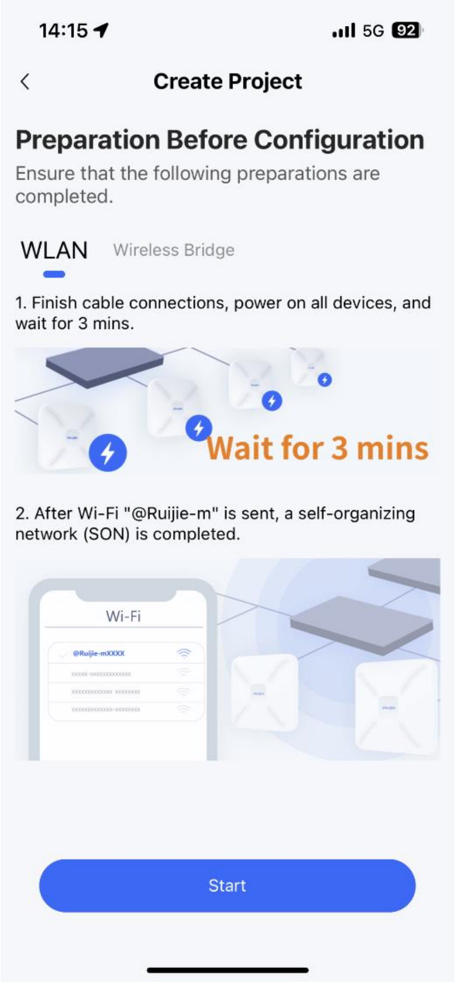
(1) After the network environment is established according to the preceding figure, start the Ruijie Cloud app and choose **Project** > **Add a project**.



(2) Select **Connect to Wi-Fi** and add a project.



(3) Tap **Connect** to connect to the Wi-Fi signal of the Reyee AP.



14:15

Create Project

Preparation Before Configuration

Ensure that the following preparations are completed.

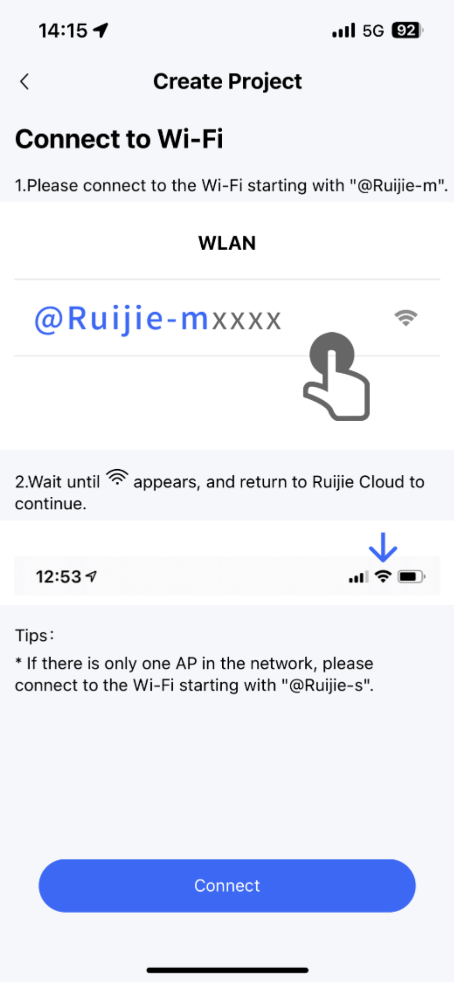
WLAN Wireless Bridge

1. Finish cable connections, power on all devices, and wait for 3 mins.

Wait for 3 mins

2. After Wi-Fi "@Ruijie-m" is sent, a self-organizing network (SON) is completed.

Start



14:15

Create Project

Connect to Wi-Fi

1.Please connect to the Wi-Fi starting with "@Ruijie-m".

WLAN

@Ruijie-mxxxx

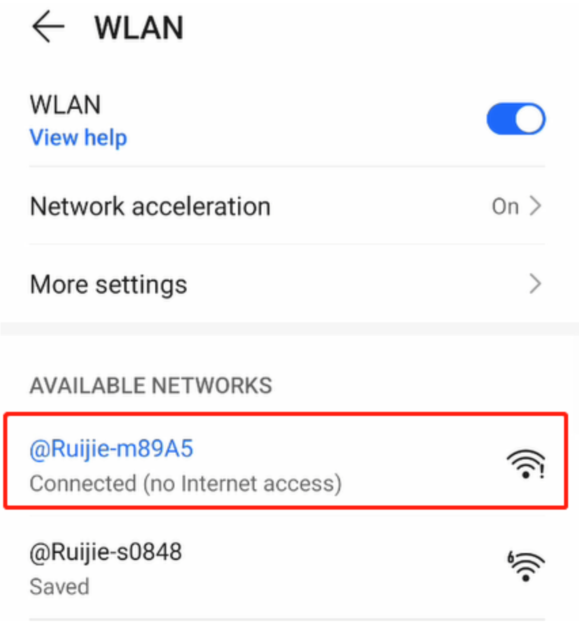
2.Wait until ᯤ appears, and return to Ruijie Cloud to continue.

12:53

Tips:

* If there is only one AP in the network, please connect to the Wi-Fi starting with "@Ruijie-s".

Connect



WLAN

WLAN
View help

Network acceleration On

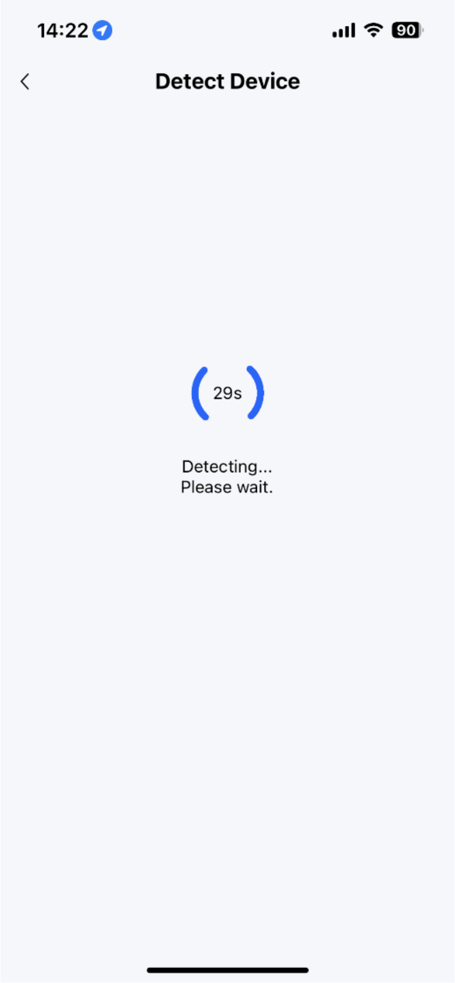
More settings

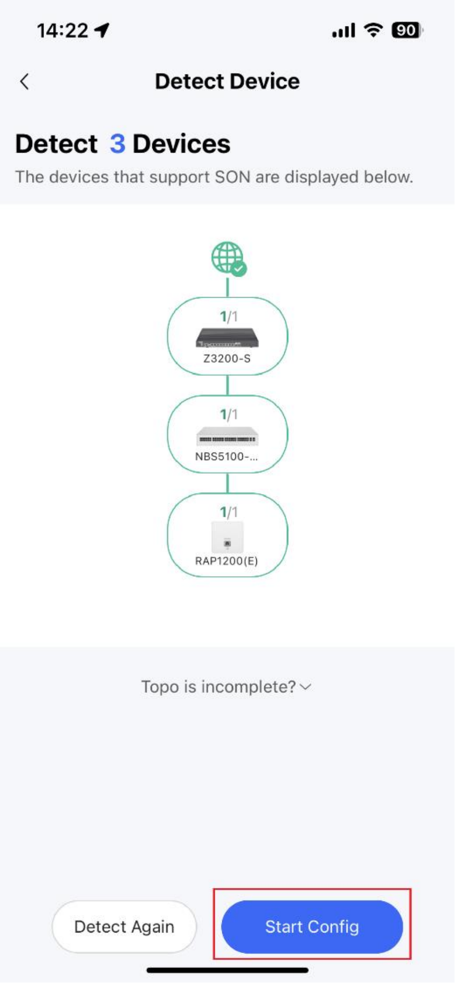
AVAILABLE NETWORKS

@Ruijie-m89A5
Connected (no Internet access)

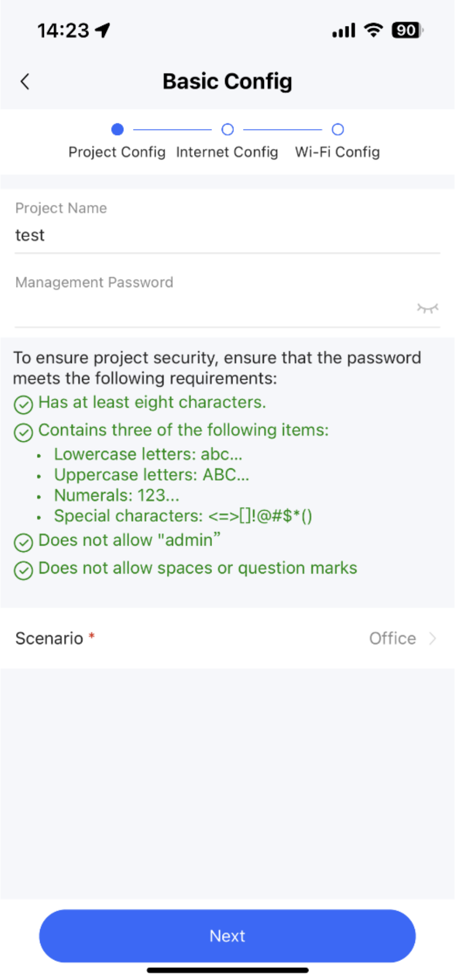
@Ruijie-s0848
Saved

(4) Wait for about 30s until the system automatically generates the network topology. Then, tap **Start Config**.





(5) Enter the project name and password and tap **Next**.



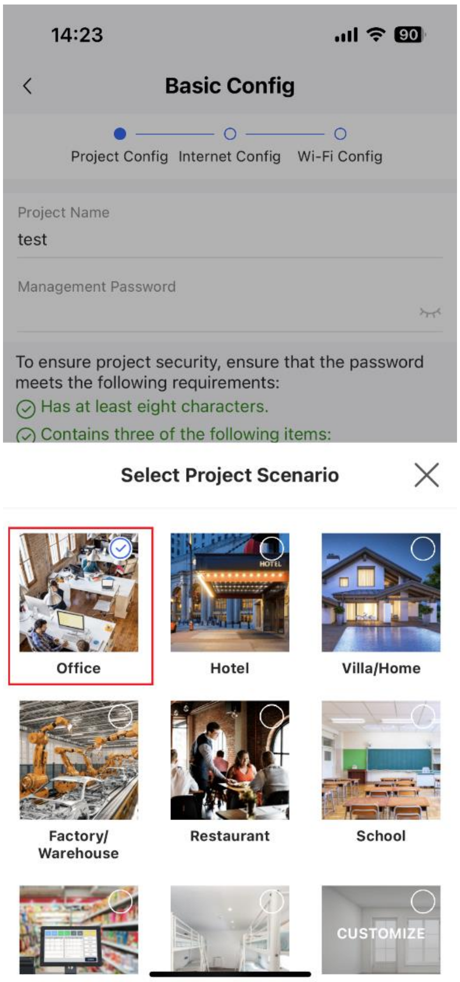
Project Name
test

Management Password

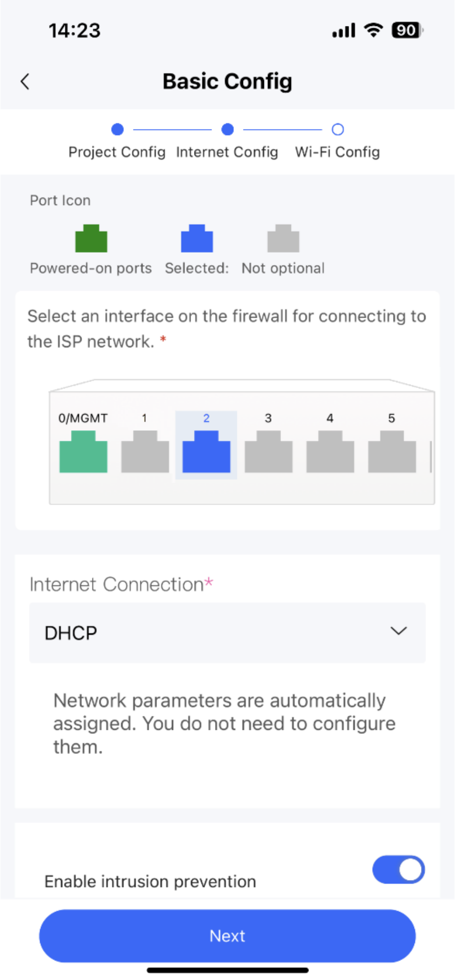
To ensure project security, ensure that the password meets the following requirements:

- Has at least eight characters.
- Contains three of the following items:
  - Lowercase letters: abc...
  - Uppercase letters: ABC...
  - Numerals: 123...
  - Special characters: <=>[]!@#$*()
- Does not allow "admin”
- Does not allow spaces or question marks

Scenario * Office



(6) Select the firewall interface (WAN interface) connected to the Internet, set an Internet access method, and tap **Next**.



Select an interface on the firewall for connecting to the ISP network. *

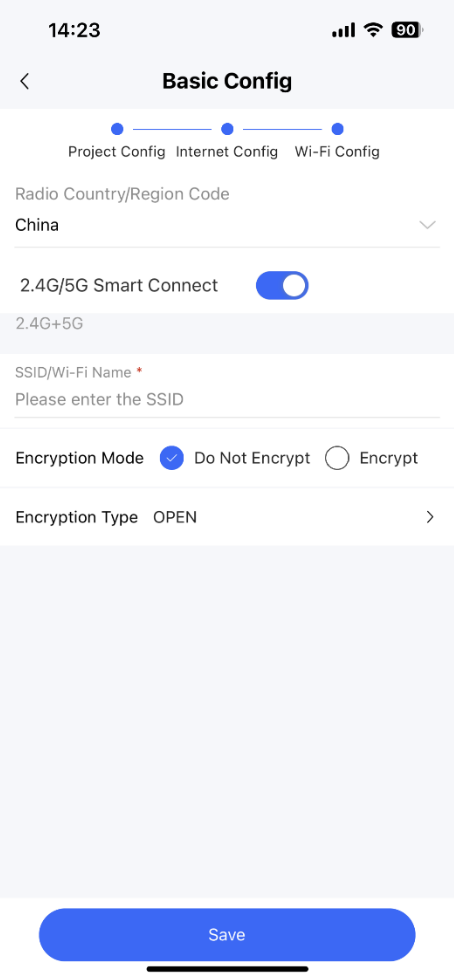
Internet Connection*

DHCP

Network parameters are automatically assigned. You do not need to configure them.

Enable intrusion prevention

(7) Set the Wi-Fi name and password and tap **Save**.



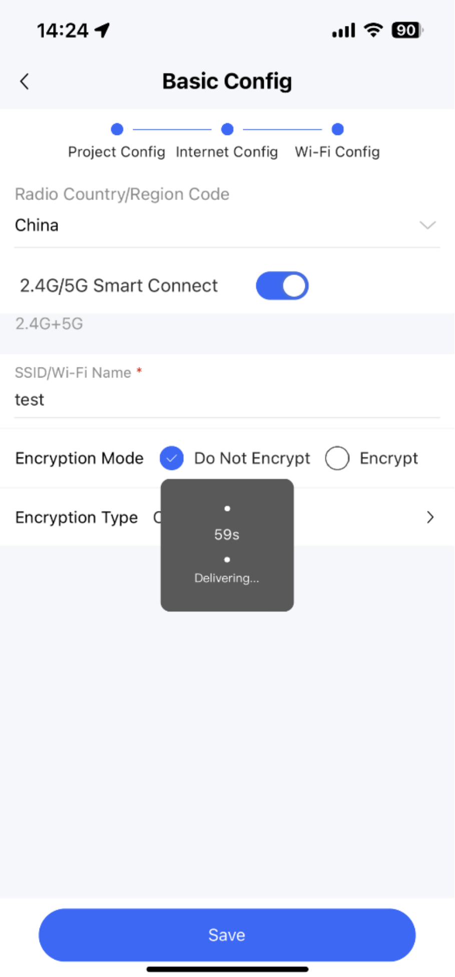
Radio Country/Region Code
China

2.4G/5G Smart Connect
2.4G+5G

SSID/Wi-Fi Name *
Please enter the SSID

Encryption Mode ● Do Not Encrypt ○ Encrypt

Encryption Type OPEN



Radio Country/Region Code
China

2.4G/5G Smart Connect
2.4G+5G

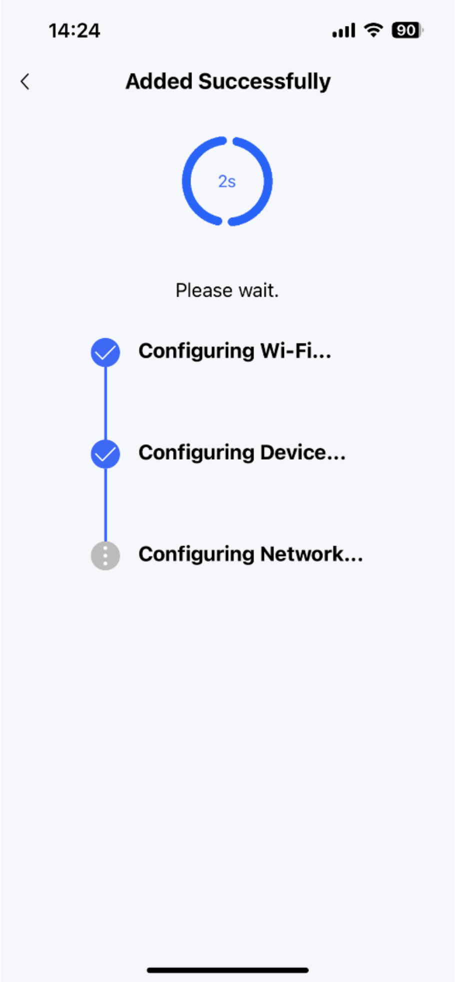
SSID/Wi-Fi Name *
test

Encryption Mode ● Do Not Encrypt ○ Encrypt

Encryption Type O

59s
Delivering...

(8) After successful configuration delivery, connect to the new Wi-Fi.



14:24

Added Successfully

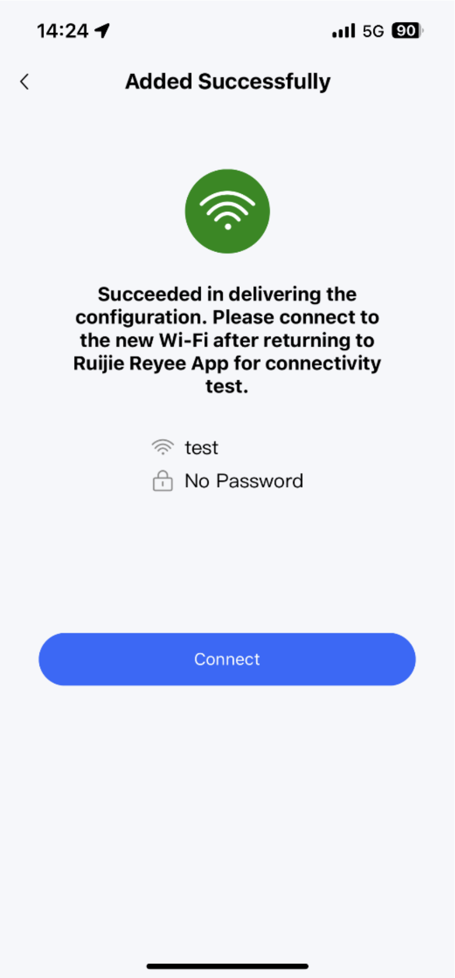
2s

Please wait.

Configuring Wi-Fi...

Configuring Device...

Configuring Network...



14:24

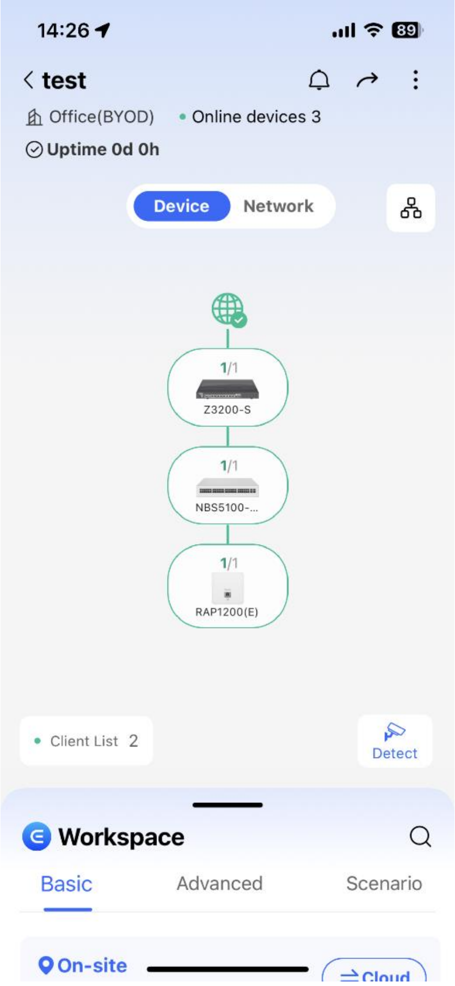
Added Successfully

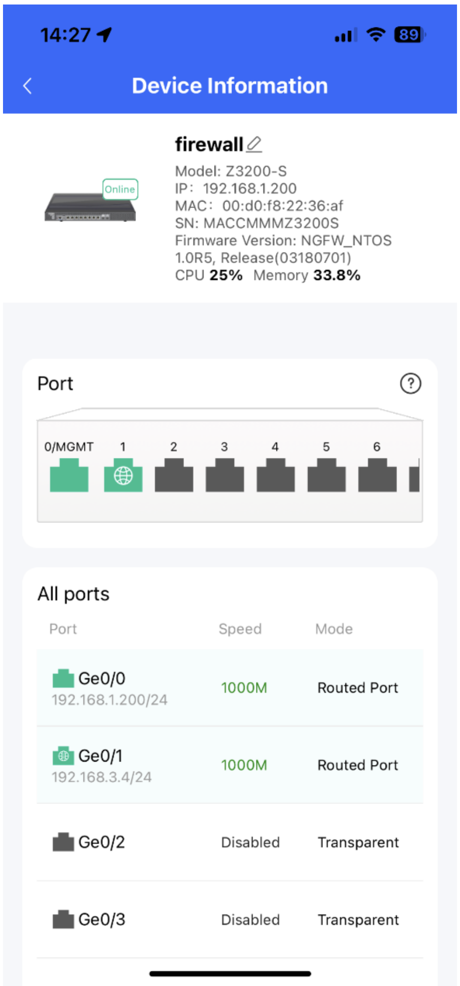
Succeeded in delivering the configuration. Please connect to the new Wi-Fi after returning to Ruijie Reyee App for connectivity test.

test

No Password

(9) Access the project management page and tap the firewall icon in the topology to view the interface status or modify the device name.





firewall
Model: Z3200-S
IP: 192.168.1.200
MAC: 00:d0:f8:22:36:af
SN: MACCMMMZ3200S
Firmware Version: NGFW_NTOS 1.0R5, Release(03180701)
CPU 25% Memory 33.8%

All ports

Port	Speed	Mode
Ge0/0 192.168.1.200/24	1000M	Routed Port
Ge0/1 192.168.3.4/24	1000M	Routed Port
Ge0/2	Disabled	Transparent
Ge0/3	Disabled	Transparent

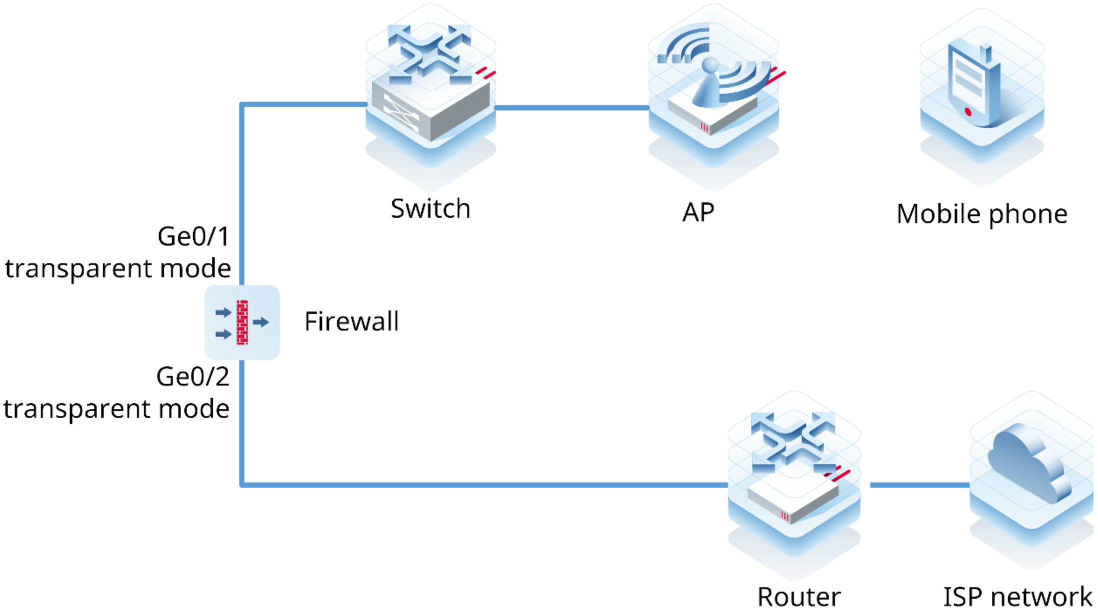
6.1.4 Deployment Using Ruijie Cloud App (Transparent Mode)

1. Application Scenario

When the firewall is uplinked to a router and downlinked to a switch, the transparent mode is recommended. The uplink and downlink interfaces are configured to work in transparent mode.

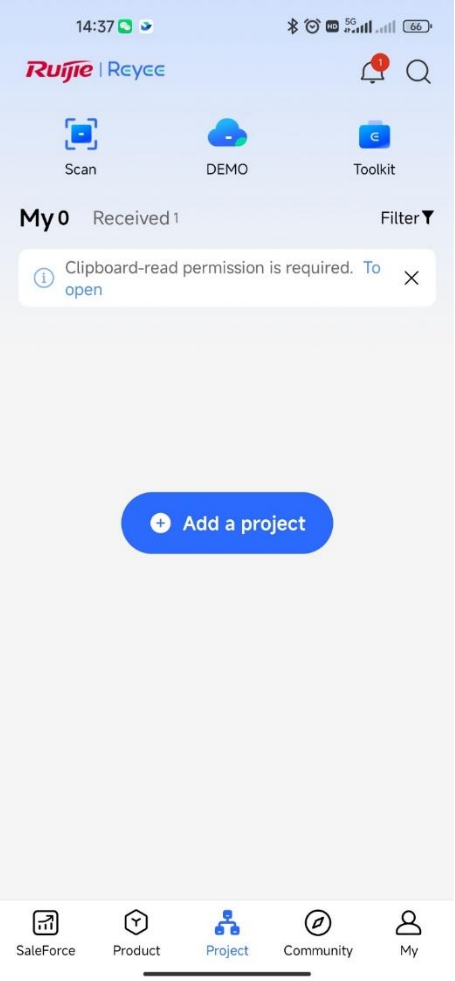
Note

You do not need to connect the firewall to the PC in Wi-Fi deployment using the Ruijie Cloud app.



2. Procedure

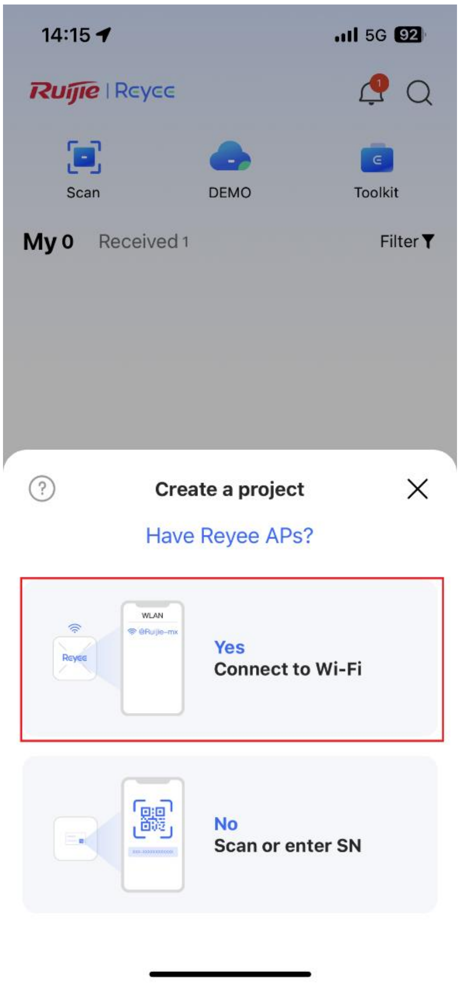
(1) After the network environment is established according to the preceding figure, start the Ruijie Cloud app and choose **Project** > **Add a project**.



Clipboard-read permission is required. To open

Add a project

(2) Select **Connect to Wi-Fi** and add a project.



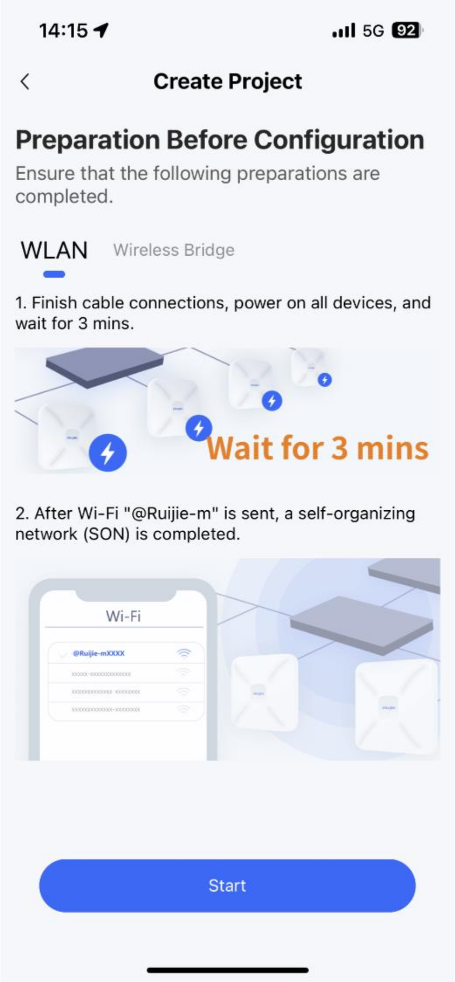
Create a project

Have Reyee APs?

Yes
Connect to Wi-Fi

No
Scan or enter SN

(3) Tap **Connect** to connect to the Wi-Fi signal of the Reyee AP.



14:15

Create Project

Preparation Before Configuration

Ensure that the following preparations are completed.

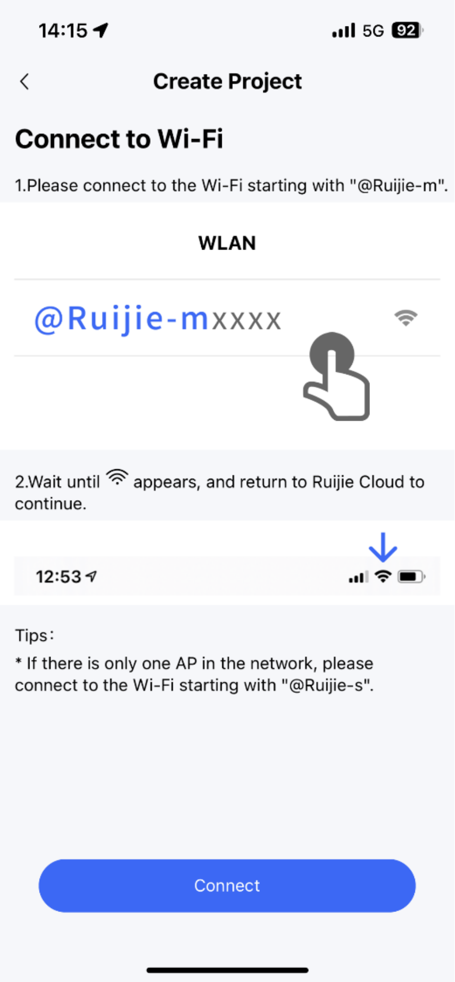
WLAN Wireless Bridge

1. Finish cable connections, power on all devices, and wait for 3 mins.

Wait for 3 mins

2. After Wi-Fi "@Ruijie-m" is sent, a self-organizing network (SON) is completed.

Start



14:15

Create Project

Connect to Wi-Fi

1.Please connect to the Wi-Fi starting with "@Ruijie-m".

WLAN

@Ruijie-mxxxx

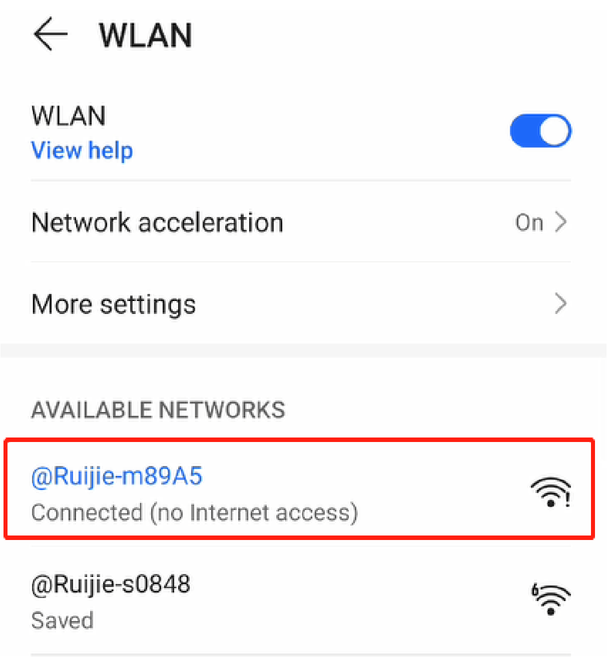
2.Wait until appears, and return to Ruijie Cloud to continue.

12:53

Tips:

* If there is only one AP in the network, please connect to the Wi-Fi starting with "@Ruijie-s".

Connect



WLAN

WLAN

View help

Network acceleration On

More settings

AVAILABLE NETWORKS

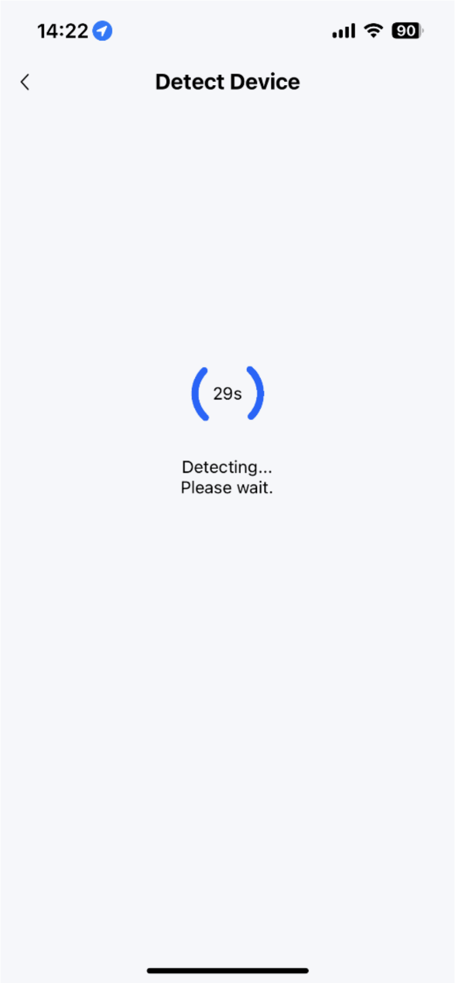
@Ruijie-m89A5

Connected (no Internet access)

@Ruijie-s0848

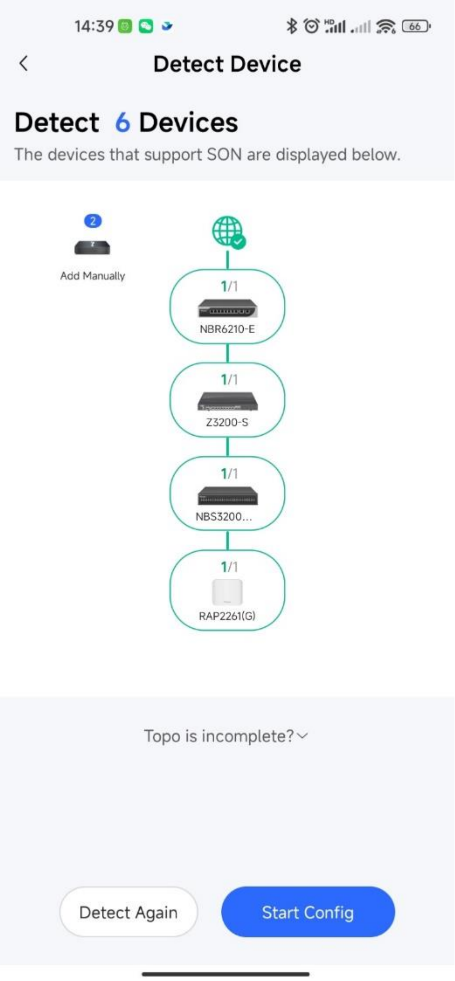
Saved

(4) Wait for about 30s until the system automatically generates the network topology. Then, tap **Start Config**.



Detect Device

Detecting...
Please wait.

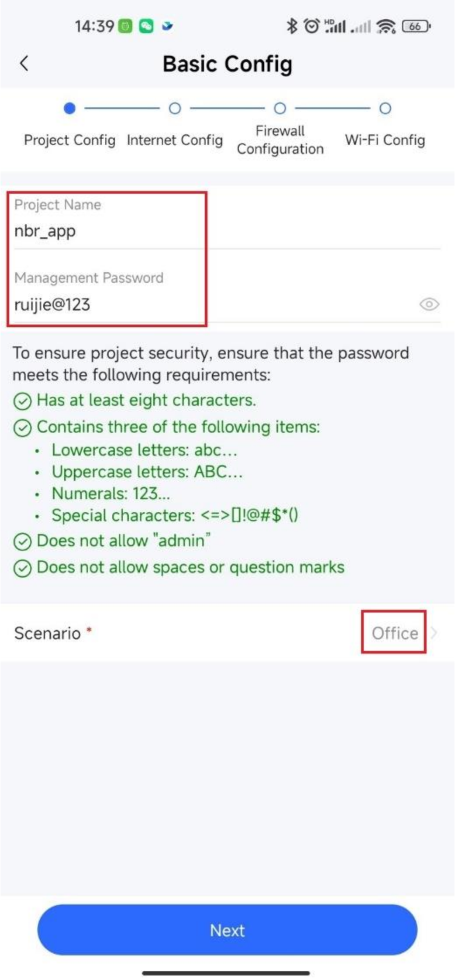


Detect Device

Detect 6 Devices

The devices that support SON are displayed below.

(5) Enter the project name and password and tap **Next**.



Project Name
nbr_app

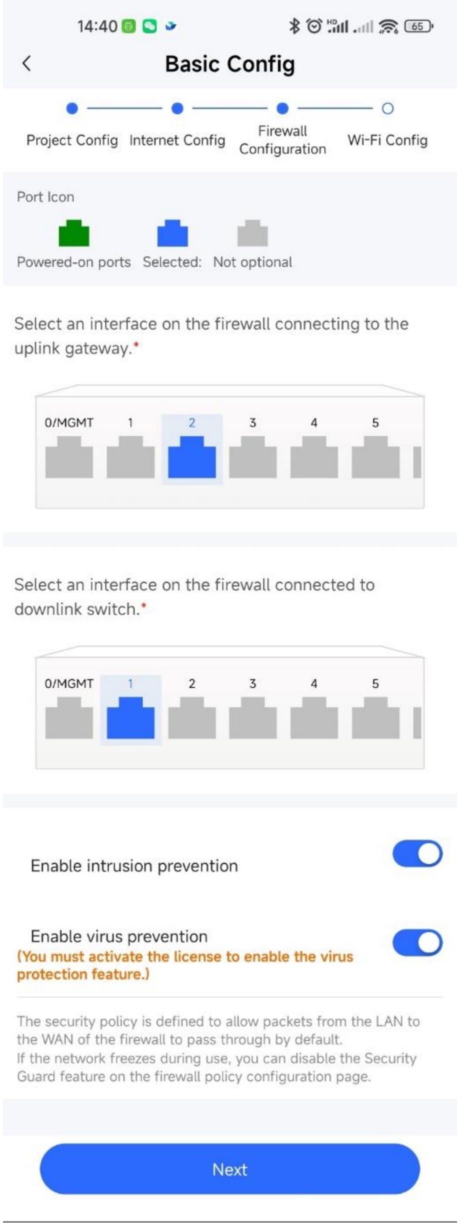
Management Password
ruijie@123

To ensure project security, ensure that the password meets the following requirements:

- Has at least eight characters.
- Contains three of the following items:
  - Lowercase letters: abc…
  - Uppercase letters: ABC…
  - Numerals: 123...
  - Special characters: <=>[]!@#$*()
- Does not allow "admin"
- Does not allow spaces or question marks

Scenario * Office

(6) Select the firewall interfaces connected to the router and switch, and tap **Next**.



Basic Config

Project Config Internet Config Firewall Configuration Wi-Fi Config

Port Icon

Powered-on ports Selected: Not optional

Select an interface on the firewall connecting to the uplink gateway.*

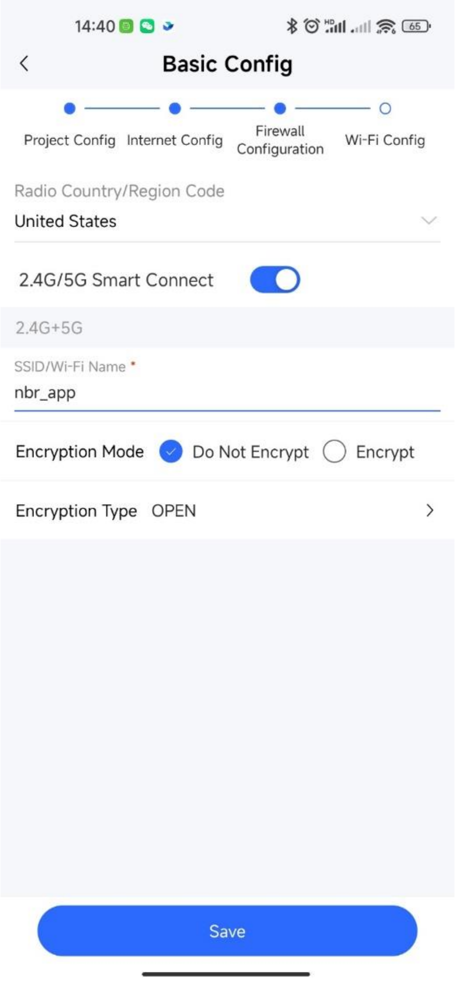
Select an interface on the firewall connected to downlink switch.*

Enable intrusion prevention

Enable virus prevention
(You must activate the license to enable the virus protection feature.)

The security policy is defined to allow packets from the LAN to the WAN of the firewall to pass through by default.
If the network freezes during use, you can disable the Security Guard feature on the firewall policy configuration page.

(7) Set the Wi-Fi name and password and tap **Save**.



14:40

Basic Config

Radio Country/Region Code
United States

2.4G/5G Smart Connect

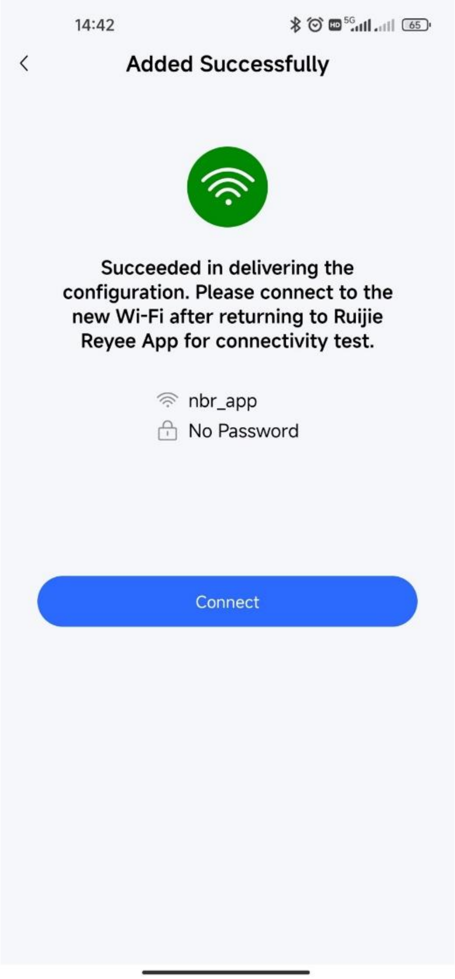
2.4G+5G

SSID/Wi-Fi Name *
nbr_app

Encryption Mode ● Do Not Encrypt ○ Encrypt

Encryption Type OPEN

(8) After successful configuration delivery, connect to the new Wi-Fi.



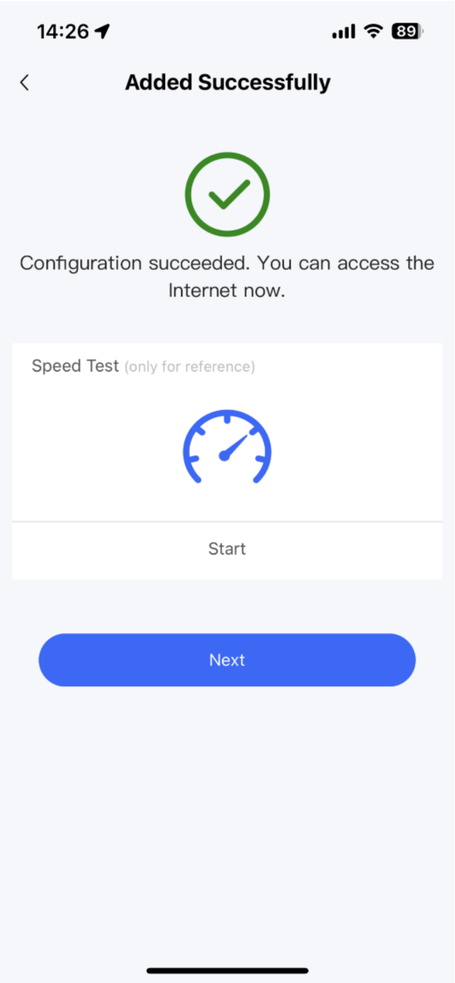
14:42

Added Successfully

Succeeded in delivering the configuration. Please connect to the new Wi-Fi after returning to Ruijie Reyee App for connectivity test.

nbr_app

No Password



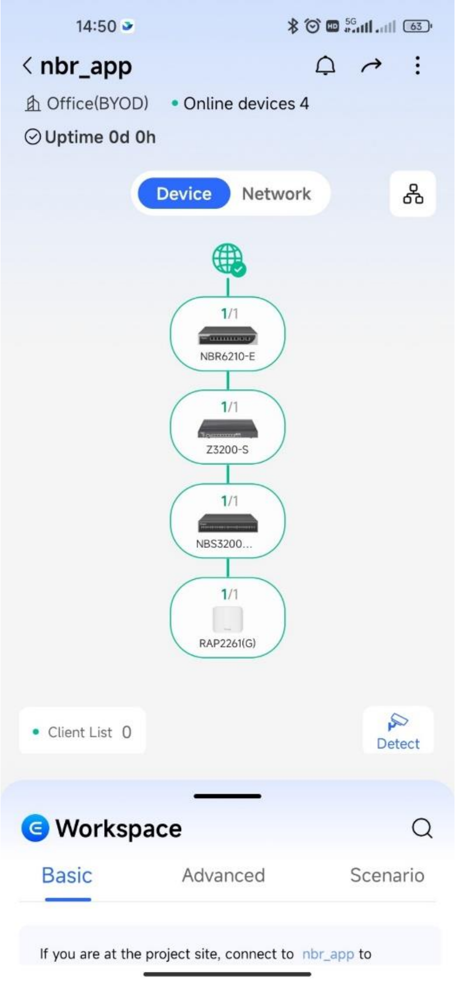
14:26

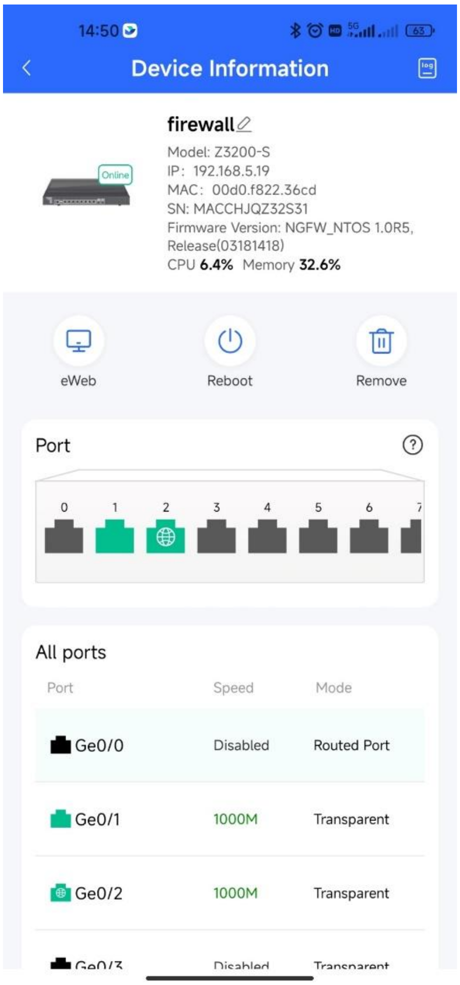
Added Successfully

Configuration succeeded. You can access the Internet now.

Speed Test (only for reference)

(9) Access the project management page and tap the firewall icon in the topology to view the interface status or modify the device name.





firewall

Model: Z3200-S
IP: 192.168.5.19
MAC: 00d0.f822.36cd
SN: MACCHJQZ32S31
Firmware Version: NGFW_NTOS 1.0R5, Release(03181418)
CPU 6.4% Memory 32.6%

Port	Speed	Mode
Ge0/0	Disabled	Routed Port
Ge0/1	1000M	Transparent
Ge0/2	1000M	Transparent
Ge0/3	Disabled	Transparent

6.2 Transparent Mode

6.2.1 Preparations

Confirm the following information before performing the configuration:

- If you deploy the firewall in transparent mode, you need to confirm the network scale and port type (GE electrical port, GE optical port, or 10GE optical port). As out-of-band management is used in bridge mode, an independent cable is required to connect the management interface to the network. You need to plan the IP address and next hop of the management interface and ensure that the management interface of the firewall can be connected to the Internet and managed on the cloud.
- If a service system is involved, check whether servers are deployed and whether the servers permit access from external users.
- Software version obtaining methods

Method	Path
Official website	https://www.ruijienetworks.com/ Choose **Support** > **Download** > **Reyee** and find the latest version of the Z-S series firewall under RG-WALL 1600-Z-S series cloud management firewalls.
Web management page of the firewall	Choose **System** > **System Maintenance** > **System Upgrade** > **Online Upgrade** > **Recommended Version** to upgrade to the latest version (recommended) in online mode.
Ruijie Cloud	After the device goes online on the Ruijie Cloud, you can remotely upgrade the device in online mode on the Ruijie Cloud (without the need for local upgrade). Choose **Monitoring** > **Device** > **Firewall**, select a device, select a version, and click **Upgrade**.

⚠ **Caution**

If the quick onboarding wizard is not used for the deployment, you must adjust the system time in advance. Otherwise, the time clock is inaccurate, which may affect reports and logs. To set the system time, choose **System** > **System Config** > **System Time**.

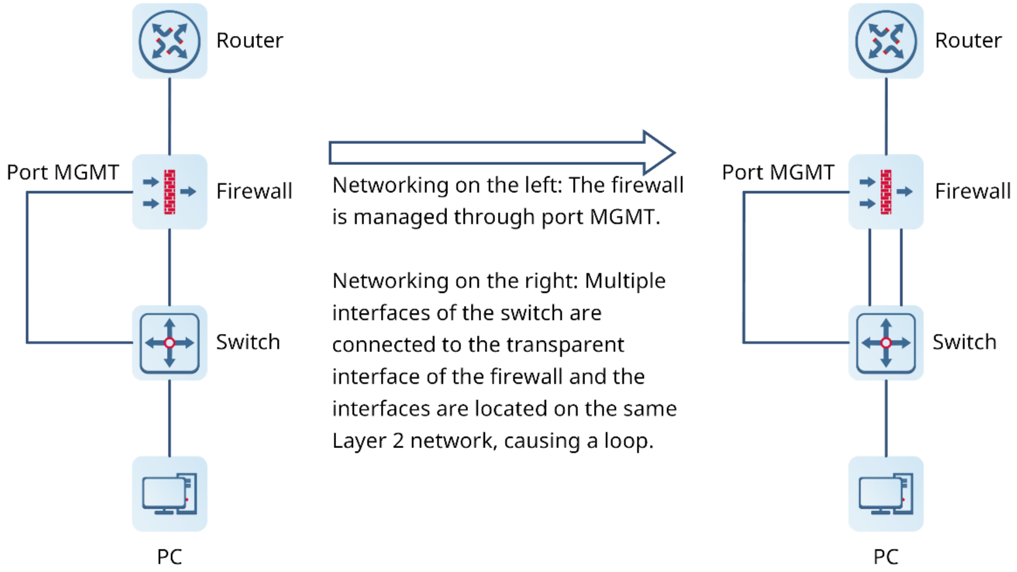
6.2.2 Deployment in Transparent Mode (Quick Deployment)

Network Requirements

In transparent mode, the firewall is used as a network cable with the filtering function and is deployed between the existing gateway and the LAN terminal, without the need to change the network topology and the configurations of other network devices. In transparent bridge mode, the firewall provides only transparent data forwarding and security protection functions but not the route-based forwarding function, as shown in the following figure.

The LAN in this topology can be a Layer 2 network or a Layer 3 network. You can select a structure model for the LAN based on the network scale and requirements of the customer. The configurations of the egress router and core switch are the same as those in the networking without a firewall. As a result, this section describes only the firewall configuration and ignores the configurations of the egress router and core switch.

Network Topology


Router
Port MGMT
Firewall
Switch
PC
Networking on the left: The firewall is managed through port MGMT.
Networking on the right: Multiple interfaces of the switch are connected to the transparent interface of the firewall and the interfaces are located on the same Layer 2 network, causing a loop.
Router
Port MGMT
Firewall
Switch
PC

In this example, the firewall connects to the egress router through the WAN interface and connects to the core switch through the LAN interface. Port 0/MGMT (Ge0/0) of the firewall is used as the management interface to connect to the core switch (with management interface address set to 192.168.200.199 in this example) and the next-hop address 192.168.200.1 is the management address of the switch (successful ping to the Internet). The addresses can be set according to the actual needs during deployment.

Configuration Points

(1) Implement quick onboarding. Select a deployment mode (transparent mode) and configure a WAN interface and a LAN interface to complete Internet access. Configure an IP address and the next hop for the management interface (0/MGMT) to ensure successful connection to the Internet.

- WAN interface: Applicable to **connect to the egress device**. The WAN interface directly connects the firewall to an egress router or another device.
- LAN interface: Applicable for **connection to LAN** devices, such as servers, PCs, switches, and printers.

(2) (Optional) Check the connectivity. The system automatically checks whether the firewall is connected to the Internet.

(3) (Optional) Import licenses.

a Before license activation, log in to the Ruijie Secure Cloud Platform (https://secloud-en.ruijienetworks.com/), choose **Device Authorization** > **Activate License**, and generate a license file. (The account of the Secure Cloud Platform is used to activate and change the license. Keep the account safe.)

b Select an activation method (online activation or offline activation) based on network connection information of the firewall.

(4) Complete the quick onboarding configuration.

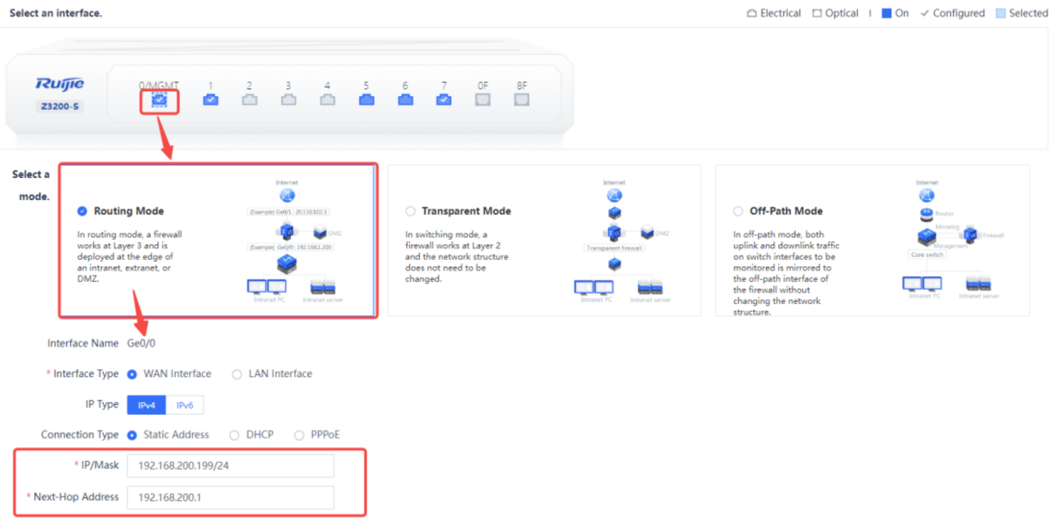
(5) (Optional) Implement remote O&M on the cloud.

Procedure

(1) Implement quick onboarding.

a Configure interfaces.

- Configure an IP address and next hop for the 0/MGMT management interface (Ge0/0) and connect it to the network using an independent network cable to ensure that the management interface can access the Internet. (The IP addresses in this example are for reference only.)
- Configure a WAN interface and a LAN interface to complete Internet access. In this example, the LAN interface is Ge0/1 and the WAN interface is Ge0/6.


Select an interface.

Select a mode.

● Routing Mode

In routing mode, a firewall works at Layer 3 and is deployed at the edge of an intranet, extranet, or DMZ.

○ Transparent Mode

In switching mode, a firewall works at Layer 2 and the network structure does not need to be changed.

○ Off-Path Mode

In off-path mode, both uplink and downlink traffic on switch interfaces to be monitored is mirrored to the off-path interface of the firewall without changing the network structure.

Interface Name Ge0/0

* Interface Type ● WAN Interface ○ LAN Interface

IP Type IPv4 IPv6

Connection Type ● Static Address ○ DHCP ○ PPPoE

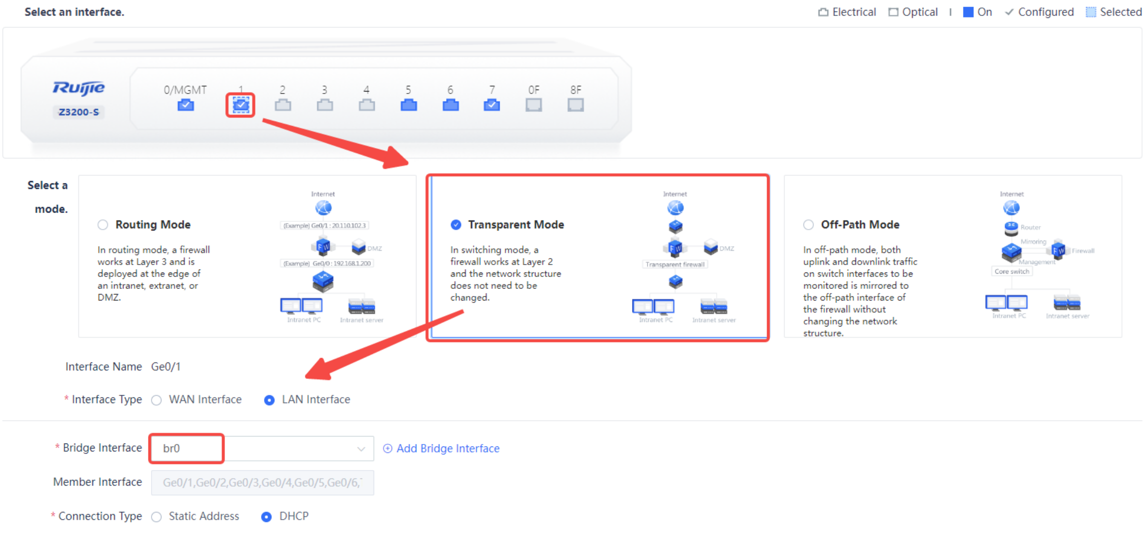
* IP/Mask 192.168.200.199/24

* Next-Hop Address 192.168.200.1

b Configure the WAN interface and LAN interface and set the mode to transparent mode.

Note

The management interface cannot be set to the transparent mode.



Select an interface.

Select a mode.

○ Routing Mode
In routing mode, a firewall works at Layer 3 and is deployed at the edge of an intranet, extranet, or DMZ.

● Transparent Mode
In switching mode, a firewall works at Layer 2 and the network structure does not need to be changed.

○ Off-Path Mode
In off-path mode, both uplink and downlink traffic on switch interfaces to be monitored is mirrored to the off-path interface of the firewall without changing the network structure.

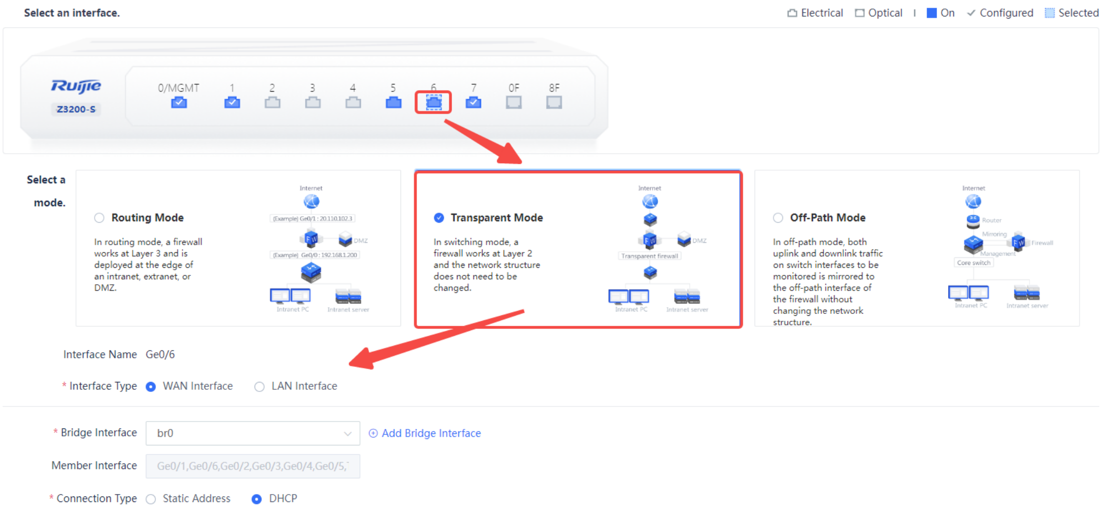
Interface Name Ge0/1

* Interface Type ○ WAN Interface ● LAN Interface

* Bridge Interface br0 ⊕ Add Bridge Interface

Member Interface Ge0/1,Ge0/2,Ge0/3,Ge0/4,Ge0/5,Ge0/6,

* Connection Type ○ Static Address ● DHCP



Select an interface.

Select a mode.

○ Routing Mode
In routing mode, a firewall works at Layer 3 and is deployed at the edge of an intranet, extranet, or DMZ.

● Transparent Mode
In switching mode, a firewall works at Layer 2 and the network structure does not need to be changed.

○ Off-Path Mode
In off-path mode, both uplink and downlink traffic on switch interfaces to be monitored is mirrored to the off-path interface of the firewall without changing the network structure.

Interface Name Ge0/6

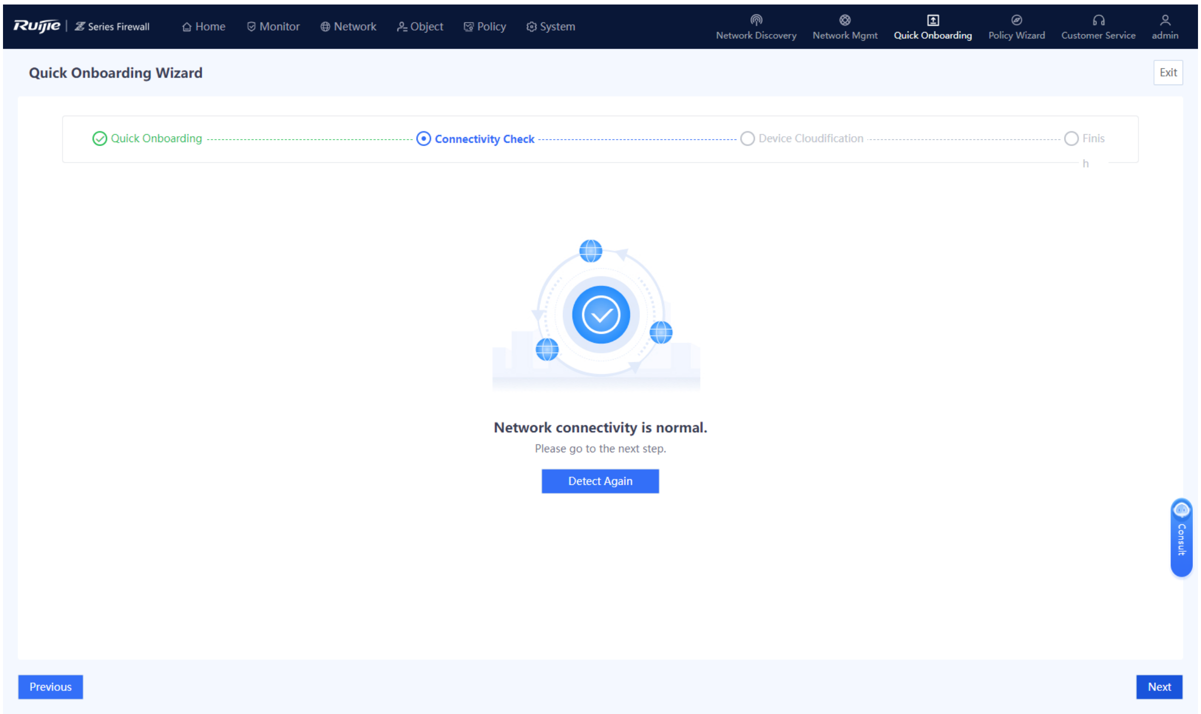
* Interface Type ● WAN Interface ○ LAN Interface

* Bridge Interface br0 ⊕ Add Bridge Interface

Member Interface Ge0/1,Ge0/6,Ge0/2,Ge0/3,Ge0/4,Ge0/5,

* Connection Type ○ Static Address ● DHCP

(2) (Optional) Check the connectivity.

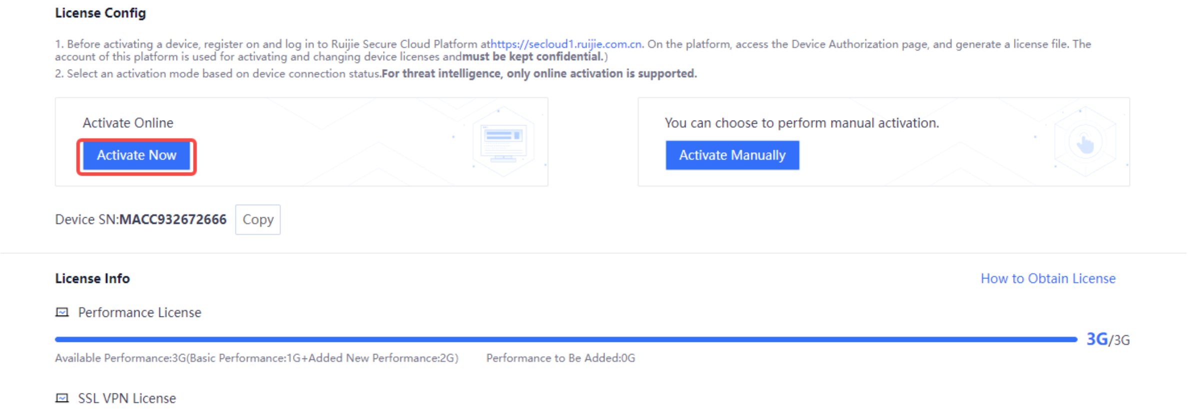


Quick Onboarding Wizard

Network connectivity is normal.

Please go to the next step.

(3) Import licenses.



License Config

1. Before activating a device, register on and log in to Ruijie Secure Cloud Platform athttps://secloud1.ruijie.com.cn. On the platform, access the Device Authorization page, and generate a license file. The account of this platform is used for activating and changing device licenses and**must be kept confidential.**)

2. Select an activation mode based on device connection status.**For threat intelligence, only online activation is supported.**

Activate Online

You can choose to perform manual activation.

Device SN:**MACC932672666**

License Info

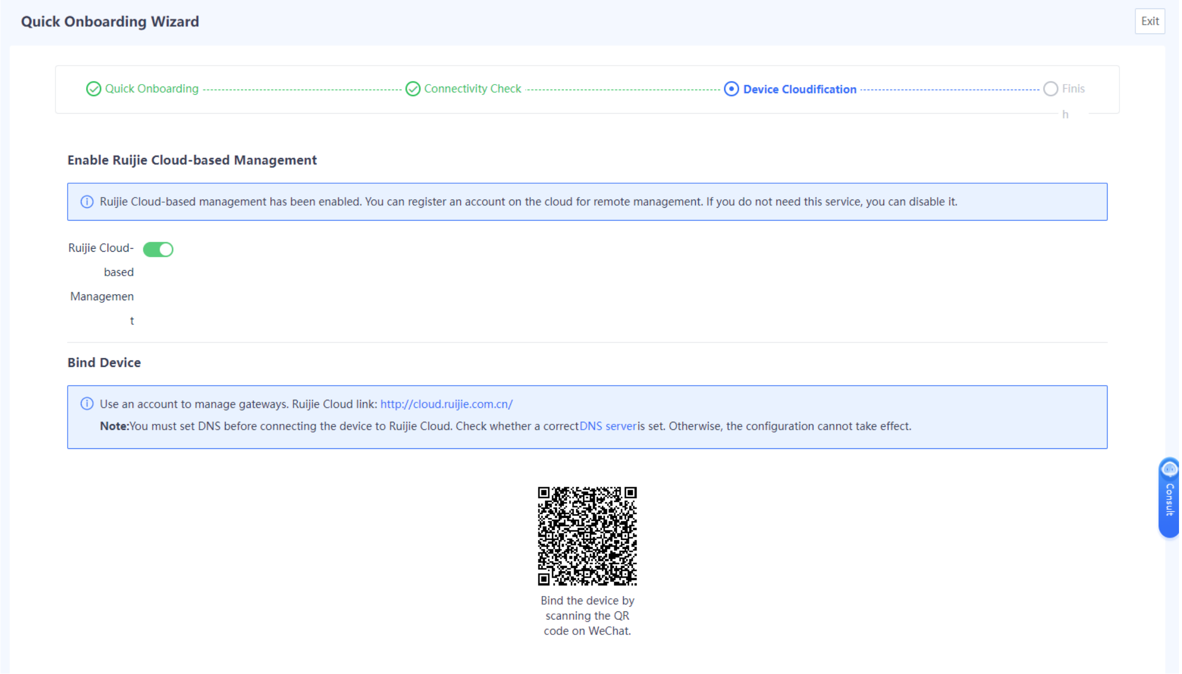
Performance License

3G/3G

Available Performance:3G(Basic Performance:1G+Added New Performance:2G) Performance to Be Added:0G

SSL VPN License

(4) Complete the quick onboarding configuration and bind the firewall to the Ruijie Cloud to implement remote O&M.



Quick Onboarding Wizard

Enable Ruijie Cloud-based Management

Ruijie Cloud-based management has been enabled. You can register an account on the cloud for remote management. If you do not need this service, you can disable it.

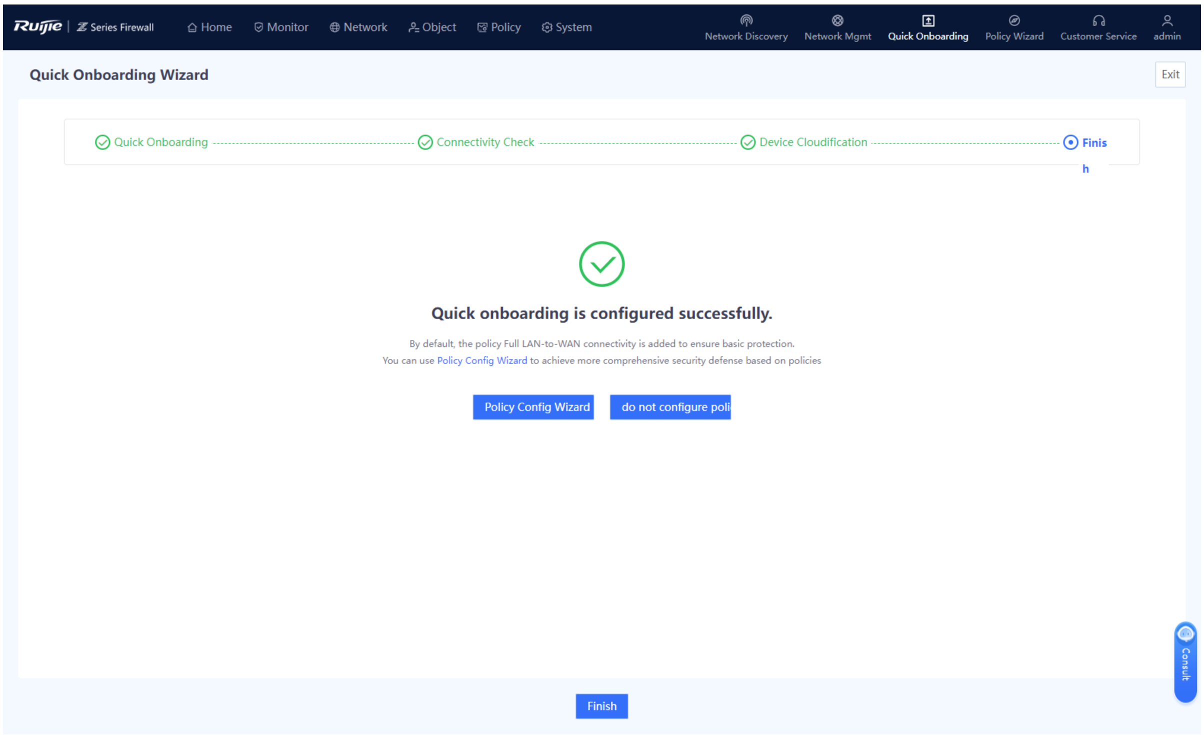
Ruijie Cloud-based Management

Bind Device

Use an account to manage gateways. Ruijie Cloud link: http://cloud.ruijie.com.cn/

Note: You must set DNS before connecting the device to Ruijie Cloud. Check whether a correctDNS serveris set. Otherwise, the configuration cannot take effect.

Bind the device by scanning the QR code on WeChat.



Quick Onboarding Wizard

Quick onboarding is configured successfully.

By default, the policy Full LAN-to-WAN connectivity is added to ensure basic protection.
You can use Policy Config Wizard to achieve more comprehensive security defense based on policies

Configuration Verification

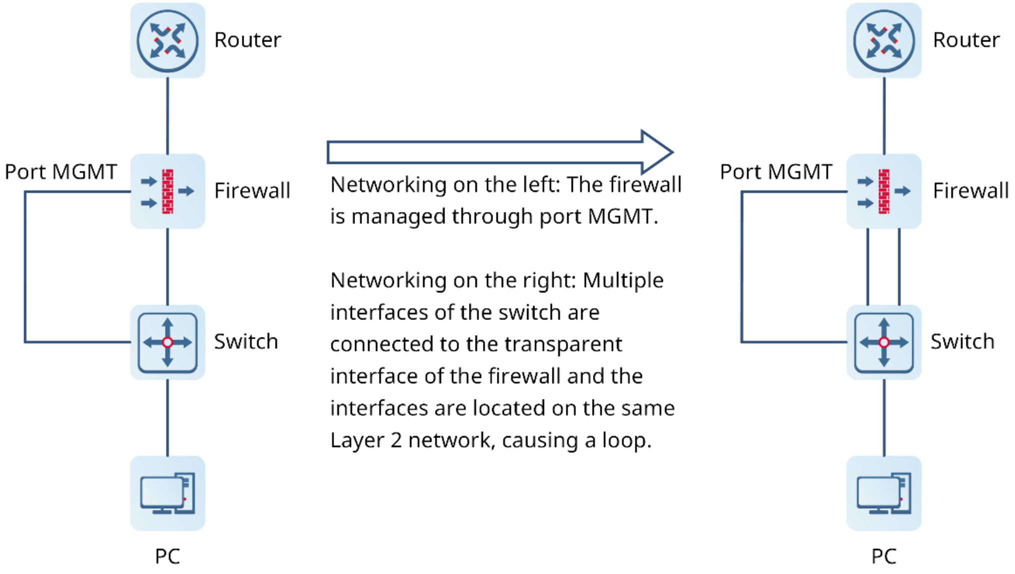
In transparent mode, the firewall can access the Internet without the need to modify the network environment, including the client IP address and gateway IP address.

6.2.3 Out-of-Band Management in Transparent Mode (Custom Deployment)

Network Requirements

Out-of-band management needs to be implemented when the firewall is deployed in transparent mode.

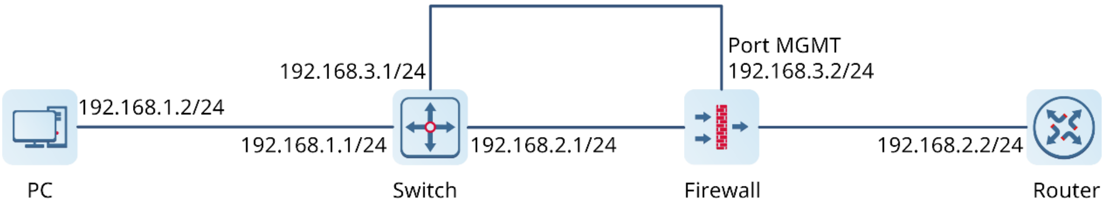
- An IP address must be configured for the management interface of the firewall to ensure connectivity to the management PC.
- The local route generated by the added management IP address does not cause conflicts such as asynchronous route that affects normal service data transmission.
- After all firewall interfaces (except the management interface) are converted to the transparent mode, they (WAN interface and LAN interface) must be in the same transparent bridge. Pay attention to prevent loops.



Networking on the left: The firewall is managed through port MGMT.

Networking on the right: Multiple interfaces of the switch are connected to the transparent interface of the firewall and the interfaces are located on the same Layer 2 network, causing a loop.

Network Topology



Configuration Points

- Configure a management IP address and an access method for the management interface.

- Ensure network connectivity between the PC and the management interface.

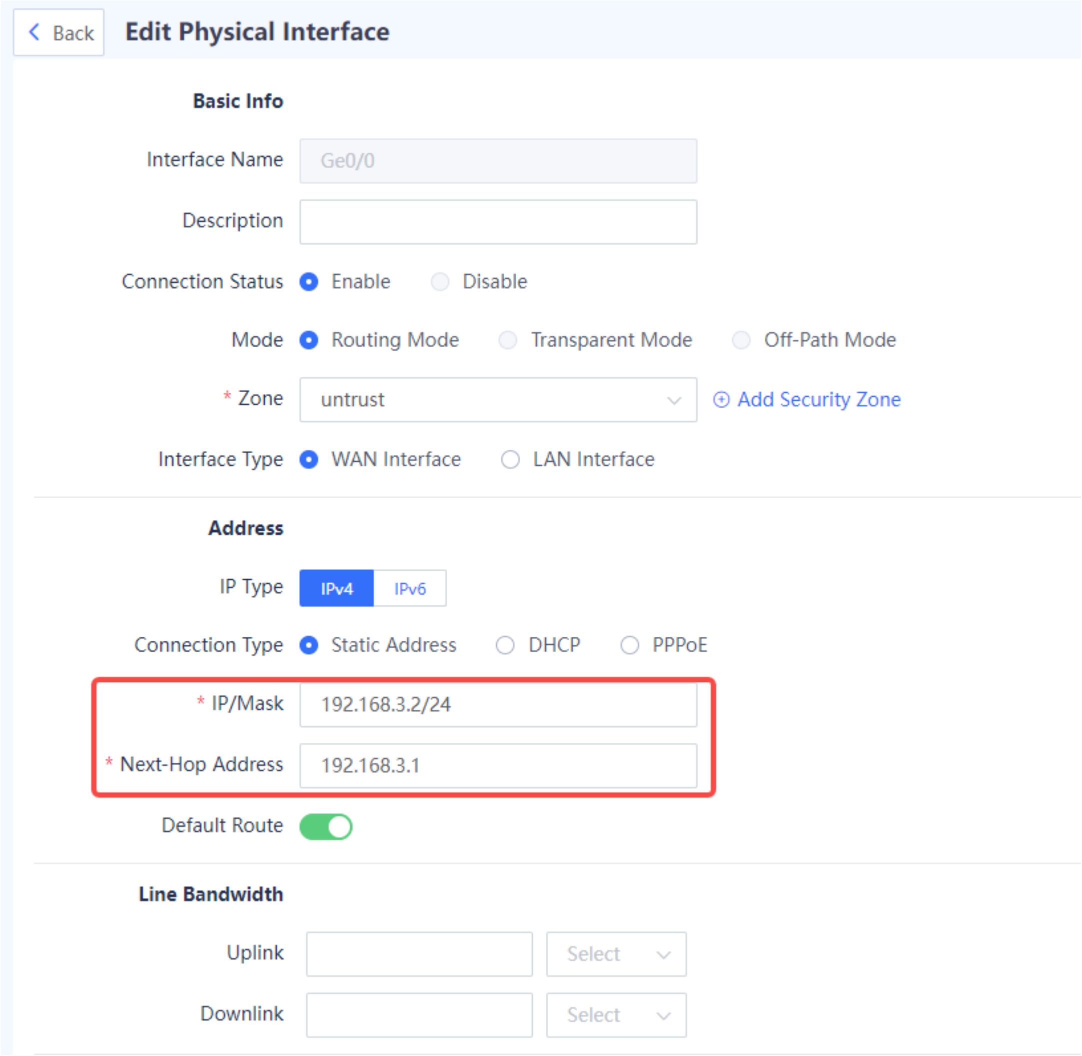
Procedure

(1) Configure the management interface Ge0/0.

a Choose **Network** > **Interface** > **Physical Interface**.

b Select **Ge0/0** and click **Edit**.

c Configure attributes of Ge0/0 and click **Save**.



Basic Info

Interface Name: Ge0/0

Description:

Connection Status: ● Enable ○ Disable

Mode: ● Routing Mode ○ Transparent Mode ○ Off-Path Mode

* Zone: untrust

Interface Type: ● WAN Interface ○ LAN Interface

Address

IP Type: IPv4 IPv6

Connection Type: ● Static Address ○ DHCP ○ PPPoE

* IP/Mask: 192.168.3.2/24

* Next-Hop Address: 192.168.3.1

Default Route: on

Line Bandwidth

Uplink: Select

Downlink: Select

Item	Description
Interface Type	Type of the Ge0/0 interface. As a management interface, Ge0/0 needs to connect to the Internet. As a result, you need to set the interface type to WAN interface.

Item	Description
IP/Mask	Set a valid IP address without conflicts that complies with requirements. 192.168.3.2/24
Next-Hop Address	192.168.3.1

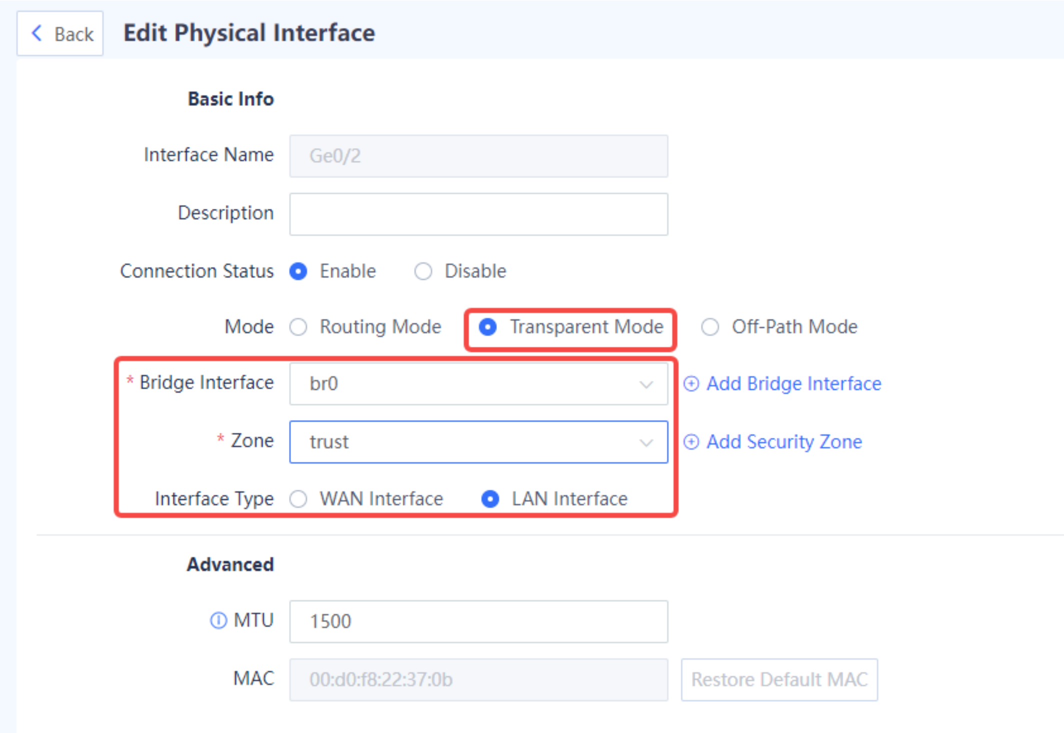
⚠ **Caution**

The management interface cannot be converted to the transparent mode.

(2) Convert other interfaces to the transparent mode.

a Choose **Network** > **Interface** > **Physical Interface**.

b Select the corresponding interface and click **Edit**.



< Back **Edit Physical Interface**

Basic Info

Interface Name: Ge0/2

Description:

Connection Status: ● Enable ○ Disable

Mode: ○ Routing Mode ● Transparent Mode ○ Off-Path Mode

* Bridge Interface: br0 ⊕ Add Bridge Interface

* Zone: trust ⊕ Add Security Zone

Interface Type: ○ WAN Interface ● LAN Interface

Advanced

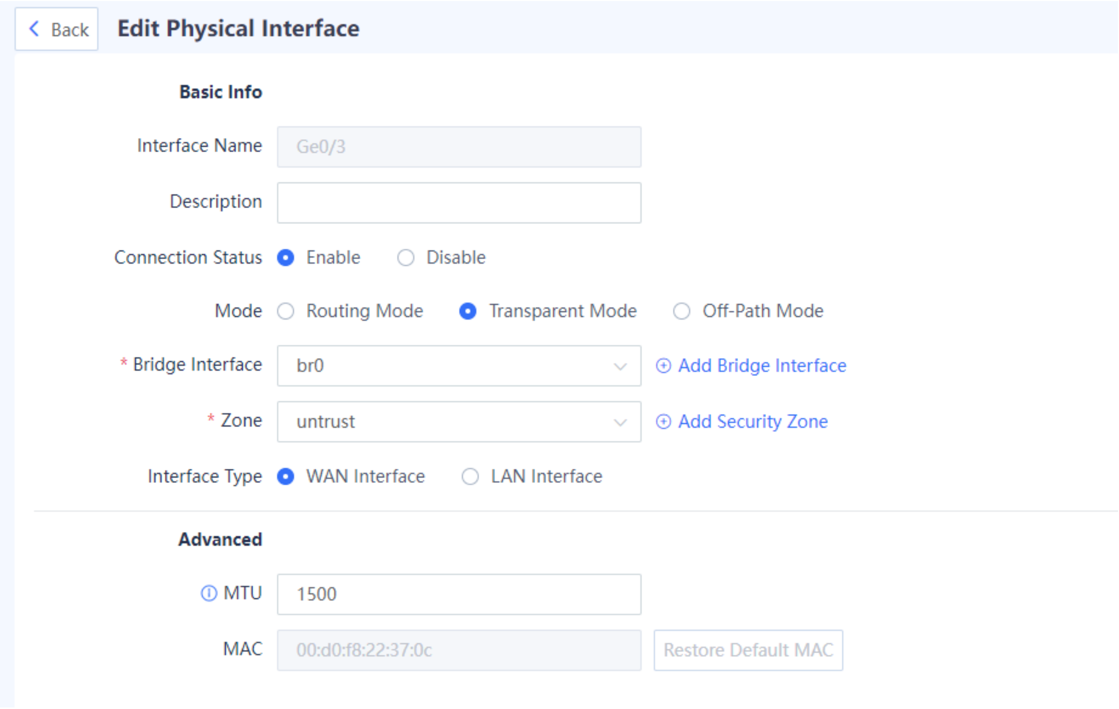
ⓘ MTU: 1500

MAC: 00:d0:f8:22:37:0b Restore Default MAC

c Configure attributes of Ge0/2 and click **Save**.

Item	Description
Mode	In out-of-band management, set all interfaces except the management interface to transparent mode.
Bridge Interface	Set to the default bridge interface **br0**.
Zone	Set to **trust**.
Interface Type	Set to **LAN Interface**.

d Repeat steps a and b to set Ge0/3.



Basic Info

Interface Name: Ge0/3

Description:

Connection Status: ● Enable ○ Disable

Mode: ○ Routing Mode ● Transparent Mode ○ Off-Path Mode

* Bridge Interface: br0

* Zone: untrust

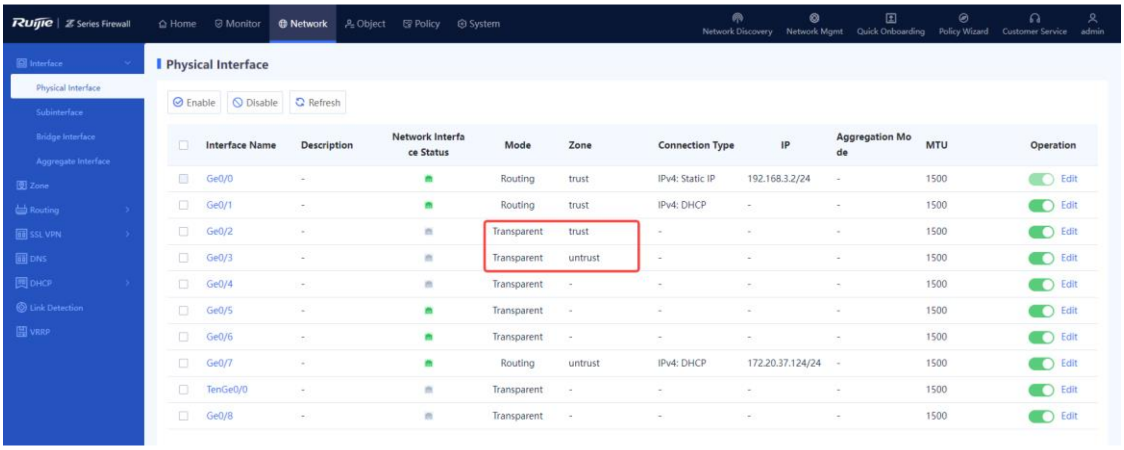
Interface Type: ● WAN Interface ○ LAN Interface

Advanced

MTU: 1500

MAC: 00:d0:f8:22:37:0c

The following figure shows the configuration result.



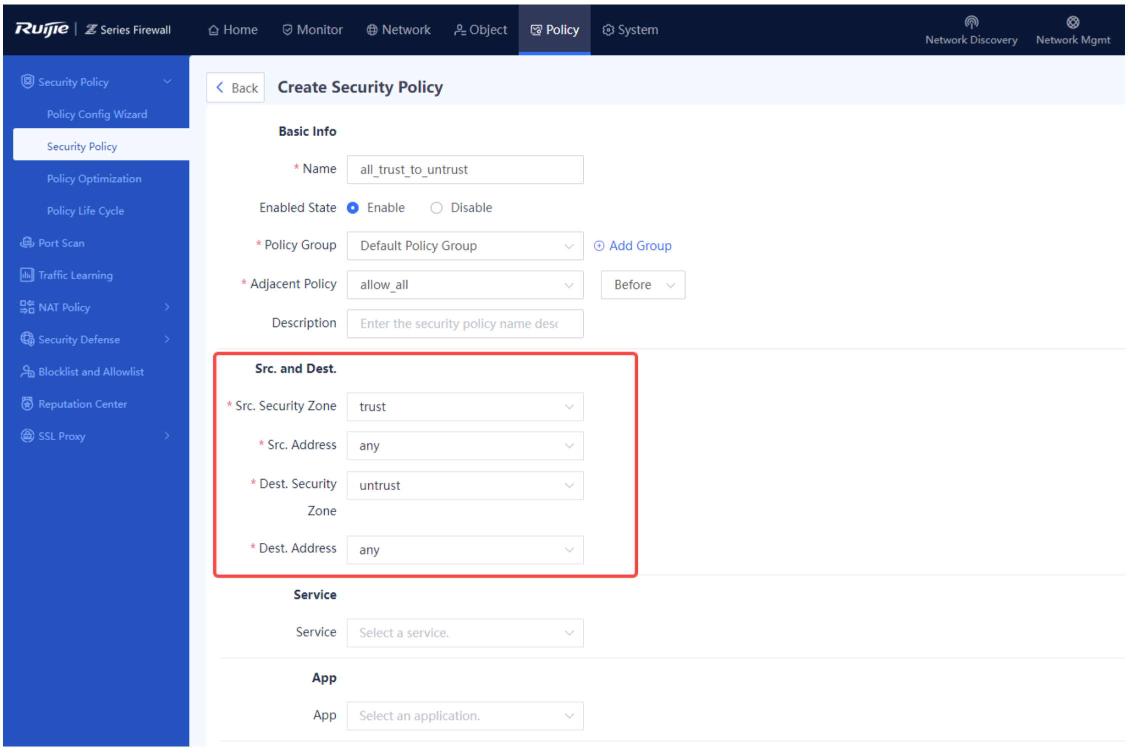
Physical Interface

Interface Name	Description	Network Interface Status	Mode	Zone	Connection Type	IP	Aggregation Mode	MTU	Operation
Ge0/0	-	●	Routing	trust	IPv4: Static IP	192.168.3.2/24	-	1500	Edit
Ge0/1	-	●	Routing	trust	IPv4: DHCP	-	-	1500	Edit
Ge0/2	-	●	Transparent	trust	-	-	-	1500	Edit
Ge0/3	-	●	Transparent	untrust	-	-	-	1500	Edit
Ge0/4	-	●	Transparent	-	-	-	-	1500	Edit
Ge0/5	-	●	Transparent	-	-	-	-	1500	Edit
Ge0/6	-	●	Transparent	-	-	-	-	1500	Edit
Ge0/7	-	●	Routing	untrust	IPv4: DHCP	172.20.37.124/24	-	1500	Edit
TenGe0/0	-	●	Transparent	-	-	-	-	1500	Edit
Ge0/8	-	●	Transparent	-	-	-	-	1500	Edit

(3) Configure a permit policy for traffic from zone **trust** to **untrust**.

a Choose **Policy** > **Security Policy** > **Security Policy**.

b Click **Create**.



Create Security Policy

Basic Info

* Name: all_trust_to_untrust

Enabled State: ● Enable ○ Disable

* Policy Group: Default Policy Group ⊕ Add Group

* Adjacent Policy: allow_all Before

Description: Enter the security policy name desc

Src. and Dest.

* Src. Security Zone: trust

* Src. Address: any

* Dest. Security Zone: untrust

* Dest. Address: any

Service

Service: Select a service.

App

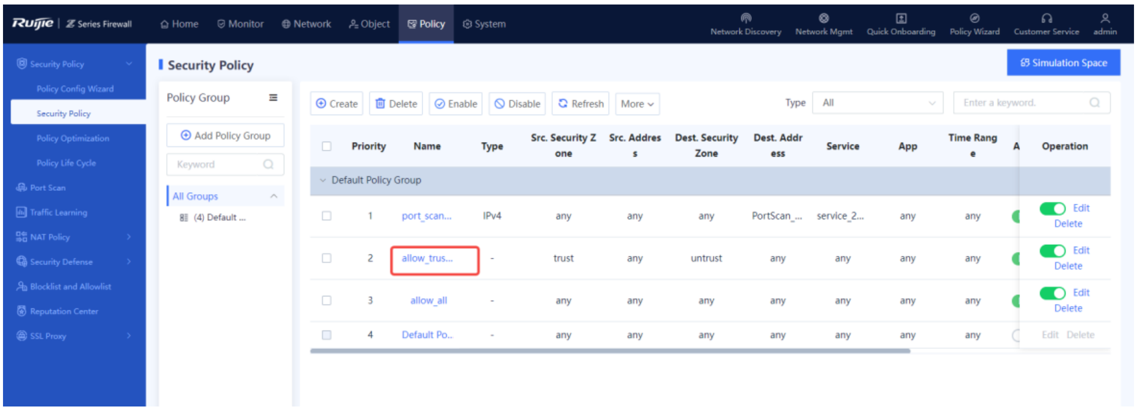
App: Select an application.

(4) Configure parameters for the new security policy and click **Save**.

Item	Description
Policy Group	Set to the default policy group.

Item	Description
Src. Security Zone	Set to **trust**.
Src. Address	Set to **any**. This policy is applicable to all IP addresses in the source security zone after it takes effect.
Dest. Security Zone	Set to **untrust**.
Dest. Address	Set to **any**. This policy is applicable to all IP addresses in the destination security zone after it takes effect.

The following figure shows the configuration result.



□	Priority	Name	Type	Src. Security Zone	Src. Address	Dest. Security Zone	Dest. Address	Service	App	Time Range	A	Operation
Default Policy Group												
□	1	port_scan...	IPv4	any	any	any	PortScan_...	service_2...	any	any		Edit Delete
□	2	allow_trus...	-	trust	any	untrust	any	any	any	any		Edit Delete
□	3	allow_all	-	any	any	any	any	any	any	any		Edit Delete
□	4	Default Po...	-	any	any	any	any	any	any	any		Edit Delete

Caution

- Access from the Internet to the firewall through NAT mapping may fail because the security policy permits only traffic from the security zone **trust** to **untrust**. To ensure successful access from the Internet to the firewall through NAT, you need to permit traffic from the security zone **untrust** to **trust** in a security policy.
- All firewall interfaces except the management interface can be switched to transparent mode. Interfaces in transparent mode cannot be configured with an IP address. When all the other interfaces are switched to transparent mode, the firewall can only be managed through the IP address of the bridge interface or the management interface.

Configuration Verification

Set the IP address of the PC to 192.168.1.2/24. Visit https://192.168.3.1 to access the web management page of the firewall.

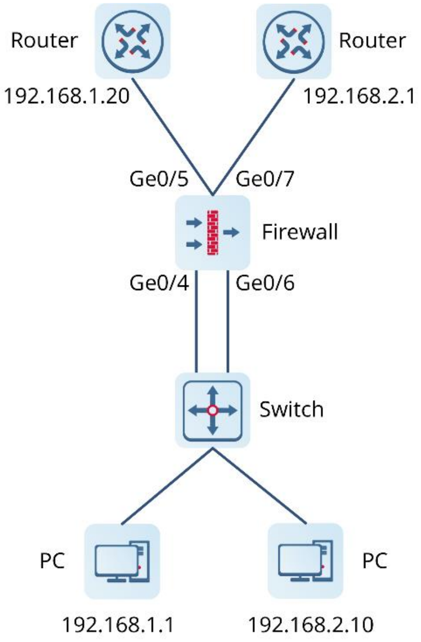
- You can successfully log in to the web management page to configure and manage the firewall.
- The PC on the same network segment as the management IP address can normally access the network.

6.2.4 Multi-bridge Deployment Mode

Application Scenario

Two groups of bridges need to be configured in the customer site: bridge 1: WAN 1 interface + LAN 1 interface; bridge 2: WAN 2 interface + LAN 2 interface.

Network Topology



Configuration Points

- Create four security zones **trust1**, **untrust1**, **trust2**, and **untrust2**.
- Create two groups of bridge interfaces **br1** and **br2**.
- Create two pairs of transparent interfaces and add them to different bridge interfaces and security zones. For example, add WAN 1 and LAN 1 to **br1**, with WAN 1 to security zone **untrust1** and LAN 1 to security zone **trust1**; add WAN 2 and LAN 2 to **br2**, with WAN 2 to security zone **untrust2** and LAN 2 to security zone **trust2**.
- Create two security policies to permit traffic between the specified zones.

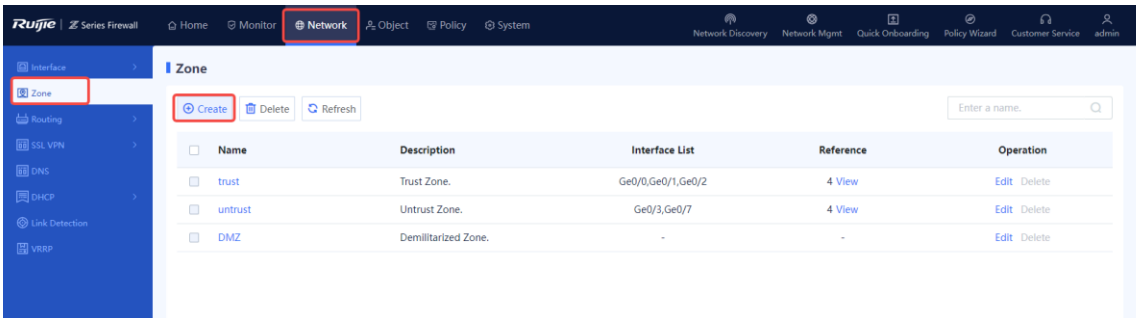
Caution

The multi-bridge function is supported from NTOS1.0R4. If your version is lower than NTOS1.0R4, upgrade it to NTOS1.0R4 or higher.

Procedure

(1) Create security zones.

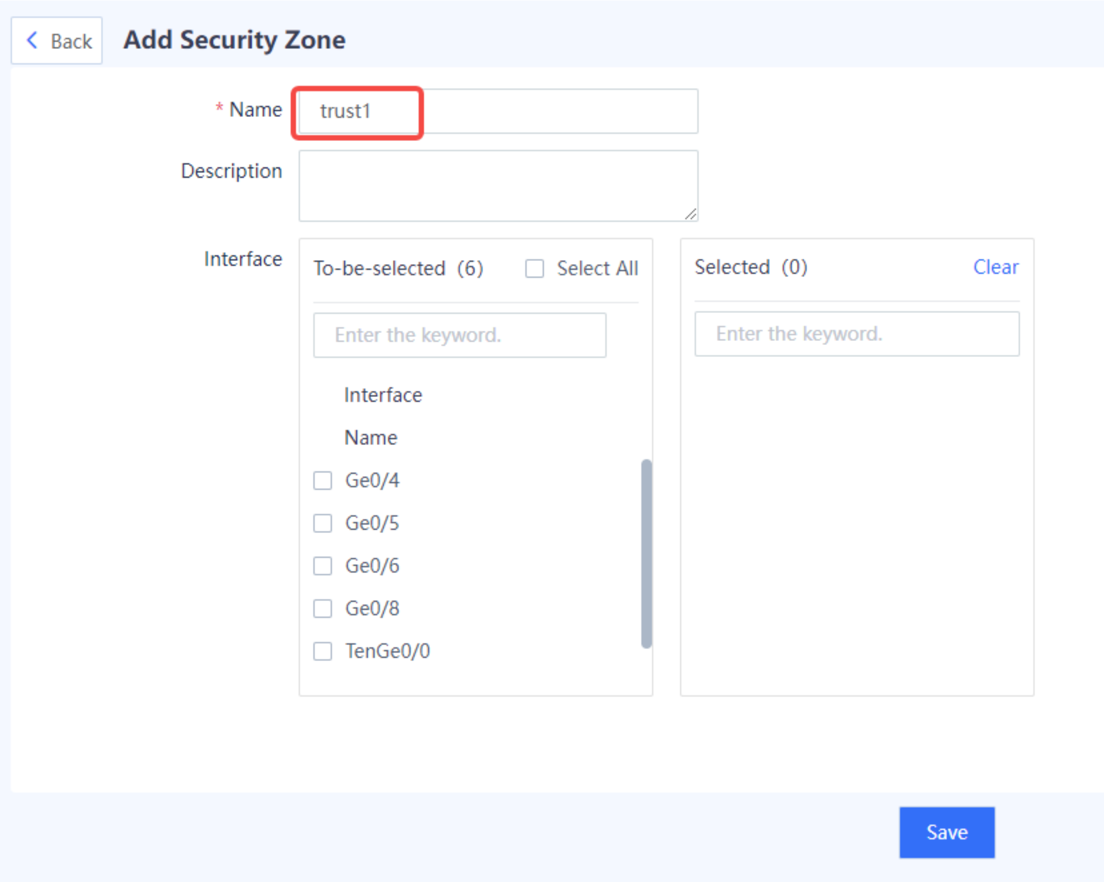
a Choose **Network** > **Zone**.



Zone

Name	Description	Interface List	Reference	Operation
trust	Trust Zone.	Ge0/0,Ge0/1,Ge0/2	4 View	Edit Delete
untrust	Untrust Zone.	Ge0/3,Ge0/7	4 View	Edit Delete
DMZ	Demilitarized Zone.	-	-	Edit Delete

b Click **Create** and create security zone **trust1**.



Add Security Zone

* Name: trust1

Description:

Interface: To-be-selected (6) □ Select All

Interface Name
□ Ge0/4
□ Ge0/5
□ Ge0/6
□ Ge0/8
□ TenGe0/0

Selected (0)

c Configure parameters for the security zone **trust1** and click **Save**.

d Repeat the preceding steps to create other security zones.

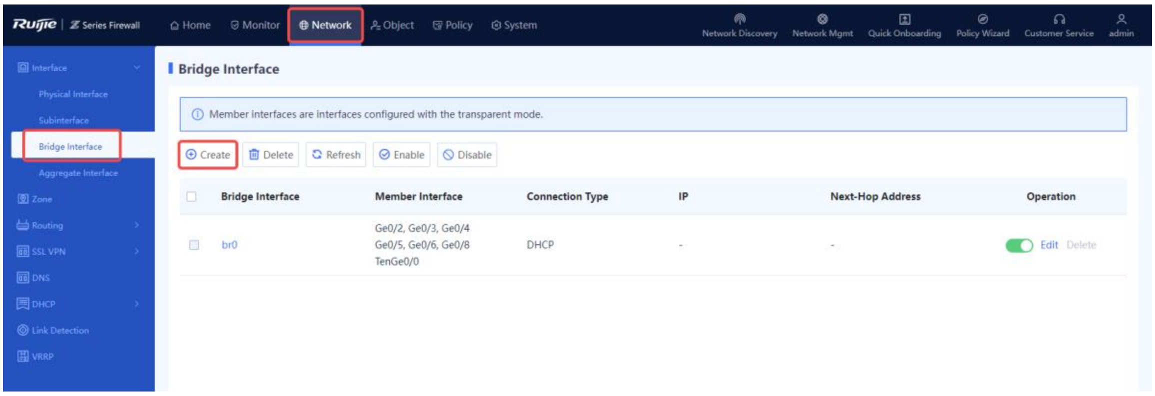
Caution

The security zone name must be unique.

---

(2) Create bridge interfaces.

a Choose **Network** > **Interface** > **Bridge Interface**.

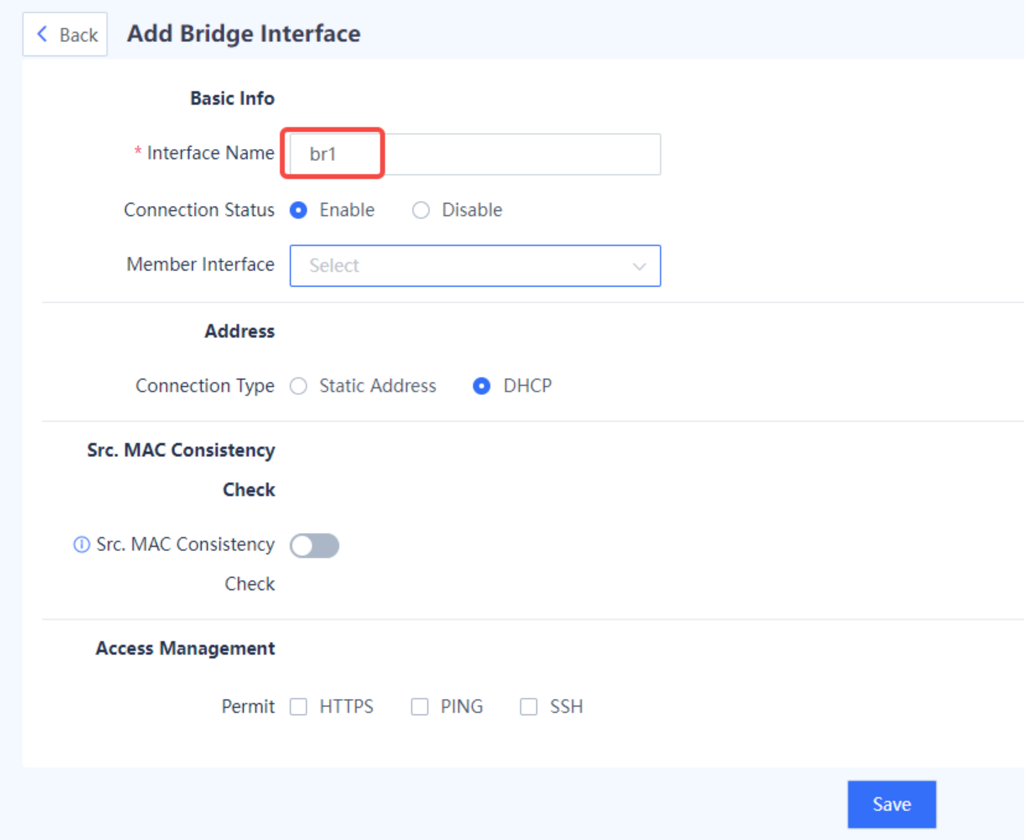


Bridge Interface

ⓘ Member interfaces are interfaces configured with the transparent mode.

□	Bridge Interface	Member Interface	Connection Type	IP	Next-Hop Address	Operation
□	br0	Ge0/2, Ge0/3, Ge0/4 Ge0/5, Ge0/6, Ge0/8 TenGe0/0	DHCP	-	-	Edit Delete

b Click **Create** and create bridge interface **br1**.



Add Bridge Interface

Basic Info

* Interface Name: br1

Connection Status: ● Enable ○ Disable

Member Interface: Select

Address

Connection Type: ○ Static Address ● DHCP

Src. MAC Consistency Check

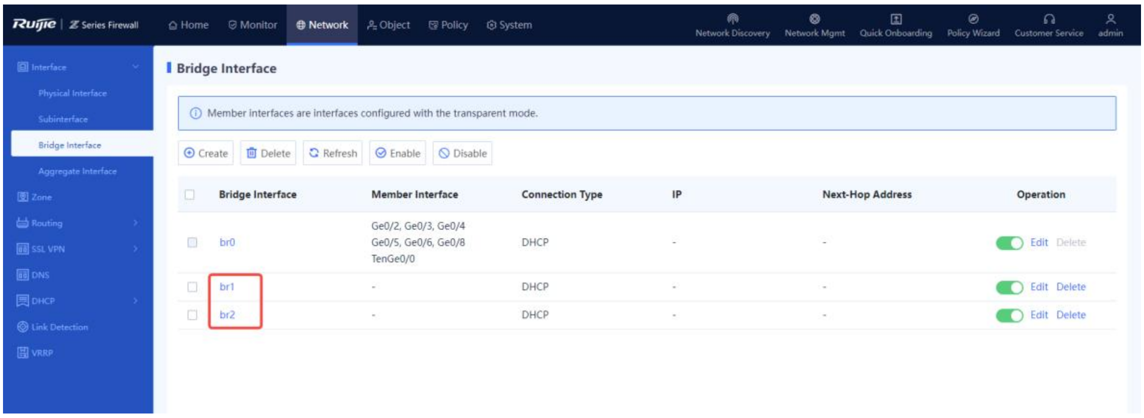
ⓘ Src. MAC Consistency Check

Access Management

Permit: □ HTTPS □ PING □ SSH

c Configure parameters for the bridge **br1** and click **Save**.

d Repeat the preceding steps to create bridge interface **br2**.



Bridge Interface

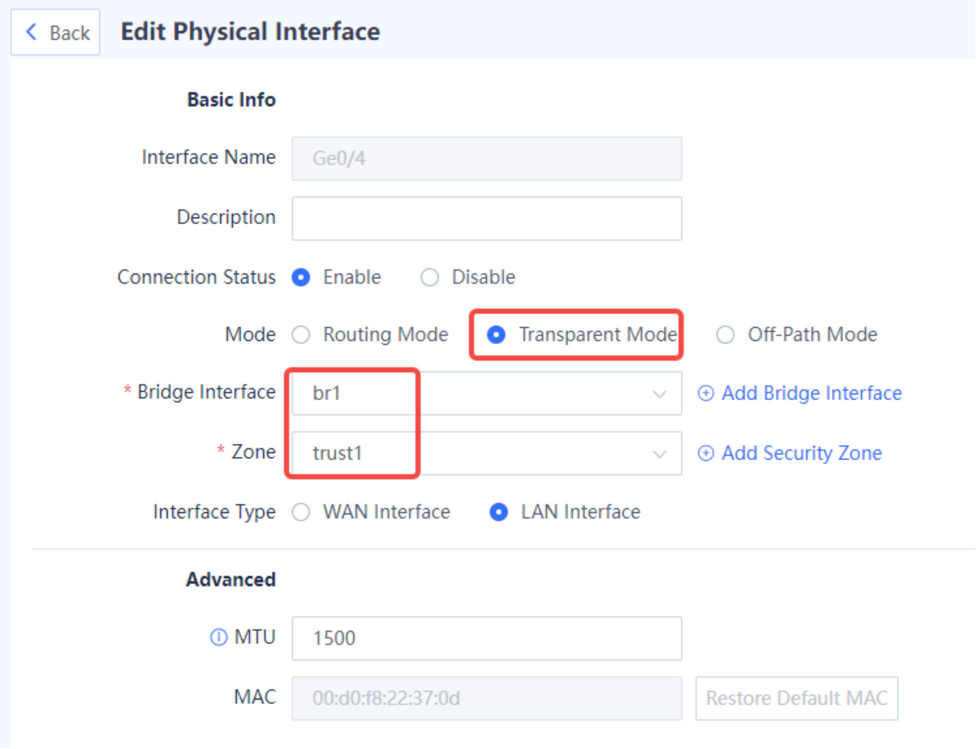
Member interfaces are interfaces configured with the transparent mode.

□	Bridge Interface	Member Interface	Connection Type	IP	Next-Hop Address	Operation
□	br0	Ge0/2, Ge0/3, Ge0/4 Ge0/5, Ge0/6, Ge0/8 TenGe0/0	DHCP	-	-	Edit Delete
□	br1	-	DHCP	-	-	Edit Delete
□	br2	-	DHCP	-	-	Edit Delete

(3) Convert two pairs of interfaces to transparent mode and add them to the corresponding bridge interfaces and zones.

a Choose **Network** > **Interface** > **Physical Interface**.

b Select the corresponding interface and click **Edit**.



Edit Physical Interface

Basic Info

Interface Name: Ge0/4

Description:

Connection Status: ● Enable ○ Disable

Mode: ○ Routing Mode ● Transparent Mode ○ Off-Path Mode

* Bridge Interface: br1

* Zone: trust1

Interface Type: ○ WAN Interface ● LAN Interface

Advanced

MTU: 1500

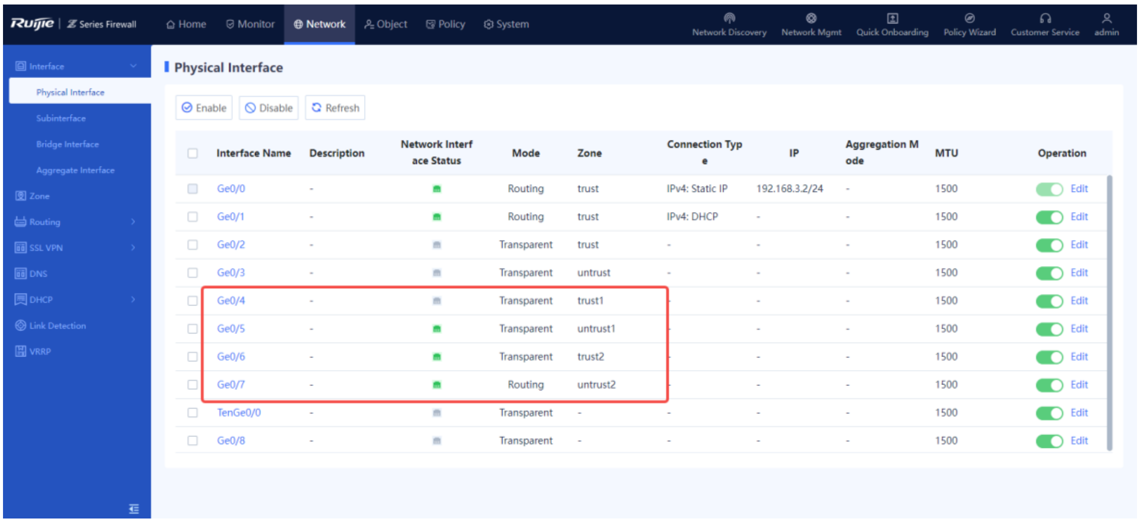
MAC: 00:d0:f8:22:37:0d

c Configure parameters for the interface and click **Save**.

Set **Mode** to **Transparent Mode**, **Bridge Interface** to **br1**, and **Zone** to **trust1**.

d Repeat the preceding steps to convert Ge0/5 to transparent mode and add it **br1** and **untrust1**; convert Ge0/6 to transparent mode and add it **br2** and **trust2**; convert Ge0/7 to transparent mode and add it to **br2** and **untrust2**.

The following figure shows the configuration result.



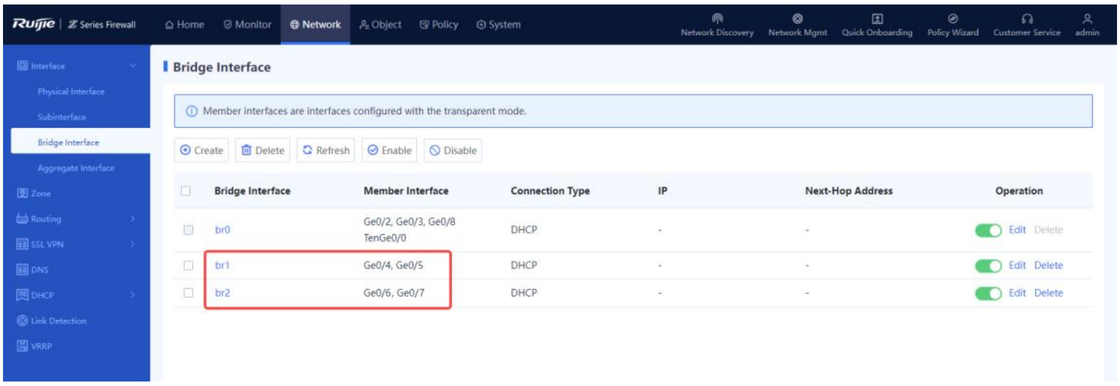
Physical Interface

□	Interface Name	Description	Network Interface Status	Mode	Zone	Connection Type	IP	Aggregation Mode	MTU	Operation
□	Ge0/0	-	🟩	Routing	trust	IPv4: Static IP	192.168.3.2/24	-	1500	Edit
□	Ge0/1	-	🟩	Routing	trust	IPv4: DHCP	-	-	1500	Edit
□	Ge0/2	-	▨	Transparent	trust	-	-	-	1500	Edit
□	Ge0/3	-	▨	Transparent	untrust	-	-	-	1500	Edit
□	Ge0/4	-	▨	Transparent	trust1	-	-	-	1500	Edit
□	Ge0/5	-	🟩	Transparent	untrust1	-	-	-	1500	Edit
□	Ge0/6	-	🟩	Transparent	trust2	-	-	-	1500	Edit
□	Ge0/7	-	🟩	Routing	untrust2	-	-	-	1500	Edit
□	TenGe0/0	-	▨	Transparent	-	-	-	-	1500	Edit
□	Ge0/8	-	▨	Transparent	-	-	-	-	1500	Edit

Caution

When all interfaces except Ge0/0 are set to transparent mode, the management interface must be configured with an IP address and the next hop to ensure device access through the management interface.

Choose **Network** > **Interface** > **Bridge Interface**. On the page that is displayed, you can find members of a bridge interface.



Bridge Interface

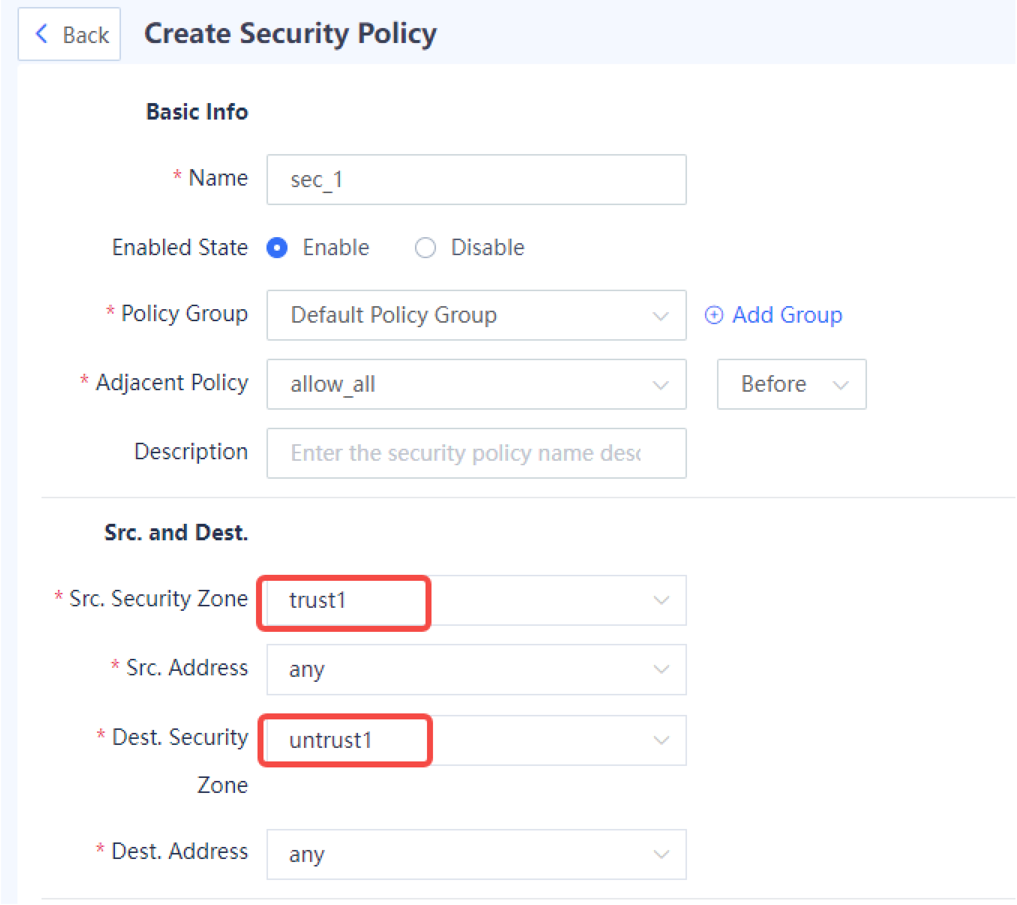
Member interfaces are interfaces configured with the transparent mode.

□	Bridge Interface	Member Interface	Connection Type	IP	Next-Hop Address	Operation
□	br0	Ge0/2, Ge0/3, Ge0/8 TenGe0/0	DHCP	-	-	Edit Delete
□	br1	Ge0/4, Ge0/5	DHCP	-	-	Edit Delete
□	br2	Ge0/6, Ge0/7	DHCP	-	-	Edit Delete

(4) Create security policies 1 and 2 and associate zones **trust1** and **untrust1** with security policy 1 and zones **trust2** and **untrust2** with security policy 2.

a Choose **Policy** > **Security Policy**.

b Click **Create** and create security policy 1.



Back **Create Security Policy**

Basic Info

* Name: sec_1

Enabled State: ● Enable ○ Disable

* Policy Group: Default Policy Group

* Adjacent Policy: allow_all Before

Description: Enter the security policy name desc

Src. and Dest.

* Src. Security Zone: trust1

* Src. Address: any

* Dest. Security Zone: untrust1

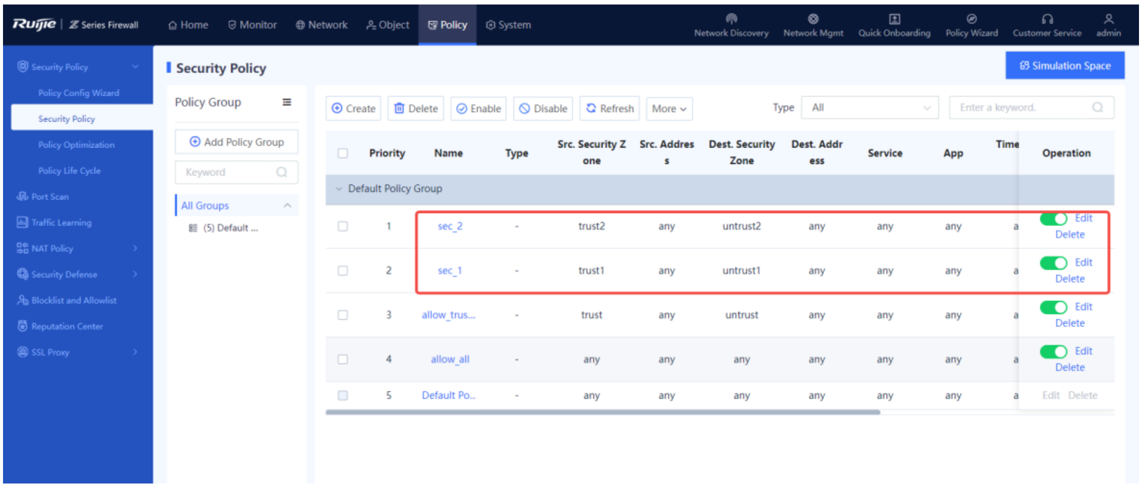
* Dest. Address: any

c Configure parameters for security policy 1 and click **Save**.

Item	Description
Name	**sec_1**
Policy Group	Set to the default policy group.
Src. Security Zone	Set to **trust1**.
Src. Address	Set to **any**. This policy is applicable to all IP addresses in the source security zone after it takes effect.
Dest. Security	Set to **untrust1**.

Item	Description
Zone	
Dest. Address	Set to **any**. This policy is applicable to all IP addresses in the destination security zone after it takes effect.

d Repeat the preceding steps to create security policy 2 and associate it with zones **trust2** and **untrust2**.



Security Policy

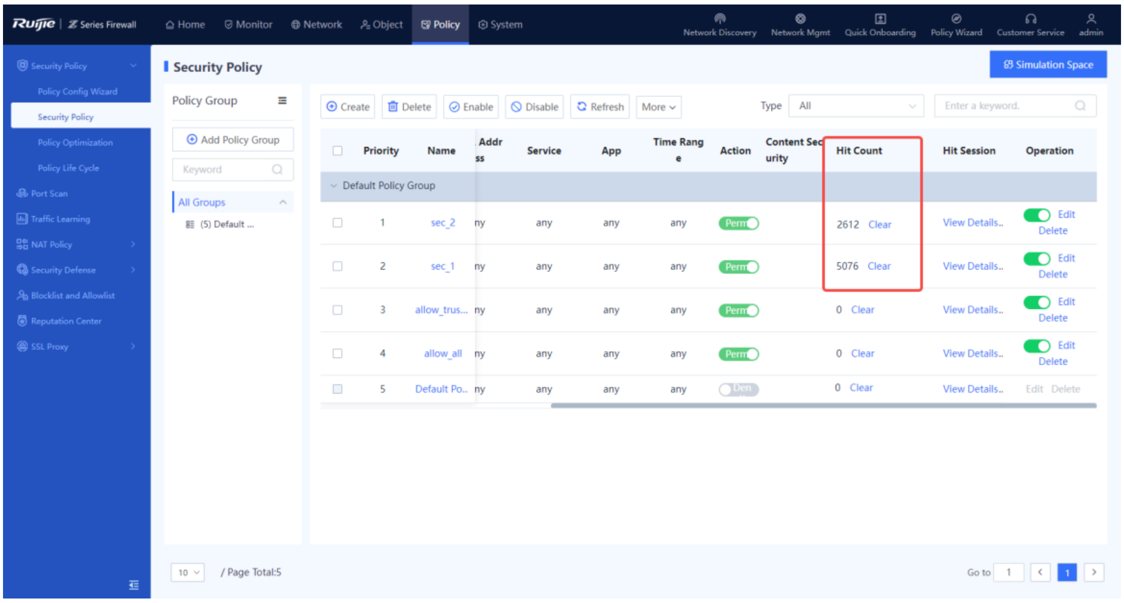
Type: All

	Priority	Name	Type	Src. Security Zone	Src. Address	Dest. Security Zone	Dest. Address	Service	App	Time	Operation
Default Policy Group											
□	1	sec_2	-	trust2	any	untrust2	any	any	any	a	Edit Delete
□	2	sec_1	-	trust1	any	untrust1	any	any	any	a	Edit Delete
□	3	allow_trus...	-	trust	any	untrust	any	any	any	a	Edit Delete
□	4	allow_all	-	any	any	any	any	any	any	a	Edit Delete
□	5	Default Po...	-	any	any	any	any	any	any	a	Edit Delete

Configuration Verification

(1) Deploy two PCs in LAN 1 and LAN 2 respectively. Confirm that the PCs can normally access the Internet over the uplink gateways.

The following figure shows the number of hits of each security policy.



□	Priority	Name	Addr ss	Service	App	Time Range	Action	Content Security	Hit Count	Hit Session	Operation
Default Policy Group											
□	1	sec_2	ny	any	any	any	Perm		2612 Clear	View Details..	Edit Delete
□	2	sec_1	ny	any	any	any	Perm		5076 Clear	View Details..	Edit Delete
□	3	allow_trus...	ny	any	any	any	Perm		0 Clear	View Details..	Edit Delete
□	4	allow_all	ny	any	any	any	Perm		0 Clear	View Details..	Edit Delete
□	5	Default Po..	ny	any	any	any	Den		0 Clear	View Details..	Edit Delete

(2) PC1 can normally access 192.168.2.1.

(3) PC2 can normally access 192.168.1.20.

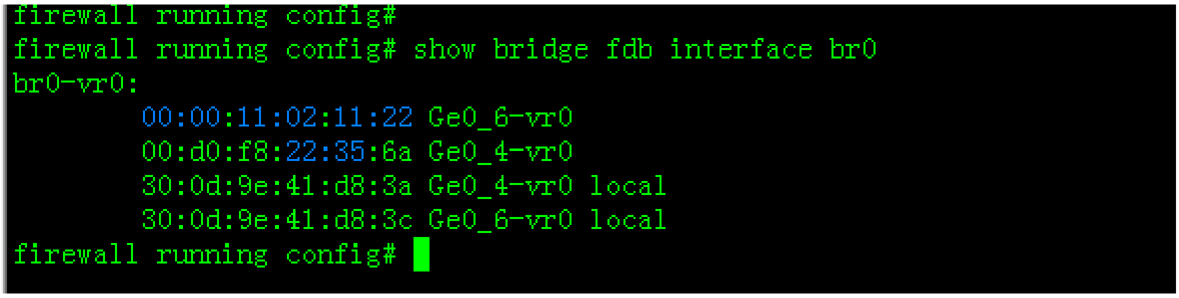
6.2.5 Precautions for Deploying Transparent Bridge Mode

Suggestions

Configure security policies to permit traffic between interfaces working in transparent mode.

Precautions

Run commands as shown in the following figure to view MAC addresses learned by the firewall.



```
firewall running config#
firewall running config# show bridge fdb interface br0
br0-vr0:
        00:00:11:02:11:22 Ge0_6-vr0
        00:d0:f8:22:35:6a Ge0_4-vr0
        30:0d:9e:41:d8:3a Ge0_4-vr0 local
        30:0d:9e:41:d8:3c Ge0_6-vr0 local
firewall running config#
```

Function Restrictions

- IPsec VPN and SSL VPN cannot be configured in transparent mode, which does not support dynamic routes, policy-based routing, or DHCP.
- The management interface Ge0/0 cannot be converted to transparent mode.

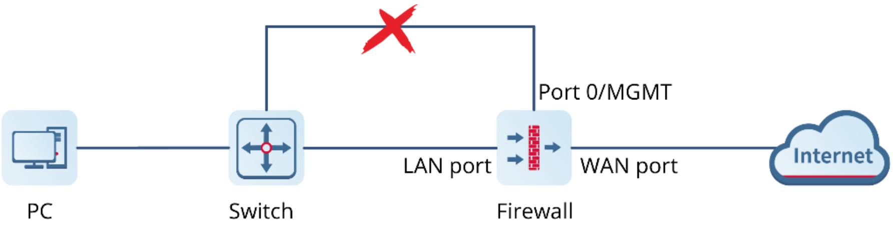
6.2.6 Configuring a Bridge Interface

Application Scenario

Bridge interfaces are applicable to firewall deployment in transparent mode.

A bridge interface is a logical virtual interface composed of physical interfaces in transparent mode. You need to correctly configure an IP address and gateway to enable the firewall to forward traffic at Layer 3 through the bridge interface. The firewall supports multiple groups of bridge interfaces, and traffic of the bridge groups is isolated from one another.

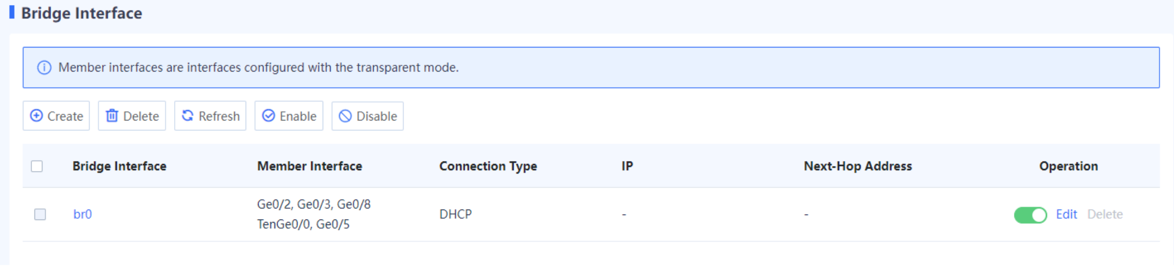
In actual networking, you do not need to separately connect port 0/MGMT to devices such as switch. Remote O&M can be implemented through the bridge interface, which is easy to implement.



Procedure

(1) Choose **Network** > **Interface** > **Bridge Interface**.

The system displays the bridge interface configured in the current system. The firewall has a default bridge interface named **br0**, which cannot be deleted.


Bridge Interface

ⓘ Member interfaces are interfaces configured with the transparent mode.

□	Bridge Interface	Member Interface	Connection Type	IP	Next-Hop Address	Operation
□	br0	Ge0/2, Ge0/3, Ge0/8 TenGe0/0, Ge0/5	DHCP	-	-	Edit Delete

Note

Members of a bridge interface are interfaces working in transparent mode.

(2) Perform the corresponding operation on the bridge interface based on service requirements.

- If a new physical interface works in transparent mode, click **Refresh** to obtain the latest member interface information.

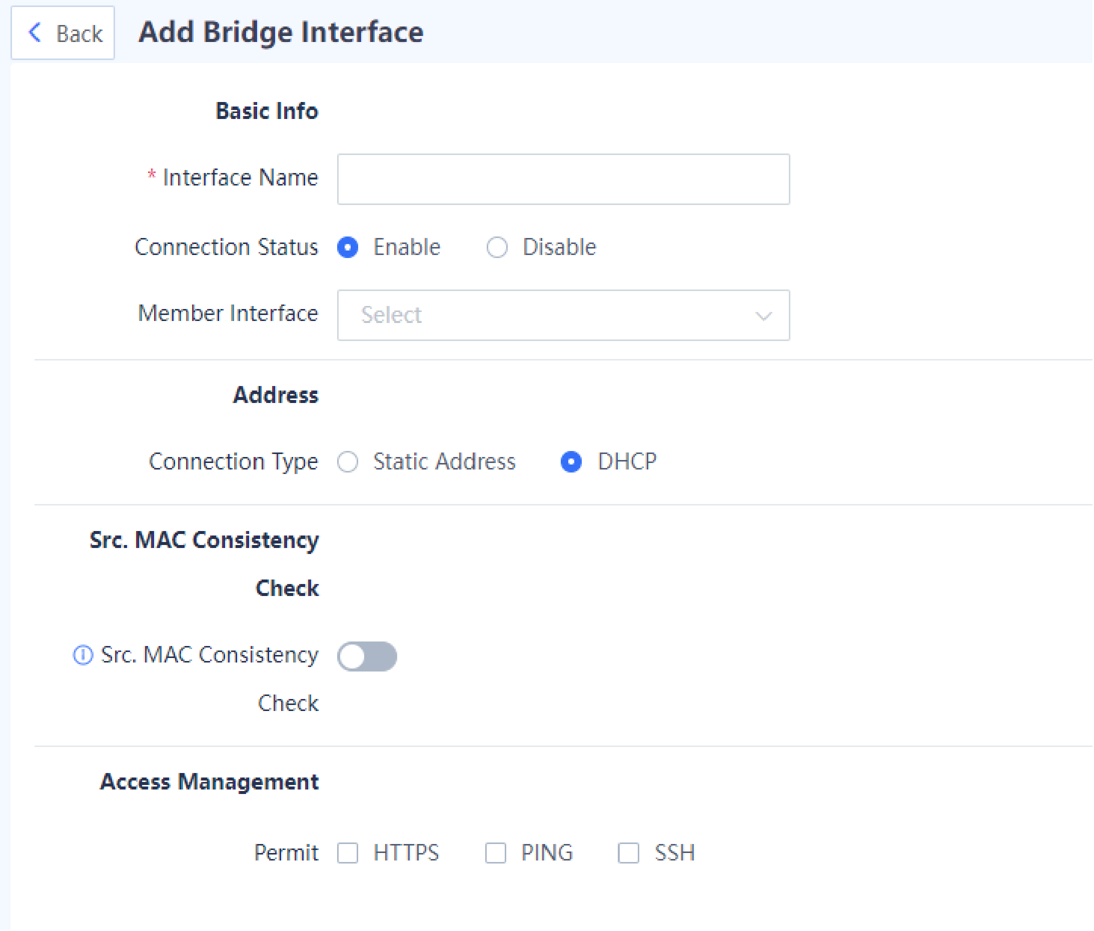
- Click ● to enable or disable the bridge interface.
- Click **Delete** to delete the bridge interface.

Caution

- The default bridge interface **br0** of the firewall cannot be deleted.
- The bridge interface with a member interface cannot be deleted. You need to remove the member interfaces before you delete a bridge interface.

- Click **Edit** and configure the bridge interface. Click **Create** and create a new bridge interface.

  Configure parameters for the bridge interface on the **Edit Bridge Interface** or **Add Bridge Interface** page and click **Save**.



< Back **Add Bridge Interface**

Basic Info

* Interface Name

Connection Status ● Enable ○ Disable

Member Interface Select

Address

Connection Type ○ Static Address ● DHCP

Src. MAC Consistency Check

Src. MAC Consistency Check

Access Management

Permit □ HTTPS □ PING □ SSH

Item	Description	Remarks
Interface	Name of a bridge interface.	● Characters such as

Item	Description	Remarks
Name		`~!#%^&*+\\|{};:'"/<>? and spaces are not allowed. ● The name is specified when you create a bridge interface and cannot be modified in later steps. [Example] br1
Connection Status	Whether to enable the bridge interface.	[Example] Enable
Member Interface	Member interface in the bridge interface. Members of the bridge interface are interfaces set to transparent mode. One bridge interface can contain multiple transparent interfaces, but each transparent interface can belong to only one bridge interface.	To add a member to the bridge interface, set **Bridge Interface** to the current bridge interface when you configure the corresponding member interface (such as physical interface or aggregate interface). [Example] Ge0/2
Address		
Connection Type	Connection type of the bridge interface. The options are as follows: ● **Static Address**: Applicable when the network administrator specifies an IP address for the device based on the predefined IP address planning. This connection type requires the network administrator to possess	[Example] Static Address

Item	Description	Remarks
	certain network knowledge. When this option is selected, you need to set IP/Mask and Next-Hop Address. ● **DHCP**: Applicable when the network administrator is not professional. The bridge interface automatically obtains an IP address from the upper-layer DHCP server for Internet access.	
IP/Mask	IP address and mask of the interface.	You need to set this parameter when **Connection Type** is set to **Static Address**. [Example] 192.168.20.1/24
Next-Hop Address	Next router address to reach the router with the destination address.	You need to set this parameter when **Connection Type** is set to **Static Address**. [Example] 192.168.20.2/24
Default Route	Whether to enable the default route.	[Example] Enable
Src. MAC Consistency Check	Whether to enable source MAC address consistency check. If you select **Enable**, the firewall checks the source MAC address of the packet with the source MAC address in the session. If they are different, the firewall does not	[Example] Enable

Item	Description	Remarks
	check the session status of the packet but transparently forwards the packet over the bridge network directly.	
Access Management	Whether the bridge interface supports HTTPS, ping, and SSH.	The configuration takes effect when local defense is enabled on the device. [Example] Select **HTTPS**.

6.3 Routing Mode

6.3.1 Preparations

Confirm the following information before performing the configuration:

- If you deploy the firewall in routing mode, you need to confirm the network scale, the number of users who want to access the Internet, access mode (static address, ADSL dialup, or dynamic address obtaining through DHCP), port type (GE electrical port, GE optical port, or 10GE optical port), access bandwidth, and IP address planning.
- If a service system is involved, check whether servers are deployed and whether the servers permit access from external users.
- Check whether users need to use applications such as video conference.

Note

In the current version, the NAT mode does not support applications such as video and conference.

- Software version obtaining methods

Method	Path
Official website	https://www.ruijienetworks.com/

	Choose **Support** > **Download** > **Reyee** and find the latest version of the Z-S series firewall under RG-WALL 1600-Z-S series cloud management firewalls.
Web management page of the firewall	Choose **System** > **System Maintenance** > **System Upgrade** > **Online Upgrade** > **Recommended Version** to upgrade to the latest version (recommended) in online mode.
Ruijie Cloud	After the device goes online on the Ruijie Cloud, you can remotely upgrade the device in online mode on the Ruijie Cloud (without the need for local upgrade). Choose **Monitoring** > **Device** > **Firewall**, select a device, select a version, and click **Upgrade**.

⚠ **Caution**

If the quick onboarding wizard is not used for the deployment, you must adjust the system time in advance. Otherwise, the time clock is inaccurate, which may affect reports and logs. To set the system time, choose **System** > **System Config** > **System Time**.

6.3.2 Single-Line Onboarding (Quick Deployment)

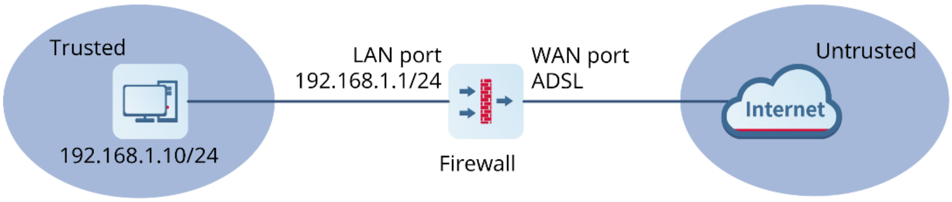
Network Requirements

As shown in the following figure, the firewall functions as an ONU directly connected to the network egress. In this networking, the firewall is similar to a router that participates in routing topology building. The WAN interface can use a static IP address or an address dynamically allocated through DHCP or dial up using ADSL to communicate with terminals in the LAN network segment 192.168.1.0/24.

ⓘ **Note**

DHCP is disabled on firewall interfaces by default. Any interface on the firewall can be used as a LAN interface or a WAN interface.

Network Topology



Assume that the username and password allocated by the ISP are **admin** and **ruijie@123**.

Configuration Points

(1) Implement quick onboarding. Select a deployment mode (routing mode) and configure a WAN interface and a LAN interface to complete Internet access.

- WAN interface: Applicable to Internet access to connect the firewall to the Internet. Generally, the WAN interface is directly connected to the FTTH ONU of the ISP. The following connection types are supported based on the interface type:
  - Static address: Applicable when the network administrator specifies an IP address for the device based on the predefined IP address planning. This connection type requires the network administrator to possess certain network knowledge. The IP address/mask and next-hop address must be configured.
  - DHCP: Applicable when no professional network administrator is available. The user terminal automatically obtains an IP address to access the Internet after the terminal is connected to the firewall.
  - ADSL dialup: Applicable for dialup access to the ISP network. The account and password of the dialup user must be configured.
- LAN interface: Applicable for **connection to LAN** devices, such as PCs, switches, and printers.

(2) (Optional) Check the connectivity. The system automatically checks whether the firewall is connected to the Internet.

(3) (Optional) Import licenses.

a Before license activation, log in to the Ruijie Secure Cloud Platform (https://secloud-en.ruijienetworks.com), choose **Device Authorization** > **Activate License**, and generate a license file. (The account of the Secure Cloud Platform is used to activate and change the license. Keep the account safe.)

b Select an activation method (online activation or offline activation) based on network connection information of the firewall.

(4) Complete the quick onboarding configuration.

(5) (Optional) Implement remote O&M on the cloud.

Procedure

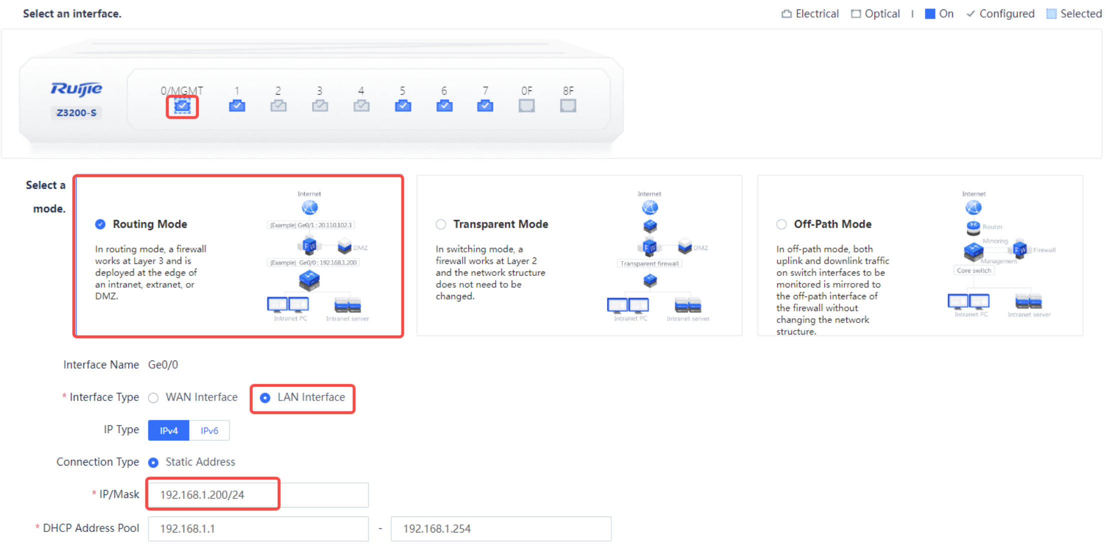
(1) Implement quick onboarding.

a Configure the IP addresses of the PC and the 0/MGMT management interface to be on the same network segment. Visit https://192.168.1.200 (default address) to log in to the device using the default account and password (**admin** and **firewall**).

b Configure a WAN interface and a LAN interface to complete Internet access.

In this example, Ge0/0 (port 0/MGMT by default) is used as the LAN interface and Ge0/1 (enabled with DHCP for dynamic address allocation) is used as the WAN interface.

c Set the mode to routing.



Select an interface. ☐ Electrical ☐ Optical | ■ On ✓ Configured ▢ Selected

Select a mode.

● Routing Mode
In routing mode, a firewall works at Layer 3 and is deployed at the edge of an intranet, extranet, or DMZ.

○ Transparent Mode
In switching mode, a firewall works at Layer 2 and the network structure does not need to be changed.

○ Off-Path Mode
In off-path mode, both uplink and downlink traffic on switch interfaces to be monitored is mirrored to the off-path interface of the firewall without changing the network structure.

Interface Name Ge0/0

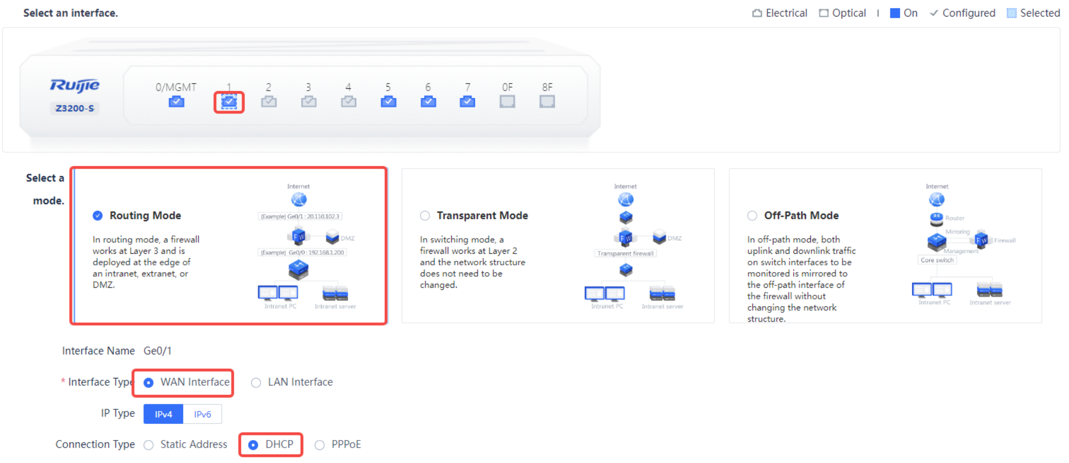
* Interface Type ○ WAN Interface ● LAN Interface

IP Type [IPv4] IPv6

Connection Type ● Static Address

* IP/Mask 192.168.1.200/24

* DHCP Address Pool 192.168.1.1 - 192.168.1.254



Select an interface. ☐ Electrical ☐ Optical | ■ On ✓ Configured ▢ Selected

Select a mode.

● Routing Mode
In routing mode, a firewall works at Layer 3 and is deployed at the edge of an intranet, extranet, or DMZ.

○ Transparent Mode
In switching mode, a firewall works at Layer 2 and the network structure does not need to be changed.

○ Off-Path Mode
In off-path mode, both uplink and downlink traffic on switch interfaces to be monitored is mirrored to the off-path interface of the firewall without changing the network structure.

Interface Name Ge0/1

* Interface Type ● WAN Interface ○ LAN Interface

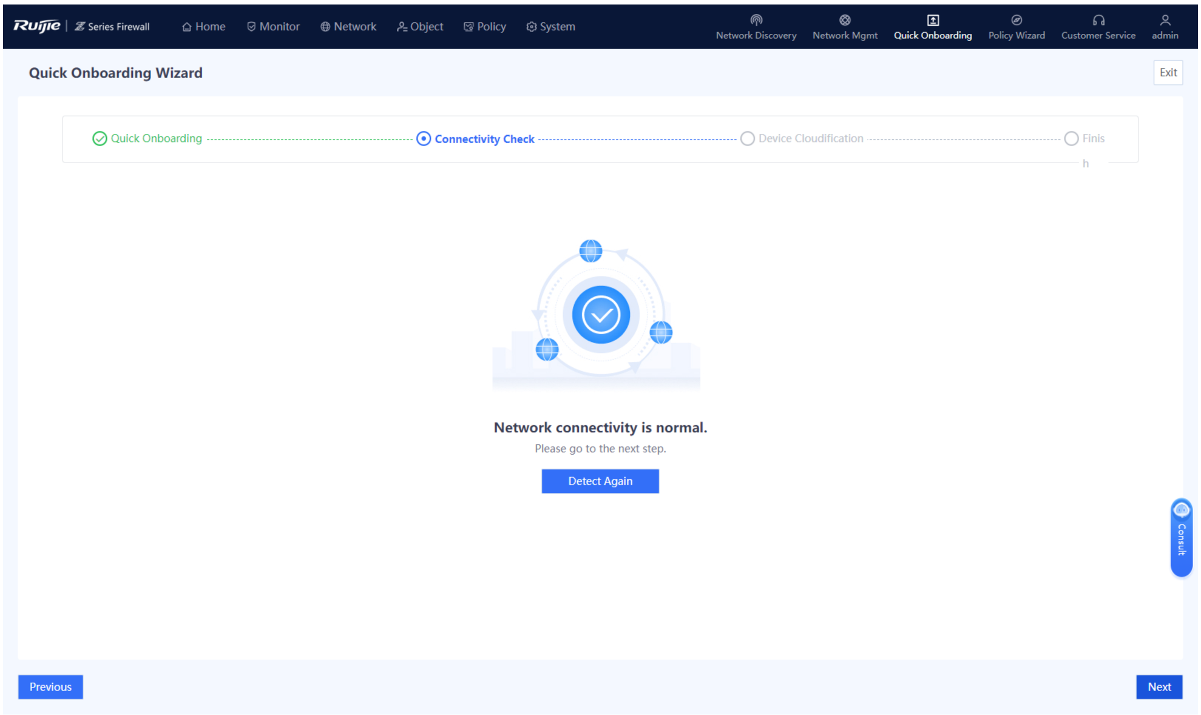
IP Type [IPv4] IPv6

Connection Type ○ Static Address ● DHCP ○ PPPoE

⚠ **Caution**

Each interface can be separately configured to work in routing or bridge mode.

(2) (Optional) Check the connectivity.

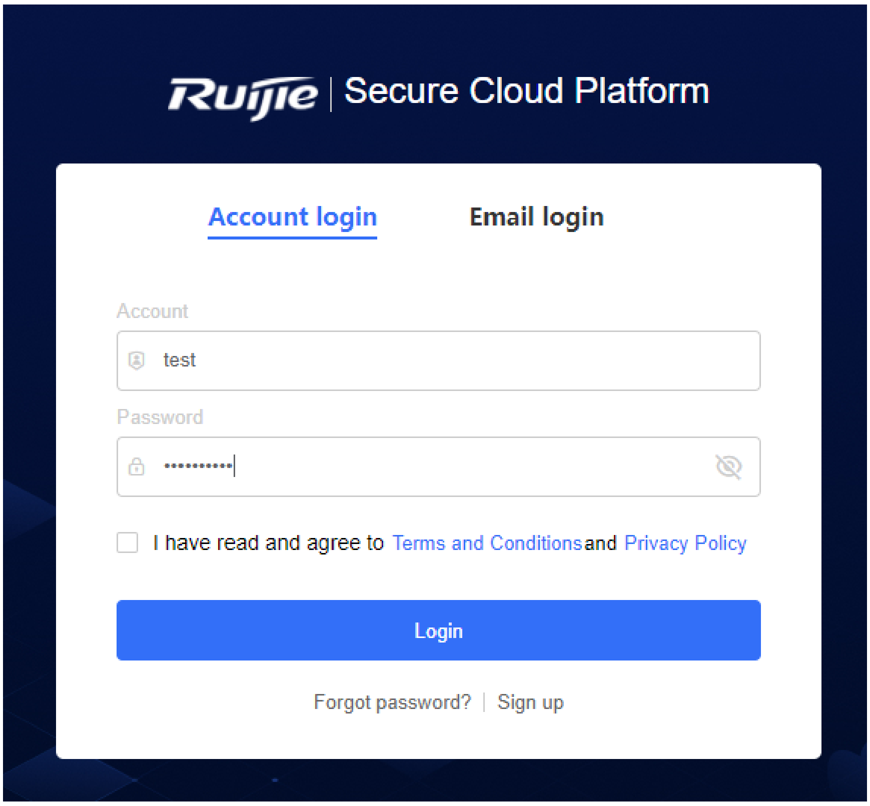


Network connectivity is normal.

Please go to the next step.

(3) (Optional) Import licenses.

a Before license activation, log in to the Ruijie Secure Cloud Platform (https://secloud-en.ruijienetworks.com).



Account: test

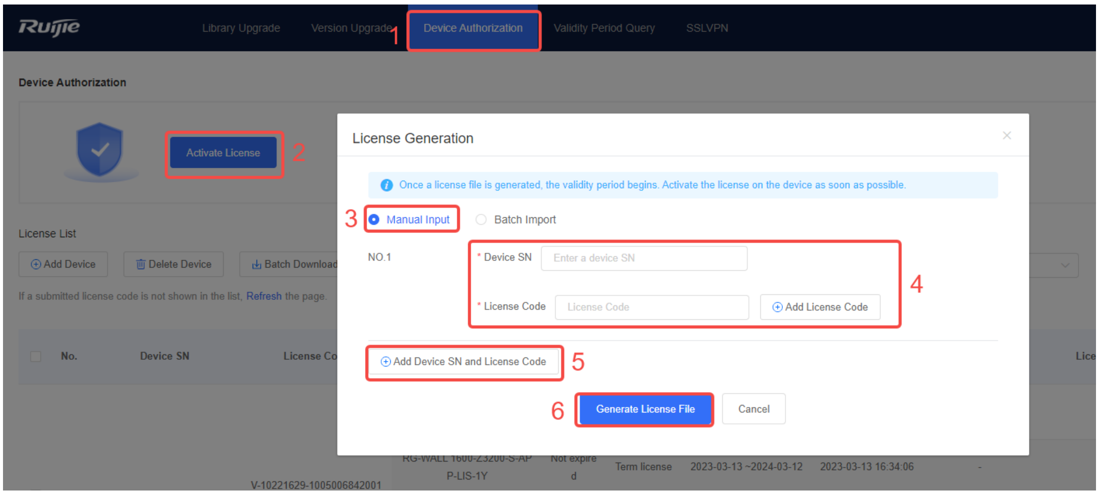
Password: ••••••••••

□ I have read and agree to Terms and Conditions and Privacy Policy

b Choose **Device Authorization** > **Activate License** and generate a license file.

Note

(The account of the Secure Cloud Platform is used to activate and change the license. Keep the account safe.)



If a submitted license code is not shown in the list, Refresh the page.

Once a license file is generated, the validity period begins. Activate the license on the device as soon as possible.

● Manual Input ○ Batch Import

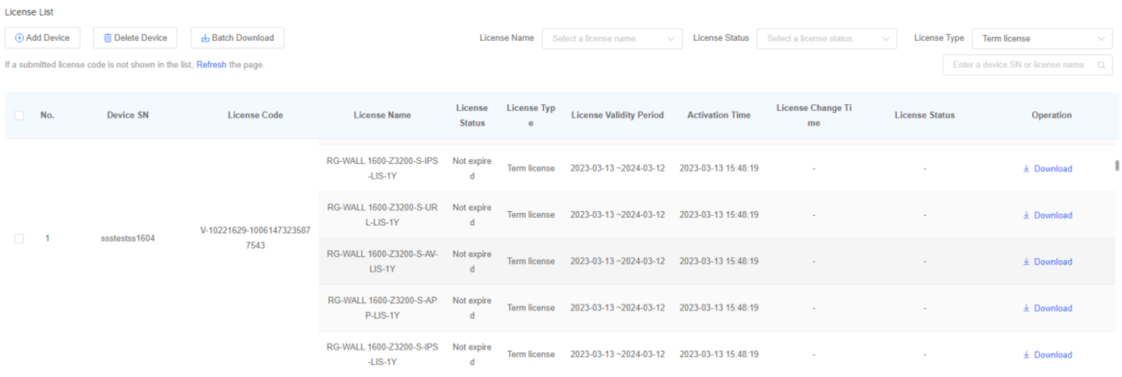
NO.1

* Device SN: Enter a device SN

* License Code: License Code

V-10221629-1005006842001 RG-WALL 1600-Z3200-S-AP P-LIS-1Y Not expired Term license 2023-03-13 ~2024-03-12 2023-03-13 16:34:06 -

c Download the license file.



License List

License Name: Select a license name.
License Status: Select a license status.
License Type: Term license

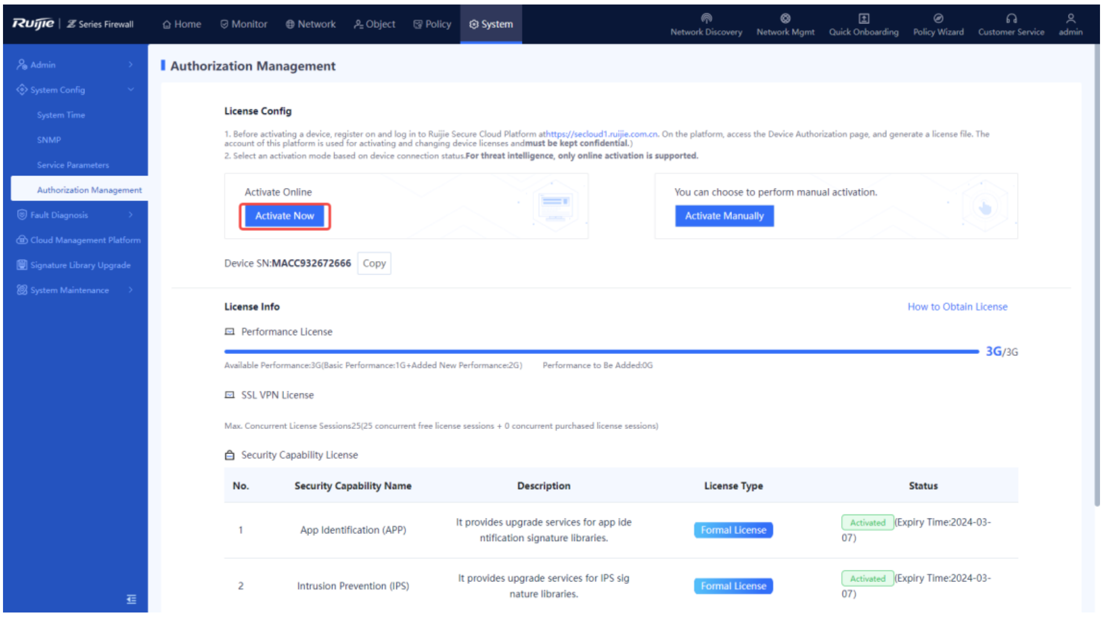
If a submitted license code is not shown in the list, Refresh the page.

Enter a device SN or license name.

	No.	Device SN	License Code	License Name	License Status	License Type	License Validity Period	Activation Time	License Change Time	License Status	Operation
□	1	ssstestss1604	V-10221629-10061473235877543	RG-WALL 1600-Z3200-S-IPS-LIS-1Y	Not expired	Term license	2023-03-13 ~2024-03-12	2023-03-13 15:48:19	-	-	Download
				RG-WALL 1600-Z3200-S-URL-LIS-1Y	Not expired	Term license	2023-03-13 ~2024-03-12	2023-03-13 15:48:19	-	-	Download
				RG-WALL 1600-Z3200-S-AV-LIS-1Y	Not expired	Term license	2023-03-13 ~2024-03-12	2023-03-13 15:48:19	-	-	Download
				RG-WALL 1600-Z3200-S-APP-LIS-1Y	Not expired	Term license	2023-03-13 ~2024-03-12	2023-03-13 15:48:19	-	-	Download
				RG-WALL 1600-Z3200-S-IPS-LIS-1Y	Not expired	Term license	2023-03-13 ~2024-03-12	2023-03-13 15:48:19	-	-	Download

d Select an activation method based on network connection information of the firewall.

o Online activation



Authorization Management

License Config

1. Before activating a device, register on and log in to Ruijie Secure Cloud Platform athttps://secloud1.ruijie.com.cn. On the platform, access the Device Authorization page, and generate a license file. The account of this platform is used for activating and changing device licenses and**must be kept confidential.**)
2. Select an activation mode based on device connection status.**For threat intelligence, only online activation is supported.**

Activate Online

You can choose to perform manual activation.

Device SN:**MACC932672666** Copy

License Info

How to Obtain License

Performance License

3G/3G

Available Performance:3G(Basic Performance:1G+Added New Performance:2G) Performance to Be Added:0G

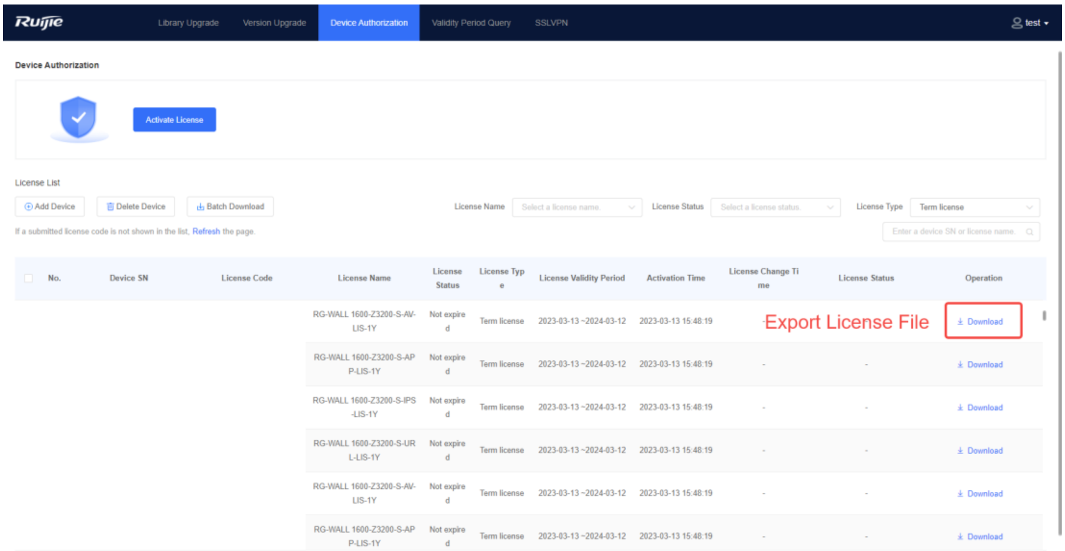
SSL VPN License

Max. Concurrent License Sessions25(25 concurrent free license sessions + 0 concurrent purchased license sessions)

Security Capability License

No.	Security Capability Name	Description	License Type	Status
1	App Identification (APP)	It provides upgrade services for app identification signature libraries.	Formal License	Activated (Expiry Time:2024-03-07)
2	Intrusion Prevention (IPS)	It provides upgrade services for IPS signature libraries.	Formal License	Activated (Expiry Time:2024-03-07)

o Offline activation



Device Authorization

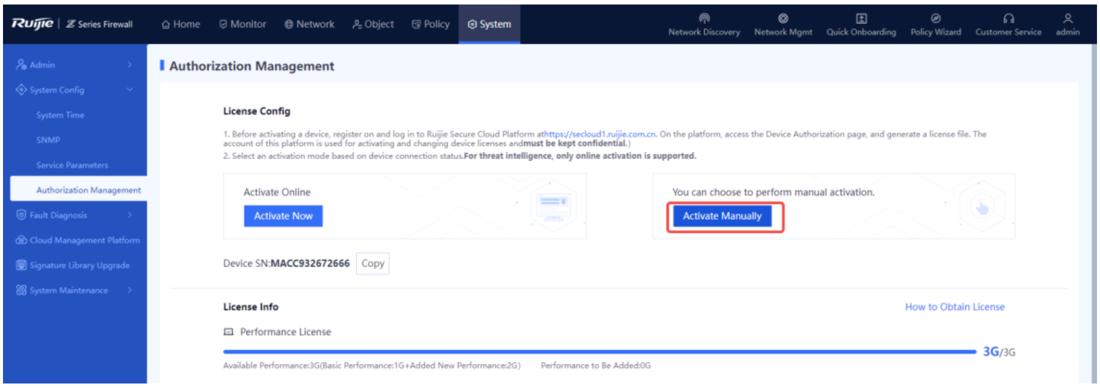
License List

License Name: Select a license name. License Status: Select a license status. License Type: Term license

Enter a device SN or license name.

If a submitted license code is not shown in the list, Refresh the page.

No.	Device SN	License Code	License Name	License Status	License Type	License Validity Period	Activation Time	License Change Time	License Status	Operation
			RG-WALL 1600-Z3200-S-AV-LIS-1Y	Not expired	Term license	2023-03-13 ~2024-03-12	2023-03-13 15:48:19	-		Download
			RG-WALL 1600-Z3200-S-APP-LIS-1Y	Not expired	Term license	2023-03-13 ~2024-03-12	2023-03-13 15:48:19	-	-	Download
			RG-WALL 1600-Z3200-S-IPS-LIS-1Y	Not expired	Term license	2023-03-13 ~2024-03-12	2023-03-13 15:48:19	-	-	Download
			RG-WALL 1600-Z3200-S-URL-LIS-1Y	Not expired	Term license	2023-03-13 ~2024-03-12	2023-03-13 15:48:19	-	-	Download
			RG-WALL 1600-Z3200-S-AV-LIS-1Y	Not expired	Term license	2023-03-13 ~2024-03-12	2023-03-13 15:48:19	-	-	Download
			RG-WALL 1600-Z3200-S-APP-LIS-1Y	Not expired	Term license	2023-03-13 ~2024-03-12	2023-03-13 15:48:19	-	-	Download



Authorization Management

License Config

1. Before activating a device, register on and log in to Ruijie Secure Cloud Platform athttps://secloud1.ruijie.com.cn. On the platform, access the Device Authorization page, and generate a license file. The account of this platform is used for activating and changing device licenses and**must be kept confidential.**)

2. Select an activation mode based on device connection status.**For threat intelligence, only online activation is supported.**

Activate Online

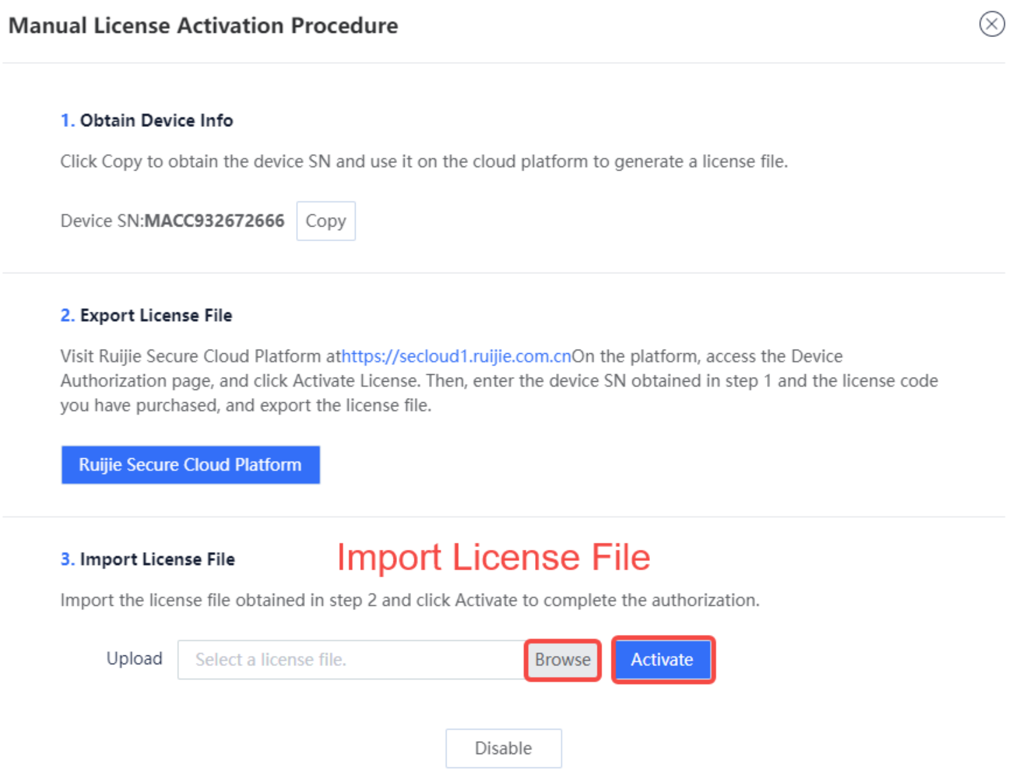
You can choose to perform manual activation.

Device SN:**MACC932672666**

License Info

Performance License 3G/3G

Available Performance:3G(Basic Performance:1G+Added New Performance:2G) Performance to Be Added:0G



Manual License Activation Procedure

1. Obtain Device Info

Click Copy to obtain the device SN and use it on the cloud platform to generate a license file.

Device SN:**MACC932672666**

2. Export License File

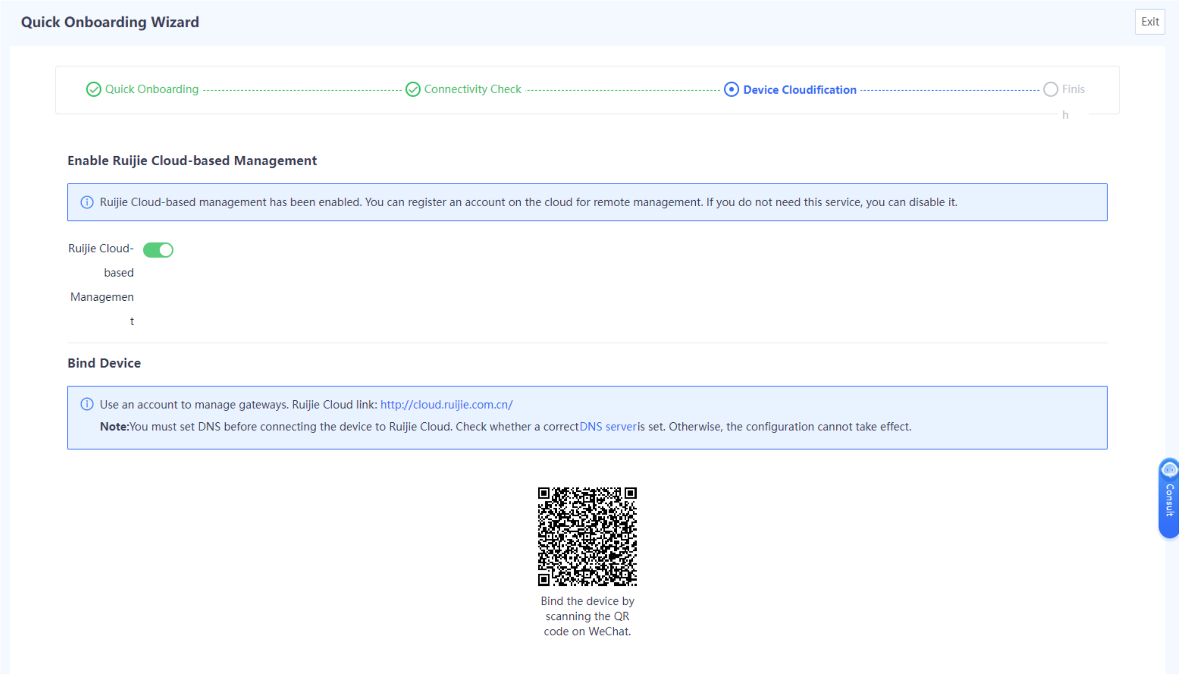
Visit Ruijie Secure Cloud Platform athttps://secloud1.ruijie.com.cnOn the platform, access the Device Authorization page, and click Activate License. Then, enter the device SN obtained in step 1 and the license code you have purchased, and export the license file.

3. Import License File

Import the license file obtained in step 2 and click Activate to complete the authorization.

Upload: Select a license file.

(4) Complete the quick onboarding configuration and bind the firewall to the Ruijie Cloud to implement remote O&M.



Quick Onboarding Wizard

Enable Ruijie Cloud-based Management

Ruijie Cloud-based management has been enabled. You can register an account on the cloud for remote management. If you do not need this service, you can disable it.

Ruijie Cloud-based Management

Bind Device

Use an account to manage gateways. Ruijie Cloud link: http://cloud.ruijie.com.cn/

Note: You must set DNS before connecting the device to Ruijie Cloud. Check whether a correctDNS serveris set. Otherwise, the configuration cannot take effect.

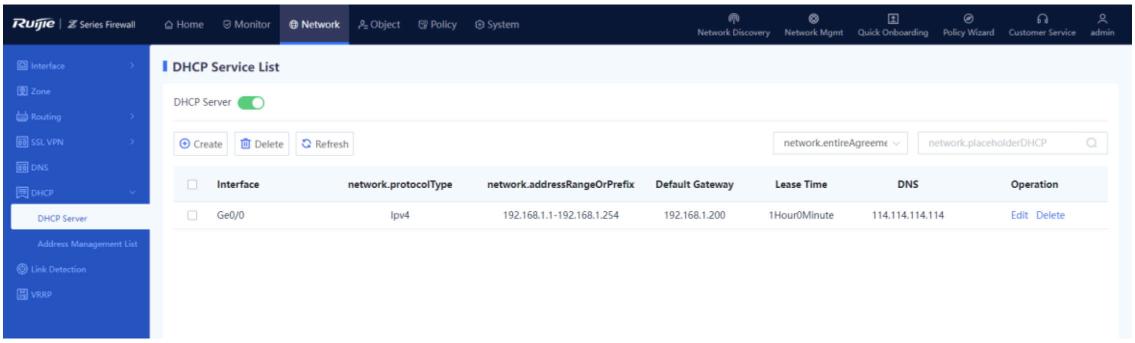
Bind the device by scanning the QR code on WeChat.

Configuration Verification

Set the IP address of the PC to 192.168.1.1/24, gateway address to 192.168.1.200, and DNS server addresses to 114.114.114.114 (primary) and 223.5.5.5 (secondary). (The address of the local DNS server must be used.) The PC can normally access the Internet.

Precautions

- By default, DHCP is disabled on the firewall interface. To allow downstream PCs to dynamically obtain IP addresses to access the Internet, choose **Network** > **DHCP** > **DHCP Server** and enable **DHCP Server**.

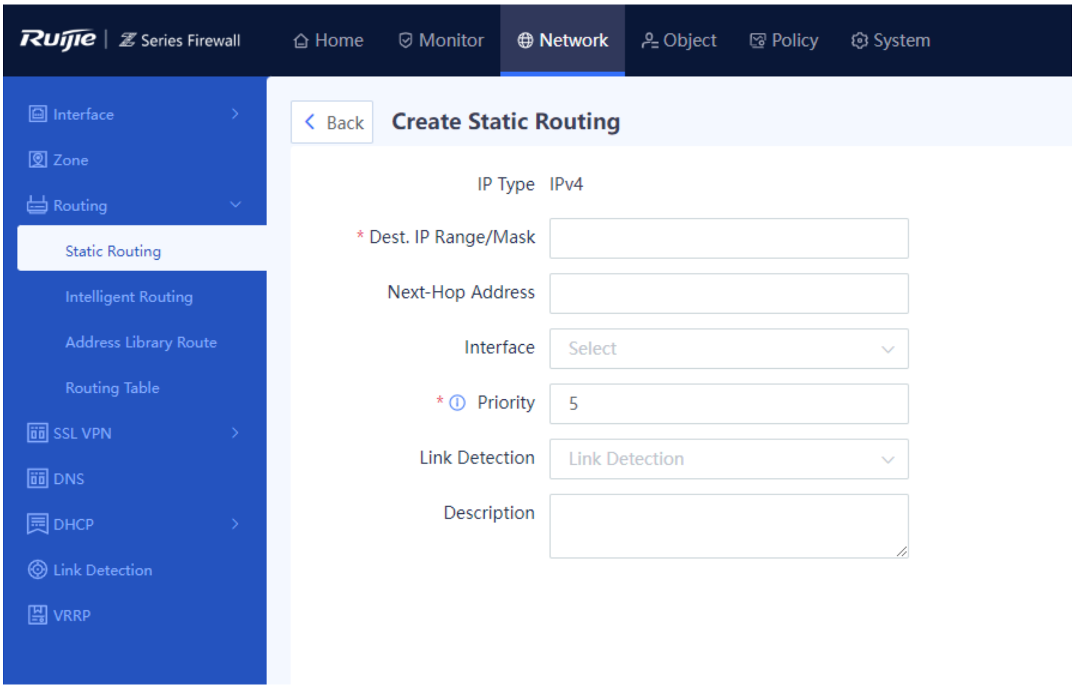


DHCP Service List

DHCP Server ●

□	Interface	network.protocolType	network.addressRangeOrPrefix	Default Gateway	Lease Time	DNS	Operation
□	Ge0/0	Ipv4	192.168.1.1-192.168.1.254	192.168.1.200	1Hour0Minute	114.114.114.114	Edit Delete

- The routing mode deployment in this section uses Layer 2 networking as an example to describe how to implement Internet access. If the downstream network of the firewall is a Layer 3 network, for example, the gateway of the downstream terminal is not the firewall, you need to add a static route to the LAN network segment based on the actual network planning. (In this static route, the destination network segment is the LAN service network segment and the next-hop address is the address of the interface connecting the downstream device to the firewall.)



Create Static Routing

IP Type IPv4

* Dest. IP Range/Mask

Next-Hop Address

Interface Select

* Priority 5

Link Detection Link Detection

Description

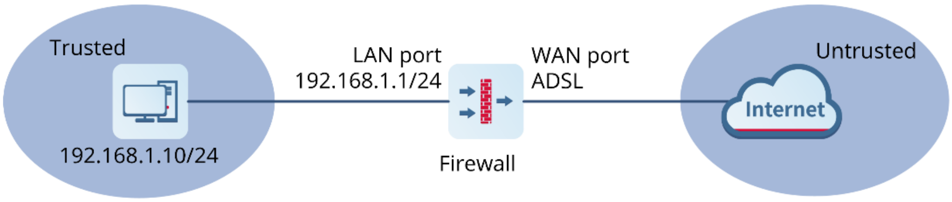
6.3.3 Single-Line Onboarding (Custom Deployment)

1. Onboarding Through Single ADSL Line

Network Requirements

The PC is located in the LAN network segment 192.168.1.0/24. The WAN interface dials up using PPPoE to obtain an IP address from the ISP. The PC wants to access the Internet through the firewall.

Network Topology



Item	Description
Ge0/6	LAN interface, which belongs to the security zone trust. The IP address is 192.168.1.1.
Ge0/7	WAN interface, which belongs to the security zone untrust. This interface dials up to obtain an IP address from the ISP. The username and password allocated by the ISP are **admin** and **ruijie@123**.

Configuration Points

Step	Description	Key Configuration
Configure interfaces.	Select two interfaces on the device and set the interface type to WAN interface and LAN interface respectively. ● WAN interface: Used to	● WAN interface: Set Connection Type to PPPoE and add the interface to the security zone untrust. The system automatically generates a default route.

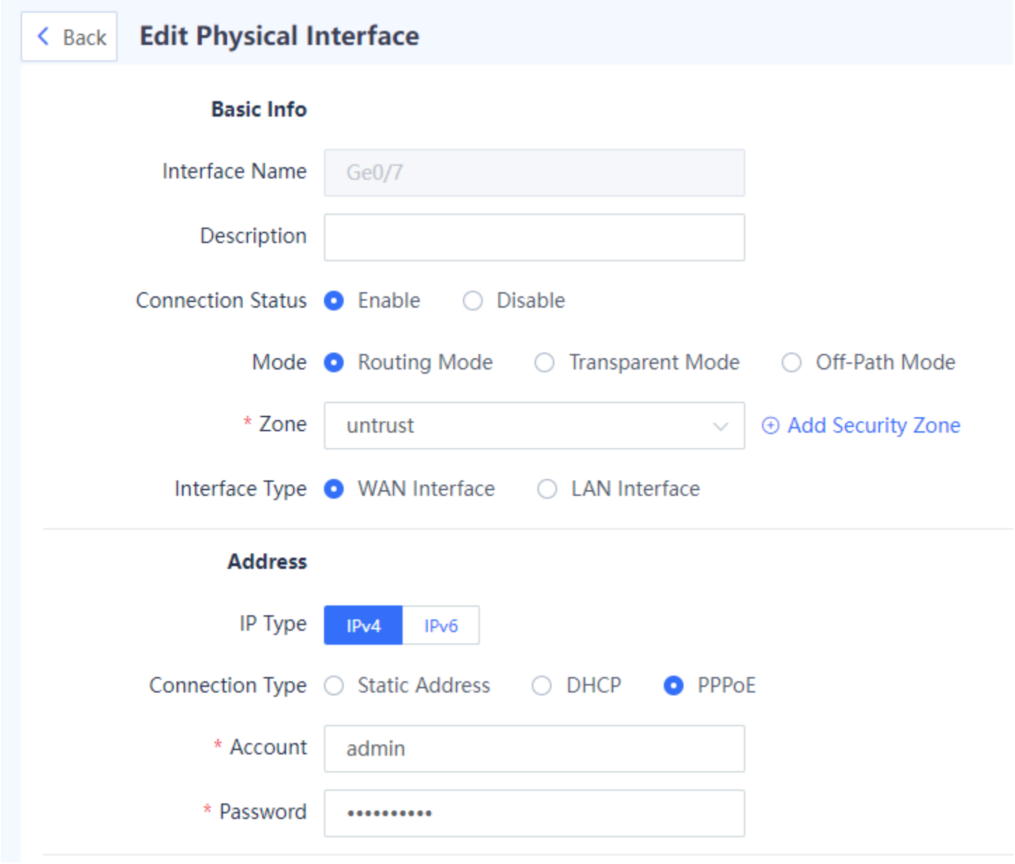
	connect to the Internet. ● LAN interface: Used to connect to the LAN.	● LAN interface: Set the IP address to 192.168.1.1/24 and add the interface to the security zone trust. You can choose to enable some management functions on the interface.
Create an address object.	To facilitate management, configure the IP address of the LAN user as an address object.	Set the name to **lan** and IP address to 192.168.1.10.
Create a security policy.	Create a policy to control traffic between the LAN interface and WAN interface.	● Src. Security Zone: trust ● Src. Address: lan ● Dest. Security Zone: untrust ● Dest. Address: any
Configure NAT.	Configure source NAT to allow the LAN user to normally access the Internet.	● Src. Security Zone: trust ● Src. Address: lan ● Dest. Security Zone: untrust ● Dest. Address: any ● Src. Address Translated to: Outbound Interface Address

Procedure

(1) Configure the WAN interface.

a Choose **Network** > **Interface** > **Physical Interface**.

b Select the physical interface to be used as the WAN interface and click **Edit**.



< Back **Edit Physical Interface**

Basic Info

Interface Name: Ge0/7

Description:

Connection Status: ● Enable ○ Disable

Mode: ● Routing Mode ○ Transparent Mode ○ Off-Path Mode

* Zone: untrust

⊕ Add Security Zone

Interface Type: ● WAN Interface ○ LAN Interface

Address

IP Type: IPv4 IPv6

Connection Type: ○ Static Address ○ DHCP ● PPPoE

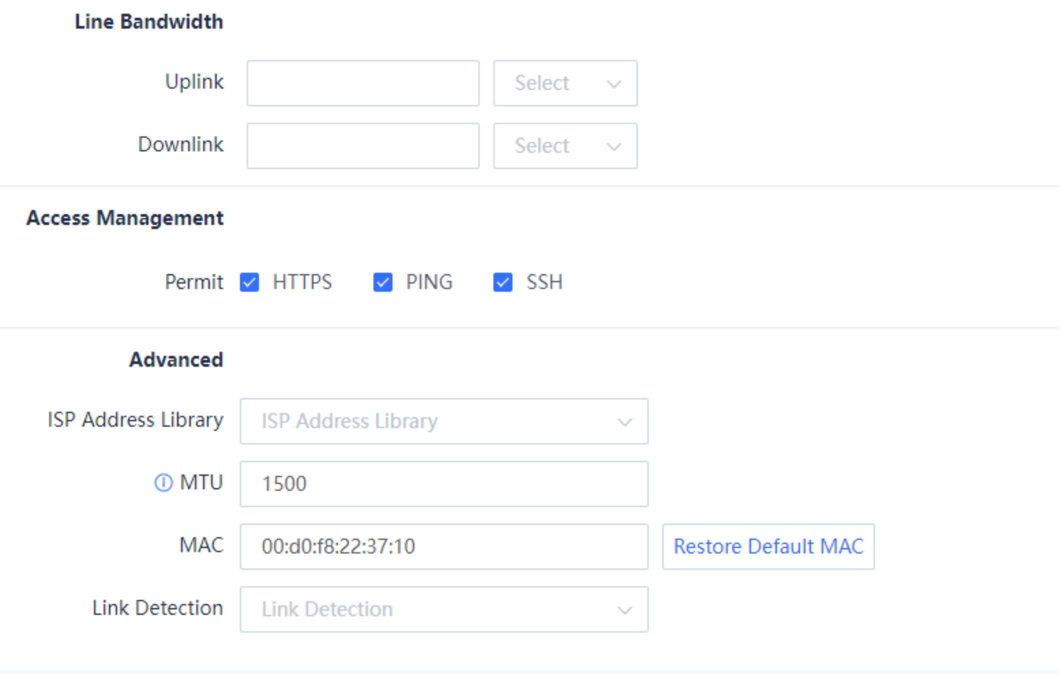
* Account: admin

* Password: ••••••••••

c Set parameters for the interface.

Item	**Description**
Mode	Routing Mode
Zone	untrust
Interface Type	WAN Interface
Connection Type	PPPoE
Account	admin
Password	ruijie@123

d Enable management functions on the interface as required. You are advised to enable the HTTPS, ping, and SSH services only on the LAN interface.



Line Bandwidth

Uplink: Select

Downlink: Select

Access Management

Permit ☑ HTTPS ☑ PING ☑ SSH

Advanced

ISP Address Library: ISP Address Library

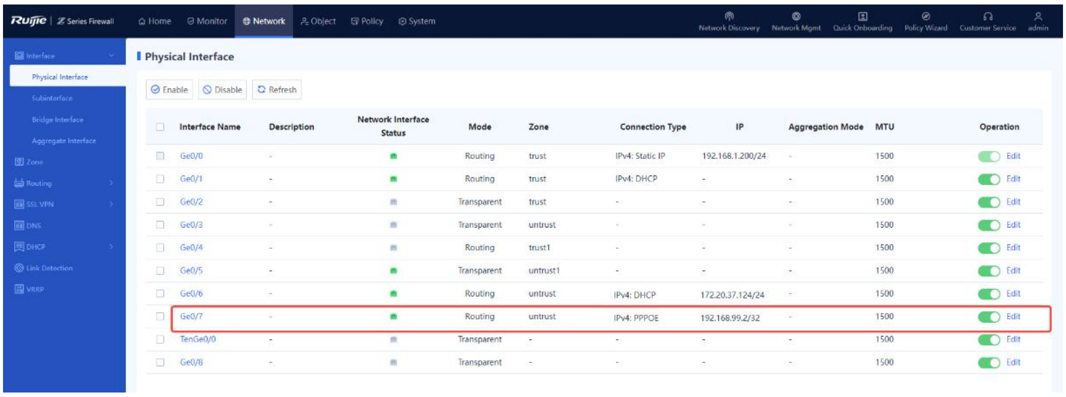
MTU: 1500

MAC: 00:d0:f8:22:37:10 Restore Default MAC

Link Detection: Link Detection

e Click **Save**.

After successful configuration, interface information marked in the red block is displayed, as shown in the following figure.



Physical Interface

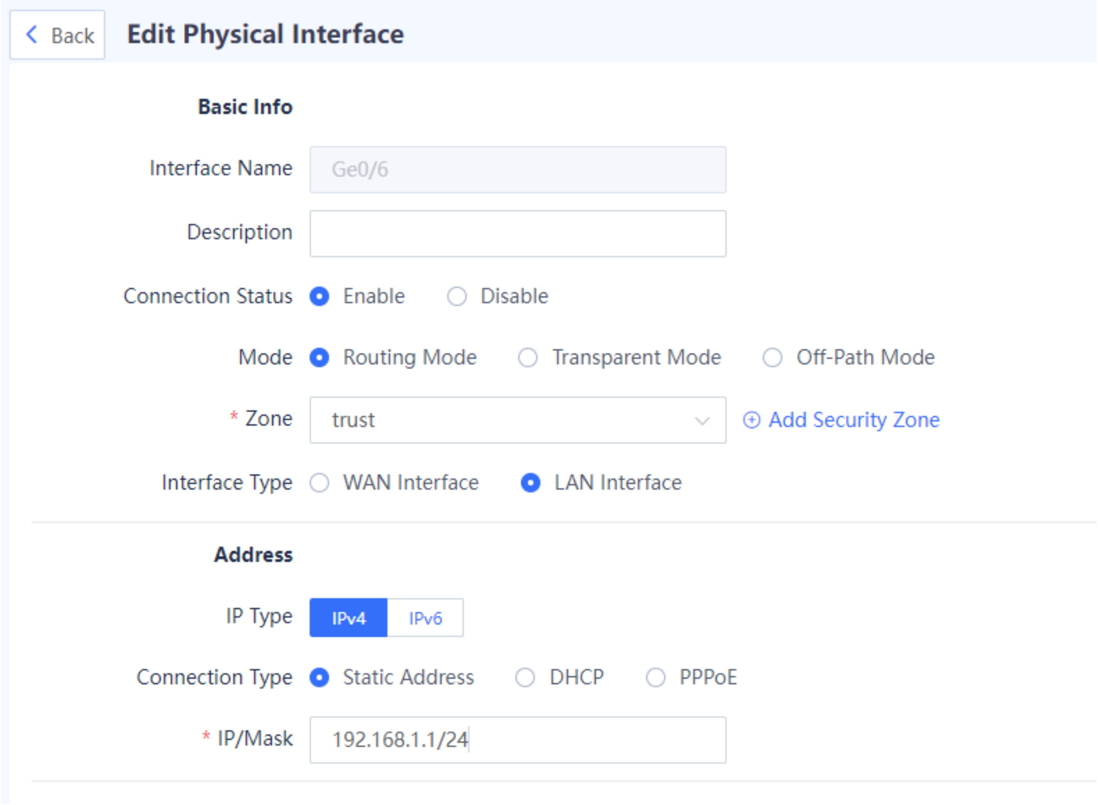
Enable Disable Refresh

□	Interface Name	Description	Network Interface Status	Mode	Zone	Connection Type	IP	Aggregation Mode	MTU	Operation
□	Ge0/0	-	●	Routing	trust	IPv4: Static IP	192.168.1.200/24	-	1500	Edit
□	Ge0/1	-	●	Routing	trust	IPv4: DHCP	-	-	1500	Edit
□	Ge0/2	-	●	Transparent	trust	-	-	-	1500	Edit
□	Ge0/3	-	●	Transparent	untrust	-	-	-	1500	Edit
□	Ge0/4	-	●	Routing	trust1	-	-	-	1500	Edit
□	Ge0/5	-	●	Transparent	untrust1	-	-	-	1500	Edit
□	Ge0/6	-	●	Routing	untrust	IPv4: DHCP	172.20.37.124/24	-	1500	Edit
□	Ge0/7	-	●	Routing	untrust	IPv4: PPPOE	192.168.99.2/32	-	1500	Edit
□	TenGe0/0	-	●	Transparent	-	-	-	-	1500	Edit
□	Ge0/8	-	●	Transparent	-	-	-	-	1500	Edit

(2) Configure the LAN interface.

a Choose **Network** > **Interface** > **Physical Interface**.

b Select the physical interface to be used as the LAN interface and click **Edit**.



< Back **Edit Physical Interface**

Basic Info

Interface Name: Ge0/6

Description:

Connection Status: ● Enable ○ Disable

Mode: ● Routing Mode ○ Transparent Mode ○ Off-Path Mode

* Zone: trust ⊕ Add Security Zone

Interface Type: ○ WAN Interface ● LAN Interface

Address

IP Type: IPv4 IPv6

Connection Type: ● Static Address ○ DHCP ○ PPPoE

* IP/Mask: 192.168.1.1/24

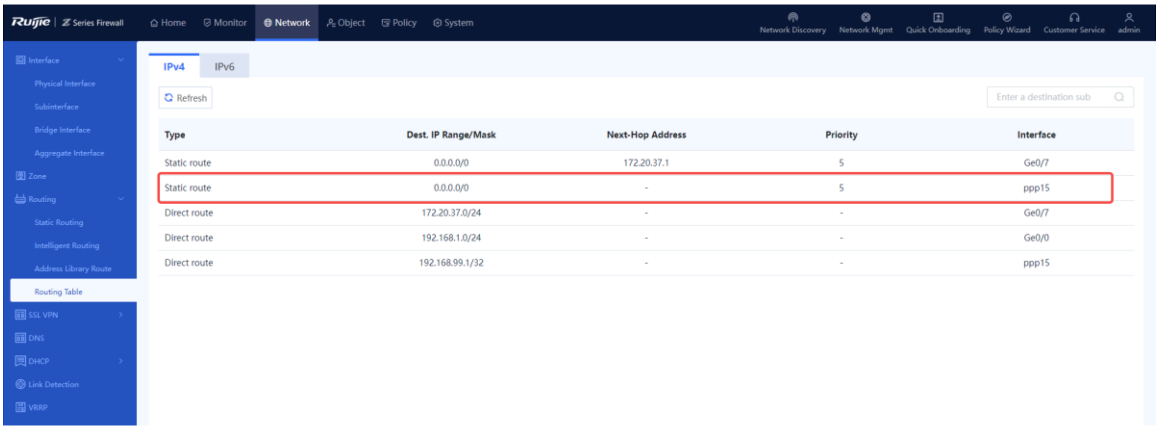
c Set parameters for the interface.

Item	Description
Mode	Routing Mode
Zone	trust
Interface Type	LAN Interface
Connection Type	Static Address
IP/Mask	192.168.1.1/24

d Enable management functions on the interface as required. You are advised to enable the HTTPS, ping, and SSH services only on the LAN interface.

e Click **Save**.

After the WAN interface and LAN interface are successfully configured, choose **Network** > **Routing** > **Routing Table**. You can find that the device automatically generates a default route.

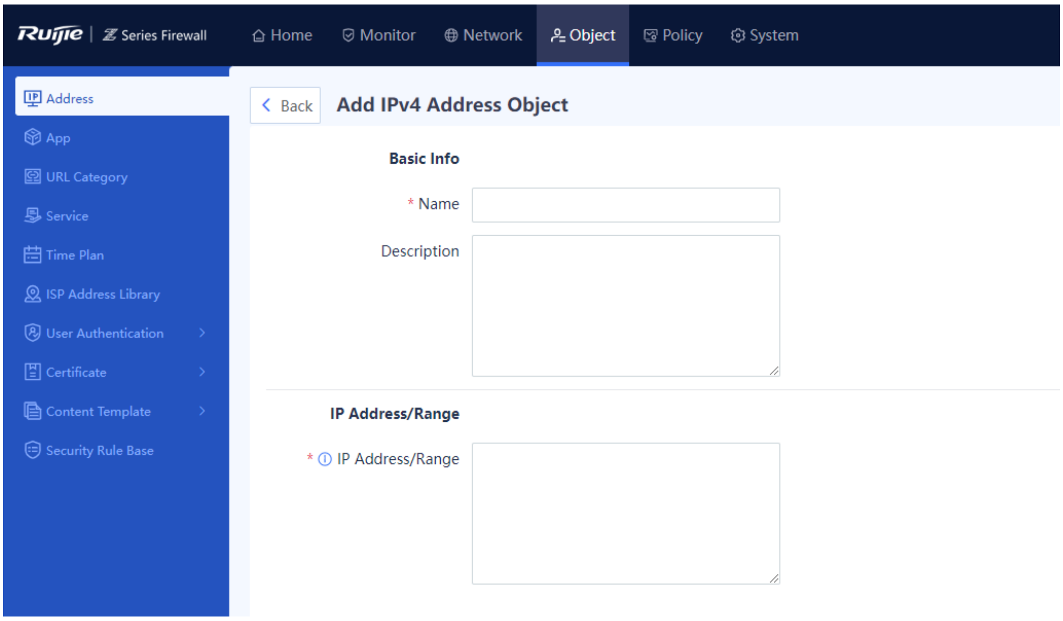


Type	Dest. IP Range/Mask	Next-Hop Address	Priority	Interface
Static route	0.0.0.0/0	172.20.37.1	5	Ge0/7
Static route	0.0.0.0/0	-	5	ppp15
Direct route	172.20.37.0/24	-	-	Ge0/7
Direct route	192.168.1.0/24	-	-	Ge0/0
Direct route	192.168.99.1/32	-	-	ppp15

(3) Configure address resources.

a Choose **Object** > **Address** > **IPv4 Address**.

b Click **Create** and add an address object with a LAN IP address.



Add IPv4 Address Object

Basic Info

* Name

Description

IP Address/Range

* IP Address/Range

c Set parameters for the address object.

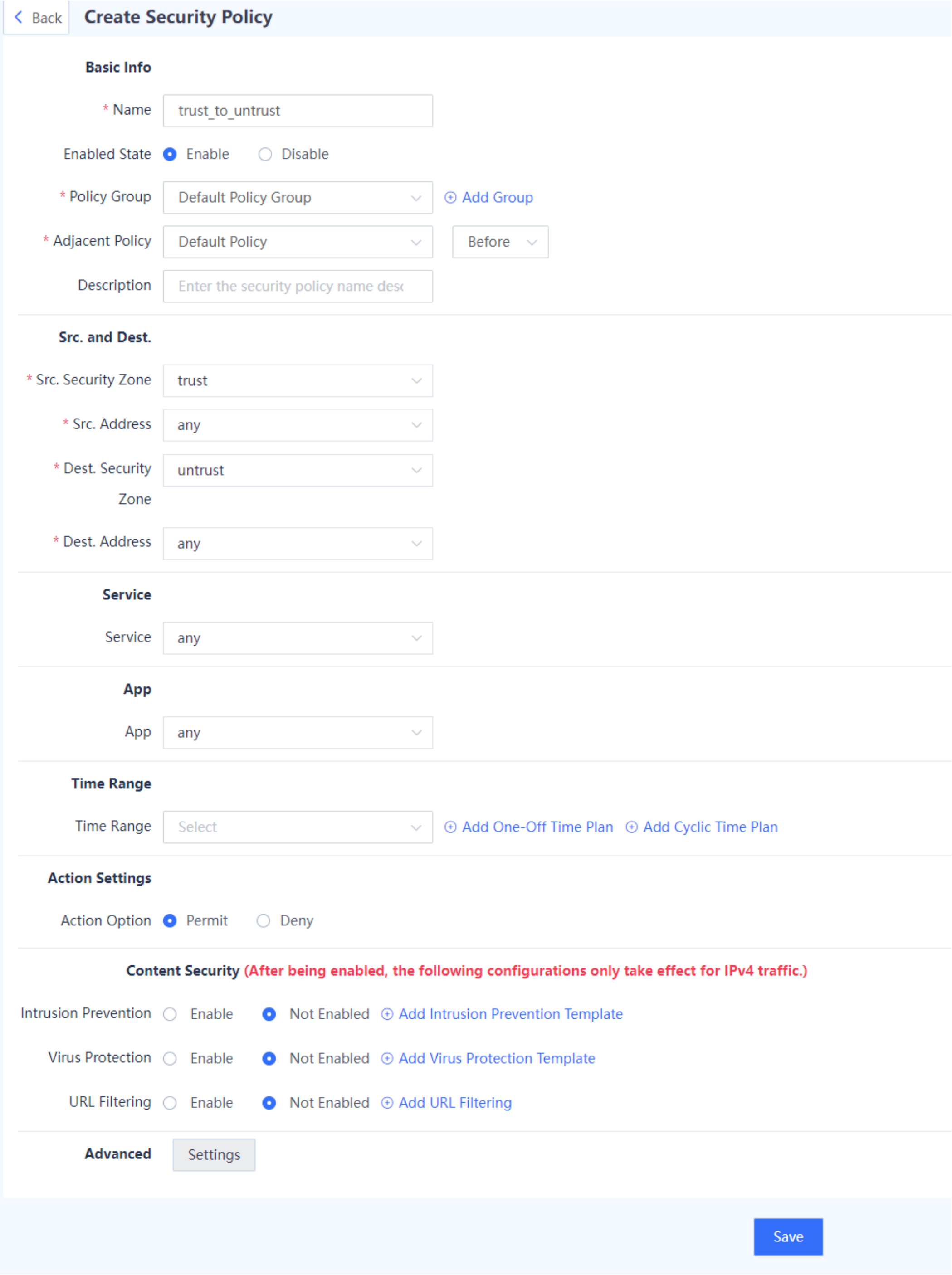
Set **Name** to **lan** and **IP Address/Range** to **192.168.1.10**.

d Click **Save**.

(4) Create a security policy.

a Choose **Policy** > **Security Policy** > **Security Policy**.

b Click **Create** and create a security policy.



< Back **Create Security Policy**

Basic Info

* Name: trust_to_untrust

Enabled State: ● Enable ○ Disable

* Policy Group: Default Policy Group ⊕ Add Group

* Adjacent Policy: Default Policy Before

Description: Enter the security policy name desc

Src. and Dest.

* Src. Security Zone: trust

* Src. Address: any

* Dest. Security Zone: untrust

* Dest. Address: any

Service

Service: any

App

App: any

Time Range

Time Range: Select ⊕ Add One-Off Time Plan ⊕ Add Cyclic Time Plan

Action Settings

Action Option: ● Permit ○ Deny

Content Security (After being enabled, the following configurations only take effect for IPv4 traffic.)

Intrusion Prevention: ○ Enable ● Not Enabled ⊕ Add Intrusion Prevention Template

Virus Protection: ○ Enable ● Not Enabled ⊕ Add Virus Protection Template

URL Filtering: ○ Enable ● Not Enabled ⊕ Add URL Filtering

Advanced Settings

Save

c Set parameters for the policy.

Item	Description
Src. Security Zone	trust

Item	Description
Src. Address	lan
Dest. Security Zone	untrust
Dest. Address	any
Service	any
App	any

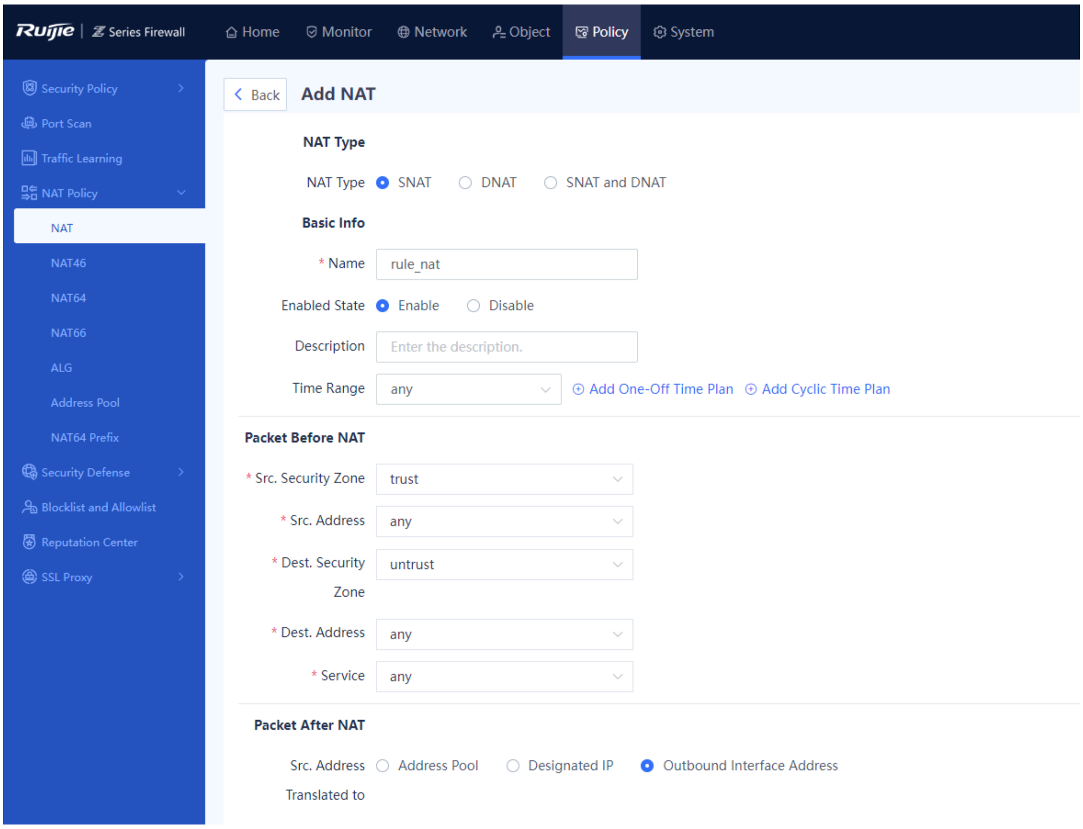
d Click **Confirm**.

(5) Configure a NAT policy.

a Choose **Policy** > **NAT Policy** > **NAT**.

b Click **Create**.

Add a source NAT policy to translate the source address of traffic sent by a device in the zone **trust** and going out from a device in the zone **untrust**.



Add NAT

NAT Type

NAT Type ● SNAT ○ DNAT ○ SNAT and DNAT

Basic Info

* Name: rule_nat

Enabled State ● Enable ○ Disable

Description: Enter the description.

Time Range: any ⊕ Add One-Off Time Plan ⊕ Add Cyclic Time Plan

Packet Before NAT

* Src. Security Zone: trust

* Src. Address: any

* Dest. Security Zone: untrust

* Dest. Address: any

* Service: any

Packet After NAT

Src. Address Translated to ○ Address Pool ○ Designated IP ● Outbound Interface Address c Set parameters for the NAT policy.

Item	Description
Src. Security Zone	trust
Src. Address	lan
Dest. Security Zone	untrust
Dest. Address	any
Src. Address Translated to	Outbound Interface Address

d Click **Save**.

Configuration Verification

Set the IP address of the PC to 192.168.1.10/24, gateway address to 192.168.1.1, and DNS server addresses to 114.114.114.114 (primary) and 223.5.5.5 (secondary). (The address of the local DNS server must be used.)

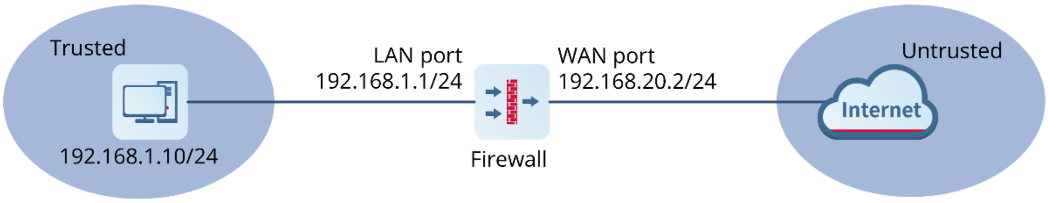
The PC can successfully ping the address 114.114.114.114.

2. Onboarding Through Static Address

Network Requirements

The computer is located in the LAN network segment 192.168.1.0/24. The WAN interface is connected to a dedicated line and specified by a static address by the ISP. The computer wants to access the Internet through the firewall.

Network Topology



Item	Description
Ge0/1	LAN interface, which belongs to the security zone **trust**. The IP address is 192.168.1.1/24.
Ge0/6	WAN interface, which belongs to the security zone **untrust**. The fixed IP address allocated by the ISP to this interface and the gateway address are 192.168.20.2/20 and 192.168.20.1, respectively.
DNS	The DNS address is 192.168.58.110, which is obtained from the ISP.

Configuration Points

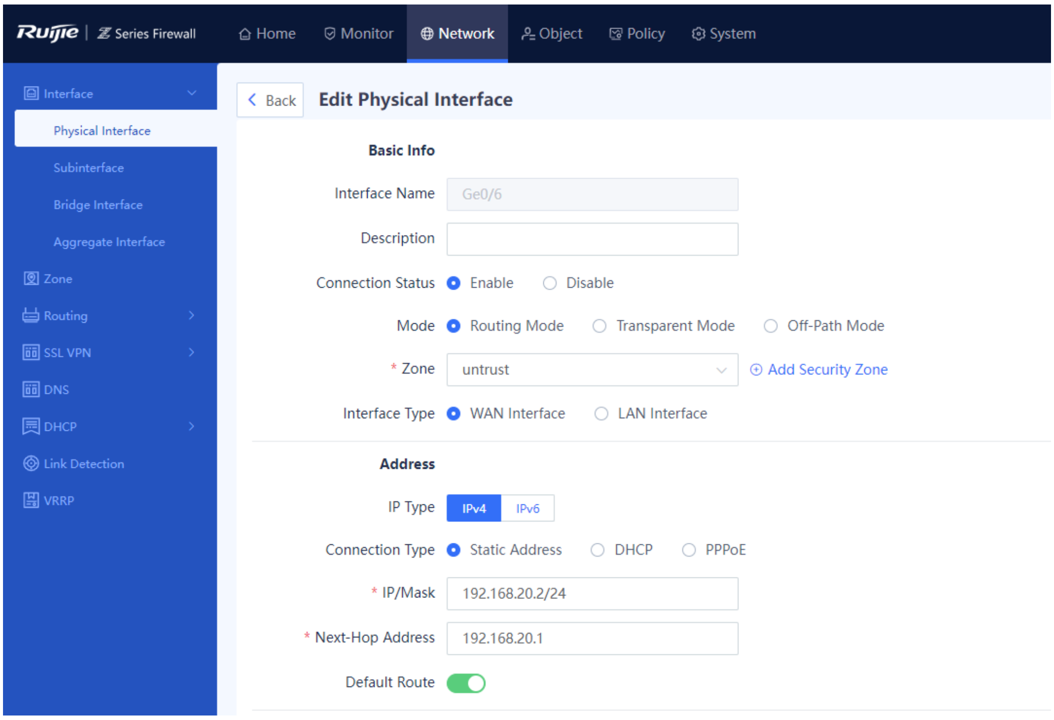
Step	**Description**	**Key Configuration**
Configure interfaces.	Select two interfaces on the device and set the interface type to WAN interface and LAN interface respectively. ● WAN interface: Used to connect to the Internet. ● LAN interface: Used to connect to the LAN.	● WAN interface: Set **Connection Type** to **Static Address** and configure the next-hop address. ● Add the interface to the security zone untrust. The system automatically generates a default route. ● LAN interface: Set the IP address to 192.168.1.1/24 and add the interface to the security zone trust. You can choose to enable some management functions on the interface.
Create an address object.	To facilitate management, configure the IP address of the LAN user as an address object.	Set the name to **lan** and IP address to 192.168.1.10.
Create a security policy.	Create a policy to control traffic between the LAN interface and WAN interface.	● Src. Security Zone: trust ● Src. Address: lan ● Dest. Security Zone: untrust ● Dest. Address: any
Configure NAT.	Configure source NAT to allow the LAN user to normally access the Internet.	● Src. Security Zone: trust ● Src. Address: lan ● Dest. Security Zone: untrust ● Dest. Address: any ● Src. Address Translated to: Outbound Interface Address

Procedure

(1) Configure the WAN interface.

a Choose **Network** > **Interface** > **Physical Interface**.

b Select the physical interface to be used as the WAN interface and click **Edit**.



Edit Physical Interface

Basic Info

Interface Name: Ge0/6

Description:

Connection Status: ● Enable ○ Disable

Mode: ● Routing Mode ○ Transparent Mode ○ Off-Path Mode

* Zone: untrust ⊕ Add Security Zone

Interface Type: ● WAN Interface ○ LAN Interface

Address

IP Type: IPv4 IPv6

Connection Type: ● Static Address ○ DHCP ○ PPPoE

* IP/Mask: 192.168.20.2/24

* Next-Hop Address: 192.168.20.1

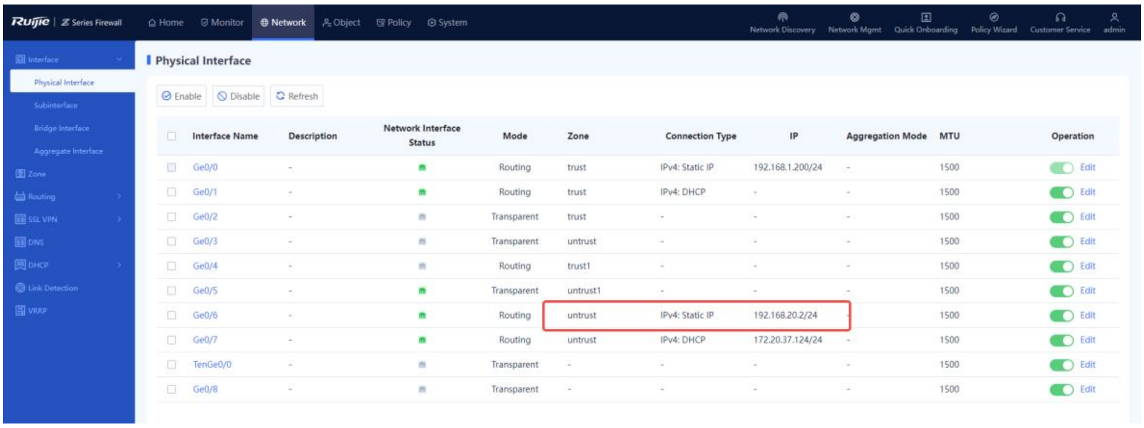
Default Route: on

c Set parameters for the interface.

Item	Description
Mode	Routing Mode
Zone	untrust
Interface Type	WAN Interface
Connection Type	Static Address
IP/Mask	192.168.20.2/24
Next-Hop Address	192.168.20.1

d Click **Save**.

After successful configuration, interface information marked in the red block is displayed, as shown in the following figure.



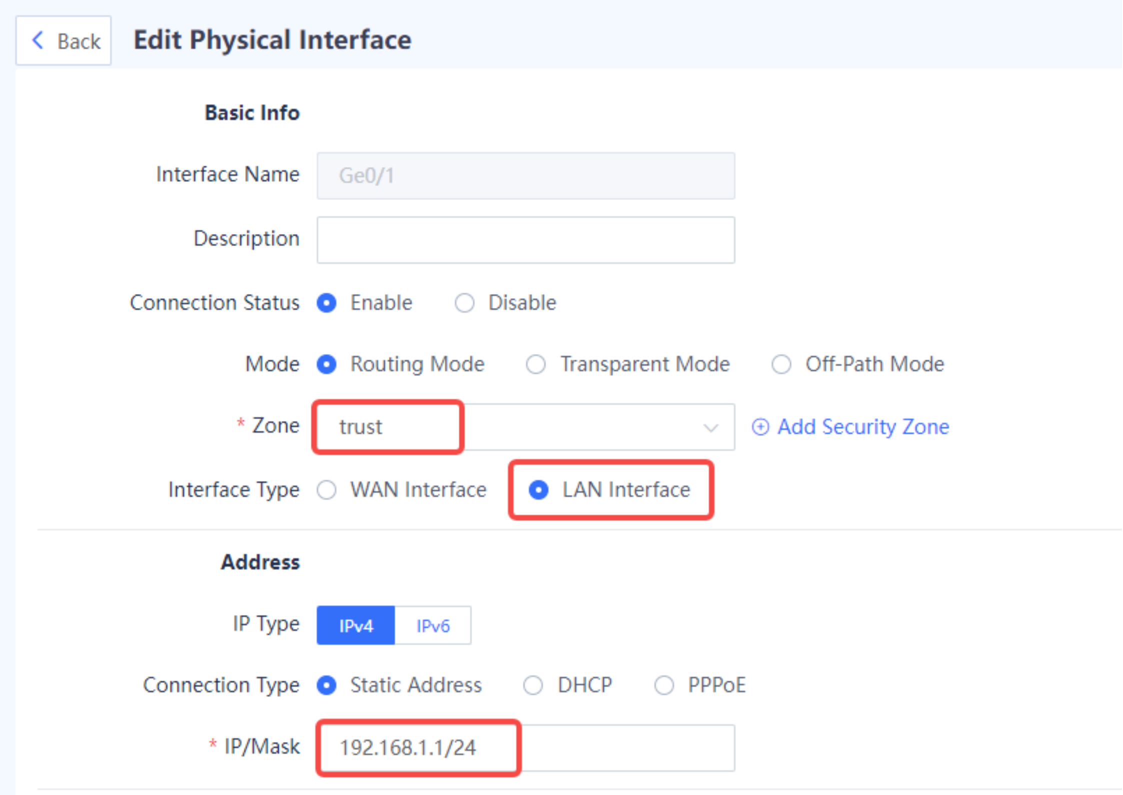
Physical Interface

Interface Name	Description	Network Interface Status	Mode	Zone	Connection Type	IP	Aggregation Mode	MTU	Operation
Ge0/0	-	●	Routing	trust	IPv4: Static IP	192.168.1.200/24	-	1500	Edit
Ge0/1	-	●	Routing	trust	IPv4: DHCP	-	-	1500	Edit
Ge0/2	-	○	Transparent	trust	-	-	-	1500	Edit
Ge0/3	-	○	Transparent	untrust	-	-	-	1500	Edit
Ge0/4	-	○	Routing	trust1	-	-	-	1500	Edit
Ge0/5	-	●	Transparent	untrust1	-	-	-	1500	Edit
Ge0/6	-	●	Routing	untrust	IPv4: Static IP	192.168.20.2/24	-	1500	Edit
Ge0/7	-	●	Routing	untrust	IPv4: DHCP	172.20.37.124/24	-	1500	Edit
TenGe0/0	-	○	Transparent	-	-	-	-	1500	Edit
Ge0/8	-	○	Transparent	-	-	-	-	1500	Edit

(2) Configure the LAN interface.

a Choose **Network** > **Interface** > **Physical Interface**.

b Select the physical interface to be used as the LAN interface and click **Edit**.



Edit Physical Interface

Basic Info

Interface Name: Ge0/1

Description:

Connection Status: ● Enable ○ Disable

Mode: ● Routing Mode ○ Transparent Mode ○ Off-Path Mode

* Zone: trust

Interface Type: ○ WAN Interface ● LAN Interface

Address

IP Type: IPv4 IPv6

Connection Type: ● Static Address ○ DHCP ○ PPPoE

* IP/Mask: 192.168.1.1/24

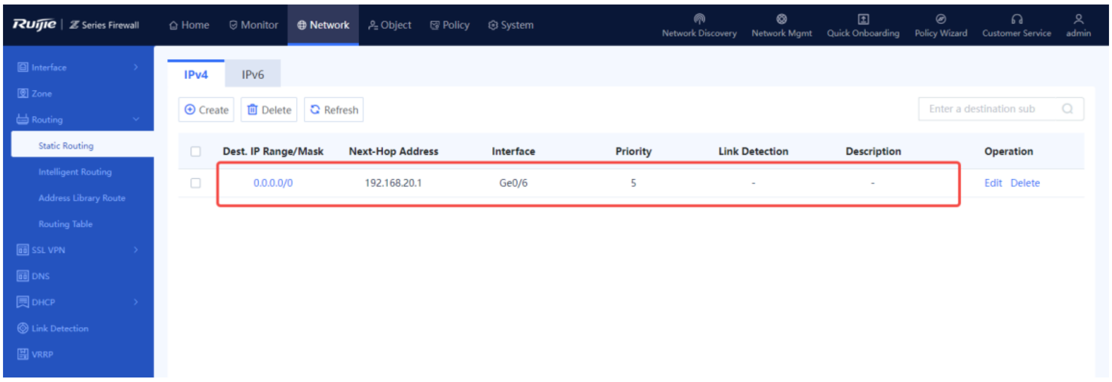
c Set parameters for the interface.

Item	Description
Mode	Routing Mode
Zone	trust
Interface Type	LAN Interface
Connection Type	Static Address
IP/Mask	192.168.1.1/24

d Enable management functions on the interface as required. You are advised to enable the HTTPS, ping, and SSH services only on the LAN interface.

e Click **Save**.

After the WAN interface and LAN interface are successfully configured, choose **Network** > **Routing** > **Routing Table**. You can find that the device automatically generates a default route.

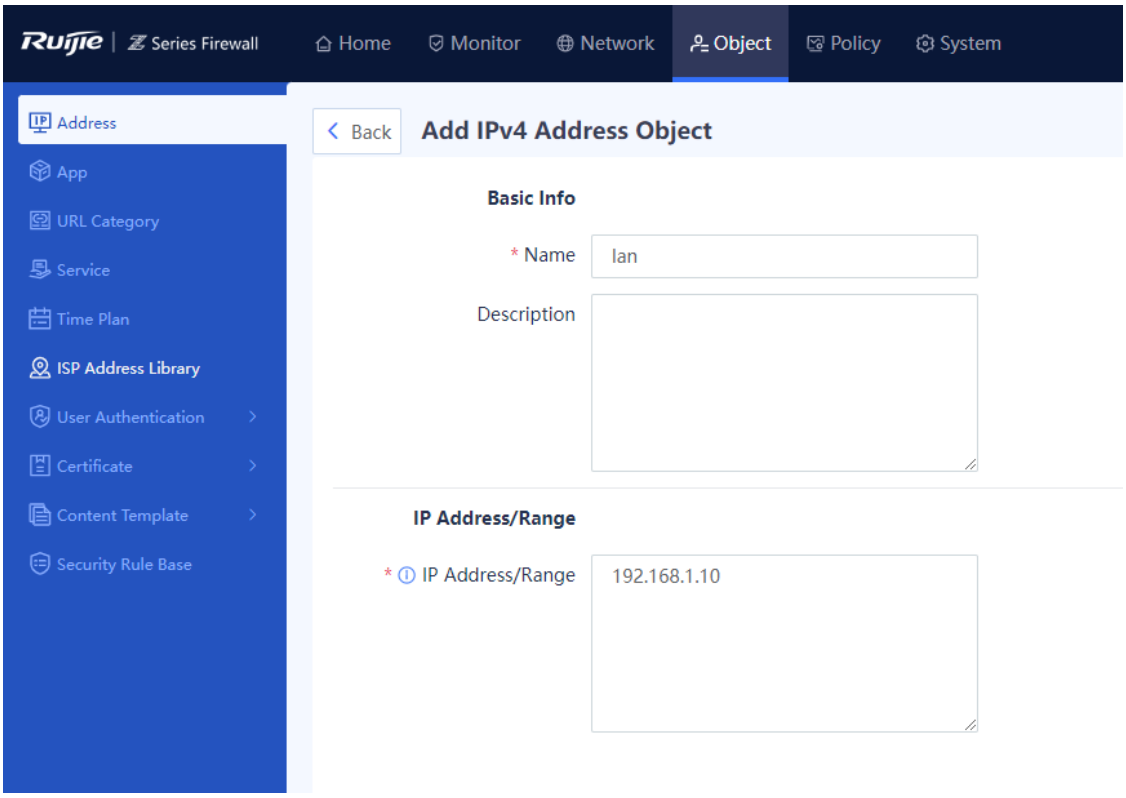


□	Dest. IP Range/Mask	Next-Hop Address	Interface	Priority	Link Detection	Description	Operation
□	0.0.0.0/0	192.168.20.1	Ge0/6	5	-	-	Edit Delete

(3) Configure address resources.

a Choose **Object** > **Address** > **IPv4 Address**.

b Click **Create** and add an address object with a LAN IP address.



Add IPv4 Address Object

Basic Info

* Name: lan

Description:

IP Address/Range

* IP Address/Range: 192.168.1.10

c Set parameters for the address object.

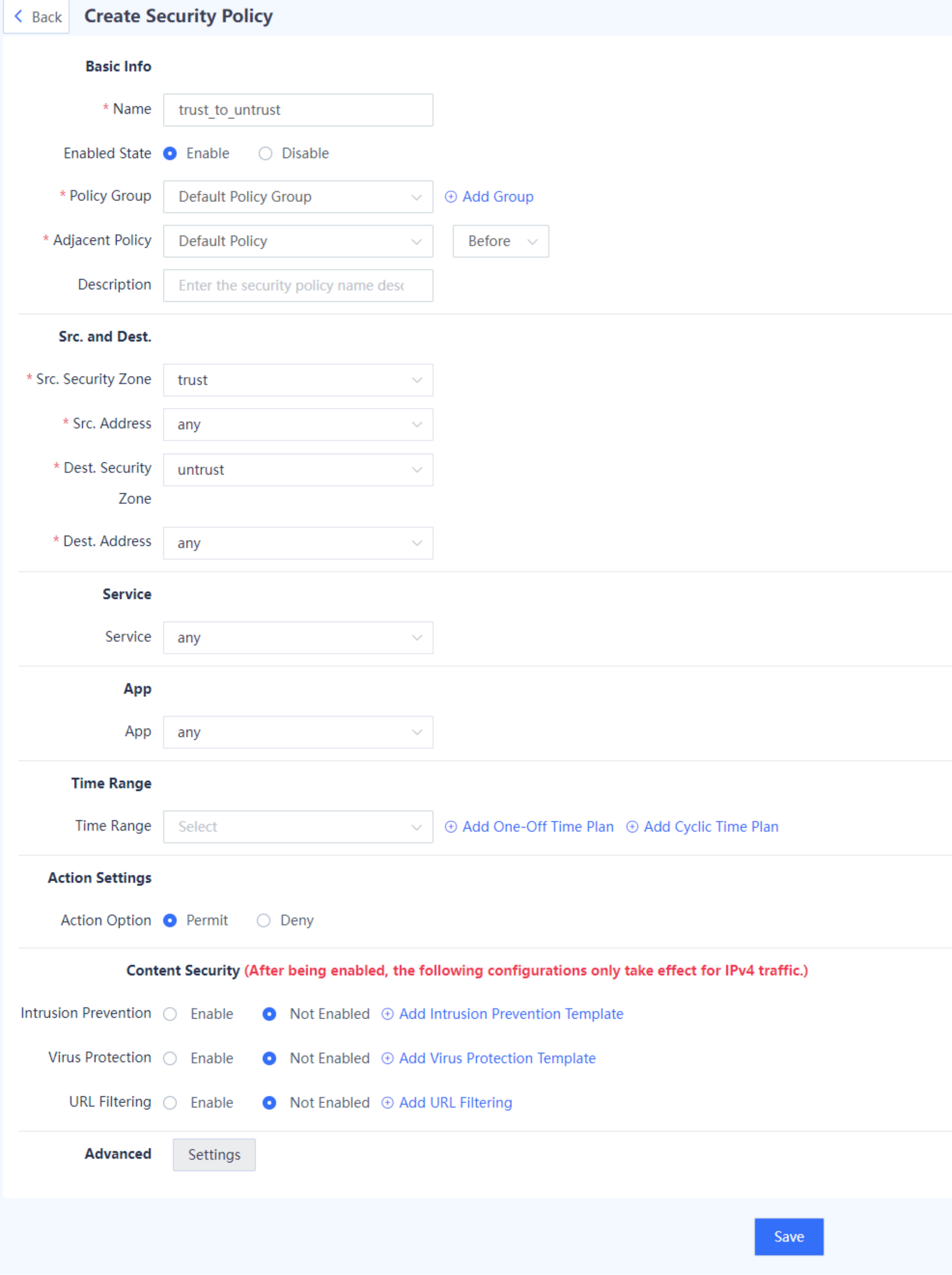
Set **Name** to **lan** and **IP Address/Range** to **192.168.1.10**.

d Click **Save**.

(4) Create a security policy.

a Choose **Policy** > **Security Policy**.

b Click **Create** and create a security policy.



< Back **Create Security Policy**

Basic Info

* Name: trust_to_untrust

Enabled State: ● Enable ○ Disable

* Policy Group: Default Policy Group ⊕ Add Group

* Adjacent Policy: Default Policy, Before

Description: Enter the security policy name desc

Src. and Dest.

* Src. Security Zone: trust

* Src. Address: any

* Dest. Security Zone: untrust

* Dest. Address: any

Service

Service: any

App

App: any

Time Range

Time Range: Select ⊕ Add One-Off Time Plan ⊕ Add Cyclic Time Plan

Action Settings

Action Option: ● Permit ○ Deny

Content Security (After being enabled, the following configurations only take effect for IPv4 traffic.)

Intrusion Prevention: ○ Enable ● Not Enabled ⊕ Add Intrusion Prevention Template

Virus Protection: ○ Enable ● Not Enabled ⊕ Add Virus Protection Template

URL Filtering: ○ Enable ● Not Enabled ⊕ Add URL Filtering

Advanced Settings

c Set parameters for the security policy.

Item	**Description**
Src. Security Zone	trust
Src. Address	lan

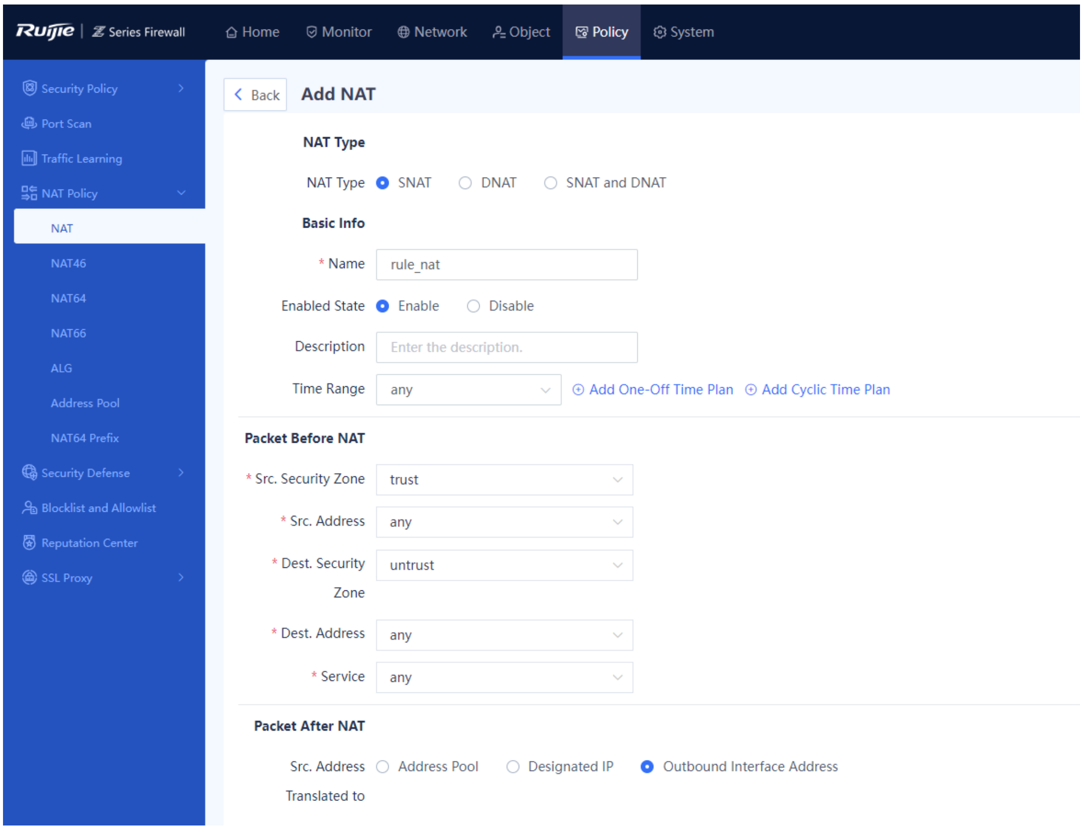
Item	Description
Dest. Security Zone	untrust
Dest. Address	any
Service	any
App	any

d Click **Save**.

(5) Configure a NAT policy.

a Choose **Policy** > **NAT Policy** > **NAT**.

b Click **Create** and add a source NAT policy to translate the source address of traffic sent by a device in the zone **trust** and going out from a device in the zone **untrust**.



Add NAT

NAT Type

NAT Type ● SNAT ○ DNAT ○ SNAT and DNAT

Basic Info

* Name: rule_nat

Enabled State ● Enable ○ Disable

Description: Enter the description.

Time Range: any

Packet Before NAT

* Src. Security Zone: trust

* Src. Address: any

* Dest. Security Zone: untrust

* Dest. Address: any

* Service: any

Packet After NAT

Src. Address Translated to ○ Address Pool ○ Designated IP ● Outbound Interface Address

c Set parameters for the NAT policy.

Item	Description
Src. Security Zone	trust
Src. Address	lan
Dest. Security Zone	untrust
Dest. Address	any
Src. Address Translated to	Outbound Interface Address

d Click **Save**.

Configuration Verification

Set the IP address of the PC to 192.168.1.10/24, gateway address to 192.168.1.1, and DNS server addresses to 114.114.114.114 (primary) and 223.5.5.5 (secondary). (The address of the local DNS server must be used.)

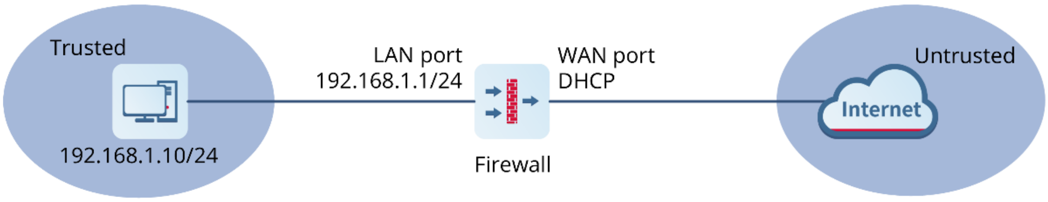
The PC can successfully ping the address 114.114.114.114.

3. Onboarding Through DHCP

Network Requirements

The PC is located in the LAN network segment 192.168.1.0/24. The WAN interface is connected to a dedicated line and specified by a static address by the ISP. The PC wants to access the Internet through the firewall.

Network Topology



Item	Description
Ge0/6	LAN interface, which belongs to the security zone trust. The IP address is 192.168.1.1/24.
Ge0/7	WAN interface, which belongs to the security zone untrust. This interface obtains an IP address through DHCP.

Configuration Points

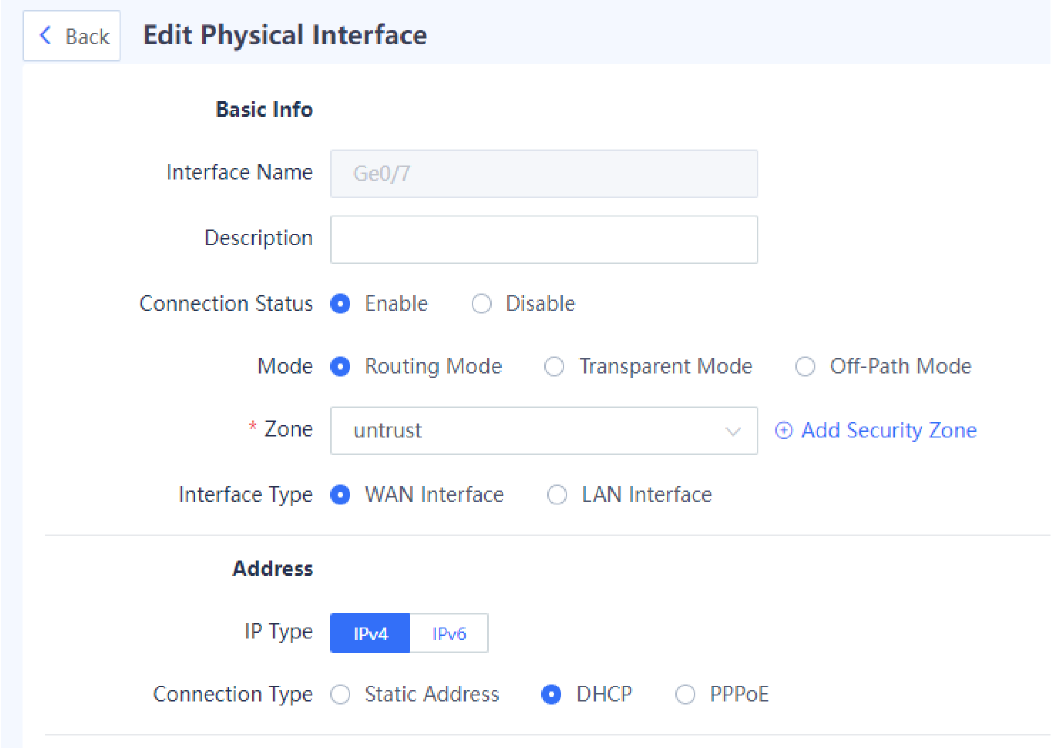
Step	Description	Key Configuration
Configure interfaces.	Select two interfaces on the device and set the interface type to WAN interface and LAN interface respectively. ● WAN interface: Used to connect to the Internet. ● LAN interface: Used to connect to the LAN.	● WAN interface: Set **Connection Type** to **DHCP**. Add the interface to the security zone untrust. After the WAN interface obtains an IP address through DHCP, the system automatically generates a default route. ● LAN interface: Set the IP address to 192.168.1.1/24 and add the interface to the security zone trust. You can choose to enable some management functions on the interface.
Create an address object.	To facilitate management, configure the IP address of the LAN user as an address object.	Set the name to **lan** and IP address to 192.168.1.10.
Create a security policy.	Create a policy to control traffic between the LAN interface and WAN interface and enable NAT.	● Src. Security Zone: trust ● Src. Address: lan ● Dest. Security Zone: untrust ● Dest. Address: any

Procedure

(1) Configure the WAN interface.

a Choose **Network** > **Interface** > **Physical Interface**.

b Select the physical interface to be used as the WAN interface and click **Edit**.



< Back **Edit Physical Interface**

Basic Info

Interface Name: Ge0/7

Description:

Connection Status ● Enable ○ Disable

Mode ● Routing Mode ○ Transparent Mode ○ Off-Path Mode

* Zone: untrust ⊕ Add Security Zone

Interface Type ● WAN Interface ○ LAN Interface

Address

IP Type: IPv4 | IPv6

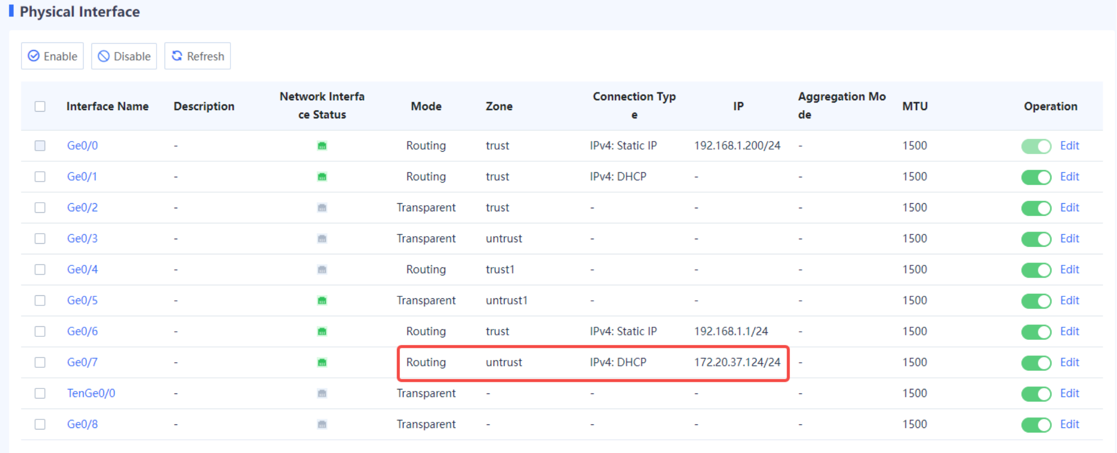
Connection Type ○ Static Address ● DHCP ○ PPPoE

c Set parameters for the interface.

Item	**Description**
Mode	Routing Mode
Zone	untrust
Interface Type	WAN Interface
Connection Type	DHCP

d Click **Save**.

After successful configuration, interface information marked in the red block is displayed, as shown in the following figure.



Physical Interface

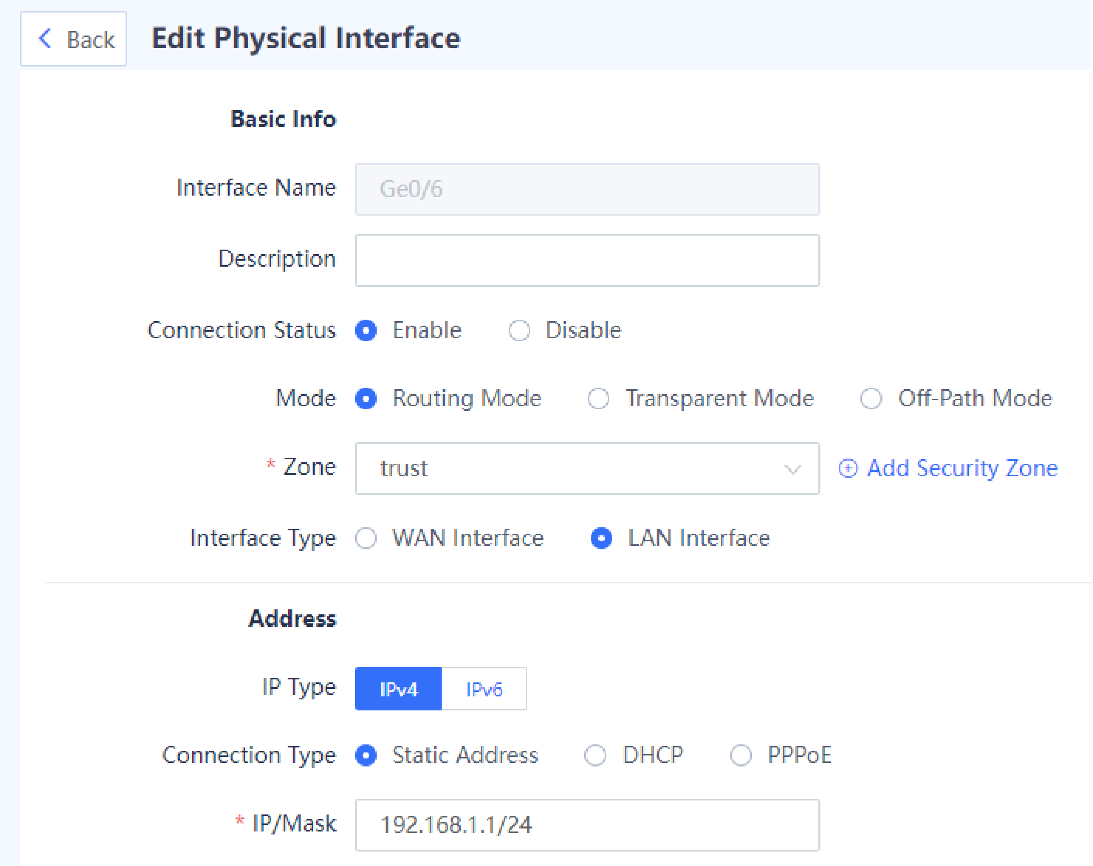
Enable Disable Refresh

□	Interface Name	Description	Network Interface Status	Mode	Zone	Connection Type	IP	Aggregation Mode	MTU	Operation
□	Ge0/0	-	🟩	Routing	trust	IPv4: Static IP	192.168.1.200/24	-	1500	Edit
□	Ge0/1	-	🟩	Routing	trust	IPv4: DHCP	-	-	1500	Edit
□	Ge0/2	-	▨	Transparent	trust	-	-	-	1500	Edit
□	Ge0/3	-	▨	Transparent	untrust	-	-	-	1500	Edit
□	Ge0/4	-	▨	Routing	trust1	-	-	-	1500	Edit
□	Ge0/5	-	🟩	Transparent	untrust1	-	-	-	1500	Edit
□	Ge0/6	-	🟩	Routing	trust	IPv4: Static IP	192.168.1.1/24	-	1500	Edit
□	Ge0/7	-	🟩	Routing	untrust	IPv4: DHCP	172.20.37.124/24	-	1500	Edit
□	TenGe0/0	-	▨	Transparent	-	-	-	-	1500	Edit
□	Ge0/8	-	▨	Transparent	-	-	-	-	1500	Edit

(2) Configure the LAN interface.

a Choose **Network** > **Interface** > **Physical Interface**.

b Select the physical interface to be used as the LAN interface and click **Edit**.



< Back **Edit Physical Interface**

Basic Info

Interface Name: Ge0/6

Description:

Connection Status: ● Enable ○ Disable

Mode: ● Routing Mode ○ Transparent Mode ○ Off-Path Mode

* Zone: trust ⊕ Add Security Zone

Interface Type: ○ WAN Interface ● LAN Interface

Address

IP Type: IPv4 | IPv6

Connection Type: ● Static Address ○ DHCP ○ PPPoE

* IP/Mask: 192.168.1.1/24

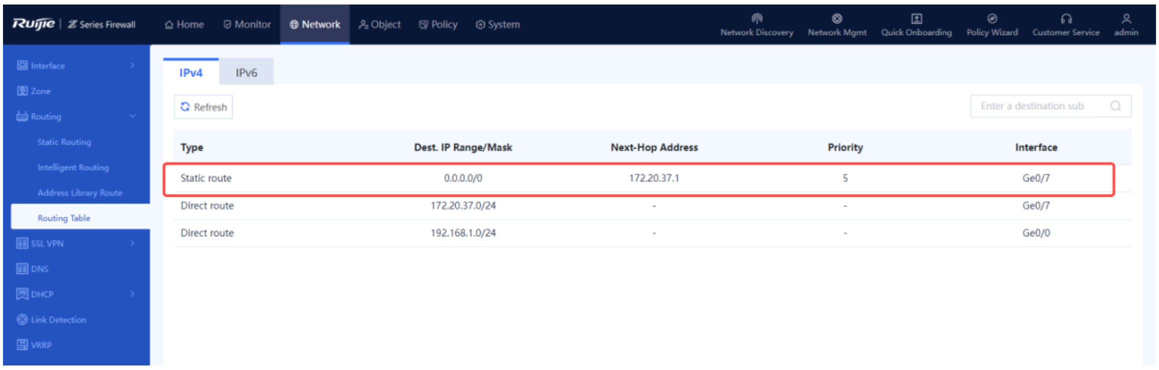
c Set parameters for the interface.

Item	Description
Mode	Routing Mode
Zone	trust
Interface Type	LAN Interface
Connection Type	Static Address
IP/Mask	192.168.1.1/24

d Enable management functions on the interface as required. You are advised to enable the HTTPS, ping, and SSH services only on the LAN interface.

e Click **Save**.

After the WAN interface and LAN interface are successfully configured, choose **Network** > **Routing** > **Routing Table**. You can find that the device automatically generates a default route.

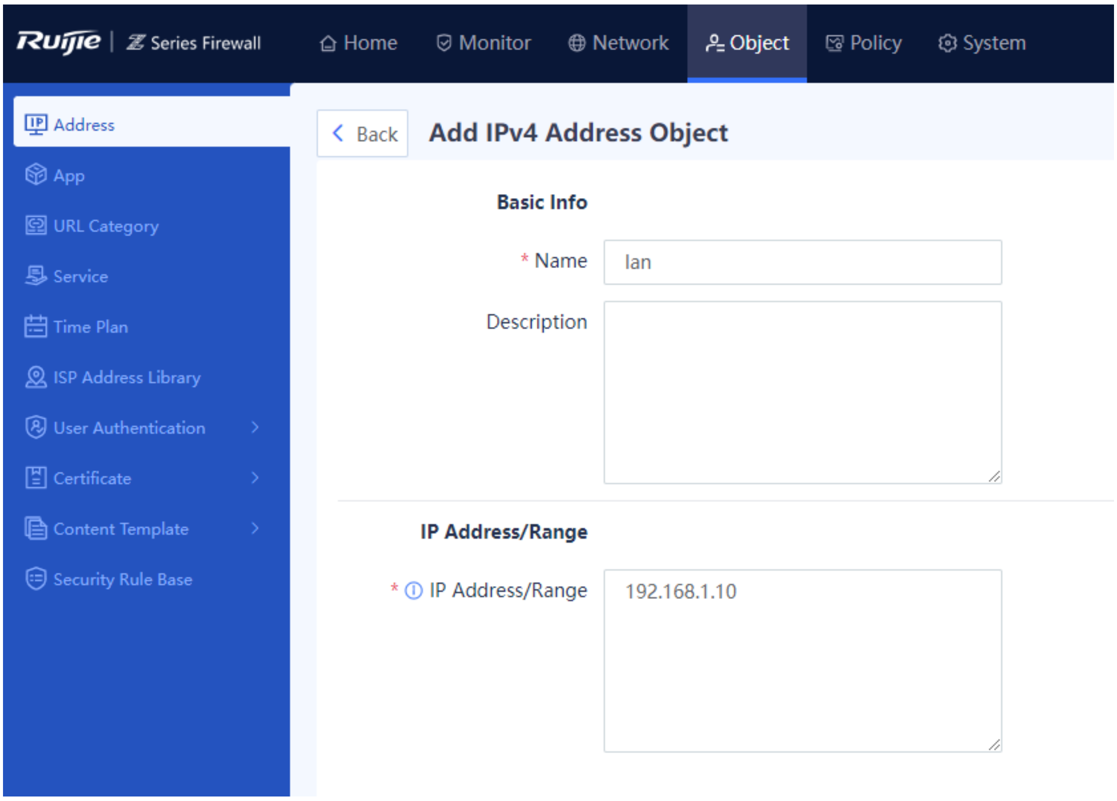


Type	Dest. IP Range/Mask	Next-Hop Address	Priority	Interface
Static route	0.0.0.0/0	172.20.37.1	5	Ge0/7
Direct route	172.20.37.0/24	-	-	Ge0/7
Direct route	192.168.1.0/24	-	-	Ge0/0

(3) Configure address resources.

a Choose **Object** > **Address** > **IPv4 Address**.

b Click **Create** and add an address object with a LAN IP address.



Add IPv4 Address Object

Basic Info

* Name: lan

Description:

IP Address/Range

* IP Address/Range: 192.168.1.10

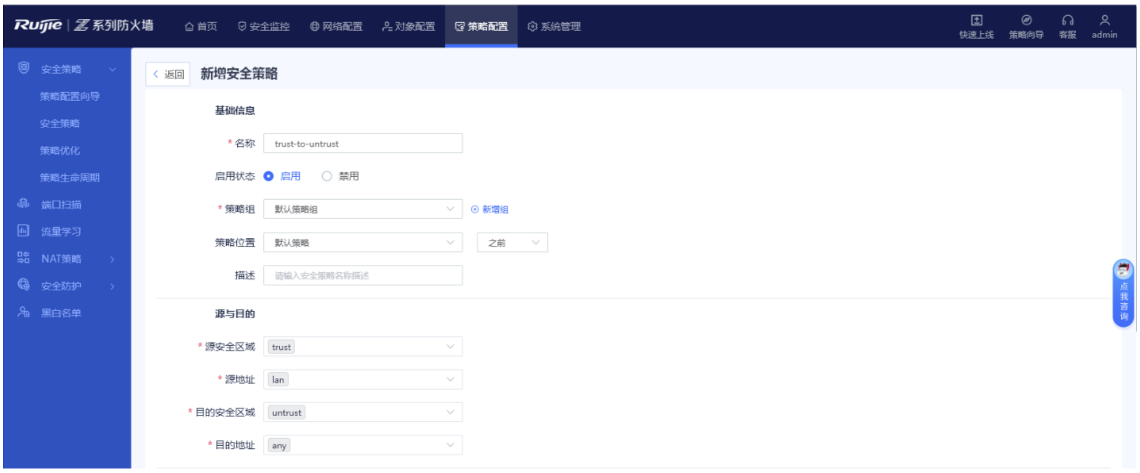
c Set **Name** to **lan** and **IP Address/Range** to **192.168.1.10**.

d Click **Save**.

(4) Create a security policy.

a Choose **Policy** > **Security Policy**.

b Click **Create**.



新增安全策略

基础信息

* 名称: trust-to-untrust

启用状态: ● 启用 ○ 禁用

* 策略组: 默认策略组

策略位置: 默认策略 之前

描述: 请输入安全策略名称描述

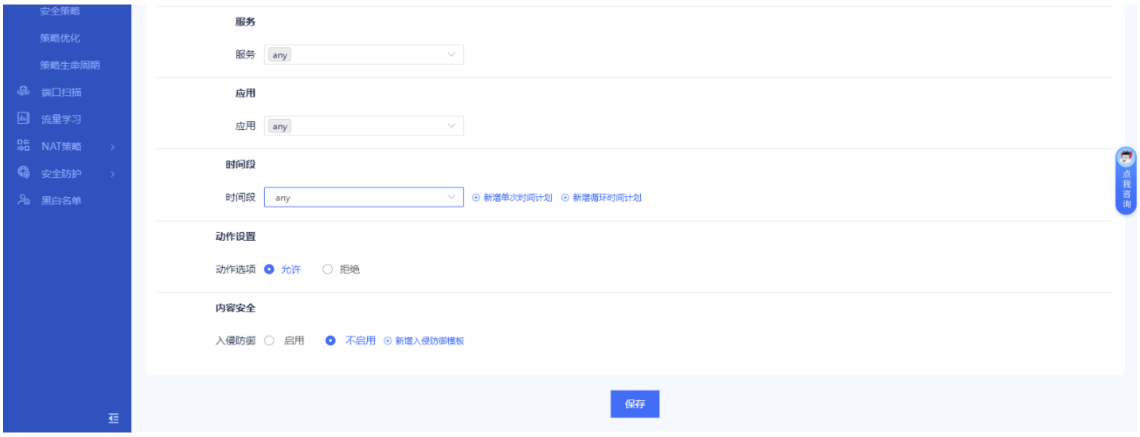
源与目的

* 源安全区域: trust

* 源地址: lan

* 目的安全区域: untrust

* 目的地址: any



服务

服务 any

应用

应用 any

时间段

时间段 any ⊕ 新增单次时间计划 ⊕ 新增循环时间计划

动作设置

动作选项 ● 允许 ○ 拒绝

内容安全

入侵防御 ○ 启用 ● 不启用 ⊕ 新增入侵防御模板

保存

c Set parameters for the security policy.

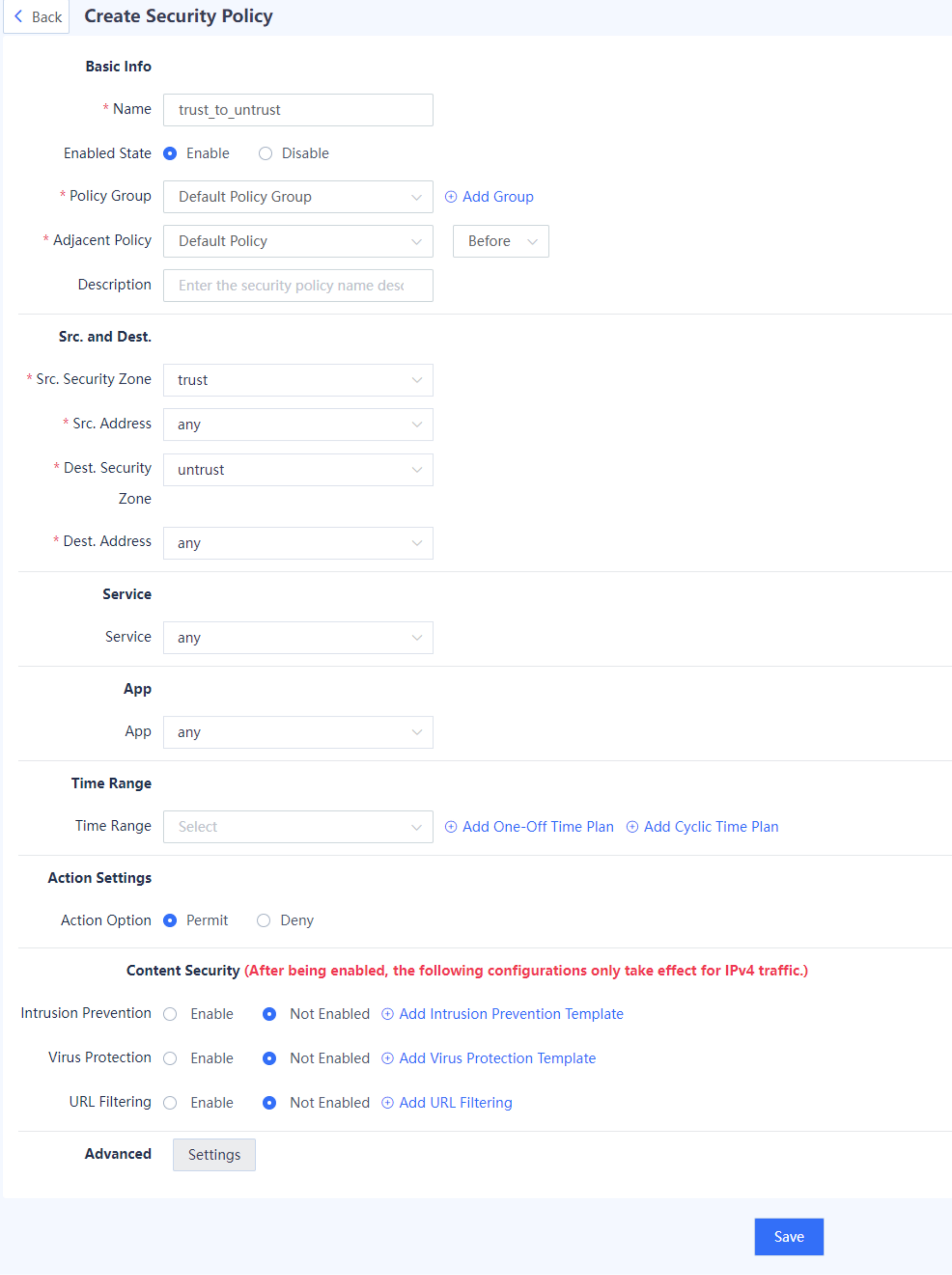
Item	**Description**
Src. Security Zone	trust
Src. Address	lan
Dest. Security Zone	untrust
Dest. Address	any
Service	any
App	any

d Click **Save**.

(5) Configure a NAT policy.

a Choose **Policy** > **NAT Policy** > **NAT**.

b Click **Create** and add a source NAT policy to translate the source address of traffic sent by a device in the zone **trust** and going out from a device in the zone **untrust**.



Create Security Policy

Basic Info

* Name: trust_to_untrust

Enabled State: ● Enable ○ Disable

* Policy Group: Default Policy Group

* Adjacent Policy: Default Policy | Before

Description: Enter the security policy name desc

Src. and Dest.

* Src. Security Zone: trust

* Src. Address: any

* Dest. Security Zone: untrust

* Dest. Address: any

Service

Service: any

App

App: any

Time Range

Time Range: Select

Action Settings

Action Option: ● Permit ○ Deny

Content Security (After being enabled, the following configurations only take effect for IPv4 traffic.)

Intrusion Prevention: ○ Enable ● Not Enabled

Virus Protection: ○ Enable ● Not Enabled

URL Filtering: ○ Enable ● Not Enabled

Advanced: Settings

c Set parameters for the NAT policy.

Item	Description
Src. Security Zone	trust
Src. Address	lan

Item	Description
Dest. Security Zone	untrust
Dest. Address	any
Src. Address Translated to	Outbound Interface Address

d Click **Save**.

Configuration Verification

Set the IP address of the PC to 192.168.1.10/24, gateway address to 192.168.1.1, and DNS server addresses to 114.114.114.114 (primary) and 223.5.5.5 (secondary). (The address of the local DNS server must be used.) The PC can successfully ping the address 114.114.114.114.

6.4 Off-Path Mode

6.4.1 Preparations

Confirm the following information before performing the configuration:

- If you deploy the firewall in off-path mode, you need to confirm the network scale and port type (GE electrical port, GE optical port, or 10GE optical port). As out-of-band management is used in off-path mode, an independent cable is required to connect the management interface to the network. You need to plan the IP address and next hop of the management interface and ensure that the management interface of the firewall can be connected to the Internet and managed on the cloud.
- If a service system is involved, check whether servers are deployed and whether the servers permit access from external users.
- Software version obtaining methods

Method	Path
Official website	https://www.ruijienetworks.com/ Choose **Support** > **Download** > **Reyee** and find the latest version of the Z-S series firewall under RG-WALL 1600-Z-S series cloud

Method	Path
	management firewalls.
Web management page of the firewall	Choose **System** > **System Maintenance** > **System Upgrade** > **Online Upgrade** > **Recommended Version** to upgrade to the latest version (recommended) in online mode.
Ruijie Cloud	After the device goes online on the Ruijie Cloud, you can remotely upgrade the device in online mode on the Ruijie Cloud (without the need for local upgrade). Choose **Monitoring** > **Device** > **Firewall**, select a device, select a version, and click **Upgrade**.

⚠ **Caution**

If the quick onboarding wizard is not used for the deployment, you must adjust the system time in advance. Otherwise, the time clock is inaccurate, which may affect reports and logs. To set the system time, choose **System** > **System Config** > **System Time**.

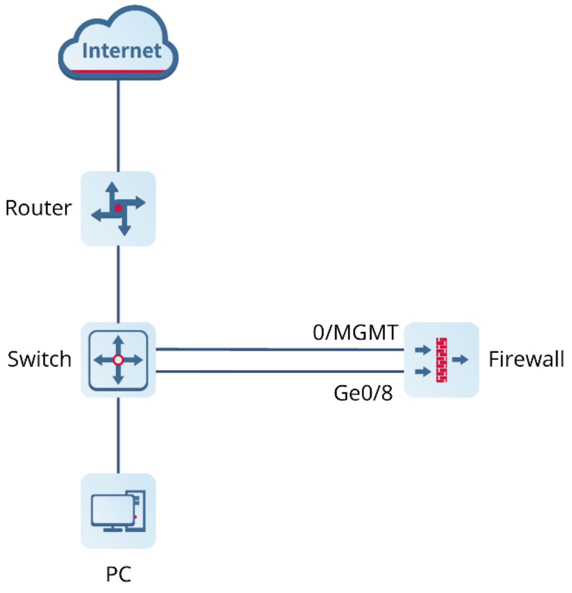
6.4.2 Deployment in Off-Path Mode (Quick Deployment)

Network Requirements

If the customer wants to use a firewall to monitor the network security information on the live network but does not want to change the physical structure of the current network, the firewall can be deployed in off-path mode. In this mode, the firewall is connected to the switch in off-path mode, and traffic of the switch is mirrored to the off-path interface for detection, providing the security protection function. This mode monitors the security of the customer network without changing the network structure and affecting data forwarding of the customer.

In off-path mode, the firewall does not forward traffic, but provides security protection for the monitored areas instead.

Network Topology



Configuration Points

(1) Implement quick onboarding. Select a deployment mode (off-path mode) and configure an off-path interface. Configure an IP address and the next hop for the management interface (0/MGMT) to ensure successful connection to the Internet.

(2) (Optional) Check the connectivity. The system automatically checks whether the firewall is connected to the Internet.

(3) (Optional) Import licenses.

a Before license activation, log in to the Ruijie Secure Cloud Platform (https://secloud-en.ruijienetworks.com/), choose **Device Authorization** > **Activate License**, and generate a license file. (The account of the Secure Cloud Platform is used to activate and change the license. Keep the account safe.)

b Select an activation method (online activation or offline activation) based on network connection information of the firewall.

(4) Complete the quick onboarding configuration.

(5) (Optional) Implement remote O&M on the cloud.

(6) Mirror the switch traffic to the off-path interface of the firewall. (Omitted)

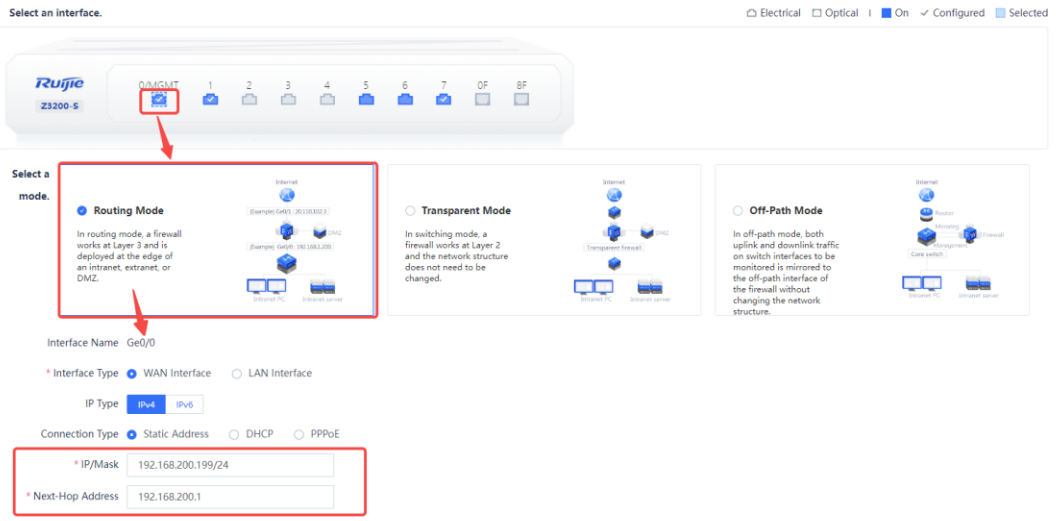
(7) Create a security policy to permit the off-path detection traffic.

Procedure

(1) Implement quick onboarding.

a Configure interfaces.

- Configure an IP address and next hop for the 0/MGMT management interface (Ge0/0) and connect it to the network using an independent network cable to ensure that the management interface can access the Internet. (The IP addresses in this example are for reference only.)



● Routing Mode

In routing mode, a firewall works at Layer 3 and is deployed at the edge of an intranet, extranet, or DMZ.

○ Transparent Mode

In switching mode, a firewall works at Layer 2 and the network structure does not need to be changed.

○ Off-Path Mode

In off-path mode, both uplink and downlink traffic on switch interfaces to be monitored is mirrored to the off-path interface of the firewall without changing the network structure.

Interface Name Ge0/0

* Interface Type ● WAN Interface ○ LAN Interface

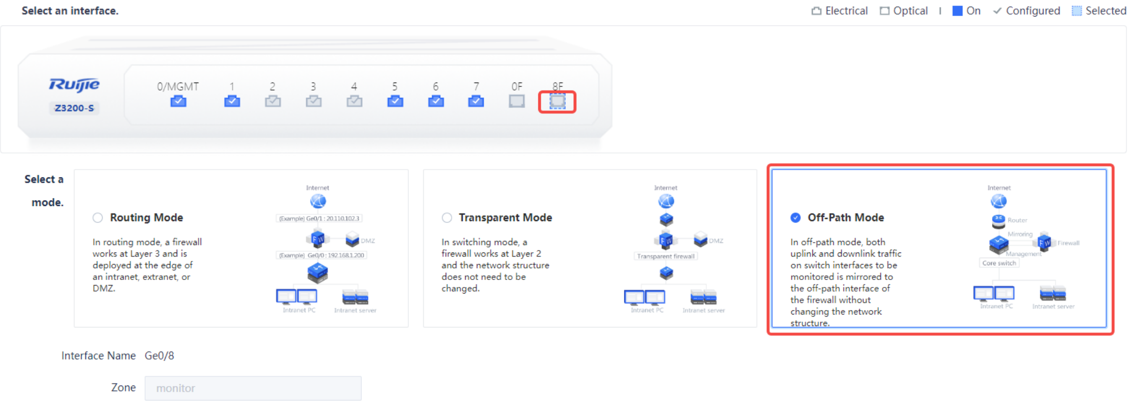
IP Type [IPv4] IPv6

Connection Type ● Static Address ○ DHCP ○ PPPoE

* IP/Mask 192.168.200.199/24

* Next-Hop Address 192.168.200.1

- Configure another interface as the off-path interface. This example uses Ge0/8 as the off-path interface.



○ Routing Mode

In routing mode, a firewall works at Layer 3 and is deployed at the edge of an intranet, extranet, or DMZ.

○ Transparent Mode

In switching mode, a firewall works at Layer 2 and the network structure does not need to be changed.

● Off-Path Mode

In off-path mode, both uplink and downlink traffic on switch interfaces to be monitored is mirrored to the off-path interface of the firewall without changing the network structure.

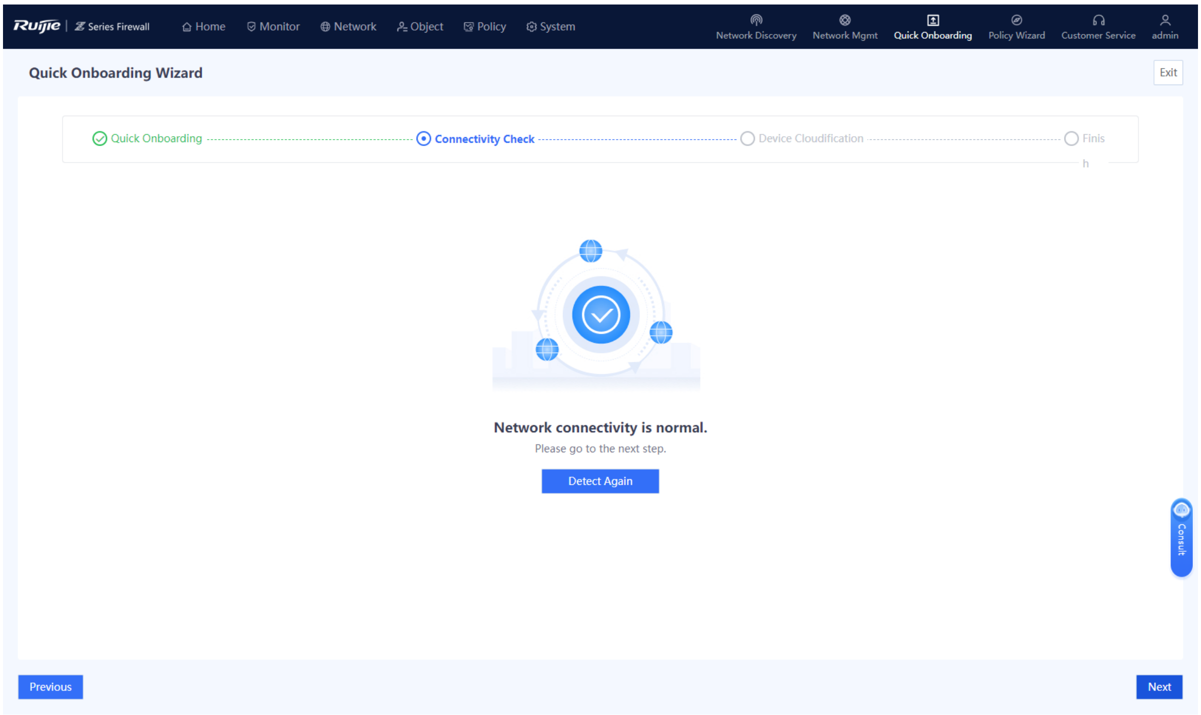
Interface Name Ge0/8

Zone monitor

Note

The management interface cannot be set to the off-path mode.

(2) (Optional) Check the connectivity.

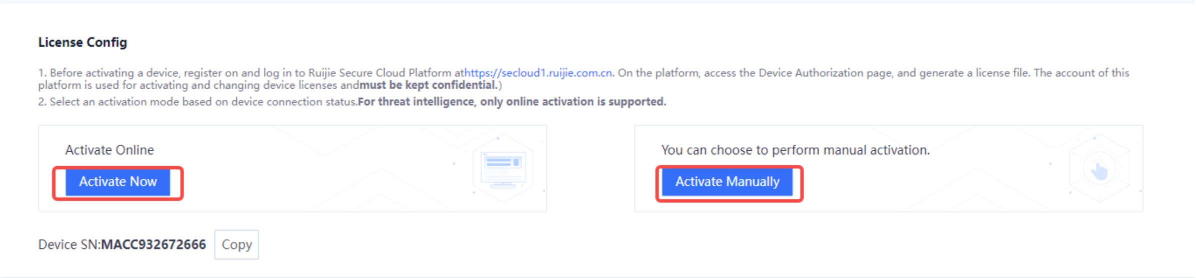


Quick Onboarding Wizard

Network connectivity is normal.

Please go to the next step.

(3) Import licenses.



License Config

1. Before activating a device, register on and log in to Ruijie Secure Cloud Platform athttps://secloud1.ruijie.com.cn. On the platform, access the Device Authorization page, and generate a license file. The account of this platform is used for activating and changing device licenses and**must be kept confidential.**)

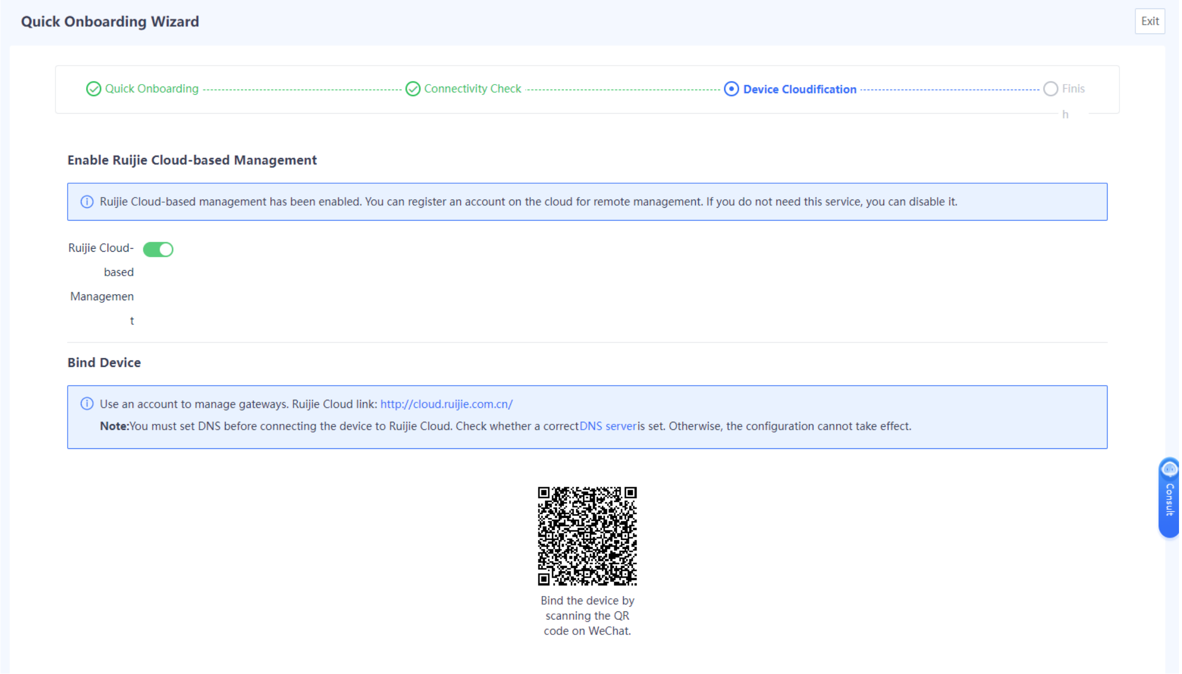
2. Select an activation mode based on device connection status.**For threat intelligence, only online activation is supported.**

Activate Online

You can choose to perform manual activation.

Device SN:**MACC932672666**

(4) Complete the quick onboarding configuration and log in to Ruijie Cloud to implement remote O&M.



Quick Onboarding Wizard

Enable Ruijie Cloud-based Management

Ruijie Cloud-based management has been enabled. You can register an account on the cloud for remote management. If you do not need this service, you can disable it.

Ruijie Cloud-based Management: ●

Bind Device

Use an account to manage gateways. Ruijie Cloud link: http://cloud.ruijie.com.cn/

Note: You must set DNS before connecting the device to Ruijie Cloud. Check whether a correctDNS serveris set. Otherwise, the configuration cannot take effect.

Bind the device by scanning the QR code on WeChat.

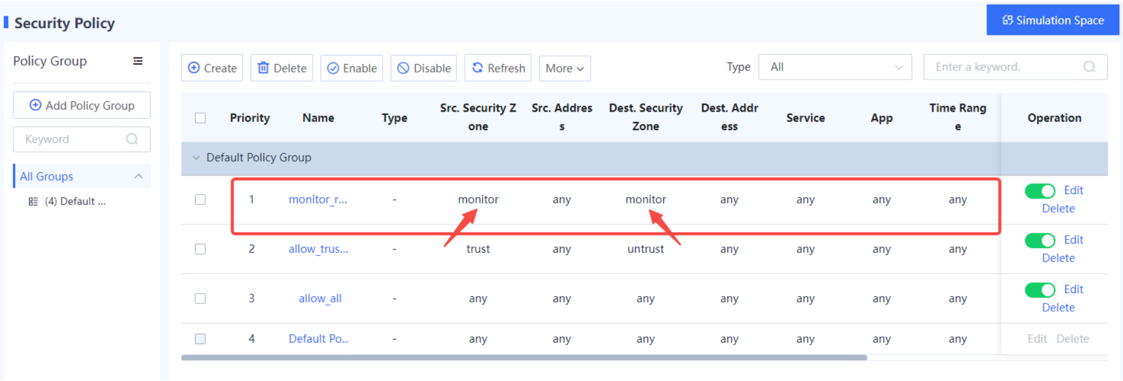
(5) Configure the switch to mirror both uplink and downlink traffic on switch interfaces to be monitored to the off-path interface Ge0/8. (Omitted)

Note

There are slight differences in the configuration method of different switches. For details, see the product manual.

(6) Create a security policy.

After the quick deployment configuration is complete, the security policy **allow_all** is generated automatically. This security policy permits all traffic by default. To control and detect the traffic in off-path mode, you need to create a security policy in which both **Src. Security Zone** and **Dest. Security Zone** are set to **monitor**.

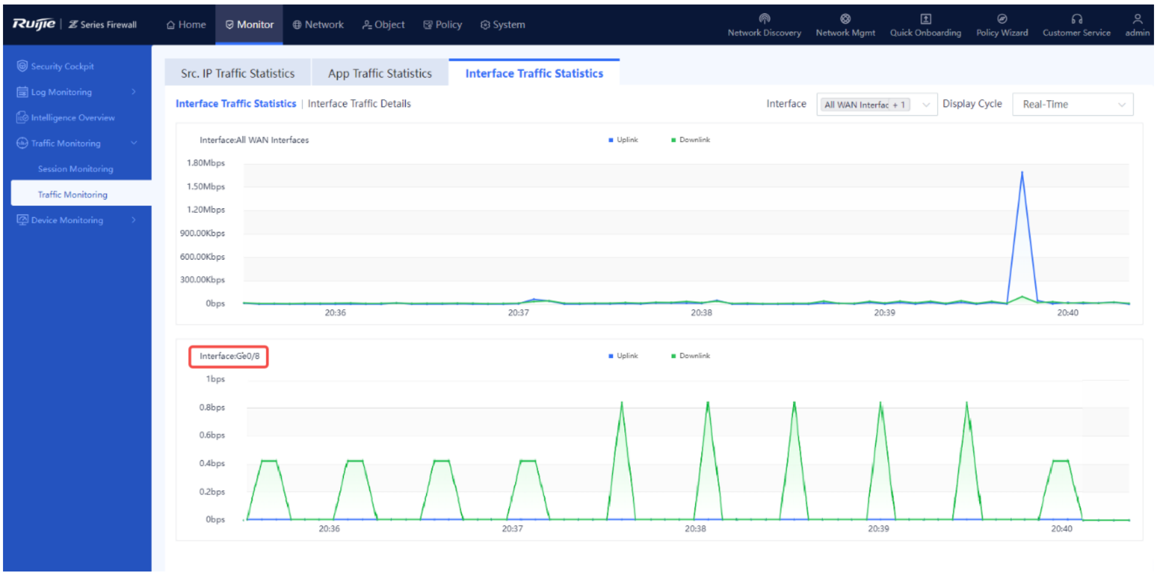


Security Policy

□	Priority	Name	Type	Src. Security Zone	Src. Address	Dest. Security Zone	Dest. Address	Service	App	Time Range	Operation
Default Policy Group											
□	1	monitor_r...	-	monitor	any	monitor	any	any	any	any	Edit Delete
□	2	allow_trus...	-	trust	any	untrust	any	any	any	any	Edit Delete
□	3	allow_all	-	any	any	any	any	any	any	any	Edit Delete
□	4	Default Po...	-	any	any	any	any	any	any	any	Edit Delete

Configuration Verification

Choose **Monitor** > **Traffic Monitoring** > **Traffic Monitoring** > **Interface Traffic Statistics** and check whether there is traffic on the Ge0/8 port.



Interface: All WAN Interfac + 1
Display Cycle: Real-Time

6.4.3 Configuring an Off-Path Interface (Custom Deployment)

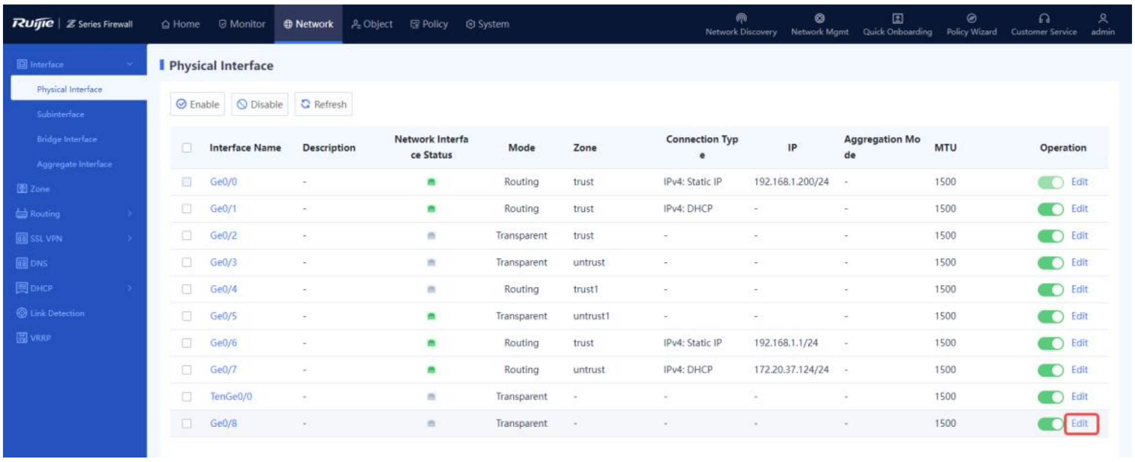
Configuration Points

An off-path interface is an interface set to off-path mode and is used only to receive mirrored traffic but cannot forward traffic. Security zone **monitor** defines the zone traffic of which needs to be monitored, and all off-path interfaces belong to the zone **monitor**. When you create a security policy in off-path mode, you need to set both **Src. Security Zone** and **Dest. Security Zone** to **monitor**.

Procedure

(1) Configure interfaces.

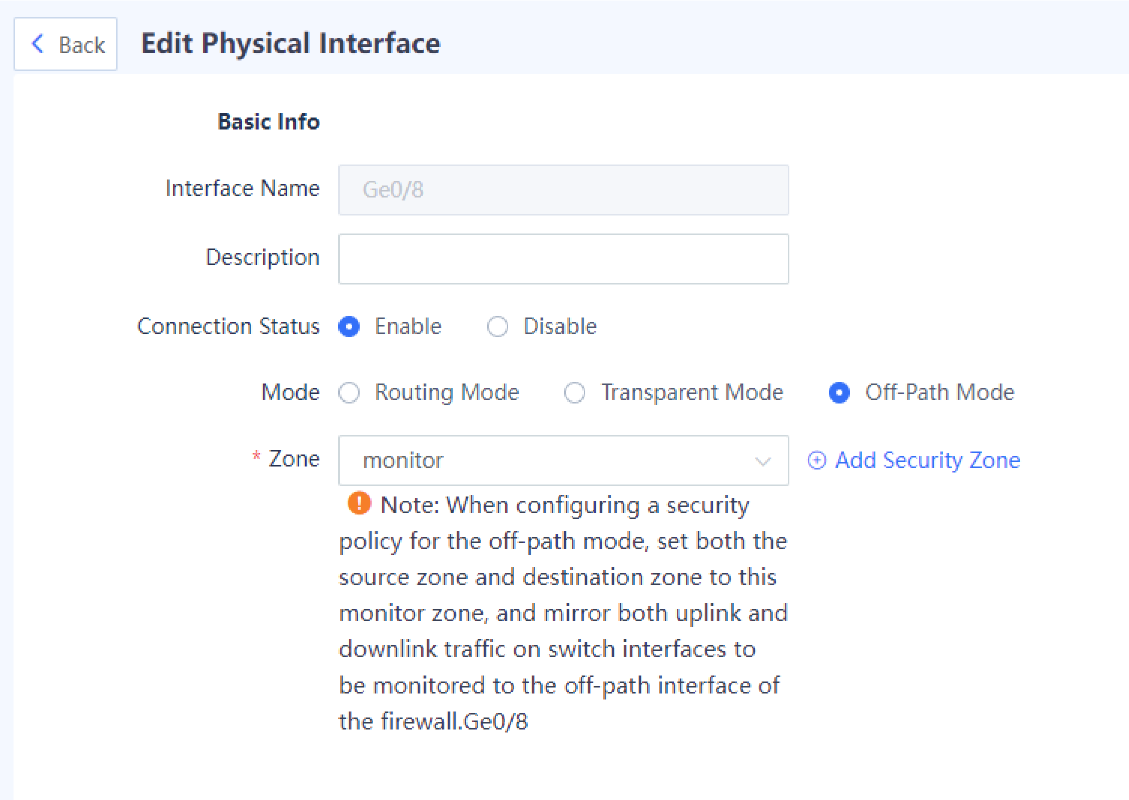
a Choose **Network** > **Interface** > **Physical Interface**, find the desired interface, and click **Edit** in the **Operation** column. The Ge0/8 port is used as an example.



Physical Interface

□	Interface Name	Description	Network Interface Status	Mode	Zone	Connection Type	IP	Aggregation Mode	MTU	Operation
□	Ge0/0	-	🟩	Routing	trust	IPv4: Static IP	192.168.1.200/24	-	1500	Edit
□	Ge0/1	-	🟩	Routing	trust	IPv4: DHCP	-	-	1500	Edit
□	Ge0/2	-	▨	Transparent	trust	-	-	-	1500	Edit
□	Ge0/3	-	▨	Transparent	untrust	-	-	-	1500	Edit
□	Ge0/4	-	▨	Routing	trust1	-	-	-	1500	Edit
□	Ge0/5	-	🟩	Transparent	untrust1	-	-	-	1500	Edit
□	Ge0/6	-	🟩	Routing	trust	IPv4: Static IP	192.168.1.1/24	-	1500	Edit
□	Ge0/7	-	🟩	Routing	untrust	IPv4: DHCP	172.20.37.124/24	-	1500	Edit
□	TenGe0/0	-	▨	Transparent	-	-	-	-	1500	Edit
□	Ge0/8	-	▨	Transparent	-	-	-	-	1500	Edit

b Set **Mode** to **Off-Path Mode** and retain the default value **monitor** for **Zone**.



Edit Physical Interface

Basic Info

Interface Name: Ge0/8

Description:

Connection Status: ● Enable ○ Disable

Mode: ○ Routing Mode ○ Transparent Mode ● Off-Path Mode

* Zone: monitor

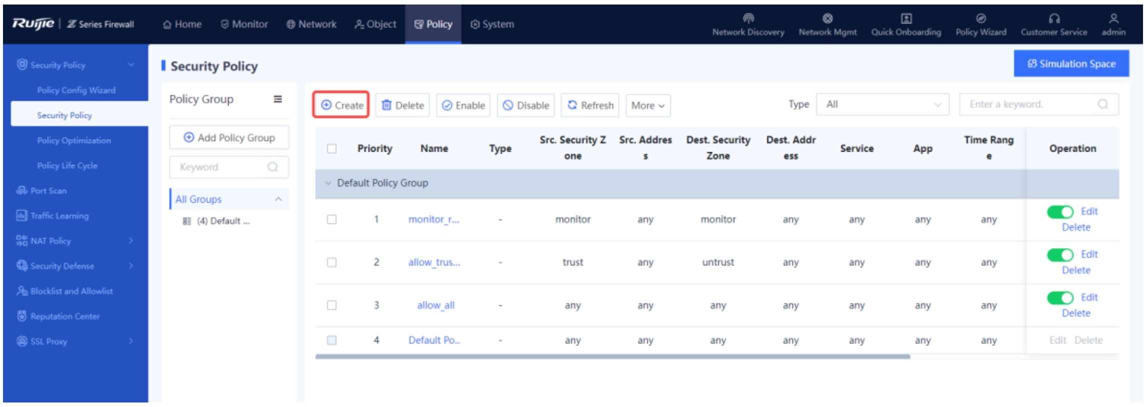
Note: When configuring a security policy for the off-path mode, set both the source zone and destination zone to this monitor zone, and mirror both uplink and downlink traffic on switch interfaces to be monitored to the off-path interface of the firewall.Ge0/8

c Click **Save**.

(2) Create a security policy.

The security zone of the off-path interface is **monitor** by default. To facilitate management, you are advised to separately configure a security control policy for off-path detection traffic.

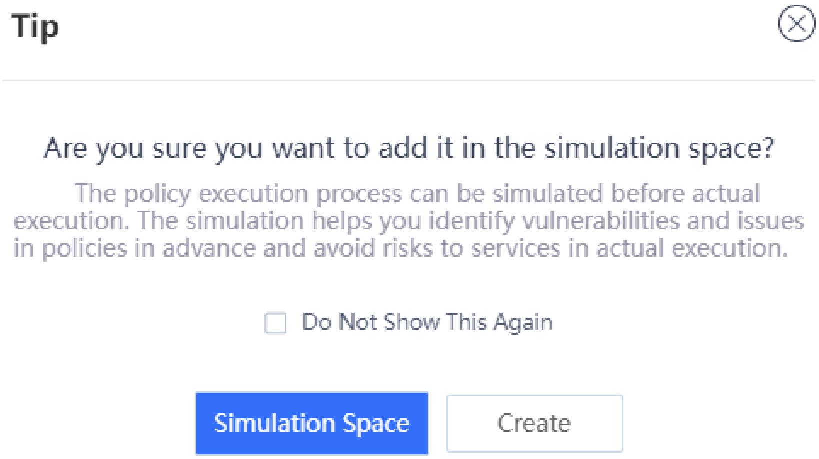
a Choose **Policy** > **Security Policy** and click **Create**.



Security Policy

	Priority	Name	Type	Src. Security Zone	Src. Address	Dest. Security Zone	Dest. Address	Service	App	Time Range	Operation
Default Policy Group											
□	1	monitor_r...	-	monitor	any	monitor	any	any	any	any	Edit Delete
□	2	allow_trus...	-	trust	any	untrust	any	any	any	any	Edit Delete
□	3	allow_all	-	any	any	any	any	any	any	any	Edit Delete
□	4	Default Po...	-	any	any	any	any	any	any	any	Edit Delete

b Access the simulation space and run the configured security policies in advance to ensure their security, or click **Create** to apply the security policy to the firewall.



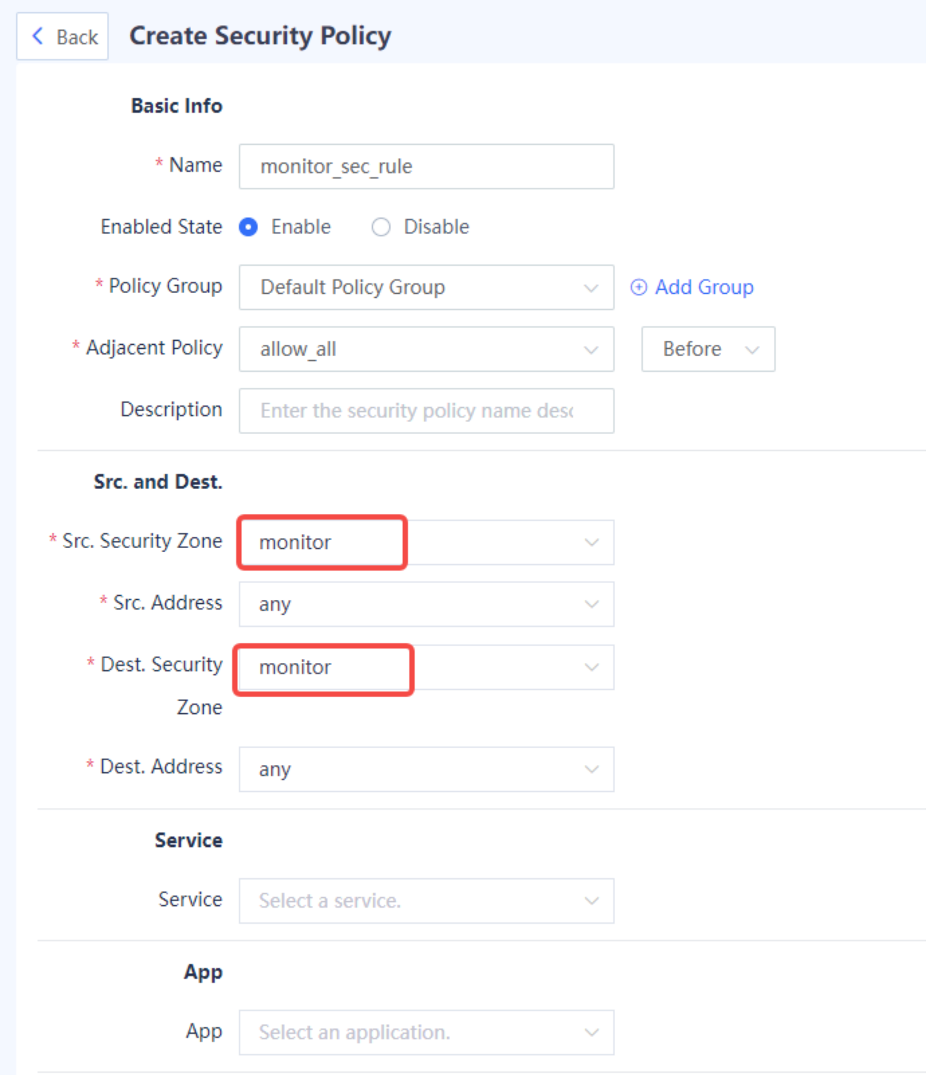
Tip

Are you sure you want to add it in the simulation space?

The policy execution process can be simulated before actual execution. The simulation helps you identify vulnerabilities and issues in policies in advance and avoid risks to services in actual execution.

□ Do Not Show This Again

c Create a security policy in which both **Src. Security Zone** and **Dest. Security Zone** are set to **monitor** to implement access control and detection on the off-path traffic based on actual needs.



< Back **Create Security Policy**

Basic Info

* Name: monitor_sec_rule

Enabled State: ● Enable ○ Disable

* Policy Group: Default Policy Group ⊕ Add Group

* Adjacent Policy: allow_all Before

Description: Enter the security policy name desc

Src. and Dest.

* Src. Security Zone: monitor

* Src. Address: any

* Dest. Security Zone: monitor

* Dest. Address: any

Service

Service: Select a service.

App

App: Select an application.

6.4.4 Precautions for Deploying Off-Path Mode

- When you deploy the firewall as the off-path detection device, you need to connect the interface receiving the detection traffic to the switch and configure the switch to mirror both uplink and downlink traffic on switch interfaces to be monitored to the firewall interface for detection.
- When you create a security policy in off-path mode (for access control of the off-path detection traffic), you need to set both **Src. Security Zone** and **Dest. Security Zone** to **monitor**.
- When off-path detection is enabled on the interface, the firewall detects traffic passing through the interface rather than forwarding the traffic.

7 Common Operations

7.1 NAT Policy

7.1.1 NAT Technology

Network Address Translation (NAT) is to translate the source address (port) or destination address (port) in a packet into the desired address. NAT includes the following two steps:

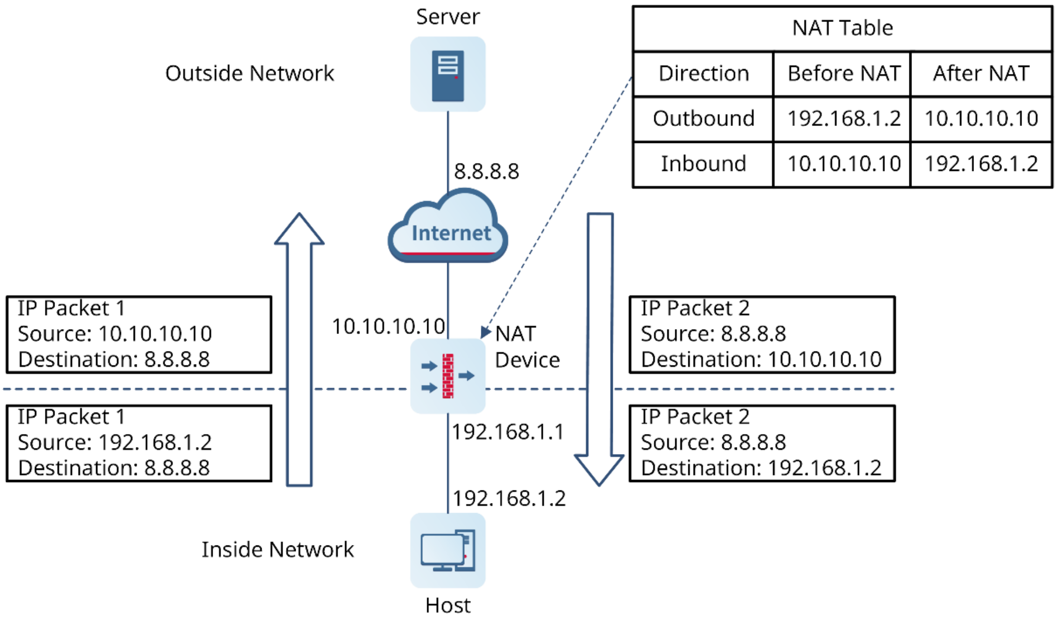
(1) Translate the original address into the mapped address.

(2) Restore the address in the returned packet.

The advantages of NAT are:

- Private network addresses can be used on an intranet. Private network addresses are not routable on the Internet, and can only be used after being converted to public network addresses.
- NAT hides the real IP addresses so that attackers cannot know the real addresses of hosts.
- If two network addresses overlap, they can use NAT to communicate with each other.

The following figure shows a typical working process of NAT.


Server
Outside Network
8.8.8.8
Internet
10.10.10.10
NAT Device
192.168.1.1
192.168.1.2
Inside Network
Host
IP Packet 1 Source: 10.10.10.10 Destination: 8.8.8.8
IP Packet 1 Source: 192.168.1.2 Destination: 8.8.8.8
IP Packet 2 Source: 8.8.8.8 Destination: 10.10.10.10
IP Packet 2 Source: 8.8.8.8 Destination: 192.168.1.2

NAT Table		
Direction	Before NAT	After NAT
Outbound	192.168.1.2	10.10.10.10
Inbound	10.10.10.10	192.168.1.2

(1) IP packet 1 sent by the intranet user host (192.168.1.2) to the extranet server (8.8.8.8) will pass through the NAT device.

(2) After checking the packet header, the NAT device finds that packet 1 is destined for the Internet, so it translates the private address 192.168.1.2 in its source IP address field into a public network address 10.10.10.10 that can be routed on the Internet and sends packet 1 to the extranet server. In addition, the NAT device records the mapping relationship in the NAT table.

(3) After reply packet 2 (whose initial destination IP address is 10.10.10.10) sent by the extranet server to the intranet host arrives at the NAT device, the NAT device checks the header again, searches the NAT table for the record of the current network address, and then replaces the initial destination IP address with the private address 192.168.1.2.

(4) The NAT process described above is transparent to the endpoints (such as the host and server in the figure). The extranet server only knows that the IP address of intranet host is 10.10.10.10, but does not know the address 192.168.1.2. Therefore, NAT "hides" the private network of the enterprise.

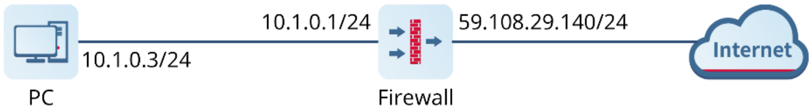
The Z-S series firewalls support multiple NAT modes to implement unidirectional and bidirectional translation between public IP addresses and private IP addresses. They are often used as specialized NAT devices. The NAT modes supported by Z-S series firewalls include:

- Static NAT
- Dynamic NAT
- PAT

1. Static NAT

Static NAT fixedly translates the original addresses into mapped addresses, regardless of inbound and outbound. As shown in Figure 7-1, 10.1.0.3 and 59.108.29.187 are one-to-one mapped. Different from dynamic NAT and PAT, static NAT is a fixed translation procedure, so the destination network can also access the source network.

Figure 7-1 Static NAT Example

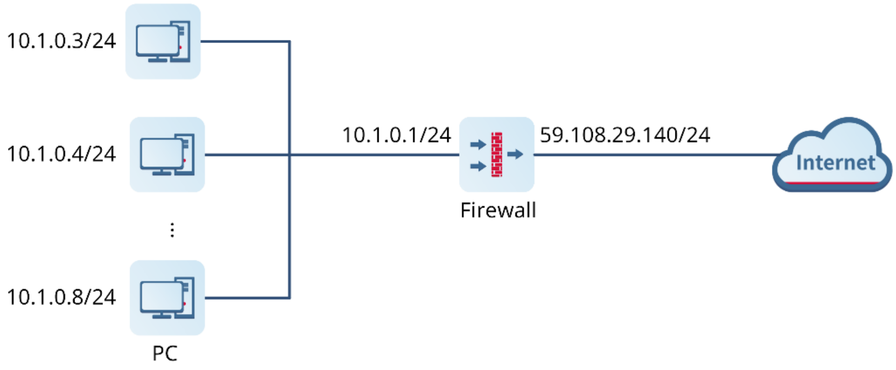


NAT Direction	Address Before NAT	Address After NAT
SNAT	10.1.0.3	59.108.29.187
DNAT	59.108.29.187	10.1.0.3

2. Dynamic NAT

Dynamic NAT translates a group of original IP addresses into a pool of mapped addresses that can be routed on the destination network. The number of addresses in the mapped address pool can be smaller than the number of original IP address. The translation process is a one-to-one mapping between the original address and the mapped address. This mapping relationship is available only when the session is valid. When the session becomes invalid, the mapping relationship is canceled. As shown in Figure 7-2, addresses 10.1.0.[3-8] are translated into addresses 59.108.29.[90-99], to implement the communication between the intranet and the Internet. However, the devices on the Internet do not know the addresses 10.1.0.[3-8].

Figure 7-2 Dynamic NAT Example

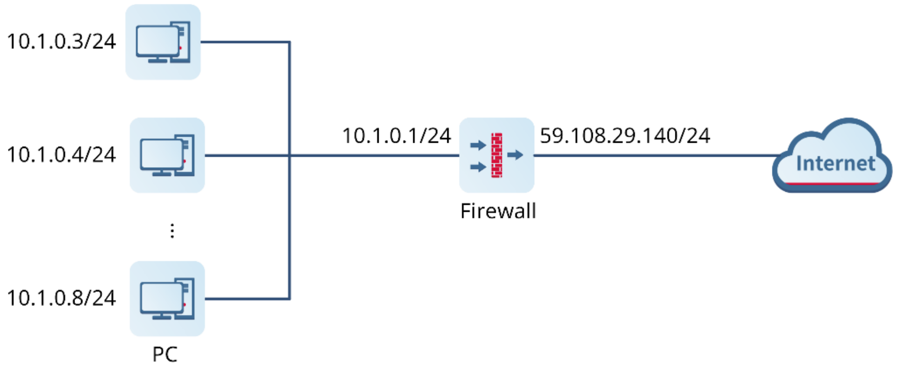


NAT Direction	Address Before NAT	Address After NAT
SNAT	10.1.0.3-10.1.0.8	59.108.29.90-59.108.29.99
DNAT	59.108.29.90-59.108.29.99	10.1.0.3-10.1.0.8

3. PAT

Port Address Translation (PAT) maps multiple IP addresses into one public IP address. In the process of address translation, the original addresses and the original ports are translated into mapped addresses and ports whose numbers are greater than 1024. Every connection requires an independent translation process because the source ports of the connections' original IP addresses are different. As shown in Figure 7-3, 10.1.0.3:1025 and 10.1.0.3:1026 requires different translation processes. PAT can fully use existing public IP address resources on the Internet.

Figure 7-3 PAT Example



NAT Direction	Address Before NAT	Address After NAT
SNAT	10.1.0.3-10.1.0.8	59.108.29.140
DNAT	59.108.29.140	10.1.0.3-10.1.0.8

4. Firewall Policy-based NAT

Z-S series firewalls can realize fine-grained control of the above NAT modes, so that the NAT function can fully meet the needs of customers, which is very flexible and convenient. You can perform NAT policy control from the following dimensions:

- Perform NAT for certain addresses.
- Perform NAT in the required time segments.
- Perform NAT for certain destination addresses.
- Perform NAT for certain services.
- Perform NAT from a specified port to another specified port.

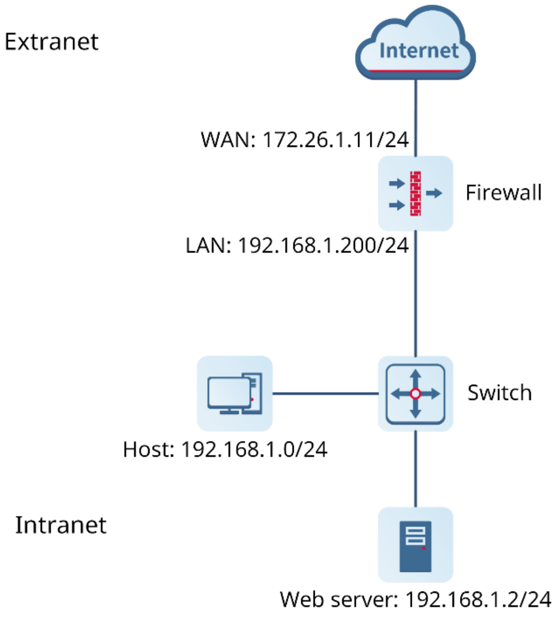
7.1.2 Configuring Destination Address Translation (One-to-One Port Mapping)

Network Requirements

After completing the basic firewall configurations, you need to map a web server (192.168.1.2) on the intranet to the address of an extranet port (172.26.1.116) so that users on the extranet can access this server.

In addition, intranet users can use the public network address to access the server.

Network Topology



Configuration Points

(1) Complete basic network access settings.

(2) Configure the security policy.

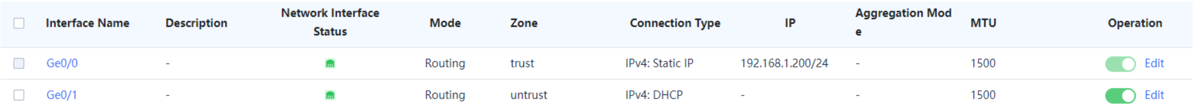
(3) Configure port mapping.

Procedure

(1) Complete basic network access settings.

For details, see 6.2 Transparent Mode.

The interface configuration is as follows:

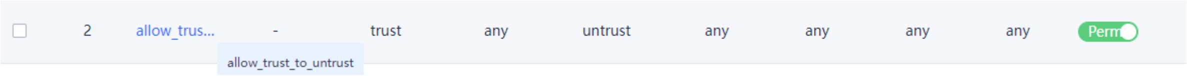


□	Interface Name	Description	Network Interface Status	Mode	Zone	Connection Type	IP	Aggregation Mode	MTU	Operation
□	Ge0/0	-	🟩	Routing	trust	IPv4: Static IP	192.168.1.200/24	-	1500	Edit
□	Ge0/1	-	🟩	Routing	untrust	IPv4: DHCP	-	-	1500	Edit

(2) Configure the security policy.

For details, see 7.7 DHCP Management.

The policy configuration is as follows:



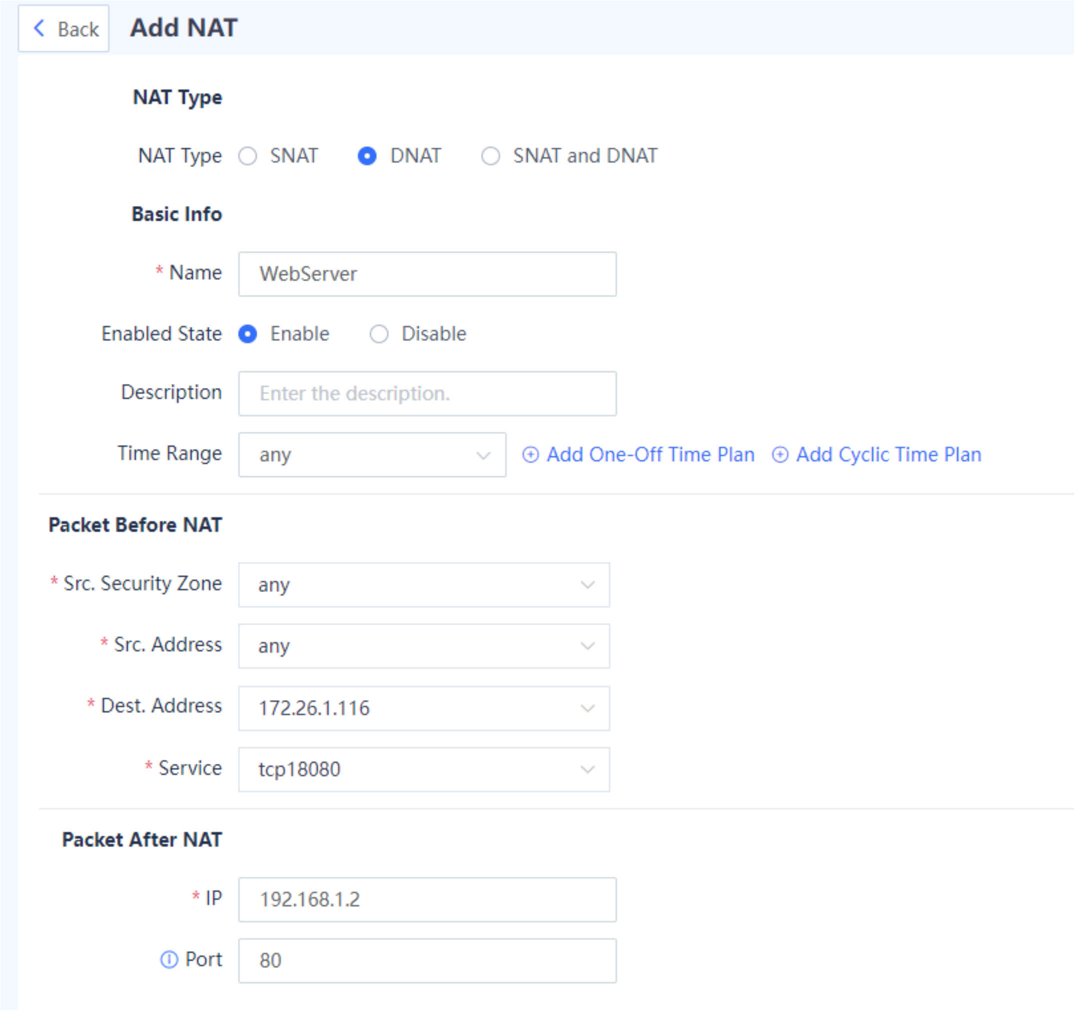
□	2	allow_trus... allow_trust_to_untrust	-	trust	any	untrust	any	any	any	any	Perm

(3) Configure port mapping.

a Choose **Policy** > **NAT Policy** > **NAT**.

b Above the operation area, click **Create**.

The system displays the **Add NAT** page.



NAT Type

NAT Type ○ SNAT ● DNAT ○ SNAT and DNAT

Basic Info

* Name: WebServer

Enabled State: ● Enable ○ Disable

Description: Enter the description.

Time Range: any

Packet Before NAT

* Src. Security Zone: any

* Src. Address: any

* Dest. Address: 172.26.1.116

* Service: tcp18080

Packet After NAT

* IP: 192.168.1.2

Port: 80

Item	Description
Basic Info	
Name	WebServer
Enabled State	Enable
Packet Before NAT	

Item	Description
Src. Security Zone	untrust and trust
Src. Address	any
Dest. Address	WAN interface address: 172.26.1.116
Service	Source port: 0-65535; destination port 18080 (external port)
Packet After NAT	
IP Address	192.168.1.2
Port	80 (internal port)

c Click **Save**.

Verification

Users can visit http://172.26.1.116 from the Internet.

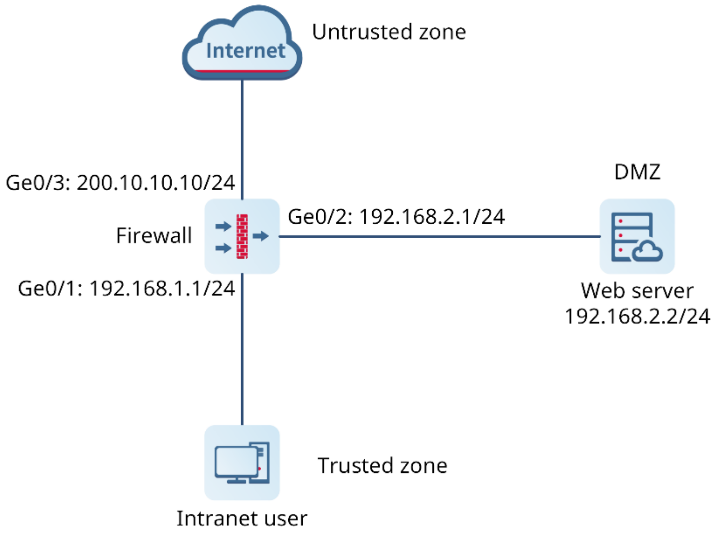
7.1.3 Configuring Bidirectional Address Translation (Allowing Intranet PCs to Access the Map Server by Using a Public Network Address)

Network Requirements

After completing the basic firewall configurations, you need to map a web server (192.168.2.2) on the intranet to the address of an extranet port (200.10.10.10) so that users on the intranet and the extranet can access this server.

- The web server is in the intranet server zone (zone: DMZ; IP address: 192.168.2.2; service: HTTPS).
- Extranet users need to access the server by accessing the extranet port address of the firewall (zone: untrust; IP address: 200.10.10.10; port 50000).
- Intranet users (zone: trust) also need to access the server by accessing the extranet port address of the firewall (zone: untrust; IP address: 200.10.10.10; port 50000), and the source address used to access the server is the extranet port of the firewall.

Network Topology



Configuration Points

(1) Complete basic network access settings.

(2) Configure the security policy.

(3) Configure bidirectional address translation.

a Configure the destination address translation policy for extranet users.

b Configure the twice NAT policy for intranet users.

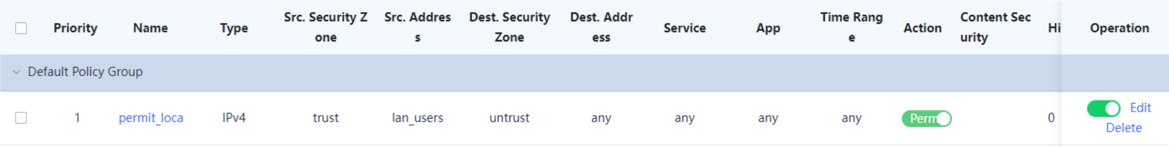
Procedure

(1) Complete basic network access settings.

For details, see 6.2 Transparent Mode.

(2) Configure the security policy.

The policy configuration is as follows:



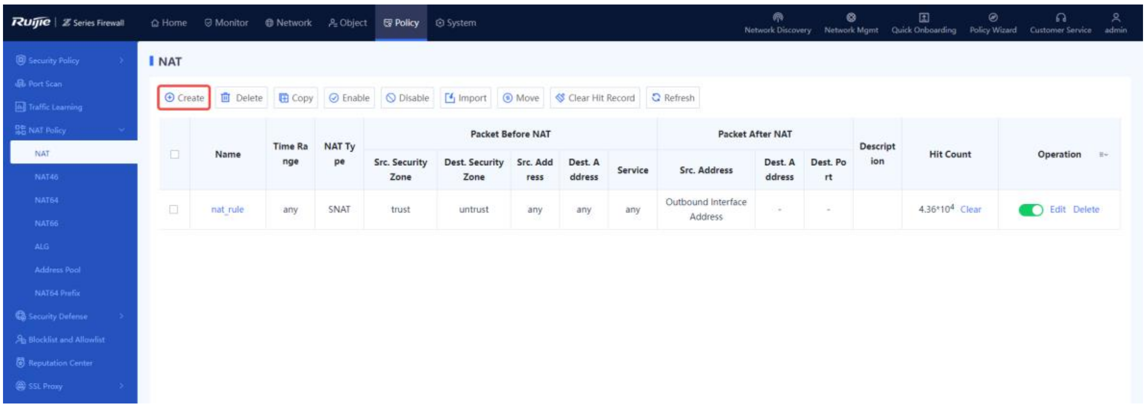
□	Priority	Name	Type	Src. Security Zone	Src. Address	Dest. Security Zone	Dest. Address	Service	App	Time Range	Action	Content Security	Hi	Operation
Default Policy Group														
□	1	permit_loca	IPv4	trust	lan_users	untrust	any	any	any	any	Perm		0	Edit Delete

(3) Configure port mapping.

Configure the destination address translation policy for extranet users.

a Choose **Policy** > **NAT Policy** > **NAT**.

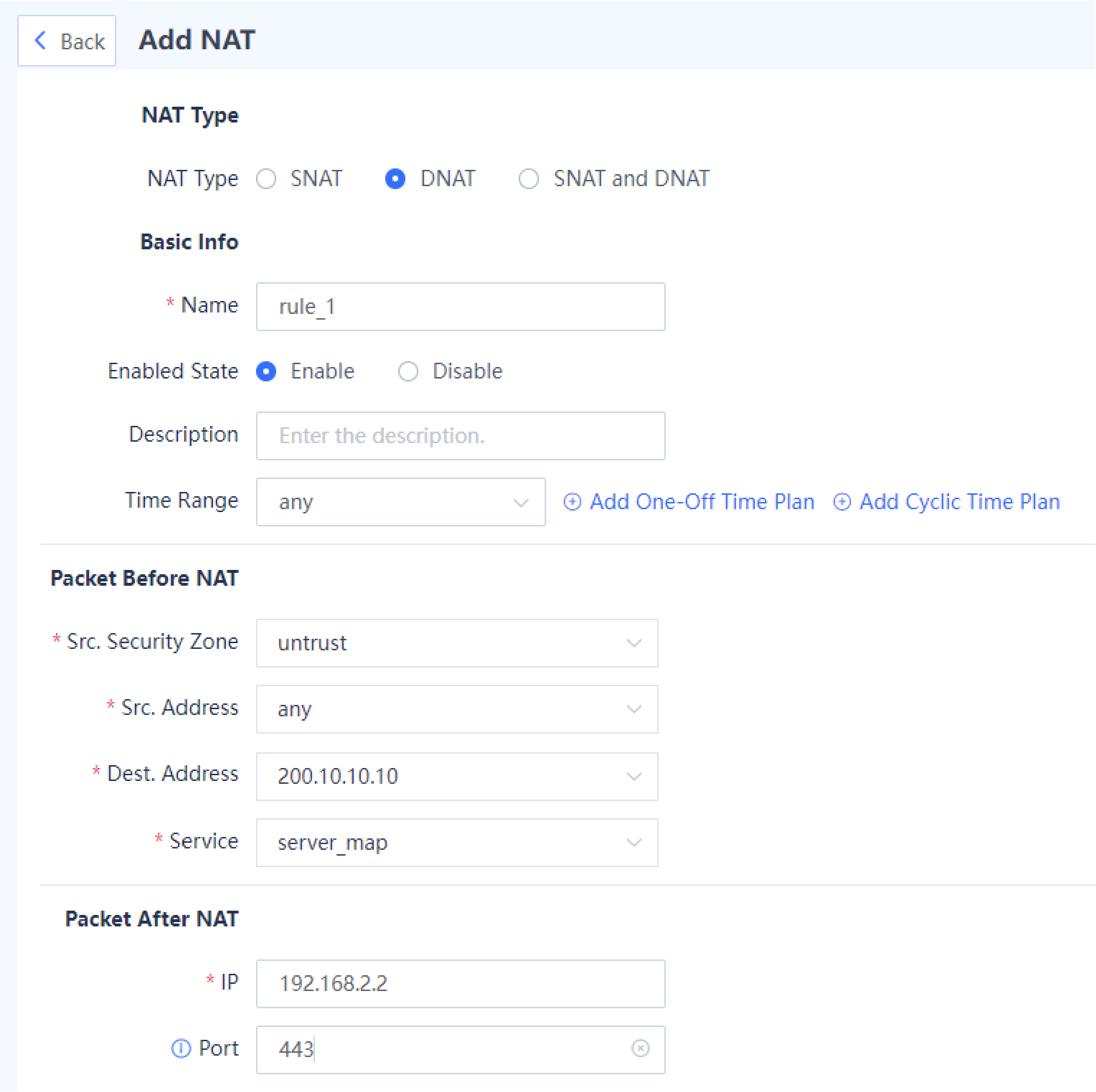
b Click **Create**.



NAT

□	Name	Time Range	NAT Type	Packet Before NAT					Packet After NAT			Description	Hit Count	Operation
				Src. Security Zone	Dest. Security Zone	Src. Address	Dest. Address	Service	Src. Address	Dest. Address	Dest. Port			
□	nat_rule	any	SNAT	trust	untrust	any	any	any	Outbound Interface Address	-	-		$4.36*10^4$ Clear	Edit Delete

c Set the parameters related to destination address translation.



Add NAT

NAT Type

NAT Type ○ SNAT ● DNAT ○ SNAT and DNAT

Basic Info

* Name: rule_1

Enabled State ● Enable ○ Disable

Description: Enter the description.

Time Range: any

Packet Before NAT

* Src. Security Zone: untrust

* Src. Address: any

* Dest. Address: 200.10.10.10

* Service: server_map

Packet After NAT

* IP: 192.168.2.2

Port: 443

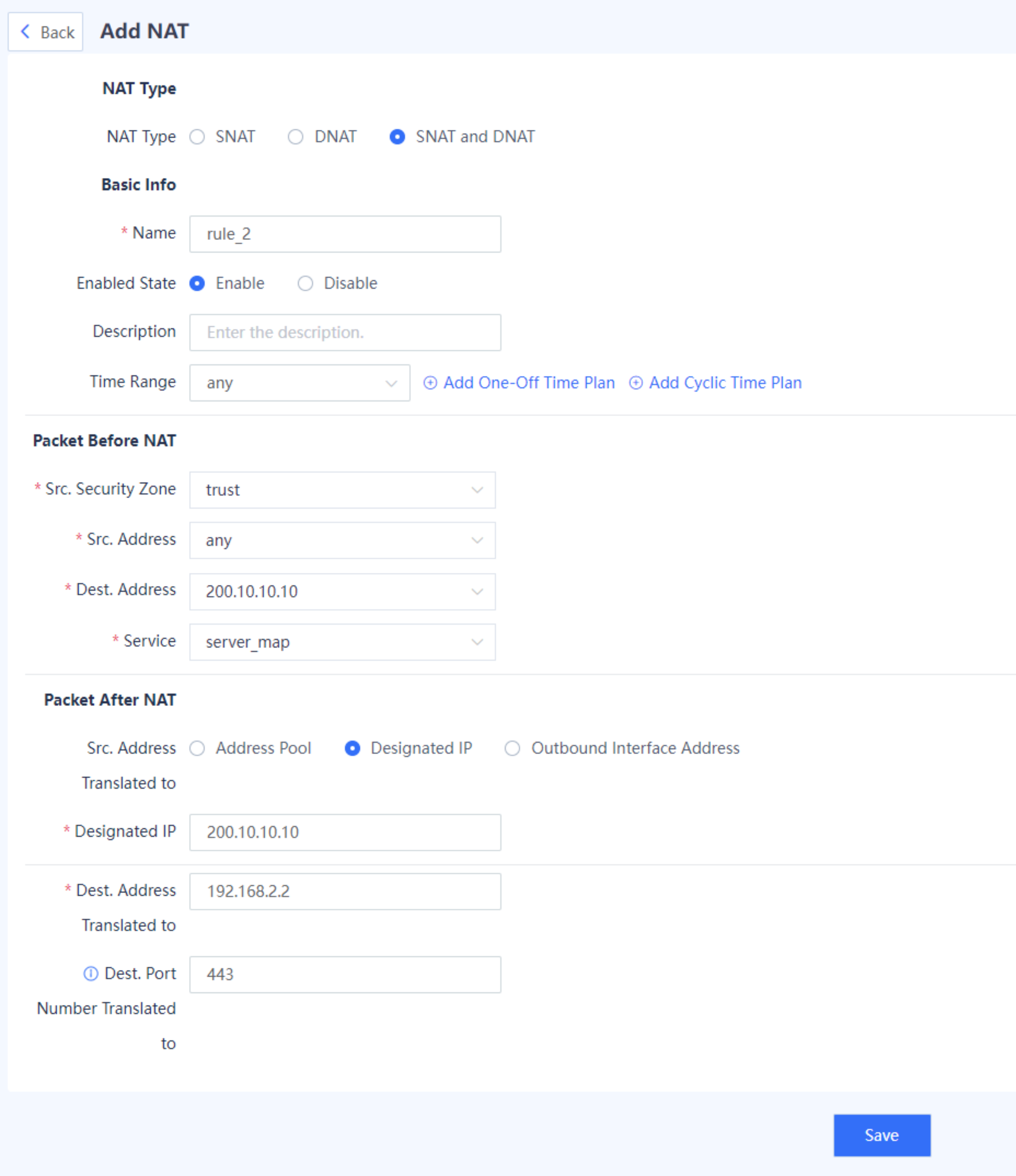
Item	Description
Basic Info	
Name	rule_1
Enabled State	Enable
Packet Before NAT	
Src. Security Zone	untrust
Src. Address	any
Dest. Address	Extranet port IP address of the firewall: 200.10.10.10
Service	Create a customized service **server_map** (for example, TCP, source port 0-65535, and destination port 50000).
Packet After NAT	
IP Address	Set the destination address to the IP address of web server in the DMZ, 192.168.2.2.
Port	Set the destination port to 443 (web server port).

(4) Configure the twice NAT policy for intranet users.

a Choose **Policy** > **NAT Policy** > **NAT**.

b Click **Create**.

c Set the parameters for twice NAT.



< Back **Add NAT**

NAT Type

NAT Type ○ SNAT ○ DNAT ● SNAT and DNAT

Basic Info

* Name: rule_2

Enabled State ● Enable ○ Disable

Description: Enter the description.

Time Range: any ⊕ Add One-Off Time Plan ⊕ Add Cyclic Time Plan

Packet Before NAT

* Src. Security Zone: trust

* Src. Address: any

* Dest. Address: 200.10.10.10

* Service: server_map

Packet After NAT

Src. Address Translated to ○ Address Pool ● Designated IP ○ Outbound Interface Address

* Designated IP: 200.10.10.10

* Dest. Address Translated to: 192.168.2.2

ⓘ Dest. Port Number Translated to: 443

Item	Description
Basic Info	
Name	rule_2
Enabled State	Enable
Packet Before NAT	

Item	Description
Src. Security Zone	trust
Src. Address	any
Dest. Address	Extranet port IP address of the firewall
Service	Create a customized service **server_map** (for example, TCP, source port 0-65535, and destination port 50000).
Packet After NAT	
Src. Address Translated to	In source address translation, configure the specified IP address 200.10.10.10 as the firewall's extranet address. If the firewall has multiple extranet addresses, you can configure an address pool as the extranet address, and then apply the address pool. Note: If the extranet address is configured as an egress interface address, the source IP address will be translated into 192.168.2.1, which does not meet requirements.
Designated IP	Firewall's extranet address, for example, 200.10.10.10
Dest. Address Translated to	Set the destination address to the IP address of web server in the DMZ, 192.168.2.2.
Dest. Port Number Translated to	Set the destination port to 443 (web server port)

d Click **Save**.

Verification

Visit http://200.10.10.10:50000 outside the intranet.

7.1.4 Importing NAT Policies in a Batch

Application Scenario

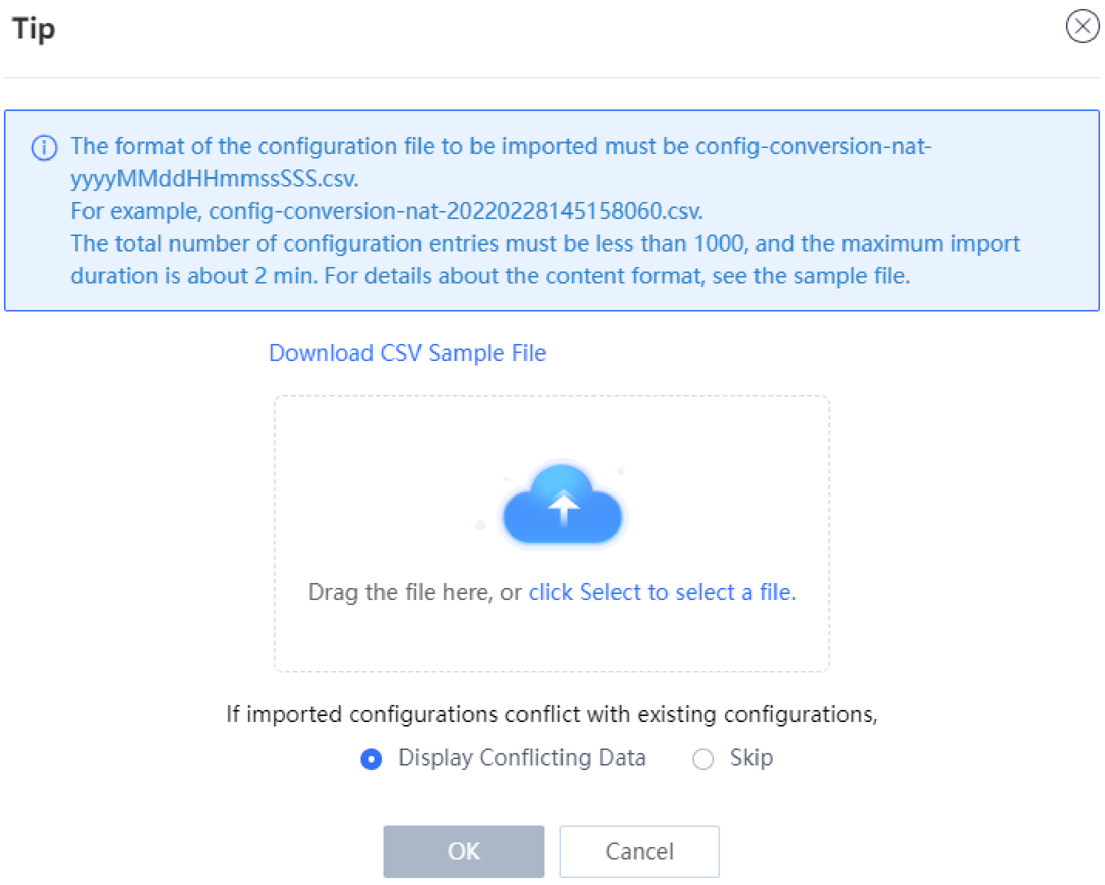
Z-S series firewalls provide the configuration file template. You can download the configuration file template, modify it according to actual service situations, and import the template to generate security policies fast.

Procedure

(1) Choose **Policy** > **NAT Policy** > **NAT**.

(2) In the operation area, click **Import**.

The system displays a tip.



Tip

The format of the configuration file to be imported must be config-conversion-nat-yyyyMMddHHmmssSSS.csv.
For example, config-conversion-nat-20220228145158060.csv.
The total number of configuration entries must be less than 1000, and the maximum import duration is about 2 min. For details about the content format, see the sample file.

Download CSV Sample File

Drag the file here, or click Select to select a file.

If imported configurations conflict with existing configurations,

● Display Conflicting Data ○ Skip

(3) Click **Download CSV Sample File** to download the configuration file template and fill in the configuration information.

Note

After modifying the configuration file, check whether the naming of the configuration file meets the system requirements. The naming format of the configuration file is: config-conversion-nat-{*yyyyMMddHHmmssSSS*}.csv.

(4) Drag the configuration file to the upload area or click **Select** to upload the configuration file to the device.

(5) Configure the handling method used when data conflicts.

When the imported data conflicts with the existing data, the handling processing methods can be used:

- **conflict data is displayed**: The system displays the conflicting configuration items and the conflict reason for you to modify the configuration file.
- **Skip**: The system ignores conflicting configuration items and no action is required.

(6) Click **OK**.

The system automatically writes the configuration file information to the device for the configuration to take effect.

7.2 Security Defense

7.2.1 Principle and Application Scenario

1. Local Defense

When traditional devices in a complex network undergo network attacks or heavy traffic, the following situations may occur:

- Extra high CPU utilization.
- Slow CLI response or no response.
- Loss of link or network control protocol packets, causing link or network jitter.
- Processing bandwidth occupied by illegal packets, resulting in a failure to process important protocol packets.

There are two reasons for these problems. One reason is that the processing capabilities of the traditional devices' control planes and forwarding planes are different. The other reason is that there is a lack of protection mechanism for the control plane. Z-S series firewalls can classify, filter, and limit the rate of data packets to be processed at the control layer, thus protecting key resources at the control layer. Z-S series firewalls support flexible combinations of associated various objects (region objects, address objects, and service objects) to formulate various local defense policies suitable for actual network security needs, accurately controlling the access rights of devices, and ensuring device security.

2. Security Defense

There may be many forms of attacks in customers' network environment, such as traffic-targeted DDoS attacks and packet- or protocol-targeted attacks (such as teardrop, smurf, and redirect). The target may be a user on the intranet or the device itself. Therefore, you can configure policies to help intranet users and devices defend against attacks. Local defense provides default policies to ensure the normal operation of the device. For ARP attacks on the intranet, security defense provides static ARP configuration, proxy ARP, and anti-ARP spoofing functions.

- Protocol attacks (malformed packet attack)

  Protocol attacks exploit the implementation vulnerabilities of protocol stack on the target device to send specific traffic or packets (malformed packets), to cause exceptions on the target device and achieve the purpose of denial of service. Common protocol attacks include land, smurf, fraggle, teardrop, WinNuke, ICMP redirect, ICMP unreachable, and large ICMP packet.

  - Land

  Attack principle/characteristics: The source address and destination address in the packet used for the land attack are the same. When a user device receives such packets, it may not know how to deal with the situation that the source address and destination address of the communication in the stack are the same, or it may send and receive the packets repeatedly, consuming a lot of system resources. As a result, the system may crash.

  - Smurf

  Attack principle/characteristics: This attack sends a packet with a specific request (such as an ICMP request) to the broadcast address of a subnet, and fills in the attacked host's address as the source address. Then all hosts on the subnet respond to a broadcast packet request and send packets to the attacked host. The host is attacked. Attackers can generate heavy attack traffic to the attacked host with a small cost.

  - Fraggle

  Attack principle/characteristics: By making a simple modification of the smurf attack, fraggle uses UDP reply packets instead of ICMP packets (attack ports 7 (echo) or 19 (chargen)).

  - Teardrop

  Attack principle/characteristics: This attack is mainly carried out by exploiting vulnerabilities in the system during IP packet reassembly. Teardrop is a UDP-based attack using malformed fragments. It sends multiple overlapping IP fragments to the attacked device (IP fragments include information such as which packet the fragment belongs to and the position in the packet). The attacker deliberately makes these fragments overlap. Some operating systems will crash and restart when they receive forged fragments with overlapping offset.

  - WinNuke

Attack principle/characteristics: WinNuke attack, also known as out-of-band transmission attack, attacks the destination ports, which are usually ports 53, 113, 137, 138, and 139. The URG bit is set to 1, that is, emergency mode.

- ICMP redirect

  Attack principle/characteristics: The attacker sends an ICMP redirect packet to the attacked host as a gateway, telling the host "the next hop to the next destination is me", so the attacked host modifies the routing table. The host's traffic is redirected to the attacker, and the attacker can sniff and hijack the traffic.

- ICMP unreachable

  Attack principle/characteristics: The attacker sends a forged ICMP unreachable packet to the attacked host, making the target host unable to access the destination host, port, or network segment and cutting off the connection between the host and the destination.

- Large ICMP packet

  Attack principle/characteristics: Attack the target system by sending large ICMP packets. Some systems may crash or restart after receiving the large ICMP packet due to improper processing.

- Flood (flow-based attack)

  Flood attacks mainly consume limited resources such as connection, bandwidth, and CPU of the attacked host to achieve deny of service of the target host. Common resource-consuming attacks include various types of flow-based flood attacks, including syn-flood, udp-flood, and icmp-flood.

- Scan

  Scan attack is usually the first step in the attacker's attempt to the target host/network. By scanning ports/IP addresses, the attacker discovers the ports, services, and OS types in the target host/network, which is the basic information for further penetration or attack. By traffic analysis, you will find that a specific host initiates a large number of connections to the consecutive ports at an IP address (attempt to detect open services) or consecutive IP addresses on a network segment (attempt to detect active hosts) in a short time.

3. Intrusion Prevention

Intrusion Prevention System (IPS) is a security product that performs in-depth inspection of traffic in real time to find threats and defend against them.

By performing in-depth detection on the traffic passing the firewall in real time, IPS can identify malicious information hidden in traffic, and report alarms and block traffic in real time to protect user hosts from malicious traffic.

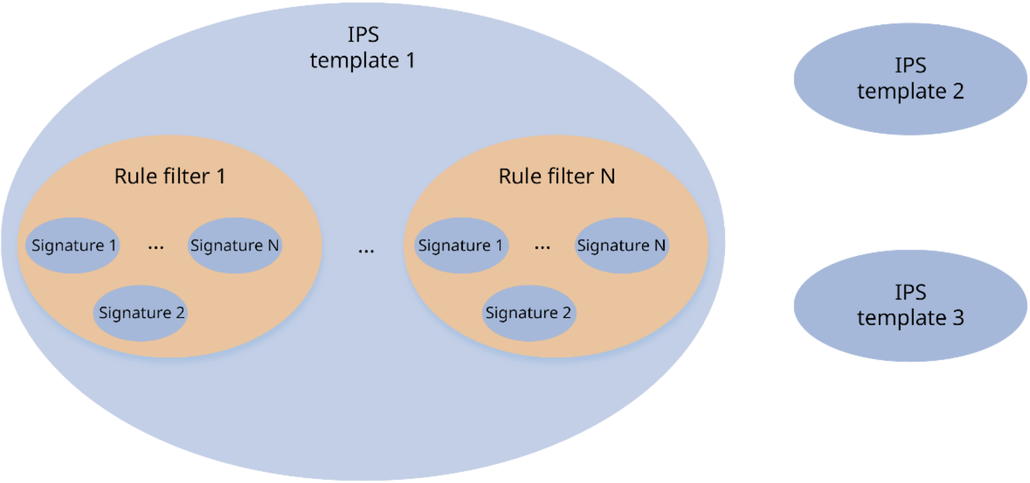
The IPS function of Z-S series firewalls is implemented using templates. Different templates can correspond to different signatures. You can customize the templates according to your needs. In addition, the device is delivered with a built-in "predefined template" that has been strictly verified.

- Custom template

  The custom template is the basic configuration of Ruijie firewall IPS. A configuration template is composed of multiple "rule filters", and each rule filter consists of several signatures. You can combine specific rules into a configuration template according to your needs.

  Figure 7-4 shows the relationships between configuration template, rule filter, and signature.

  Figure 7-4 Relationships Between Configuration Template, Rule Filter, and Signature

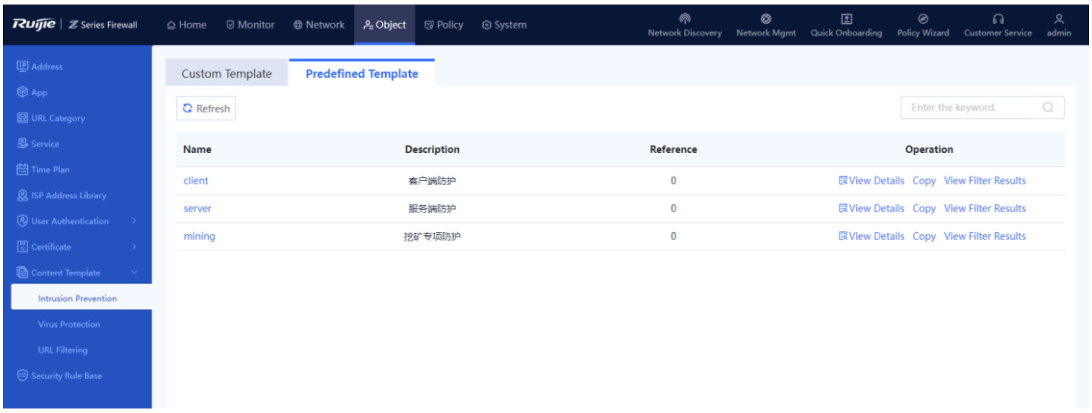


  IPS supports multiple templates. An IPS template supports multiple rule filters. Each rule filter supports multiple signatures.

- Predefined template

  The elements contained in predefined templates are consistent with those in custom templates. Their differences lie in:

- Predefined templates are a series of market-proven templates defined by Ruijie according to different usage scenarios. They can be directly used without modification or commissioning.
- The predefined templates will be updated automatically, and Ruijie will update the rule sets in the predefined templates according to the feedback from the market, which can reduce the maintenance manpower.

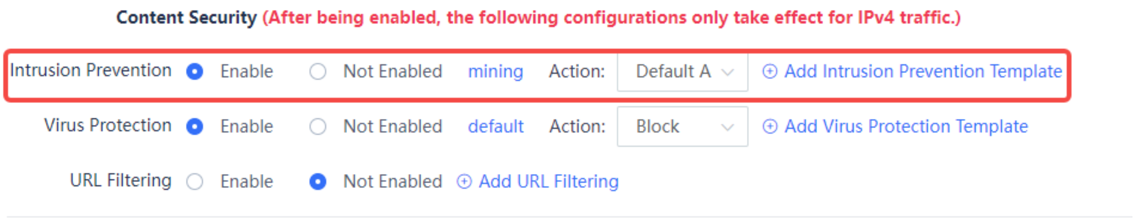


Name	Description	Reference	Operation
client	客户端防护	0	View Details Copy View Filter Results
server	服务端防护	0	View Details Copy View Filter Results
mining	挖矿专项防护	0	View Details Copy View Filter Results

- IPS template referenced by policy

When the template configuration is completed, the IPS function of Z-S series firewall takes effect only after you reference the IPS template on the policy page. After referencing the template, you can select the actions to be performed on the traffic that hits the template according to your needs:

- Default Action: All traffic that hits the signature is processed using the actions of the signature.
- Alarm: Alarms are reported for all traffic that hits the signature, ignoring the actions of the signature.
- Block: All traffic that hits the signature is blocked, ignoring the actions of the signature.



Content Security (After being enabled, the following configurations only take effect for IPv4 traffic.)

Intrusion Prevention ● Enable ○ Not Enabled mining Action: Default A ⊕ Add Intrusion Prevention Template

Virus Protection ● Enable ○ Not Enabled default Action: Block ⊕ Add Virus Protection Template

URL Filtering ○ Enable ● Not Enabled ⊕ Add URL Filtering

4. Virus Protection

Caution

The virus protection function is supported from NTOS1.0R3. If your version is lower than NTOS1.0R3, upgrade it to NTOS1.0R3 or higher.

Virus protection is a security detection technology that analyzes network traffic and files in real time to identify hidden viruses, and reports alarms or blocks the traffic to protect the security of intranet data.

This function supports virus detection for video files, audio files, image files, executable files, documents, compressed files, web files, code files, script files, and text files transmitted by HTTPS, HTTP, FTP, SMTP, and POP3. Before detecting HTTPS traffic, you need to configure the SSL proxy function. For more information about SSL proxy, see 7.3 Configuring SSL Proxy Policies.

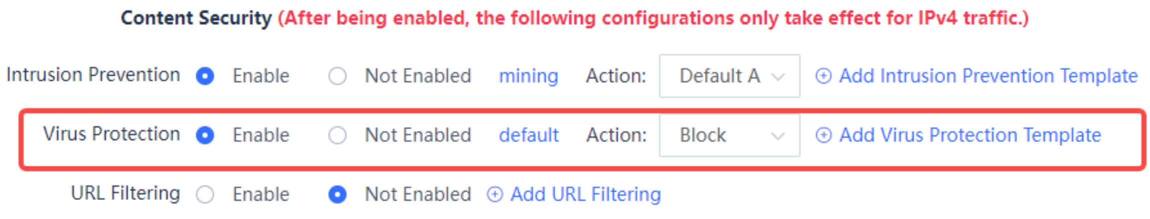
The firewall supports two virus detection modes: quick scan and deep scan. Different modes use different virus protection signature libraries:

- Quick scan: Use the **Virus Protection Signature Library (Quick Scan)**. The virus detection rate is low but the performance overhead is small.
- Deep scan: Use the **Virus Protection Signature Library (Deep Scan)**. The virus detection rate is high but the performance overhead is large.

The virus protection function of Z-S series firewalls is implemented using templates. Different templates detect different protocols. You can customize the templates according to your needs. In addition, the device is delivered with a built-in "predefined template" that has been strictly verified.

When the template configuration is completed, the function takes effect only after you reference the virus protection template on the security policy page. After referencing the template, you can select the actions to be performed on the traffic that hits the template according to your needs:

- Alarm: Always report alarms when virus is detected in traffic (only alarm, no blocking)
- Block: Block all traffic with virus detected.



Content Security (After being enabled, the following configurations only take effect for IPv4 traffic.)

Intrusion Prevention ● Enable ○ Not Enabled mining Action: Default A ⊕ Add Intrusion Prevention Template

Virus Protection ● Enable ○ Not Enabled default Action: Block ⊕ Add Virus Protection Template

URL Filtering ○ Enable ● Not Enabled ⊕ Add URL Filtering

5. Threat intelligence

Most of the typical security capabilities (such as AV and IPS) of firewalls are based on the analysis of traffic content. The firewalls use regularly updated signatures, rules and other information for detection, which has problems such as large detection costs and difficulty in dealing with new network threats such as Advanced Persistent Threat (APT) and zero-day vulnerabilities.

Threat Intelligence (TI) introduces real-time and global security threat knowledge to firewalls, enabling the firewalls to identify and filter malicious traffic with less computing overhead. Therefore, TI becomes an indispensable part of the multi-layer security protection system of firewalls.

The TI module can match threat intelligence based on the destination IP address of the traffic and the domain name in the DNS query, and perform blocking or alarming actions on the data that matches the threat intelligence, to block malicious IP addresses and domain names.

Data sources of threat intelligence include:

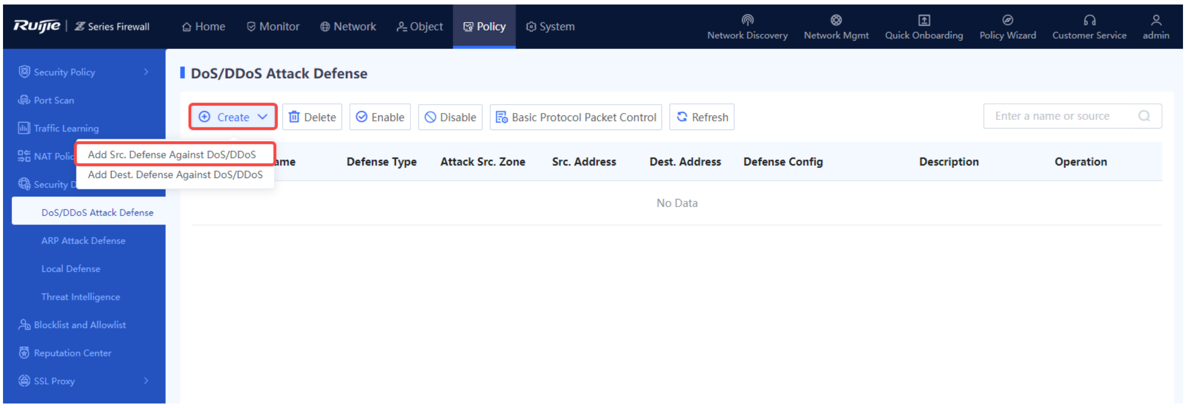
- Threat intelligence signature library: Contains a large amount of threat signature data and can be upgraded to obtain the latest data. After the TI authorization is activated, the firewall can perform security detection based on the threat intelligence signature library to enhance the capability of identifying and blocking threats. If the TI function is not authorized or authorization expires, detection based on the threat intelligence signature library is unavailable.
- Custom threat intelligence: In addition to the intelligence contained in the threat intelligence signature library, the system allows you to import malicious intelligence that you have collected. When threat is detected, the system matches the threat against the Custom Threat Intelligence first. The data matching Custom Threat Intelligence is blocked and a security log is recorded. In the unauthorized state, Custom Threat Intelligence can still be used for matching.

7.2.2 DoS/DDoS Attack Defense

1. Configuring Source Defense Against DoS/DDoS

Procedure

(1) Choose **Policy** > **Security Defense** > **DoS/DDoS Attack Defense**.



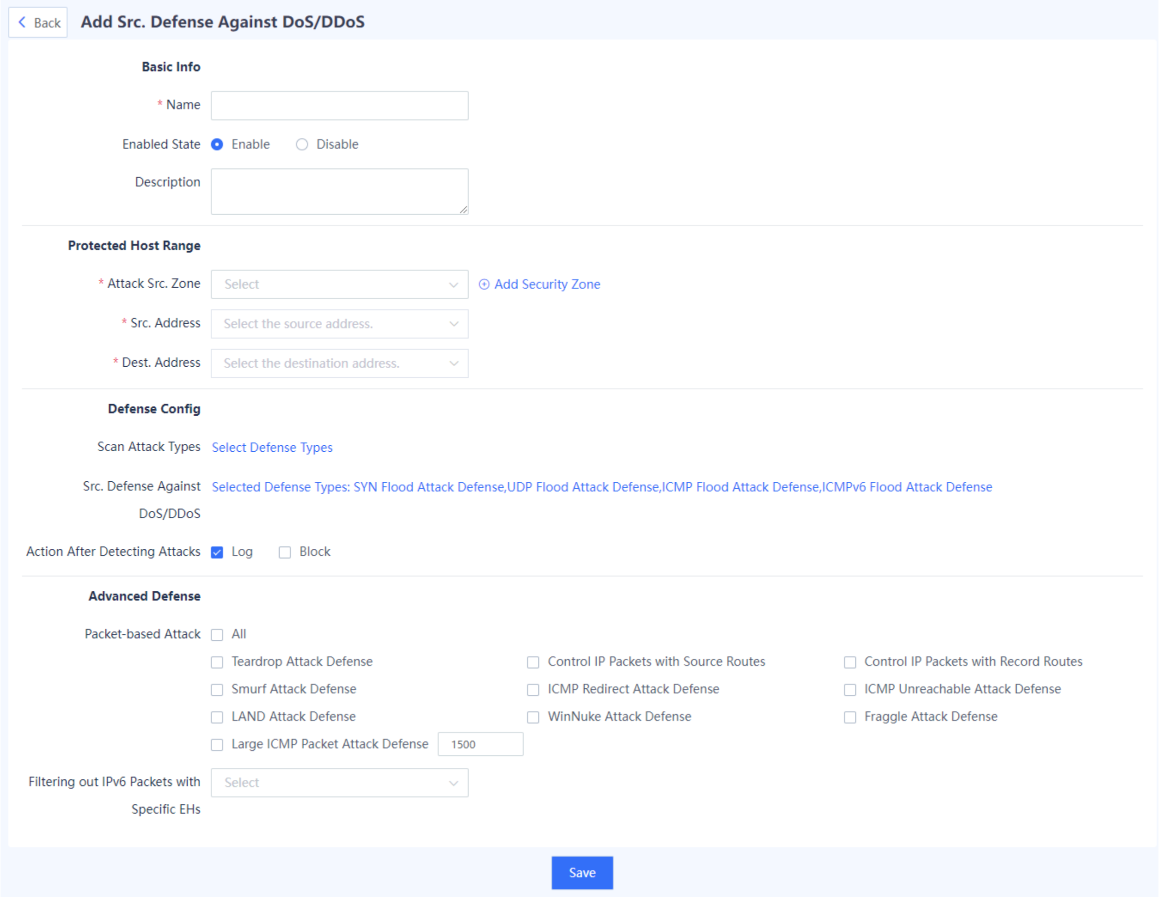
DoS/DDoS Attack Defense

ame	Defense Type	Attack Src. Zone	Src. Address	Dest. Address	Defense Config	Description	Operation

No Data

(2) Above the operation area, click **Create** and select **Add Src. Defense Against DoS/DDoS**.

The system displays the **Add Src. Defense Against DoS/DDoS** page.



Add Src. Defense Against DoS/DDoS

Basic Info

* Name

Enabled State ● Enable ○ Disable

Description

Protected Host Range

* Attack Src. Zone Select ⊕ Add Security Zone

* Src. Address Select the source address.

* Dest. Address Select the destination address.

Defense Config

Scan Attack Types Select Defense Types

Src. Defense Against DoS/DDoS Selected Defense Types: SYN Flood Attack Defense,UDP Flood Attack Defense,ICMP Flood Attack Defense,ICMPv6 Flood Attack Defense

Action After Detecting Attacks ☑ Log □ Block

Advanced Defense

Packet-based Attack □ All

□ Teardrop Attack Defense □ Control IP Packets with Source Routes □ Control IP Packets with Record Routes

□ Smurf Attack Defense □ ICMP Redirect Attack Defense □ ICMP Unreachable Attack Defense

□ LAND Attack Defense □ WinNuke Attack Defense □ Fraggle Attack Defense

□ Large ICMP Packet Attack Defense 1500

Filtering out IPv6 Packets with Specific EHs Select

(3) Set the parameters related to DoS/DDoS attack defense policy.

<table>
<tr><th>Item</th><th>Description</th><th>Remarks</th></tr>
<tr><td colspan="3">Basic Info</td></tr>
<tr><td>Name</td><td>Name of the DoS/DDoS attack defense policy.</td><td>Characters such as `~!#%^&*+\|{};:'"/<>? and spaces are not allowed.
[Example]
DoS_policy_1</td></tr>
<tr><td>Enabled State</td><td>Whether to enable the policy immediately after configuration is completed.</td><td>[Example]
Enable</td></tr>
<tr><td>Description</td><td>Description of the DoS/DDoS attack defense policy.</td><td>Characters such as `~!#%^&*+\|{};:'"/<>? are not allowed.
[Example]
New policy</td></tr>
<tr><td colspan="3">Protected Host Range
Range of the attack source associated with the policy. The policy takes effect when matching.</td></tr>
<tr><td>Attack Src. Zone</td><td>The policy checks the traffic from this security zone.</td><td>[Example]
any</td></tr>
<tr><td>Src. Address</td><td>The policy checks the traffic from this address set.</td><td><b>any</b> indicates all addresses.
[Example]
any</td></tr>
<tr><td>Dest. Address</td><td>The policy checks the traffic to this address set.</td><td><b>any</b> indicates all addresses.
[Example]
any</td></tr>
</table>

Item	Description	Remarks
Defense Config		
Scan Attack Types		
IP Scan Defense	Whether IP scan defense is enabled.	[Example] Enabled
Limit (pps)	Threshold for detecting an IP scan attack and triggering protection.	[Example] 10000
Blocking Duration (s)	Duration of traffic blocking after an attack is detected.	[Example] 300s
Port Scan Defense	Whether port scan defense is enabled.	[Example] Enabled
Limit (pps)	Threshold for detecting a port scan attack and triggering protection.	[Example] 10000
Blocking Duration (s)	Duration of traffic blocking after an attack is detected.	[Example] 300s
DoS/DDoS Attack Defense (Based on Src. IP)		
Attack defense type.	Defense against SYN flood, UDP flood, ICMP flood, and ICMPv6 flood.	Click an attack defense type to enable defense against the specific attacks. [Example] Select **SYN Flood Attack Defense**.
Src. IP	Global trigger threshold of flood attack	[Example]

Item	Description	Remarks
Blocking Limit (pps)	defense.	2000
Blocking Duration (s)	Duration of traffic blocking after an attack is detected.	[Example] 300s
Action After Detecting Attacks	Action taken after the system detects an attack, including: **Log**: Only record a security log, but not block traffic. **Block**: Only block traffic, but not record a security log.	[Example] Select **Log** and **Block**.
Advanced Defense		
Packet-based Attack	Whether defense against packet-based attacks is enabled.	[Example] All
Filtering out IPv6 Packets with Specific EHs	Filter out the IPv6 packets with the extended headers of the specified type.	[Example] Empty EHs

(4) Click **Save** to complete the configuration of DoS/DDoS attack defense policy.

Follow-up Procedure

- To modify an existing policy, click **Edit**. To delete a policy, click **Delete**. To enable or disable the policy, click the switch.
- To delete multiple policies in a batch, select the policies that you want to delete and click **Delete**.
- To enable multiple policies in a batch, select the policies that you want to enable and click **Enable**.
- To disable multiple policies in a batch, select the policies that you want to disable and click

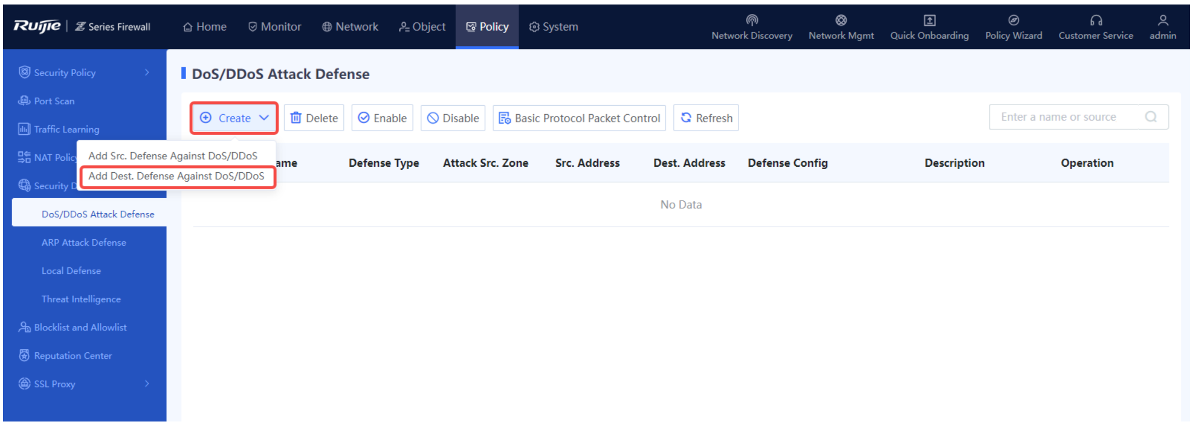
Disable.

- Enter the policy names, policy associated objects, full or part of the policy description in the search box to search for the policies. Fuzzy search is supported.

2. Configuring Destination Defense Against DoS/DDoS

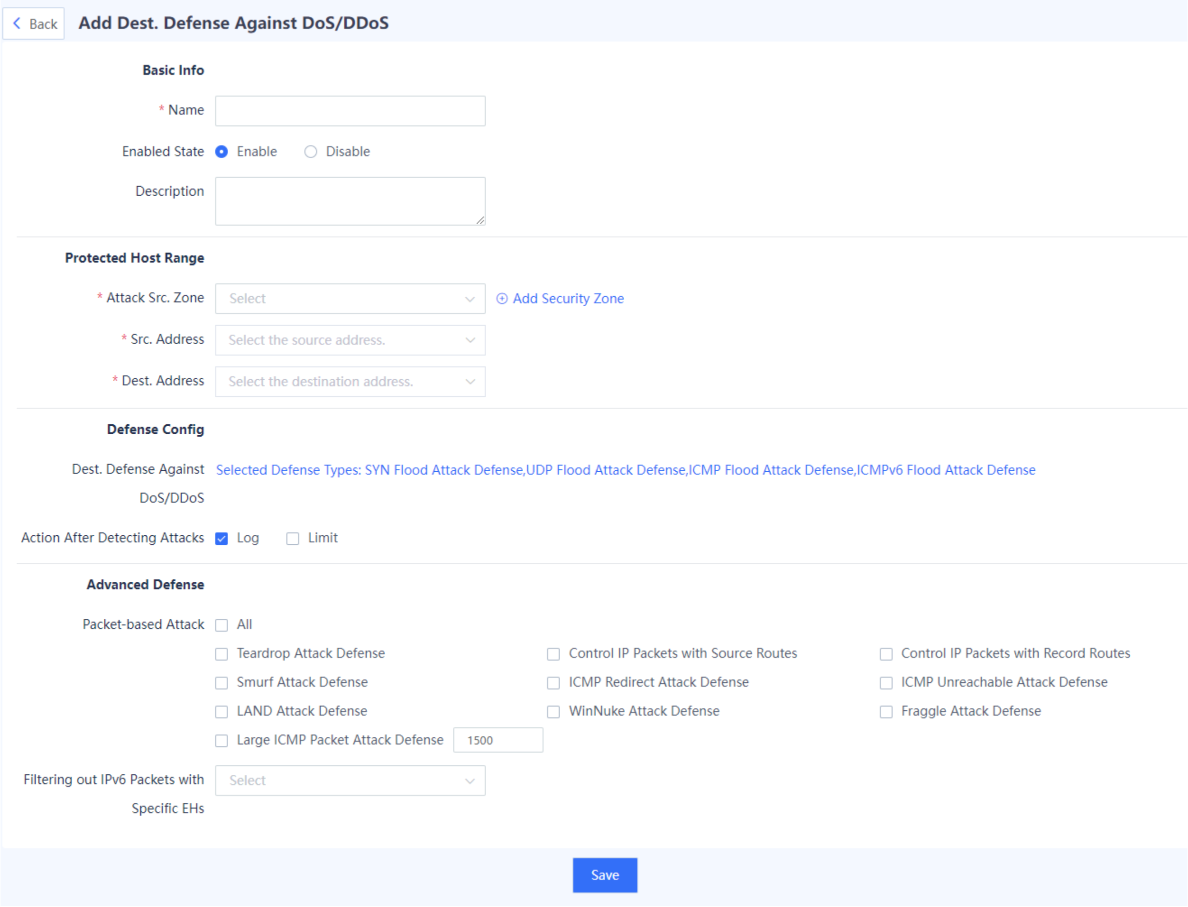
Procedure

(1) Choose **Policy** > **Security Defense** > **DoS/DDoS Attack Defense**.



(2) Above the operation area, click **Create** and select **Add Dest. Defense Against DoS/DDoS**.

The system displays the **Add Dest. Defense Against DoS/DDoS** page.



< Back **Add Dest. Defense Against DoS/DDoS**

Basic Info

* Name

Enabled State ● Enable ○ Disable

Description

Protected Host Range

* Attack Src. Zone Select ⊕ Add Security Zone

* Src. Address Select the source address.

* Dest. Address Select the destination address.

Defense Config

Dest. Defense Against DoS/DDoS Selected Defense Types: SYN Flood Attack Defense,UDP Flood Attack Defense,ICMP Flood Attack Defense,ICMPv6 Flood Attack Defense

Action After Detecting Attacks ☑ Log □ Limit

Advanced Defense

Packet-based Attack □ All

□ Teardrop Attack Defense □ Control IP Packets with Source Routes □ Control IP Packets with Record Routes

□ Smurf Attack Defense □ ICMP Redirect Attack Defense □ ICMP Unreachable Attack Defense

□ LAND Attack Defense □ WinNuke Attack Defense □ Fraggle Attack Defense

□ Large ICMP Packet Attack Defense 1500

Filtering out IPv6 Packets with Specific EHs Select

(3) Set the parameters related to DoS/DDoS attack defense policy.

Item	Description	Remarks
Basic Info		
Name	Name of the DoS/DDoS attack defense policy.	Characters such as \`~!#%^&*+\\\|{};:'"/<>? and spaces are not allowed. [Example] DoS_policy_1
Enabled State	Whether to enable the policy immediately after configuration is completed.	[Example] Enable
Description	Description of the DoS/DDoS attack	Characters such as \`~!#%^&*+\\\|{};:'"/<>? are not

Item	Description	Remarks
	defense policy.	allowed. [Example] New policy
Protected Host Range Range of the attack source associated with the policy. The policy takes effect when matching.		
Attack Src. Zone	The policy checks the traffic from this security zone.	[Example] any
Src. Address	The policy checks the traffic from this address set.	**any** indicates all addresses. [Example] any
Dest. Address	The policy checks the traffic to this address set.	**any** indicates all addresses. [Example] any
Defense Config		
Dest. Defense Against DoS/DDoS		
Attack defense type.	Defense against SYN flood, UDP flood, ICMP flood, and ICMPv6 flood.	Click an attack defense type to enable defense against the specific attacks. [Example] Select **SYN Flood Attack Defense**.
Dest. IP Rate Limit (pps)	Global trigger threshold of flood attack defense.	[Example] 10000

Item	Description	Remarks
Effective Time (s)	Time in which the traffic rate is limited below the threshold after an attack is detected.	[Example] 300s
Action After Detecting Attacks	Action taken after the system detects an attack, including: **Log**: Only record a security log, but not limit the traffic rate. **Limit**: Only limit the traffic rate, but not record a security log.	[Example] Select **Log** and **Limit**.
Advanced Defense		
Packet-based Attack	Whether defense against packet-based attacks is enabled.	[Example] All
Filtering out IPv6 Packets with Specific EHs	Filter out the IPv6 packets with the extended headers of the specified type.	[Example] Empty EHs

(4) Click **Save** to complete the configuration of DoS/DDoS attack defense policy.

Follow-up Procedure

- To modify an existing policy, click **Edit**. To delete a policy, click **Delete**. To enable or disable the policy, click the switch.
- To delete multiple policies in a batch, select the policies that you want to delete and click **Delete**.
- To enable multiple policies in a batch, select the policies that you want to enable and click **Enable**.
- To disable multiple policies in a batch, select the policies that you want to disable and click **Disable**.
- Enter the policy names, policy associated objects, full or part of the policy description in the

search box to search for the policies. Fuzzy search is supported.

7.2.3 Intrusion Prevention

Application Scenario

By performing in-depth detection on the traffic passing the firewall in real time, IPS can report alarms and block traffic in real time to protect user hosts from malicious traffic.

Configuration Points

(1) Customize the intrusion prevention template.

(2) Set the parameters of intrusion prevention template (rule filter).

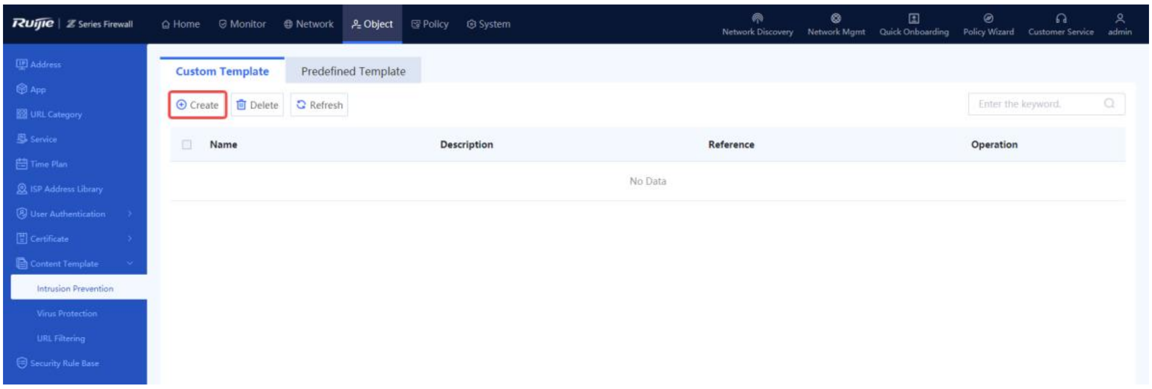
(3) Reference the IPS custom template to security policy and select actions (alarming, blocking, or default action).

Procedure

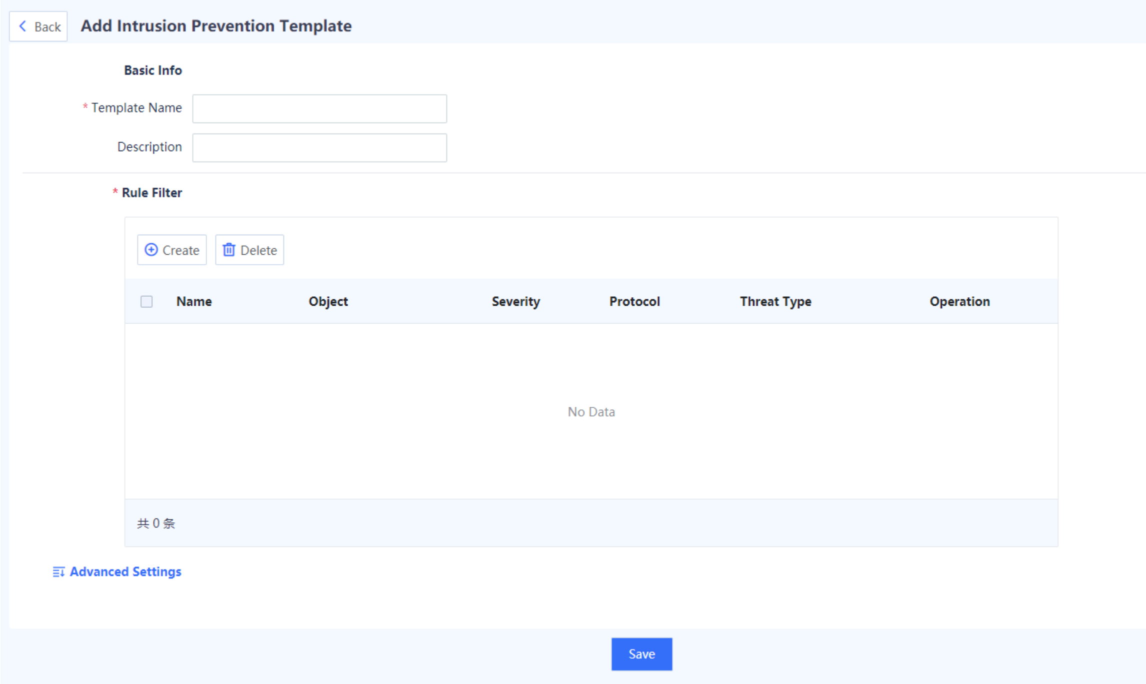
(1) Add an intrusion prevention template.

a Choose **Object** > **Content Template** > **Intrusion Prevention** > **Custom Template**.

b Click **Create** to enter the **Add Intrusion Prevention Template** page.



Name	Description	Reference	Operation
No Data			



Add Intrusion Prevention Template

Basic Info

* Template Name

Description

* Rule Filter

□	Name	Object	Severity	Protocol	Threat Type	Operation

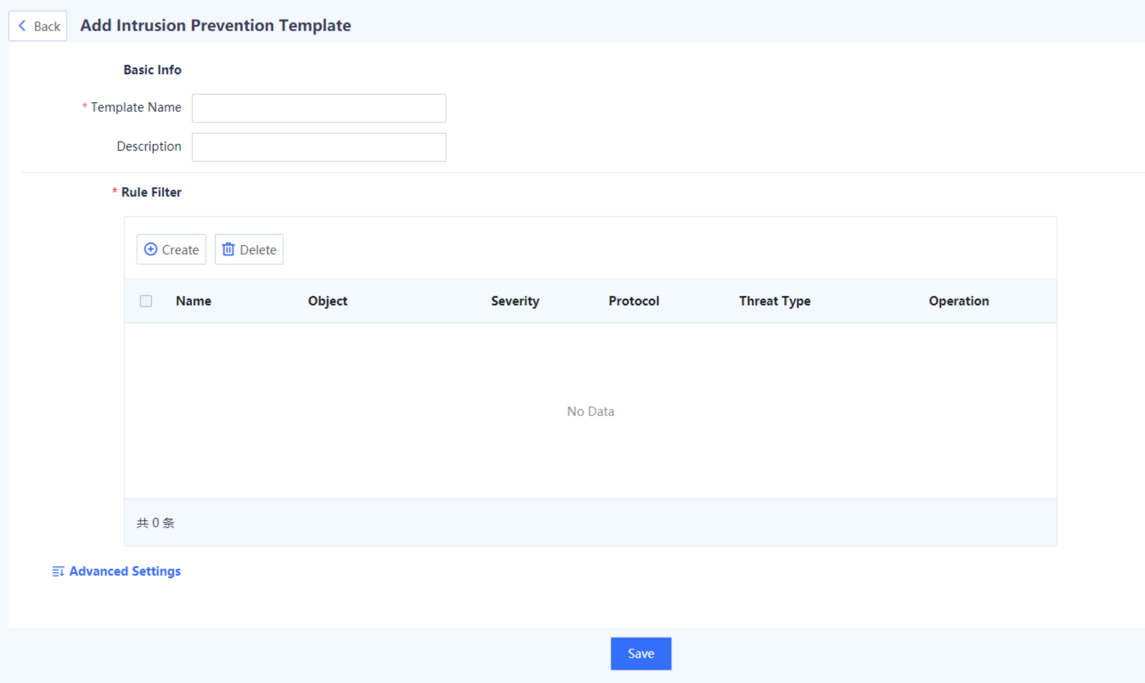
No Data

共 0 条

(2) Add a rule filter and set parameters.

a Enter the name and description of the custom template based on the actual intrusion prevention scenario or protection requirements.

b In the **Rule Filter** area, click **Create**, set parameters, and click **Confirm**.



Add Intrusion Prevention Template

Basic Info

* Template Name

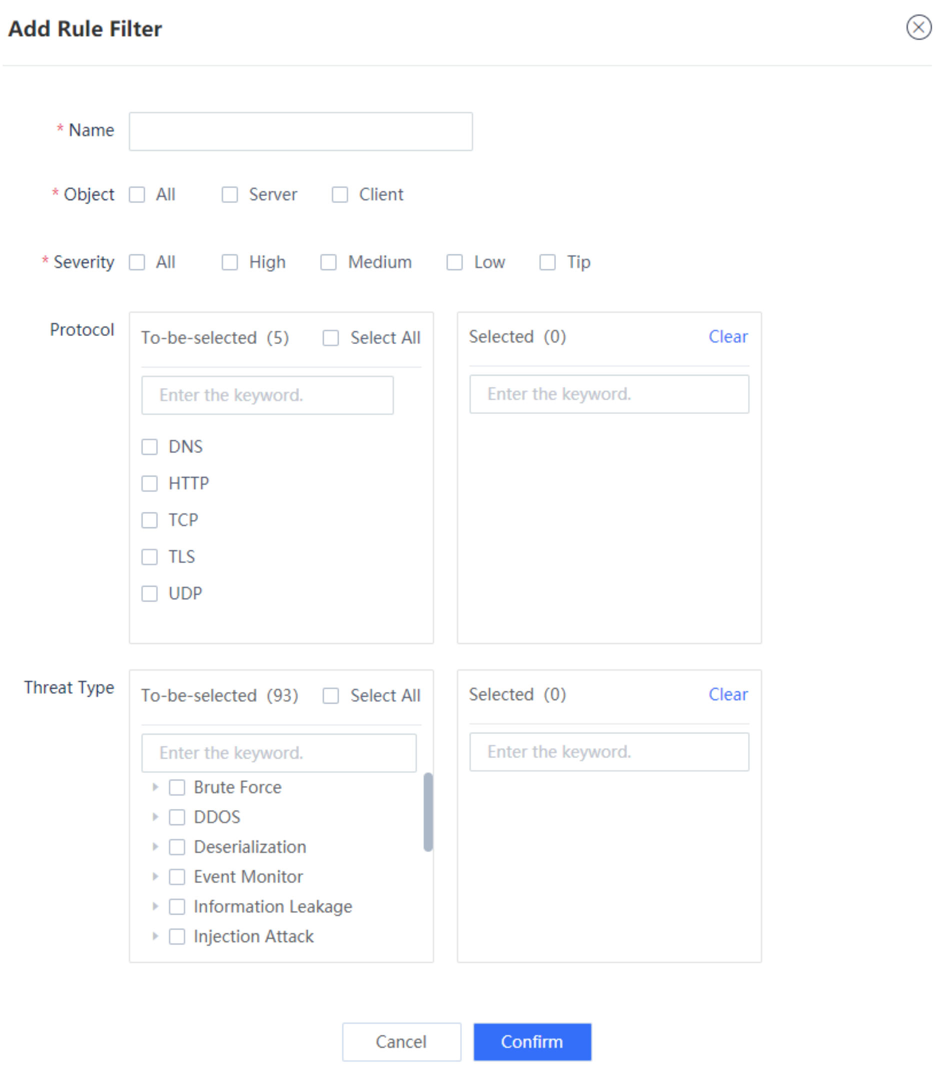
Description

* Rule Filter

□	Name	Object	Severity	Protocol	Threat Type	Operation

No Data

共 0 条



Add Rule Filter ⊗

* Name

* Object □ All □ Server □ Client

* Severity □ All □ High □ Medium □ Low □ Tip

Protocol

To-be-selected (5) □ Select All | Selected (0) Clear

Enter the keyword. | Enter the keyword.

□ DNS
□ HTTP
□ TCP
□ TLS
□ UDP

Threat Type

To-be-selected (93) □ Select All | Selected (0) Clear

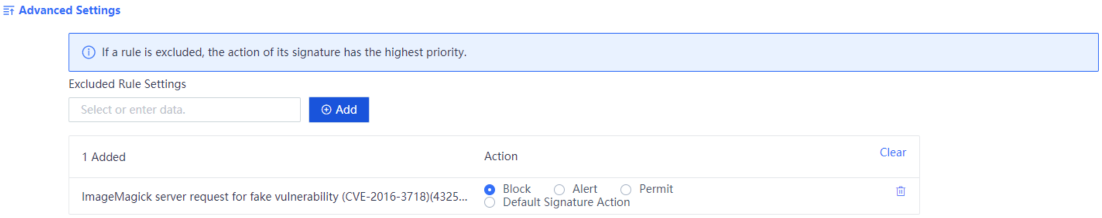
Enter the keyword. | Enter the keyword.

▸ □ Brute Force
▸ □ DDOS
▸ □ Deserialization
▸ □ Event Monitor
▸ □ Information Leakage
▸ □ Injection Attack

- **Name**: Customized. You are advised to configure a name that can describe the filter function.
- **Object**: Objects to be protected.
- **Severity**: Defense severity. For example, if only **High** is selected, only the security rules with high severity can hit the filter.
- **Protocol**: Protocols to be detected. The protocol traffic that is not specified does not hit the filter.
- **Threat Type**: Types of threats to be detected. The threat traffic that is not specified does not hit the filter. If you have no special protection requirements, select all.

c (Optional) Click ☰ before **Advanced Settings** to expand the advanced settings.

Click the input box to select excluded rules, click **Add**, and configure the action for the rule in the list. After a rule is configured as excluded, the action of the excluded rule is taken on the packets that hit the rule, but the action set in the template does not take effect.



Advanced Settings

ⓘ If a rule is excluded, the action of its signature has the highest priority.

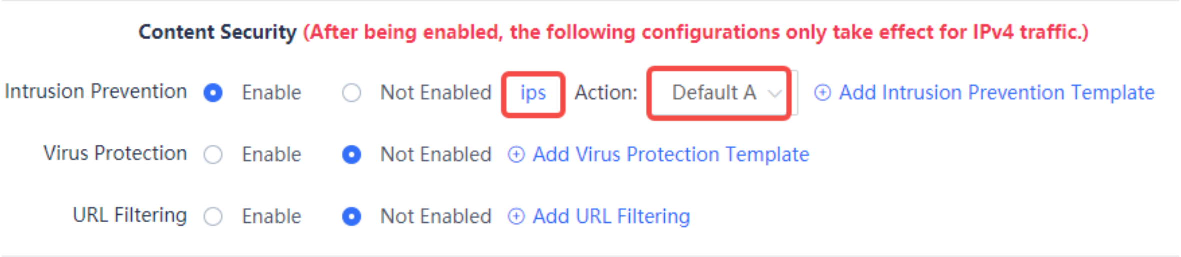
Excluded Rule Settings

Select or enter data. [⊕ Add]

1 Added	Action	Clear
ImageMagick server request for fake vulnerability (CVE-2016-3718)(4325...	● Block ○ Alert ○ Permit ○ Default Signature Action	🗑

d Click **Save** to complete the configuration of intrusion prevention template.

(3) Choose **Policy** > **Security Policy** > **Create Security Policy** to associate the security policy with intrusion prevention. Configure the template as predefined, set the action to alarming, blocking, or default (default action refers to the recommended action predefined in the system in Security Rule Base.

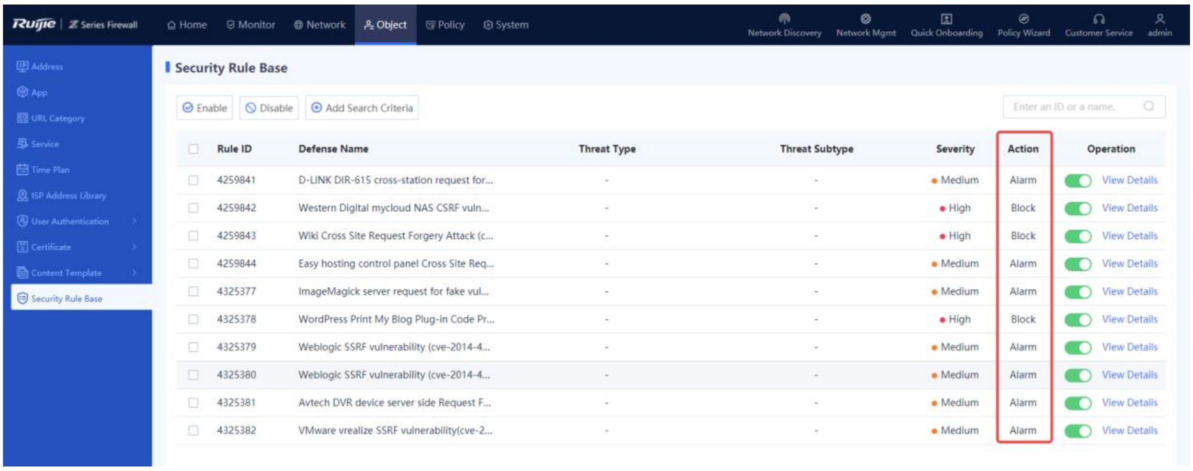


Content Security (After being enabled, the following configurations only take effect for IPv4 traffic.)

Intrusion Prevention ● Enable ○ Not Enabled ips Action: Default A ⊕ Add Intrusion Prevention Template

Virus Protection ○ Enable ● Not Enabled ⊕ Add Virus Protection Template

URL Filtering ○ Enable ● Not Enabled ⊕ Add URL Filtering



Security Rule Base

Enable | Disable | Add Search Criteria | Enter an ID or a name.

□	Rule ID	Defense Name	Threat Type	Threat Subtype	Severity	Action	Operation
□	4259841	D-LINK DIR-615 cross-station request for...	-	-	● Medium	Alarm	View Details
□	4259842	Western Digital mycloud NAS CSRF vuln...	-	-	● High	Block	View Details
□	4259843	Wiki Cross Site Request Forgery Attack (c...	-	-	● High	Block	View Details
□	4259844	Easy hosting control panel Cross Site Req...	-	-	● Medium	Alarm	View Details
□	4325377	ImageMagick server request for fake vul...	-	-	● Medium	Alarm	View Details
□	4325378	WordPress Print My Blog Plug-in Code Pr...	-	-	● High	Block	View Details
□	4325379	Weblogic SSRF vulnerability (cve-2014-4...	-	-	● Medium	Alarm	View Details
□	4325380	Weblogic SSRF vulnerability (cve-2014-4...	-	-	● Medium	Alarm	View Details
□	4325381	Avtech DVR device server side Request F...	-	-	● Medium	Alarm	View Details
□	4325382	VMware vrealize SSRF vulnerability(cve-2...	-	-	● Medium	Alarm	View Details

7.2.4 Virus Protection

Application Scenario

If intranet users often download various application data from the Internet or the intranet servers often need to receive data uploaded by Internet users, you can configure virus protection policies on the firewall to detect virus in the passing traffic and configure real-time alarming and blocking to protect user hosts from malicious traffic.

Caution

The virus protection function is supported from NTOS1.0R3. If your version is lower than NTOS1.0R3, upgrade it to NTOS1.0R3 or higher.

Configuration Points

(1) Customize the virus protection template.

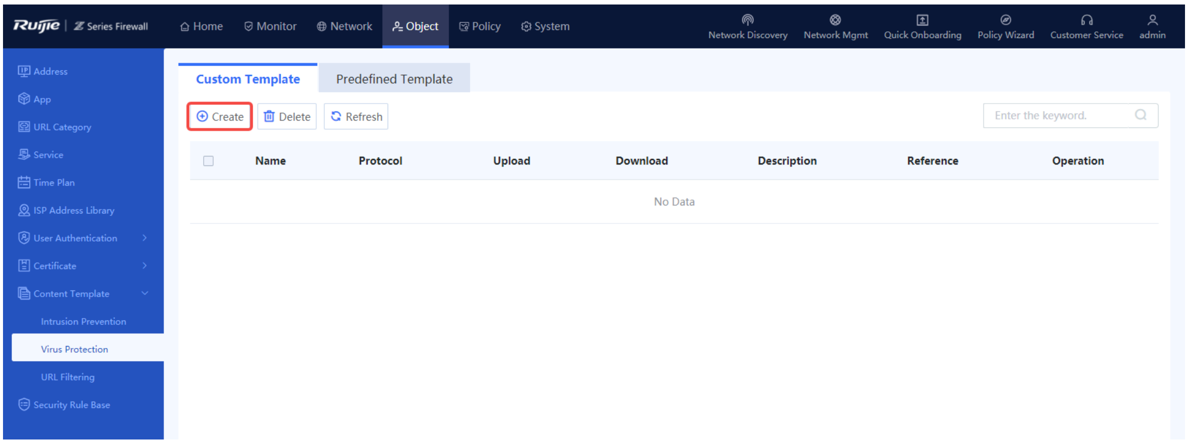
(2) Reference the virus protection template to security policy and select actions (alarming or blocking).

(3) To detect HTTPS traffic, you need to configure the SSL proxy function. For more information about SSL proxy, see 7.3 Configuring SSL Proxy Policies.

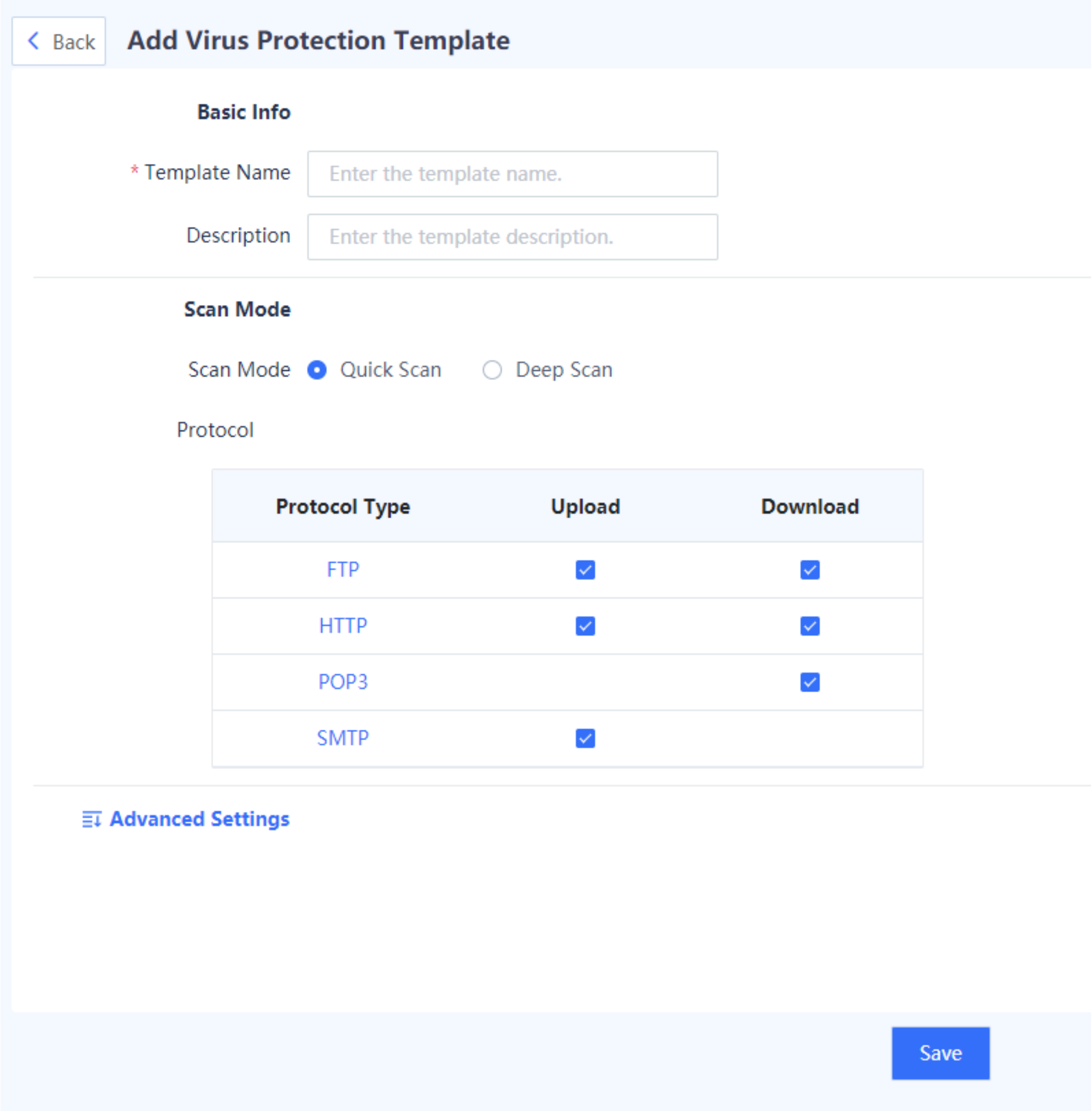
Procedure

(1) Add a virus protection template.

Choose **Object** > **Content Template** > **Virus Protection** > **Custom Template**. Above the operation area, click **Create**.



□	Name	Protocol	Upload	Download	Description	Reference	Operation
				No Data			



Basic Info

* Template Name: Enter the template name.

Description: Enter the template description.

Scan Mode

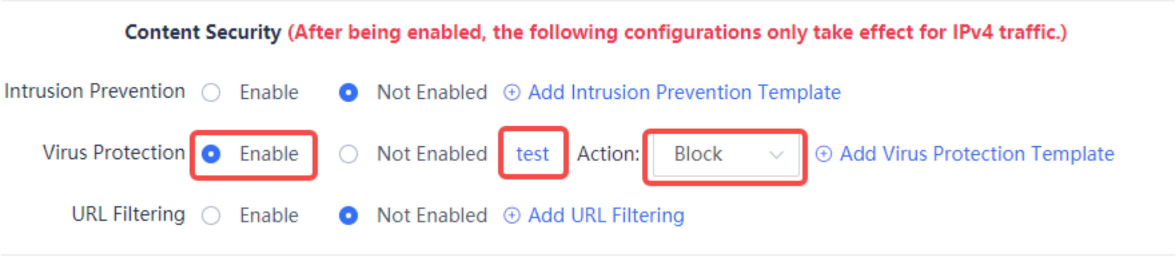
Scan Mode ● Quick Scan ○ Deep Scan

Protocol

Protocol Type	Upload	Download
FTP	☑	☑
HTTP	☑	☑
POP3		☑
SMTP	☑	

- **Quick Scan**: Use the **Virus Protection Signature Library (Quick Scan)**. The virus detection rate is low but the performance overhead is small.
- **Deep Scan**: Use the **Virus Protection Signature Library (Deep Scan)**. The virus detection rate is high but the performance overhead is large.
- **Protocol**: Detect virus for the uploaded or downloaded packets of the specified protocol. The packets of unspecified protocols are forwarded directly without virus detection.
- If the specified MD5 value or application is configured as excluded, the firewall will directly forward the packets of the specified MD5 value or application.

(2) Choose **Policy** > **Security Policy** > **Create Security Policy** to associate the security policy with virus protection. Select a virus protection template and set the action to Alarm or Block.



Content Security (After being enabled, the following configurations only take effect for IPv4 traffic.)

Intrusion Prevention ○ Enable ● Not Enabled ⊕ Add Intrusion Prevention Template

Virus Protection ● Enable ○ Not Enabled test Action: Block ⊕ Add Virus Protection Template

URL Filtering ○ Enable ● Not Enabled ⊕ Add URL Filtering

7.2.5 ARP Attack Defense

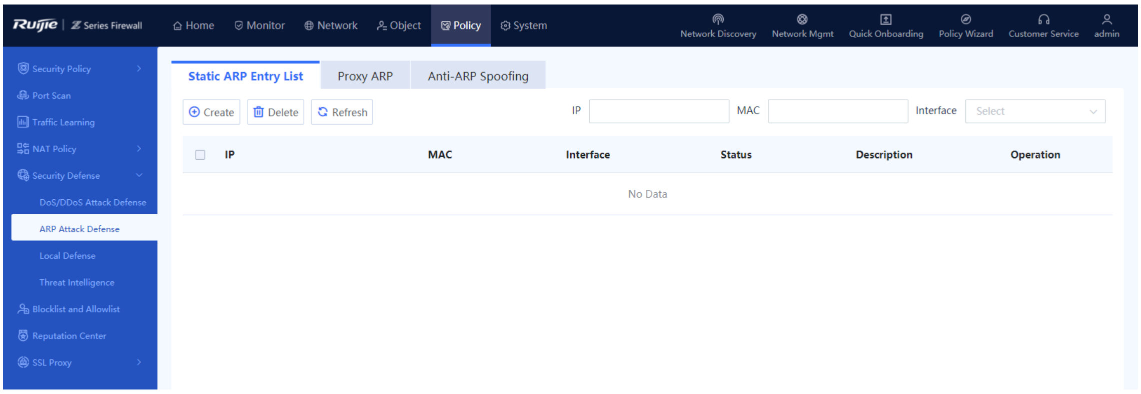
1. Configuring Static ARP

Application Scenario

Configuring static ARP entries can protect ARP entries from being modified by received forged gratuitous ARP packets or ARP response packets.

Procedure

(1) Choose **Policy** > **Security Defense** > **ARP Attack Defense** > **Static ARP Entry List**.



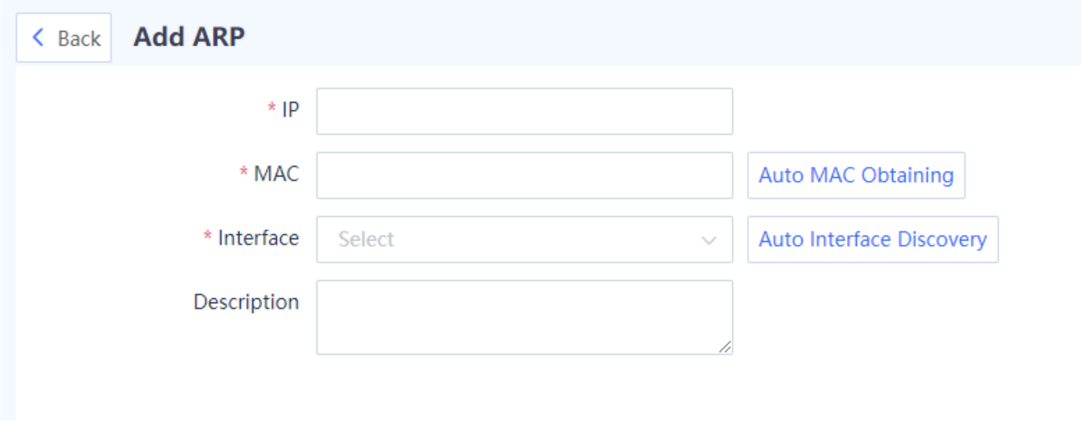
IP MAC Interface Select

□	IP	MAC	Interface	Status	Description	Operation
No Data						

The static ARP entries configured on the device are displayed. The **Status** column shows whether the interfaces bound to the entries are valid or invalid.

(2) Above the operation area, click **Create**.

The system displays the **Add ARP** page.



(3) Configure the basic information of the static ARP entry.

Item	Description	Remarks
IP	IP address to be bound to the static ARP entry.	[Example] 192.168.10.3
MAC	MAC address to be bound to the static ARP entry.	Two configuration methods are supported: ● Fill in the information manually. ● Click **Auto MAC Obtaining**. The device will search for the MAC address matching the IP address according to the available ARP entry information. If no address is found, the system displays "No address is matched." [Example] 11:22:33:44:55:66
Interfac e	Physical interface to be bound.	Two configuration methods are supported: ● Fill in the information manually. ● Click **Auto Interface Discovery**. The device will configure the interface that may match the IP address according to the related information. If no interface is found, the system displays "No interface is matched." [Example] Ge0/1

(4) Click **Save** to complete the configuration of static ARP policy.

Follow-up Procedure

- To edit an existing policy, click **Edit**.
- To delete multiple policies in a batch, select the policies that you want to delete and click **Delete**.
- Enter the related parameters in the search box to filter the query result.

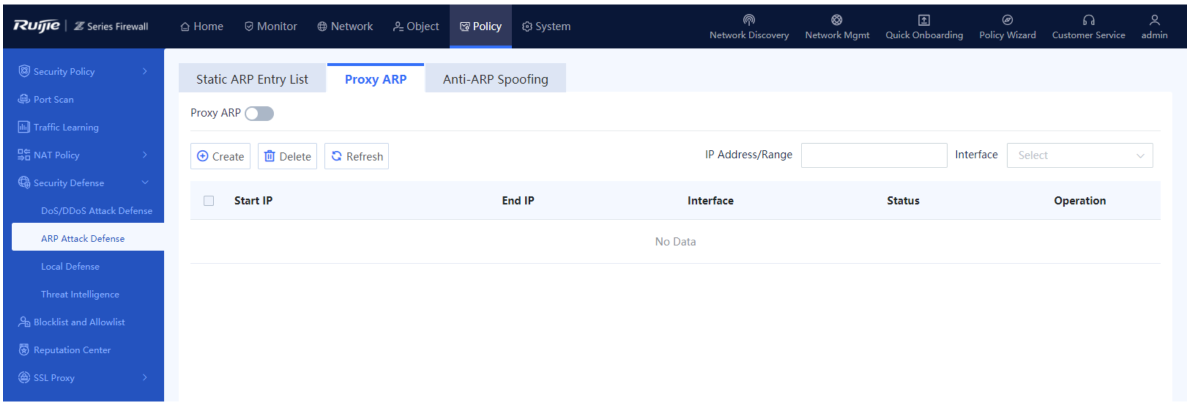
2. Configuring Proxy ARP

Application Scenario

When receiving an ARP request from the interface proxy network segment, the firewall responds and provides the MAC address of the interface.

Procedure

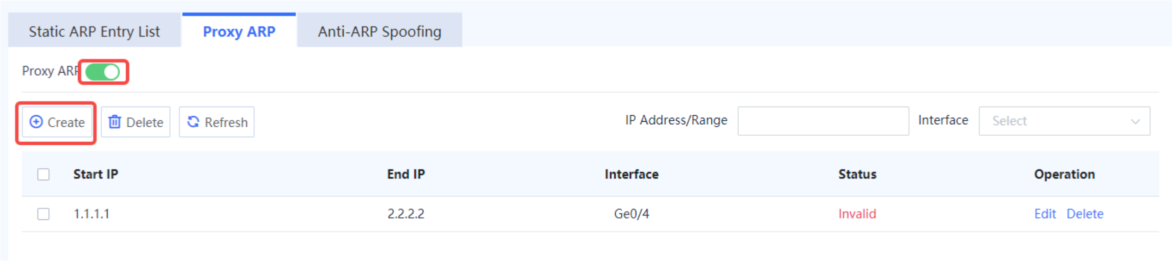
(1) Choose **Policy** > **Security Defense** > **ARP Attack Defense** > **Proxy ARP**.



□	Start IP	End IP	Interface	Status	Operation
No Data					

The proxy ARP network segments configured on the device are displayed. The **Status** column shows whether the interfaces bound to the entries are valid or invalid.

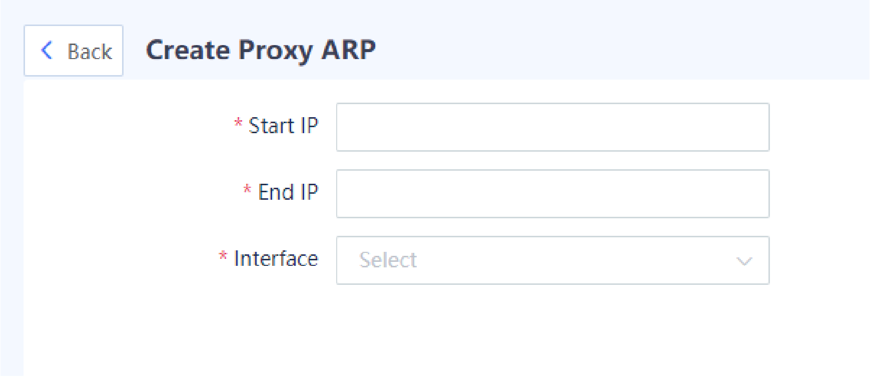
(2) Enable **Proxy ARP**.



□	Start IP	End IP	Interface	Status	Operation
□	1.1.1.1	2.2.2.2	Ge0/4	Invalid	Edit Delete

(3) Click **Create**.

The system displays the **Create Proxy ARP** page.



Back

Create Proxy ARP

* Start IP

* End IP

* Interface: Select

(4) Fill in the start IP address and end IP address of proxy and select the proxy interface.

(5) Click **Save** to complete the configuration of proxy ARP.

Follow-up Procedure

- To modify an existing proxy ARP configuration, click **Edit**.
- To delete multiple policies in a batch, select the policies that you want to delete and click **Delete**.

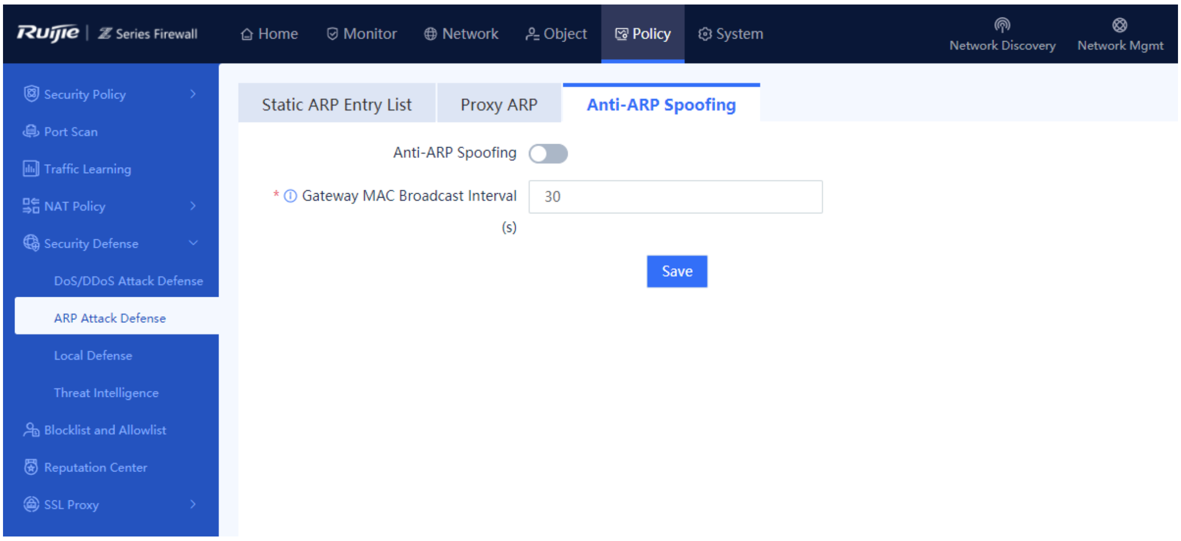
3. Configuring Anti-ARP Spoofing

Application Scenario

The firewall periodically sends gratuitous ARP broadcast packets to allow terminals on the same network segment to obtain the correct MAC address of the firewall, thus preventing attackers from forging the gateway.

Procedure

(1) Choose **Policy** > **Security Defense** > **ARP Attack Defense** > **Anti-ARP Spoofing**.



Anti-ARP Spoofing

* Gateway MAC Broadcast Interval (s): 30

(2) Enable **Anti-ARP Spoofing**.

(3) Modify **Gateway MAC Broadcast Interval**. The unit is second.

(4) Click **Save** to save the configuration.

7.2.6 Local Defense

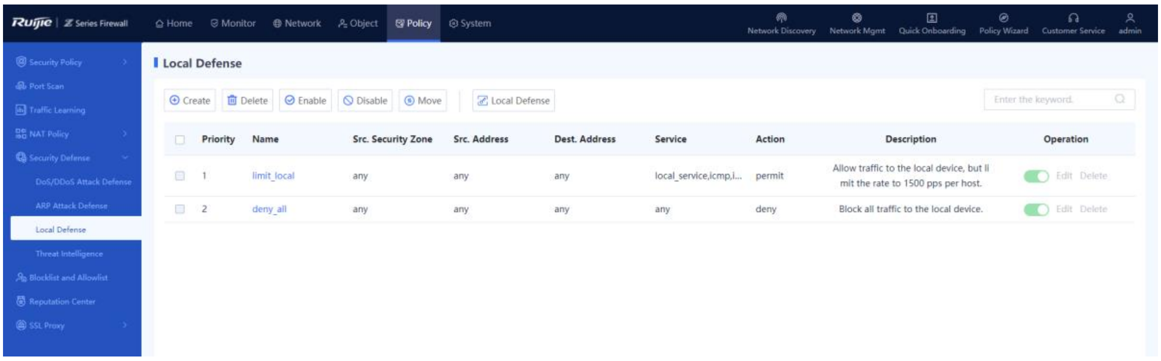
Application Scenario

The local defense function can block or restrict specified types of packets sent to the local device. For example, you can specify the ping packets in the traffic sent to the local device. Then the device directly discards the ping packets to forbid any ping operation to the local device, thus ensuring the normal running of the device.

The local defense function has two default policies that cannot be modified to ensure that the device is protected from traffic attacks after this function is delivered.

Procedure

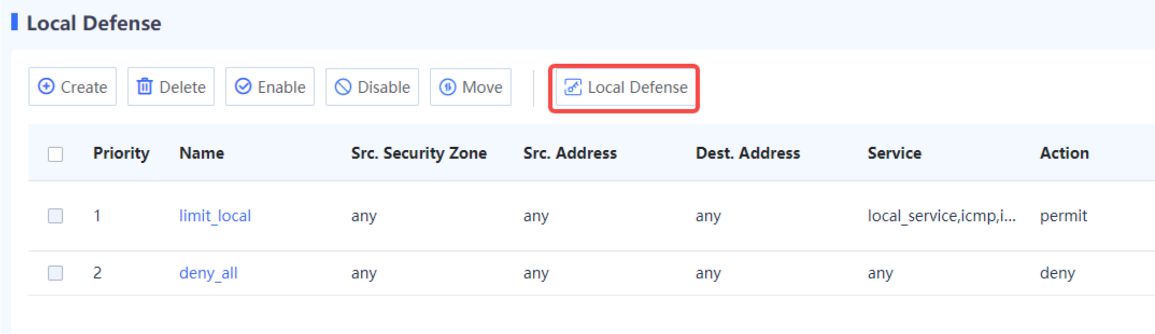
(1) Choose **Policy** > **Security Defense** > **Local Defense**.



Local Defense

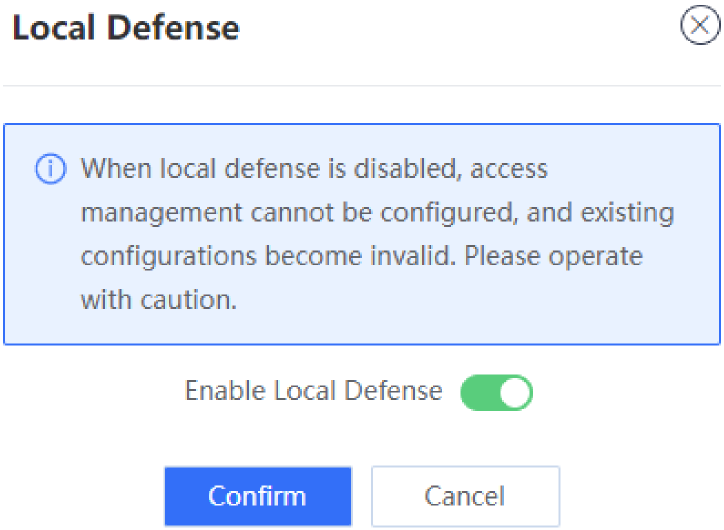
□	Priority	Name	Src. Security Zone	Src. Address	Dest. Address	Service	Action	Description	Operation
□	1	limit_local	any	any	any	local_service,icmp,i...	permit	Allow traffic to the local device, but li mit the rate to 1500 pps per host.	Edit Delete
□	2	deny_all	any	any	any	any	deny	Block all traffic to the local device.	Edit Delete

(2) Click **Local Defense**. Toggle on **Enable Local Defense** and click **Confirm**.



Local Defense

□	Priority	Name	Src. Security Zone	Src. Address	Dest. Address	Service	Action
□	1	limit_local	any	any	any	local_service,icmp,i...	permit
□	2	deny_all	any	any	any	any	deny

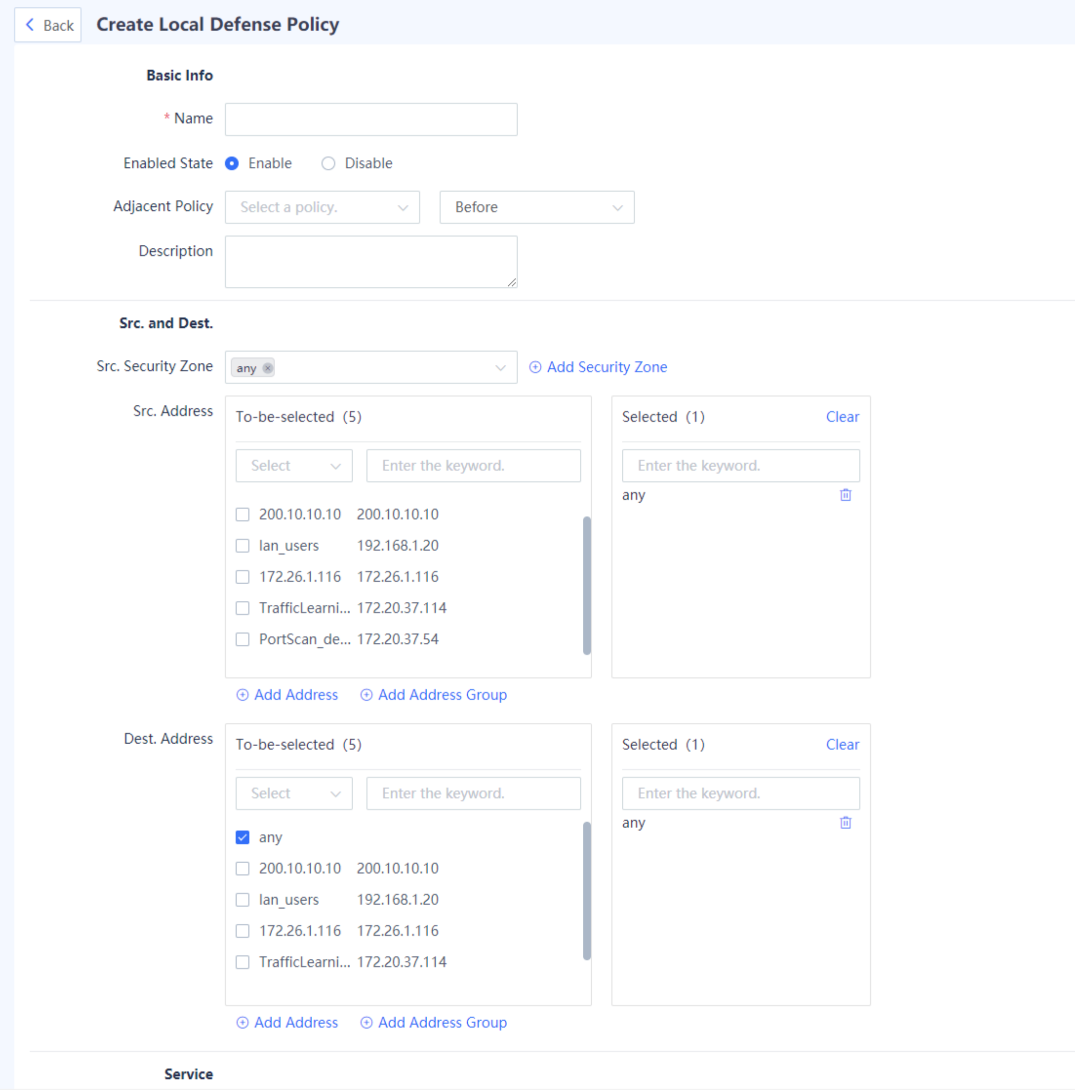


Local Defense

When local defense is disabled, access management cannot be configured, and existing configurations become invalid. Please operate with caution.

Enable Local Defense ●

(3) Click **Create** to enter the **Create Local Defense Policy** page.



Create Local Defense Policy

Basic Info

* Name

Enabled State ● Enable ○ Disable

Adjacent Policy Select a policy. Before

Description

Src. and Dest.

Src. Security Zone any

Src. Address

To-be-selected (5)

□ 200.10.10.10	200.10.10.10
□ lan_users	192.168.1.20
□ 172.26.1.116	172.26.1.116
□ TrafficLearni...	172.20.37.114
□ PortScan_de...	172.20.37.54

Selected (1): any

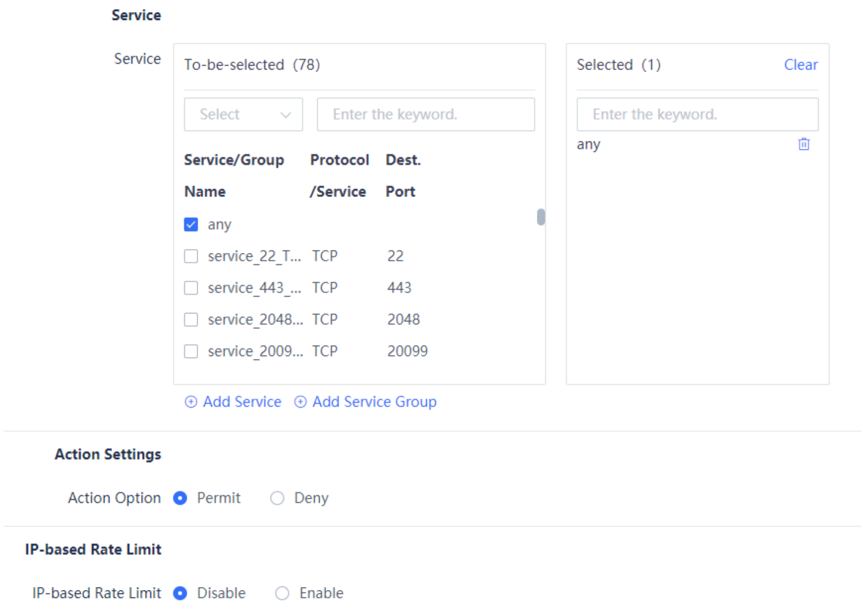
Dest. Address

To-be-selected (5)

☑ any	
□ 200.10.10.10	200.10.10.10
□ lan_users	192.168.1.20
□ 172.26.1.116	172.26.1.116
□ TrafficLearni...	172.20.37.114

Selected (1): any

Service



Service

Service

To-be-selected (78)

Select | Enter the keyword.

Service/Group Name	Protocol /Service	Dest. Port
☑ any		
□ service_22_T...	TCP	22
□ service_443_...	TCP	443
□ service_2048...	TCP	2048
□ service_2009...	TCP	20099

Selected (1) Clear

Enter the keyword.

any

⊕ Add Service ⊕ Add Service Group

Action Settings

Action Option ● Permit ○ Deny

IP-based Rate Limit

IP-based Rate Limit ● Disable ○ Enable

(4) Set the parameters of local defense policy.

Item	Description	Remarks
Basic Info		
Name	Name of the local defense policy.	Characters such as \`~!#%^&*+|{};:'"/<>? and spaces are not allowed. [Example] policy_1
Enabled State	Whether the policy is enabled in the system.	[Example] Enable
Adjacent Policy	Move the new policy before or after the specified policy. The closer a policy is to the front, the higher its priority is in matching.	-
Description	Security policy description.	Characters such as \`~!#%^&*+|{};:'"/<>? are not allowed.
Src. and Dest. Associate the policy with source security zone, source address object, destination address object, and service object. The policy takes effect when all the four items are hit.		
Src. Security Zone	The policy checks the traffic from this zone.	**any** indicates traffic of all zones. [Example] any
Src. Address	The policy checks the traffic from this address set.	**any** indicates all addresses. [Example] any

Dest. Address	The policy checks the traffic to this address set.	**any** indicates all addresses. [Example] any
Service	The policy checks the traffic of this service.	**any** indicates all services. [Example] any
Action Settings		
Action Option	Action taken on the traffic that hits the policy.	[Example] Permit
IP-based Rate Limit		
IP-based Rate Limit	Whether to restrict the number of packets that can pass per second in the traffic matching the policy. ● **Disable**: not restricted ● **Enable**: restricted. The **Packets Allowed to Pass Through Each Host (pps)** field needs to be set.	[Example] Disable

(5) Click **Save**.

Follow-up Procedure

- To delete multiple policies in a batch, select the policies that you want to delete and click **Delete** in the above bar.
- To enable multiple policies in a batch, select the policies that you want to enable and click **Enable** in the above bar.
- To disable multiple policies in a batch, select the policies that you want to disable and click **Disable** in the above bar.

- To adjust the policy priority, click **Move**. The closer a policy is to the front, the higher its priority is in matching.
- Enter the policy names, policy associated objects, full or part of the policy description in the search box to search for the policies. Fuzzy search is supported.

7.2.7 Threat Intelligence

1. Overview

Most of the typical security capabilities (such as AV and IPS) of firewalls are based on the analysis of traffic content. The firewalls use regularly updated signatures, rules and other information for detection, which has problems such as large detection costs and difficulty in dealing with new network threats such as Advanced Persistent Threat (APT) and zero-day vulnerabilities.

Threat Intelligence (TI) introduces real-time and global security threat knowledge to firewalls, enabling the firewalls to identify and filter out malicious traffic with less computing overhead. Therefore, TI becomes an indispensable part of the multi-layer security defense system of firewalls.

The TI module can match threat intelligence based on the destination IP address of the traffic and the domain name in the DNS query, and perform blocking or alarming actions on the data that matches the threat intelligence, to block malicious IP addresses and domain names.

⚠ **Caution**

The TI function is supported from NTOS1.0R4. If your version is lower than NTOS1.0R4, upgrade it to NTOS1.0R4 or higher.

2. Enabling TI

Application Scenario

Enable the TI function on the firewall to block and alarm malicious IP traffic and malicious domain name query traffic, thus improving security defense effects.

Prerequisites

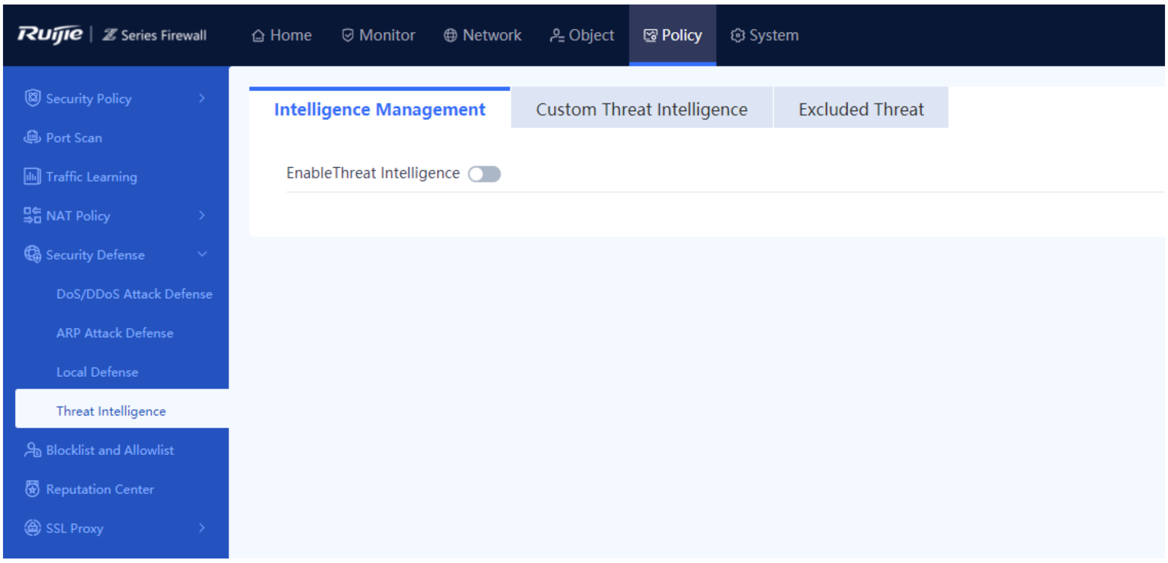
You have been authorized and activated the TI capability.

ℹ **Note**

If the TI function is not authorized or authorization expires, the detection based on threat intelligence signature library is unavailable, and only the custom TI configured manually can be used. In this case, the threat intelligence signature library cannot be upgraded.

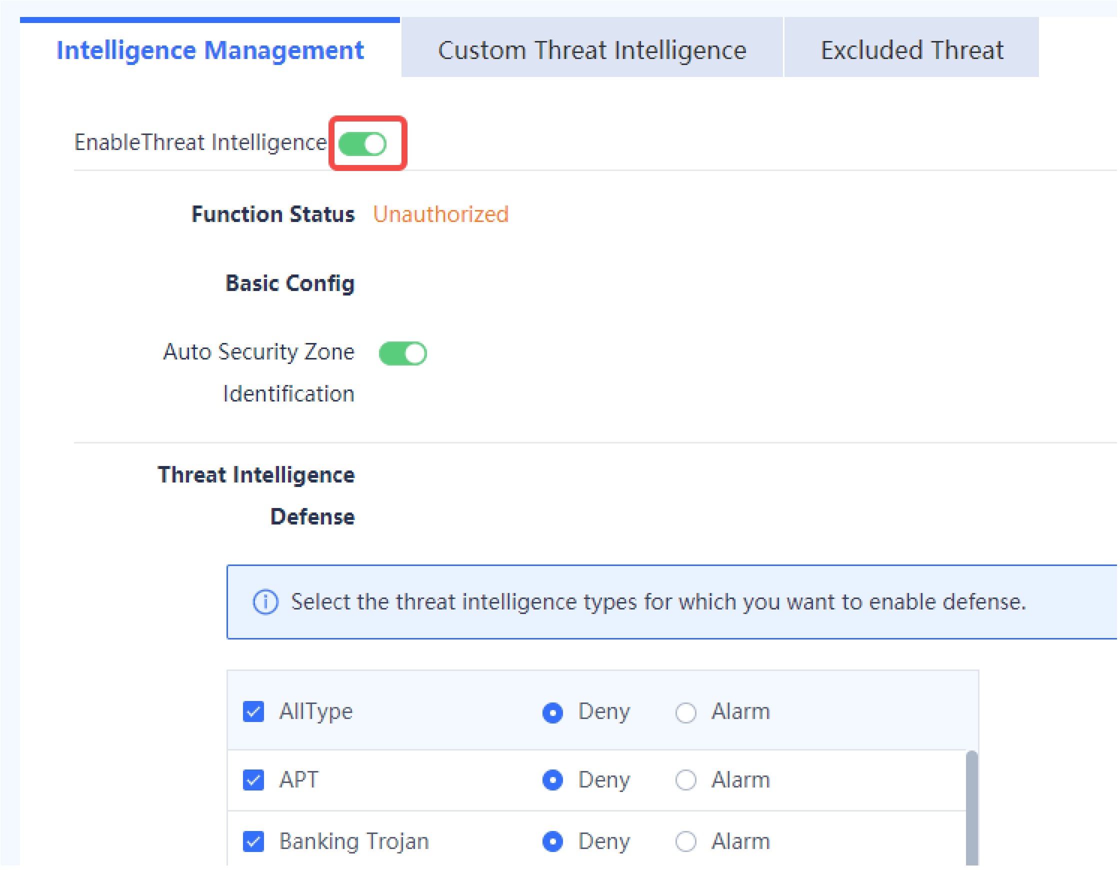
Procedure

(1) Choose **Policy** > **Security Defense** > **Threat Intelligence** > **Intelligence Management**.



EnableThreat Intelligence

(2) Click to enable the TI function.



EnableThreat Intelligence

Function Status Unauthorized

Basic Config

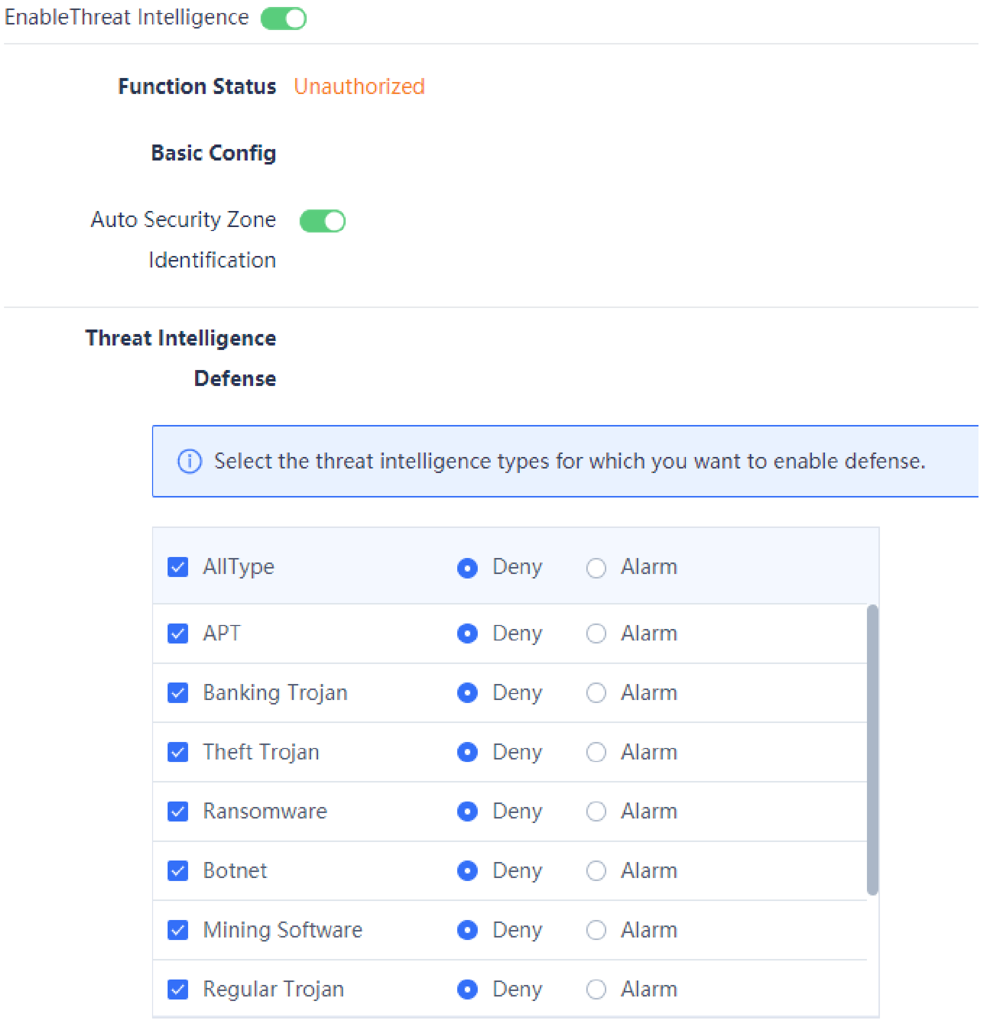
Auto Security Zone Identification

Threat Intelligence Defense

ⓘ Select the threat intelligence types for which you want to enable defense.

☑ AllType	● Deny	○ Alarm
☑ APT	● Deny	○ Alarm
☑ Banking Trojan	● Deny	○ Alarm

(3) Set the parameters of TI.



EnableThreat Intelligence ●

Function Status Unauthorized

Basic Config

Auto Security Zone Identification ●

Threat Intelligence Defense

ⓘ Select the threat intelligence types for which you want to enable defense.

☑ AllType	● Deny	○ Alarm
☑ APT	● Deny	○ Alarm
☑ Banking Trojan	● Deny	○ Alarm
☑ Theft Trojan	● Deny	○ Alarm
☑ Ransomware	● Deny	○ Alarm
☑ Botnet	● Deny	○ Alarm
☑ Mining Software	● Deny	○ Alarm
☑ Regular Trojan	● Deny	○ Alarm

Item	Description	Remarks
Function Status	Current status of the TI function ● **Unauthorized**: The TI function license is not activated, or online authorization fails. ● **Normal**: The TI function license is activated. The function is available and the library can be updated. ● **Server Error**: The TI function license is activated, but the secure cloud platform cannot connect to the threat	The status is displayed automatically according to the current TI function status. [Example] Normal

Item	Description	Remarks
	intelligence signature library update server. The threat intelligence signature library cannot be updated.	
Basic Config		
Auto Security Zone Identification	Whether to identify the traffic inbound and outbound security zones automatically. ● After this function is enabled, the device automatically identifies the inbound and outbound security zones (ingress and egress) of traffic, and determines whether to perform threat signature matching for the traffic. ● If this function is disabled, you can manually specify the effective security zones for TI.	[Example] Enabled
Effective Security Zone	After the effective security zone is specified, the system performs TI matching and processing (block or alarm) for the traffic only when the outbound security zone of the traffic is the same as the specified zone.	When **Auto Security Zone Identification** is disabled, this parameter needs to be configured. [Example] untrust
Threat Intelligence Defense		
Type	Select the TI type to defend against.	Select to enable defense. [Example] APT
Action	Action to be taken on the traffic matching the TI:	[Example] Deny

Item	Description	Remarks
	● **Deny**: Block traffic and record a security log. ● **Alarm**: Not block traffic, but record a security log.	

(4) Click **Save** to complete the configuration.

3. Customizing Threat Intelligence

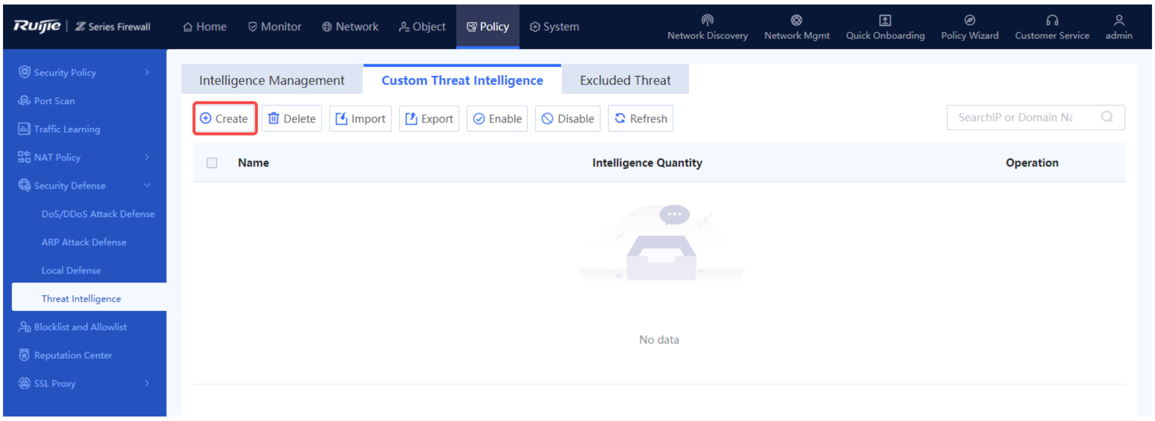
Application Scenario

In addition to the threat intelligence contained in the threat intelligence signature library, the system allows you to import malicious intelligence that you have collected. When threat is detected, the system matches the threat against the custom threat intelligence first. The data matching custom threat intelligence is blocked and a security log is recorded.

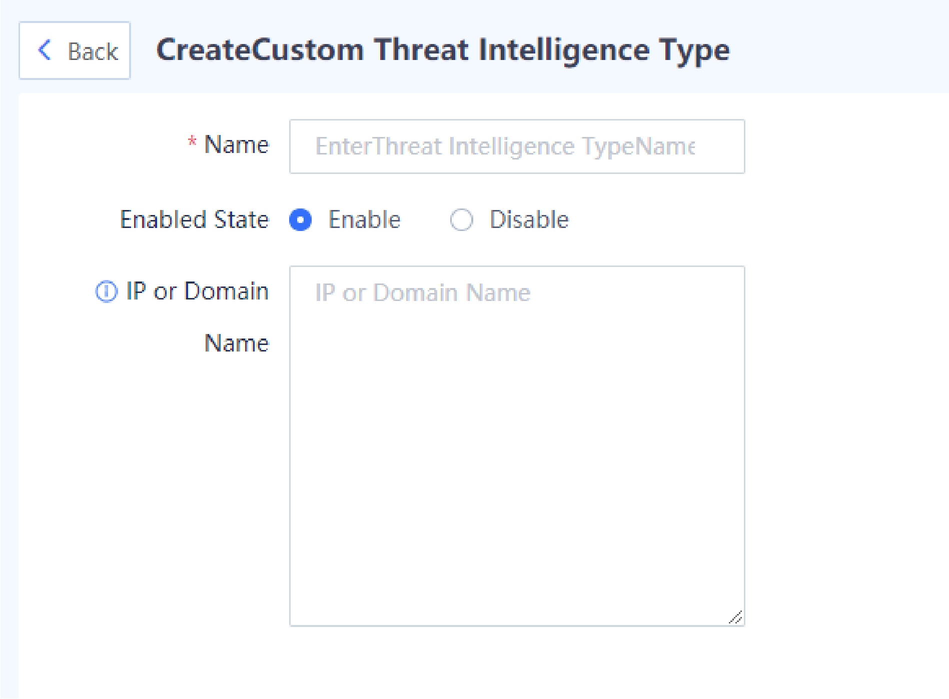
In the unauthorized state, custom threat intelligence can still be used for matching.

- Manually configure the custom TI.

(1) Choose **Policy** > **Security Defense** > **Threat Intelligence** > **Custom Threat Intelligence**.



(2) Click **Create** to enter the **Create Custom Threat Intelligence Type** page.



< Back **CreateCustom Threat Intelligence Type**

* Name: EnterThreat Intelligence TypeName

Enabled State ● Enable ○ Disable

ⓘ IP or Domain Name: IP or Domain Name

(3) Set the parameters of custom TI.

Item	Description	Remarks
Name	Name of the custom TI.	[Example] Trojan
Enabled Status	Whether to enable the TI. The disabled TI will not be matched.	[Example] Enable
IP or Domain Name	IP address or DNS name to be checked and blocked.	● If multiple IP addresses or domain names need to be configured, enter one IP address or domain name per line, and press **Enter** to separate lines. ● The domain name matching rule is full match. [Example] www.xxx.com

(4) Click **Save** to complete the configuration.

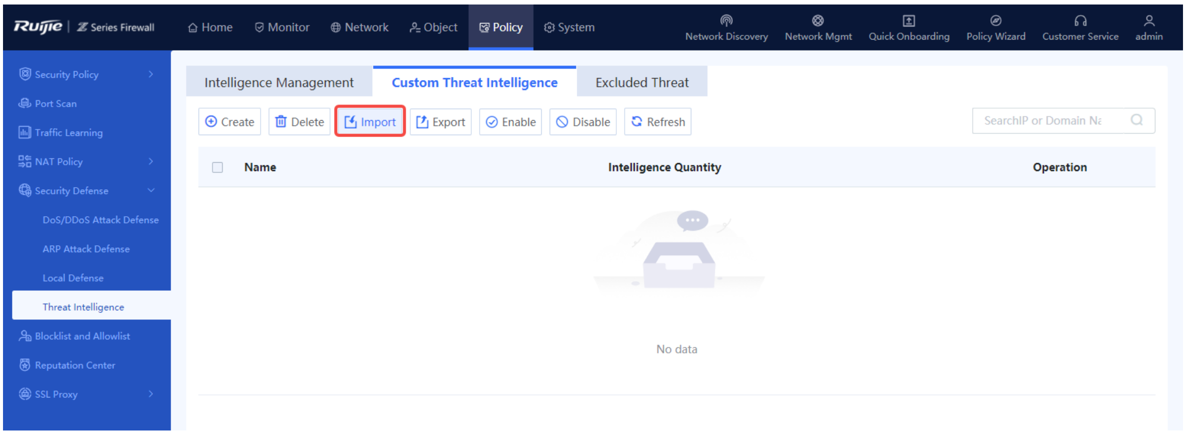
- Batch import custom TI.

Application Scenario

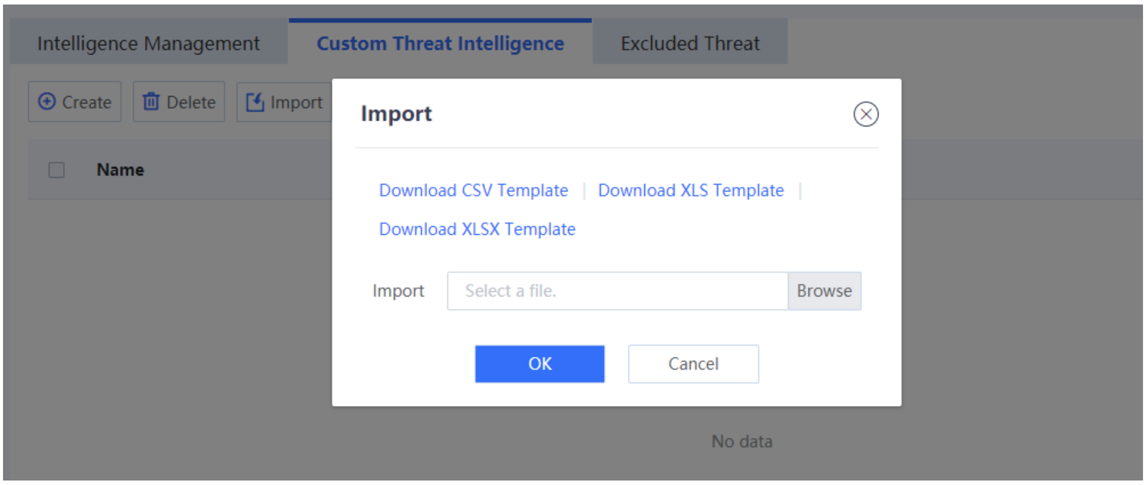
When you need to add a large number of TI types, you can fill in TI information in a template, and import them in a batch with one click.

Procedure

(1) Choose **Policy** > **Security Defense** > **Threat Intelligence** > **Custom Threat Intelligence**.

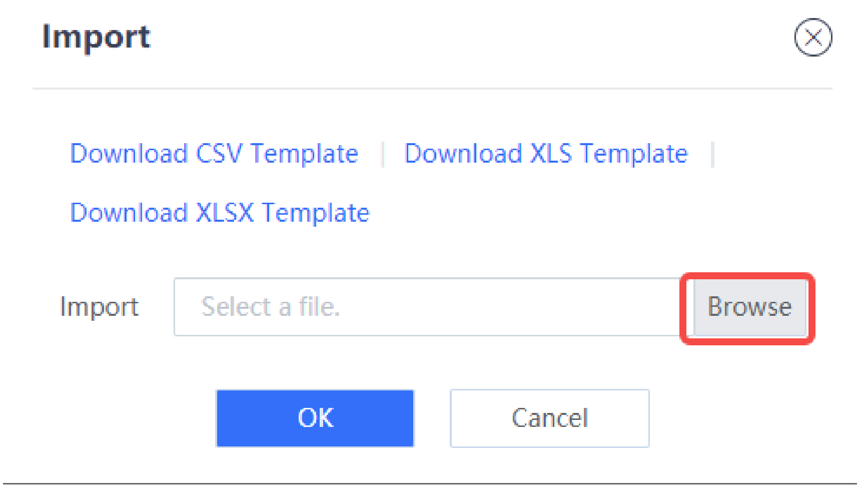


(2) Click **Import**. The **Import** dialog box is displayed.



(3) Three formats of templates are supported. Click **Download CSV Template**, **Download XLS Template**, or **Download XLSX Template** to download the corresponding template.

(4) Fill in the TI information in the template. Return to the web page, click **Browse**, and upload the configuration file.



(5) Click **Confirm** to complete the file import.

Follow-up Procedure

- To modify the custom TI, click **Edit**.
- To delete the custom TI, click **Delete**.
- To enable or disable the custom TI, click ●.
- To enable or disable the TI types in a batch, select the TI types in the same status and click **Enable** or **Disable**.
- To save the custom TI to a local device, select the custom TI and click **Export**. The exported TI can be imported to other devices.

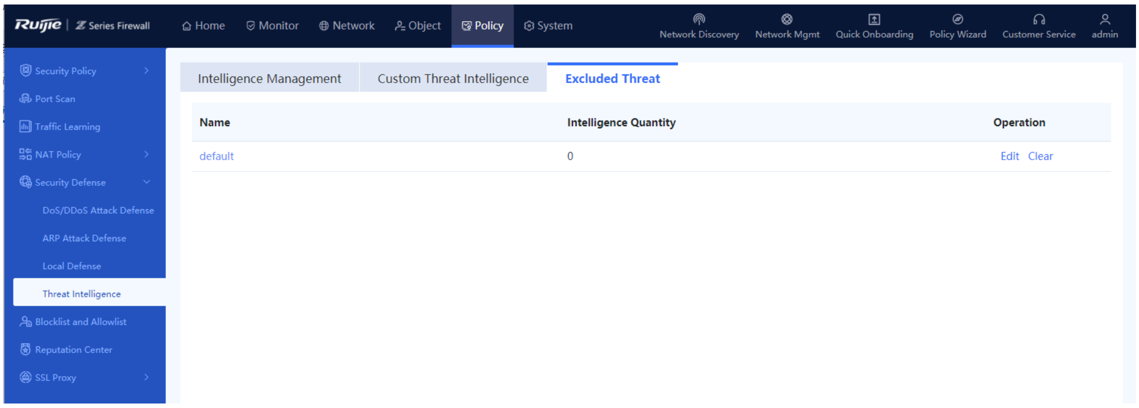
4. Configuring Excluded Threat

Application Scenario

If the user's normal data is intercepted by mistake due to the not-updated threat intelligence content or other reasons, or if an IP address/domain name is not malicious, you can add the IP address/domain name to the excluded threat list. The traffic matching the excluded threat list will be permitted by the TI module.

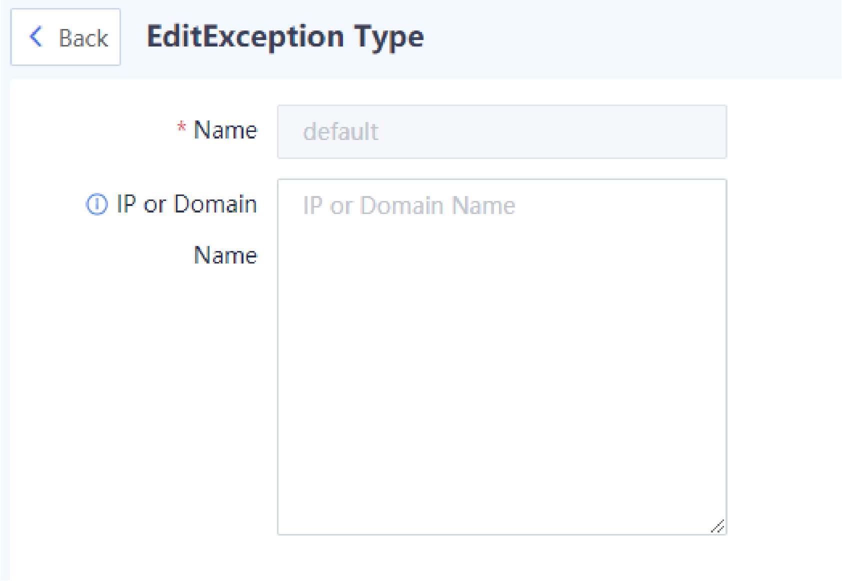
Procedure

(1) Choose **Policy** > **Security Defense** > **Threat Intelligence** > **Excluded Threat**.



Name	Intelligence Quantity	Operation
default	0	Edit Clear

(2) Click **Edit** in the **Operation** column of the **default** entry.



EditException Type

* Name: default

IP or Domain Name: IP or Domain Name

(3) Set the parameters of excluded threat.

Item	Description	Remarks
Name	Excluded threat name.	[Example] default
IP or Domain Name	IP address or domain name of the excluded threat.	If multiple IP addresses or domain names need to be configured, enter one IP address or domain name per line, and press **Enter** to separate lines. [Example]

Item	Description	Remarks
		www.xxx.com

Follow-up Procedure

- To modify the configuration of an excluded threat, click **Edit**.
- To delete all the IP addresses or domain names configured for an excluded threats, click **Clear**.

5. Viewing Threat Intelligence Logs

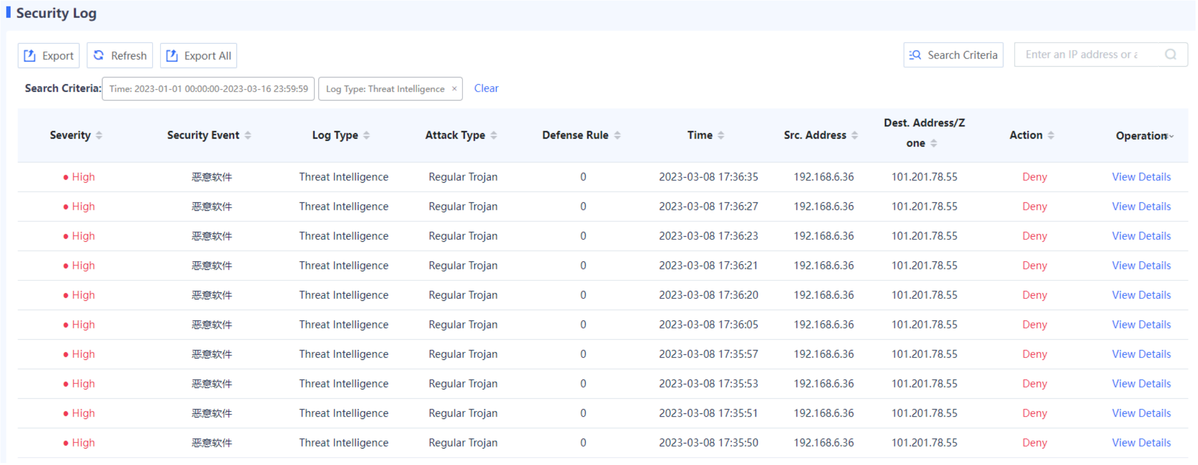
Application Scenario

When a malicious connection matches the threat intelligence, a security log is generated, and the log type is **Threat Intelligence**. By checking the logs, you can view the specific attack information and matched threat intelligence type, helping you take further actions.

Procedure

(1) Choose **Monitor** > **Log Monitoring** > **Security Log**.

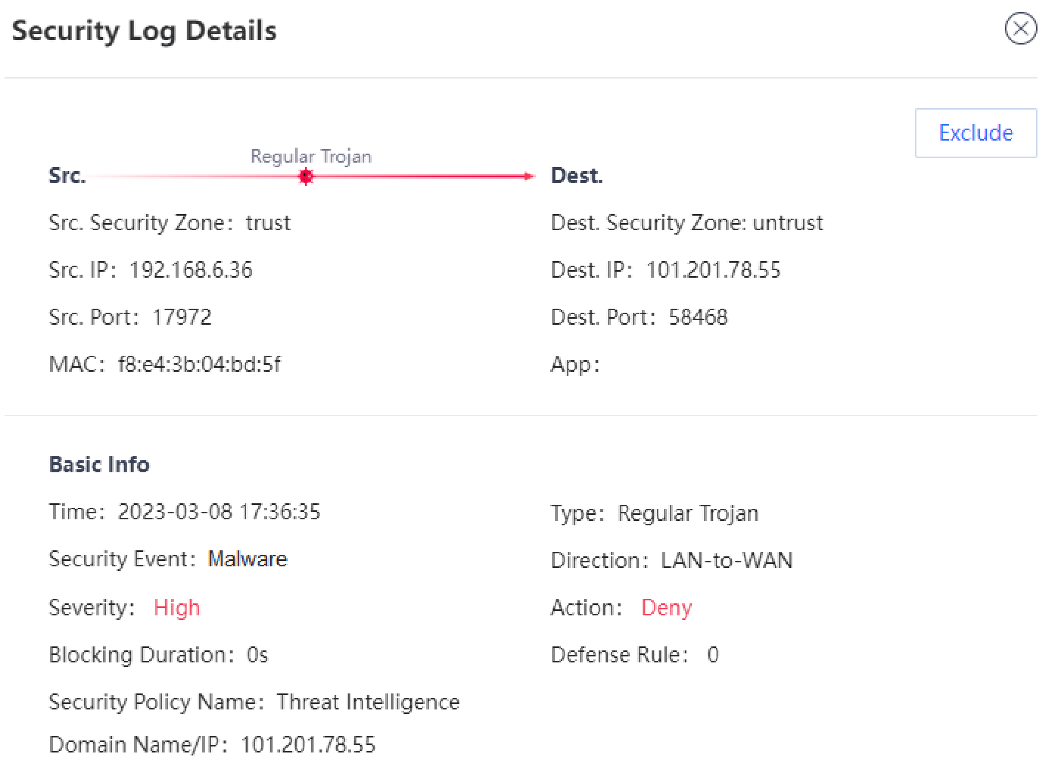
(2) The threat intelligence log information is displayed on the web UI.



Search Criteria: Time: 2023-01-01 00:00:00-2023-03-16 23:59:59 | Log Type: Threat Intelligence × | Clear

Severity	Security Event	Log Type	Attack Type	Defense Rule	Time	Src. Address	Dest. Address/Zone	Action	Operation
● High	恶意软件	Threat Intelligence	Regular Trojan	0	2023-03-08 17:36:35	192.168.6.36	101.201.78.55	Deny	View Details
● High	恶意软件	Threat Intelligence	Regular Trojan	0	2023-03-08 17:36:27	192.168.6.36	101.201.78.55	Deny	View Details
● High	恶意软件	Threat Intelligence	Regular Trojan	0	2023-03-08 17:36:23	192.168.6.36	101.201.78.55	Deny	View Details
● High	恶意软件	Threat Intelligence	Regular Trojan	0	2023-03-08 17:36:21	192.168.6.36	101.201.78.55	Deny	View Details
● High	恶意软件	Threat Intelligence	Regular Trojan	0	2023-03-08 17:36:20	192.168.6.36	101.201.78.55	Deny	View Details
● High	恶意软件	Threat Intelligence	Regular Trojan	0	2023-03-08 17:36:05	192.168.6.36	101.201.78.55	Deny	View Details
● High	恶意软件	Threat Intelligence	Regular Trojan	0	2023-03-08 17:35:57	192.168.6.36	101.201.78.55	Deny	View Details
● High	恶意软件	Threat Intelligence	Regular Trojan	0	2023-03-08 17:35:53	192.168.6.36	101.201.78.55	Deny	View Details
● High	恶意软件	Threat Intelligence	Regular Trojan	0	2023-03-08 17:35:51	192.168.6.36	101.201.78.55	Deny	View Details
● High	恶意软件	Threat Intelligence	Regular Trojan	0	2023-03-08 17:35:50	192.168.6.36	101.201.78.55	Deny	View Details

(3) Click **View Details** to display attack log details.



Security Log Details

Src. Security Zone: trust

Src. IP: 192.168.6.36

Src. Port: 17972

MAC: f8:e4:3b:04:bd:5f

Dest. Security Zone: untrust

Dest. IP: 101.201.78.55

Dest. Port: 58468

App:

Basic Info

Time: 2023-03-08 17:36:35

Type: Regular Trojan

Security Event: Malware

Direction: LAN-to-WAN

Severity: High

Action: Deny

Blocking Duration: 0s

Defense Rule: 0

Security Policy Name: Threat Intelligence

Domain Name/IP: 101.201.78.55

Exclude: If you confirm that a threat is a false positive, click **Exclude** to add the threat intelligence information in this security log to the excluded threat list and allow subsequent traffic.

Note

For more information and configurations about the fields in security logs, see 8.3.2 Querying Security Logs.

7.2.8 URL Filtering

1. Configuring a URL Category

Application Scenario

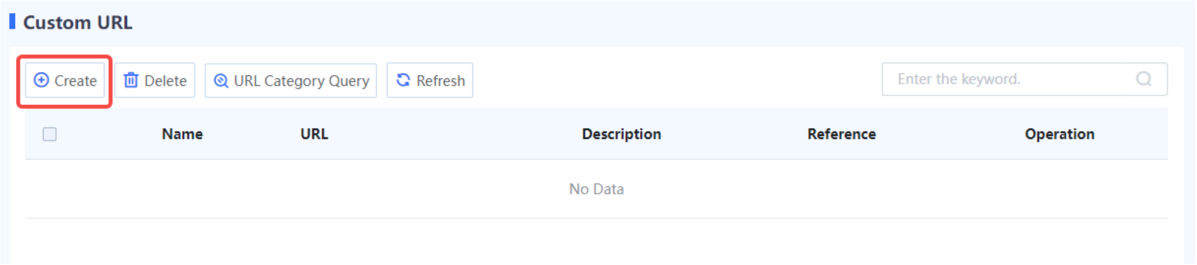
The URL category function is used to categorize web pages that intranet users can access to facilitate monitoring and management. With URL filtering templates, the firewall can prevent users from accessing malicious websites, and guarantee the access bandwidth for web pages of a specific category. For example, enable the firewall to preferentially guarantee traffic of office web pages and block traffic from other web pages.

Configure a URL category to categorize web pages that intranet users can access to facilitate monitoring and management.

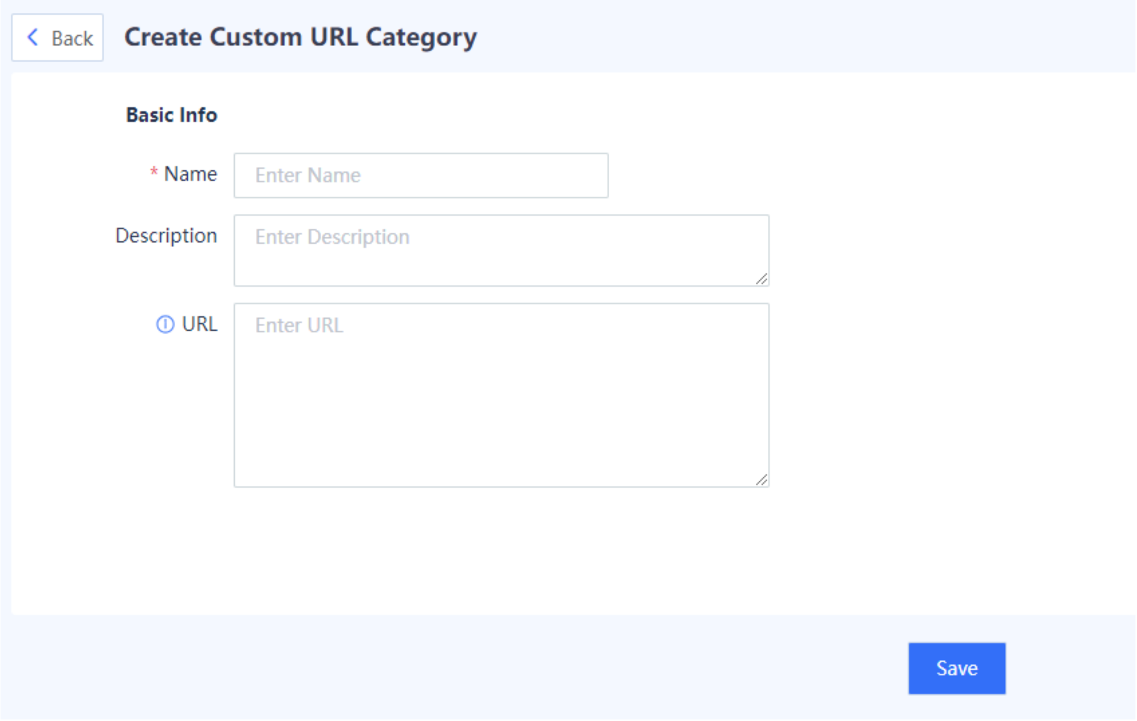
Procedure

(1) Choose **Object** > **URL Category**.

(2) Click **Create**.



(3) Enter URL category information.



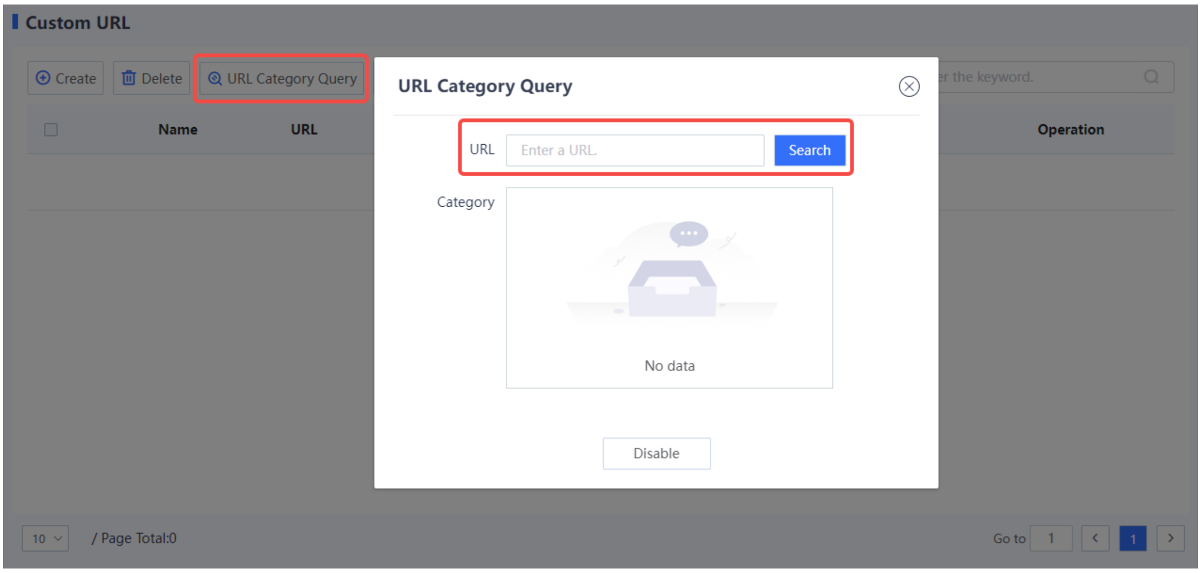
Item	Description	Remarks
Basic Info		
Name	URL category name.	[Example] category_1
Description	Description of the URL category.	N/A

Item	Description	Remarks
URL	URLs in this category. A URL can contain the wildcard character (*). Enter one URL per line. Press **Enter** to separate lines. Note: ● If a URL contains the pound sign (#), the sign and the string after the sign do not take effect for matching. For example, if **www.test.com/#123** is configured, all the domain names that start with **www.test.com/** will be matched. ● If a URL contains the characters **http://** or **https://**, these characters will be automatically removed during matching. ● If an IPv6 address is configured as a URL, the input format should be [*IPv6 address*]. For example, **[2001::1]**.	[Example] www.abc1.com www.abc2.com

(4) After verifying the configuration, click **Save**.

Follow-up Procedure

- To delete multiple URL categories in a batch, select the categories and click **Delete**. Only URL categories with no reference can be deleted.
- Click **URL Category Query**. In the dialog box that is displayed, enter a URL to query its category.



Application Scenario

Configure a URL filtering template to block or report alarms for specific URL categories. Detection can be triggered only after a URL filtering template is referenced by a security policy. For details about security policies, see 7.6 Security Policy.

Precautions

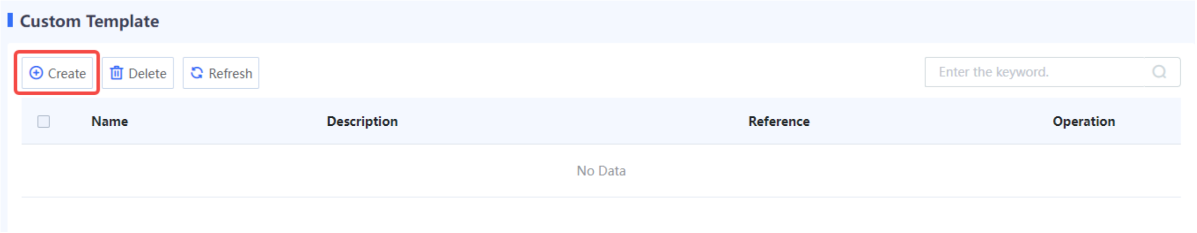
- To detect HTTPS-based URLs, you need to configure an SSL proxy policy. For details about SSL proxy, see 7.3 Configuring SSL Proxy Policies.
- After you configure custom URL categories, URLs that are not in the custom categories are classified as uncategorized. When detecting traffic that accesses uncategorized URLs, the device processes the traffic according to the action set for uncategorized URLs.

2. Configuring a URL filtering template

Procedure

(1) Choose **Object** > **Content Template** > **URL Filtering**.

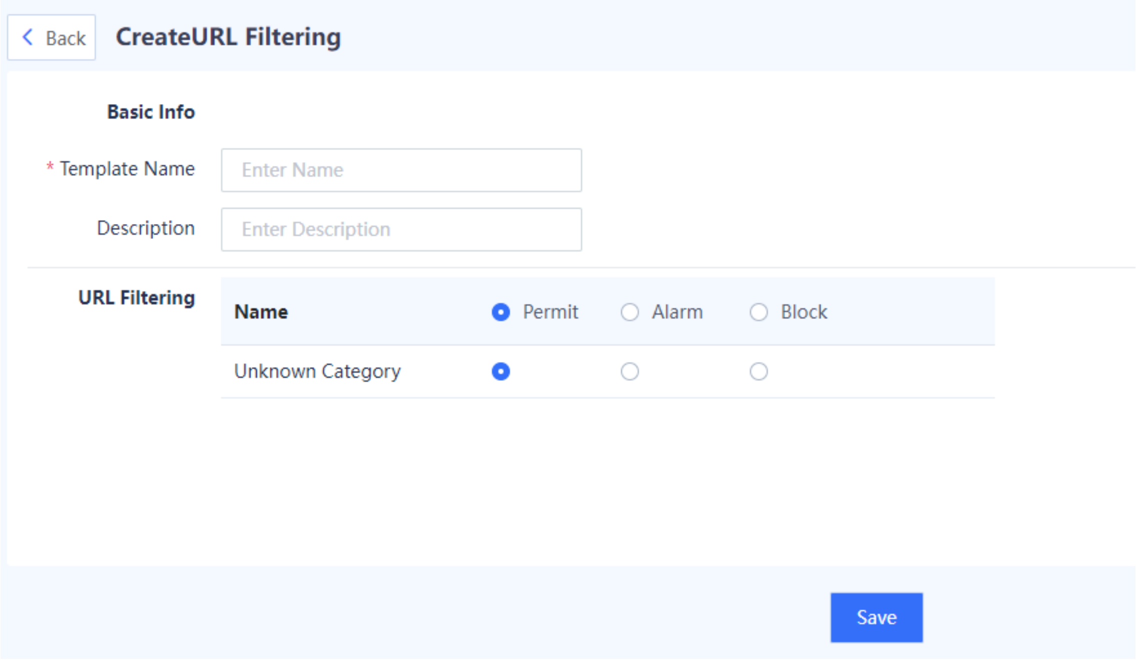
(2) Click **Create**.



Custom Template

□	Name	Description	Reference	Operation
No Data				

(3) Enter URL filtering template information.



< Back **CreateURL Filtering**

Basic Info

* Template Name: Enter Name

Description: Enter Description

URL Filtering

Name	● Permit	○ Alarm	○ Block
Unknown Category	●	○	○

Item	Description	Remarks
Basic Info		
Template Name	Name of the URL filtering template.	[Example] Template_1
Description	Description of the URL filtering template.	N/A
URL Filtering		
URL Filtering	Set processing actions for different URL categories: ● **Permit**: Permit traffic that accesses the URLs of the specific categories. ● **Alarm**: Permit traffic that accesses the URLs of the specific categories and generate an alarm log. ● **Block**: Block traffic that accesses the URLs of the specific categories and generate an alarm log.	N/A

(4) After verifying the configuration, click **Save**.

Follow-up Procedure

Refer to a URL filtering template in a security policy. For details about security policies, see 7.6 Security Policy.

7.3 Configuring SSL Proxy Policies

7.3.1 Overview

To protect data security and privacy, traffic of many applications is encrypted by Transport Layer Security (TLS) during transmission. To detect the content of TLS encrypted traffic, the firewall needs to decrypt traffic as proxy so that the function modules such as intrusion prevention and virus protection can detect the decrypted traffic and files. Currently, the firewall can only decrypt the HTTPS encrypted traffic.

The following table describes the application scenarios of SSL proxy.

Scenario	Similarity	Difference
Client protection	The firewall sets up an SSL connection with client and server respectively, to send and receive SSL encrypted data. The firewall decrypts the encrypted data from the client, performs security check, re-encrypts the data that passes the check, and sends it to the server.	The firewall uses the temporary server certificate re-issued by the imported CA certificate to set up SSL connection with the client.
Server protection		The firewall uses the imported server certificate to set up SSL connection with the client.

7.3.2 Configuring an SSL Proxy Template

Application Scenario

Configure this function if you need to perform virus protection detection or IPS detection for HTTPS encrypted traffic. The system predefines the default template, which can be directly referenced or customized according to your needs.

Note

After configuring an SSL proxy template, you need to reference it in the SSL proxy policy to decrypt traffic. The SSL proxy policy is used to set the matching conditions of packets and whether to decrypt them after they are hit. The SSL proxy template specifies how the device decrypts packets that hit the policy.

Prerequisites

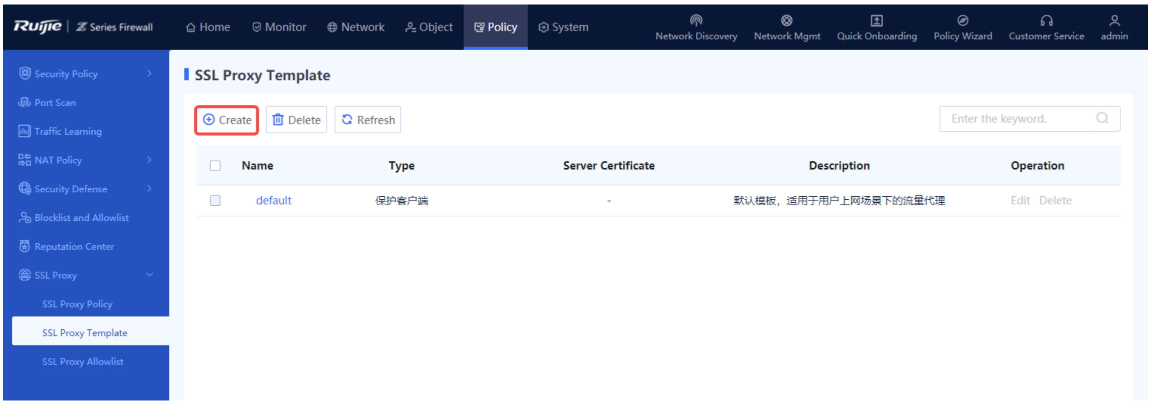
If you select **Protect Client** as the SSL proxy template type, import the SSL proxy certificate (CA certificate) first. For details about SSL proxy certificate import, see 7.3.3 1. Importing SSL Proxy Certificate.

If you select **Protect Server** as the SSL proxy template type, import the server certificate first. For details about server certificate import, see 7.3.3 2. Importing Server Certificate.

Procedure

(1) Choose **Policy** > **SSL Proxy** > **SSL Proxy Template**.

(2) Click **Create** to enter the **Create SSL Proxy Template** page.



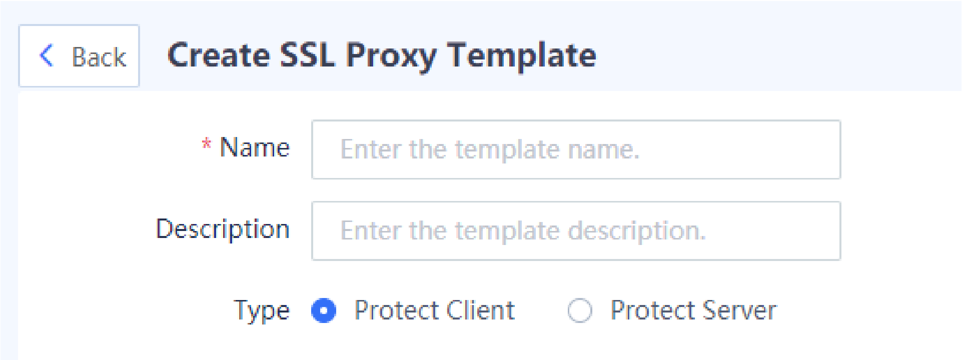
SSL Proxy Template

□	Name	Type	Server Certificate	Description	Operation
□	default	保护客户端	-	默认模板，适用于用户上网场景下的流量代理	Edit Delete

(3) Enter the template name and description, select template type, and click **Save**.

Note

If the type is set as **Protect Server**, the server certificate needs to be selected.



Create SSL Proxy Template

* Name: Enter the template name.

Description: Enter the template description.

Type: ● Protect Client ○ Protect Server

<table>
<tr><th>Item</th><th>Description</th><th>Remarks</th></tr>
<tr><td>Name</td><td>Name of the SSL proxy template.</td><td>Characters such as `~!#%^&*+\|{};:'"/<>? and spaces are not allowed.
[Example]
profile</td></tr>
<tr><td>Description</td><td>Proxy template description.</td><td>Characters such as `~!#%^&*+\|{};:'"/<>? are not allowed.</td></tr>
<tr><td>Type</td><td>The type can be <b>Protect Client</b> or <b>Protect Server</b>.</td><td>Select the type according to the actual networking scenario.
[Example]
Protect Client</td></tr>
<tr><td>Server Certificate</td><td>Used to establish the trust relationship between the device and client in the process of SSL proxy.</td><td>Required only when the template type is Protect Server.
Imported server certificates can be selected.</td></tr>
</table>

Follow-up Procedure

Create an SSL proxy policy and reference the SSL proxy template.

7.3.3 Importing Certificate

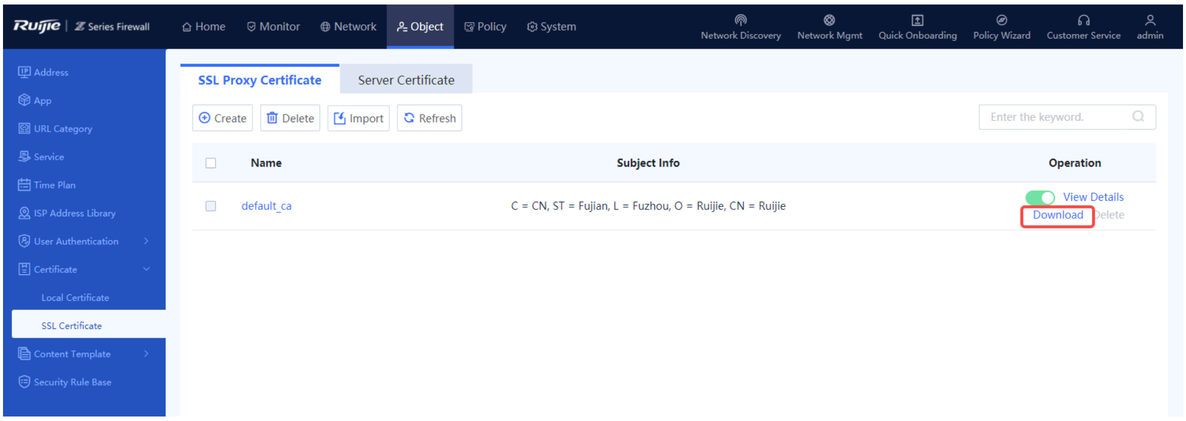
1. Importing SSL Proxy Certificate

Application Scenario

If HTTPS encrypted traffic needs to be decrypted and the SSL proxy template type is set to **Protect Client**, you must import an SSL proxy certificate (that is, a CA certificate). The device provides a predefined certificate. You can also import a new certificate as needed.

Precautions

After configuring the SSL proxy certificate, click **Download** in the row where the trusted certificate resides, save the SSL proxy certificate to the local device, and then import it to the client to make the client trust it. If you do not install this certificate and the SSL proxy is enabled on the firewall, when the client accesses website by using the browser through HTTPS, an alarm indicating that the server certificate is not issued by a trusted CA is displayed. In some cases, connection may even be directly interrupted, affecting the user's Internet access.

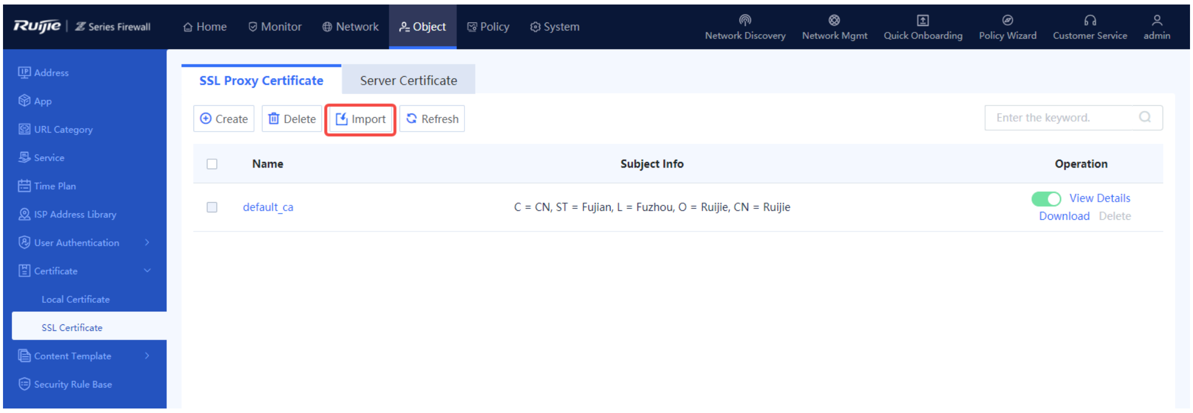


Name	Subject Info	Operation
default_ca	C = CN, ST = Fujian, L = Fuzhou, O = Ruijie, CN = Ruijie	View Details Download Delete

Procedure

(1) Choose **Object** > **Certificate** > **SSL Certificate** > **SSL Proxy Certificate**.

(2) Click **Import** to enter the **Import SSL Proxy Certificate** page.

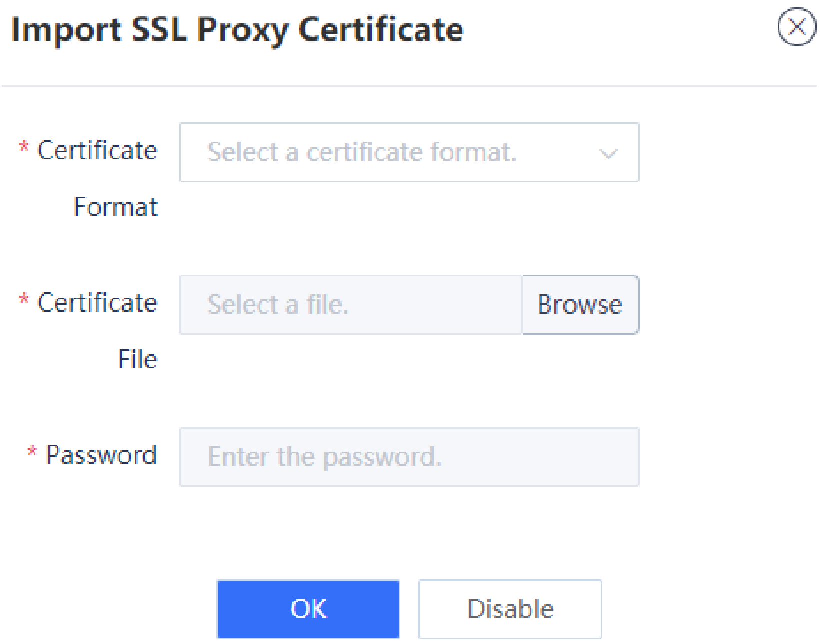


Name	Subject Info	Operation
default_ca	C = CN, ST = Fujian, L = Fuzhou, O = Ruijie, CN = Ruijie	View Details Download Delete

Note

It is recommended that you import a certificate. You can click **Create** to add a CA certificate.

(3) Select a certificate format. Click **Browse** to upload the certificate file, enter the certificate password, and click **Confirm**.



Import SSL Proxy Certificate

* Certificate Format: Select a certificate format.

* Certificate File: Select a file. Browse

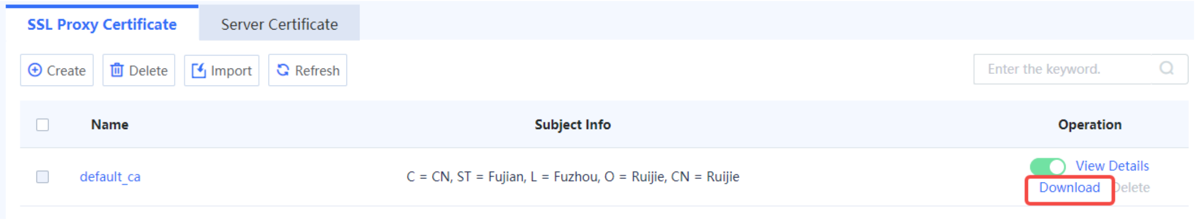
* Password: Enter the password.

Item	Description	Remarks
Certificate Format	Select the certificate format according to the suffix of the imported certificate file, and you can import certificates in PEM, P12, or CRT format.	● The certificate with the p12 or pem suffix already contains the key. You need to specify the password of the certificate when importing the certificate. ● The certificate with the crt suffix does not contain a key and a separate key file is required. When you import the certificate, specify the key file and password of the key file. [Example] P12
Certificate File	Imported SSL proxy certificate file.	Click **Browse** to select a certificate file to be uploaded from the local device.
Key File	Separate key file attached with the certificate.	The certificate file with the crt suffix does not contain a key. You need to upload the key file and specify the password for the key file when importing the certificate.

Item	Description	Remarks
Password	Password of the key file.	● Certificate with the p12 or pem suffix: You need to specify the password of the certificate when importing the certificate. ● Certificate with the crt suffix: When you import the certificate, specify the key file and password of the key file.

Follow-up Procedure

- is used to configure whether to trust the SSL proxy certificate. When the icon is red, the certificate is not trusted; when the icon is green, the certificate is trusted. Click the icon to modify the credibility of the certificate. Only one trusted SSL proxy certificate can exist on the device.
- Download the SSL proxy certificate, and import it into the client to make the client trust it.



□	Name	Subject Info	Operation
□	default_ca	C = CN, ST = Fujian, L = Fuzhou, O = Ruijie, CN = Ruijie	View Details Download Delete

- Click **View Details** to view details about the SSL proxy certificate.
- To delete a newly imported SSL proxy certificate, click **Delete**. The default SSL proxy certificate cannot be deleted.
- You can enter the certificate name in the search box in the upper right corner of the page to search for a certificate.

2. Importing Server Certificate

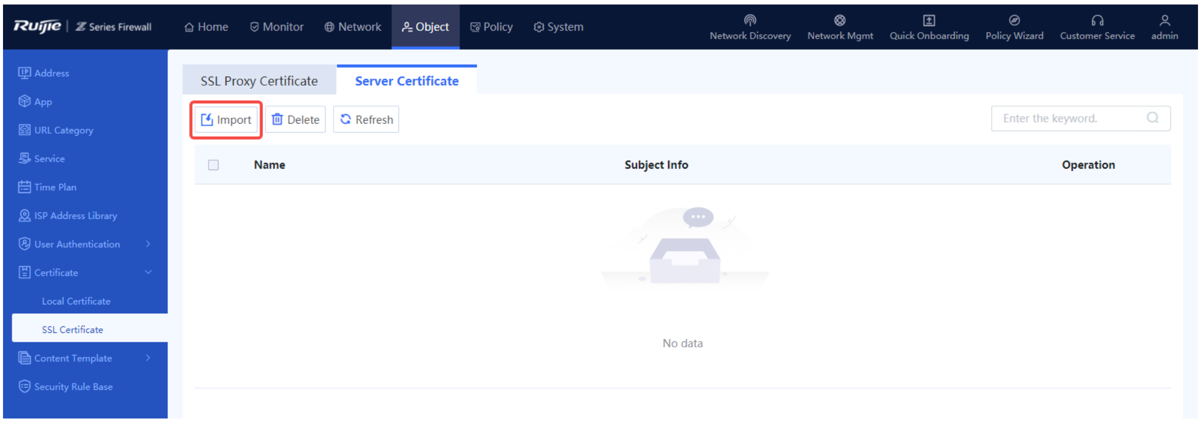
Application Scenario

If you need to decrypt the HTTPS encrypted traffic and the SSL proxy template type is set to **Protect Server**, you must import a server certificate.

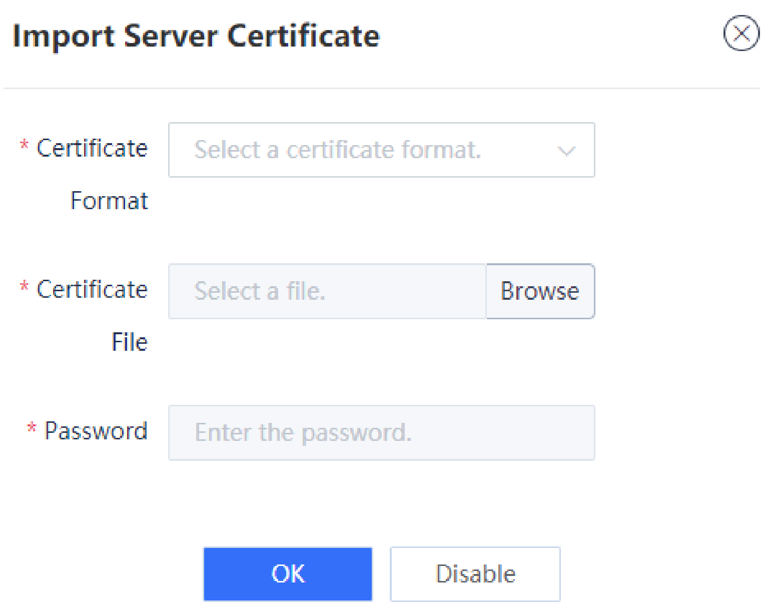
Procedure

(1) Choose **Object** > **Certificate** > **SSL Certificate** > **Server Certificate**.

(2) Click **Import** to enter the **Import Server Certificate** page.



(3) Select a certificate format. Click **Browse** to upload the certificate file, enter the certificate password, and click **Confirm**.



Item	Description	Remarks
Certificate Format	Select the certificate format according to the suffix of the imported certificate file, and you can import server certificates in PEM,	● The certificate with the p12 or pem suffix already contains the key. You need to specify the password of the certificate when importing the certificate. ● The certificate with the crt suffix does not contain a key and a separate key file is required. When you import the certificate, specify the key

Item	Description	Remarks
	P12, or CRT format.	file and password of the key file. [Example] P12
Certificate File	Imported server certificate file.	Click **Browse** to select a certificate file to be uploaded from the local device.
Key File	Separate key file attached with the certificate.	The certificate file with the crt suffix does not contain a key. You need to upload the key file and specify the password for the key file when importing the certificate.
Password	Password of the key file.	● Certificate with the p12 or pem suffix: You need to specify the password of the certificate when importing the certificate. ● Certificate with the crt suffix: When you import the certificate, specify the key file and password of the key file.

7.3.4 Configuring an SSL Proxy Policy

Application Scenario

Configure this function if you need to perform virus protection detection or IPS detection for HTTPS encrypted traffic.

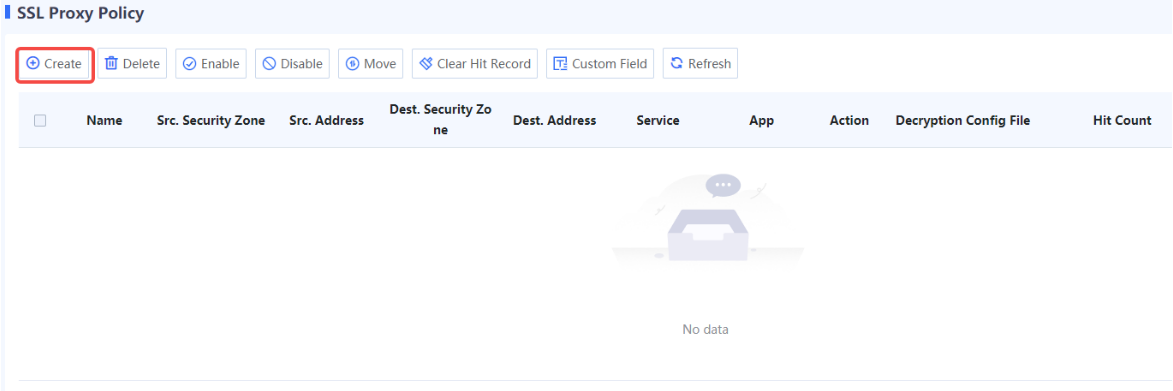
Prerequisites

The SSL proxy template has been created. For details about SSL proxy template creation, see 7.3.2 Configuring an SSL Proxy Template.

Procedure

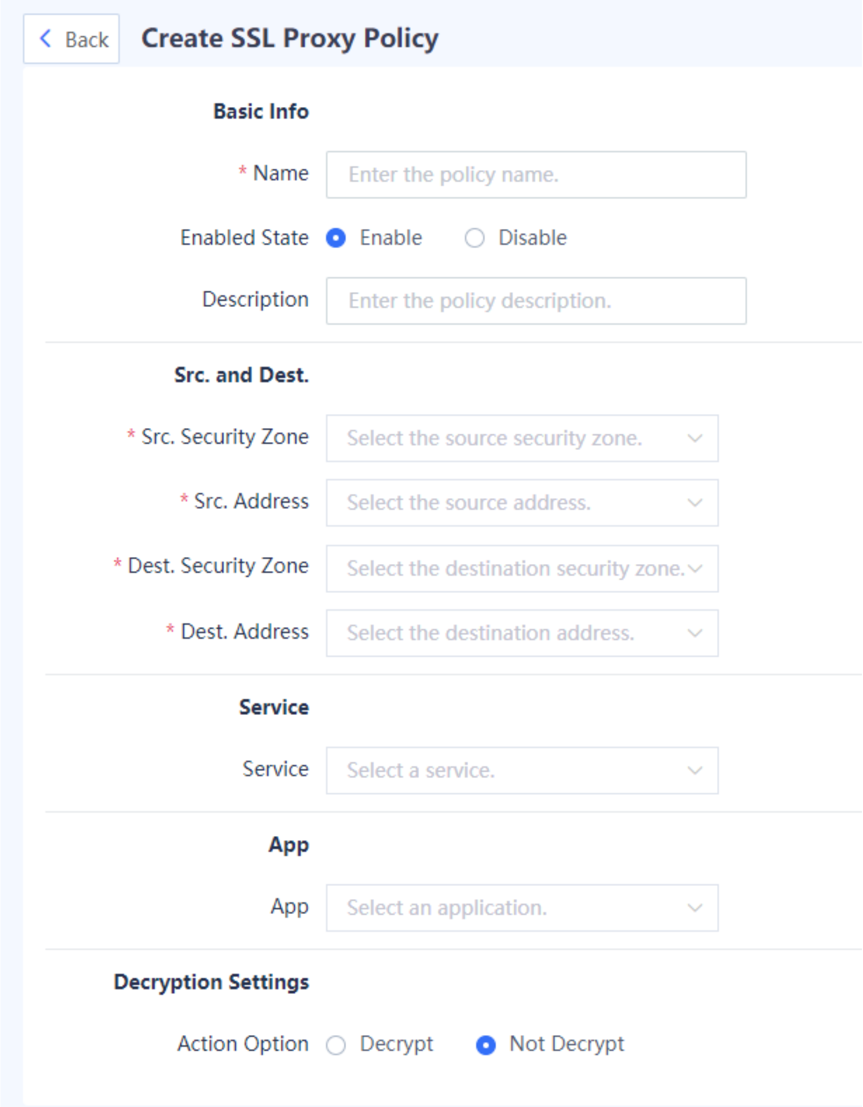
(1) Choose **Policy** > **SSL Proxy** > **SSL Proxy Policy**.

(2) Click **Create** to enter the **Create SSL Proxy Policy** page.



□	Name	Src. Security Zone	Src. Address	Dest. Security Zone	Dest. Address	Service	App	Action	Decryption Config File	Hit Count

(3) Configure the SSL proxy policy according to the following table.


Back
Create SSL Proxy Policy
Basic Info
Src. and Dest.
Service
App
Decryption Settings
Select the source security zone.
Select the source address.
Select the destination security zone.
Select the destination address.
Select a service.
Select an application.

* Name: Enter the policy name.

Enabled State: ● Enable ○ Disable

Description: Enter the policy description.

* Src. Security Zone

* Src. Address

* Dest. Security Zone

* Dest. Address

Service

App

Action Option: ○ Decrypt ● Not Decrypt

Item	**Description**	**Remarks**
Basic Info		
Name	Name of the SSL proxy policy.	Characters such as `~!#%^&*+\/0::"/<>? and spaces are not allowed. [Example] SSLPolicy_1
Enabled State	Whether to enable the new SSL proxy policy.	[Example] Enabled
Description	Description of SSL proxy policy.	Characters such as `~!#%^&*+|{};:'"/<>? are not allowed. [Example] Decrypt the HTTPS encrypted traffic from security zone 1 to security zone 2.
Src. and Dest.		
Src. Security Zone	Source security zone that initiates the target data connection.	[Example] trust
Src. Address	Source address that initiates the target data connection.	Click the drop-down list, and select a source address in the **To-be-selected** area. The selected address is automatically added to the **Selected** area. [Example] Any
Dest. Security Zone	Destination security zone of the target data connection.	[Example] trust

Item	Description	Remarks
Dest. Address	Destination address of the target data connection.	Click the drop-down list, and select a destination address in the **To-be-selected** area. The selected address is automatically added to the **Selected** area. [Example] Any
Service	Service type of the target data connection request.	[Example] Any
App	Application type of the target data connection request.	[Example] Any
Action Option	Action taken by the SSL proxy policy, decrypting or not decrypting the content of target data connection. If **Decrypt** is selected, the SSL proxy template must be specified.	[Example] Decrypt

(4) After the configuration is completed, click **Save**.

Follow-up Procedure

- View or clear the number of times a policy is hit on the **SSL Proxy Policy** page.
- To move a policy to a specified position, select the policy and click **Move**. The closer a policy is to the front, the higher its priority is in matching.

7.3.5 Allowlist

1. Domain Name Allowlist

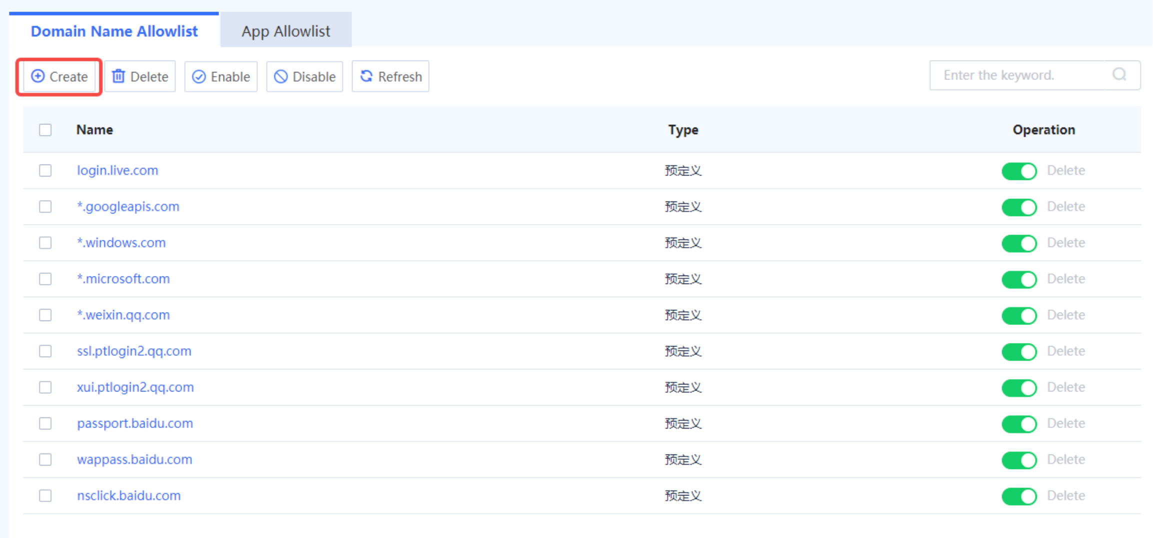
Application Scenario

If the traffic of certain domain names does not need to be decrypted, you can add the domain names to the allowlist. The device does not decrypt the traffic of the domain names in the allowlist. The device has added the commonly used domain names and the domain names that do not need to be or cannot be accessed by SSL proxy to the allowlist. The predefined allowlist cannot be deleted, but can be forbidden according to actual situation.

Procedure

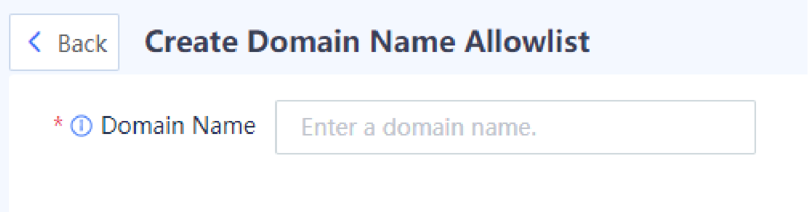
(1) Choose **Policy** > **SSL Proxy** > **SSL Proxy Allowlist** > **Domain Name Allowlist**.

(2) Click **Create** to enter the **Create Domain Name Allowlist** page.



□	Name	Type	Operation
□	login.live.com	预定义	● Delete
□	*.googleapis.com	预定义	● Delete
□	*.windows.com	预定义	● Delete
□	*.microsoft.com	预定义	● Delete
□	*.weixin.qq.com	预定义	● Delete
□	ssl.ptlogin2.qq.com	预定义	● Delete
□	xui.ptlogin2.qq.com	预定义	● Delete
□	passport.baidu.com	预定义	● Delete
□	wappass.baidu.com	预定义	● Delete
□	nsclick.baidu.com	预定义	● Delete

(3) Enter the domain name and click **Save**.



* Domain Name: Enter a domain name.

2. Application Allowlist

Application Scenario

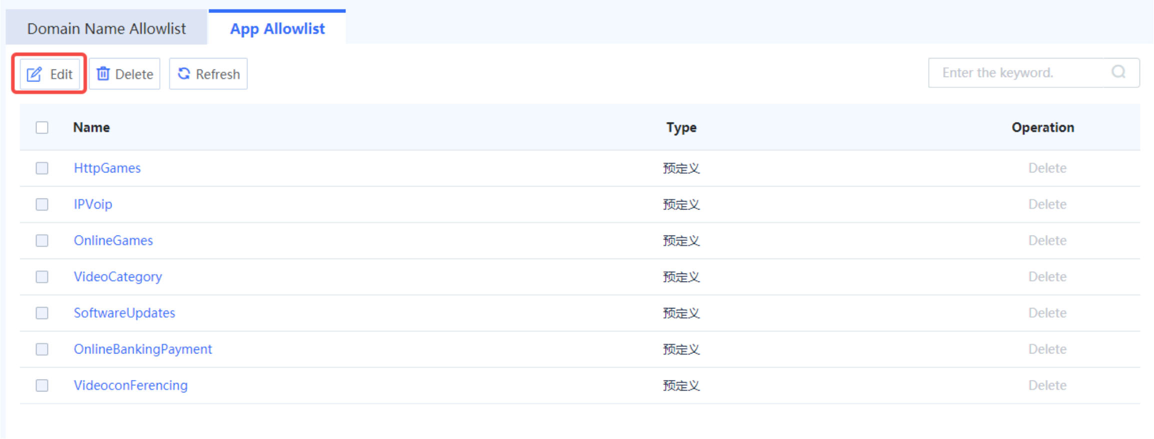
If the traffic of certain applications does not need to be decrypted, you can add the applications to the allowlist. The device does not decrypt the traffic of the applications in the allowlist.

The preconfigured application allowlist of SSL proxy includes the commonly used applications, the applications that do not need to be or cannot be accessed by SSL proxy. You can add applications to the predefined application allowlist.

Procedure

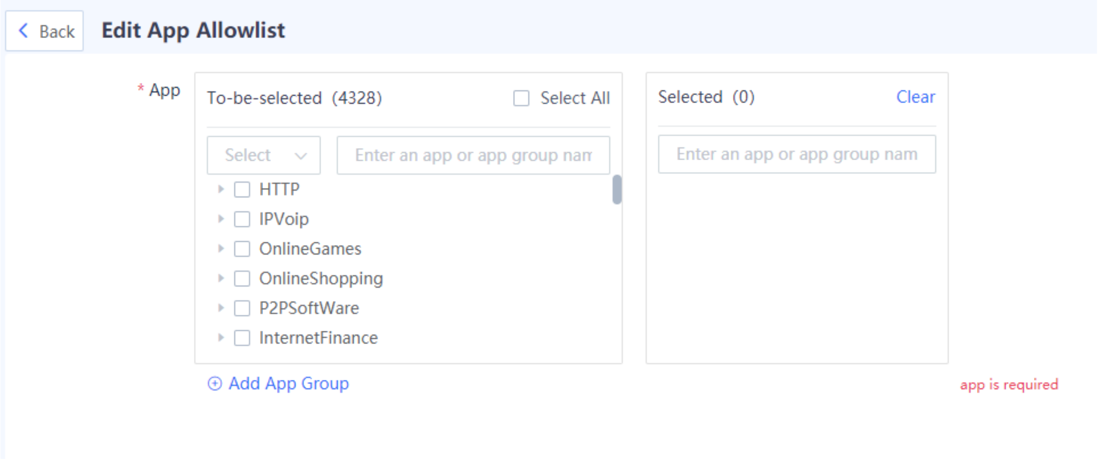
(1) Choose **Policy** > **SSL Proxy** > **SSL Proxy Allowlist** > **App Allowlist**.

(2) Click **Edit** to enter the **Edit App Allowlist** page.



☐	Name	Type	Operation
☐	HttpGames	预定义	Delete
☐	IPVoip	预定义	Delete
☐	OnlineGames	预定义	Delete
☐	VideoCategory	预定义	Delete
☐	SoftwareUpdates	预定义	Delete
☐	OnlineBankingPayment	预定义	Delete
☐	VideoconFerencing	预定义	Delete

(3) Select the applications or application group to be added to the allowlist, and click **Save**.



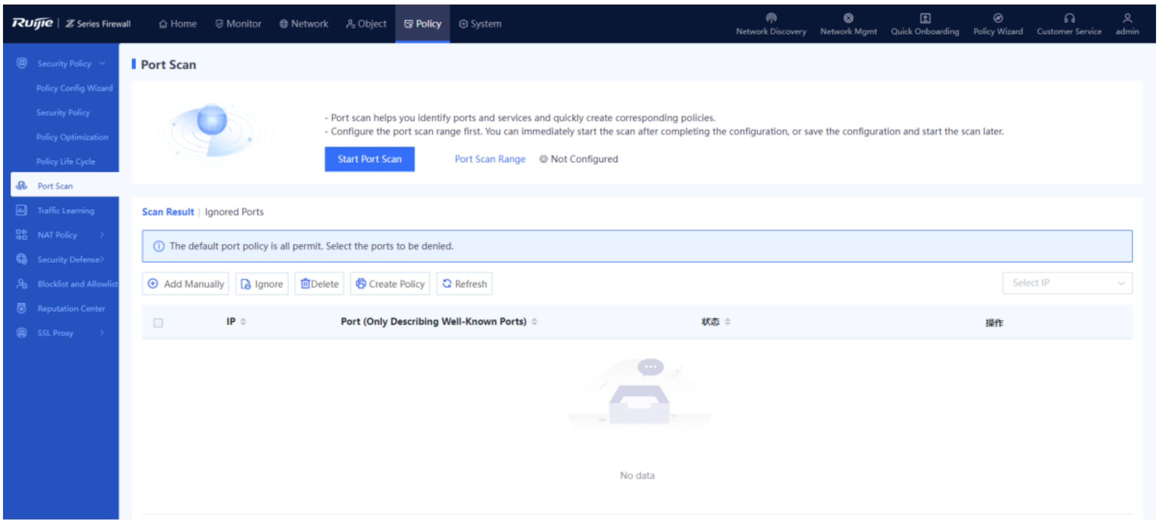
7.4 Port Scan

Application Scenario

The port scan function can help administrators quickly identify the IP address and open port information of the intranet server, and choose whether to generate security policies based on the scan results. This can help build a secure enterprise intranet.

Procedure

(1) Choose **Policy** > **Port Scan**.



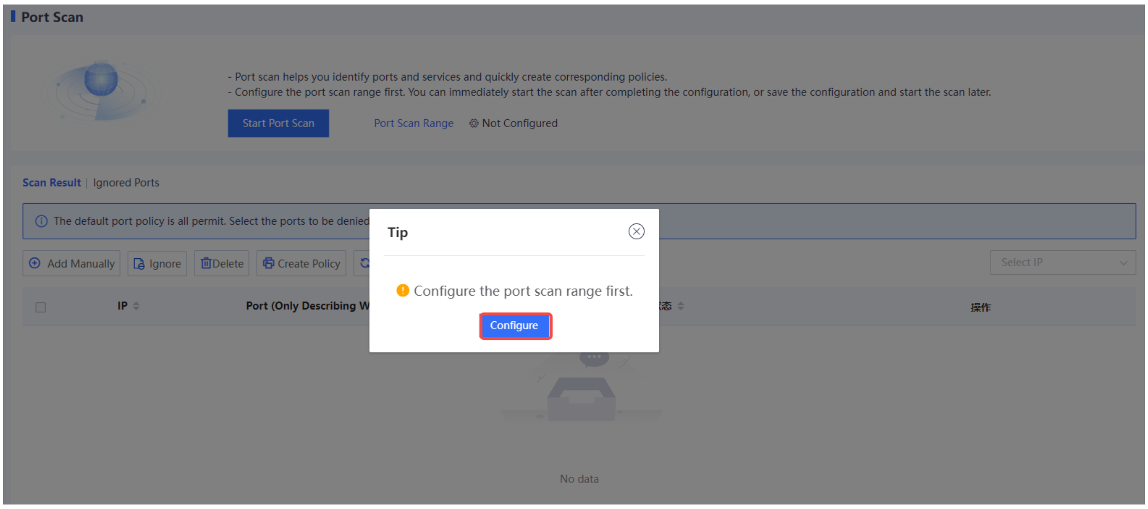
- Port scan helps you identify ports and services and quickly create corresponding policies.
- Configure the port scan range first. You can immediately start the scan after completing the configuration, or save the configuration and start the scan later.

The default port policy is all permit. Select the ports to be denied.

(2) (Optional) If the port scan range is not configured, configure it first.

a Click **Start Port Range**.

If the system displays "Configure the port scan range first.", click **Configure**.



- Port scan helps you identify ports and services and quickly create corresponding policies.
- Configure the port scan range first. You can immediately start the scan after completing the configuration, or save the configuration and start the scan later.

The default port policy is all permit. Select the ports to be denied

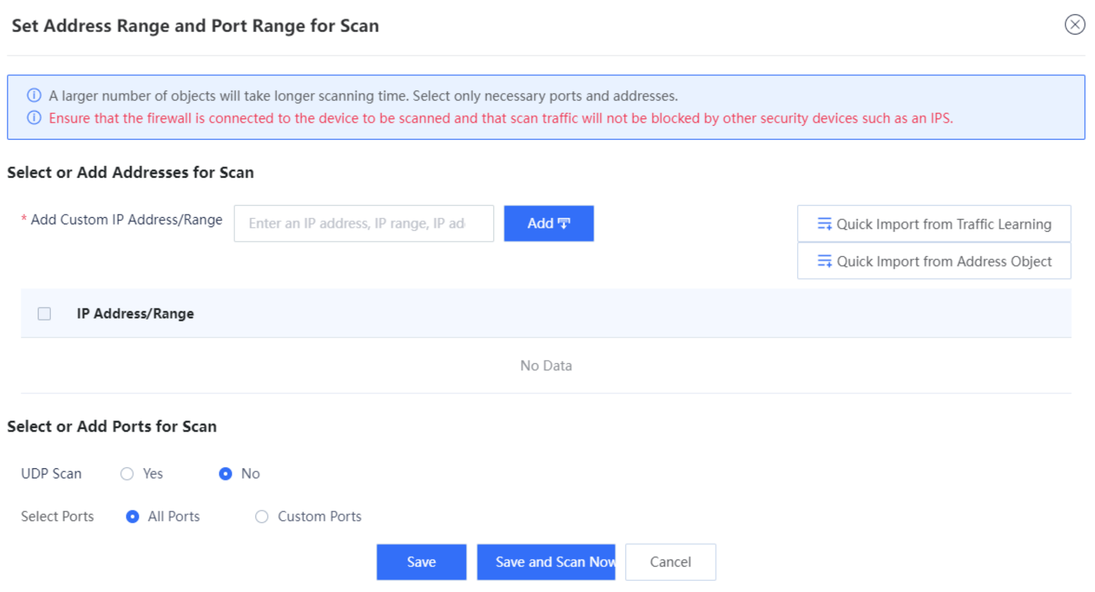
Configure the port scan range first.

b Select or add the IP address to be scanned.

Enter the IP address or range to be scanned in the **Add Custom IP Address/Range** input box, and click **Add** to add it to the **IP Address/Range** area.

Note

To quickly add IP addresses, click **Quick Import from Traffic Learning** or **Quick Import from Address Object**.



Set Address Range and Port Range for Scan

ⓘ A larger number of objects will take longer scanning time. Select only necessary ports and addresses.

ⓘ Ensure that the firewall is connected to the device to be scanned and that scan traffic will not be blocked by other security devices such as an IPS.

Select or Add Addresses for Scan

* Add Custom IP Address/Range [Enter an IP address, IP range, IP ad] Add

Quick Import from Traffic Learning

Quick Import from Address Object

□ IP Address/Range
No Data

Select or Add Ports for Scan

UDP Scan ○ Yes ● No

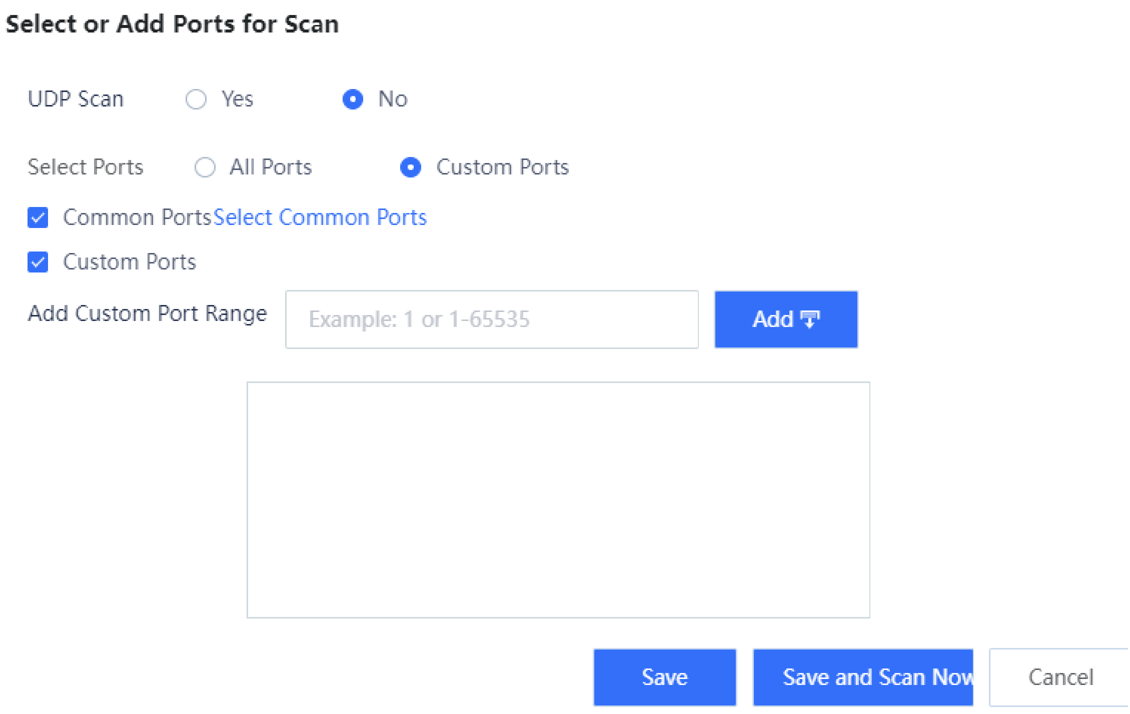
Select Ports ● All Ports ○ Custom Ports

Save | Save and Scan Now | Cancel

c Select or add the port to be scanned.

Note

If UDP scan is not enabled, you are advised to select **All Ports**.



Select or Add Ports for Scan

UDP Scan ○ Yes ● No

Select Ports ○ All Ports ● Custom Ports

☑ Common Ports Select Common Ports

☑ Custom Ports

Add Custom Port Range [Example: 1 or 1-65535] Add

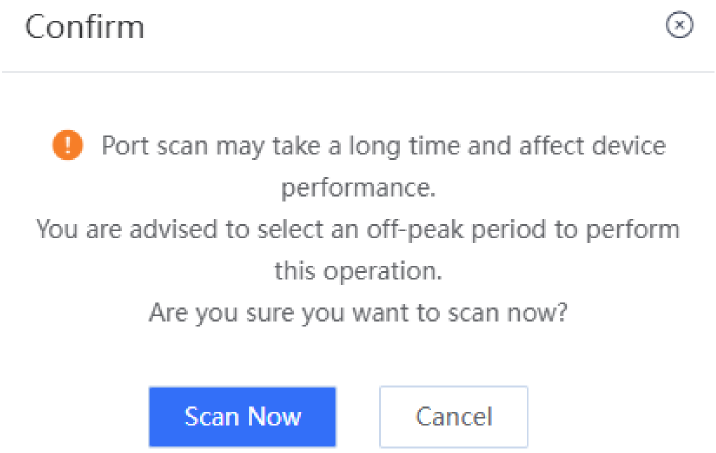
Save | Save and Scan Now | Cancel

Item	Description	Remarks
UDP Scan	Whether to perform UDP scan.	[Example] Yes
Select Ports	Select the port to be scanned: ● **All Ports**: Scan all ports. ● **Custom Ports**: Customize the ports to be scanned. ● Select **Common Ports** to add common service ports. You can click **Select Common Ports** to select common service ports. ● Select **Custom Ports** to add the ports to be scanned.	[Example] All Ports

d Choose whether to start port scan immediately according to service situation.

- When services are busy, click **Save** to save the port scan configuration. You can start port scan when services are idle.
- When services are idle, click **Save and Scan Now** to save the port scan configuration and start port scan immediately.

Confirm the system prompt and click **Scan Now**.

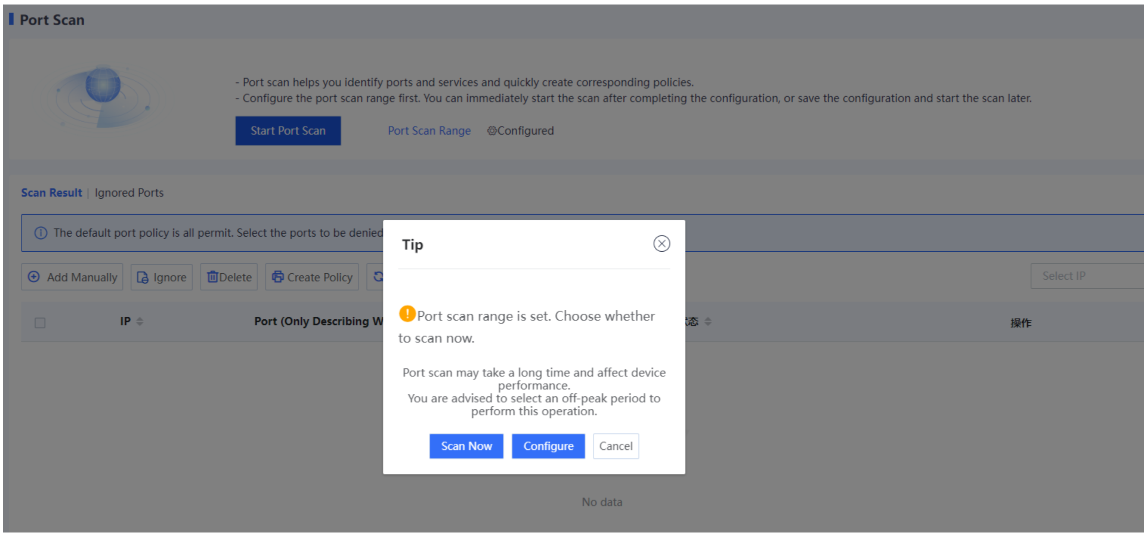

Confirm

Port scan may take a long time and affect device performance.
You are advised to select an off-peak period to perform this operation.
Are you sure you want to scan now?

(3) (Optional) If port scan policy has been configured:

a Click **Start Port Scan**.

b Click **Scan Now** to start port scan.



Port Scan

- Port scan helps you identify ports and services and quickly create corresponding policies.
- Configure the port scan range first. You can immediately start the scan after completing the configuration, or save the configuration and start the scan later.

Port Scan Range ⚙Configured

The default port policy is all permit. Select the ports to be denied

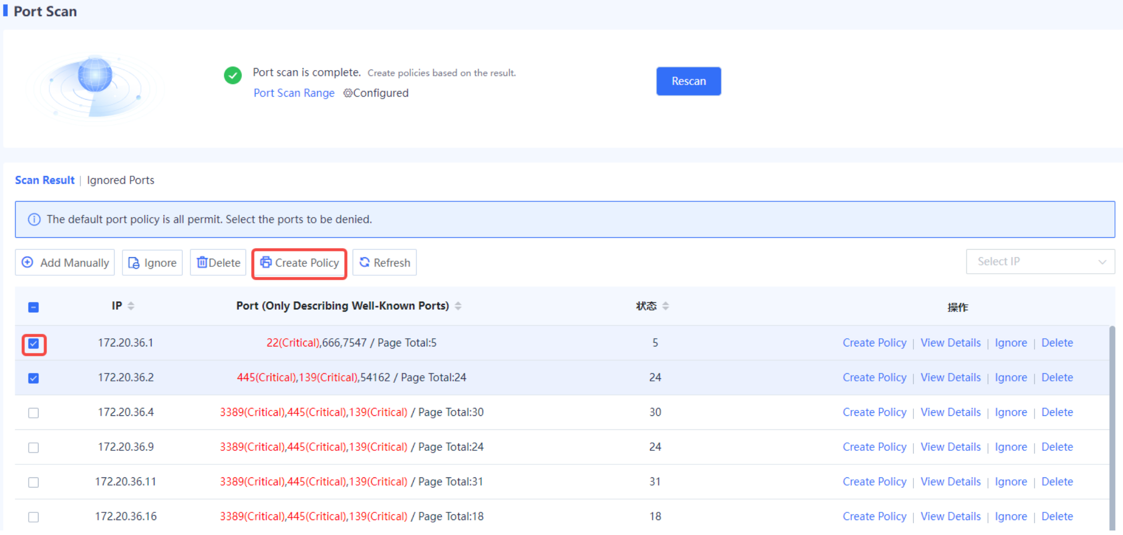
Tip

Port scan range is set. Choose whether to scan now.

Port scan may take a long time and affect device performance.
You are advised to select an off-peak period to perform this operation.

No data

(4) When port scan is finished, select the scan result and click **Create Policy**.



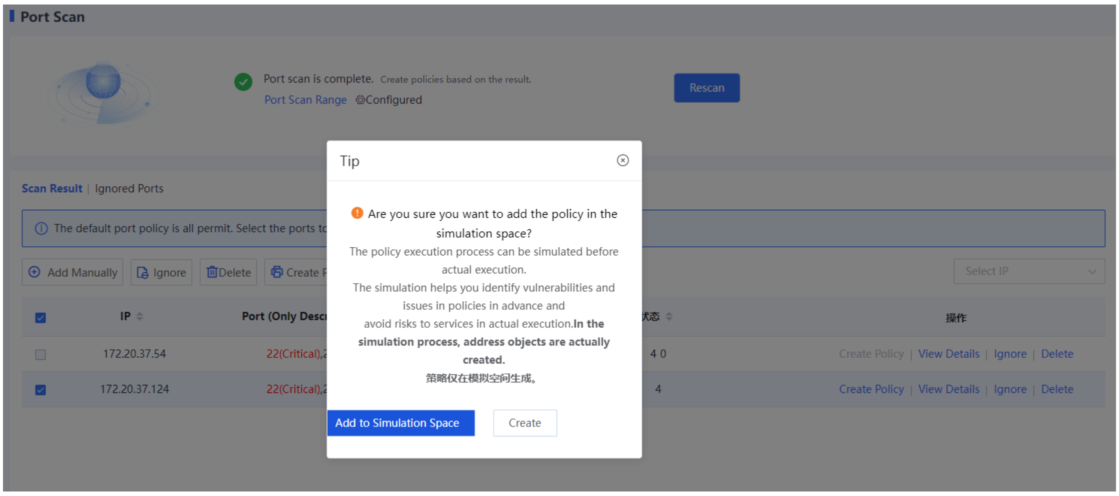
Port Scan

Port scan is complete. Create policies based on the result.

Port Scan Range ⚙Configured

The default port policy is all permit. Select the ports to be denied.

	IP	Port (Only Describing Well-Known Ports)	状态	操作
☑	172.20.36.1	22(Critical),666,7547 / Page Total:5	5	Create Policy | View Details | Ignore | Delete
☑	172.20.36.2	445(Critical),139(Critical),54162 / Page Total:24	24	Create Policy | View Details | Ignore | Delete
□	172.20.36.4	3389(Critical),445(Critical),139(Critical) / Page Total:30	30	Create Policy | View Details | Ignore | Delete
□	172.20.36.9	3389(Critical),445(Critical),139(Critical) / Page Total:24	24	Create Policy | View Details | Ignore | Delete
□	172.20.36.11	3389(Critical),445(Critical),139(Critical) / Page Total:31	31	Create Policy | View Details | Ignore | Delete
□	172.20.36.16	3389(Critical),445(Critical),139(Critical) / Page Total:18	18	Create Policy | View Details | Ignore | Delete



Port Scan

Port scan is complete. Create policies based on the result.

Port Scan Range ⚙Configured

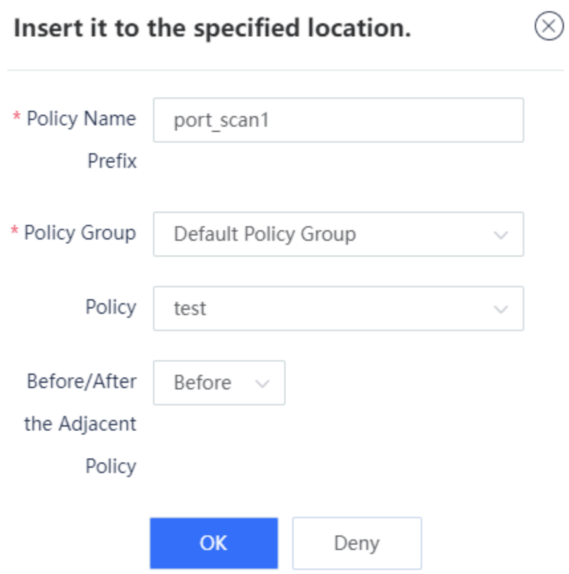
The default port policy is all permit. Select the ports t

Tip

Are you sure you want to add the policy in the simulation space?
The policy execution process can be simulated before actual execution.
The simulation helps you identify vulnerabilities and issues in policies in advance and
avoid risks to services in actual execution.**In the simulation process, address objects are actually created.**
策略仅在模拟空间生成。

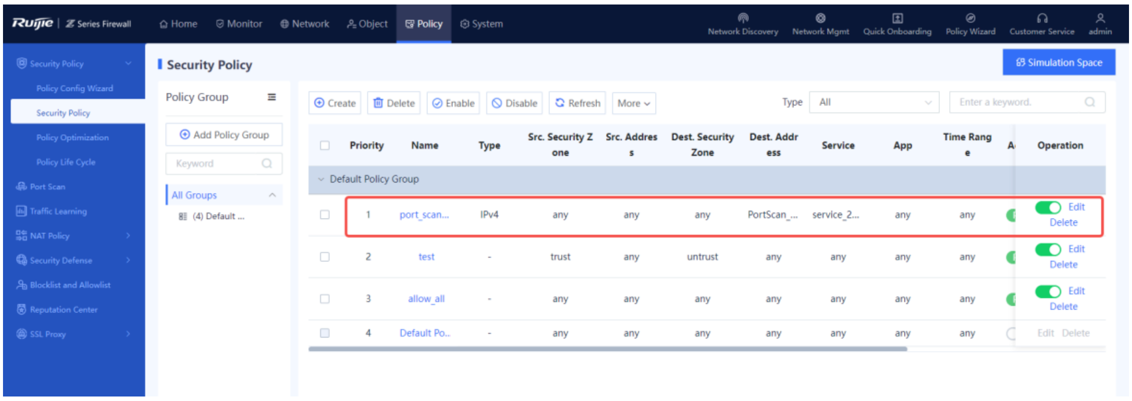
	IP	Port (Only Desc	状态	操作
□	172.20.37.54	22(Critical),2	4 0	Create Policy | View Details | Ignore | Delete
☑	172.20.37.124	22(Critical),2	4	Create Policy | View Details | Ignore | Delete

- Click **Create** to add the generated security policy to the security policy list.



Insert it to the specified location.

* Policy Name Prefix	port_scan1
* Policy Group	Default Policy Group
Policy	test
Before/After the Adjacent Policy	Before

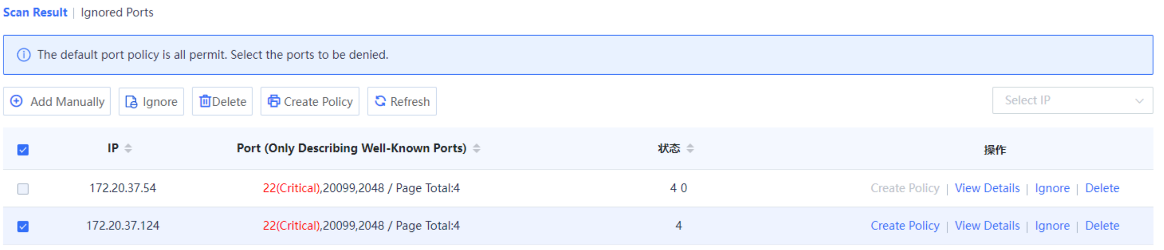


Security Policy

□	Priority	Name	Type	Src. Security Zone	Src. Address	Dest. Security Zone	Dest. Address	Service	App	Time Range	A	Operation
Default Policy Group												
□	1	port_scan...	IPv4	any	any	any	PortScan_...	service_2...	any	any		Edit Delete
□	2	test	-	trust	any	untrust	any	any	any	any		Edit Delete
□	3	allow_all	-	any	any	any	any	any	any	any		Edit Delete
□	4	Default Po...	-	any	any	any	any	any	any	any		Edit Delete

- Click **Add to Simulation Space** to add the generated policy to the simulation space. Run the policy in simulation mode and then add it to the security policy list.

Follow-up Procedure



Scan Result | Ignored Ports

The default port policy is all permit. Select the ports to be denied.

☑	IP	Port (Only Describing Well-Known Ports)	状态	操作
□	172.20.37.54	22(Critical),20099,2048 / Page Total:4	4 0	Create Policy | View Details | Ignore | Delete
☑	172.20.37.124	22(Critical),20099,2048 / Page Total:4	4	Create Policy | View Details | Ignore | Delete

- Move the cursor to the scanned port number, and the page displays the purpose of commonly used ports and the risk information of high-risk ports.

- Select an IP address and click **Create Policy** to generate a security policy for the IP address. On the port scan details page, you can set security policy actions, or edit policies on the security policy page.
- Select an IP address and click **View Details** to view the open port number of the IP address and generate a security policy for a single port number.
- Select an IP address and click **Ignore** to add all ports of the IP address to the ignored list and set the ignore period. (You can also add a single port to the ignored list on the port scan details page.) The device does not scan these ports in the ignore period. When the ignore period expires, the port is removed from the ignored list and the device can scan it.
- Select an IP address and click **Delete** to delete the scan result.

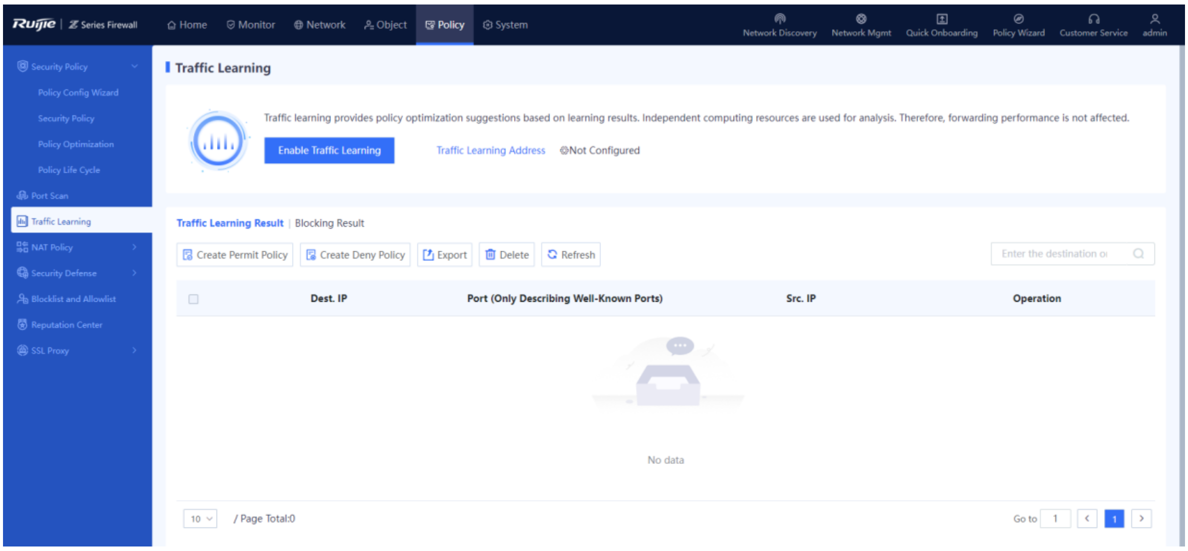
7.5 Traffic Learning

Application Scenario

During device deployment, you can sort out the assets on the network only after analyzing the traffic logs in a certain period. The traffic learning function automatically analyzes traffic logs, and sorts out the assets' IP addresses, open ports, and access relationships between assets on the network based on the assets' IP addresses or IP address ranges set by the customer.

Procedure

(1) Choose **Policy** > **Traffic Learning**.



Traffic Learning

Traffic learning provides policy optimization suggestions based on learning results. Independent computing resources are used for analysis. Therefore, forwarding performance is not affected.

Traffic Learning Address: Not Configured

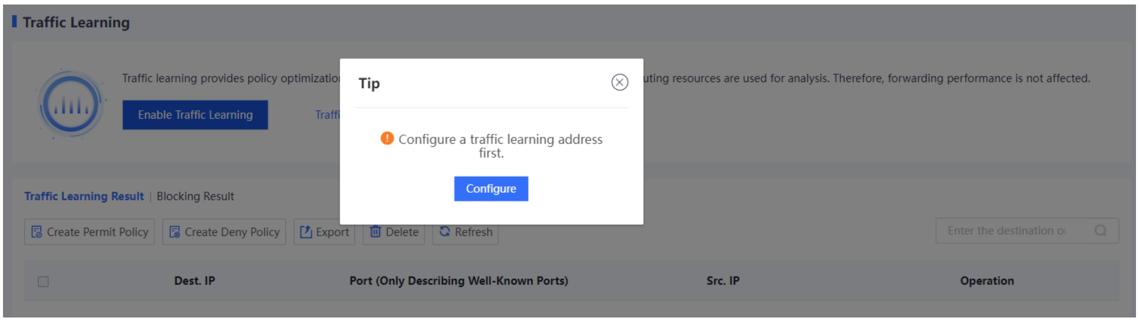
□	Dest. IP	Port (Only Describing Well-Known Ports)	Src. IP	Operation

No data

10 / Page Total:0

(2) (Optional) If the traffic learning address is not configured, configure it first.

a Click **Enable Traffic Learning** and click **Configure** in the prompt box to configure the traffic learning address.

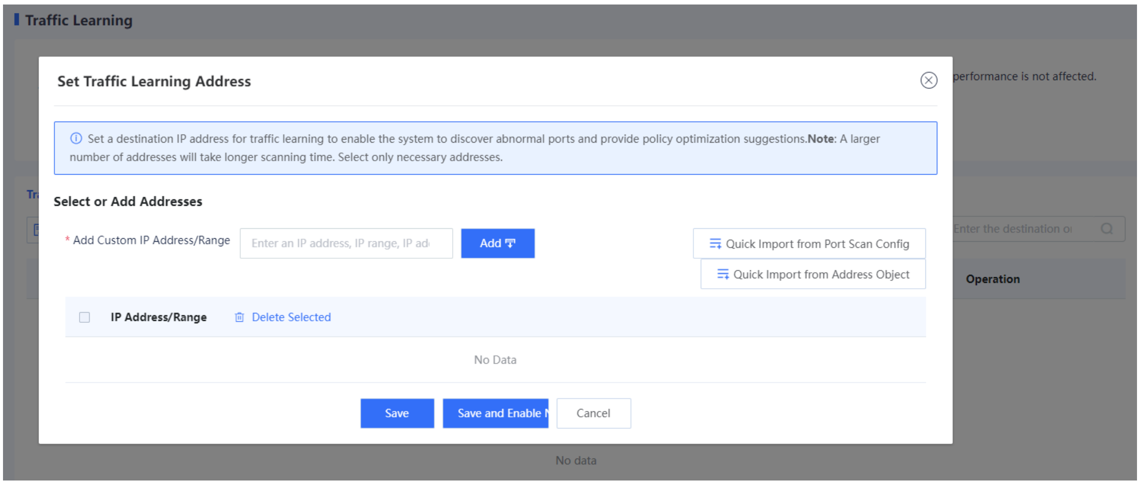


Traffic learning provides policy optimizatio … uting resources are used for analysis. Therefore, forwarding performance is not affected.

Configure a traffic learning address first.

b Select or add the IP address to be learned.

Enter the IP address or range to be learned in the **Add Custom IP Address/Range** input box, and click **Add** to add it to the **IP Address/Range** area.


Traffic Learning
Set Traffic Learning Address
performance is not affected.
Select or Add Addresses
* Add Custom IP Address/Range
Enter an IP address, IP range, IP ad
Add
Quick Import from Port Scan Config
Quick Import from Address Object
IP Address/Range
Delete Selected
No Data
Save
Save and Enable N
Cancel
Operation
Enter the destination o
No data

Set a destination IP address for traffic learning to enable the system to discover abnormal ports and provide policy optimization suggestions.**Note**: A larger number of addresses will take longer scanning time. Select only necessary addresses.

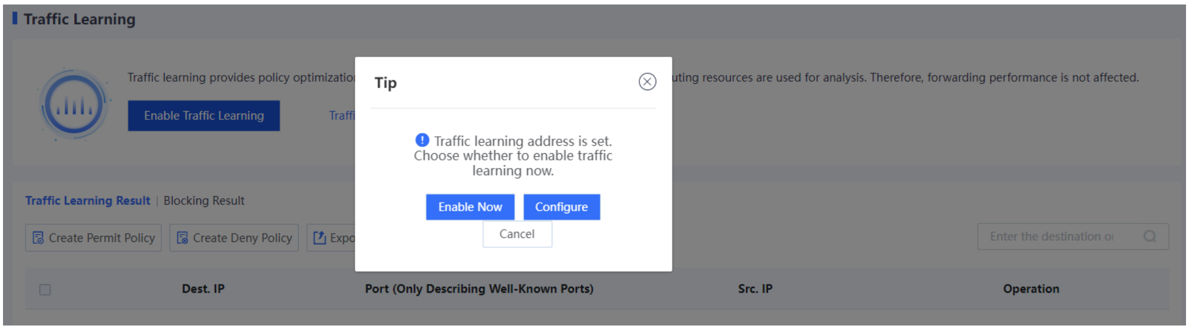
Note

To quickly add IP addresses, click **Quick Import from Port Scan Config** or **Quick Import from Address Object**.

c Choose whether to enable traffic learning immediately according to service situation.

- When services are busy, click **Save** to save the traffic learning address configuration. You can enable traffic learning when services are idle.
- When services are idle, click **Save and Enable Now** to save the traffic learning address configuration and enable traffic learning immediately.

(3) (Optional) If the traffic learning address has been configured, click **Enable Traffic Learning** to modify the traffic learning address or enable traffic learning immediately.



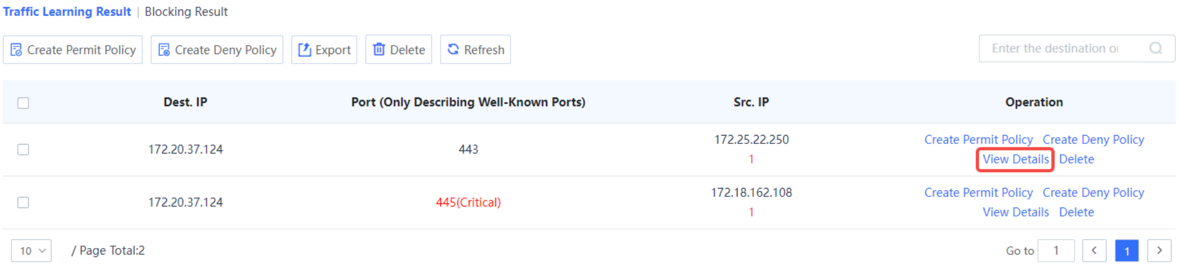
Traffic learning provides policy optimizatio… uting resources are used for analysis. Therefore, forwarding performance is not affected.

Traffic learning address is set. Choose whether to enable traffic learning now.

□	Dest. IP	Port (Only Describing Well-Known Ports)	Src. IP	Operation

Verification

- To view the information about learned IP addresses and ports, click the **Traffic Learning Result** tab. To view the detailed access relationship, click **View Details**.

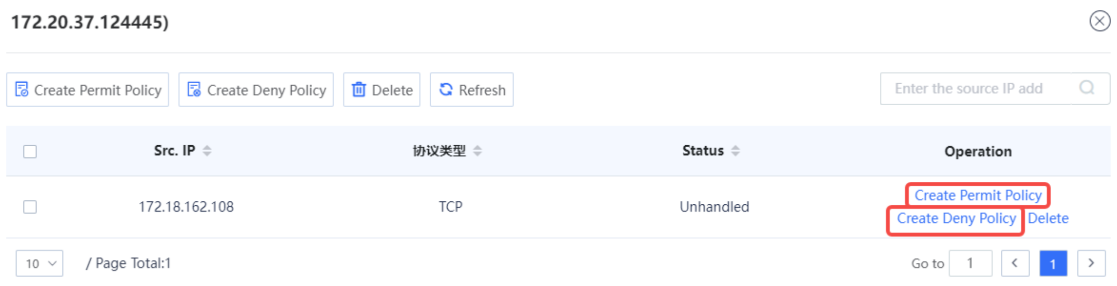


□	Dest. IP	Port (Only Describing Well-Known Ports)	Src. IP	Operation
□	172.20.37.124	443	172.25.22.250 1	Create Permit Policy Create Deny Policy View Details Delete
□	172.20.37.124	445(Critical)	172.18.162.108 1	Create Permit Policy Create Deny Policy View Details Delete

/ Page Total:2

- You can choose to generate a deny policy or a permit policy for a specific traffic learning result.

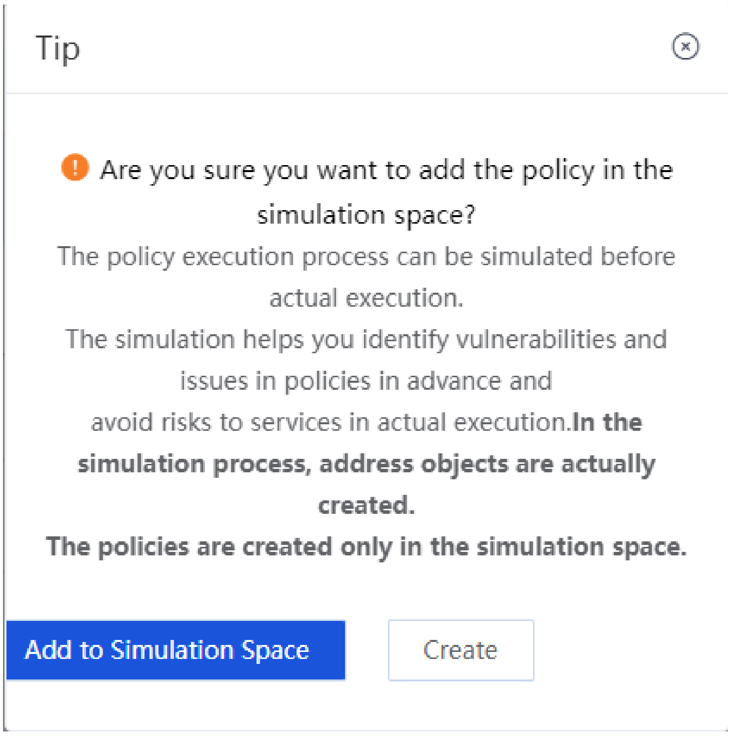
a On the traffic learning result page, click **Create Deny Policy** or **Create Permit Policy**.



□	Src. IP	协议类型	Status	Operation
□	172.18.162.108	TCP	Unhandled	Create Permit Policy Create Deny Policy Delete

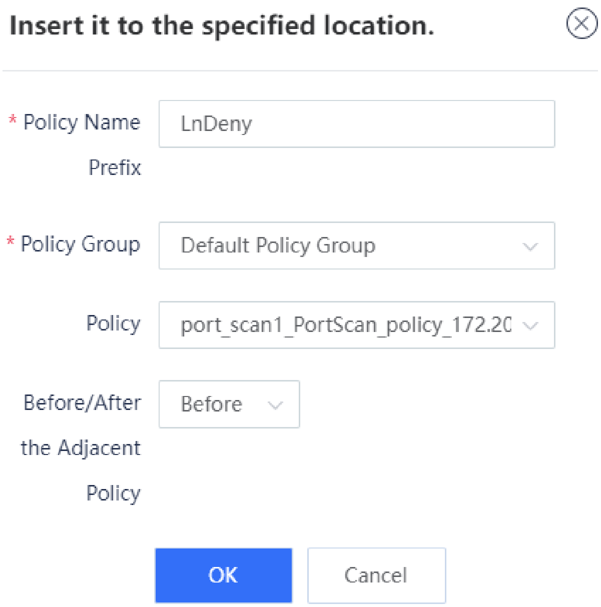
/ Page Total:1

b Add this policy to the simulation space or directly to the security policy list according to service requirements.



Tip

Are you sure you want to add the policy in the simulation space?
The policy execution process can be simulated before actual execution.
The simulation helps you identify vulnerabilities and issues in policies in advance and avoid risks to services in actual execution.**In the simulation process, address objects are actually created.**
The policies are created only in the simulation space.



Insert it to the specified location.

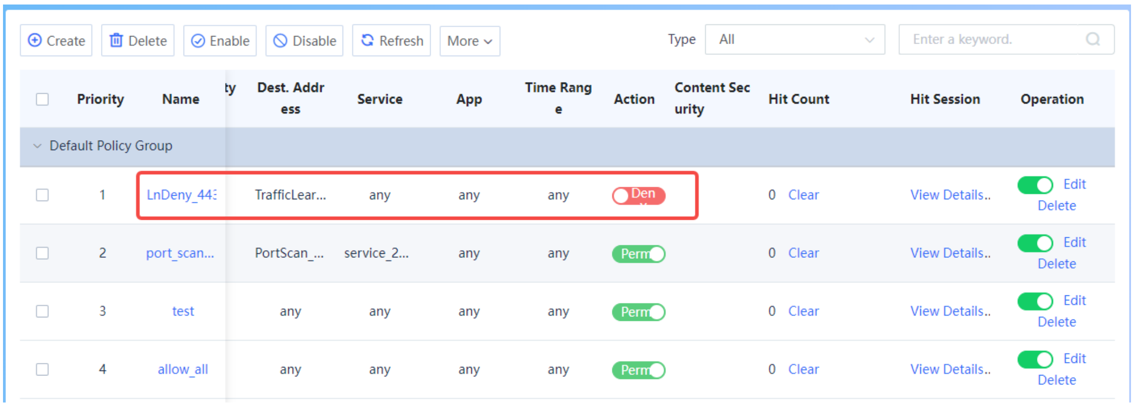
* Policy Name Prefix: LnDeny

* Policy Group: Default Policy Group

Policy: port_scan1_PortScan_policy_172.2C

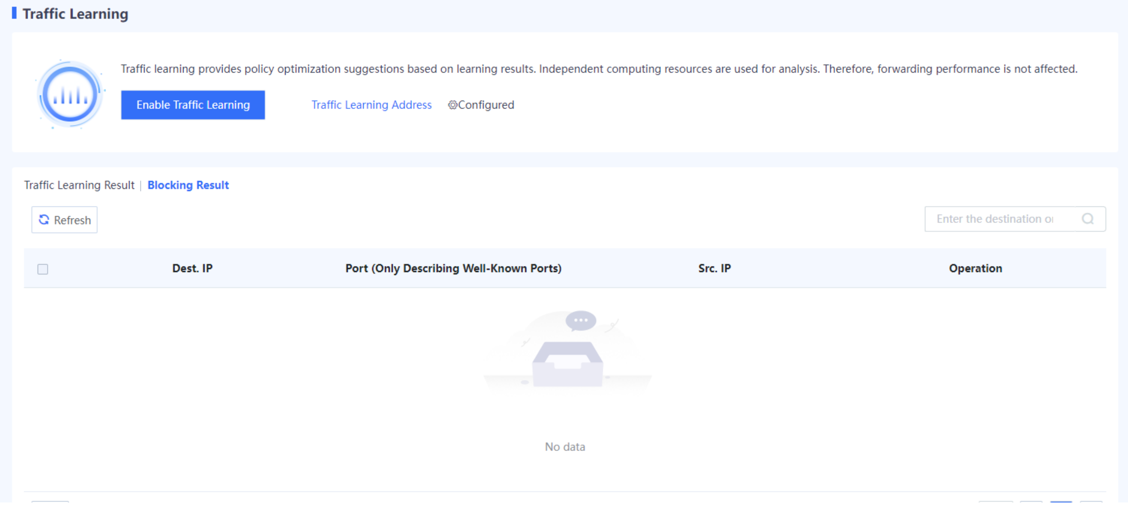
Before/After the Adjacent Policy: Before

c After confirming that the policy is appropriate in the simulation space, add it to the security policy list.



□	Priority	Name	ty	Dest. Address	Service	App	Time Range	Action	Content Security	Hit Count	Hit Session	Operation
Default Policy Group												
□	1	LnDeny_443		TrafficLear...	any	any	any	Den		0 Clear	View Details..	Edit Delete
□	2	port_scan...		PortScan_...	service_2...	any	any	Perm		0 Clear	View Details..	Edit Delete
□	3	test		any	any	any	any	Perm		0 Clear	View Details..	Edit Delete
□	4	allow_all		any	any	any	any	Perm		0 Clear	View Details..	Edit Delete

d To view the learned blocked access relationships, click the **Blocking Result** tab; to view the number of blocking times, blocking policy, blocked service, and the time of the last block, click **View Details**.



Traffic Learning

Traffic learning provides policy optimization suggestions based on learning results. Independent computing resources are used for analysis. Therefore, forwarding performance is not affected.

□	Dest. IP	Port (Only Describing Well-Known Ports)	Src. IP	Operation

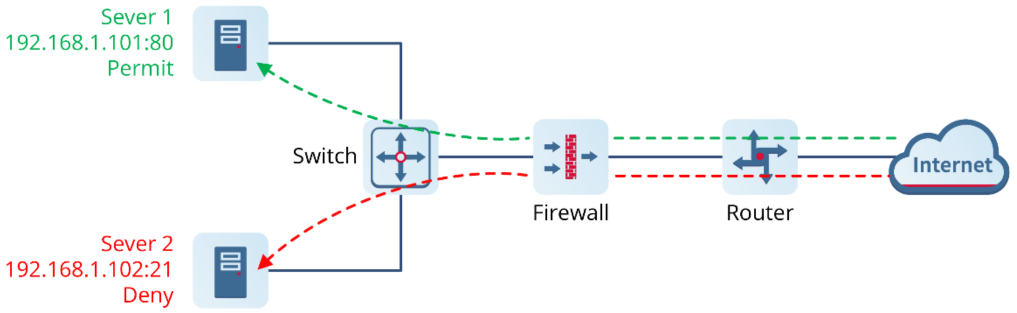
No data

7.6 Security Policy

7.6.1 Overview

The firewall verifies the passing traffic based on the security policy. Only the traffic matching the security policy with the permit action can be forwarded. For example, a firewall can be located at the boundary between an intranet and the Internet. A security policy is configured to establish a designated channel between the intranet and the Internet to filter sensitive data access.

With the stateful inspection packet filtering technology, firewalls can decide whether to allow packets to pass based on parameters such as IP address, service, port, and application type, and filter data at Layer 3 (network layer) and Layer 4 (transport layer).



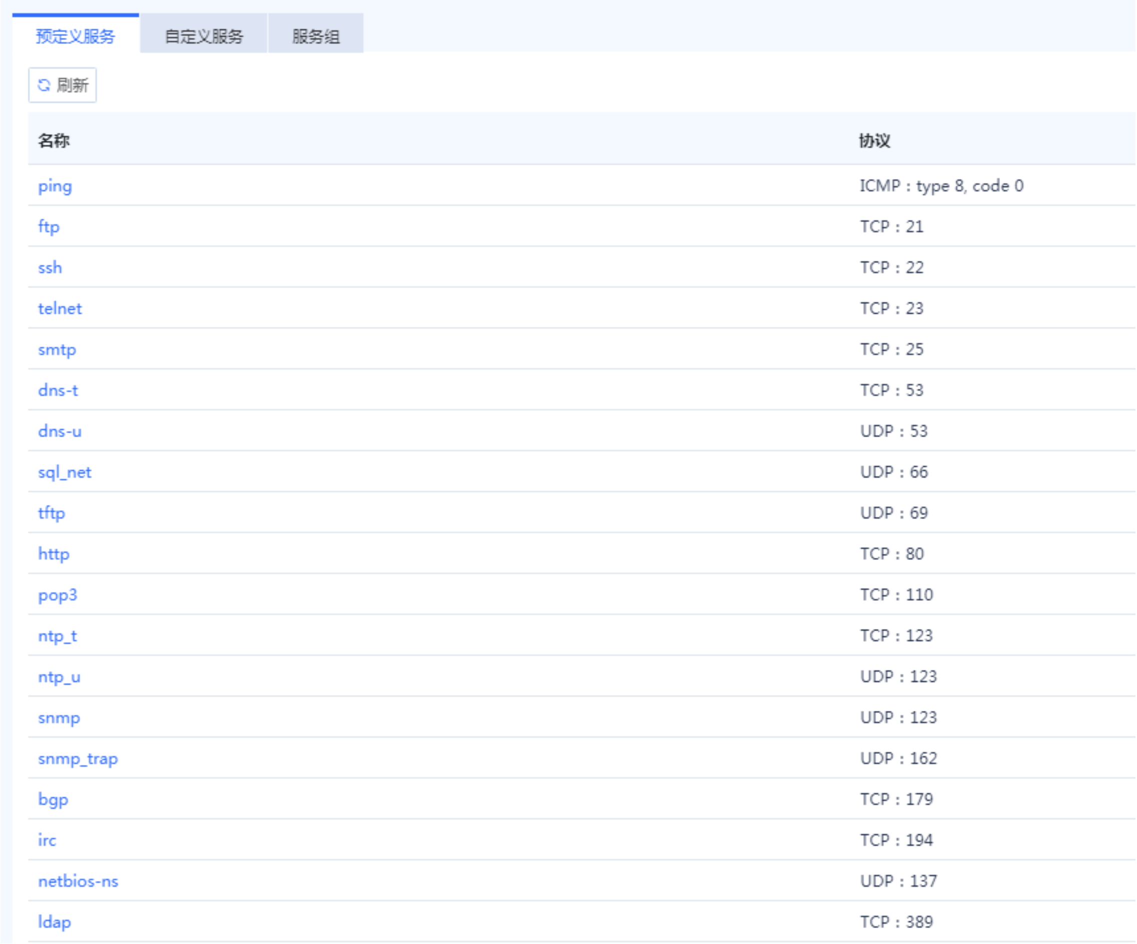
As shown in the figure above, the firewall can filter the source and destination IP addresses and ports. For example, the firewall can be configured to allow or deny some IP addresses on the intranet to access the Internet, and allow or deny some IP addresses on the Internet to access the intranet.

Z-S series firewalls support multiple address objects:

- Single IP address (for example, 202.1.1.1)
- IP address network segment (for example, 192.168.1.0/255.255.255.0)
- IP address range (for example: 172.16.1.100-172.16.2.200)

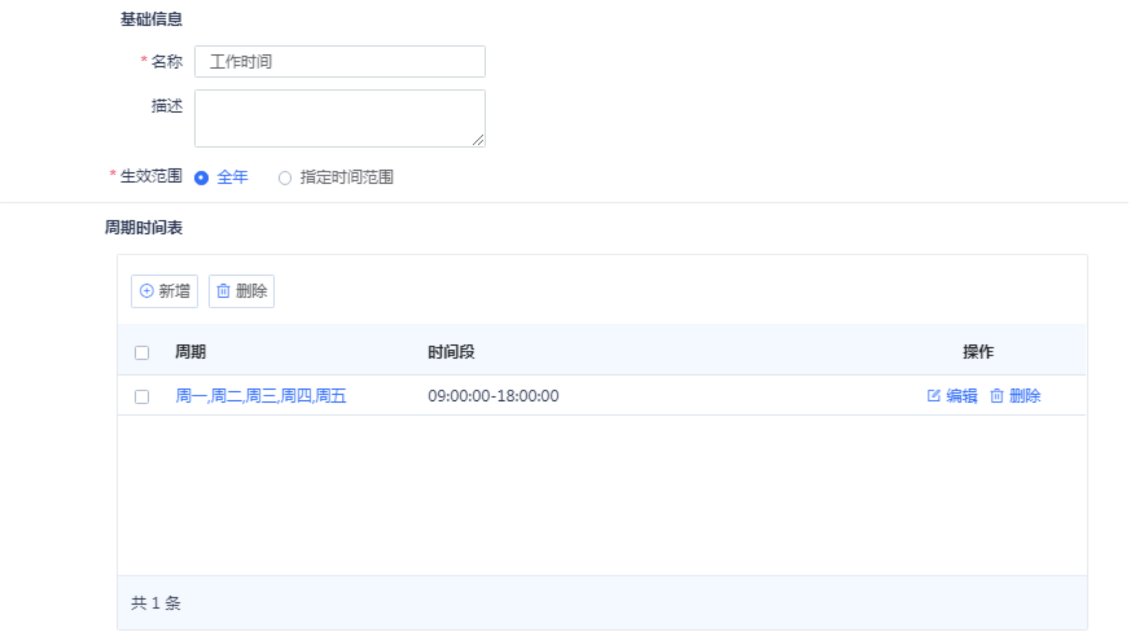
For different IP addresses/segments with the same access permission, you can add them to an address group and reference them uniformly in the firewall policy.

Z-S series firewalls are preconfigured with port information for common network services, such as TCP port 80 used for HTTP and TCP port 21/20 for FTP. You can also customize TCP/UDP/ICMP/IP services and ports. Similarly, you can add different services and ports into a group for uniform reference by the policy.



名称	协议
ping	ICMP : type 8, code 0
ftp	TCP : 21
ssh	TCP : 22
telnet	TCP : 23
smtp	TCP : 25
dns-t	TCP : 53
dns-u	UDP : 53
sql_net	UDP : 66
tftp	UDP : 69
http	TCP : 80
pop3	TCP : 110
ntp_t	TCP : 123
ntp_u	UDP : 123
snmp	UDP : 123
snmp_trap	UDP : 162
bgp	TCP : 179
irc	TCP : 194
netbios-ns	UDP : 137
ldap	TCP : 389

In addition to the IP address/port-based filtering function that traditional firewalls have, Z-S series firewalls can enforce different security policies for different time periods. For example, QQ is forbidden during working hours (such as 9:00-18:00 every day from Monday to Friday), but allowed in other time segments. This policy can be automatically implemented through the time-based policy of Z-S series firewalls.



基础信息

* 名称 工作时间

描述

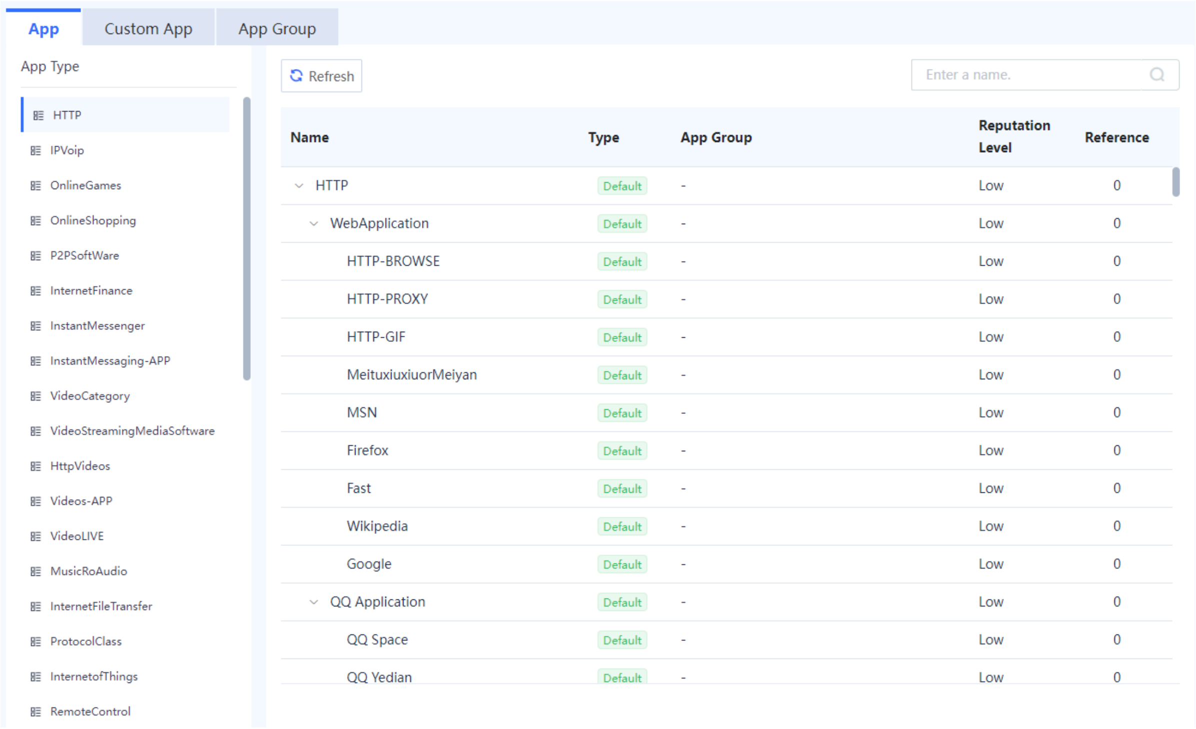
* 生效范围 ● 全年 ○ 指定时间范围

周期时间表

☐	周期	时间段	操作
☐	周一,周二,周三,周四,周五	09:00:00-18:00:00	编辑 删除

共 1 条

In addition, Z-S series firewalls can also enforce different security policies for the type of application of traffic. For example, to prevent intranet and extranet users from accessing game apps anywhere, anytime, configure a security policy and associate it with game apps.



Name	Type	App Group	Reputation Level	Reference
HTTP	Default	-	Low	0
WebApplication	Default	-	Low	0
HTTP-BROWSE	Default	-	Low	0
HTTP-PROXY	Default	-	Low	0
HTTP-GIF	Default	-	Low	0
MeituxiuxiuorMeiyan	Default	-	Low	0
MSN	Default	-	Low	0
Firefox	Default	-	Low	0
Fast	Default	-	Low	0
Wikipedia	Default	-	Low	0
Google	Default	-	Low	0
QQ Application	Default	-	Low	0
QQ Space	Default	-	Low	0
QQ Yedian	Default	-	Low	0

Through the flexible combination of IP address, port, user, device, time and other parameters, a variety of firewall policies meeting actual network security needs can be configured, so that the user's security policy can be effectively implemented.

By default, the device is configured with a security policy that blocks all packets, and the default policy cannot be deleted or modified.

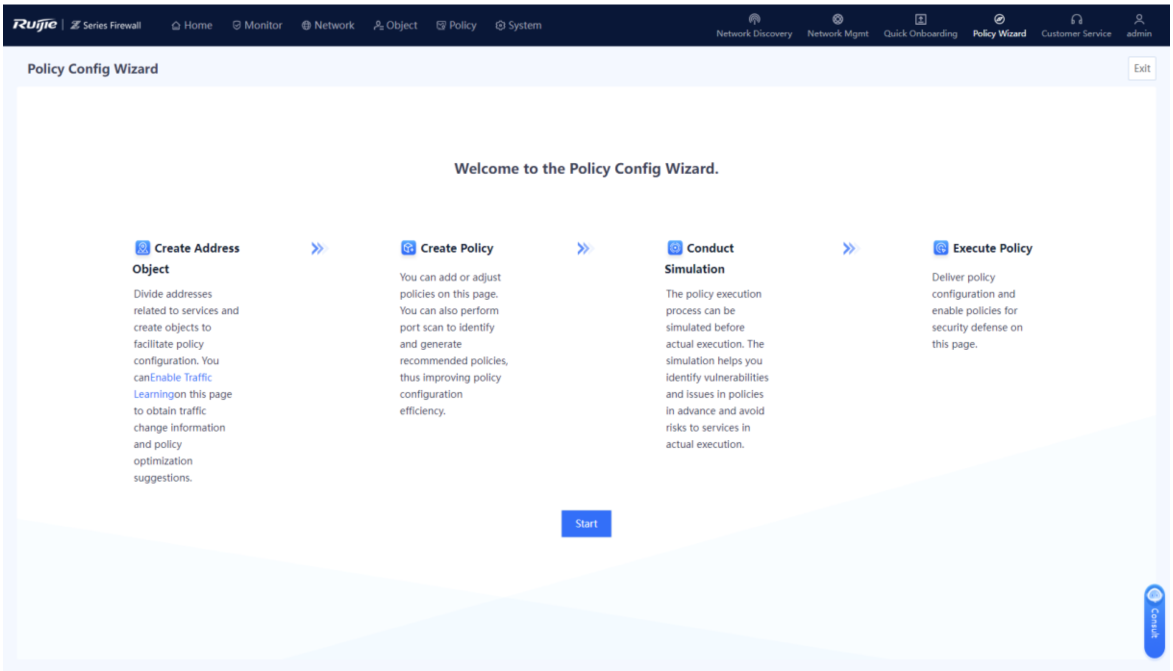
7.6.2 Configuring Security Policy (Using Wizard)

The web UI of Z-S series firewalls provides the policy configuration wizard for you to complete configuration and deployment efficiently.

Perform the following operations to enter the security policy configuration wizard:

(1) On the right of icon and panel area, click **Policy Wizard**.

(2) Click **Start** to enter the **Policy Config Wizard** page. Perform the operations according to the wizard.



Welcome to the Policy Config Wizard.

Create Address Object

Divide addresses related to services and create objects to facilitate policy configuration. You canEnable Traffic Learningon this page to obtain traffic change information and policy optimization suggestions.

Create Policy

You can add or adjust policies on this page. You can also perform port scan to identify and generate recommended policies, thus improving policy configuration efficiency.

Conduct Simulation

The policy execution process can be simulated before actual execution. The simulation helps you identify vulnerabilities and issues in policies in advance and avoid risks to services in actual execution.

Execute Policy

Deliver policy configuration and enable policies for security defense on this page.

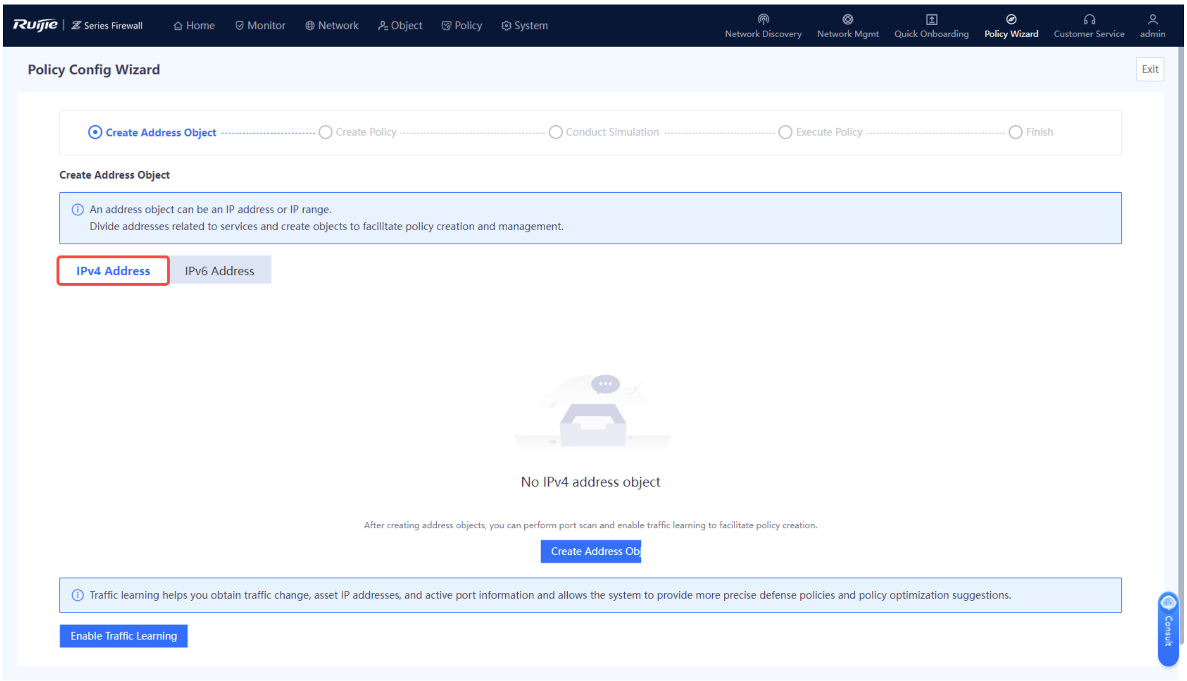
1. Creating an Address Object

Application Scenario

By using the address object, you can classify service-related IP addresses (including intranet or extranet IP addresses), facilitating management of traffic within the specified IP address range.

Procedure

(1) Address objects include IPv4 address objects and IPv6 address objects. Configure the address objects based on the actual applications. On the **Create Address Object** page, select the tab of the address object to be created, for example, **IPv4 Address**.



Create Address Object

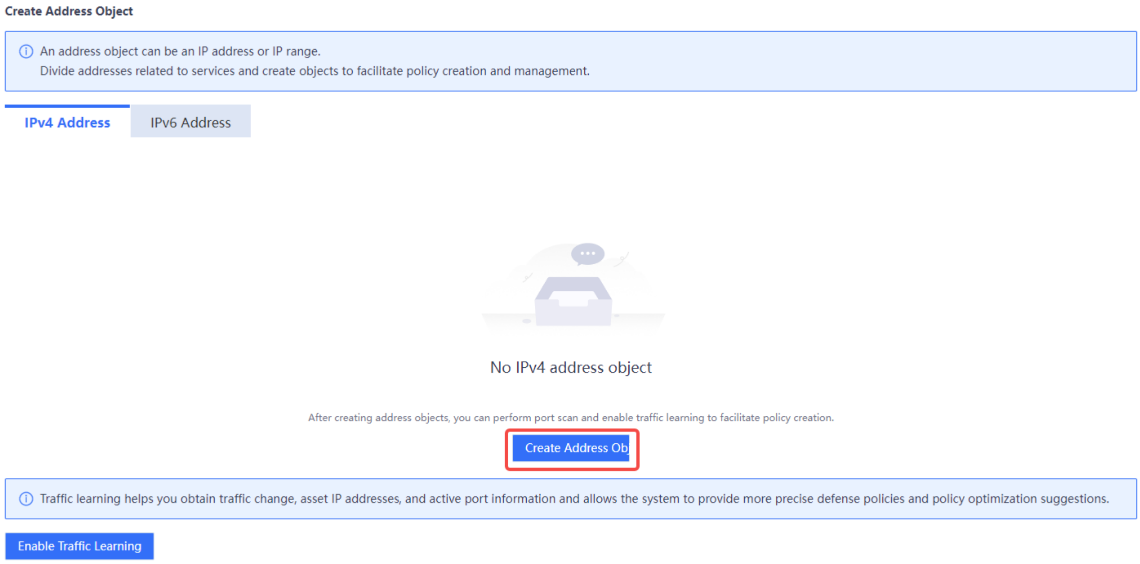
An address object can be an IP address or IP range.
Divide addresses related to services and create objects to facilitate policy creation and management.

No IPv4 address object

After creating address objects, you can perform port scan and enable traffic learning to facilitate policy creation.

Traffic learning helps you obtain traffic change, asset IP addresses, and active port information and allows the system to provide more precise defense policies and policy optimization suggestions.

(2) Click **Create Address Object**.



Create Address Object

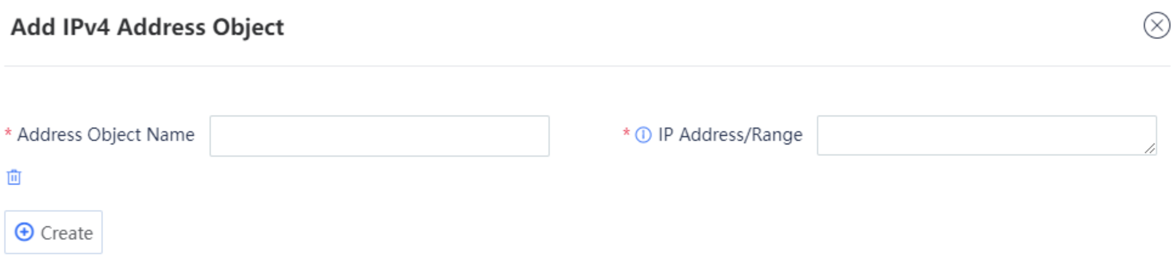
An address object can be an IP address or IP range.
Divide addresses related to services and create objects to facilitate policy creation and management.

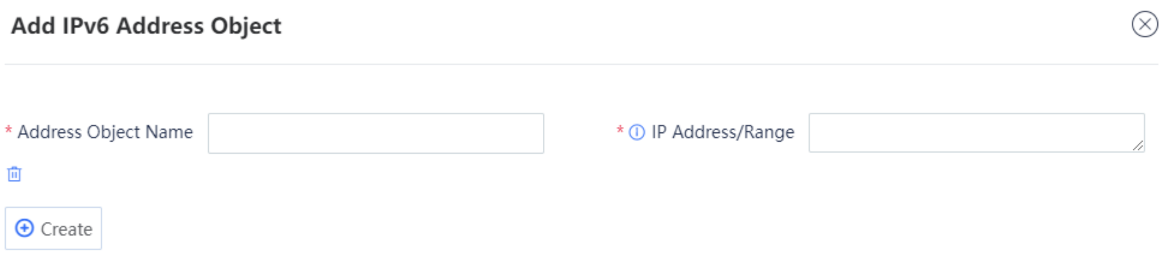
No IPv4 address object

After creating address objects, you can perform port scan and enable traffic learning to facilitate policy creation.

Traffic learning helps you obtain traffic change, asset IP addresses, and active port information and allows the system to provide more precise defense policies and policy optimization suggestions.

(3) Fill the names and IP addresses/ranges in the **Add IPv4 Address Object** or **Add IPv6 Address Object** page.





Item	**Description**	**Remarks**
Address Object Name	Name of the IP address object.	[Example] Addr1
IP Address/Range	IP address or range.	Three configuration methods are supported: ● IP address: One or multiple IP addresses. Input an IP address per line. Press **Enter** to separate lines. ○ Example 1: 192.168.20.3 ○ Example 2: 1234::100 ● IP address range: A contiguous range of addresses. Connect the start IP address and end IP address with a hyphen (-). ○ Example 1: 192.168.20.1-192.168.20.3 ○ Example 2: 1234::100-2345::100 ● Network segment: IP address network segment ○ Example 1: 192.168.1.0/24 or 192.168.1.0/255.255.255.0 ○ Example 2: 1234::100/100

Note

To add multiple address objects, click **Create**.

(4) Click **Confirm Creation**.

(5) Select address objects, and click **Next**.

Follow-up Procedure

- You can choose **Object** > **Address** to view, add, edit, and delete address objects.
- You can only delete the address with reference 0.

2. Configuring a Security Policy

Application Scenario

Configure the security policy according to the configuration wizard.

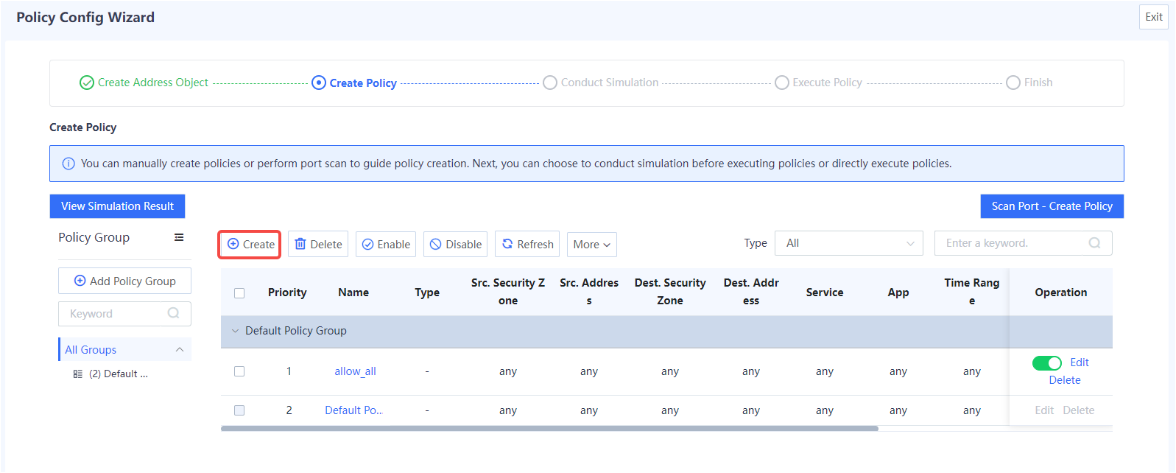
The security policy verifies the traffic passing the firewall. Only the traffic matching the security policy with the permit action can be forwarded. The security policy function provides security defense. For example, a firewall can be located at the boundary between an intranet and the Internet. A security policy is configured to establish a designated channel between the intranet and the Internet to filter sensitive data access.

Prerequisites

The security zone, service, service group, application group, time plan, and intrusion prevention policy have been created according to service requirements.

Procedure

(1) On the **Create Policy** page, click **Create**.



Policy Config Wizard

Create Policy

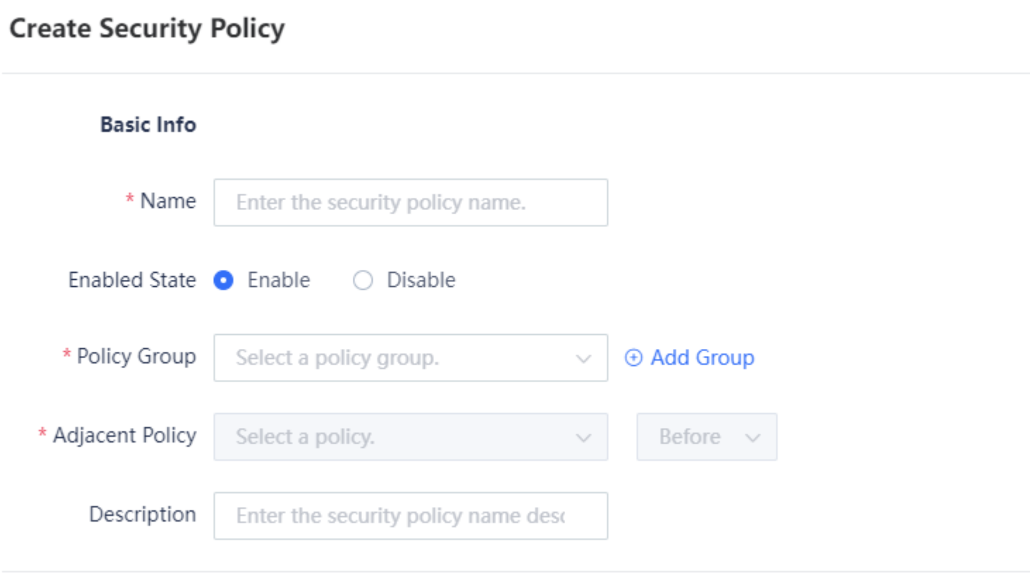
You can manually create policies or perform port scan to guide policy creation. Next, you can choose to conduct simulation before executing policies or directly execute policies.

Type: All

□	Priority	Name	Type	Src. Security Zone	Src. Address	Dest. Security Zone	Dest. Address	Service	App	Time Range	Operation
Default Policy Group											
□	1	allow_all	-	any	any	any	any	any	any	any	Edit Delete
□	2	Default Po..	-	any	any	any	any	any	any	any	Edit Delete

(2) Set parameters related to security policy.

a Configure basic information about security policy.



Create Security Policy

Basic Info

* Name: Enter the security policy name.

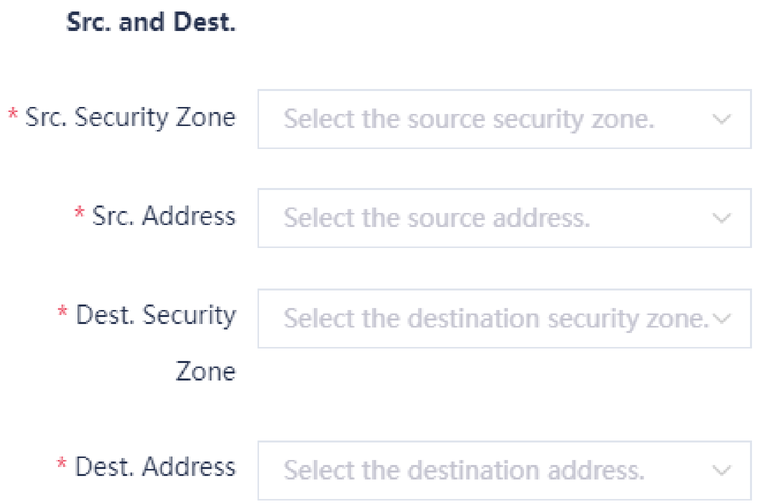
Enabled State: ● Enable ○ Disable

* Policy Group: Select a policy group. ⊕ Add Group

* Adjacent Policy: Select a policy. Before

Description: Enter the security policy name desc

b Configure the source and destination security zones and addresses of the target data connection.



Src. and Dest.

* Src. Security Zone: Select the source security zone.

* Src. Address: Select the source address.

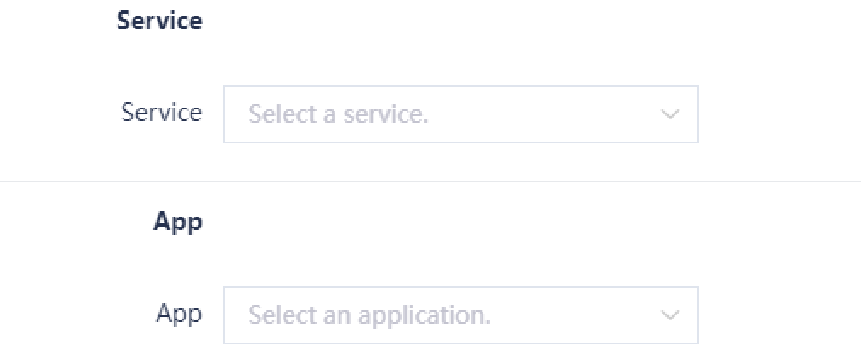
* Dest. Security Zone: Select the destination security zone.

* Dest. Address: Select the destination address.

Item	Description	Remarks
Src. Security Zone	Security zone initiating the target data connection.	Select from the drop-down list. [Example] untrust

Item	Description	Remarks
Src. Address	Source address that initiates the target data connection.	Select a source address in the **To-be-selected** area. The selected address is automatically added to the **Selected** area. [Example] Any
Dest. Security Zone	Destination security zone of the target data connection.	Select from the drop-down list. [Example] trust
Dest. Address	Destination address of the target data connection.	Select a source address in the **To-be-selected** area. The selected address is automatically added to the **Selected** area. [Example] Any

c (Optional) Select the service and application of the target data connection request.



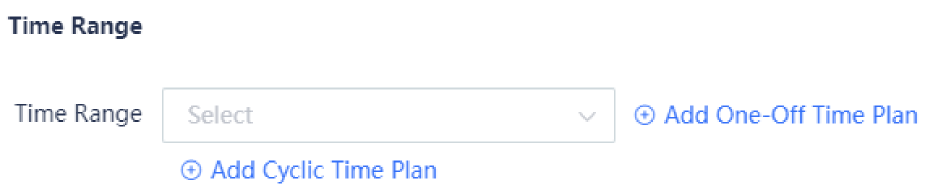
Service

Service: Select a service.

App

App: Select an application.

d (Optional) Select the time range in which the policy is effective.

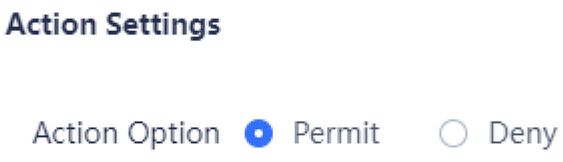


Time Range

Time Range Select ⊕ Add One-Off Time Plan

⊕ Add Cyclic Time Plan

e Configure the action taken by the security policy. Permit or deny the target data connection.

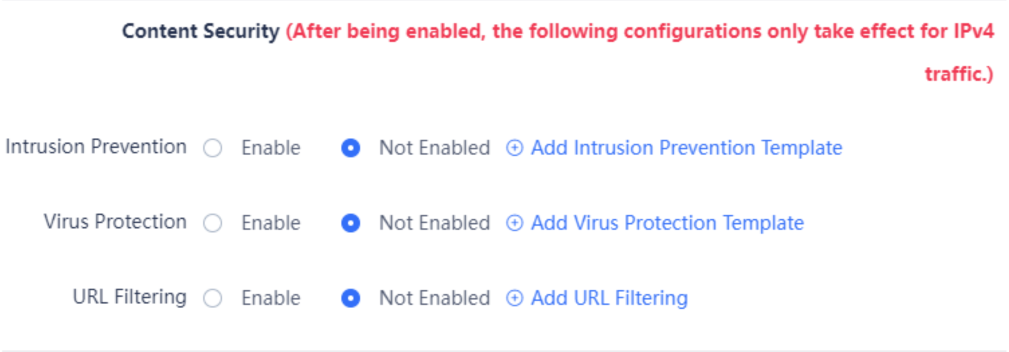


Action Settings

Action Option ● Permit ○ Deny

Action	Description
Permit	If the action is set to **Permit**, the device performs check according to whether content security check is enabled: Content security check is not enabled: Directly permit the traffic. Content security check is enabled: Process the traffic according to the content check policy.
Deny	Block the traffic.

f Set whether to enable content security checks for the target data connection, which takes effect only for IPv4 traffic.



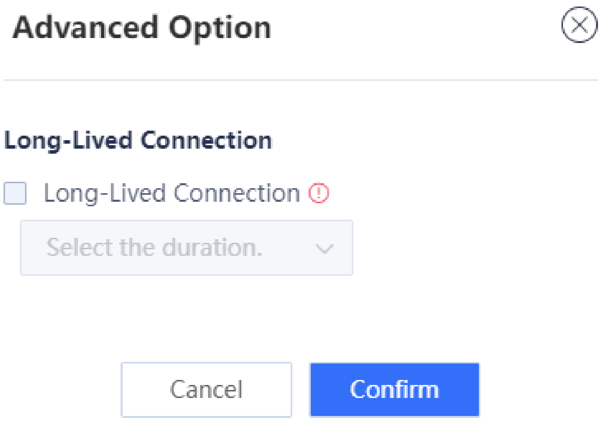
Content Security (After being enabled, the following configurations only take effect for IPv4 traffic.)

Intrusion Prevention ○ Enable ● Not Enabled ⊕ Add Intrusion Prevention Template

Virus Protection ○ Enable ● Not Enabled ⊕ Add Virus Protection Template

URL Filtering ○ Enable ● Not Enabled ⊕ Add URL Filtering

g Click **Settings** in the **Advanced** area. Configure long-lived connection attributes and click **Confirm**.



Advanced Option

Long-Lived Connection

☐ Long-Lived Connection

h Click **Save**.

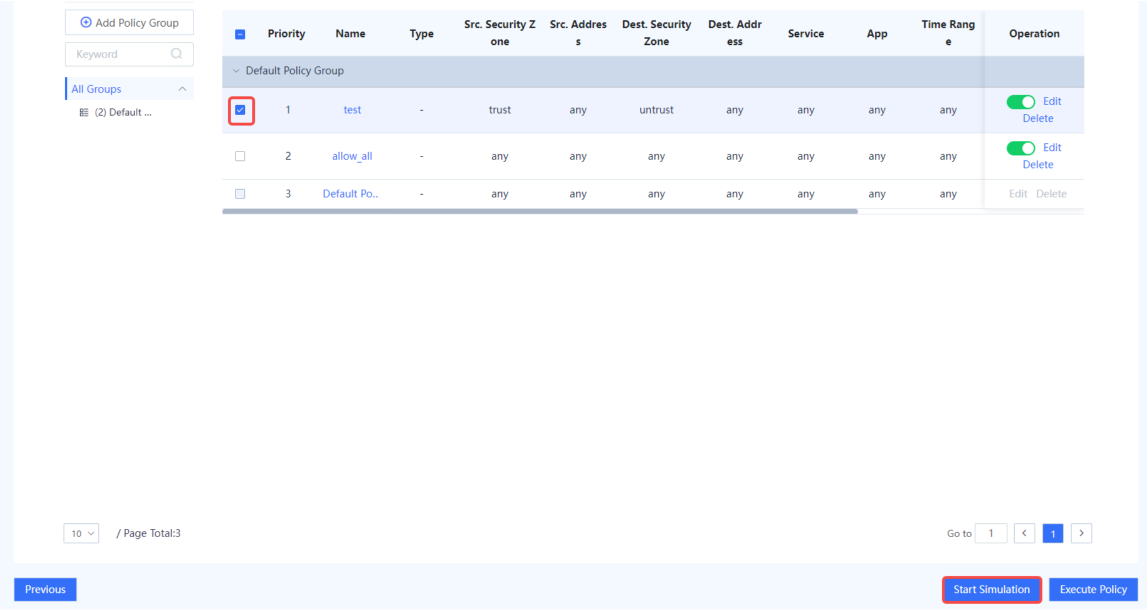
3. Simulation Run

Application Scenario

After you create a security policy, you can conduct simulation run to discover vulnerabilities or problems of the policy in advance to avoid risks to services in actual implementation.

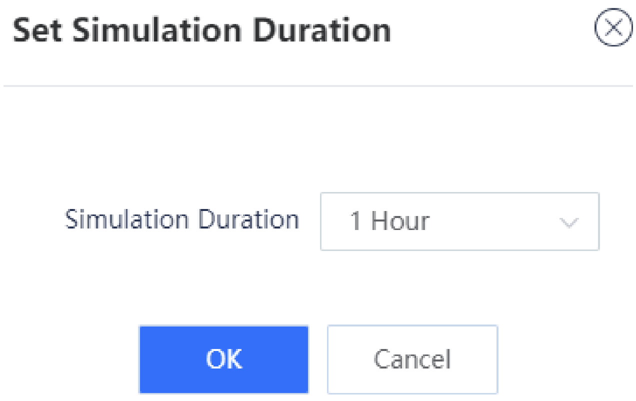
Procedure

(1) On the **Create Policy** page, select the policy for which simulation run will be performed, and click **Start Simulation**.



	Priority	Name	Type	Src. Security Zone	Src. Address	Dest. Security Zone	Dest. Address	Service	App	Time Range	Operation
Default Policy Group											
☑	1	test	-	trust	any	untrust	any	any	any	any	Edit Delete
☐	2	allow_all	-	any	any	any	any	any	any	any	Edit Delete
☐	3	Default Po..	-	any	any	any	any	any	any	any	Edit Delete

(2) In the **Set Simulation Duration** dialog box, set the duration of simulation run.

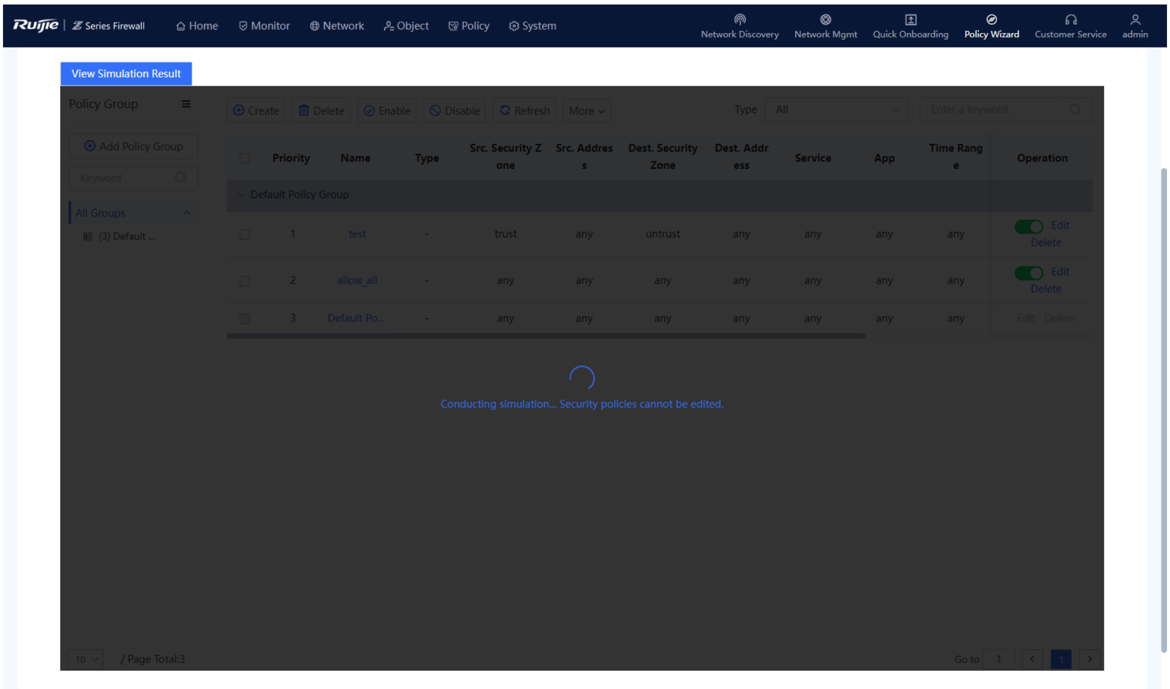


Set Simulation Duration

Simulation Duration: 1 Hour

(3) Click **OK**.

The system automatically performs simulation run for the selected policies.



	Priority	Name	Type	Src. Security Zone	Src. Address	Dest. Security Zone	Dest. Address	Service	App	Time Range	Operation
Default Policy Group											
□	1	test	-	trust	any	untrust	any	any	any	any	Edit Delete
□	2	allow_all	-	any	any	any	any	any	any	any	Edit Delete
□	3	Default Po...	-	any	any	any	any	any	any	any	Edit Delete

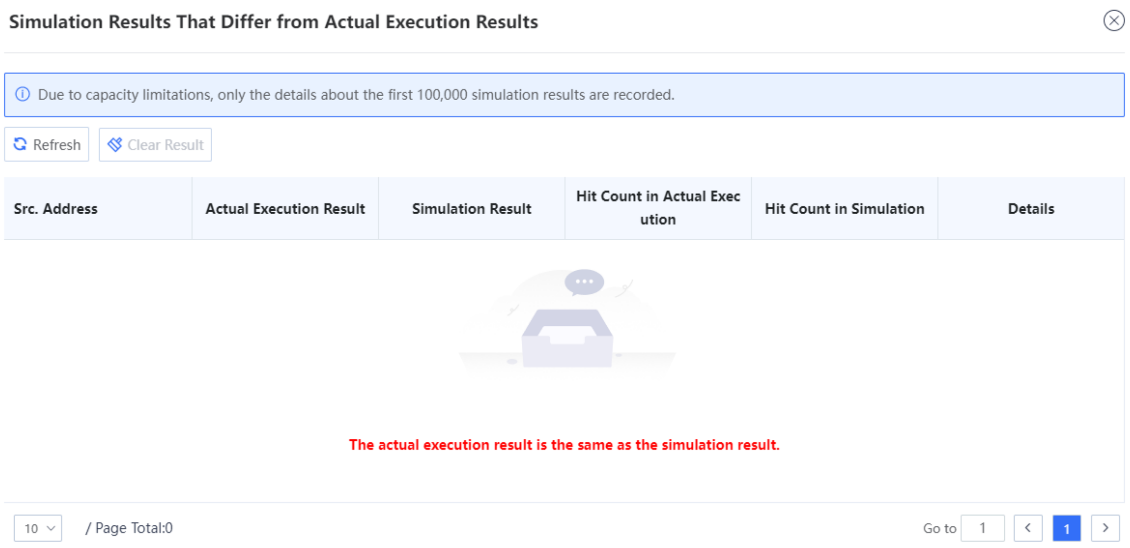
Conducting simulation... Security policies cannot be edited.

(4) When simulation run is finished, click **View Simulation Result** on the **Create Policy** page.

Simulation run results are displayed based on the source IP address:

- The number of times traffic is permitted in the real policy but blocked in the simulated policy.
- The number of times traffic is permitted in the simulated policy but blocked in the real policy.

(5) Analyze whether the simulation results differ from actual execution results.



Simulation Results That Differ from Actual Execution Results

Due to capacity limitations, only the details about the first 100,000 simulation results are recorded.

Src. Address	Actual Execution Result	Simulation Result	Hit Count in Actual Execution	Hit Count in Simulation	Details

The actual execution result is the same as the simulation result.

(6) If the simulation results are as expected, click **Apply to Real Network** to make the policy effective.

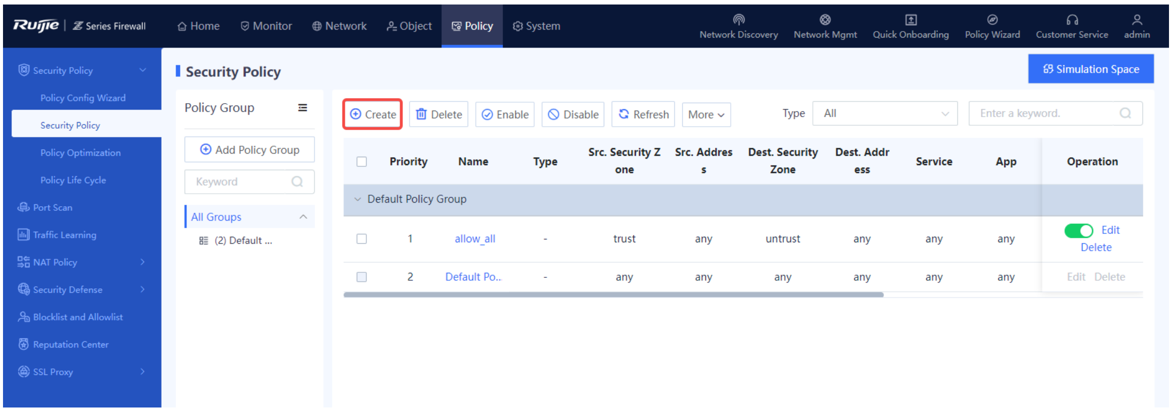
7.6.3 Configuring Security Policy (Manual)

Application Scenario

In addition to the wizard, RG-WALL 1600-Z-S series firewalls support manual configuration. You can manually configure security policies according to service needs.

Procedure

(1) Choose **Policy** > **Security Policy**.

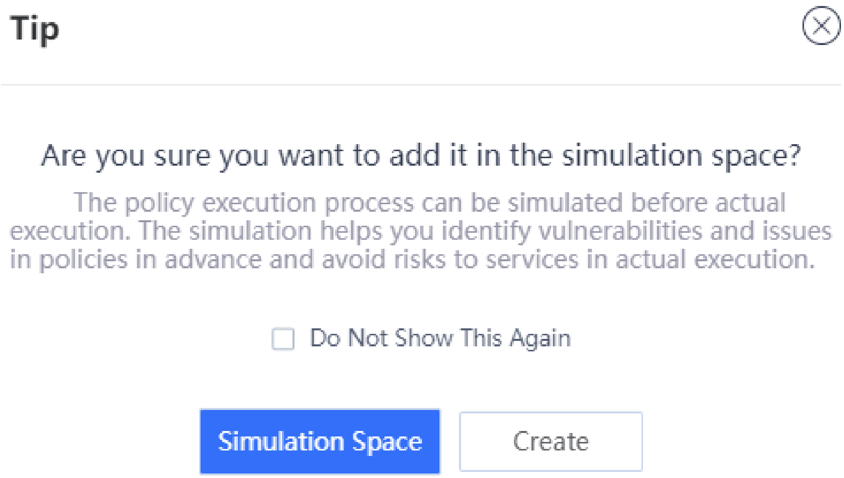


Security Policy

Priority	Name	Type	Src. Security Zone	Src. Address	Dest. Security Zone	Dest. Address	Service	App	Operation
Default Policy Group									
1	allow_all	-	trust	any	untrust	any	any	any	Edit Delete
2	Default Po..	-	any	any	any	any	any	any	Edit Delete

(2) In the operation area, click **Create**.

The system displays a tip.



Tip

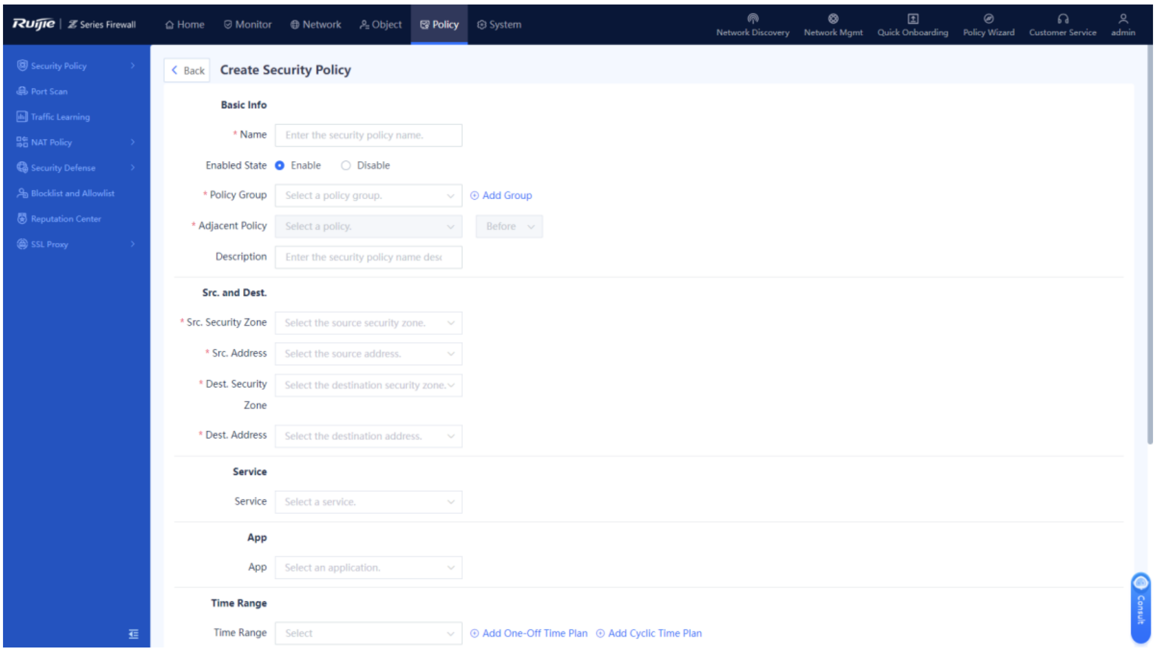
Are you sure you want to add it in the simulation space?

The policy execution process can be simulated before actual execution. The simulation helps you identify vulnerabilities and issues in policies in advance and avoid risks to services in actual execution.

□ Do Not Show This Again

(3) Click **Create**.

The system displays the **Create Security Policy** page.



Create Security Policy

Basic Info

* Name: Enter the security policy name.

Enabled State: ● Enable ○ Disable

* Policy Group: Select a policy group. ⊕ Add Group

* Adjacent Policy: Select a policy. Before

Description: Enter the security policy name desc

Src. and Dest.

* Src. Security Zone: Select the source security zone.

* Src. Address: Select the source address.

* Dest. Security Zone: Select the destination security zone.

* Dest. Address: Select the destination address.

Service

Service: Select a service.

App

App: Select an application.

Time Range

Time Range: Select ⊕ Add One-Off Time Plan ⊕ Add Cyclic Time Plan

(4) Set parameters of security policy.

Item	**Description**	**Remarks**
Basic Info		
Name	Security policy name.	Characters such as

<table>
<tr><th>Item</th><th>Description</th><th>Remarks</th></tr>
<tr><td></td><td></td><td>`~!#%^&*+\/0::"/<>? and spaces are not allowed.
[Example]
Trust_to_untrust</td></tr>
<tr><td>Enabled State</td><td>Whether to enable the new security policy.</td><td>[Example]
Enable</td></tr>
<tr><td>Policy Group</td><td>Policy group to which the new security policy belongs.</td><td>● Select from the drop-down list.
● Click <b>Add Group</b> to add a custom policy group.
[Example]
Default policy group.</td></tr>
<tr><td>Adjacent Policy</td><td>Move the new security policy before or after the specified policy. The closer a policy is to the front, the higher its priority is in matching.</td><td>-</td></tr>
<tr><td>Descriptio n</td><td>Security policy description.</td><td>Characters such as `~!#%^&*+\|{};:'"/<>? are not allowed.
[Example]
Perform virus detection for the HTTP traffic from security zone 1 to security zone 2.</td></tr>
<tr><td colspan="3">Src. and Dest.</td></tr>
<tr><td>Src. Security Zone</td><td>Source security zone initiating the target data.</td><td>● Click the drop-down list, and select a source security zone in the <b>To-be-selected</b> area. The selected zone is automatically</td></tr>
</table>

Item	Description	Remarks
		added to the **Selected** area. ● Click **Add Security Zone** to add a custom security zone. [Example] trust
Src. Address	Source address that initiates the target data connection.	Click the drop-down list, and select a source address in the **To-be-selected** area. The selected address is automatically added to the **Selected** area. [Example] Any
Dest. Security Zone	Destination security zone of the target data connection.	● Click the drop-down list, and select a destination security zone in the **To-be-selected** area. The selected zone is automatically added to the **Selected** area. ● Click **Add Security Zone** to add a custom security zone. [Example] trust
Dest. Address	Destination address of the target data connection.	Click the drop-down list, and select a destination address in the **To-be-selected** area. The selected address is automatically added to the **Selected** area. [Example] Any

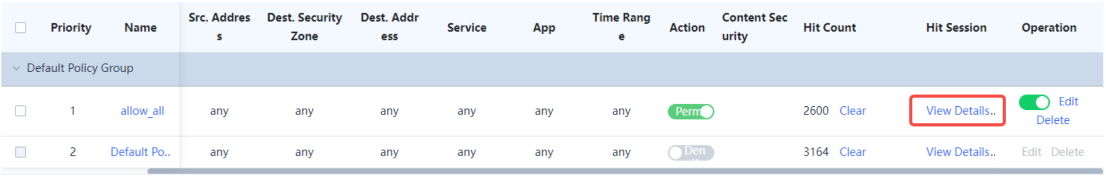
Item	Description	Remarks
Service	Service type of the target data connection request.	[Example] Any
App	Application type of the target data connection request.	[Example] Any
Time Range	Time segment in which the security policy is valid. You can associate the policy with a one-off time plan. That is, the policy takes effect only once. You can also associate the policy with a cyclic time plan. That is, the policy periodically takes effect in the specified time segment.	● To add a one-off time plan, click **Add One-Off Time Plan**. ● To add a cyclic time plan, click **Add Cyclic Time Plan**. [Example] Any
Action Option	Action taken by the security policy to permit or deny the target data connection.	[Example] Permit
Content Security	Whether intrusion prevention and virus detection are enabled for the target data connection. If you want to enable content security check, you must specify the intrusion prevention and virus protection templates, and configure the actions.	The configuration of content security takes effect on only IPv4 traffic. [Example] ● Intrusion Prevention: Enable ● Virus Protection: Enable ● URL Filtering: Not Enabled
Advanced	Advanced settings of the security policy, including: **Long-Lived Connection**: applies to the special servers that require long-lived connections. After this function is enabled, the server's connection request is not restricted by	Click **Settings**, and set parameters on the displayed **Advanced Option** page. [Example] Select **Long-Lived Connection**.

Item	Description	Remarks
	the connection timeout setting of the firewall. The connection duration needs to be set.	

(5) Click **Save**.

Follow-up Procedure

- When the security policy, virus protection policy, or intrusion prevention policy is hit, a security log is recorded. You can choose **Monitor** > **Log Monitoring** > **Security Log** to view the log information.
- When user traffic hits the security policy, click **View Details** in the hit session to view the session information.



□	Priority	Name	Src. Address	Dest. Security Zone	Dest. Address	Service	App	Time Range	Action	Content Security	Hit Count	Hit Session	Operation
Default Policy Group													
□	1	allow_all	any	any	any	any	any	any	Perm		2600 Clear	View Details..	Edit Delete
□	2	Default Po..	any	any	any	any	any	any	Den		3164 Clear	View Details..	Edit Delete

7.6.4 Adjusting Policy Order

Application Scenario

When you configure multiple security policies, the list of security policies is arranged in the order of configuration by default. The security policies that are configured earlier have higher priorities. Security policy matching is performed in the order of the policy list, that is, starting from the top of the policy list. If the traffic matches a security policy, the next policy will not be matched.

You can adjust the order of security policies to meet service requirements.

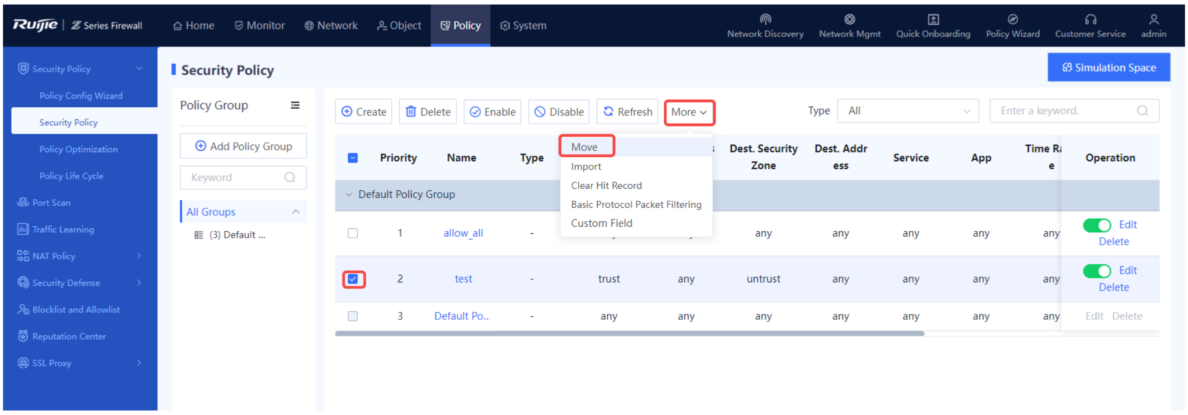
Note

- There is a default security policy in the system that has the lowest priority. It blocks all data connections.
- When a data connection fails to hit a configured policy and hit the default policy, the data connection is blocked.

Procedure

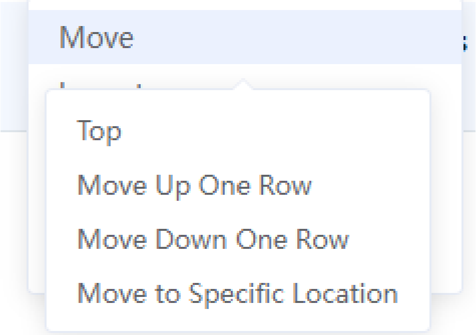
(1) Choose **Policy** > **Security Policy**.

(2) Select the policy of which the priority needs to be adjusted.



☐	Priority	Name	Type			Dest. Security Zone	Dest. Address	Service	App	Time Range	Operation
Default Policy Group											
☐	1	allow_all	-			any	any	any	any	any	Edit Delete
☑	2	test	-	trust	any	untrust	any	any	any	any	Edit Delete
☐	3	Default Po...	-	any	any	any	any	any	any	any	Edit Delete

(3) Click **More** and select **Move**. Select the required operation from the shortcut menu to move the selected policy.



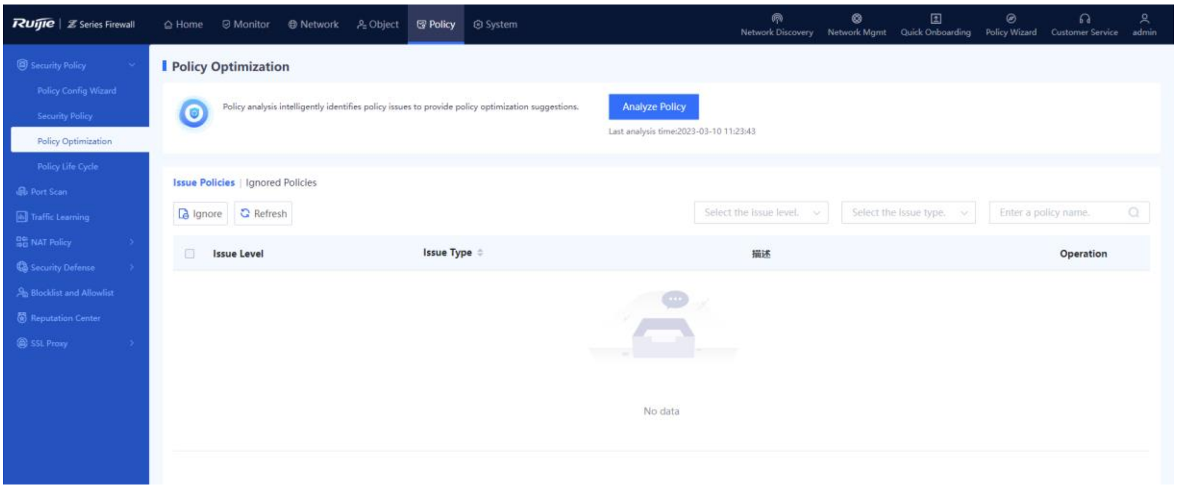
7.6.5 Optimizing Policy

Application Scenario

Affected by factors such as service accumulation and change of O&M personnel, the configuration complexity of security policies becomes increasingly high during the routine security policy O&M process. The policy optimization function of Z-S series firewalls can intelligently compare and analyze the filter conditions of the current security policies to identify redundant policies, which is convenient for O&M personnel to streamline and optimize policies, thus reducing O&M costs.

Procedure

(1) Choose **Policy** > **Security Policy** > **Policy Optimization**.

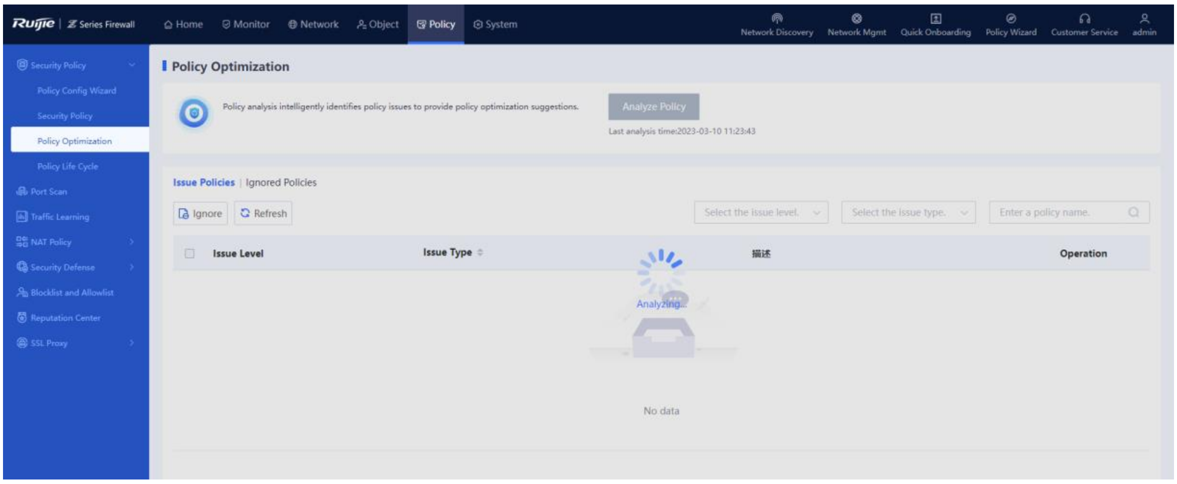


Policy Optimization

Policy analysis intelligently identifies policy issues to provide policy optimization suggestions.

Last analysis time:2023-03-10 11:23:43

(2) Click **Analyze Policy** to analyze the security policy.

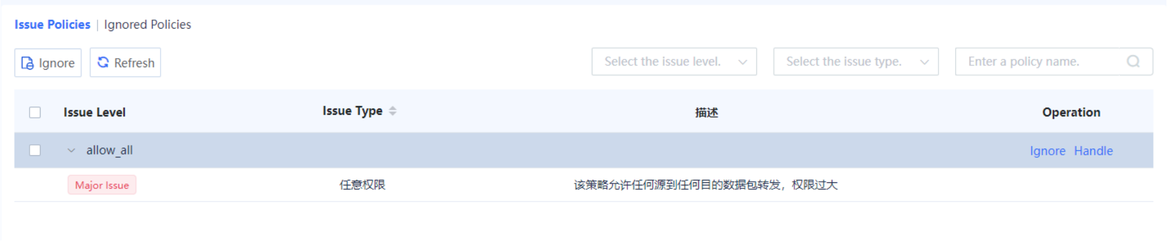


Policy Optimization

Policy analysis intelligently identifies policy issues to provide policy optimization suggestions.

Last analysis time:2023-03-10 11:23:43

After analysis is completed, the system displays the issue policy list.

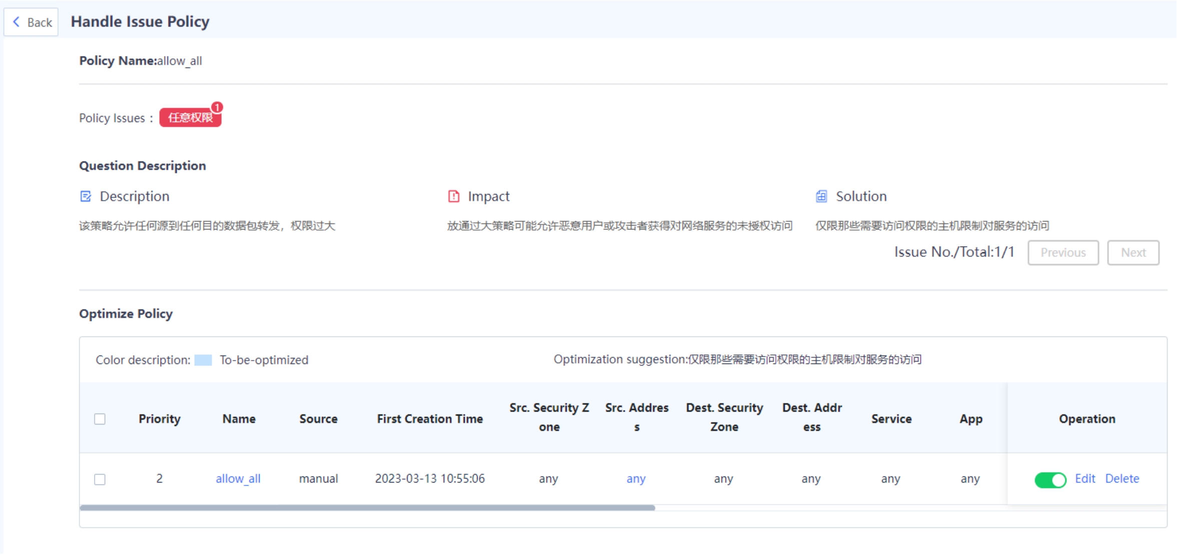


Issue Level	Issue Type	描述	Operation
allow_all			Ignore Handle
Major Issue	任意权限	该策略允许任何源到任何目的数据包转发，权限过大	

Note

After analyzing security policies using the policy optimization function, the system classifies the issues into three levels: major, minor, and to-be-optimized.

(3) Click **Handle** in the **Operation** column of the corresponding policy to view details about the policy.



< Back **Handle Issue Policy**

Policy Name:allow_all

Policy Issues： 任意权限 1

Question Description

Description
该策略允许任何源到任何目的数据包转发，权限过大

Impact
放通过大策略可能允许恶意用户或攻击者获得对网络服务的未授权访问

Solution
仅限那些需要访问权限的主机限制对服务的访问

Issue No./Total:1/1 Previous Next

Optimize Policy

Color description: ▨ To-be-optimized

Optimization suggestion:仅限那些需要访问权限的主机限制对服务的访问

□	Priority	Name	Source	First Creation Time	Src. Security Zone	Src. Address	Dest. Security Zone	Dest. Address	Service	App	Operation
□	2	allow_all	manual	2023-03-13 10:55:06	any	any	any	any	any	any	Edit Delete

The details about a specific issue and possible impact are displayed, and the solution is provided to O&M personnel as a reference.

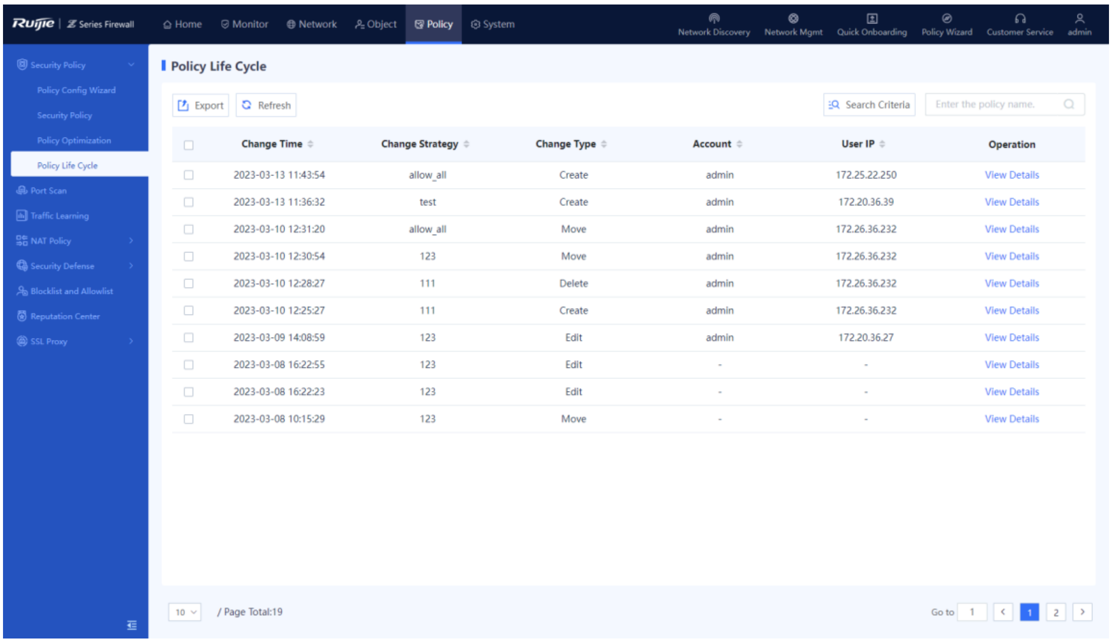
7.6.6 Policy Lifecycle Management

Application Scenario

Affected by factors such as service accumulation and change of O&M personnel, the security policies need to be repeatedly modified to meet new service requirements or solve existing problems. When encountering problems, O&M personnel often need to trace and analyze the changed policies and detailed change items. The policy lifecycle management function provided by Z-S series firewalls records the entire process of creating, modifying, and deleting each security policy, and records the operators and IP addresses of the operations in detail.

Procedure

(1) Choose **Policy** > **Security Policy** > **Policy Life Cycle**.

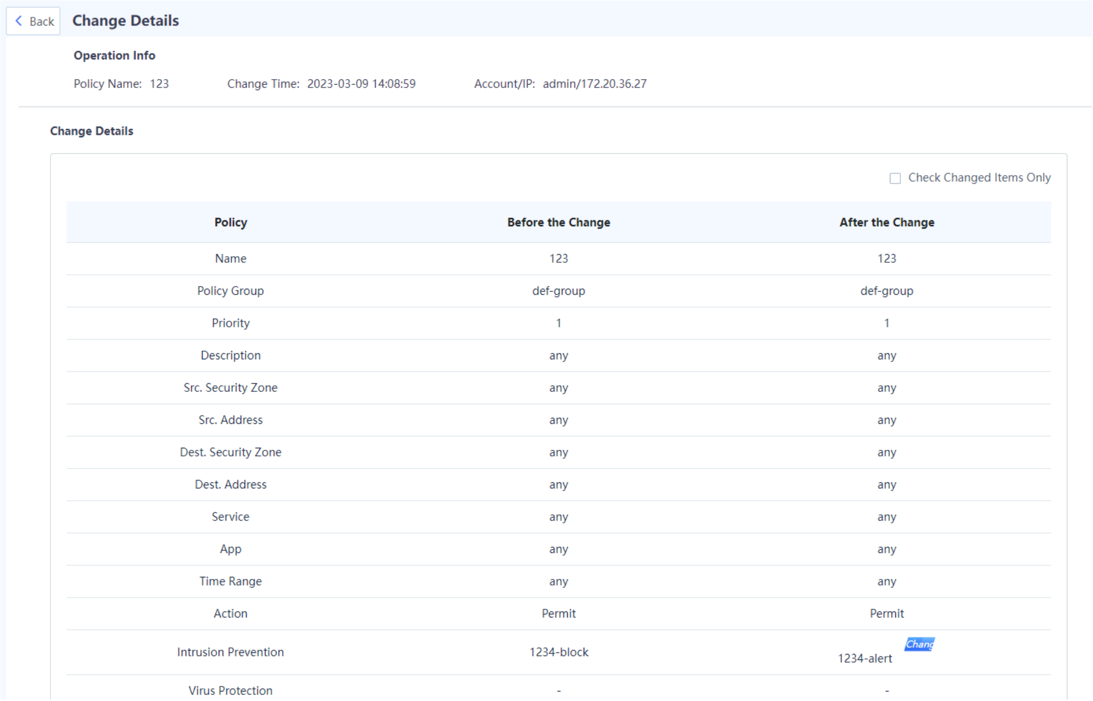


Policy Life Cycle

□	Change Time	Change Strategy	Change Type	Account	User IP	Operation
□	2023-03-13 11:43:54	allow_all	Create	admin	172.25.22.250	View Details
□	2023-03-13 11:36:32	test	Create	admin	172.20.36.39	View Details
□	2023-03-10 12:31:20	allow_all	Move	admin	172.26.36.232	View Details
□	2023-03-10 12:30:54	123	Move	admin	172.26.36.232	View Details
□	2023-03-10 12:28:27	111	Delete	admin	172.26.36.232	View Details
□	2023-03-10 12:25:27	111	Create	admin	172.26.36.232	View Details
□	2023-03-09 14:08:59	123	Edit	admin	172.20.36.27	View Details
□	2023-03-08 16:22:55	123	Edit	-	-	View Details
□	2023-03-08 16:22:23	123	Edit	-	-	View Details
□	2023-03-08 10:15:29	123	Move	-	-	View Details

/ Page Total:19

(2) Select the security policy you want to view. Click **View Details** in the **Operation** column.



Change Details

Operation Info

Policy Name: 123 Change Time: 2023-03-09 14:08:59 Account/IP: admin/172.20.36.27

Change Details

□ Check Changed Items Only

Policy	Before the Change	After the Change
Name	123	123
Policy Group	def-group	def-group
Priority	1	1
Description	any	any
Src. Security Zone	any	any
Src. Address	any	any
Dest. Security Zone	any	any
Dest. Address	any	any
Service	any	any
App	any	any
Time Range	any	any
Action	Permit	Permit
Intrusion Prevention	1234-block	1234-alert Chang
Virus Protection	-	-

On the **Details** page, you can view the details of a single change, solving the pain point of tracing security policy changes during O&M and reducing O&M costs.

7.6.7 Simulation Run

Application Scenario

Affected by factors such as service accumulation and change of O&M personnel, the configuration complexity of security policies becomes increasingly high during the routine security policy O&M process. In the middle and late stages of O&M, if the security policy is modified improperly, the risk of service interruption will increase with the complexity of the policy.

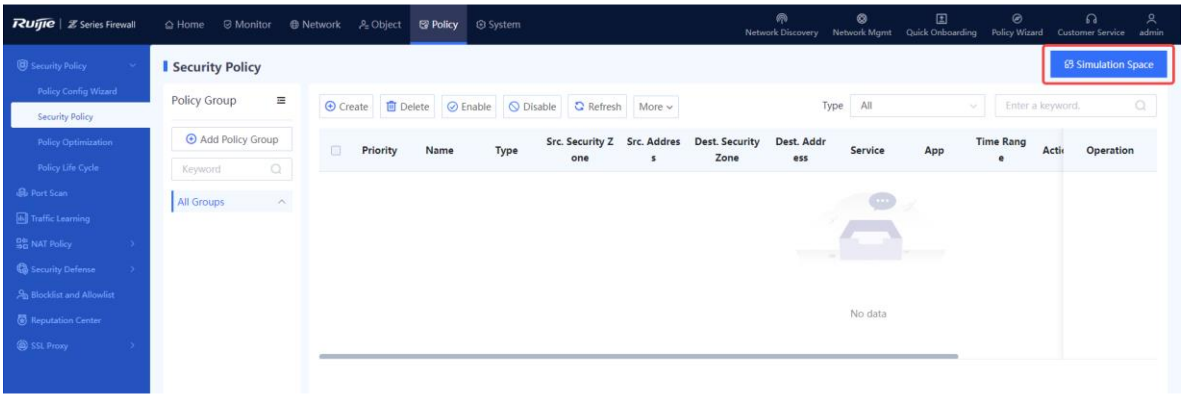
Z-S series firewalls provide a virtual space of policy simulation run for O&M personnel to verify and test policy modifications. This space does not affect the services in the real network environment. That is, the security policies in the simulation space will not permit or block real service traffic.

This function solves the problems such as service interruption caused by improper configuration in O&M, and provides O&M personnel with a test and verification environment, thus reducing O&M difficulty and risk, and lowering O&M costs.

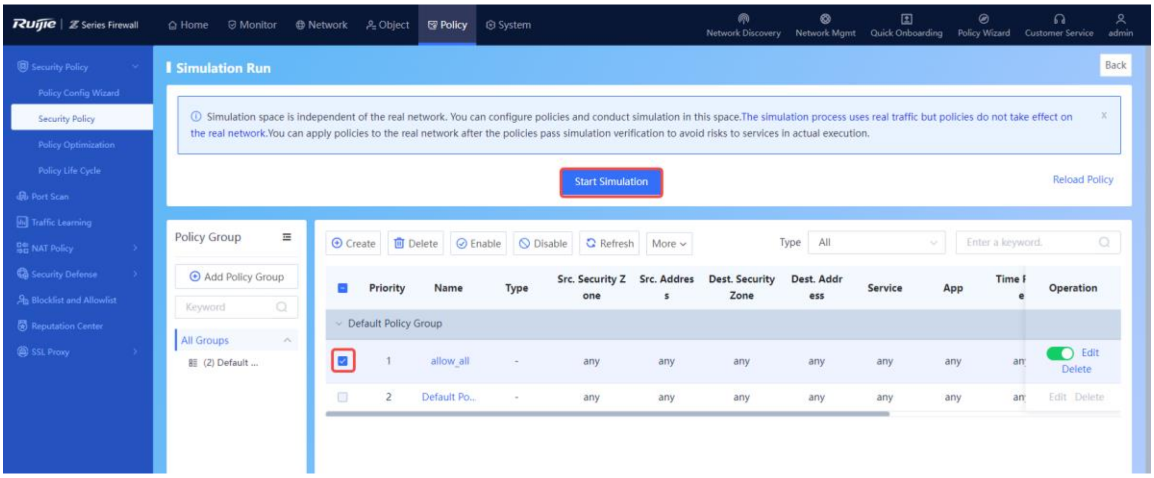
Procedure

(1) Choose **Policy** > **Security Policy** > **Security Policy**.

(2) Click **Simulation Space** in the upper right corner of the operation area.



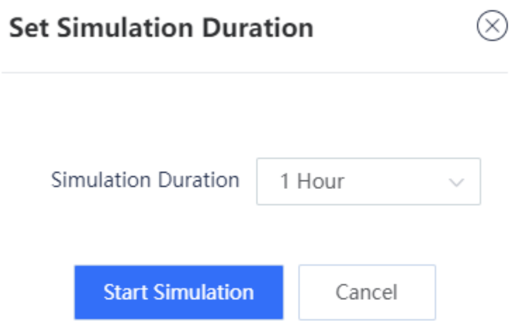
(3) Select the policy for which simulation run will be performed, and click **Start Simulation**.



Simulation space is independent of the real network. You can configure policies and conduct simulation in this space.The simulation process uses real traffic but policies do not take effect on the real network.You can apply policies to the real network after the policies pass simulation verification to avoid risks to services in actual execution.

☑	Priority	Name	Type	Src. Security Zone	Src. Address	Dest. Security Zone	Dest. Address	Service	App	Time R	Operation
Default Policy Group											
☑	1	allow_all	-	any	any	any	any	any	any	an	Edit Delete
□	2	Default Po...	-	any	any	any	any	any	any	an	Edit Delete

(4) In the **Set Simulation Duration** dialog box, set the duration of simulation run.

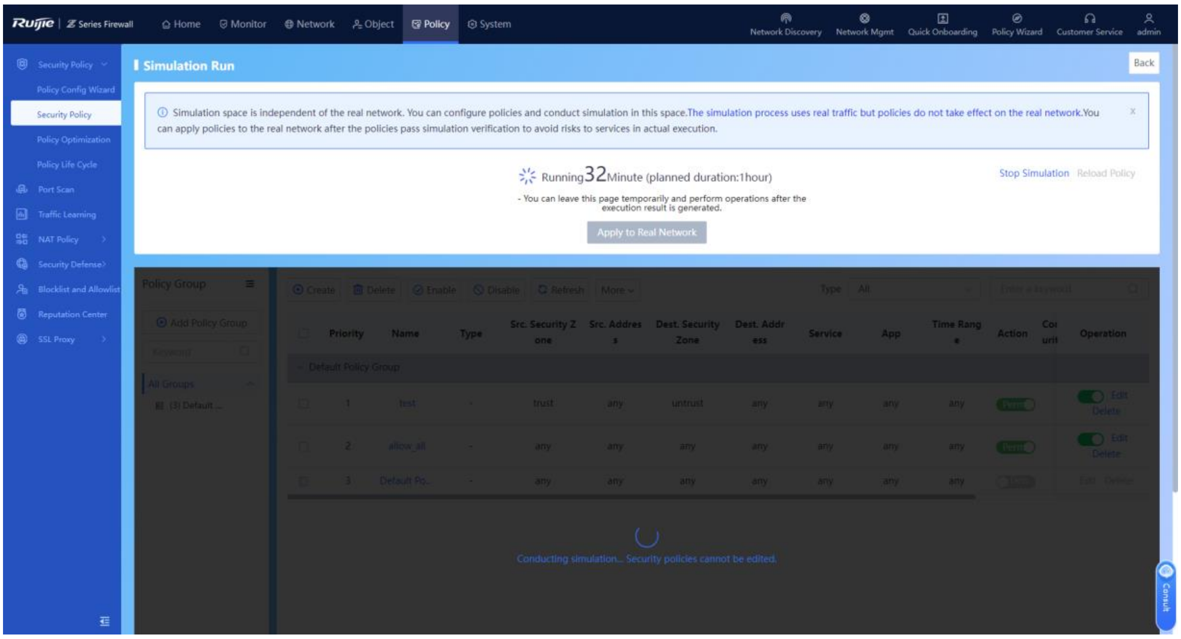


Set Simulation Duration

Simulation Duration: 1 Hour

(5) Click **Start Simulation**.

The system automatically performs simulation run for the selected policies.



Simulation Run

Simulation space is independent of the real network. You can configure policies and conduct simulation in this space.The simulation process uses real traffic but policies do not take effect on the real network.You can apply policies to the real network after the policies pass simulation verification to avoid risks to services in actual execution.

Running32Minute (planned duration:1hour)

- You can leave this page temporarily and perform operations after the execution result is generated.

	Priority	Name	Type	Src. Security Zone	Src. Address	Dest. Security Zone	Dest. Address	Service	App	Time Range	Action	Con unit	Operation
Default Policy Group													
□	1	test	-	trust	any	untrust	any	any	any	any	Permit		Edit Delete
□	2	allow_all	-	any	any	any	any	any	any	any	Permit		Edit Delete
□	3	Default Po...	-	any	any	any	any	any	any	any			Edit Delete

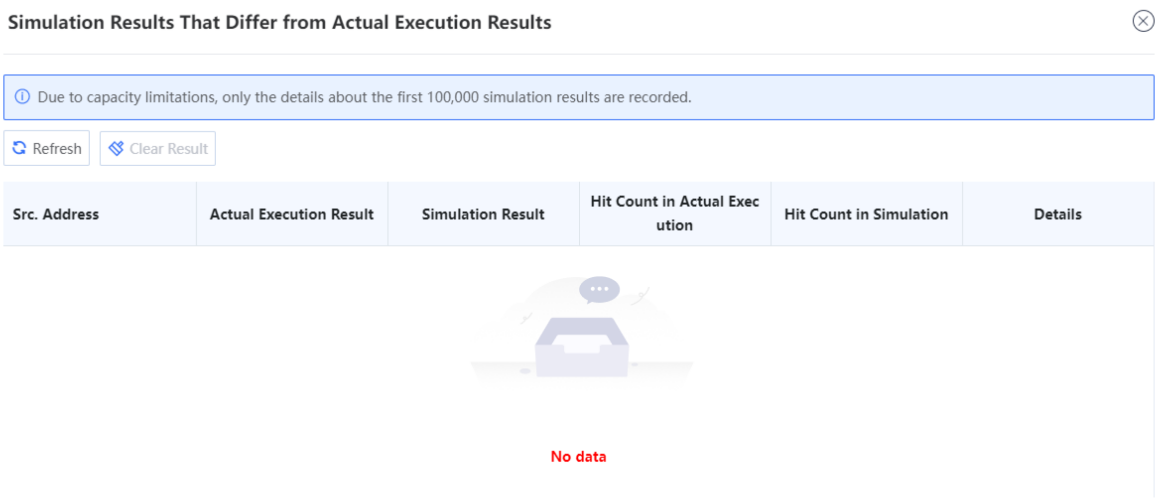
Conducting simulation... Security policies cannot be edited.

(6) When simulation run is finished, click **View Simulation Result**.

Simulation run results are displayed based on the source IP address:

- The number of times traffic is permitted in the real policy but blocked in the simulated policy.
- The number of times traffic is permitted in the simulated policy but blocked in the real policy.

(7) Analyze whether the simulation results differ from actual execution results.



Simulation Results That Differ from Actual Execution Results

ⓘ Due to capacity limitations, only the details about the first 100,000 simulation results are recorded.

Src. Address	Actual Execution Result	Simulation Result	Hit Count in Actual Execution	Hit Count in Simulation	Details

No data

(8) If the simulation results are expected, click **Apply to Real Network** to make the policy effective.

Follow-up Procedure

- O&M personnel can copy a currently effective security policy to the simulation space and modify the policy as required. For example, the O&M personnel can add, modify, and delete the policies according to service requirements.
- When the O&M personnel verify that there are no problems with the security policies in the simulation space, they can export the security policies to make them effective and replace the current security policies.

7.6.8 Importing Security Policies in a Batch

Application Scenario

Z-S series firewalls support fast generation of security policies based on imported configuration files.

The configuration files can be obtained in the following two ways:

- The device provides the configuration file template. You can download the configuration file template, and modify it according to actual service situations.
- To import the configurations from another device to a Z-S series firewall, you can configure the policy migration tool to obtain the corresponding configuration file.

Caution

The security policies containing IPv6 addresses cannot be imported in a batch.

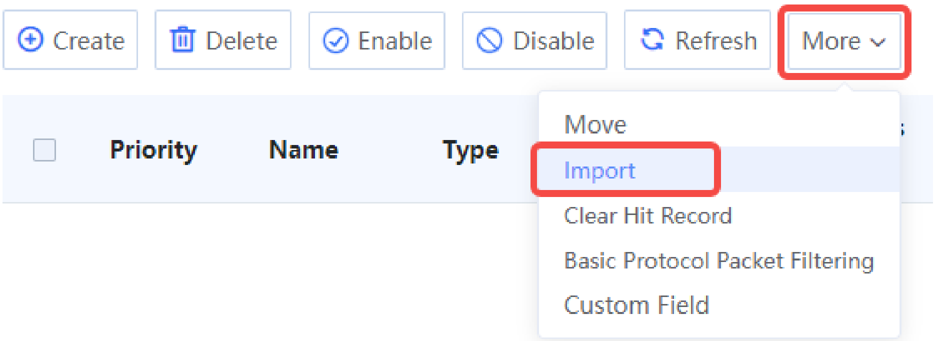
Note

For the usage of the policy migration tool, contact technical support engineers.

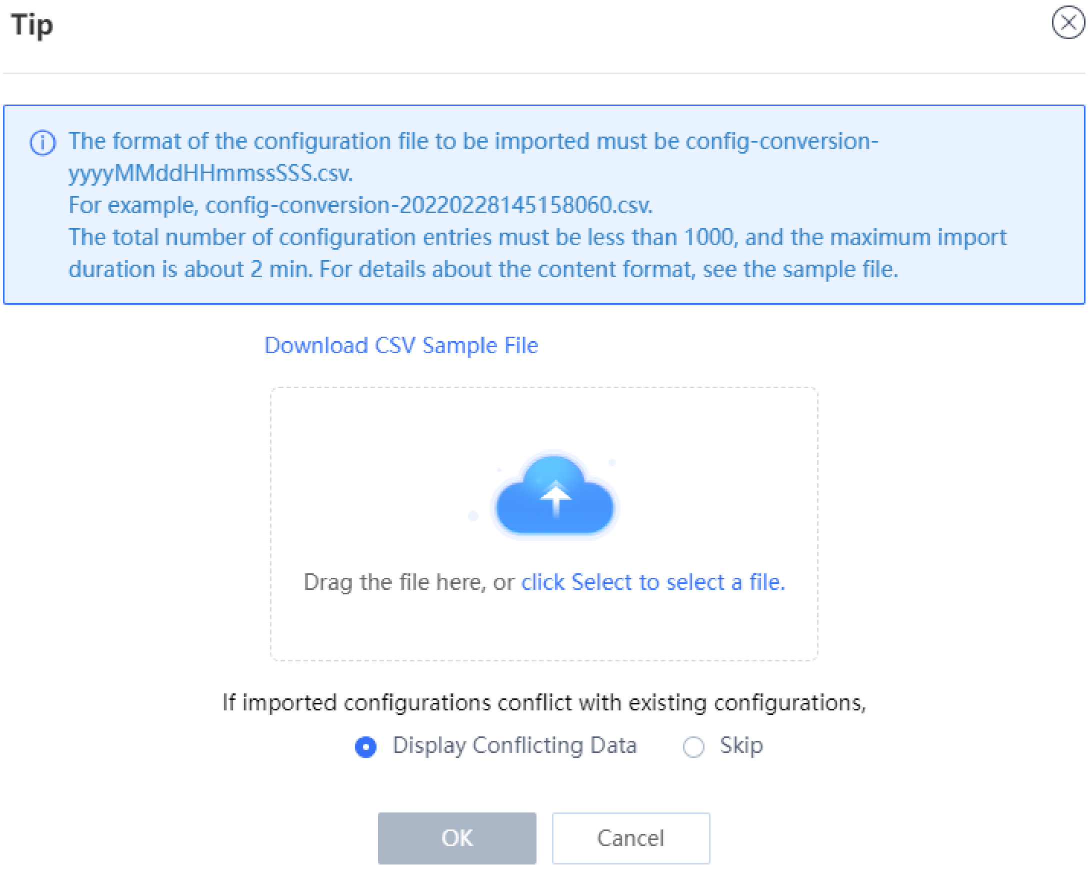
Procedure

(1) Choose **Policy** > **Security Policy**.

(2) Click **More** in the operation area and select **Import** from the drop-down list.



(3) The system displays a tip.



Tip

The format of the configuration file to be imported must be config-conversion-yyyyMMddHHmmssSSS.csv.
For example, config-conversion-20220228145158060.csv.
The total number of configuration entries must be less than 1000, and the maximum import duration is about 2 min. For details about the content format, see the sample file.

Download CSV Sample File

Drag the file here, or click Select to select a file.

If imported configurations conflict with existing configurations,

● Display Conflicting Data ○ Skip

OK Cancel

(4) Click **Download CSV Sample File** to download the configuration file template and fill in the configuration information.

Note

After modifying the configuration file, check whether the naming of the configuration file meets the system requirements. The naming format of the configuration file is: config-conversion-{yyyyMMddHHmmssSSS}.csv.

(5) Drag the configuration file to the upload area or click **Select** to upload the configuration file to the device.

(6) Configure the method used when data conflicts.

When the imported data conflicts with the existing data, the following processing methods can be used:

- **conflict data is displayed**: The system displays the conflicting configuration items and the conflict reason for you to modify the configuration file.
- **Skip**: The system ignores conflicting configuration items and no processing is required.

(7) Click **OK**.

The system automatically writes the configuration file information to the device for the configuration to take effect.

7.6.9 Enabling Basic Protocol Packet Control

Application Scenario

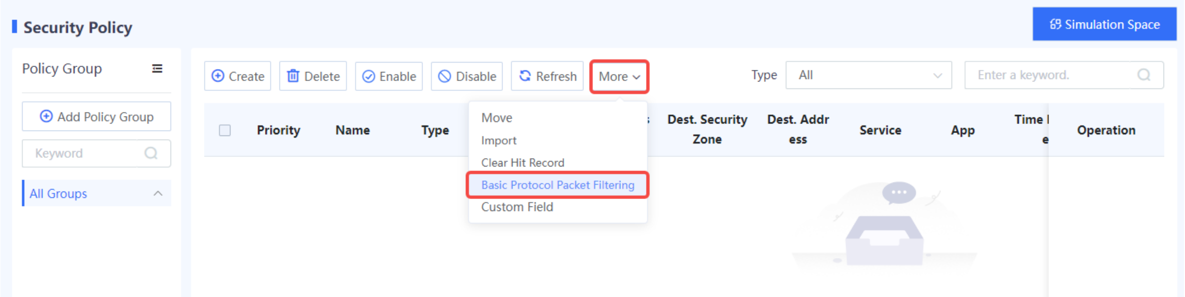
You can enable or disable the basic protocol packet control function of security policies.

By default, the firewall does not perform security control on the network basic protocol packets (such as DHCP packets and auto-discovery protocol packets). It directly forwards these packets if no additional configurations are performed so that the device can quickly access the network. If you want to control forwarding behavior of basic protocol packets by configuring a security policy, you can enable the basic protocol packet control function to control these packets.

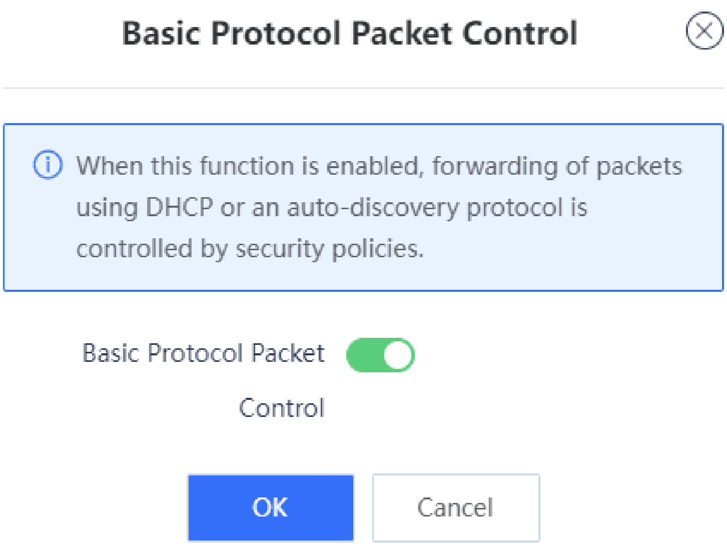
Procedure

(1) Choose **Policy** > **Security Policy** > **Security Policy**.

(2) Click **More** and select **Basic Protocol Packet Filtering** from the drop-down list.



(3) On the **Basic Protocol Packet Control** page, enable **Basic Protocol Packet Control**.



When this function is enabled, forwarding of packets using DHCP or an auto-discovery protocol is controlled by security policies.

(4) Click **OK**.

7.7 DHCP Management

7.7.1 Overview

Dynamic Host Configuration Protocol (DHCP) is a network management protocol applied on the LAN. It works using UDP and is widely used to dynamically allocate network resources that can be reused, such as IP addresses. For small networks, DHCP makes subsequent network device adding easy and fast.

DHCP provides the following benefits:

- Reduced client configuration and maintenance costs

  DHCP is easy to configure and deploy. For non-technical users, DHCP can minimize configuration-related operations on the client and reduce remote deployment and maintenance costs.

- Centralized management

  The DHCP server can be used to manage the configuration information about multiple network segments. When the configurations of a network segment change, the administrator only needs to update related configurations on the DHCP server.

  The Z-S series firewall can be configured as a DHCP server to allocate IP addresses to intranet users.

7.7.2 Configuring a DHCP Server

1. Application Scenario

The system enables the DHCP server function by default. The firewall can be configured as a DHCP server to allocate IP addresses to intranet users.

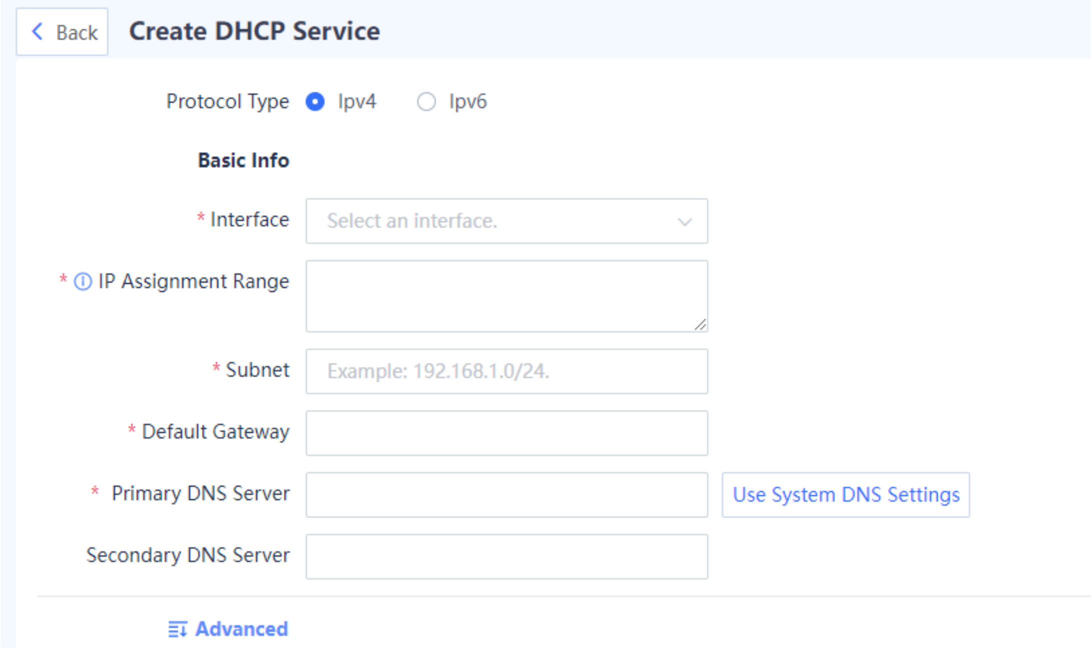
2. Configuring a DHCPv4 Server

(1) Choose **Network** > **DHCP** > **DHCP Server**.

(2) Configure the DHCP server information.

a Click **Create**.

The **Create DHCP Service** page is displayed. Set **IPv4**.



Create DHCP Service

Protocol Type ● Ipv4 ○ Ipv6

Basic Info

* Interface: Select an interface.

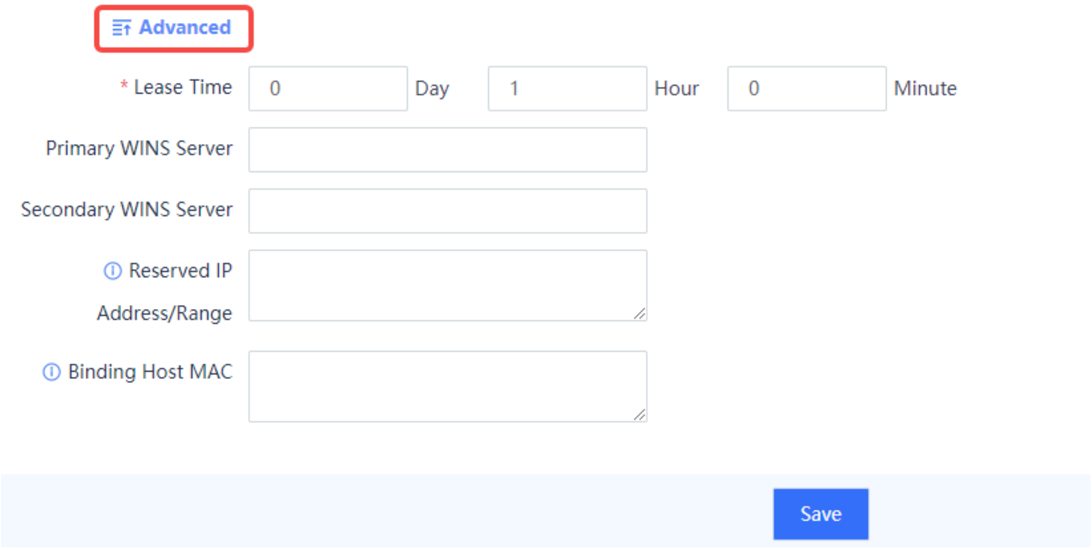
* IP Assignment Range:

* Subnet: Example: 192.168.1.0/24.

* Default Gateway:

* Primary DNS Server:

Secondary DNS Server:



* Lease Time 0 Day 1 Hour 0 Minute

Primary WINS Server

Secondary WINS Server

Reserved IP Address/Range

Binding Host MAC

b Set parameters of the DHCP server.

Item	Description	Remarks
Interface	Interface where the DHCPv4 service is configured. After the DHCPv4 service is enabled, the interface can allocate IPv4 addresses.	[Example] Ge0/1
IP Assignment Range	Range of IP addresses allocated by the DHCP server.	● Enter an IP address range per line. ● Connect the start IP address and end IP address with a hyphen (-). [Example] 192.168.1.1-192.168.1.10
Subnet	Subnet where the IP addresses are located.	Enter the subnet address/ mask bits. [Example] 192.168.1.0/24
Default Gateway	Default gateway that provides network access	[Example] 255.255.255.0

Item	Description	Remarks
	service to the terminals, which obtain IP addresses.	
Primary DNS Server	Preferred DNS server used by the DHCP service.	Click **Use System DNS Settings**. Then the system automatically fills in the system DNS server. You can also configure a public DNS server. [Example] 192.168.10.1
Secondary DNS Server	Alternative DNS server used by the DHCP service.	[Example] 192.168.30.1
Advanced		
Lease Time	Address lease period. In general, terminal devices automatically renews the lease in connected state to keep the IP address unchanged. If the lease is not renewed due to disconnection or network instability, the IP addresses are reclaimed after the lease expires. When the terminal devices recover connectivity, they will request the addresses again.	● The lease period ranges from 3 minutes to 365 days. ● The default lease period is 1 hour. [Example] 1 hour
Reserved IP Address/Range	Reserved IP addresses in the **IP Assignment Range**.	[Example] 192.168.1.2

Item	Description	Remarks
Binding Host MAC	Static bindings between the pre-assigned IP addresses specified by **IP Assignment Range** and the MAC addresses of the clients. When receiving a request for an IP address from a client with a matching MAC address, the DHCP server allocates the pre-assigned IP address that is bound to the MAC address only to this client.	The value is in the format of IP address/MAC address, where the IP address should be a pre-assigned address in the **IP Assignment Range**. Enter one binding entry per line. [Example] 192.168.10.1/d8:9e:f3:3f:d5:64

c Click **Save**.

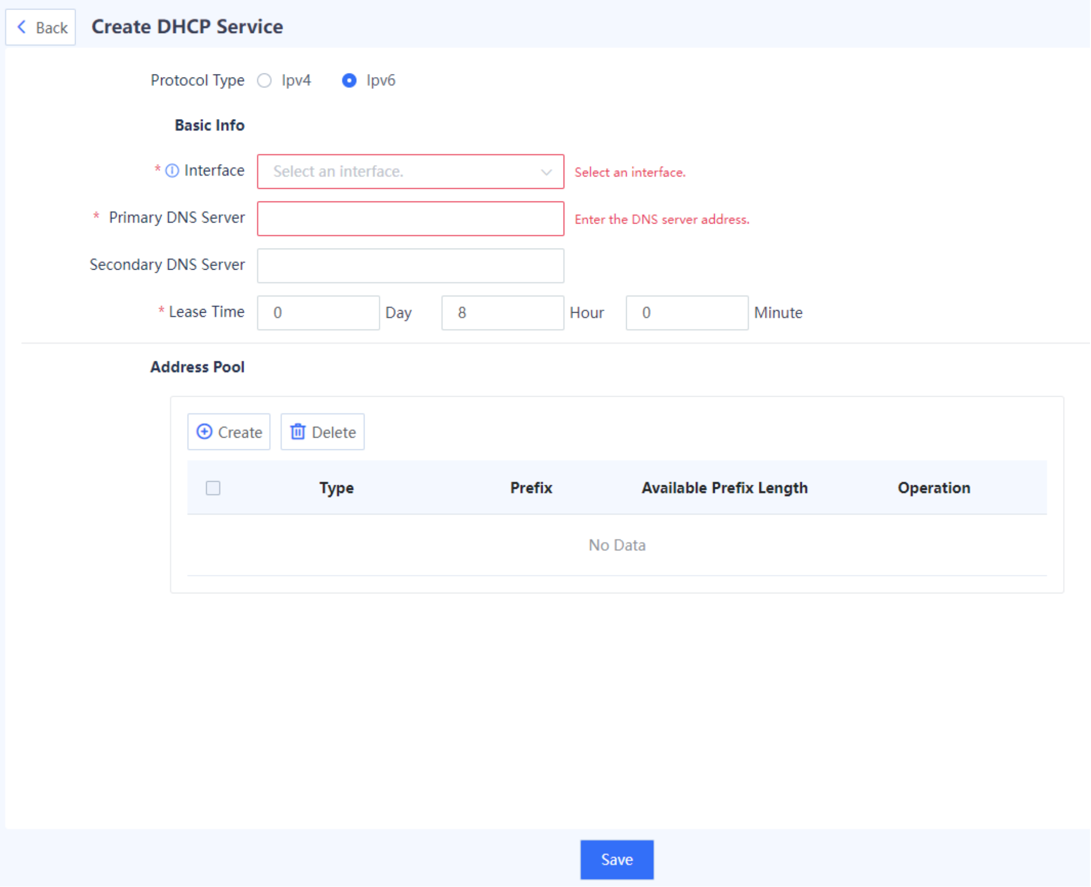
3. Configuring a DHCPv6 Server

(3) Choose **Network** > **DHCP** > **DHCP Server**.

(4) Configure the DHCP server information.

a Click **Create**.

The **Create DHCP Service** page is displayed. Set **IPv6**.



< Back **Create DHCP Service**

Protocol Type ○ Ipv4 ● Ipv6

Basic Info

* Interface: Select an interface. — Select an interface.

* Primary DNS Server: — Enter the DNS server address.

Secondary DNS Server:

* Lease Time: 0 Day 8 Hour 0 Minute

Address Pool

□	Type	Prefix	Available Prefix Length	Operation

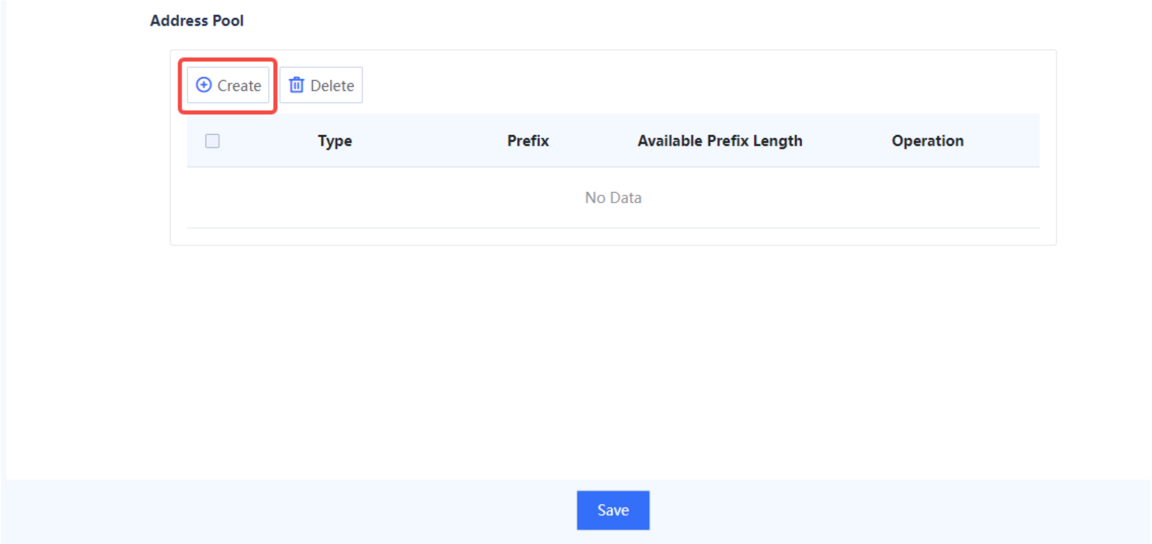
No Data

b Set parameters of the DHCP server.

Item	Description	Remarks
Interface	Interface where the DHCPv6 server is configured. After the DHCPv6 function is enabled, the interface can allocate IPv6 addresses.	[Example] Ge0/4
Primary DNS Server	Preferred DNS server used by the DHCP service.	[Example] 2001::1
Secondary DNS Server	Alternative DNS server used by the DHCP service.	[Example] 2001::2
Lease Time	Address lease period. In general, terminal devices automatically renews the lease in connected state to keep the IP address unchanged. If the lease is not renewed due to disconnection or network	[Example] 1 hour

Item	Description	Remarks
	instability, the IP addresses are reclaimed after the lease expires. When the terminal devices recover connectivity, they will request the addresses again.	

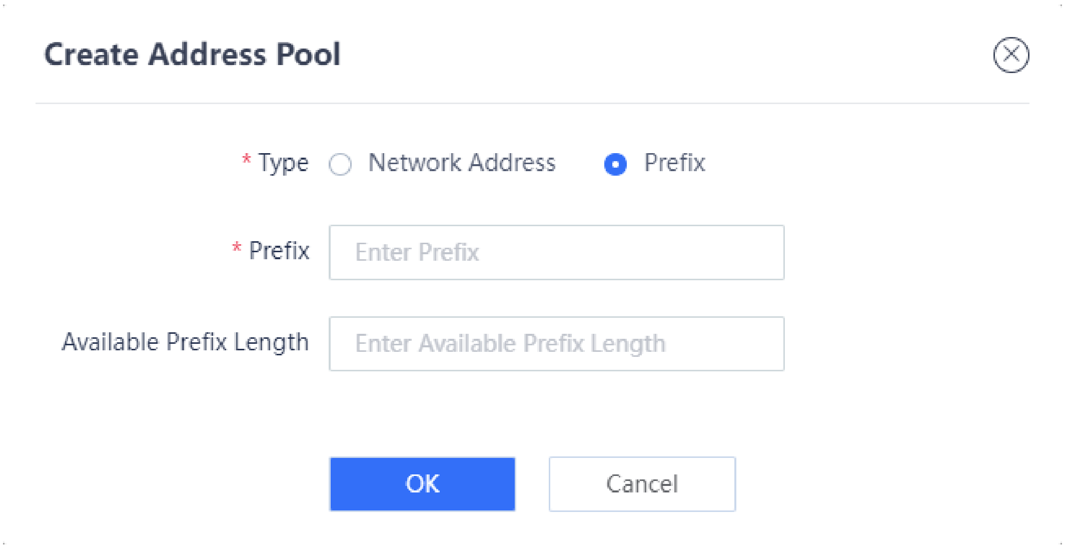
c In the **Address Pool** area, click **Create**.



Address Pool

□	Type	Prefix	Available Prefix Length	Operation
No Data				

d Select the address type and enter an available address prefix and length, and click **OK**.



Create Address Pool

* Type ○ Network Address ● Prefix

* Prefix Enter Prefix

Available Prefix Length Enter Available Prefix Length

e Click **Save**.

4. Follow-up Procedure

If only one row is left in the DHCP service list, and you want to delete the address pool, you need to disable the DHCP server first.

7.7.3 Address Management List

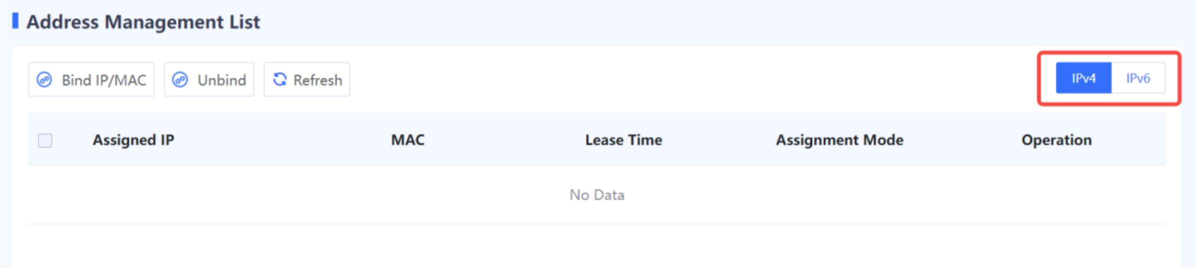
Application Scenario

You can view the IP addresses allocated by the DHCP server on the **Address Management List** page.

Procedure

(5) Choose **Network** > **DHCP** > **Address Management List**.

(6) Click **IPv4** or **IPv6** in the upper-right corner to view assigned IPv4 or IPv6 addresses.



Address Management List

□	Assigned IP	MAC	Lease Time	Assignment Mode	Operation
			No Data		

(7) Process the IP addresses.

- Select addresses and click **Bind IP/MAC** or **Bind** in the **Operation** column to fixedly allocate IP addresses to the hosts with the corresponding MAC addresses.
- Select addresses and click **Unbind** to cancel the binding relationship between IP addresses and MAC addresses.

7.8 Blocklist and Allowlist

7.8.1 Overview

Z-S series firewalls support blocklist and allowlist to block or forward packets based on IP addresses.

- Allowlist

  After the specified IP address is added to the allowlist, the firewall directly forwards the packets sent to or from the address, without performing security check, thus implementing high-speed packet forwarding.

For example, if you do not want to enforce security policies or anti-DoS/DDoS policies on some IP addresses (such as the administrator's address) on the network, you can add the IP addresses to the allowlist.

- Blocklist

  After an IP address is added to the blocklist, the packets sent to or from the address will be discarded by the device.

  For example, if you want to prevent traffic of some IP addresses (such as attackers' addresses) on the network from passing the device, add the IP addresses to the blocklist.

⚠ **Caution**

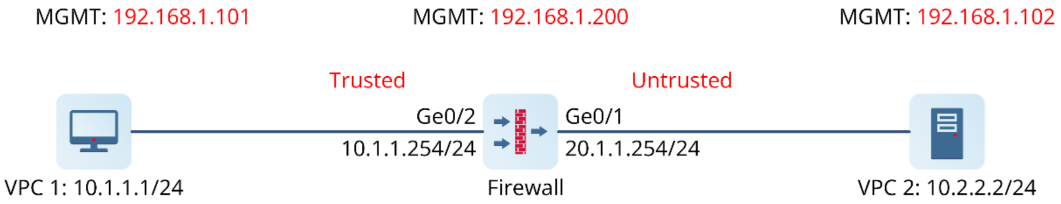
The IP addresses in blocklist cannot be used to log in to the firewall.

- Temporary blocklist

  The temporary blocklist has the same function as the blocklist, but the temporary blocklist is valid for only a period of time. When the validity period expires, the blocklist becomes invalid and is automatically deleted. When traffic hits a brute-force IPS policy, a temporary blocklist is automatically generated. The block period is the block period of the rules of brute-force IPS policy. You can also manually configure a temporary blocklist.

7.8.2 Precautions

RG-WALL 1600-Z-S series firewalls configure the blocklist and allowlist for source and destination separately. If a blocklist or allowlist needs to take effect on both the incoming and outgoing packets of an IP address, you need to add the IP address to the blocklist or allowlist of both the source and destination.



As shown in the above figure, the source address range in the security policy includes an allowlist and the security policy action is deny. If the source IP address 10.1.1.1 is in the allowlist and needs to access 10.2.2.2, consider the following two situations:

- When NAT is not configured, add destination IP address 10.2.2.2 to the blocklist and allowlist of both source and destination.

- When NAT is configured, the IP addresses will be translated. If you only add the original IP address to blocklist or allowlist, the bidirectional traffic of the IP address cannot be blocked or allowed after address translation. You also need to add the translated public address to the blocklist or allowlist. For example, when source NAT is configured, to allow all traffic of IP address 10.2.2.2 (20.1.1.254 after NAT), you need to add 10.2.2.2 to the source allowlist to allow incoming packets and add 20.1.1.254 to the destination allowlist to allow outgoing packets. (Note: This restriction will be eliminated in later versions.)

7.8.3 Creating an IPv4 Allowlist

Application Scenario

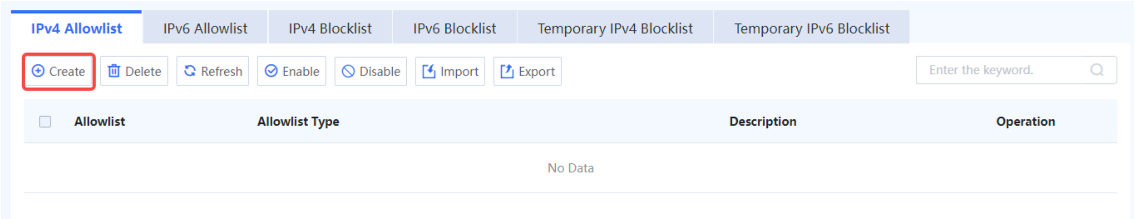
Configure an IPv4 allowlist on the web UI.

Procedure

(1) Access the **Add Allowlist** page.

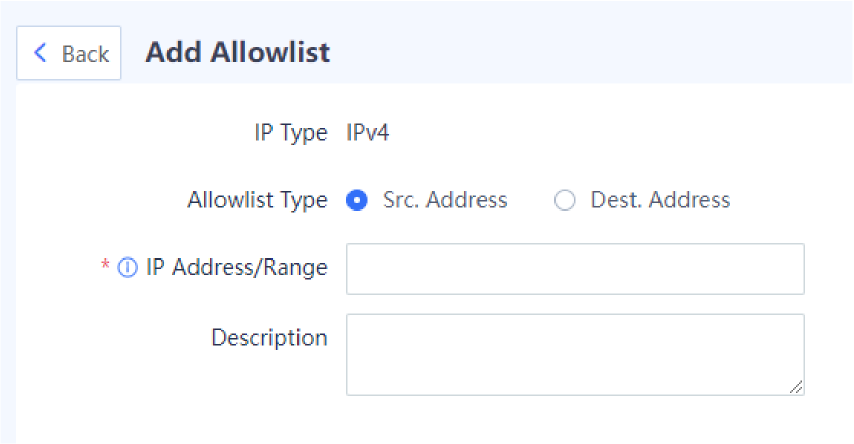
a Choose **Policy** > **Blocklist and Allowlist** > **IPv4 Allowlist**.

b Above the operation area, click **Create**.



□	Allowlist	Allowlist Type	Description	Operation
		No Data		

(2) Set parameters for the allowlist policy and click **Save**.



IP Type IPv4

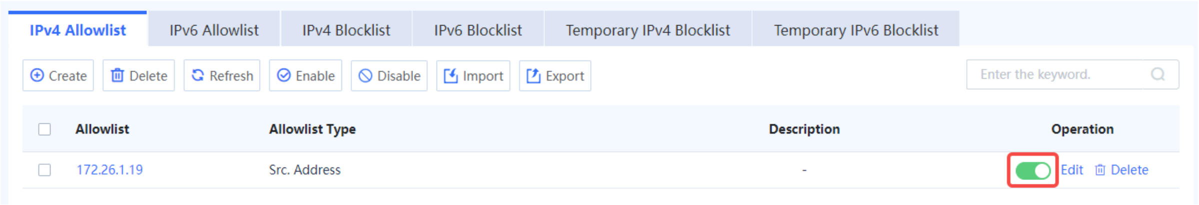
Allowlist Type ● Src. Address ○ Dest. Address

* ⓘ IP Address/Range

Description

Item	Description	Remarks
Allowlist Type	Type of the allowlist: ● **Src. Address**: Permit packets sent from this address. ● **Dest. Address**: Permit packets sent to this address.	[Example] Src. Address
IP Address/Range	Allowlist IP address/range.	The following two formats are supported: ● Single IP address: 192.168.1.1 ● IP address range: 192.168.1.1-192.168.1.10

(3) Toggle on the switch in the **Operation** column to enable the allowlist.



□	Allowlist	Allowlist Type	Description	Operation
□	172.26.1.19	Src. Address	-	Edit Delete

Follow-up Procedure

- To delete multiple allowlist policies in a batch, select the policies that you want to delete and click **Delete**.
- To enable multiple allowlist policies in a batch, select the policies that you want to enable and click **Enable**.
- To disable multiple allowlist policies in a batch, select the policies that you want to disable and click **Disable**.
- To export all allowlist configurations, click **Export**.
- Click **Import** to download the import template and upload the configured file, or directly select the CSV file to be uploaded. Then, click **Confirm** to start the import task.

- Enter the allowlist IP address, full or part of the allowlist description in the search box to search for the policies. Fuzzy search is supported.

7.8.4 Creating an IPv6 Allowlist

Application Scenario

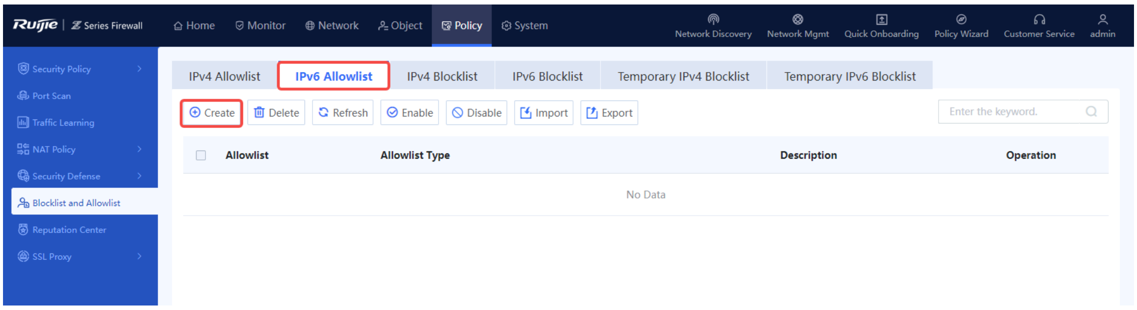
Configure an IPv6 allowlist on the web UI.

Procedure

(1) Access the **Add Allowlist** page.

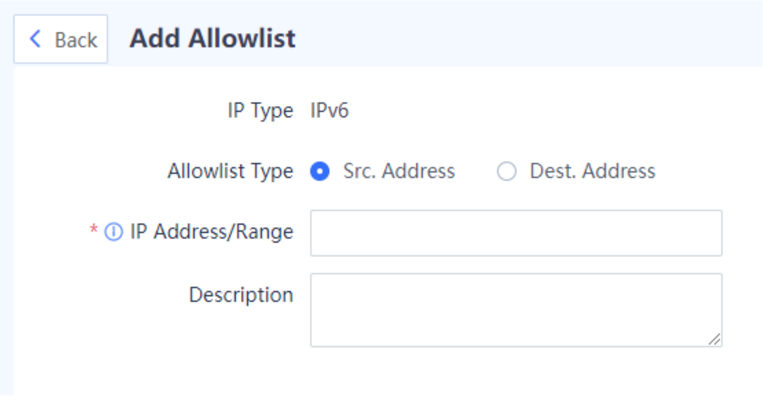
a Choose **Policy** > **Blocklist and Allowlist** > **IPv6 Allowlist**.

b Above the operation area, click **Create**.



□ Allowlist	Allowlist Type	Description	Operation
No Data			

(2) Set parameters for the allowlist policy and click **Save**.



IP Type IPv6

Allowlist Type ● Src. Address ○ Dest. Address

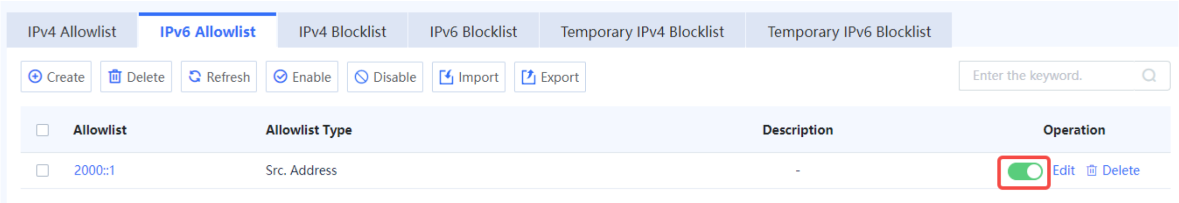
* ⓘ IP Address/Range

Description

Item	Description	Remarks
Allowlist Type	Type of the allowlist: ● **Src. Address**: Permit packets sent from this address.	[Example] Src. Address

Item	Description	Remarks
	● **Dest. Address**: Permit packets sent to this address.	
IP Address/Range	Allowlist IP address/range.	The following two formats are supported: ● Single IP address: 1234::100 ● IP address range: 1234::100-2345::100

(3) Toggle on the switch in the **Operation** column to enable the allowlist.



	Allowlist	Allowlist Type	Description	Operation
□	2000::1	Src. Address	-	Edit Delete

Follow-up Procedure

- To delete multiple allowlist policies in a batch, select the policies that you want to delete and click **Delete**.
- To enable multiple allowlist policies in a batch, select the policies that you want to enable and click **Enable**.
- To disable multiple allowlist policies in a batch, select the policies that you want to disable and click **Disable**.
- To export all allowlist configurations, click **Export**.
- Click **Import** to download the import template and upload the configured file, or directly select the CSV file to be uploaded. Then, click **Confirm** to start the import task.
- Enter the allowlist IP address, full or part of the allowlist description in the search box to search for the policies. Fuzzy search is supported.

7.8.5 Creating an IPv4 Blocklist

Application Scenario

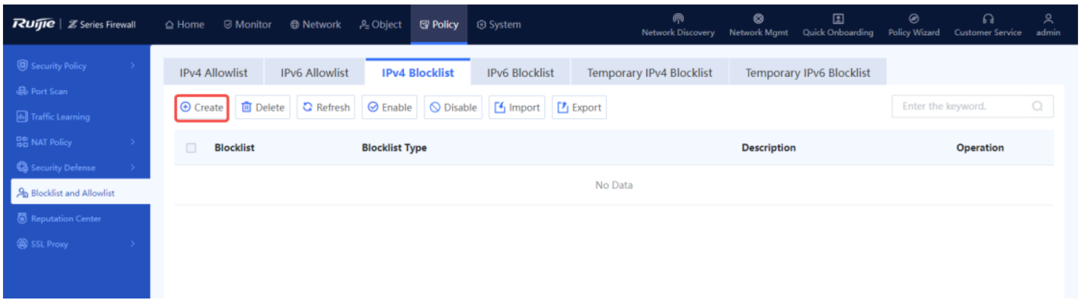
Configure an IPv4 blocklist on the web UI.

Procedure

(1) Access the **Add Blocklist** page.

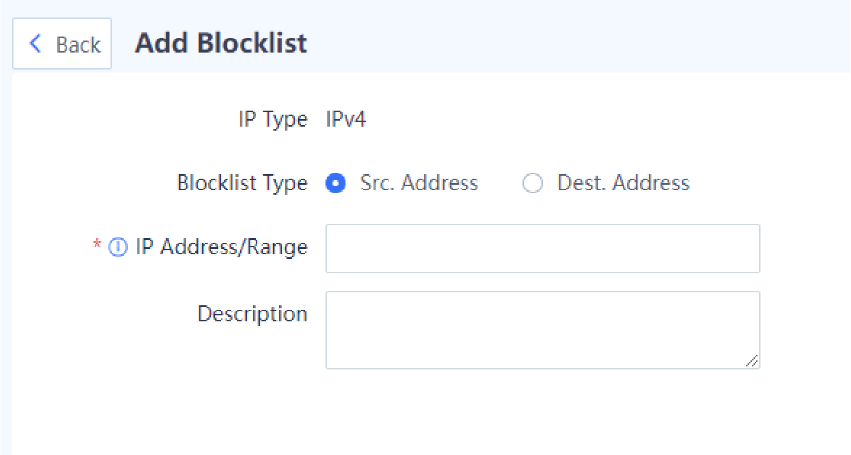
a Choose **Policy** > **Blocklist and Allowlist** > **IPv4 Blocklist**.

b In the operation area, click **Create**.



□	Blocklist	Blocklist Type	Description	Operation
No Data				

(2) Set parameters for the blocklist policy and click **Save**.



Add Blocklist

IP Type IPv4

Blocklist Type ● Src. Address ○ Dest. Address

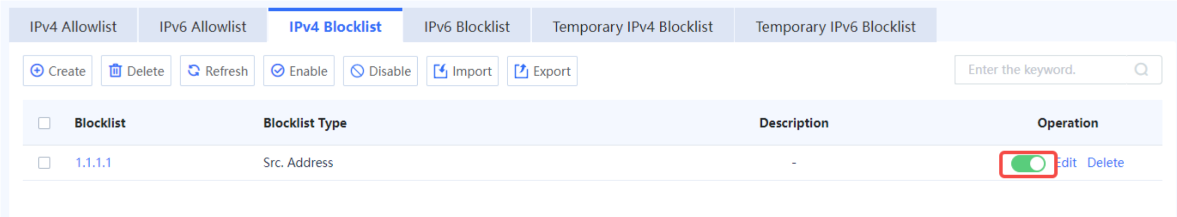
* ⓘ IP Address/Range

Description

Item	Description	Remarks
Blocklist Type	Type of the blocklist: ● **Src. Address**: Block packets sent from this address. ● **Dest. Address**: Block packets sent to this address.	[Example] Src. Address
IP Address/Range	Blocklist IP address/range.	The following two formats are supported:

Item	Description	Remarks
		● Single IP address: 192.168.1.1 ● IP address range: 192.168.1.1-192.168.1.10

(3) Toggle on the switch in the **Operation** column to enable the blocklist.



□	Blocklist	Blocklist Type	Description	Operation
□	1.1.1.1	Src. Address	-	Edit Delete

Follow-up Procedure

- To delete multiple blocklist policies in a batch, select the policies that you want to delete and click **Delete**.
- To enable multiple blocklist policies in a batch, select the policies that you want to enable and click **Enable**.
- To disable multiple blocklist policies in a batch, select the policies that you want to disable and click **Disable**.
- To export all blocklist configurations, click **Export**.
- Click **Import** to download the import template and upload the configured file, or directly select the CSV file to be uploaded. Then, click **Confirm** to start the import task.
- Enter the blocklist IP address, full or part of the blocklist description in the search box to search for the policies. Fuzzy search is supported.

7.8.6 Creating an IPv6 Blocklist

Application Scenario

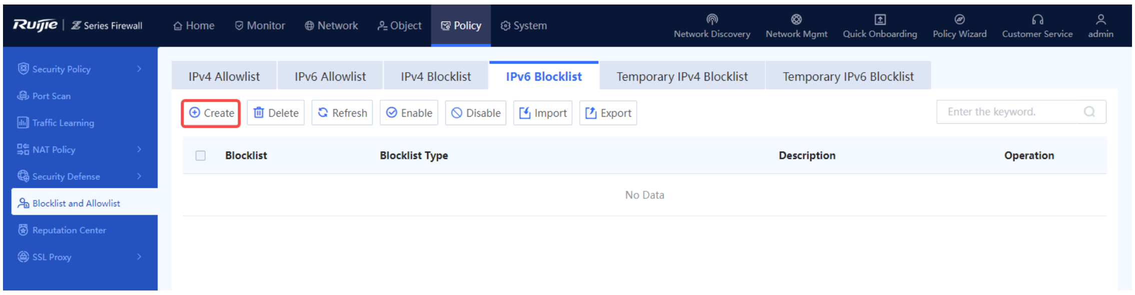
Configure an IPv6 blocklist on the web UI.

Procedure

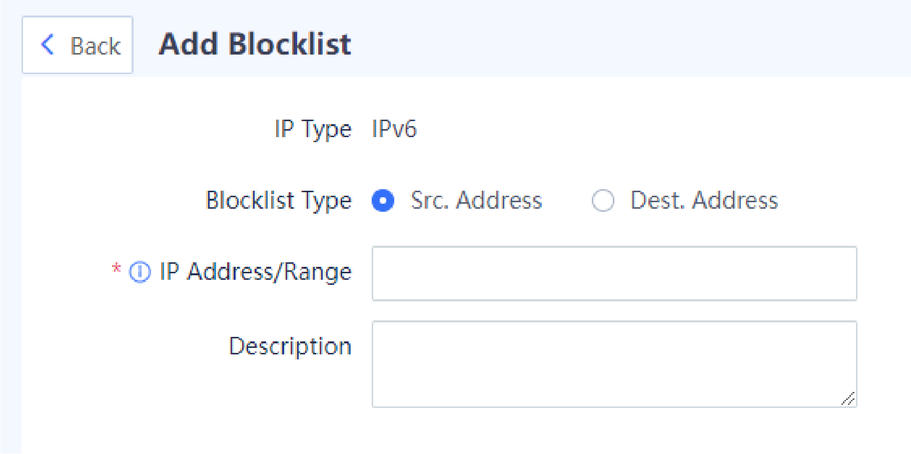
(1) Access the **Add Blocklist** page.

a Choose **Policy** > **Blocklist and Allowlist** > **IPv6 Blocklist**.

b Above the operation area, click **Create**.



(2) Set parameters for the blocklist policy and click **Save**.



IP Type IPv6

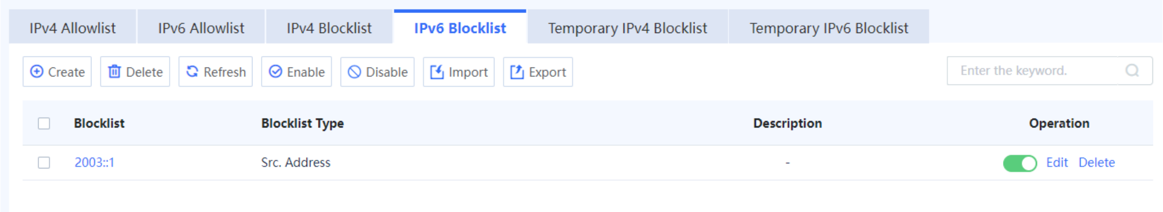
Blocklist Type ● Src. Address ○ Dest. Address

* IP Address/Range

Description

Item	Description	Remarks
Blocklist Type	Type of the blocklist: ● **Src. Address**: Block packets sent from this address. ● **Dest. Address**: Block packets sent to this address.	[Example] Src. Address
IP Address/Range	Blocklist IP address/range.	The following two formats are supported: ● Single IP address: 1234::100 ● IP address range: 1234::100-2345::100

(3) Toggle on the switch in the **Operation** column to enable the blocklist.



□	Blocklist	Blocklist Type	Description	Operation
□	2003::1	Src. Address	-	Edit Delete

Follow-up Procedure

- To delete multiple blocklist policies in a batch, select the policies that you want to delete and click **Delete**.
- To enable multiple blocklist policies in a batch, select the policies that you want to enable and click **Enable**.
- To disable multiple blocklist policies in a batch, select the policies that you want to disable and click **Disable**.
- To export all blocklist configurations, click **Export**.
- Click **Import** to download the import template and upload the configured file, or directly select the CSV file to be uploaded. Then, click **Confirm** to start the import task.
- Enter the blocklist IP address, full or part of the blocklist description in the search box to search for the policies. Fuzzy search is supported.

7.8.7 Creating a Temporary IPv4 Blocklist

Application Scenario

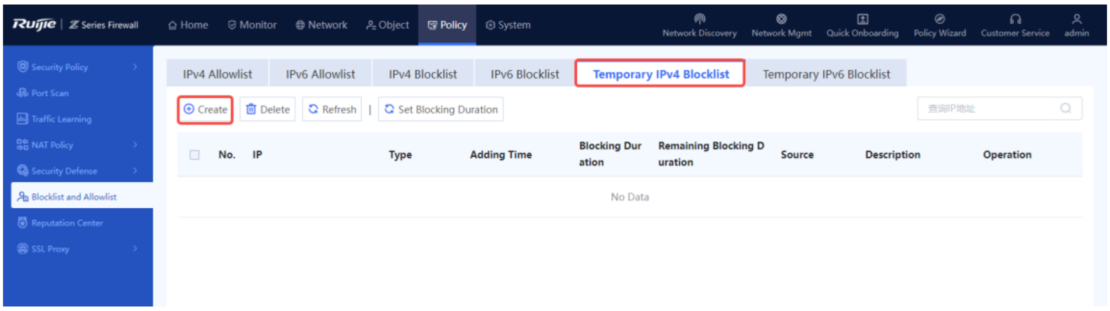
Configure a temporary IPv4 blocklist on the web UI.

Procedure

(1) Access the **Add Temporary Blocklist** page.

a Choose **Policy** > **Blocklist and Allowlist** > **Temporary IPv4 Blocklist**.

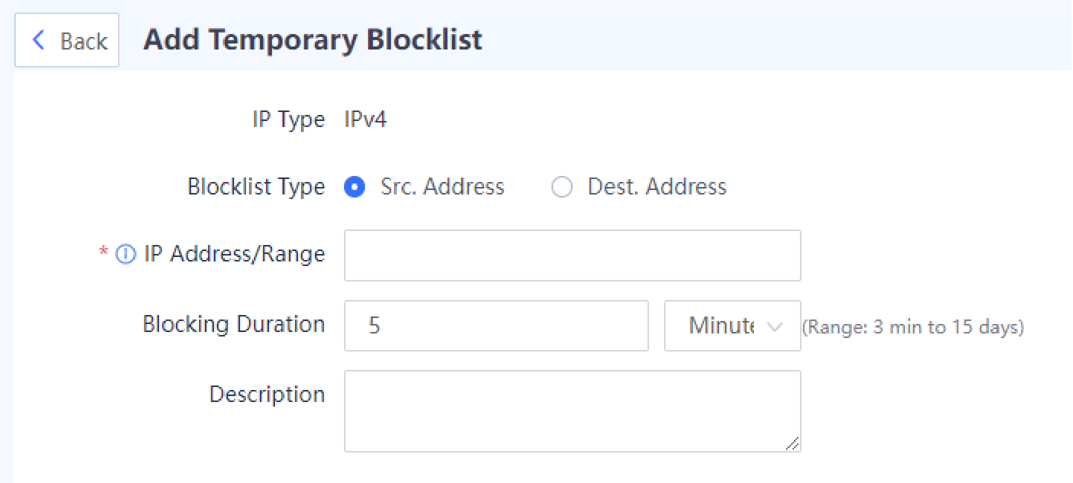
b Above the operation area, click **Create**.



□	No.	IP	Type	Adding Time	Blocking Duration	Remaining Blocking Duration	Source	Description	Operation

No Data

(2) Set parameters for the blocklist policy and click **Save**.



Add Temporary Blocklist

IP Type IPv4

Blocklist Type ● Src. Address ○ Dest. Address

* IP Address/Range

Blocking Duration 5 Minute (Range: 3 min to 15 days)

Description

Item	Description	Remarks
Blocklist Type	Type of the temporary blocklist: ● **Src. Address**: Block packets sent from this address. ● **Dest. Address**: Block packets sent to this address.	[Example] Src. Address
IP Address/Range	Temporary blocklist IP address/range.	The following two formats are supported: ● Single IP address: 192.168.1.1 ● IP address range: 192.168.1.1-192.168.1.10
Blocking Duration	Validity period of the temporary blocklist. When the validity period expires, the blocklist becomes invalid and is automatically deleted.	[Example] 5 minutes
Description	Description of the temporary	Characters such as `~!#%^&*+\\|{};:'"/<>? are not

Item	Description	Remarks
	blocklist.	allowed.

(3) After the configuration is completed, click **Save**.

Follow-up Procedure

- To delete multiple temporary blocklist policies in a batch, select the policies that you want to delete and click **Delete**.
- To configure the validity period of multiple temporary blocklist policies, select the policies and click **Set Blocking Duration**.

7.8.8 Creating a Temporary IPv6 Blocklist

Application Scenario

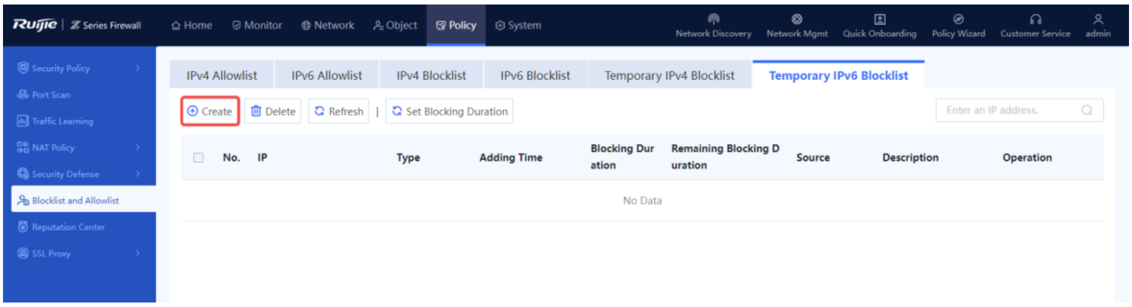
Configure a temporary IPv6 blocklist on the web UI.

Procedure

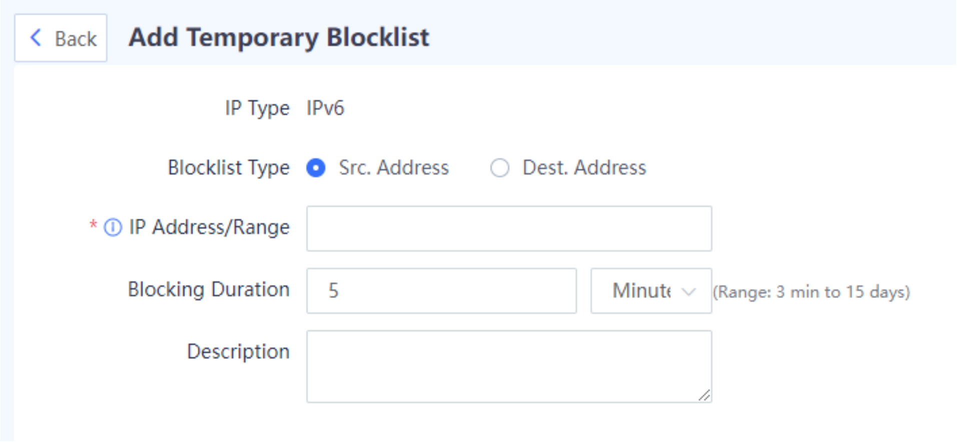
(1) Access the **Add Temporary Blocklist** page.

a Choose **Policy** > **Blocklist and Allowlist** > **Temporary IPv6 Blocklist**.

b Above the operation area, click **Create**.



(2) Set parameters for the blocklist policy and click **Save**.



< Back **Add Temporary Blocklist**

IP Type IPv6

Blocklist Type ● Src. Address ○ Dest. Address

* ⓘ IP Address/Range

Blocking Duration 5 Minute (Range: 3 min to 15 days)

Description

Item	**Description**	**Remarks**
Blocklist Type	Type of the temporary blocklist: ● **Src. Address**: Block packets sent from this address. ● **Dest. Address**: Block packets sent to this address.	[Example] Src. Address
IP Address/Range	Temporary blocklist IP address/range.	The following two formats are supported: ● Single IP address: 1234::100 ● IP address range: 1234::100-2345::100
Blocking Duration	Validity period of the temporary blocklist. When the validity period expires, the blocklist becomes invalid and is automatically deleted.	[Example] 5 minutes
Description	Description of the temporary blocklist.	Characters such as `~!#%^&*+\\\|{};:'"/<>? are not allowed.

(3) After the configuration is completed, click **Save**.

Follow-up Procedure

- To delete multiple temporary blocklist policies in a batch, select the policies that you want to delete and click **Delete**.
- To configure the validity period of multiple temporary blocklist policies, select the policies and click **Set Blocking Duration**.

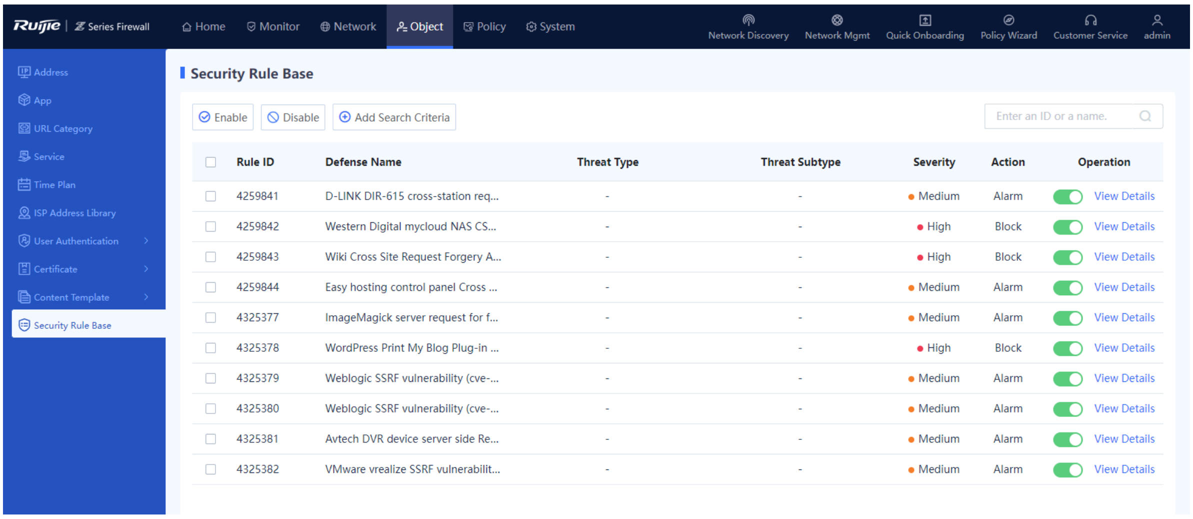
7.9 Security Rule Base Management

Application Scenario

The security rule base stores information about the features of the threats that can be detected from traffic. When traffic passes through the device, intrusion prevention matches the traffic against features in the security rule base. If matched, the device processes it according to user configuration.

Procedure

(1) Choose **Object** > **Security Rule Base**.



Security Rule Base

□	Rule ID	Defense Name	Threat Type	Threat Subtype	Severity	Action	Operation
□	4259841	D-LINK DIR-615 cross-station req...	-	-	● Medium	Alarm	View Details
□	4259842	Western Digital mycloud NAS CS...	-	-	● High	Block	View Details
□	4259843	Wiki Cross Site Request Forgery A...	-	-	● High	Block	View Details
□	4259844	Easy hosting control panel Cross ...	-	-	● Medium	Alarm	View Details
□	4325377	ImageMagick server request for f...	-	-	● Medium	Alarm	View Details
□	4325378	WordPress Print My Blog Plug-in ...	-	-	● High	Block	View Details
□	4325379	Weblogic SSRF vulnerability (cve-...	-	-	● Medium	Alarm	View Details
□	4325380	Weblogic SSRF vulnerability (cve-...	-	-	● Medium	Alarm	View Details
□	4325381	Avtech DVR device server side Re...	-	-	● Medium	Alarm	View Details
□	4325382	VMware vrealize SSRF vulnerabilit...	-	-	● Medium	Alarm	View Details

(2) Enable or disable a security rule.

- After a rule is enabled, the device detects the threats defined by the rule for the traffic passing the device.
- After a rule is disabled, the device does not detect the threats defined by the rule for the traffic passing the device.

7.10 Connecting to Ruijie Cloud

7.10.1 Overview

Ruijie Cloud is a remote management platform that manages all links and devices (such as gateway, switch, AP, and firewall) in SMB scenarios. The administrator can add devices to the Ruijie Cloud, and then manage the devices anytime, anywhere.

Note

You can bind a device to the Ruijie Cloud platform when the device is quickly online. If it is not bound, follow the steps described in this section to bind it.

7.10.2 Connecting to Ruijie Cloud

1. Enabling Ruijie Cloud

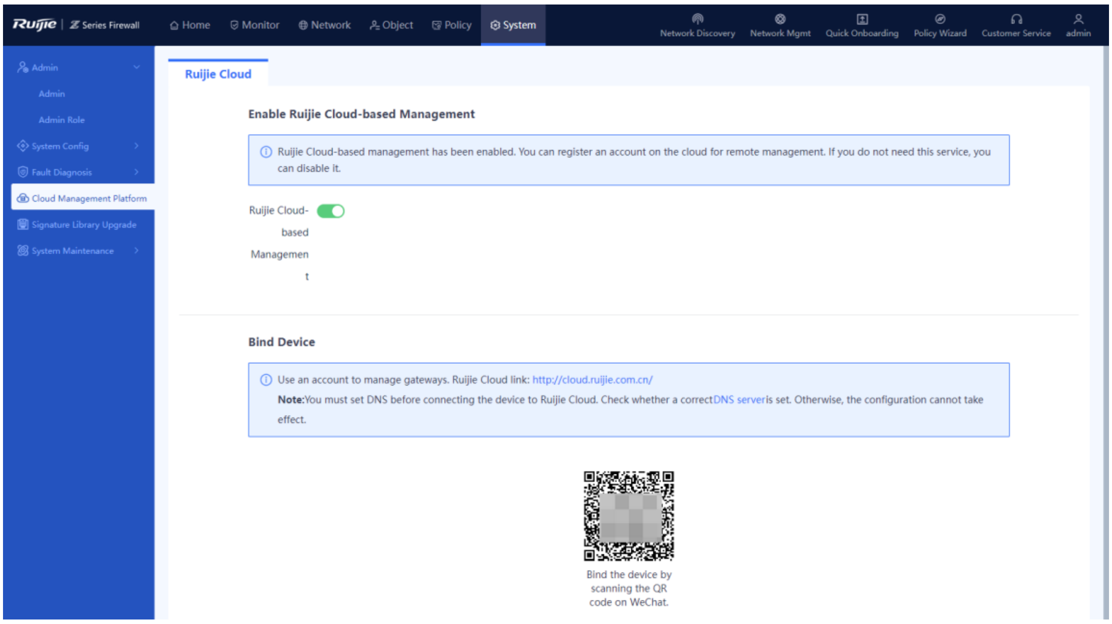
Application Scenario

Based on the Ruijie Cloud platform, you can view the basic information of devices (including software version, hardware version, MAC address, and product model), upgrade the devices, view the interface information of the devices, open reverse tunnels, and remotely control the devices through the devices' EWEB function.

Procedure

(1) Choose **System** > **Cloud Management Platform** > **Ruijie Cloud**.

(2) Enable **Ruijie Cloud-based Management** (enabled by default). Then you can manage the firewall on Ruijie Cloud.



Enable Ruijie Cloud-based Management

Ruijie Cloud-based management has been enabled. You can register an account on the cloud for remote management. If you do not need this service, you can disable it.

Ruijie Cloud-based Management

Bind Device

Use an account to manage gateways. Ruijie Cloud link: http://cloud.ruijie.com.cn/

Note: You must set DNS before connecting the device to Ruijie Cloud. Check whether a correctDNS serveris set. Otherwise, the configuration cannot take effect.

Bind the device by scanning the QR code on WeChat.

2. Binding Devices

Application Scenario

Before managing the firewall using Ruijie Cloud, you need to bind the firewall. After the firewall is bound, you can view device information and maintain the firewall on Ruijie Cloud.

Procedure

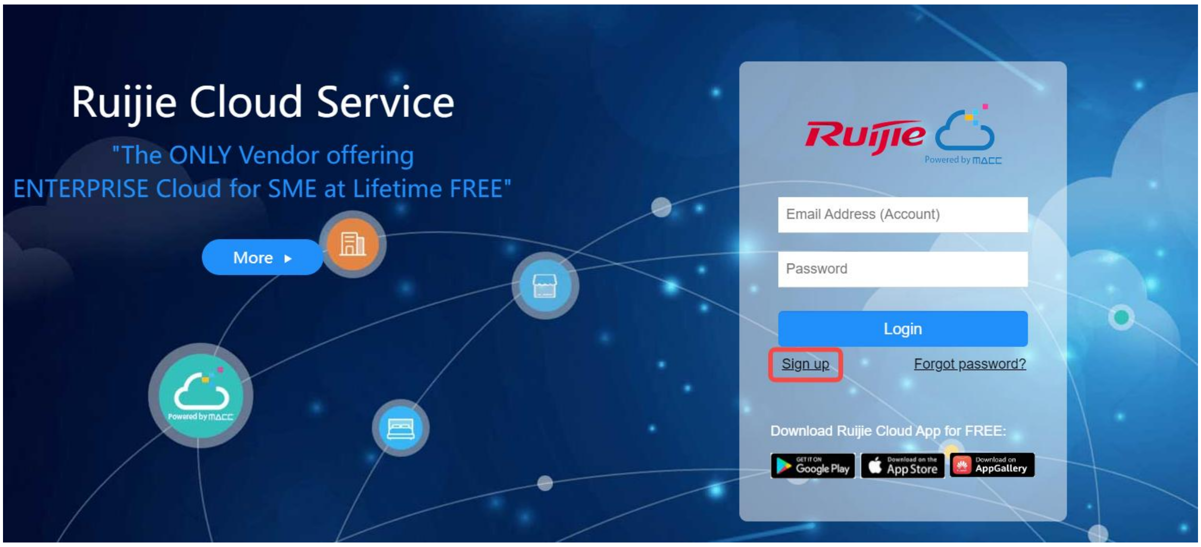
(1) Log in to the web management page of the firewall.

(2) Choose **System** > **Cloud Management Platform** > **Ruijie Cloud**.

(3) In the **Bind Device** area, click the URL address of Ruijie Cloud and register a Ruijie Cloud account.

(4) After registering the Ruijie Cloud account, you can log in to view basic device information.

Figure 7-5 Registering an Account



Ruijie Cloud Service

"The ONLY Vendor offering ENTERPRISE Cloud for SME at Lifetime FREE"

More ▸

Email Address (Account)

Password

Login

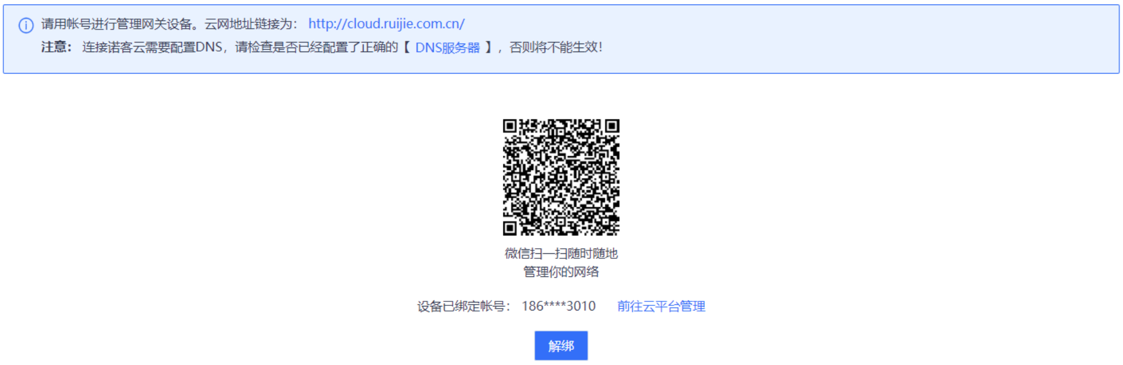
Sign up

Forgot password?

Download Ruijie Cloud App for FREE:

Follow-up Procedure

After the firewall is bound, the web page prompts you that the firewall has been bound to the related account.



ⓘ 请用帐号进行管理网关设备。云网地址链接为：http://cloud.ruijie.com.cn/

注意：连接诺客云需要配置DNS，请检查是否已经配置了正确的【 DNS服务器 】，否则将不能生效！

微信扫一扫随时随地
管理你的网络

设备已绑定帐号：186****3010 前往云平台管理

解绑

7.10.3 Operations on Ruijie Cloud

1. Viewing Device Information

Application Scenario

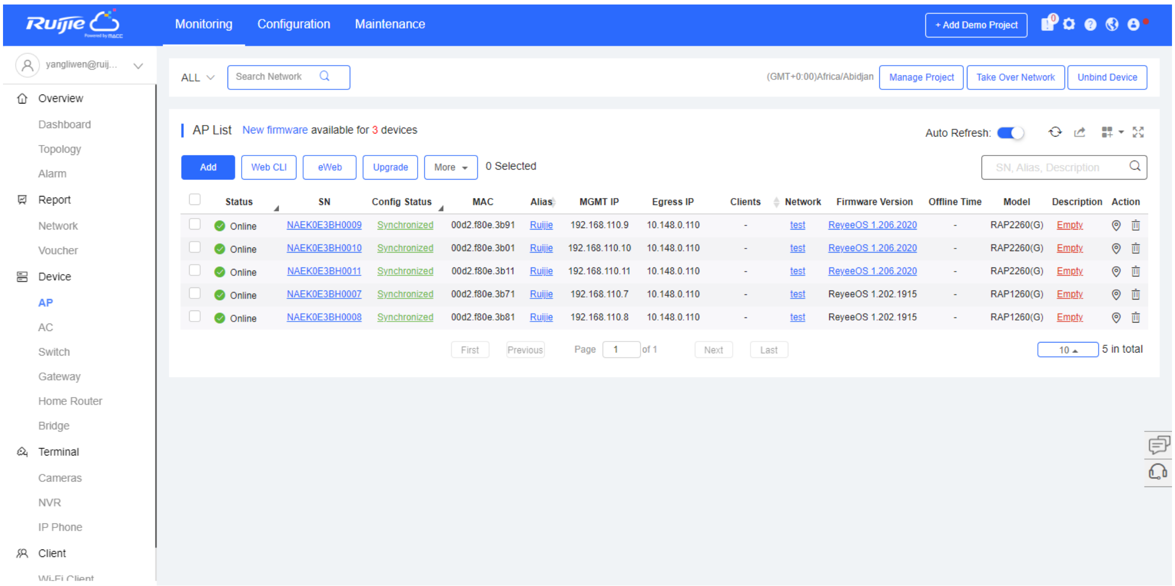
After enabling Ruijie Cloud, enter the address of Ruijie Cloud platform in the browser, log in, and then you can view device information, online status, and interface information.

Procedure

(1) Choose **Monitoring** > **Device** > **Firewall** to open the device list.

(2) View device details.

Figure 7-6 Firewall Details



(GMT+0:00)Africa/Abidjan

AP List New firmware available for 3 devices

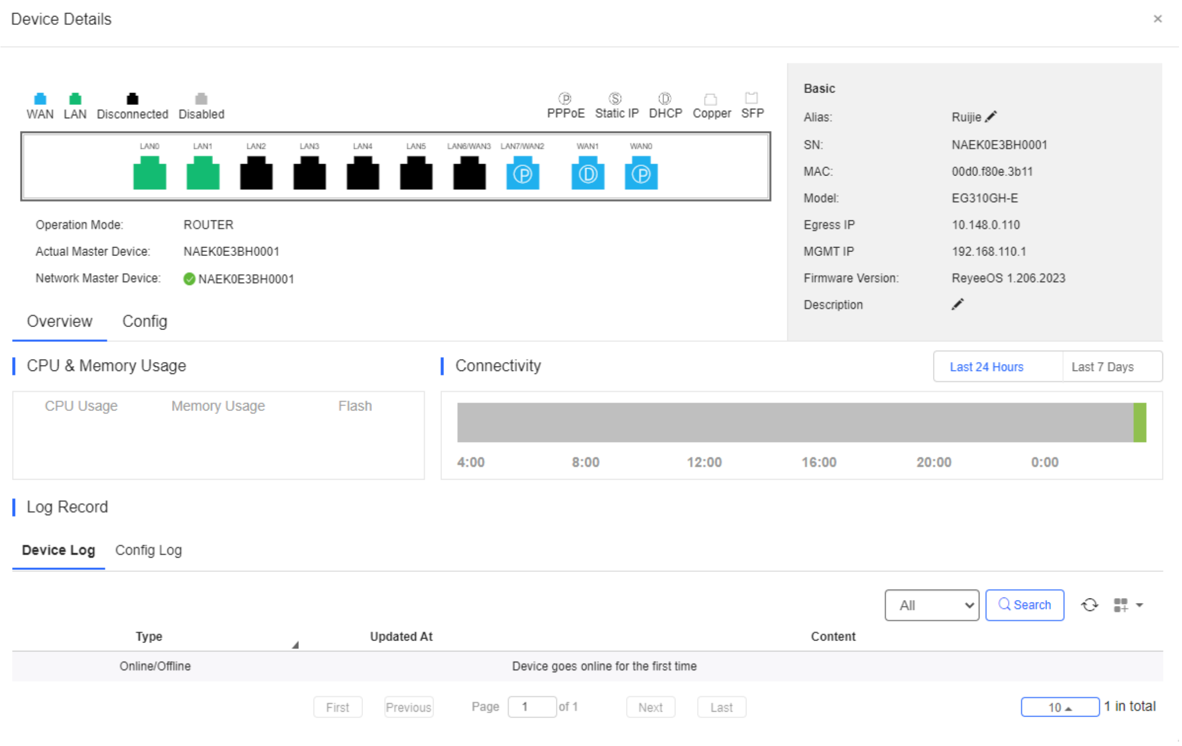
0 Selected

Status	SN	Config Status	MAC	Alias	MGMT IP	Egress IP	Clients	Network	Firmware Version	Offline Time	Model	Description	Action
Online	NAEK0E3BH0009	Synchronized	00d2.f80e.3b91	Ruijie	192.168.110.9	10.148.0.110	-	test	ReyeeOS 1.206.2020	-	RAP2260(G)	Empty	
Online	NAEK0E3BH0010	Synchronized	00d2.f80e.3b01	Ruijie	192.168.110.10	10.148.0.110	-	test	ReyeeOS 1.206.2020	-	RAP2260(G)	Empty	
Online	NAEK0E3BH0011	Synchronized	00d2.f80e.3b11	Ruijie	192.168.110.11	10.148.0.110	-	test	ReyeeOS 1.206.2020	-	RAP2260(G)	Empty	
Online	NAEK0E3BH0007	Synchronized	00d2.f80e.3b71	Ruijie	192.168.110.7	10.148.0.110	-	test	ReyeeOS 1.202.1915	-	RAP1260(G)	Empty	
Online	NAEK0E3BH0008	Synchronized	00d2.f80e.3b81	Ruijie	192.168.110.8	10.148.0.110	-	test	ReyeeOS 1.202.1915	-	RAP1260(G)	Empty	

Page 1 of 1 10 5 in total

The system displays the basic device information such as status, SN, device, management address, software version, and device model.

(3) Click **SN** to enter the device management page. View device basic information, panel information, interface information, and status.



Device Details

Operation Mode: ROUTER
Actual Master Device: NAEK0E3BH0001
Network Master Device: NAEK0E3BH0001

Basic
Alias: Ruijie
SN: NAEK0E3BH0001
MAC: 00d0.f80e.3b11
Model: EG310GH-E
Egress IP 10.148.0.110
MGMT IP 192.168.110.1
Firmware Version: ReyeeOS 1.206.2023
Description

CPU & Memory Usage

Connectivity

Log Record

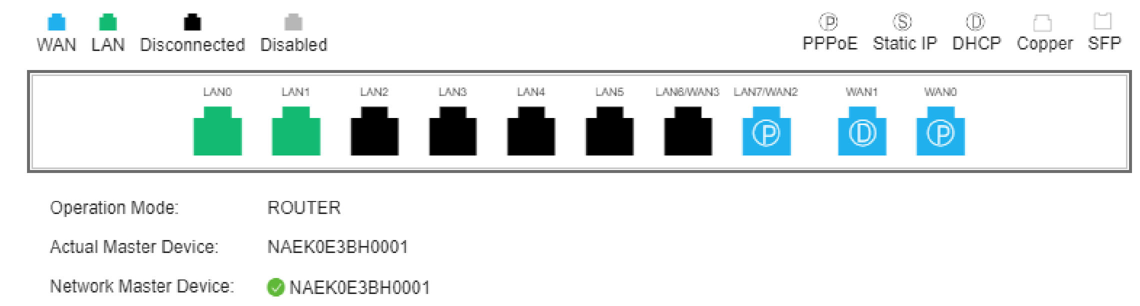
Type	Updated At	Content
Online/Offline		Device goes online for the first time

Page 1 of 1 10 1 in total

You can click the titles one by one to manage devices.

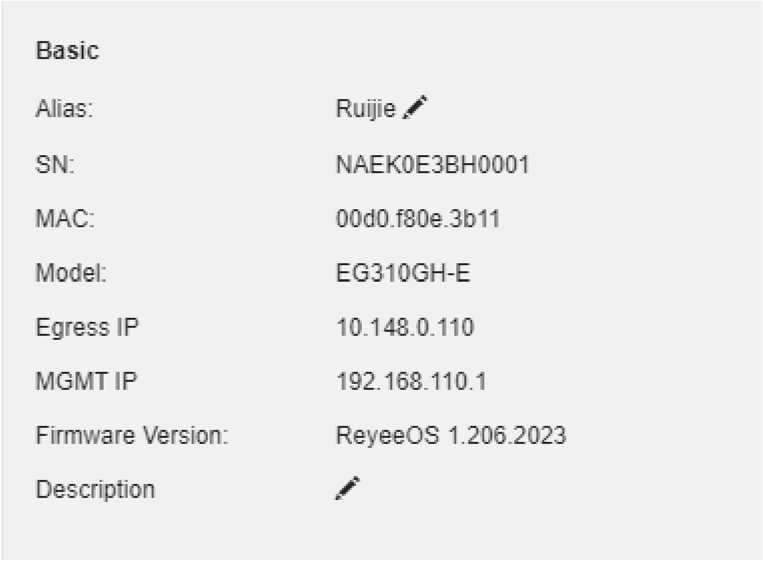
- Device panel: includes information such as interface distribution on panel.
- Basic information: includes device name, device model, SN, MAC address, and software version.
- Status: includes CPU and memory usage, offline status, and connectivity status.
- Interface information: By clicking the titles in status information, you can view detailed interface information, such as WAN/LAN port information (such as port number, mode, and subnet mask).

Figure 7-7 Device Panel Information



Operation Mode:	ROUTER
Actual Master Device:	NAEK0E3BH0001
Network Master Device:	✓ NAEK0E3BH0001

Figure 7-8 Basic Information



Basic

Alias:	Ruijie
SN:	NAEK0E3BH0001
MAC:	00d0.f80e.3b11
Model:	EG310GH-E
Egress IP	10.148.0.110
MGMT IP	192.168.110.1
Firmware Version:	ReyeeOS 1.206.2023
Description	

Figure 7-9 Status Information

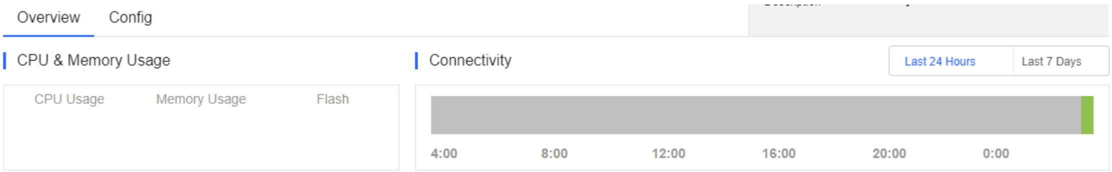
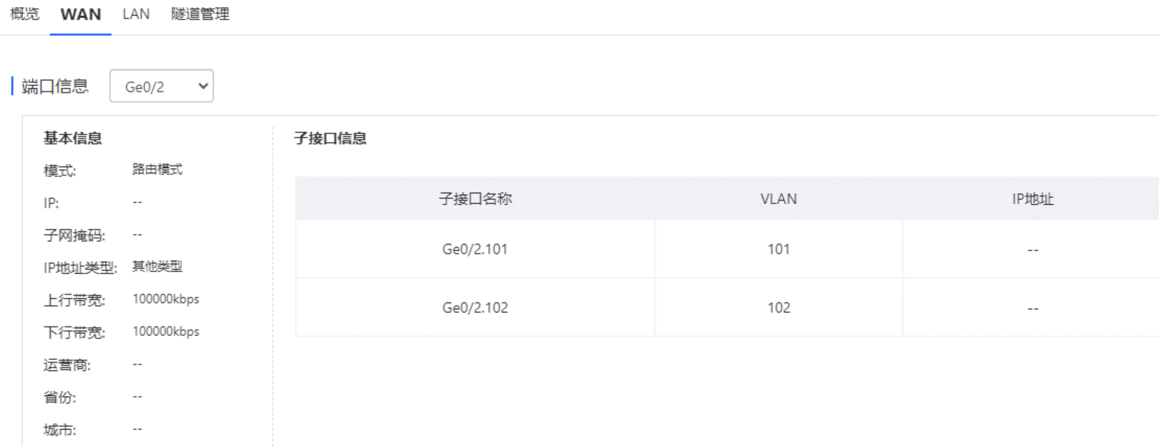


Figure 7-10 Interface Information



基本信息

模式:	路由模式
IP:	--
子网掩码:	--
IP地址类型:	其他类型
上行带宽:	100000kbps
下行带宽:	100000kbps
运营商:	--
省份:	--
城市:	--

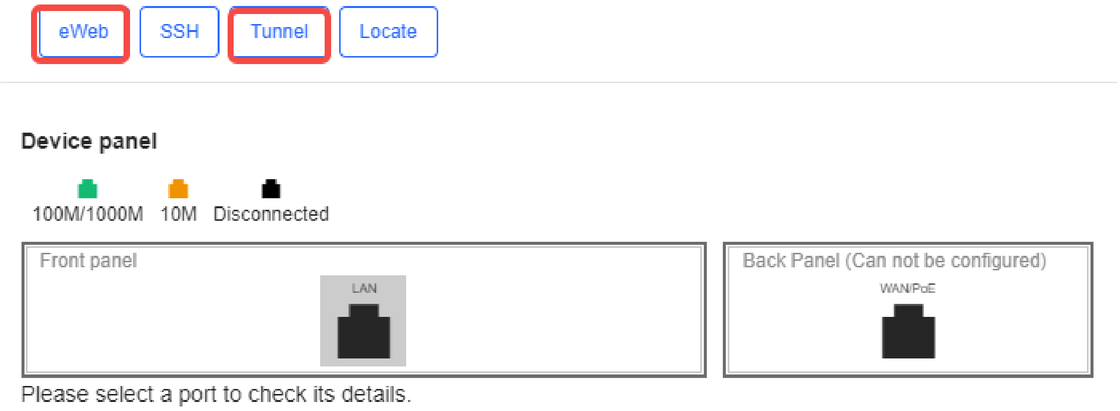
子接口信息

子接口名称	VLAN	IP地址
Ge0/2.101	101	--
Ge0/2.102	102	--

2. Managing Tunnels

(1) Click **Tunnel** or **eWeb** to access the EWEB page of the device.

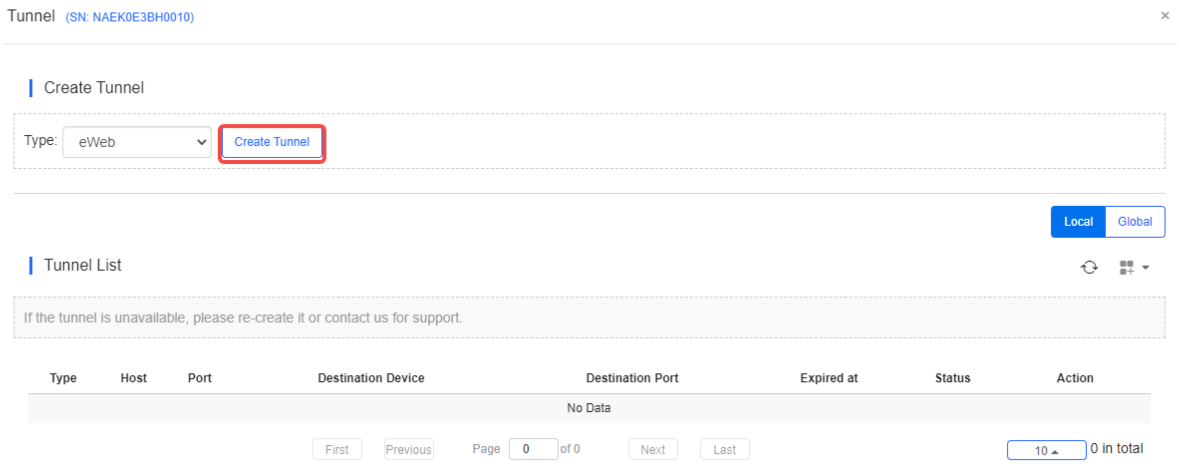
Figure 7-11 Tunnel Management



Please select a port to check its details.

(2) To add a tunnel, click **Create Tunnel**.

Figure 7-12Creating a Tunnel



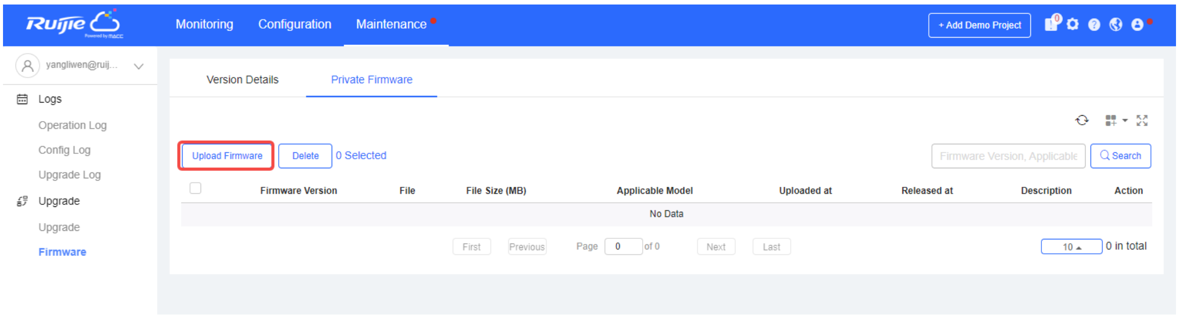
If the tunnel is unavailable, please re-create it or contact us for support.

Type	Host	Port	Destination Device	Destination Port	Expired at	Status	Action
No Data							

3. Upgrading Device Software/Firmware

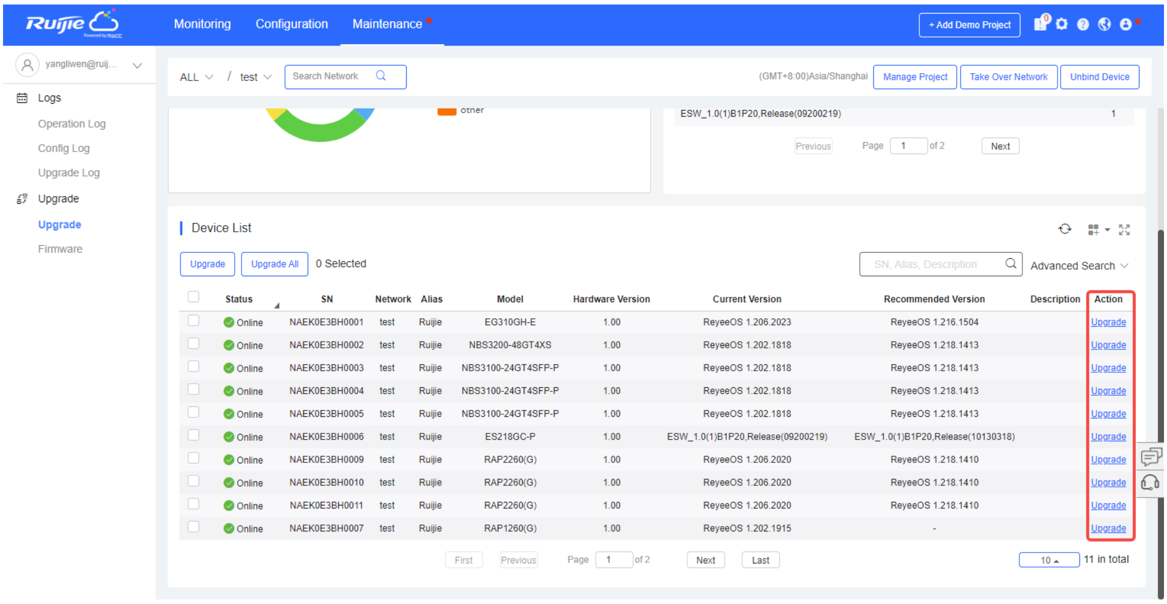
(1) Choose **Maintenance** > **Upgrade** > **Firmware** > **Private Firmware**.

(2) Click **Upload Firmware** to upload the software version/firmware version.



□	Firmware Version	File	File Size (MB)	Applicable Model	Uploaded at	Released at	Description	Action
No Data								

(3) Choose **Maintenance** > **Upgrade** > **Upgrade**, find out the device to be upgraded in **Device List**, and click **Upgrade**.

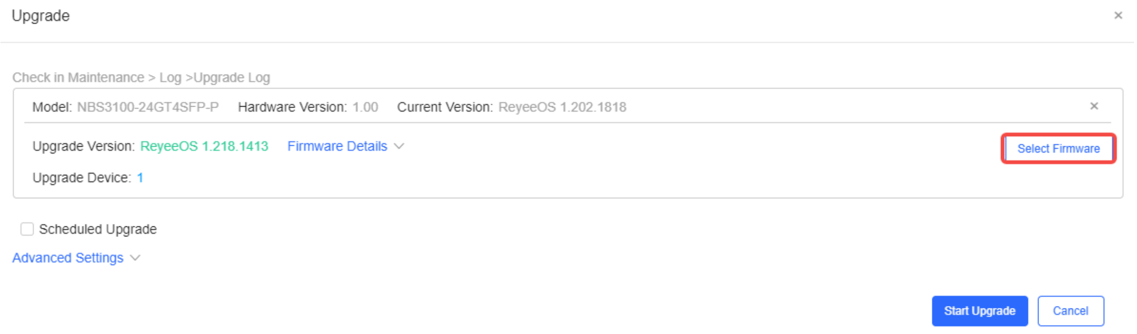


0 Selected

Status	SN	Network	Alias	Model	Hardware Version	Current Version	Recommended Version	Description	Action
Online	NAEK0E3BH0001	test	Ruijie	EG310GH-E	1.00	ReyeeOS 1.206.2023	ReyeeOS 1.216.1504		Upgrade
Online	NAEK0E3BH0002	test	Ruijie	NBS3200-48GT4XS	1.00	ReyeeOS 1.202.1818	ReyeeOS 1.218.1413		Upgrade
Online	NAEK0E3BH0003	test	Ruijie	NBS3100-24GT4SFP-P	1.00	ReyeeOS 1.202.1818	ReyeeOS 1.218.1413		Upgrade
Online	NAEK0E3BH0004	test	Ruijie	NBS3100-24GT4SFP-P	1.00	ReyeeOS 1.202.1818	ReyeeOS 1.218.1413		Upgrade
Online	NAEK0E3BH0005	test	Ruijie	NBS3100-24GT4SFP-P	1.00	ReyeeOS 1.202.1818	ReyeeOS 1.218.1413		Upgrade
Online	NAEK0E3BH0006	test	Ruijie	ES218GC-P	1.00	ESW_1.0(1)B1P20,Release(09200219)	ESW_1.0(1)B1P20,Release(10130318)		Upgrade
Online	NAEK0E3BH0009	test	Ruijie	RAP2260(G)	1.00	ReyeeOS 1.206.2020	ReyeeOS 1.218.1410		Upgrade
Online	NAEK0E3BH0010	test	Ruijie	RAP2260(G)	1.00	ReyeeOS 1.206.2020	ReyeeOS 1.218.1410		Upgrade
Online	NAEK0E3BH0011	test	Ruijie	RAP2260(G)	1.00	ReyeeOS 1.206.2020	ReyeeOS 1.218.1410		Upgrade
Online	NAEK0E3BH0007	test	Ruijie	RAP1260(G)	1.00	ReyeeOS 1.202.1915	-		Upgrade

First Previous Page 1 of 2 Next Last 10 11 in total

(4) Click **Select Firmware** to select the upgrade package file to be uploaded.



Check in Maintenance > Log >Upgrade Log

Model: NBS3100-24GT4SFP-P Hardware Version: 1.00 Current Version: ReyeeOS 1.202.1818

Upgrade Version: ReyeeOS 1.218.1413 Firmware Details

Upgrade Device: 1

□ Scheduled Upgrade

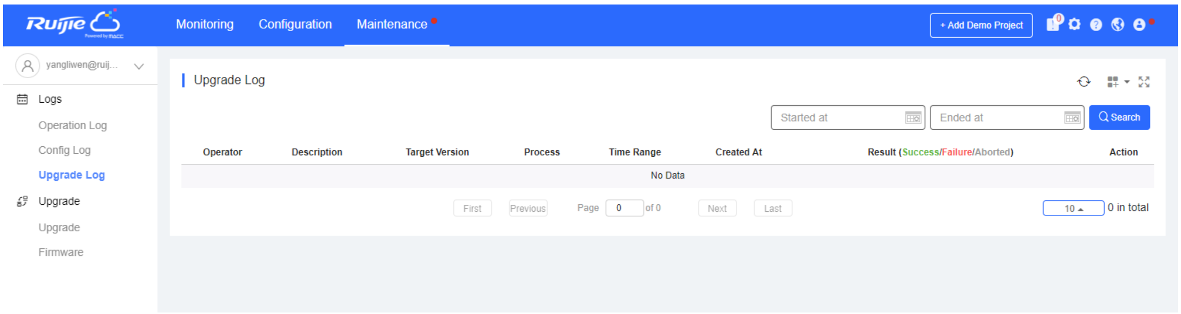
Advanced Settings

(5) Click **Start Upgrade** to start the upgrade.

Then the device performs upgrade. During the upgrade, the device will automatically restart. Wait until the upgrade is completed.

(6) When the upgrade is finished, choose **Maintenance** > **Logs** > **Upgrade Log** to view the upgrade result.

Figure 7-13 Upgrade Result



Operator	Description	Target Version	Process	Time Range	Created At	Result (Success/Failure/Aborted)	Action
No Data							

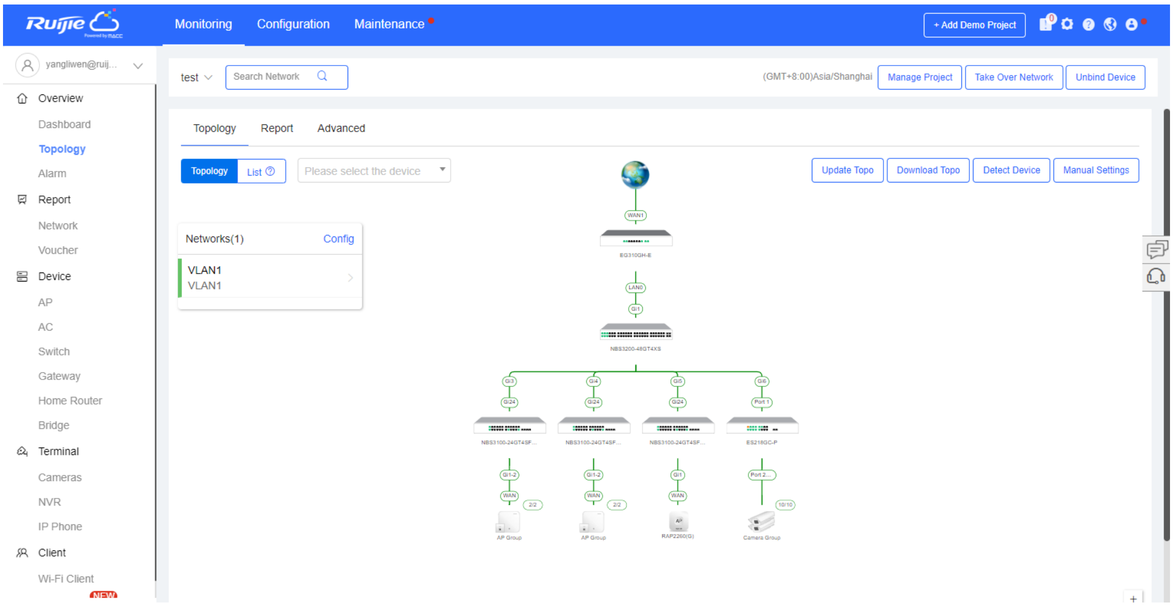
4. Viewing Network Topology

The relationships between the firewall and other network devices can be discovered on Ruijie Cloud and the topology is generated.

Caution

- When there are multiple default routes on the firewall, or when both bridge interfaces and routing interfaces are used, you will find that the topology on Ruijie Cloud is abnormal.
- When the firewall is in transparent mode, port 0/MGMT does not need to be connected separately.

Choose **Monitoring** > **Overview** > **Topology** to view the topology of firewall and other network devices.



Follow-up Procedure

- To obtain the latest topology, click **Update Topo**.
- To download the network topology, click **Download Topo**.
- To edit the topology and add the devices that are not discovered automatically, click **Manual Settings**.

7.11 DNS Server Configuration

Application Scenario

The Domain Name System (DNS), a distributed database on the Internet that provides mutual mapping between domain names and IP addresses, makes it easier for users to access the Internet without having to memorize IP strings that can be directly read by machines. Domain name resolution (or host name resolution) is a process where the IP address corresponding to a given host name is finally obtained.

Prerequisites

The system supports at most three DNS servers. DNS server 1 has the highest priority and DNS server 3 has the lowest priority. The system uses the server with the highest priority first.

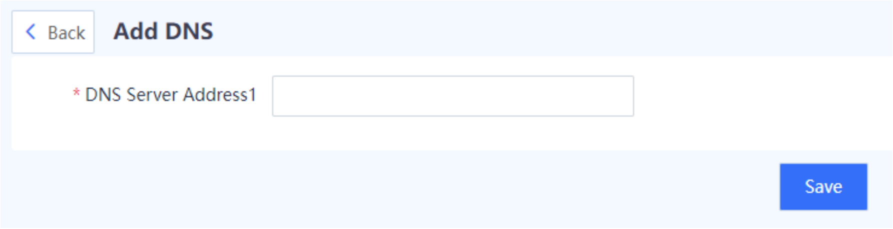
Procedure

(1) Choose **Network** > **DNS**.

(2) Set the IP address of DNS server 1.

a Click **Create**.

The system displays the **Add DNS** page.



b Enter the IP address of the DNS server 1 in the **DNS Server Address1** input box.

c Click **Save**.

(3) (Optional) If multiple DNS servers are configured in the network environment, you can set the IP address for the second or third DNS server.

7.12 Intelligent Routing

Application Scenario

Intelligent Routing, also called policy-based routing (PBR) or application-based routing, is a mechanism for routing and forwarding based on user-specified policies. By using intelligent routing, you can redirect the packets that meet the matching conditions to the specified outbound interface and next hop.

After PBR is configured, the device first filters the packets according to the configured rules, and then forwards the matched packets according to the specified forwarding policy. PBR creates rules according to specific fields (source or destination IP address and protocol type) in the data packets, and forwards the data packets through a specific interface.

In a multi-path scenario where no routing rules are configured, if the device is connected to different service networks through different paths, the traffic will be evenly routed over the paths. In this situation, the access data to service networks may be incorrectly sent to other networks, causing a network abnormality. You can configure PBR to control data isolation and forwarding among networks.

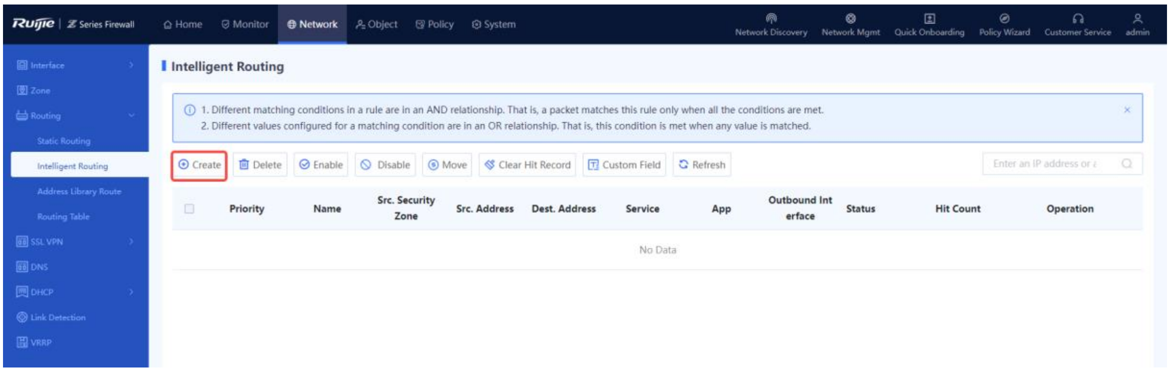
Note

- PBR is supported from NTOS1.0R3. If your version is lower than NTOS1.0R3, upgrade it to NTOS1.0R3 or higher.
- Application routing is supported from NTOS1.0R4. If your version is lower than NTOS1.0R4, upgrade it to NTOS1.0R4 or higher.

Procedure

(1) Choose **Network** > **Routing** > **Intelligent Routing**.

(2) Click **Create** to enter the **Create Intelligent Routing** page.

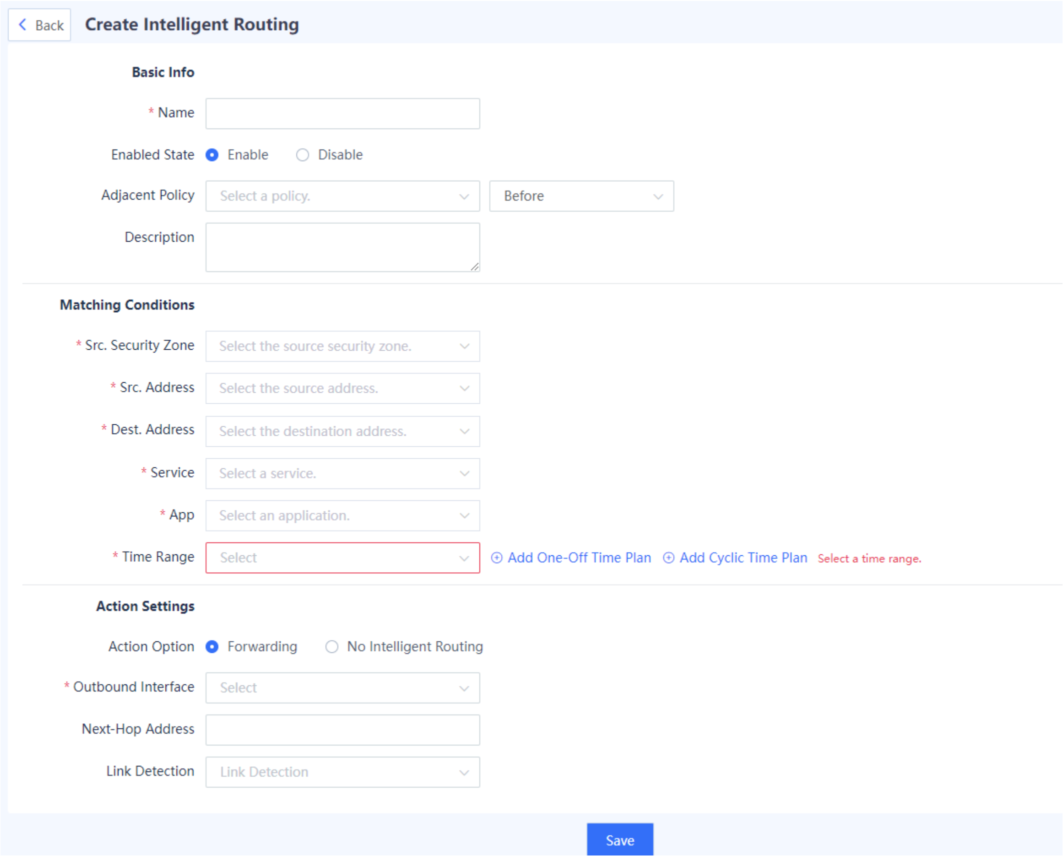


Intelligent Routing

1. Different matching conditions in a rule are in an AND relationship. That is, a packet matches this rule only when all the conditions are met.
2. Different values configured for a matching condition are in an OR relationship. That is, this condition is met when any value is matched.

□	Priority	Name	Src. Security Zone	Src. Address	Dest. Address	Service	App	Outbound Interface	Status	Hit Count	Operation
No Data											

(3) Set parameters of intelligent routing.



< Back **Create Intelligent Routing**

Basic Info

* Name

Enabled State ● Enable ○ Disable

Adjacent Policy Select a policy. Before

Description

Matching Conditions

* Src. Security Zone Select the source security zone.

* Src. Address Select the source address.

* Dest. Address Select the destination address.

* Service Select a service.

* App Select an application.

* Time Range Select ⊕ Add One-Off Time Plan ⊕ Add Cyclic Time Plan Select a time range.

Action Settings

Action Option ● Forwarding ○ No Intelligent Routing

* Outbound Interface Select

Next-Hop Address

Link Detection Link Detection

Save

Item	Description	Remarks
Basic Info		
Name	Name of intelligent routing.	Characters such as `~!#%^&*+\/0::"/<>? and spaces are not allowed. [Example] Policy_1
Enabled State	Whether to enable the new intelligent routing.	[Example] Enabled
Adjacent Policy	Move the new policy before or after the specified policy. The closer a policy is to the front, the higher its	-

Item	**Description**	**Remarks**
	priority is in matching.	
Description	Route description.	Characters such as `~!#%^&*+\\\|{};:'"/<>? are not allowed.
Matching Conditions		
Src. Security Zone	Forwards the packets from this source security zone based on the policy.	● Click the drop-down list, and select a source security zone in the **To-be-selected** area. The selected zone is automatically added to the **Selected** area. ● Click **Add Security Zone** to add a custom security zone. [Example] trust
Src. Address	Forwards the packets from this source address or address group based on the policy.	Click the drop-down list, and select a source address in the **To-be-selected** area. The selected address is automatically added to the **Selected** area. [Example] Any
Dest. Address	Forwards the packets to this destination address or address group based on the policy.	Click the drop-down list, and select a destination address in the **To-be-selected** area. The selected address is automatically added to the **Selected** area. [Example] Any

Item	Description	Remarks
Service	Forwards the packets of this service type based on the policy.	[Example] Any
App	Forwards the packets of this application type based on the policy.	[Example] Any
Time Range	Time range in which the intelligent routing is effective.	[Example] Any
Action Settings		
Action Option	Whether to forward the matched packets based on the policy. If forwarded, you need to configure **Outbound Interface** and **Next-Hop Address**.	[Example] Forwarding
Link Detection	Link detection policy associated with outbound interface. This configuration can detect the network connectivity between the outbound interface and the next hop in real time. If the network connection between the outbound interface and the next hop is abnormal, this route becomes invalid.	For details about link detection, see 7.15 Link Detection.

(4) Click **Save**.

7.13 Address Library Routing (ISP-based Routing)

7.13.1 Overview

The ISP address library stores all the IP addresses on ISP's network. After the ISP address library is configured and bound to the device's WAN interface, the route to the corresponding ISP's IP address is generated, so that the packets destined for the ISP's network are forwarded through the corresponding outbound interface, meeting the ISP-based routing requirements in multi-egress scenarios and optimizing the forwarding path of traffic.

To customize an ISP address library, you can add routes or import routes in file format to the library.

7.13.2 Configuring an ISP Address Library

1. Creating an ISP Address Library Manually

Application Scenario

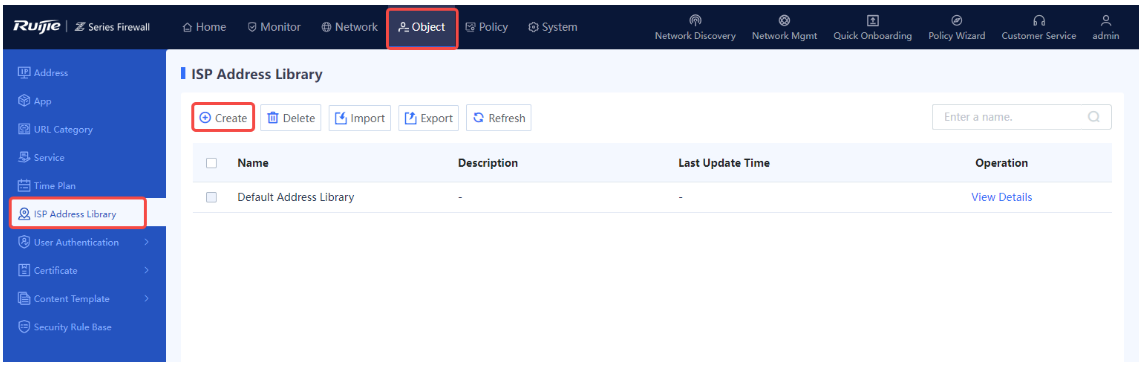
You can add addresses to the ISP address library one by one. This method is applicable to the address library containing a few addresses.

Procedure

(1) Open the **Create ISP Address Library** page.

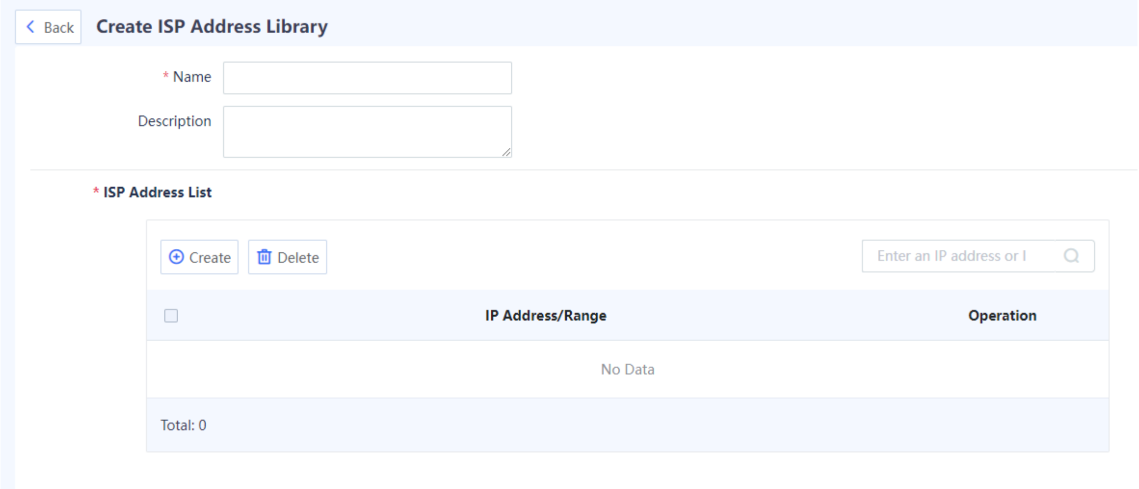
a Choose **Object** > **ISP Address Library**.

b Above the operation area, click **Create**.



	Name	Description	Last Update Time	Operation
□	Default Address Library	-	-	View Details

(2) Set parameters of the ISP address library.



Back Create ISP Address Library

* Name

Description

* ISP Address List

Create Delete Enter an IP address or I

□	IP Address/Range	Operation
	No Data	

Total: 0

Item	Description	Remarks
Name	Name of the ISP address library.	Characters such as \`~!#%^&*+\\\|{};:'"/<>? and spaces are not allowed. [Example] Address library 1
Description	Description of the ISP address library.	Characters such as \`~!#%^&*+\\\|{};:'"/<>? are not allowed. [Example] Address library 1
ISP Address List	IP addresses contained in the address library.	Click **Create** to enter a single IP address or an IP address range. Three configuration methods are supported: ● IP address: One or multiple IP addresses. Input an IP address per line. Press **Enter** to separate lines. Example: 192.168.20.3 ● IP address range: A contiguous range of addresses. Connect the start IP address and end IP address with a hyphen (-). Example:

Item	Description	Remarks
		192.168.20.1-192.168.20.3. ● Network segment: IP address network segment. Example: 192.168.1.0/24 or 192.168.1.0/255.255.255.0

(3) Click **Save**.

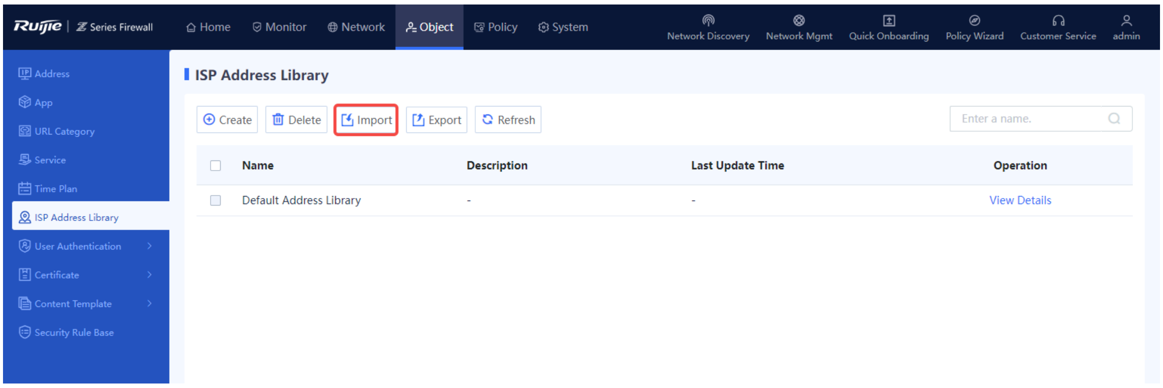
2. Importing an Address File to an ISP Address Library

Application Scenario

You can create the ISP address library by importing an address file. This method is applicable to the address library containing many addresses.

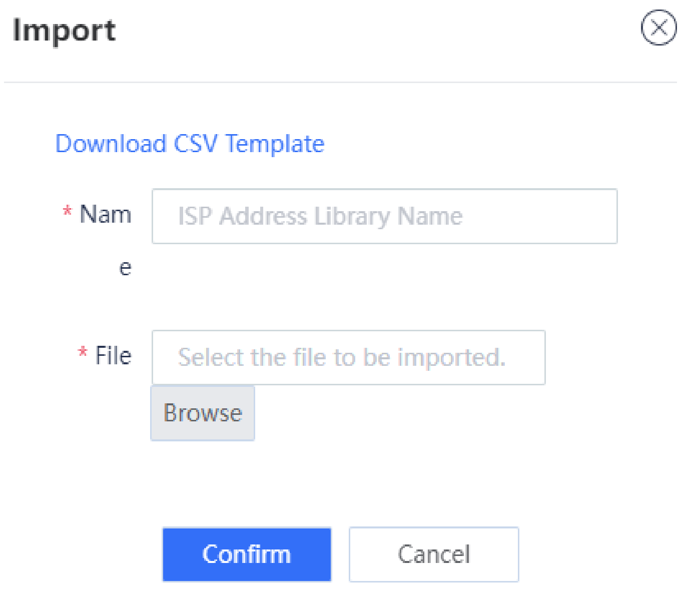
Procedure

(1) Choose **Object** > **ISP Address Library** and click **Import** in the operation area.



Name	Description	Last Update Time	Operation
Default Address Library	-	-	View Details

(2) Click **Download CSV Template** to download the template of the ISP address library file and enter IP addresses in the template.



(3) In the **Import** dialog box, enter the name of the ISP address library and click **Browse** to select the address library file. The file to be imported must be a CSV file.

(4) Click **Confirm**.

Follow-up Procedure

- To delete the imported ISP address library, click **Delete**.

⚠ **Caution**

- The ISP address library in use (that is, associated with device interface) cannot be deleted.
- The default address library preconfigured in the system cannot be deleted or modified.

- To modify the IP addresses included in the address library, click **Edit**.

3. Upgrading ISP Address Library

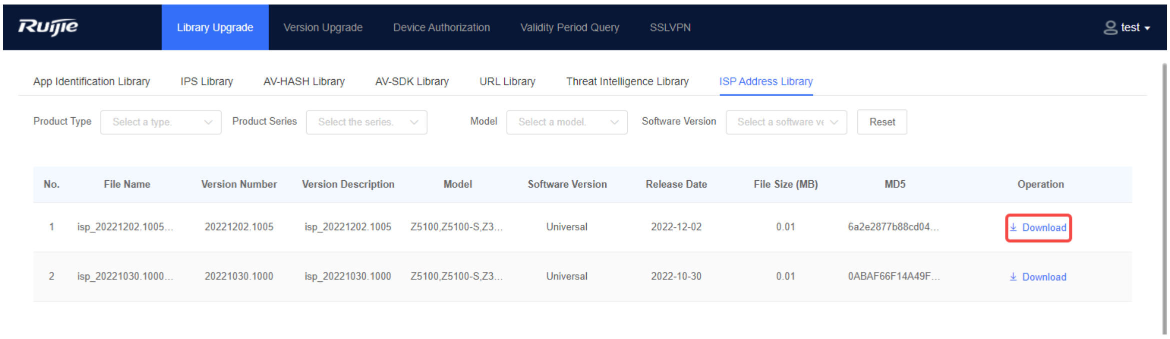
Application Scenario

The ISP address library is continuously updated. By upgrading the ISP address library, the device can obtain and generate the latest address library routes.

Procedure

(1) Log in to the Secure Cloud Platform and download the upgrade file of ISP address library.

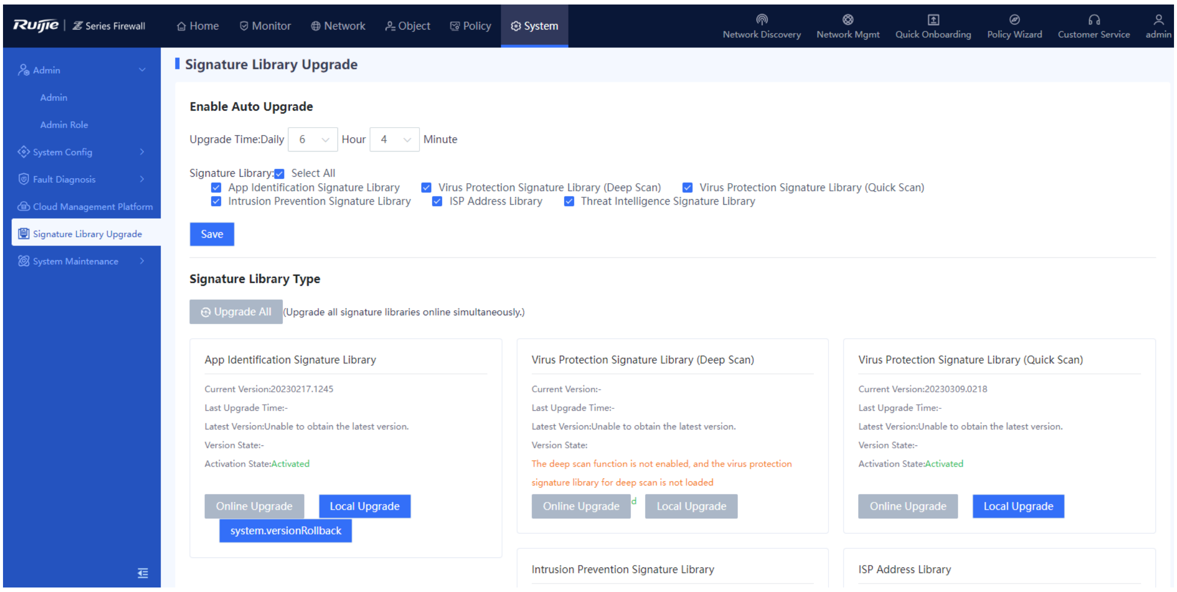
Log in to https://secloud-en.ruijienetworks.com, choose **Signature Library Upgrade** > **ISP Address Library**, and select a suitable version to download.



No.	File Name	Version Number	Version Description	Model	Software Version	Release Date	File Size (MB)	MD5	Operation
1	isp_20221202.1005...	20221202.1005	isp_20221202.1005	Z5100,Z5100-S,Z3...	Universal	2022-12-02	0.01	6a2e2877b88cd04...	Download
2	isp_20221030.1000...	20221030.1000	isp_20221030.1000	Z5100,Z5100-S,Z3...	Universal	2022-10-30	0.01	0ABAF66F14A49F...	Download

(2) Open the **Signature Library Upgrade** page.

Open the web page on the device, and choose **System** > **Signature Library Upgrade**.



Signature Library Upgrade

Enable Auto Upgrade

Upgrade Time:Daily 6 Hour 4 Minute

Signature Library:☑ Select All
☑ App Identification Signature Library ☑ Virus Protection Signature Library (Deep Scan) ☑ Virus Protection Signature Library (Quick Scan)
☑ Intrusion Prevention Signature Library ☑ ISP Address Library ☑ Threat Intelligence Signature Library

Signature Library Type

(Upgrade all signature libraries online simultaneously.)

App Identification Signature Library
Current Version:20230217.1245
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated

Virus Protection Signature Library (Deep Scan)
Current Version:-
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:
The deep scan function is not enabled, and the virus protection signature library for deep scan is not loaded

Virus Protection Signature Library (Quick Scan)
Current Version:20230309.0218
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated

Intrusion Prevention Signature Library

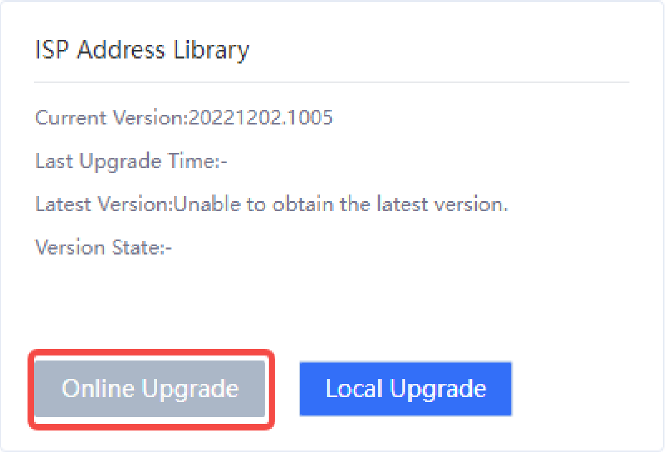
ISP Address Library

(3) Find out **ISP Address Library**, and select **Online Upgrade** or **Local Upgrade** according to actual situation.

- Online Upgrade: When the current version information about the firewall exists on the cloud platform and a new version is available, online upgrade of the device system can be performed on the firewall.

⚠ **Caution**

The firewall must be connected to the Internet.



ISP Address Library

Current Version:20221202.1005

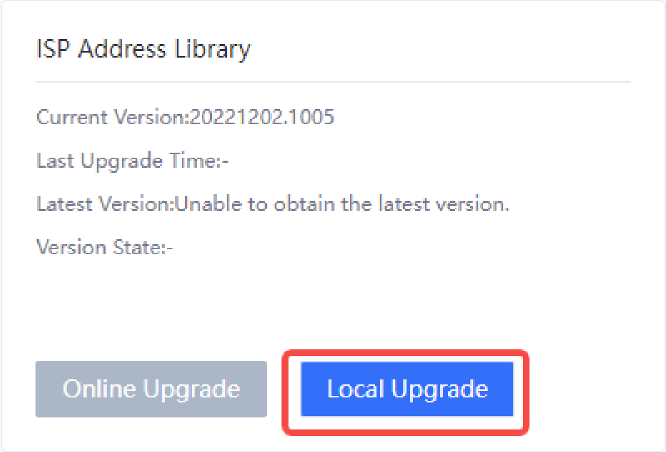
Last Upgrade Time:-

Latest Version:Unable to obtain the latest version.

Version State:-

- Local Upgrade

a Click **Local Upgrade**.



ISP Address Library

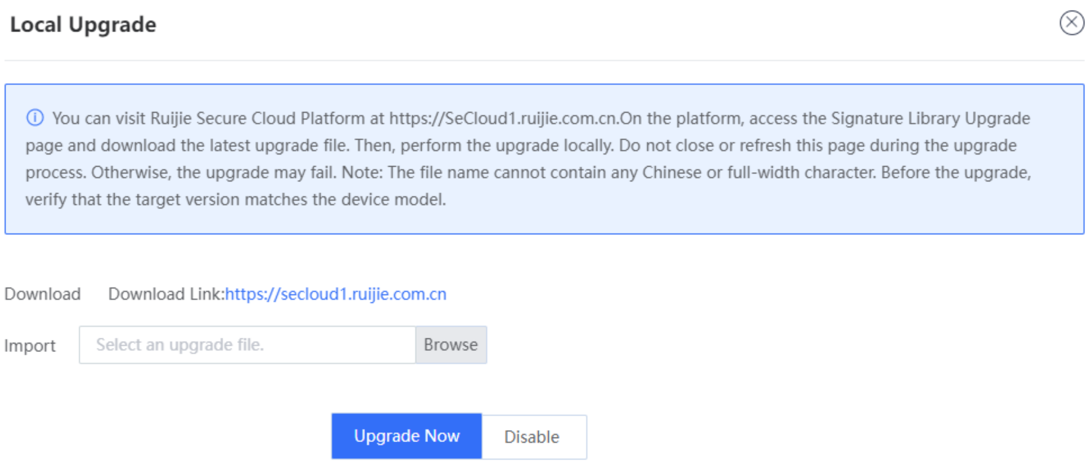
Current Version:20221202.1005

Last Upgrade Time:-

Latest Version:Unable to obtain the latest version.

Version State:-

b Upload the version file that is downloaded from the cloud platform and click **Upgrade Now**.



Local Upgrade

ⓘ You can visit Ruijie Secure Cloud Platform at https://SeCloud1.ruijie.com.cn.On the platform, access the Signature Library Upgrade page and download the latest upgrade file. Then, perform the upgrade locally. Do not close or refresh this page during the upgrade process. Otherwise, the upgrade may fail. Note: The file name cannot contain any Chinese or full-width character. Before the upgrade, verify that the target version matches the device model.

Download Download Link:https://secloud1.ruijie.com.cn

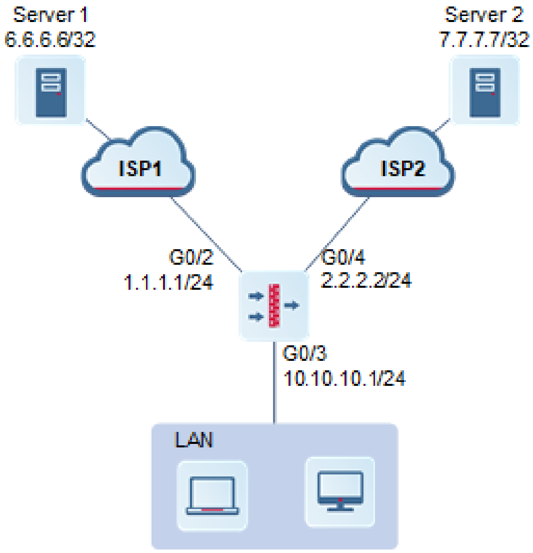
Import Select an upgrade file.

7.13.3 Configuring ISP Routing

Network Requirements

The firewall is deployed at the network egress as a security gateway. The enterprise leases a line from each of ISP 1 and ISP 2. The enterprise requires that packets accessing Server 1 be forwarded through ISP 1 link and packets accessing Server 2 be forwarded through ISP 2.

Network Topology



Configuration Points

(1) Complete basic network access settings.

(2) Configure ISP address library.

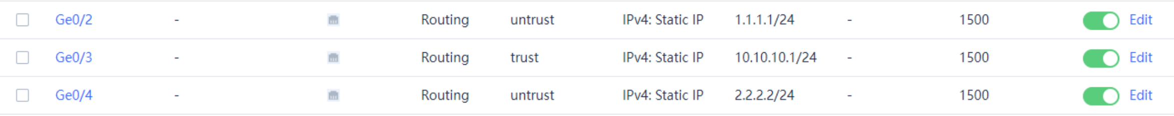
(3) Configure ISP routing (associating address library with interface).

(4) Configure the security policy.

Procedure

(1) Complete basic network access settings.

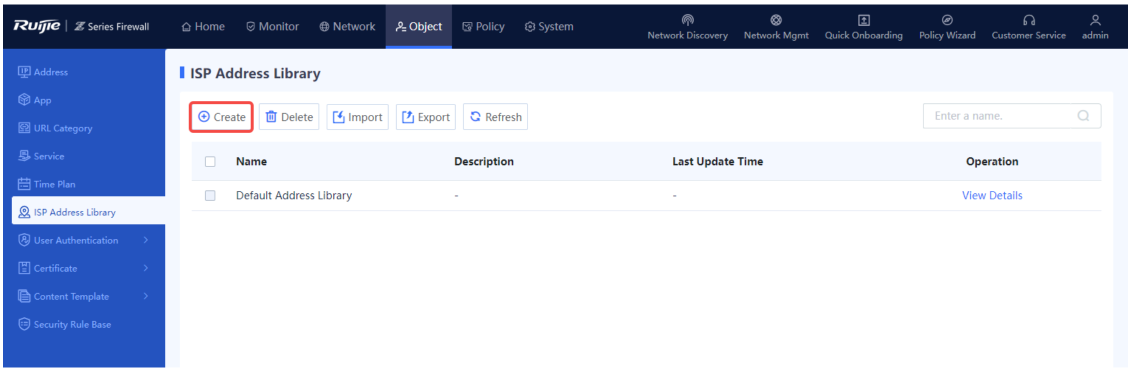
Configure the interface IP address, security zones, and gateway. For details, see 0 Routing Mode.



□	Ge0/2	-		Routing	untrust	IPv4: Static IP	1.1.1.1/24	-	1500	Edit
□	Ge0/3	-		Routing	trust	IPv4: Static IP	10.10.10.1/24	-	1500	Edit
□	Ge0/4	-		Routing	untrust	IPv4: Static IP	2.2.2.2/24	-	1500	Edit

(2) Configure ISP address library.

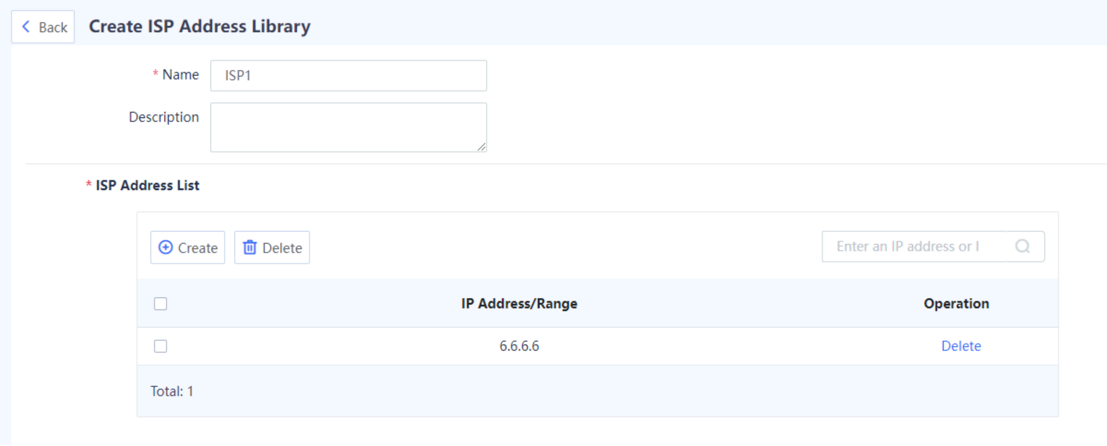
a Choose **Object** > **ISP Address Library** and click **Create**.



ISP Address Library

□	Name	Description	Last Update Time	Operation
□	Default Address Library	-	-	View Details

b Create address libraries of ISP 1 and ISP 2. Enter Server 1's IP address 6.6.6.6 for ISP1 and Server 2's IP address 7.7.7.7 for ISP 2.



Create ISP Address Library

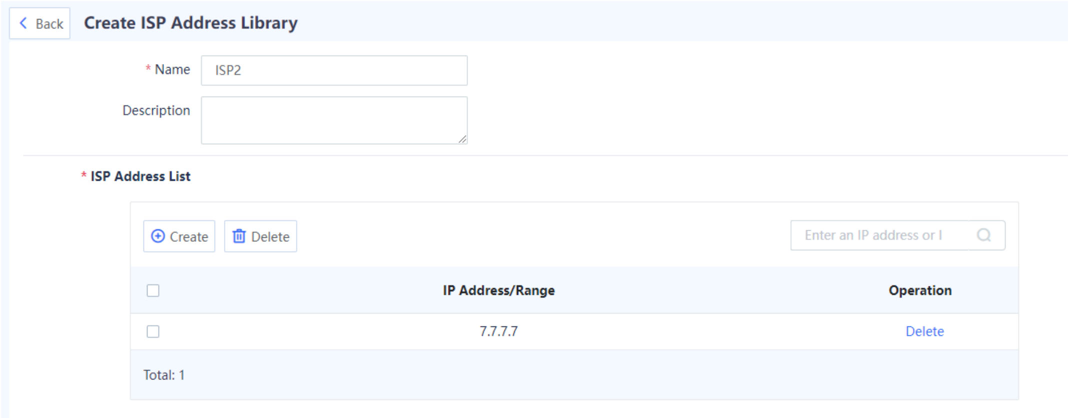
* Name: ISP1

Description:

* ISP Address List

□	IP Address/Range	Operation
□	6.6.6.6	Delete

Total: 1



< Back **Create ISP Address Library**

* Name: ISP2

Description:

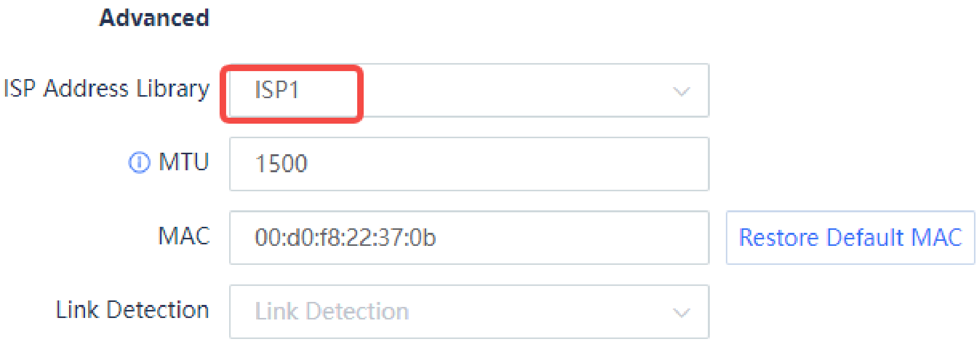
* **ISP Address List**

□	IP Address/Range	Operation
□	7.7.7.7	Delete

Total: 1

(3) Configure ISP routing (associating address library with interface).

a Choose **Network** > **Physical Interface**, find out the row where G0/2 is located, and click **Edit**. Set the ISP address library to **ISP1**.



Advanced

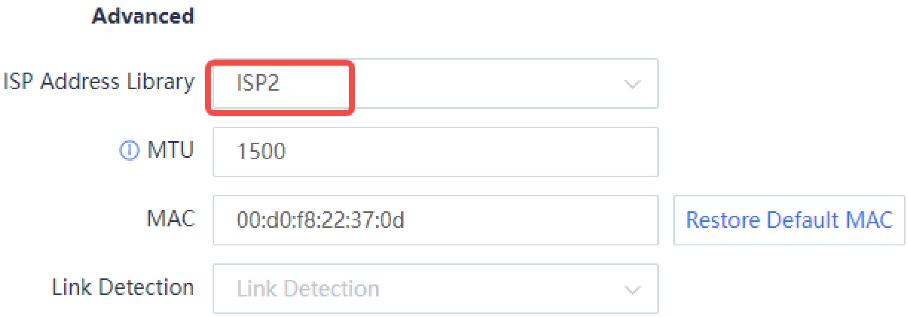
ISP Address Library: ISP1

MTU: 1500

MAC: 00:d0:f8:22:37:0b

Link Detection: Link Detection

b Choose **Network** > **Physical Interface**, find out the row where G0/4 is located, and click **Edit**. Set the ISP address library to **ISP2**.



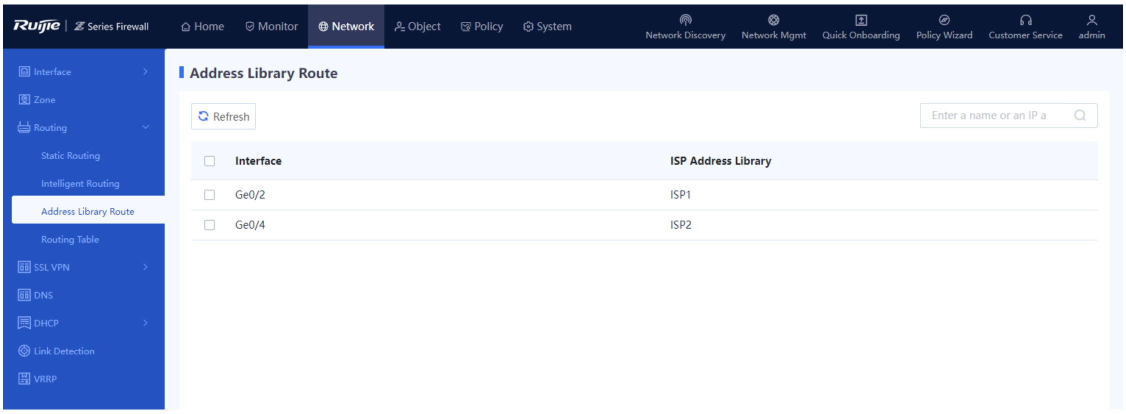
Advanced

ISP Address Library: ISP2

MTU: 1500

MAC: 00:d0:f8:22:37:0d

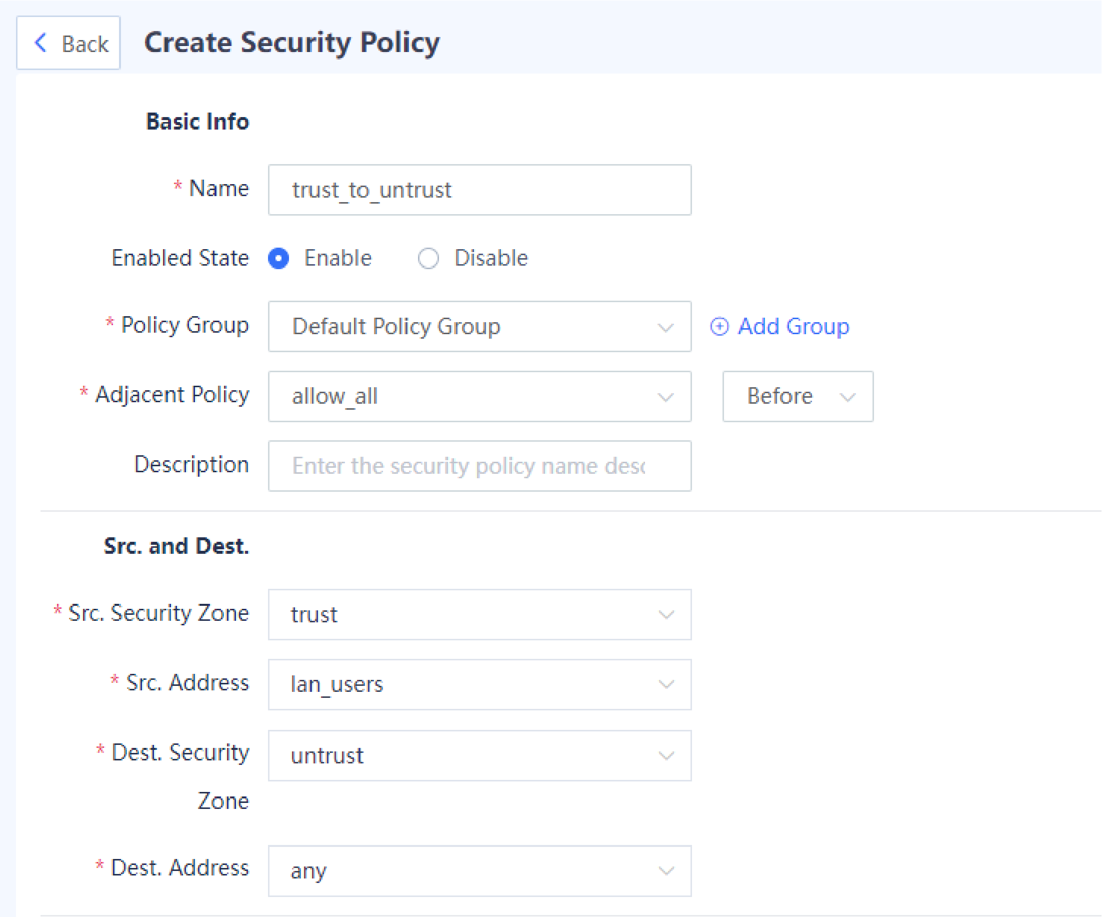
Link Detection: Link Detection



Address Library Route

□	Interface	ISP Address Library
□	Ge0/2	ISP1
□	Ge0/4	ISP2

(4) Configure the security policy: forward the traffic from Trust zone to Untrust zone.



Create Security Policy

Basic Info

* Name: trust_to_untrust

Enabled State: ● Enable ○ Disable

* Policy Group: Default Policy Group

* Adjacent Policy: allow_all Before

Description: Enter the security policy name desc

Src. and Dest.

* Src. Security Zone: trust

* Src. Address: lan_users

* Dest. Security Zone: untrust

* Dest. Address: any

7.13.4 Viewing the Routing Table of Address Library

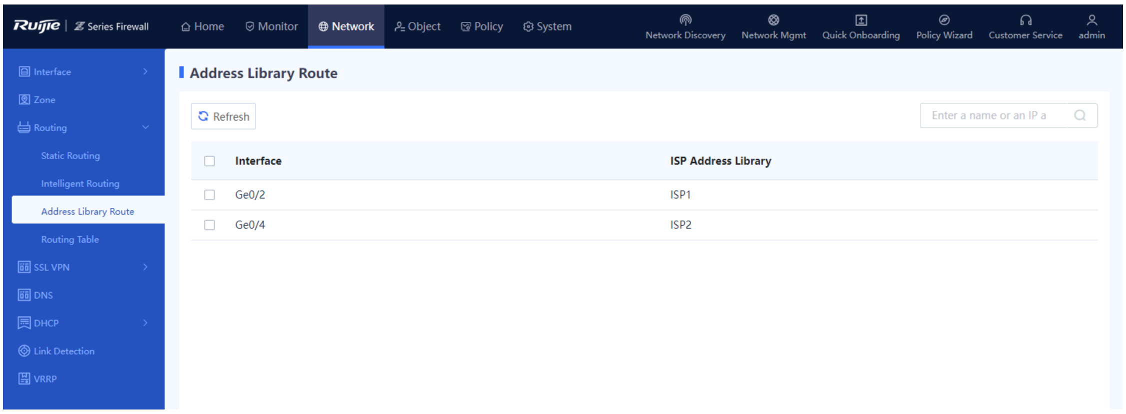
Application Scenario

The routes in address library are automatically generated after the ISP network to which the interface is connected is configured, and cannot be manually created. After an interface is associated with an ISP address set, routes are automatically generated in the address library, which are used for routing the packets. If the egress of a device is connected to multiple ISP networks, the packets destined for the specified ISP network can be forwarded through the specified outbound interface, avoiding inter-ISP access and improving traffic forwarding efficiency.

Procedure

(1) Choose **Network** > **Routing** > **Address Library Route**.

(2) View the address library routing entries on the firewall.



Address Library Route

□	Interface	ISP Address Library
□	Ge0/2	ISP1
□	Ge0/4	ISP2

7.14 Aggregate Interface

Application Scenario

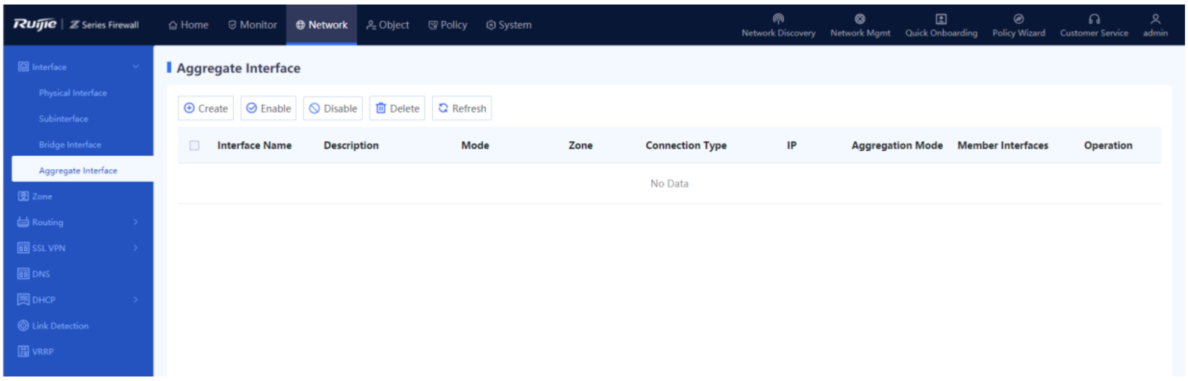
An aggregate interface binds multiple physical interfaces together to form a logical interface for link bandwidth expansion, which provides higher connection reliability.

An aggregate interface can increase link bandwidth and implement link redundancy backup.

- If the bandwidth of the link between two devices can reach 1,000 Mbps (assuming that the interface rate of both devices is 1,000 Mbps), when the service traffic carried on the link exceeds 1,000 Mbps, excess traffic is discarded. An aggregate interface can solve the problem of insufficient bandwidth in the following way: Use *n* network cables to connect two devices, and aggregate and bind these interfaces. In this way, these logically bound interfaces provide a maximum bandwidth of 1,000 Mbps x *n*.
- When two devices are connected by a single network cable, if the link is disconnected, the services carried on the link will be interrupted. However, when multiple connected interfaces are aggregated and bound, if one member link is disconnected, the device automatically distributes the traffic of the faulty link to other member links. As long as one link is working, the services carried on these interfaces will not be interrupted.

Procedure

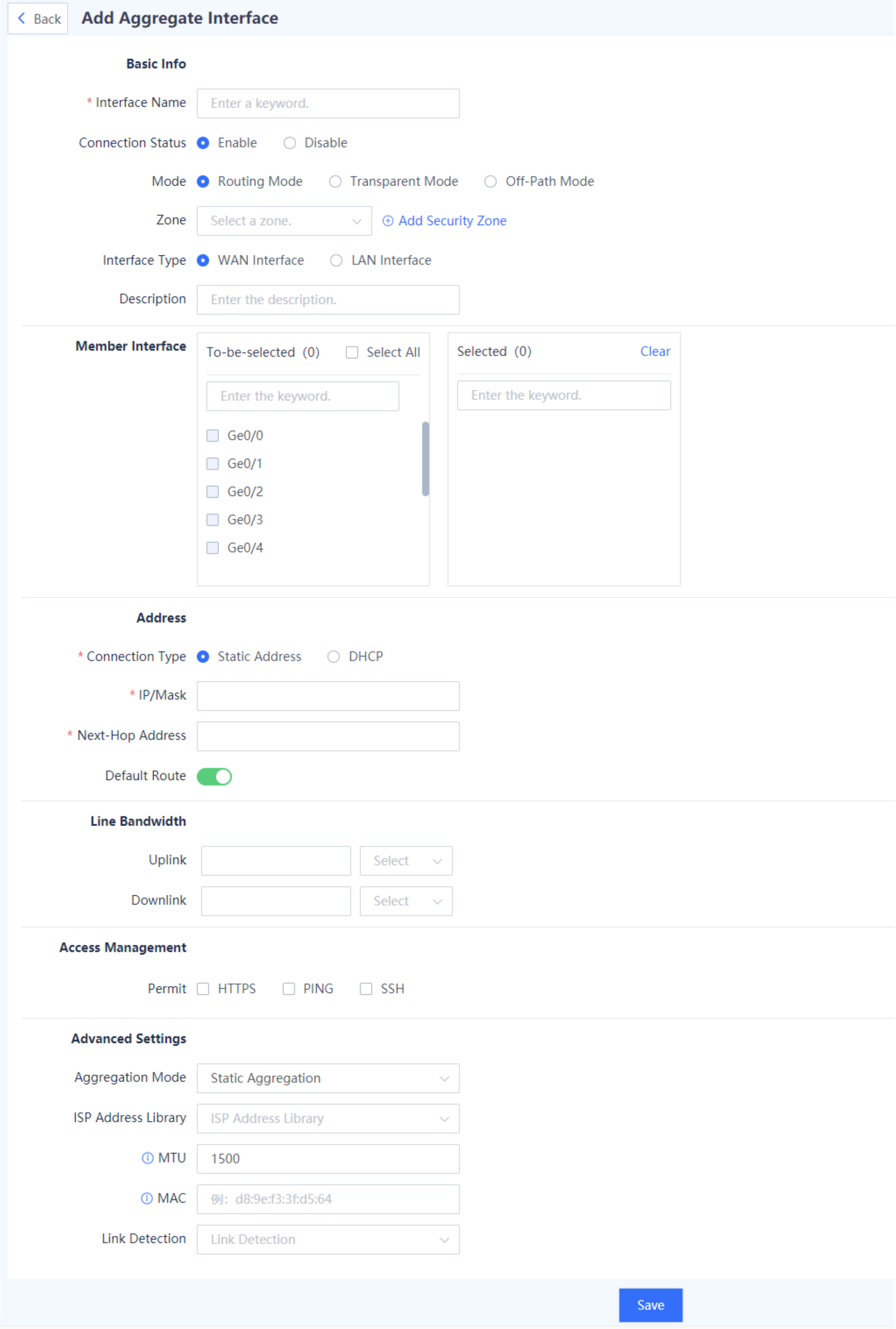
(1) Choose **Network** > **Interface** > **Aggregate Interface**.



□	Interface Name	Description	Mode	Zone	Connection Type	IP	Aggregation Mode	Member Interfaces	Operation
					No Data				

(2) Click **Create**.

The system opens the **Add Aggregate Interface** page.



< Back **Add Aggregate Interface**

Basic Info

* Interface Name: Enter a keyword.

Connection Status: ● Enable ○ Disable

Mode: ● Routing Mode ○ Transparent Mode ○ Off-Path Mode

Zone: Select a zone. ⊕ Add Security Zone

Interface Type: ● WAN Interface ○ LAN Interface

Description: Enter the description.

Member Interface

To-be-selected (0) □ Select All

Enter the keyword.

□ Ge0/0
□ Ge0/1
□ Ge0/2
□ Ge0/3
□ Ge0/4

Selected (0) Clear

Enter the keyword.

Address

* Connection Type: ● Static Address ○ DHCP

* IP/Mask:

* Next-Hop Address:

Default Route: ● (on)

Line Bandwidth

Uplink: Select

Downlink: Select

Access Management

Permit: □ HTTPS □ PING □ SSH

Advanced Settings

Aggregation Mode: Static Aggregation

ISP Address Library: ISP Address Library

ⓘ MTU: 1500

ⓘ MAC: 例：d8:9e:f3:3f:d5:64

Link Detection: Link Detection

Save

(3) Set parameters of aggregate interface.

Item	**Description**	**Remarks**
Interface Name	Name of the aggregate interface.	The interface name can contain only uppercase and lowercase letters and digits. [Example] Ag1
Connection Status	Enables or disables the interface.	[Example] Enable
Mode	Interface access mode. ● **Routing Mode**: forwards traffic based on IP addresses. ● **Transparent Mode**: forwards traffic based on MAC addresses. ● **Off-Path Mode**: only receives mirrored traffic, but does not forward traffic.	[Example] Routing Mode
Bridge Interface	Bridge group to which the interface belongs in transparent mode.	This parameter is available when the transparent mode is used. [Example] br0
Zone	Security zone to which the interface belongs.	[Example] trust
Interface Type	Logical attribute of the interface.	[Example] LAN Interface
Description	Interface description, showing the purpose of the interface.	Characters such as `~!#%^&*+\\|{};:'"/<>? are not

Item	Description	Remarks
		allowed. [Example] Expand egress bandwidth.
Member Interface	Physical interface that is added to the aggregate interface.	Up to 8 member interfaces can be included. [Example] Ge0/1
Connection Type	IP address obtaining method of the interface, including static and DHCP.	This parameter is available when the **Routing Mode** is used. [Example] Static Address
IP/Mask	IPv4 address and mask of the interface.	This parameter is available when **Connection Type** is set to **Static Address**. [Example] 192.168.1.1/24
Next-Hop Address	Next-hop address of the forwarded data. Generally, it is the address of the next routing device.	This parameter is available when **Connection Type** is set to **Static Address**. [Example] 192.168.1.2/24
Default Route	Whether to generate the default route.	[Example] Enabled
Line Bandwidth	Limited interface bandwidth, including upload bandwidth and download	Enter the bandwidth value and select a unit.

Item	Description	Remarks
	bandwidth.	The unit can be kbps or mbps. When kbps is selected as the unit, the value ranges from 1 to 100,000,000. When mbps is selected as the unit, the value ranges from 1 to 100,000. [Example] 100 kbps
Access Management	Whether the interface supports HTTPS, ping, and SSH.	The configuration takes effect when the interface mode is routing mode and local defense is enabled on the device. [Example] Select **HTTPS**.
Advanced Settings		
Aggregation Mode	For the manually configured aggregate interface, the aggregation mode is displayed as **Static Aggregation**.	Only the **Static Aggregation** is supported currently.
ISP Address Library	ISP network connected to the interface. The interface generates ISP routes based on the associated ISP address set, and the traffic with the destination addresses in different ISP networks is forwarded through the corresponding outbound interfaces.	This configuration takes effect only when the interface is configured as a WAN interface. [Example] CERNET
MTU	Maximum number of bytes in the packets sent on the interface. The	An integer ranging from 64 to 1600.

Item	Description	Remarks
	default MTU value is 1500, namely, forwarding data at the highest speed. If the upper-level device limits the packet size, causing a network interruption or delay, you can reduce the MTU to 1492, 1400, or a smaller value.	[Example] 1500
MAC	MAC address of the interface.	[Example] 30:0d:9e:41:d9:0b
Link Detection	Link detection policy associated with the local interface. This configuration can detect the network connectivity between the interface and the next hop in real time.	For details about link detection, see 7.15 Link Detection.

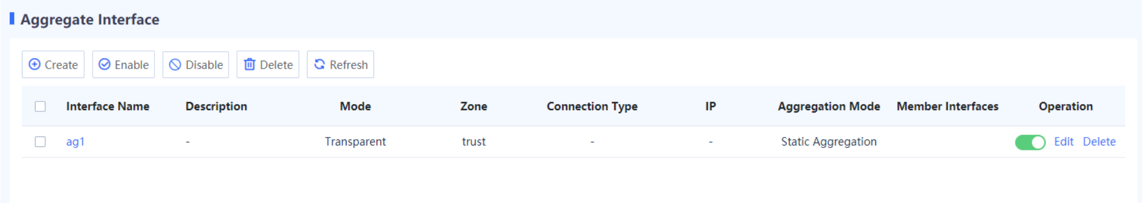
⚠ **Caution**

- A management port cannot be added to an aggregate interface.
- The interface bound to other functions (such as security zone and routing entries) cannot be added to an aggregate interface.
- A maximum of 8 aggregate interfaces can be created.

(4) Click **Save**.

Follow-up Procedure

- On the aggregate interface management page (choose **Network** > **Interface** > **Aggregate Interface**), you can modify or delete the aggregate interfaces.
- To enable or disable an aggregate interface, you can click ● .
- To process multiple aggregate interfaces in a batch, select the interface entries and click **Enable**, **Disable**, or **Delete**.



☐	Interface Name	Description	Mode	Zone	Connection Type	IP	Aggregation Mode	Member Interfaces	Operation
☐	ag1	-	Transparent	trust	-	-	Static Aggregation		Edit Delete

7.15 Link Detection

Application Scenario

Link detection checks the connectivity of network links. When it is associated with static routing and PBR, automatic route switching can be implemented. If link detection is not associated with PBR or static routing, the static routes and default routes on the interface will not be invalid even if the detection result is abnormal.

Note

This function is supported from NTOS1.0R3. If your version is lower than NTOS1.0R3, upgrade it to NTOS1.0R3 or higher.

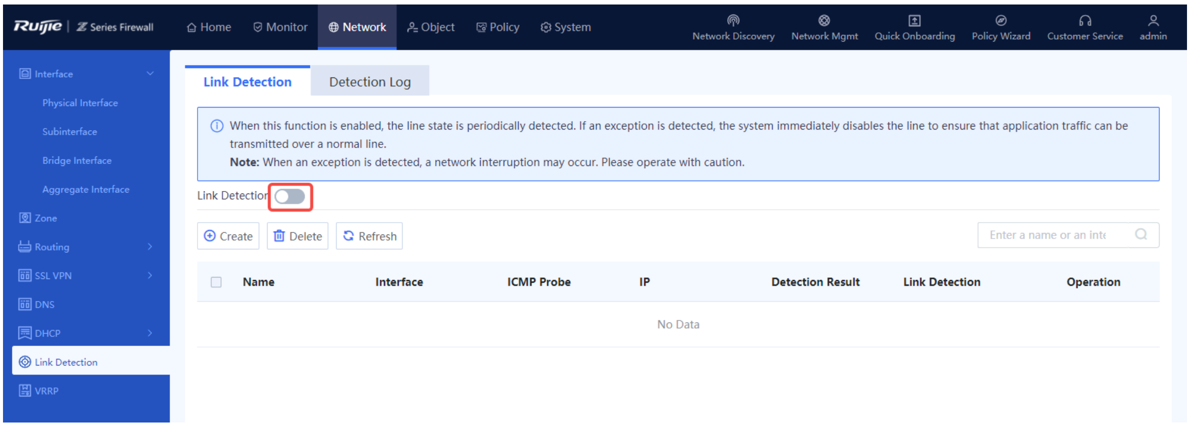
Procedure

(1) Choose **Network** > **Link Detection** > **Link Detection**.

(2) Click ○ to enable link detection.

Note

If a single detection policy is enabled but the link detection function is not enabled, the detection policy will not take effect and link detection will not be performed.

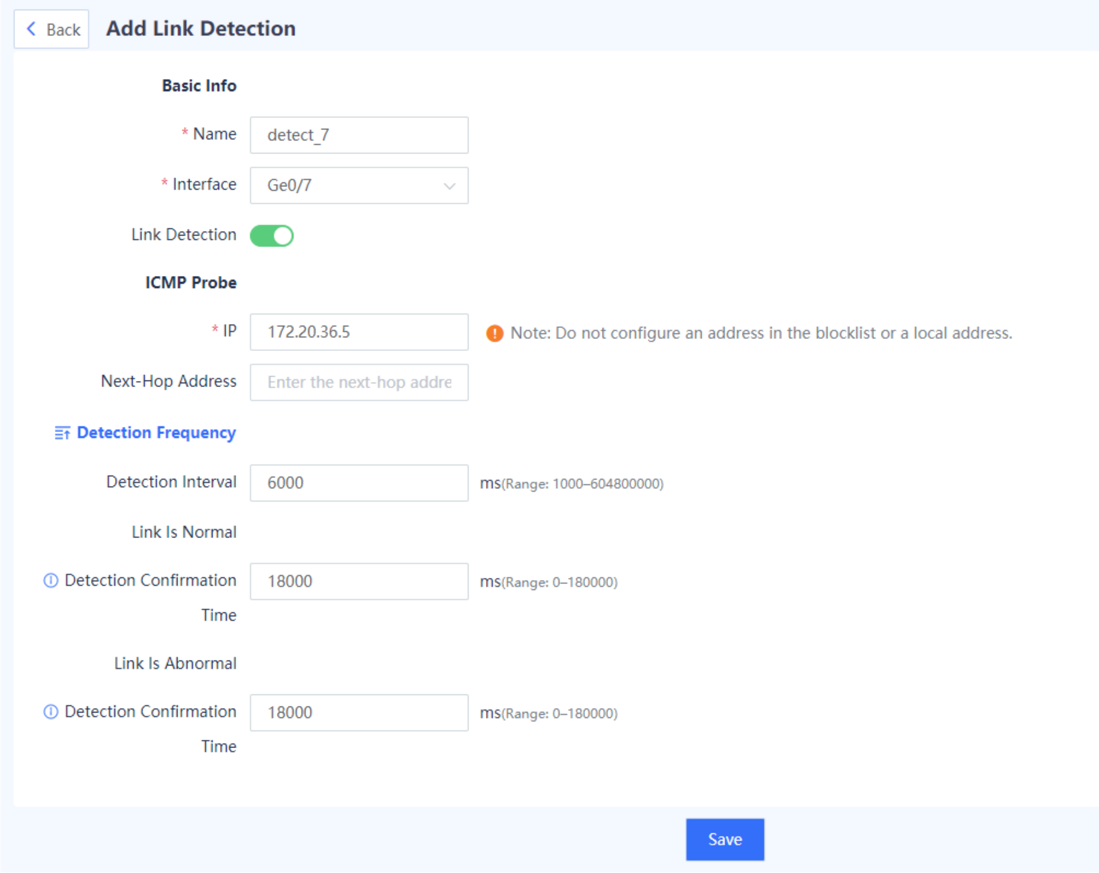


When this function is enabled, the line state is periodically detected. If an exception is detected, the system immediately disables the line to ensure that application traffic can be transmitted over a normal line.
Note: When an exception is detected, a network interruption may occur. Please operate with caution.

Link Detectior ○

☐	Name	Interface	ICMP Probe	IP	Detection Result	Link Detection	Operation
				No Data			

(3) Click **Create** to access the **Add Link Detection** page. Set the detection parameters.



< Back **Add Link Detection**

Basic Info

* Name: detect_7

* Interface: Ge0/7

Link Detection: ●

ICMP Probe

* IP: 172.20.36.5 Note: Do not configure an address in the blocklist or a local address.

Next-Hop Address: Enter the next-hop addre

Detection Frequency

Detection Interval: 6000 ms(Range: 1000–604800000)

Link Is Normal

Detection Confirmation Time: 18000 ms(Range: 0–180000)

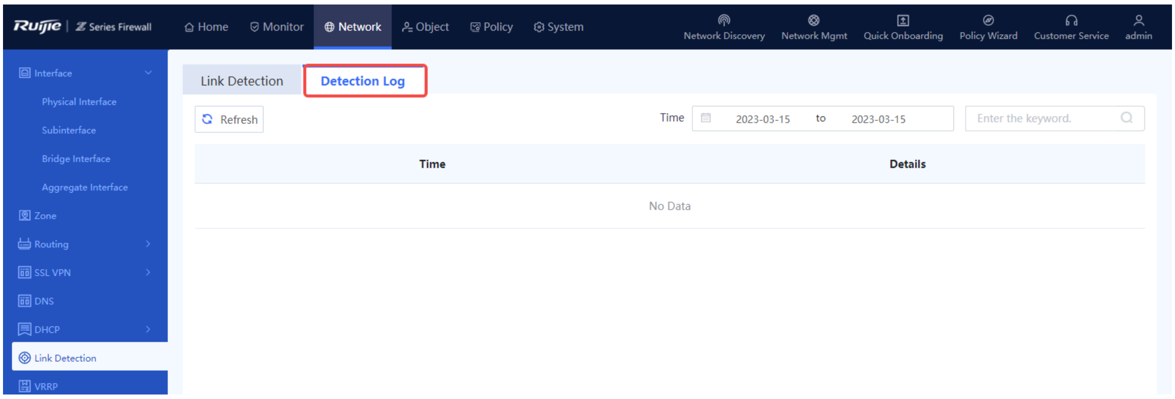
Link Is Abnormal

Detection Confirmation Time: 18000 ms(Range: 0–180000)

Save

(4) Click **Save**.

(5) After detection is completed, you can view the detection log on the **Detection Log** tab page.



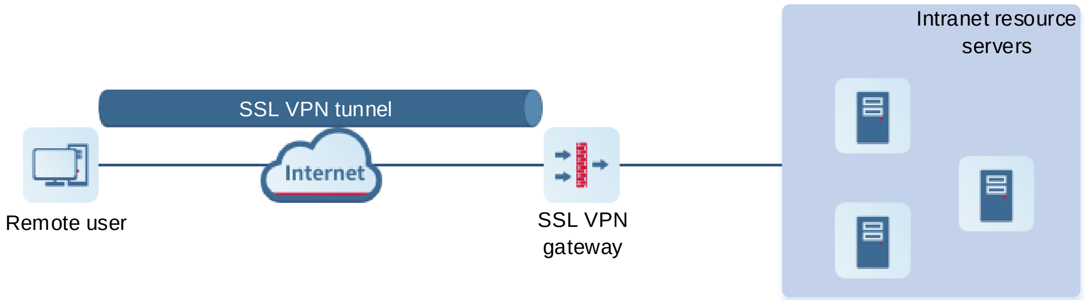
Time 2023-03-15 to 2023-03-15 Enter the keyword.

Time	Details
No Data	

7.16 SSL VPN

7.16.1 Overview

Secure Sockets Layer Virtual Private Network (SSL VPN) is an SSL-based remote access VPN technology, which uses a public network such as the Internet to establish an encrypted and secure remote access connection. In scenarios such as mobile office or remote office, customers and employees can securely access internal resources through an SSL VPN tunnel.



Principles of SSL VPN are as follows:

(1) Remote users initiate remote access requests to the SSL VPN gateway on the SSL VPN client.

(2) After receiving a request, the SSL VPN gateway authenticates the identity of the user (two authentication methods: username/password and username/password used together with hardware signature) and authorizes the user to access specific resources.

(3) Upon being authorized, the user sends a resource access request to the SSL VPN gateway.

(4) The SSL VPN gateway forwards the resource access request to the intranet resource server.

(5) The SSL VPN gateway receives the response from the intranet resource server and forwards it to the user.

The following table lists the default maximum numbers of concurrent users of the SSL VPN gateway supported by each model of the Z-S series firewall. After the maximum number of concurrent users is exceeded, new users can no longer log in to the SSL VPN gateway. You can increase the number of concurrent users by purchasing and activating SSL VPN licenses. (The number of concurrent users can be accumulated if you import multiple licenses).

Model	**Default Max. Concurrent Users**
RG-WALL 1600-Z3200-S	20

7.16.2 （Optional）Import Local Certificate

Application Scenario

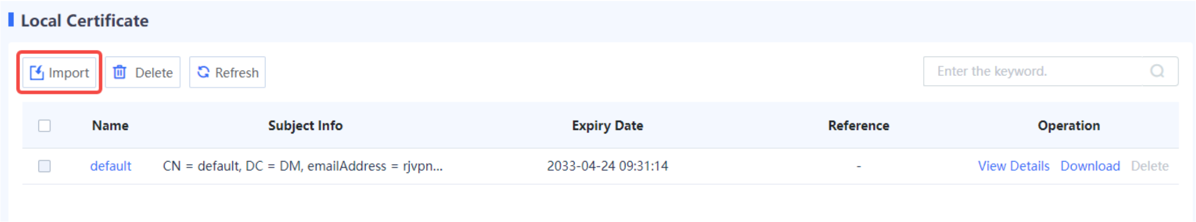
When a remote access user establishes an SSL connection with the SSL VPN gateway on the SSL VPN client, the gateway provides a local certificate to the peer end. In this way, the client can authenticate the SSL VPN gateway based on the digital certificate. If a non-CA certificate is provided, the client reports a certificate security alarm.

A firewall provides the default certificate **default**. You can import a new local certificate as required.

Procedure

(1) Choose **Object** > **Certificate** > **Local Certificate**.

(2) Click **Import**.

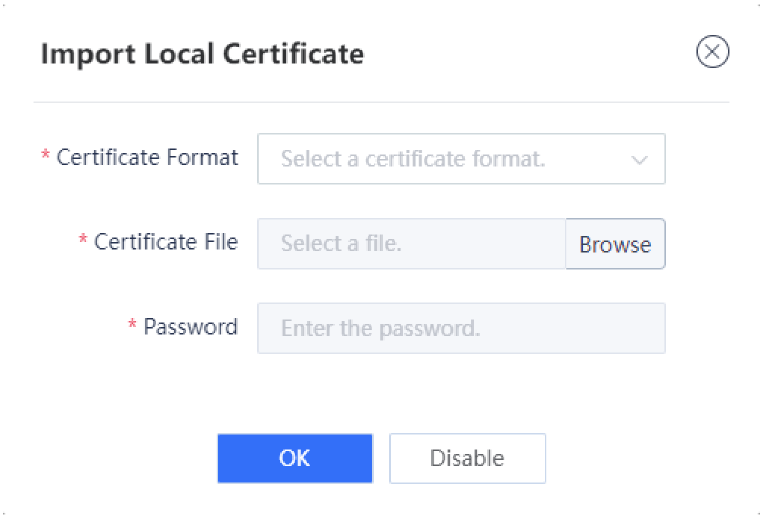


□	Name	Subject Info	Expiry Date	Reference	Operation
□	default	CN = default, DC = DM, emailAddress = rjvpn...	2033-04-24 09:31:14	-	View Details Download Delete

(3) Select a certificate format. Click **Browse** and select a certificate file. Then, enter the password, and click **OK**.

Note

Up to 20 local certificates are supported.



Follow-up Procedure

- Click **Download** to download the corresponding certificate in .pem format.
- After certificate import, you can reference the local certificate when creating the virtual gateway.
- Click **View Details** to view details about the certificate.
- To delete a newly imported certificate, click **Delete**. The default certificate cannot be deleted.
- You can enter the certificate name in the search box in the upper right corner of the page to search for a certificate.

7.16.3 Creating an SSL VPN Gateway

Application Scenario

After you create an SSL VPN gateway on the firewall, the firewall provides the SSL VPN access service to remote users through the gateway.

The firewall supports multiple SSL VPN gateways that are independent of each other. Users and resources can be separately configured and managed for different SSL VPN gateways, which meets the remote access requirements of different service departments.

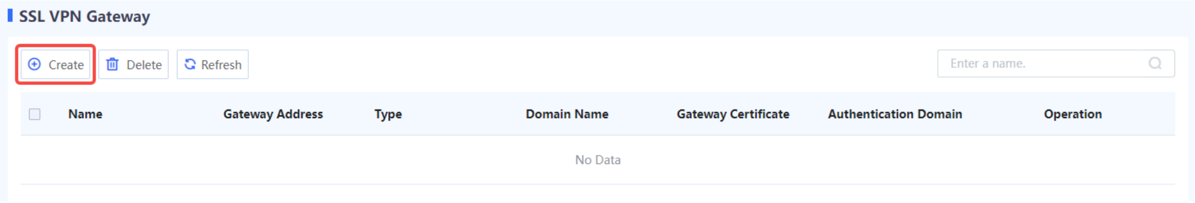
Precautions

- A user cannot log in to the same SSL VPN gateway from multiple locations at the same time. However, if the user has licenses on multiple SSL VPN gateways, the user can log in to the gateways at the same time.
- Disabling, deleting, or modifying the configuration of an SSL VPN gateway can force users to go offline. Therefore, perform these operations with caution.

Procedure

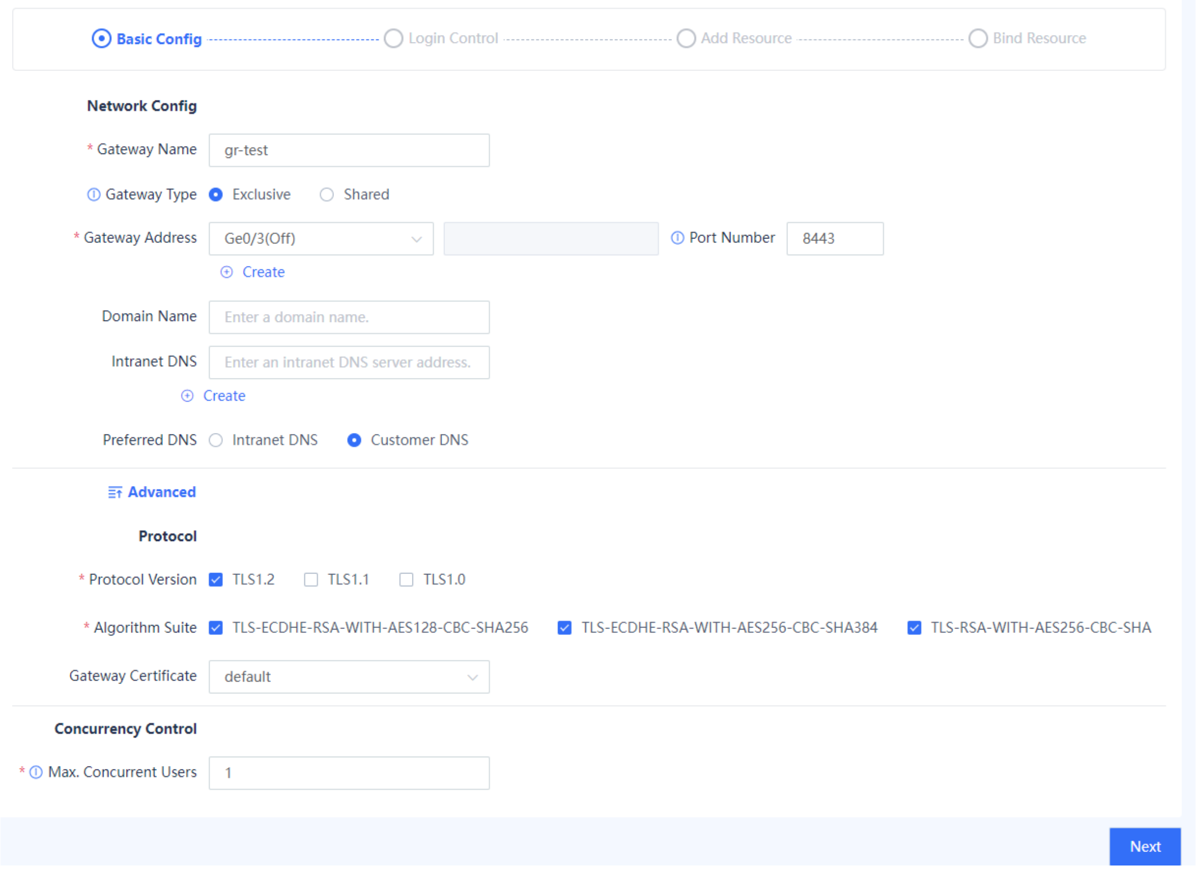
(1) Choose **Network** > **SSL VPN** > **SSL VPN Gateway**.

(2) Click **Create** to access the **Add SSL VPN Gateway** page.



□	Name	Gateway Address	Type	Domain Name	Gateway Certificate	Authentication Domain	Operation
				No Data			

(3) Configure basic information of an SSL VPN gateway.



● Basic Config ---- ○ Login Control ---- ○ Add Resource ---- ○ Bind Resource

Network Config

* Gateway Name: gr-test

ⓘ Gateway Type: ● Exclusive ○ Shared

* Gateway Address: Ge0/3(Off) ⓘ Port Number: 8443

⊕ Create

Domain Name: Enter a domain name.

Intranet DNS: Enter an intranet DNS server address.

⊕ Create

Preferred DNS: ○ Intranet DNS ● Customer DNS

Advanced

Protocol

* Protocol Version: ☑ TLS1.2 □ TLS1.1 □ TLS1.0

* Algorithm Suite: ☑ TLS-ECDHE-RSA-WITH-AES128-CBC-SHA256 ☑ TLS-ECDHE-RSA-WITH-AES256-CBC-SHA384 ☑ TLS-RSA-WITH-AES256-CBC-SHA

Gateway Certificate: default

Concurrency Control

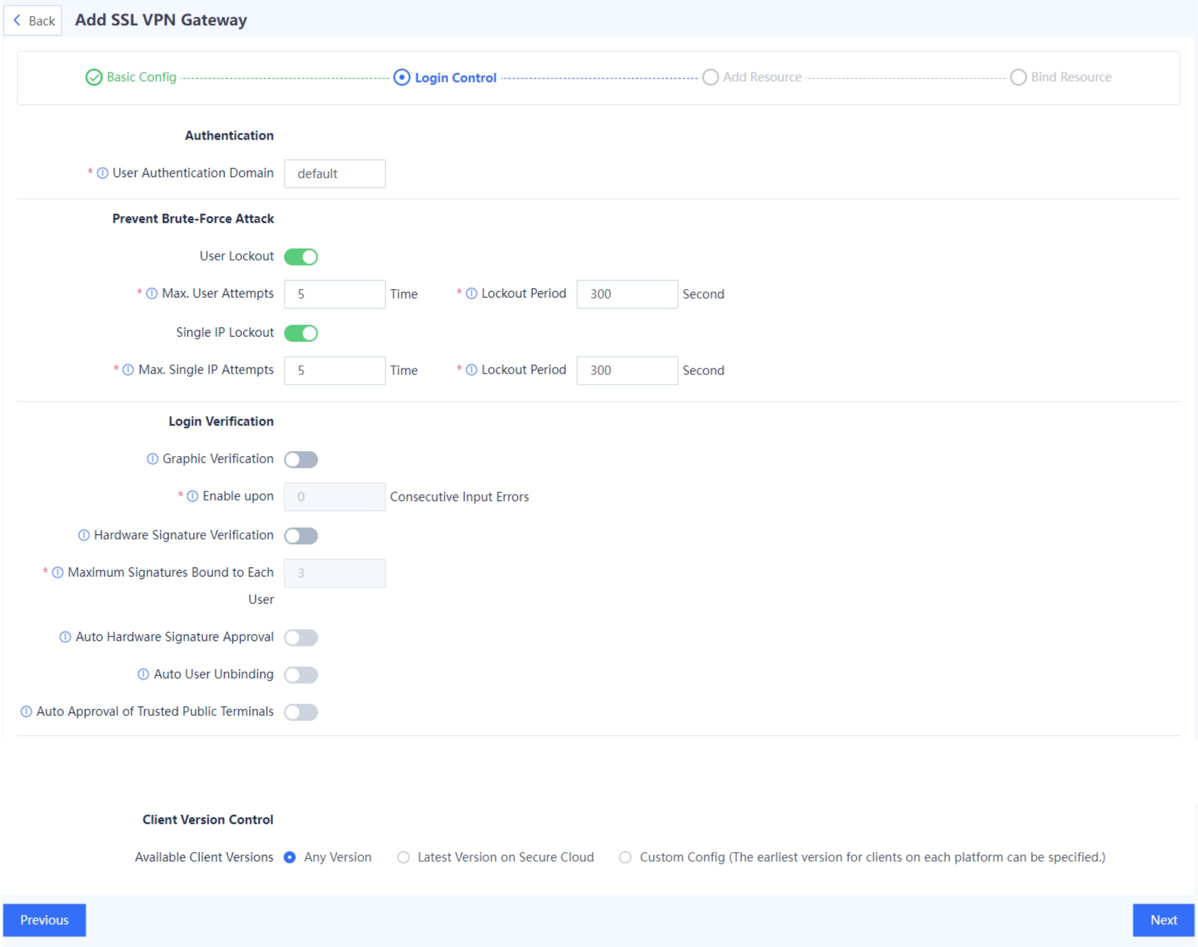
* ⓘ Max. Concurrent Users: 1

Item	Description	Remarks
Network Config		
Gateway Name	Name of the SSL VPN gateway.	[Example] gateway1
Gateway Type	● **Exclusive**: The system allocates a unique IP address and domain name to the virtual gateway, and users can log in to the SSL VPN gateway by using the IP address (or domain name) and port number. ● **Shared**: The system allocates a shared IP address and domain name to the virtual gateway, and users can log in to the SSL VPN gateway by using the domain name and port number.	[Example] Shared
Gateway Address	Address for accessing the SSL VPN gateway. You can choose an interface address or configure it manually. A	[Example] 1.1.1.1

Item	Description	Remarks
	gateway can be configured with a maximum of three addresses, each of which can be used for login.	
Port Number	Port on the virtual gateway that provides the SSL VPN service.	[Example] 8443
Domain Name	Domain name of the SSL VPN gateway. A domain name must be configured for a shared gateway. Multiple domain names can be configured to share the same gateway address and port number.	[Example] www.abc.com
Intranet DNS	IP address of the DNS server used to resolve internal domain names. You must configure this parameter when internal domain resources exist.	[Example] 192.168.0.1
Preferred DNS	Preferred DNS server used when internal network resources are accessed. You can specify the DNS server to be preferentially used for domain name resolution. If a domain name cannot be resolved, the DNS server of the client is used.	[Example] Intranet DNS
Advanced		
Protocol Version	Version of the SSL protocol used when an SSL connection is established between the SSL VPN gateway and client. The protocol version used by both ends must be the same.	[Example] TSL1.2
Algorithm Suite	Encryption algorithm used when an SSL connection is established between the SSL VPN gateway and client. The encryption algorithm used by both ends must be the same.	N/A
Gateway Certificate	Certificate used when an SSL connection is established between the SSL VPN gateway and client. The client verifies whether the SSL VPN gateway can be trusted using the certificate. For details on how to import the certificate, see 7.16.2	N/A

Item	Description	Remarks
	[（Optional）Import Local Certificate].	
Concurrency Control		
Max. Concurrent Users	Maximum number of users that can concurrently log in to the SSL VPN gateway. When the maximum number of concurrent users is reached, new users cannot log in to the SSL VPN gateway.	[Example] 20

(4) Verify the configuration and click **Next** to configure the login control parameters.



Authentication

* User Authentication Domain: default

Prevent Brute-Force Attack

User Lockout: On

* Max. User Attempts: 5 Time * Lockout Period: 300 Second

Single IP Lockout: On

* Max. Single IP Attempts: 5 Time * Lockout Period: 300 Second

Login Verification

Graphic Verification: Off

* Enable upon: 0 Consecutive Input Errors

Hardware Signature Verification: Off

* Maximum Signatures Bound to Each User: 3

Auto Hardware Signature Approval: Off

Auto User Unbinding: Off

Auto Approval of Trusted Public Terminals: Off

Client Version Control

Available Client Versions: ● Any Version ○ Latest Version on Secure Cloud ○ Custom Config (The earliest version for clients on each platform can be specified.)

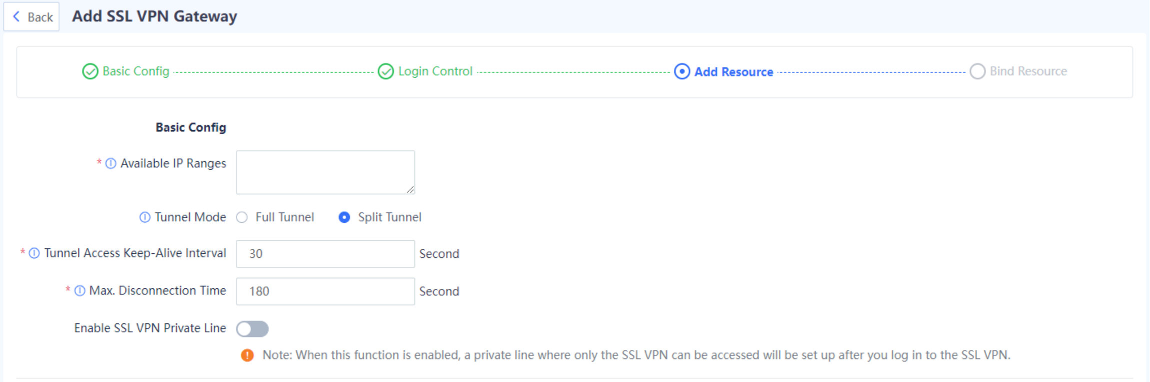
Item	Description	Remarks
Authentication		
User Authentication Domain	Authentication domain for which the login control policies configured on this page will be applied. An SSL VPN gateway can be bound to only one authentication domain.	[Example] default
Prevent Brute-Force Attack		
User Lockout	Specifies whether to enable user lockout after a certain number of consecutive failed login attempts. During the lockout period, the user cannot log in to the gateway.	[Example] Enable
Max. User Attempts	Maximum number of consecutive login failures that a user is allowed before being locked out.	[Example] 5
Lockout Period	Lockout period during which the user cannot log in to the gateway.	[Example] 300 seconds
Single IP Lockout	Specifies whether to enable locking out of a specific IP address on which a certain number of consecutive login failures are detected. During the lockout period, the user cannot log in to the gateway from this IP address.	[Example] Enable
Max. Single IP Attempts	Maximum number of consecutive login failures that are allowed from a specific IP address before it is locked out.	[Example] 5
Lockout Period	Lockout period during which the user cannot log in to the gateway from the locked IP address.	[Example] 300 seconds
Login Verification		
Graphic Verification	Specifies whether to display a graphic verification code on the gateway login page after a certain number of consecutive login failures. This function can prevent	[Example] Enable

Item	Description	Remarks
	brute-force attacks.	
Hardware Signature Verification	Specifies whether to verify the hardware signature of the device being used to log in to the gateway. The hardware signature can be manually or automatically approved. Only login requests from approved devices are allowed. You can also set the maximum number of devices a user can use to log in. Note: Hardware signature verification only takes effect for client-based logins, but does not take effect for web-based logins.	[Example] Enable
Auto Hardware Signature Approval	Specifies whether to enable automatic approval of hardware signatures for devices attempting to log in to the gateway.	[Example] Disable
Auto Unbinding	Specifies whether to allow users to unbind the hardware signatures from their accounts. If unbinding is performed when hardware signature verification is enabled, the hardware signature of the device needs to be approved again before the user logs in. For more information about how to manage hardware signatures, see 7.16.4 Hardware Signature Management.	[Example] Disable
Auto Approval of Trusted Public Terminals	Specifies whether to enable automatic approval of the trusted device whose hardware signature is imported to the firewall. Users associated with this hardware signature can log in to the gateway without manual approval.	N/A
Idle Timeout		
The idle status will time out after	Maximum duration during which an SSL VPN session remains idle before it is forcibly terminated.	[Example] 30 minutes
Client Version Control		

Item	Description	Remarks
Available Client Versions	Version of the SSL VPN client that connects to the SSL VPN gateway. Currently, only Ruijie SSL VPN client is supported. ● **Any Version**: no limit on the version of the SSL VPN client ● **Latest Version on Secure Cloud**: the latest version released on Ruijie Secure Cloud Platform ● Custom Config (The earliest version for clients on each platform can be specified.): custom client versions for each type of system	[Example] Any Version

(5) Verify the configuration and click **Next** to configure resource information.

a Configure basic information:



Add SSL VPN Gateway

Basic Config

* Available IP Ranges:

Tunnel Mode: ○ Full Tunnel ● Split Tunnel

* Tunnel Access Keep-Alive Interval: 30 Second

* Max. Disconnection Time: 180 Second

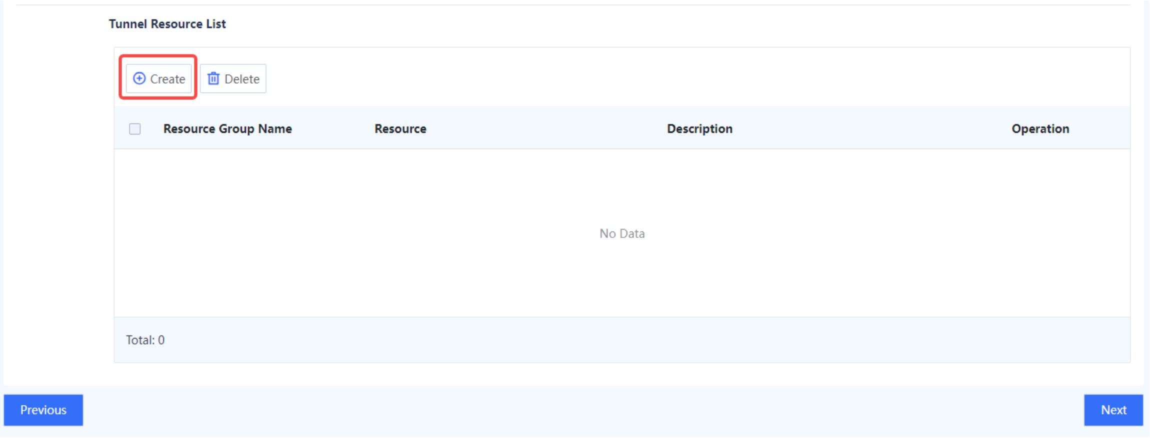
Enable SSL VPN Private Line

Note: When this function is enabled, a private line where only the SSL VPN can be accessed will be set up after you log in to the SSL VPN.

Item	Description	Remarks
Available IP Ranges	IP address range allocated to the client. The client uses the assigned IP address to establish a tunnel with the SSL VPN gateway. Once the available IP addresses are exhausted, new users cannot log in, and the IP address is released after the user logs out.	[Example] 1.1.1.1/255.255.255.0
Tunnel Mode	Supports two modes:	[Example]

Item	Description	Remarks
	● **Split Tunnel**: Only the traffic to authorized resources is sent through the SSL VPN tunnel. ● **Full Tunnel**: All user traffic, including traffic for Internet access and local communications, is sent through the SSL VPN tunnel.	Split Tunnel
Tunnel Access Keep-Alive Interval	Interval at which the SSL VPN client sends keep-alive messages to the SSL VPN gateway.	[Example] 30 seconds
Max. Disconnection Time	Maximum disconnection time. If the SSL VPN client fails to send a keep-alive message to the SSL VPN gateway within the maximum disconnection time, the SSL VPN gateway closes the tunnel, and the user is forced to go offline. The maximum disconnection time should be at least three times the tunnel access keep-alive interval.	[Example] 180 seconds
SSL VPN Private Line	If this function is enabled, users can only access the addresses in the tunnel resource group list after logging in to the SSL VPN gateway. Other resources cannot be accessed.	[Example] Disable

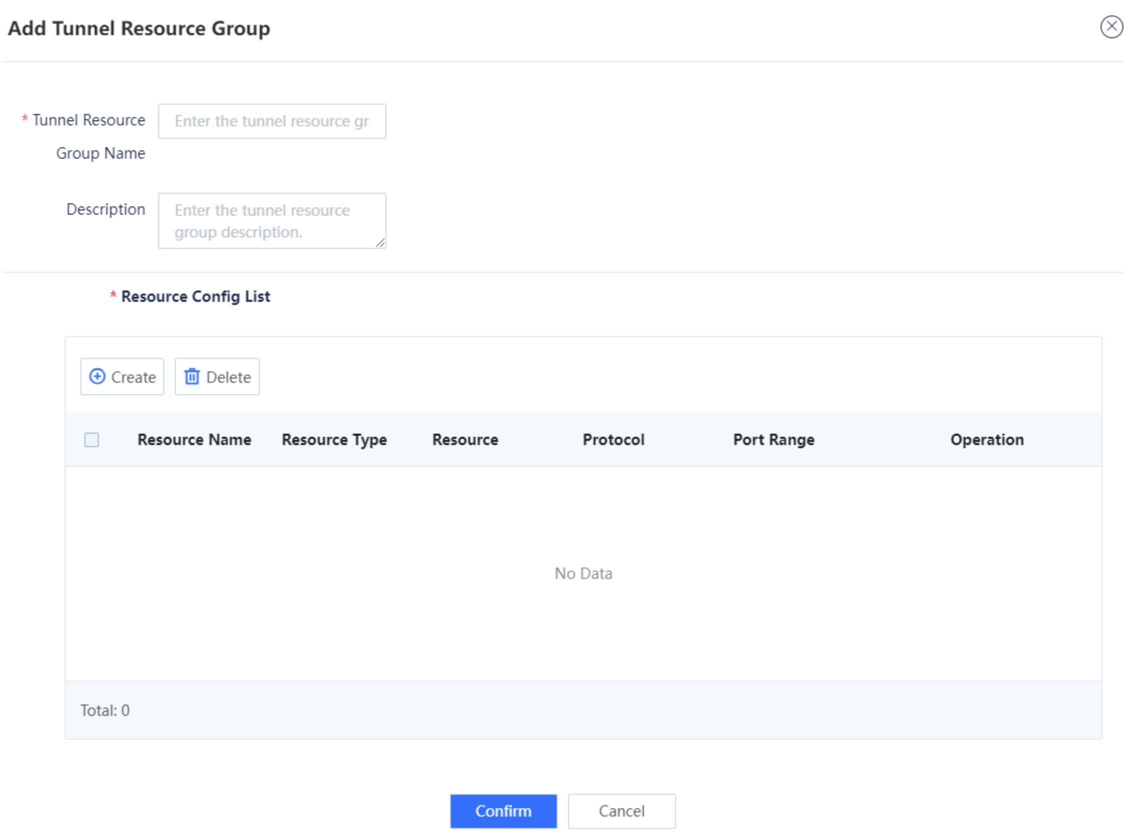
b If you set **Tunnel Mode** to **Split Tunnel**, you need to create a tunnel resource group. Click **Create** to configure the information of resources that can be accessed through this tunnel.


Tunnel Resource List

□	Resource Group Name	Resource	Description	Operation

No Data

Total: 0



Add Tunnel Resource Group

* Tunnel Resource Group Name: Enter the tunnel resource gr

Description: Enter the tunnel resource group description.

* Resource Config List

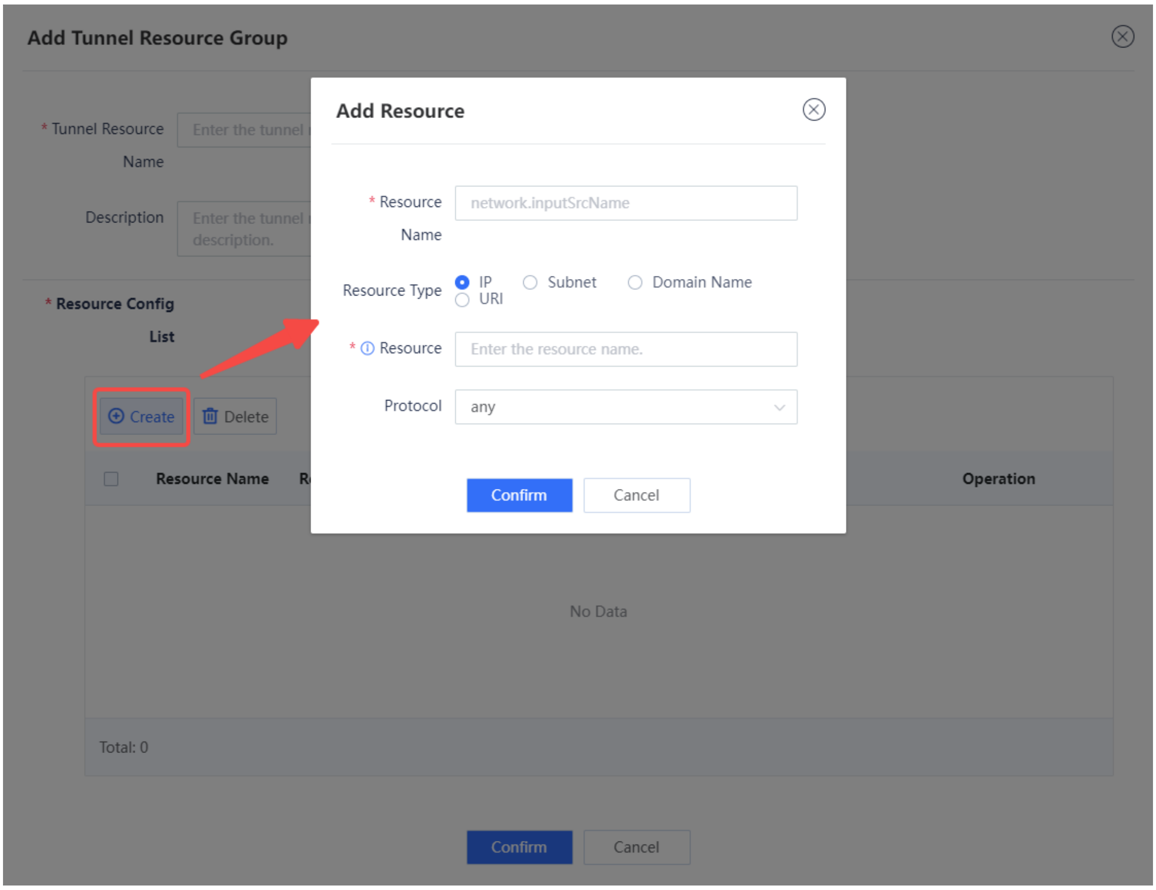
□	Resource Name	Resource Type	Resource	Protocol	Port Range	Operation

No Data

Total: 0

Item	Description	Remarks
Tunnel Resource Name	Name of the resource that can be accessed through this tunnel.	[Example] IP
Description	Tunnel resource description. Proper description helps the administrator quickly understand the function of the resource.	N/A

c In the **Tunnel Resource List** area, click **Create** to configure the information of the resources in the resource group.



Add Tunnel Resource Group

* Tunnel Resource Name: Enter the tunnel

Description: Enter the tunnel description.

* Resource Config List

Add Resource

* Resource Name: network.inputSrcName

Resource Type: ● IP ○ Subnet ○ Domain Name ○ URI

* Resource: Enter the resource name.

Protocol: any

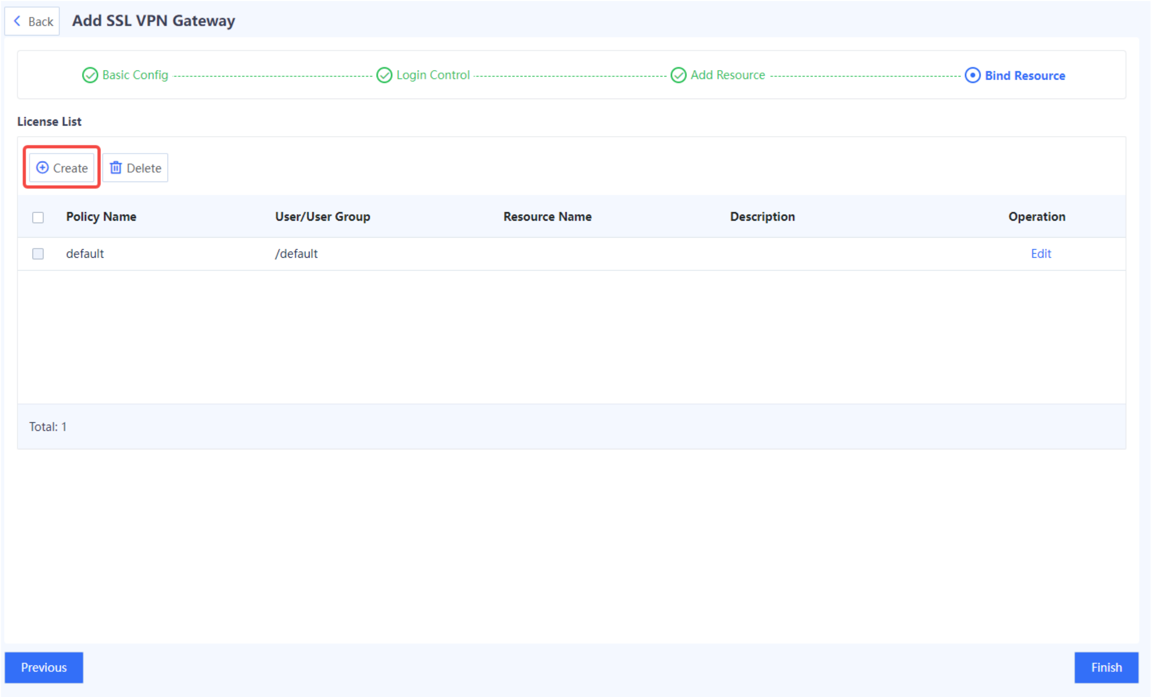
Item	Description	Remarks
Resource Name	Name of the resource that can be access through this tunnel.	[Example] IP
Resource Type	Supported resource types are as follows: ● **IP**: Only a single IP address is supported. Example: 192.168. 1.1. ● **Subnet**: IP/Mask length. Example: 192.168.1.0/24. ● **Domain Name**: Domain name. Example: www.abc.com. ● **URI**: URI. Example: <proto://ip[:port]>.	N/A
Resource	Resource to be entered based on the selected resource type. For example, enter an	N/A

Item	Description	Remarks
	IP address if **Resource Type** is set to **IP**.	
Protocol	Network protocol that specified resources use for authorized users to access. For example, if **Resource Type** is set to **IP** and this parameter is set to **any**, the user can access all external services provided at the IP address. If this parameter is set to **TCP**, the user can only access TCP-based external services provided at the IP address.	[Example] TCP

d Verify the configuration and click **Confirm** to return to the **Add Tunnel Resource Group** page.

(6) Verify the configured resource information, and click **Next** to configure the authorization policy for the resources that the user can access.

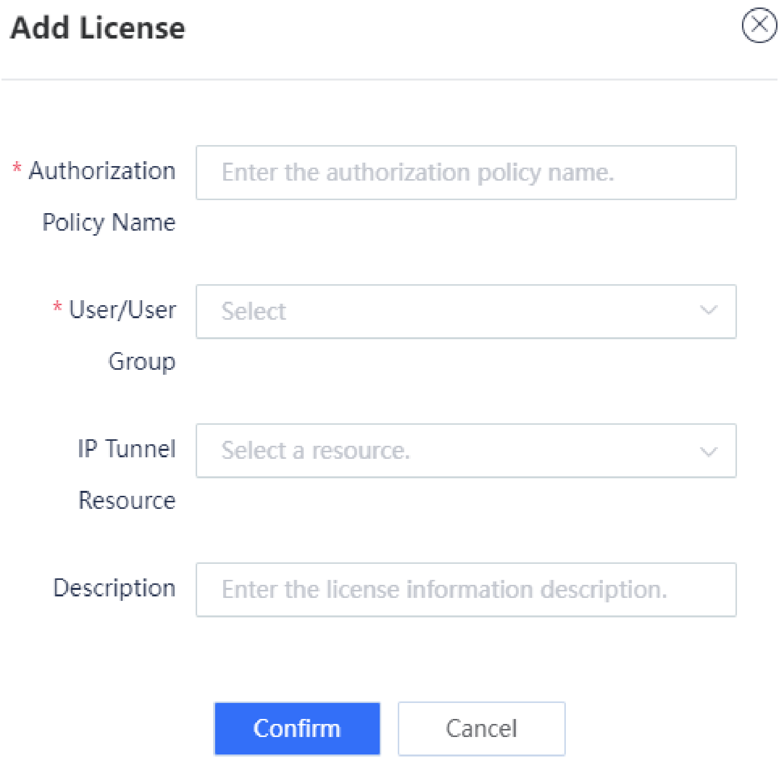
a Click **Create** to add an authorization policy, or click **Edit** in the **Operation** column to modify the existing policy.



☐	Policy Name	User/User Group	Resource Name	Description	Operation
☐	default	/default			Edit

Total: 1

b Configure parameters of an authorization policy.


Add License
* Authorization Policy Name
Enter the authorization policy name.
* User/User Group
Select
IP Tunnel Resource
Select a resource.
Description
Enter the license information description.
Confirm
Cancel

Item	Description	Remarks
Authorization Policy Name	Name of an authorization policy.	[Example] Policy_1
User/User Group	User or user group to be authorized.	[Example] User Group_1
IP Tunnel Resource	Resource group that the user or user group can access.	[Example] Resource Group_1
Description	Description of the authorization policy. A proper description helps the administrator quickly understand the function of the policy.	N/A

c Click **Confirm**.

(7) Verify the configuration and click **Finish**.

Follow-up Procedure

- After you add an SSL VPN gateway, a security policy is automatically generated to allow traffic to the SSL VPN gateway. The security policy is displayed at the top of the **Security Policy** page. To go to this page, choose **Policy**. If a network connectivity issue occurs, check whether the configuration of the security policy is valid.
- Based on the parameters configured in the basic configuration and login control steps, check whether the SSL VPN client information, such as the client version and protocol version, meets the requirements. Otherwise, authentication may fail.

7.16.4 Hardware Signature Management

Application Scenario

You can enable the hardware signature verification function, and bind hardware signatures with users. This limits the number of devices that can access the SSL VPN gateway and helps prevent unauthorized access and misuse of accounts.

Administrators can manually or automatically approve the hardware signatures of user devices that request access to the gateway. Only approved devices are allowed to access internal resources through the gateway.

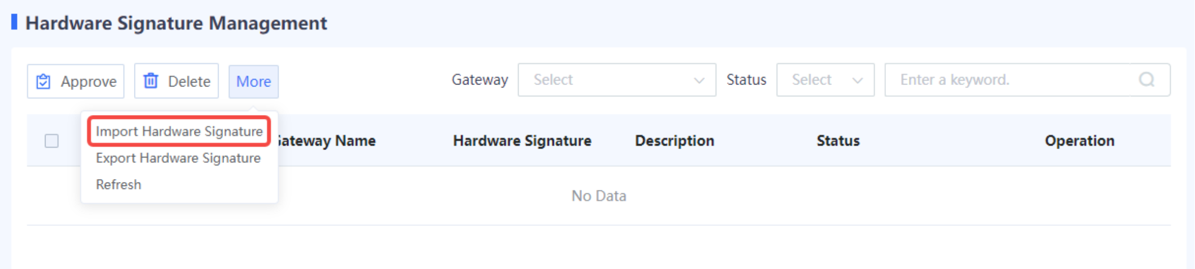
Precautions

- If the hardware signature verification and automatic approval functions are enabled when you create an SSL VPN gateway, devices with unapproved hardware signatures on this page can still log in to the gateway. After login, the device signature information will be imported and displayed on the **Hardware Signature Management** page and marked as approved.
- If you enable the hardware signature verification function but disable the automatic approval function when you create an SSL VPN gateway, the administrator needs to manually approve the devices on this page. Otherwise, the users associated with these hardware signatures cannot log in to the gateway.

Procedure

(1) Choose **Network**. > **SSL VPN** > **Hardware Signature Management**.

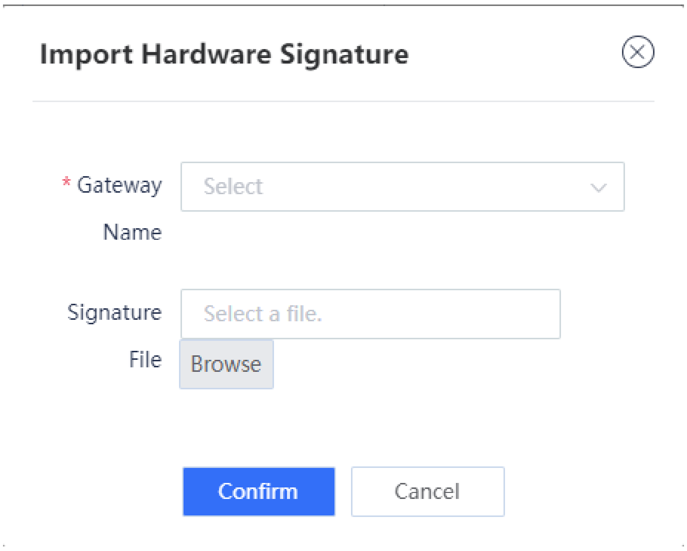
(2) Click **More** and select **Import Hardware Signature**.



(3) Select the gateway to which the hardware signature is imported. Click **Browse** to select the hardware signature file and upload it.

Note

The format of the hardware signature file is .data. To import hardware signatures in batches, contact a technical engineer for help.

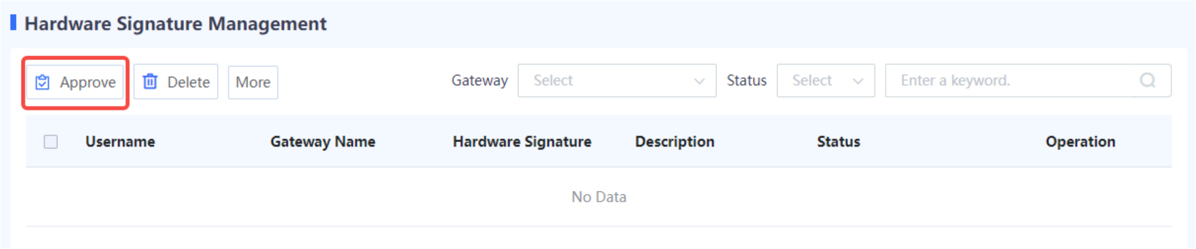


Import Hardware Signature

* Gateway Name: Select

Signature File: Select a file.

(4) Select multiple hardware signature entries in the list and click **Approve** to approve hardware signatures in batches.

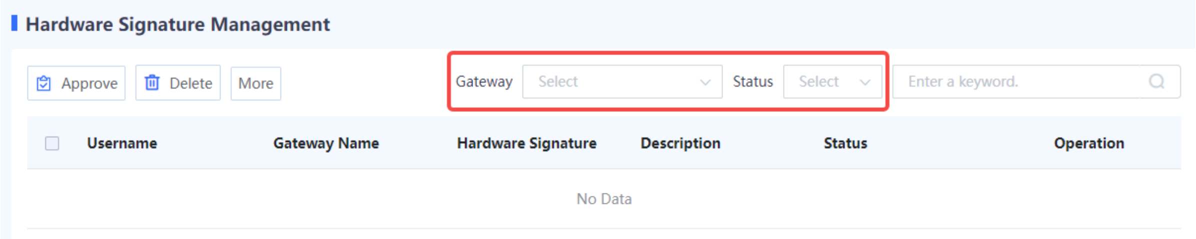


Hardware Signature Management

Gateway: Select   Status: Select   Enter a keyword.

□	Username	Gateway Name	Hardware Signature	Description	Status	Operation
No Data						

(5) (Optional) Select a gateway or approval status to view corresponding hardware signature information.



Hardware Signature Management

Gateway: Select   Status: Select   Enter a keyword.

□	Username	Gateway Name	Hardware Signature	Description	Status	Operation
No Data						

7.16.5 Operation Monitoring

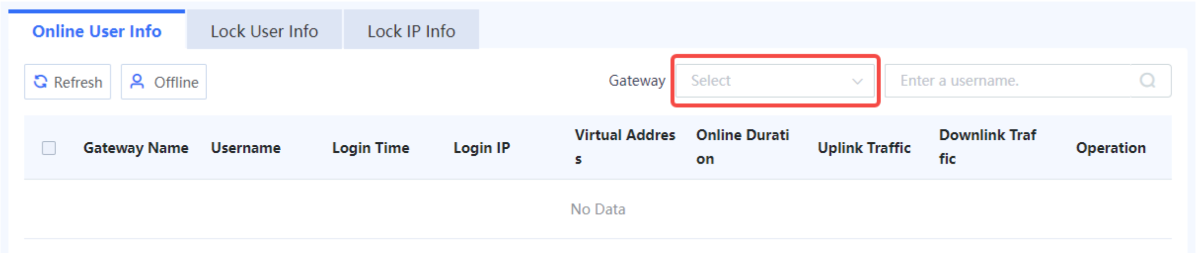
Application Scenario

Administrators can view current SSL VPN session information and perform operations such as forcing users to go offline and unlocking users and IP addresses.

1. Viewing Online User Information

(1) Choose **Network** > **SSL VPN** > **Operation Monitoring**.

(2) Click the **Online User Info** tab. The online user information of all SSL VPN gateways is displayed on this tab page. Select a gateway to view only the online user information of the selected gateway.



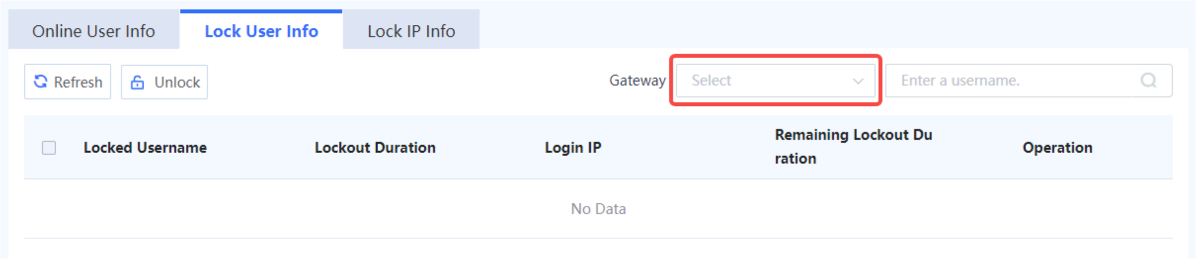
□	Gateway Name	Username	Login Time	Login IP	Virtual Address	Online Duration	Uplink Traffic	Downlink Traffic	Operation
				No Data					

(3) To force a user to go offline, click **Offline** in the **Operation** column.

2. Viewing Locked User Information

(4) Choose **Network** > **SSL VPN** > **Operation Monitoring**.

(5) Click the **Lock User Info** tab. The locked user information of all SSL VPN gateways is displayed on this tab page. Select a gateway to view only the locked user information of the selected gateway.



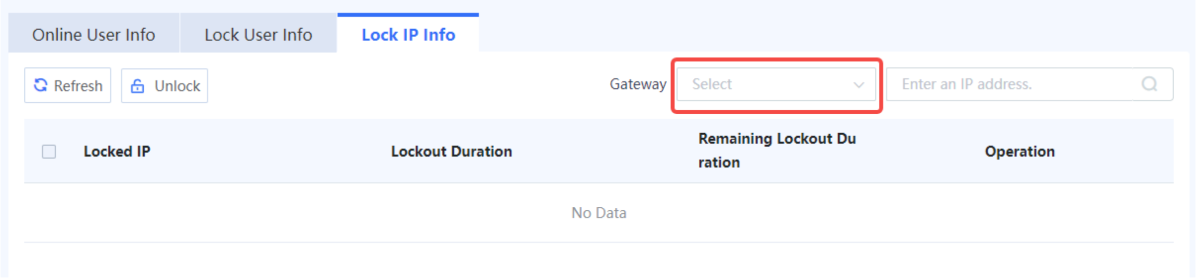
□	Locked Username	Lockout Duration	Login IP	Remaining Lockout Duration	Operation
			No Data		

(6) To unlock a user, click **Unlock** in the **Operation** column.

3. Viewing Locked IP Information

(7) Choose **Network** > **SSL VPN** > **Operation Monitoring**.

(8) Click the **Lock IP Info** tab. The locked IP information of all SSL VPN gateways is displayed on this tab page. Select a gateway to view only the locked IP information of the selected gateway.



□	Locked IP	Lockout Duration	Remaining Lockout Duration	Operation
		No Data		

(9) To unlock an IP address, click **Unlock** in the **Operation** column.

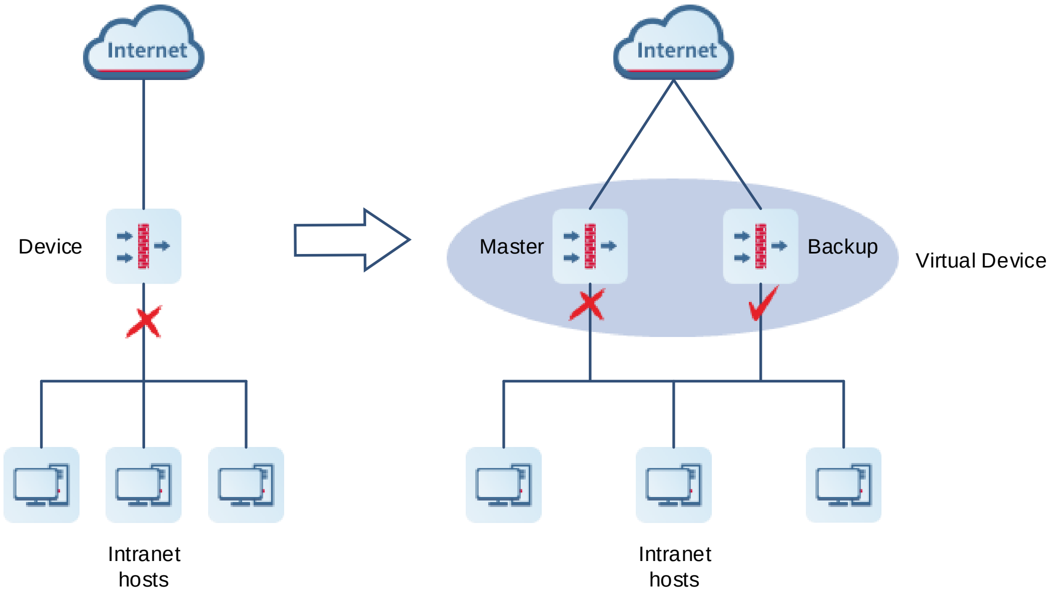
7.17 VRRP

7.17.1 Overview

Virtual Router Redundancy Protocol (VRRP) is a redundancy and fault-tolerance protocol that virtualizes a group of devices that can function as gateways into a virtual device. Intranet hosts only need to obtain the IP address of the virtual device and configure it as their gateway IP address so that they can communicate with the extranet through the virtual device.

Within the VRRP group, a master device is elected among all devices and responsible for forwarding network traffic. The remaining devices act as backup devices. If the master device fails, a new master device is elected from the backup devices to forward traffic, which ensures uninterrupted services.

VRRP improves network reliability, simplifies device configuration, and effectively prevents network interruptions caused by single-link failures.



Note

Only VRRPv2 is supported.

7.17.2 Working Process

After VRRP is configured, its working process is as follows:

(1) In a VRRP group, a master device is elected among devices based on priorities, while the remaining devices become backup devices. The master device sends gratuitous ARP messages to inform other devices and hosts of its virtual MAC address and is responsible for forwarding packets.

(2) The master device periodically sends VRRP messages to advertise its VRRP state, priority, and other information.

(3) If the master device fails, such as due to an uplink interface failure, a new master device is elected from the backup devices in the VRRP group based on priorities.

(4) Currently, VRRP supports only the preemption mode: When receiving a VRRP message, a backup device compares its priority with that of the master device in the VRRP message. If the backup device has a higher priority and the preemption delay duration expires, it automatically becomes the new master device.

(5) When the master role is taken by a new device, the new master device sends a gratuitous ARP message containing the MAC address and virtual IP address of the virtual device to notify other hosts and devices to update their ARP information. The new master device is

responsible for forwarding packets. Hosts and devices on the network are unaware of the master device switchover.

For enhanced security, VRRP provides plain text authentication. The master device adds an authentication text in the VRRP message and sends it to the backup devices. Upon receiving the VRRP message, the backup device compares the authentication text with its locally configured text. If the authentication texts match, the received VRRP message is considered valid. Otherwise, the backup device regards the VRRP message as an invalid message and discards it.

7.17.3 Configuring a VRRP Group

Application Scenario

VRRP is suitable for scenarios where redundancy is required at the routing egress to effectively prevent network interruptions caused by single-link failures.

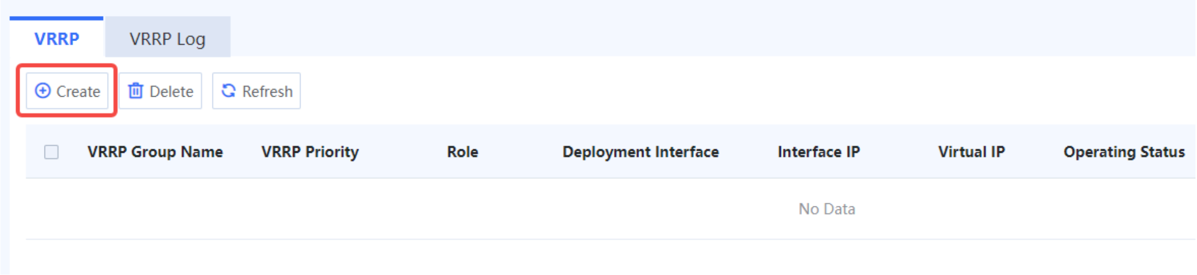
Note

Configuring multiple VRRP groups for load balancing is not supported.

Procedure

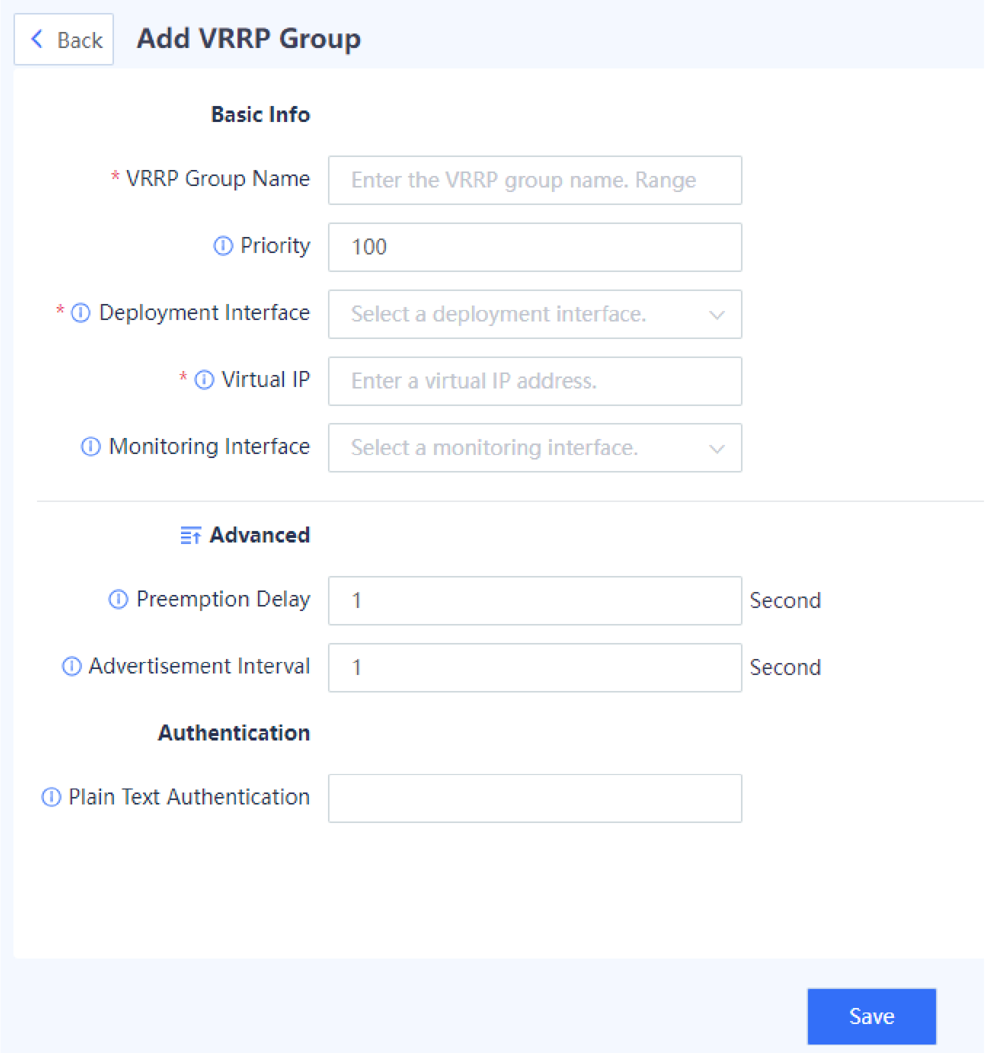
(1) Choose **Network** > **VRRP**. Click the **VRRP** tab.

(2) Click **Create** to access the **Add VRRP Group** page.



□	VRRP Group Name	VRRP Priority	Role	Deployment Interface	Interface IP	Virtual IP	Operating Status
					No Data		

(3) Configure the parameters of the VRRP group.



Add VRRP Group

Basic Info

* VRRP Group Name: Enter the VRRP group name. Range

Priority: 100

* Deployment Interface: Select a deployment interface.

* Virtual IP: Enter a virtual IP address.

Monitoring Interface: Select a monitoring interface.

Advanced

Preemption Delay: 1 Second

Advertisement Interval: 1 Second

Authentication

Plain Text Authentication:

Item	Description	Remarks
Basic Info		
VRRP Group Name	Number of the VRRP group. A group of devices with the same VRRP group name forms a virtual device.	[Example] 1
Priority	The priority of the VRRP group. A larger value indicates a higher priority. In a VRRP group, the device with the highest priority is elected as the master device.	[Example] 254

Item	Description	Remarks
Deployment Interface	Interface on which the VRRP function is enabled. You can specify only a physical interface or logical sub-interface in routing mode configured with an IPv4 address. The deployment interface and monitoring interface cannot be the same.	[Example] Ge0/4
Virtual IP	IP address of the virtual device, which is different from the IP address of the deployment interface but must be on the same network segment as the deployment interface.	[Example] 192.168.1.1
Monitoring Interface	Interface used to monitor uplink interface status changes of the device. This parameter can only be configured on the master device.	[Example] Ge0/2
Association Priority	When the status of the monitoring interface changes, this parameter determines how the VRRP priority of the local device is modified. If the monitoring interface goes Down, the priority of the device is reduced by the specified value. At this point, another device with the highest priority in the VRRP group can be elected as the new master device.	[Example] 10
Advanced		
Preemption Delay	Delay in seconds that a backup device waits before declaring itself as the master device when its priority is higher than that of the current master device.	[Example] 1
Advertisement Interval	Interval in seconds at which the master device sends VRRP messages. All devices within the same VRRP group must be configured with the same advertisement interval.	[Example] 1
Authentication		

Item	Description	Remarks
Plain Text Authentication	Determines whether VRRP messages are valid. Both the master and backup devices must be configured with the same plain text authentication key.	[Example] x30dn78k

Confirm the configuration and click **Save**.

Follow-up Procedure

- Choose **Policy** > **Security Policy** > **Security Policy**. On the **Security Policy** page, configure a policy to permit traffic on relevant interfaces. Otherwise, network connectivity issues may occur.
- Adding, deleting, or modifying VRRP configurations may cause VRRP group state changes. Eventually, the VRRP group will enter in a stable state. You can view running logs on the **VRRP Log** tab page.

7.17.4 Viewing VRRP Logs

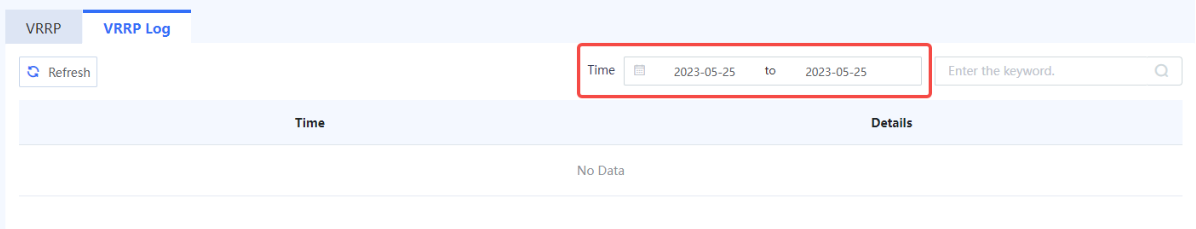
Application Scenario

A log entry is generated once the status of the master and backup devices in the VRRP group changes. This helps you check the running status of VRRP.

Procedure

Choose **Network** > **VRRP**. Click the **VRRP Log**.

Select a query period and the **VRRP Log** tab page displays the logs generated within the specified period.



7.18 User Authentication

7.18.1 Overview

When a firewall functions as an SSL VPN gateway, the firewall needs to authenticate remote access users to ensure secure connections. The user authentication process is as follows:

(1) On the VPN client, a remote user enters the IP address or domain name of the SSL VPN gateway, username, and password to request establishment of an SSL connection.

(2) The virtual gateway authenticates the user and supports the following authentication modes:

- Local authentication

  The remote user's identity information, including the username and password, is stored on the local device. After receiving the identity information, the virtual gateway authenticates the user according to the authentication domain configuration.

- Server authentication

  The remote user's identity information, including the username and password, is stored on the authentication server. (The server must be a RADIUS server.) After receiving the identity information, the virtual gateway forwards it to the RADIUS server. The server then authenticates the user and returns the authentication result to the virtual gateway.

(3) If the user passes authentication, the SSL connection is successfully established and the virtual gateway pushes authorized resources to the remote user. If the authentication fails, an authentication failure prompt is displayed on the virtual gateway login page.

Local authentication and server authentication can be used together for authenticating users.

7.18.2 User Management

1. Configuring User Groups

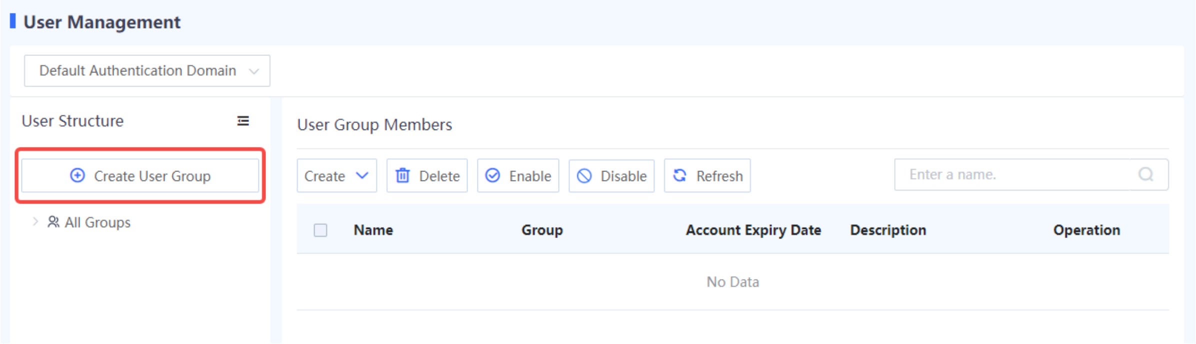
Application Scenario

Add users with similar attributes such as the same resource access requirements to a user group to facilitate unified management.

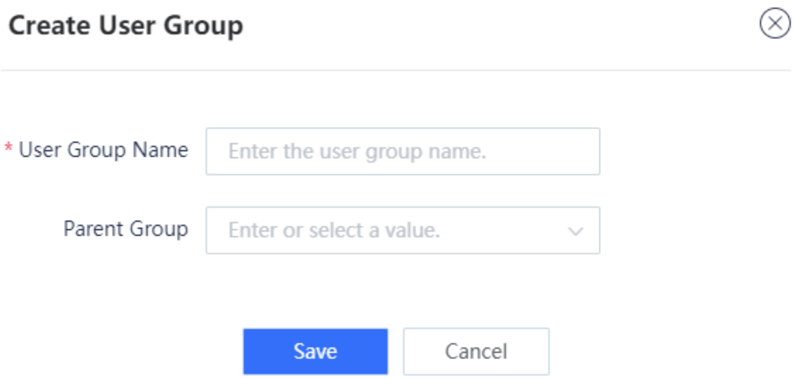
Procedure

(1) Choose **Object** > **User Authentication** > **User Management**.

(2) Click **Create User Group**.



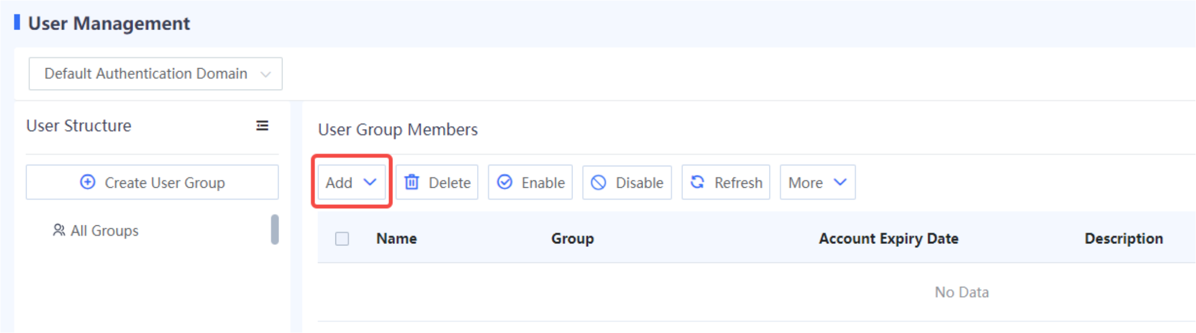
(3) Enter the user group name and select a parent group.



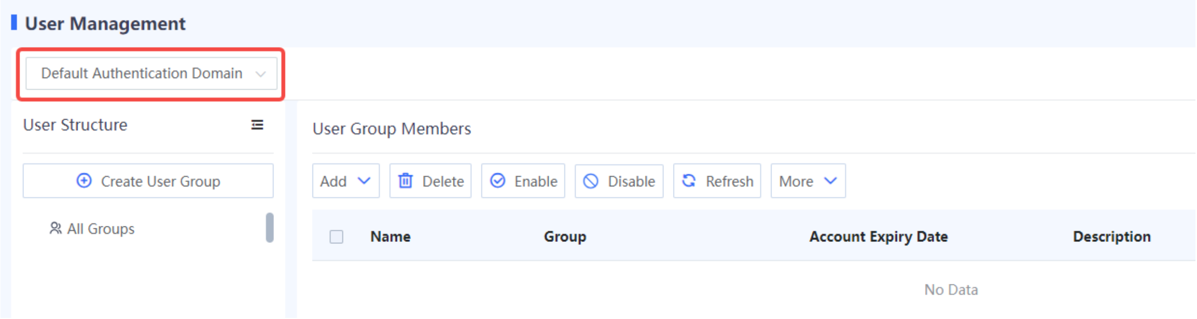
(4) After verifying the configuration, click **Save**.

Follow-up Procedure

- Click **Add** to configure users for the user group.



- Click the drop-down list in the upper left corner to select a user group and view its sub-group and user information.



2. Configuring Users

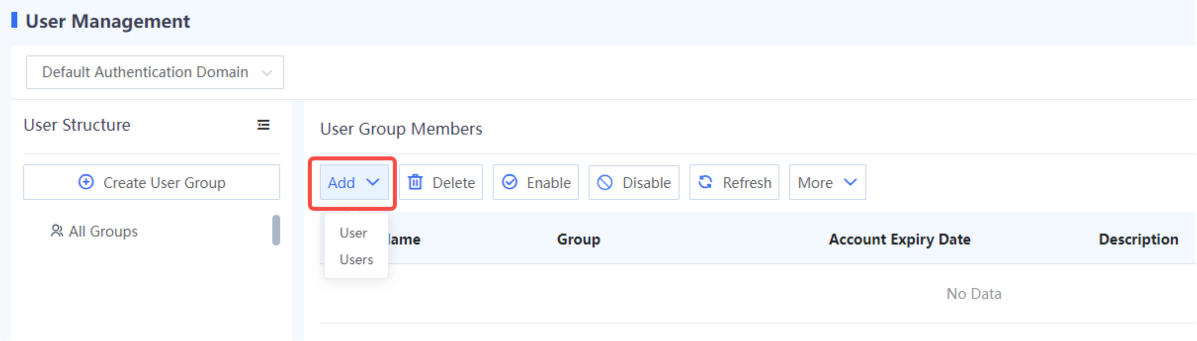
Application Scenario

When a firewall functions as an SSL VPN gateway and local authentication is required, you need to configure user identity information on the **User Management** page first. Otherwise, authentication may fail.

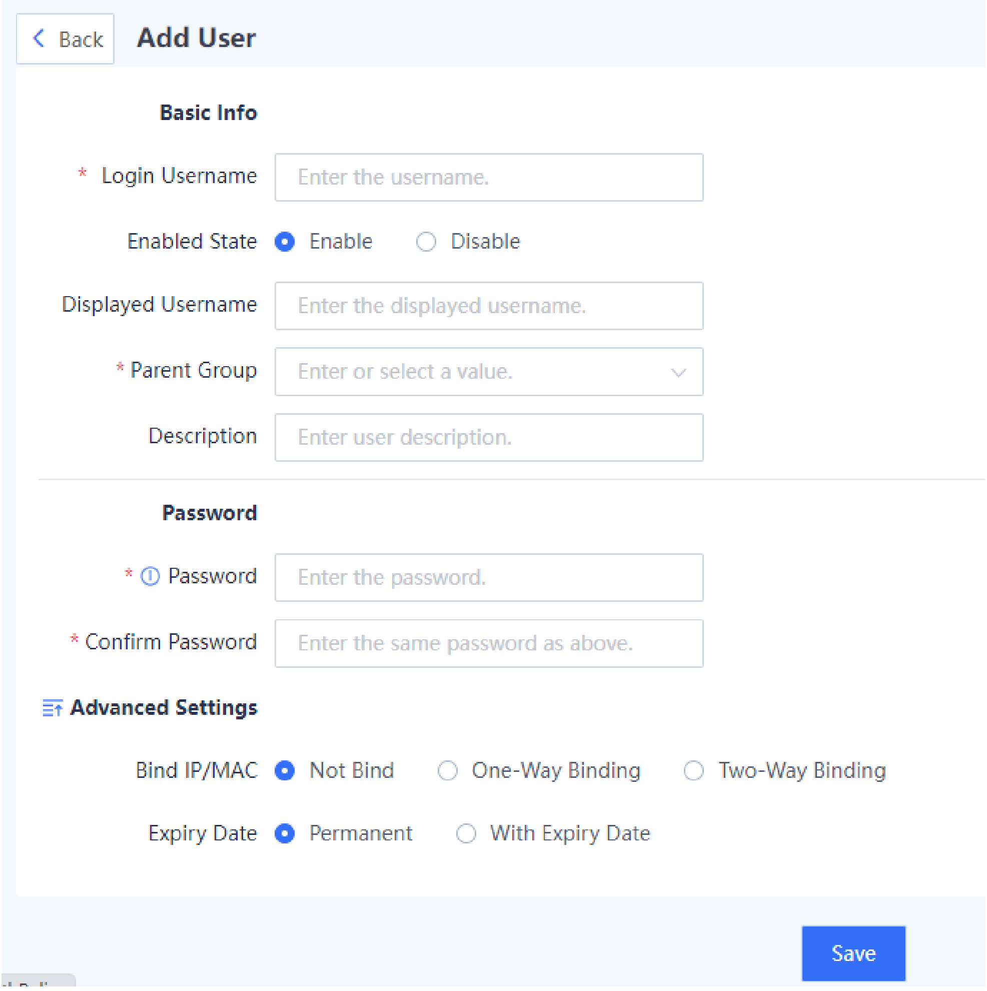
Procedure

(5) Choose **Object** > **User Authentication** > **User Management**.

(6) Click **Add**. In the drop-down list, select **User** to add one user at a time, or select **Users** to add multiple users at a time.



- Adding one user



Add User

Basic Info

* Login Username: Enter the username.

Enabled State: ● Enable ○ Disable

Displayed Username: Enter the displayed username.

* Parent Group: Enter or select a value.

Description: Enter user description.

Password

* Password: Enter the password.

* Confirm Password: Enter the same password as above.

Advanced Settings

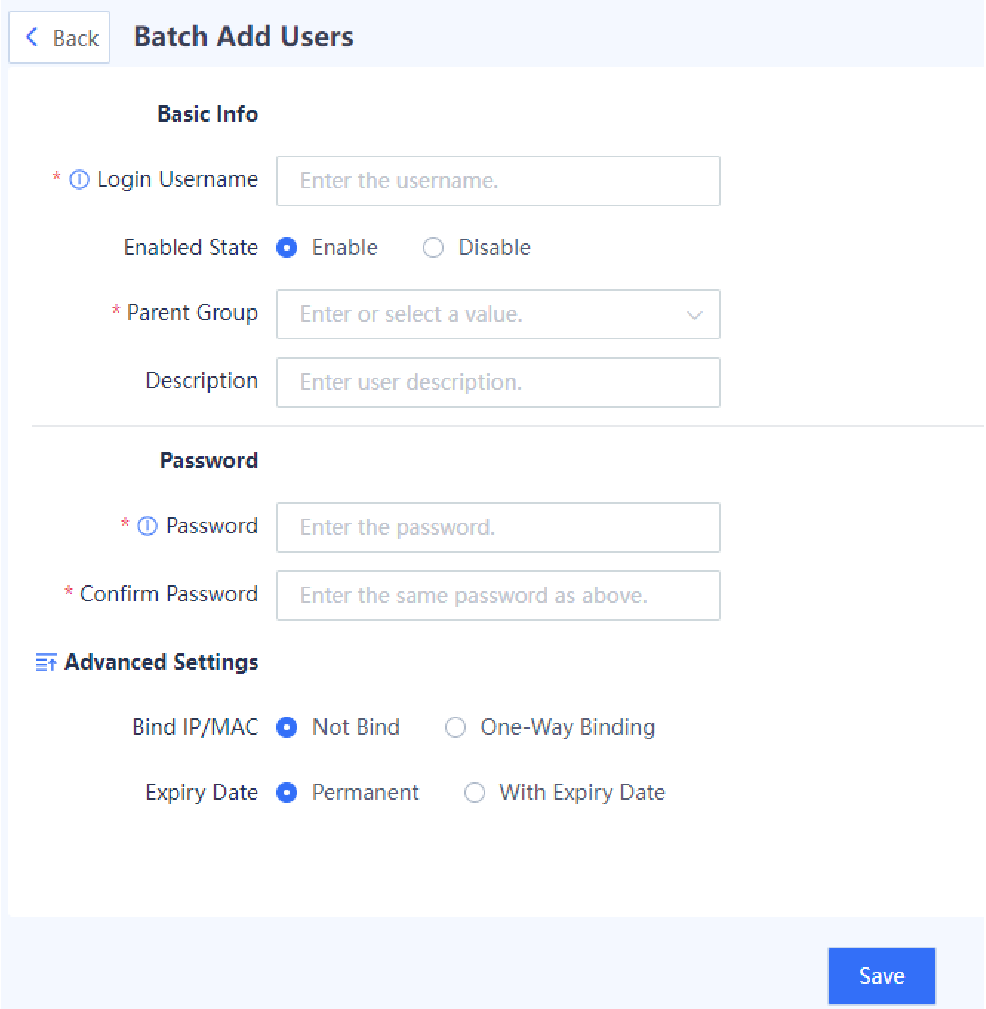
Bind IP/MAC: ● Not Bind ○ One-Way Binding ○ Two-Way Binding

Expiry Date: ● Permanent ○ With Expiry Date

Item	Description	Remarks
Basic Info		
Login Username	Username for the remote user to log in to the virtual gateway.	[Example] user1
Enabled State	Whether to enable user information for authentication. Users in disabled status cannot be authenticated.	[Example] Enable
Displayed Username	Username displayed on the virtual gateway after authentication. The value can be the same as that of **Login Username**.	[Example] user1
Group	Group to which the user belongs.	[Example] /default

Item	**Description**	**Remarks**
Description	User description.	N/A
Password		
Password	Password for the remote user to log in to the virtual gateway. For details about password complexity requirements, see 7.18.4 Authentication Settings.	N/A
Confirm Password	The value must be the same as that of **Password**.	N/A
Advanced Settings		
Bind IP/MAC	Whether to specify the IP or MAC address for user login: ● **Not Bind**: Unrestricted. ● **One-Way Binding**: A user can log in to the virtual gateway using only the specified IP or MAC address. ● **Two-Way Binding:** A user can log in to the virtual gateway using only the specified IP and MAC addresses.	N/A
Expiry Date	Expiry date of user identity information. When the expiry date is reached, the user is forced to go offline and cannot be authenticated again.	[Example] Permanent

- Adding users in a batch



< Back **Batch Add Users**

Basic Info

* Login Username: Enter the username.

Enabled State: ● Enable ○ Disable

* Parent Group: Enter or select a value.

Description: Enter user description.

Password

* Password: Enter the password.

* Confirm Password: Enter the same password as above.

Advanced Settings

Bind IP/MAC: ● Not Bind ○ One-Way Binding

Expiry Date: ● Permanent ○ With Expiry Date

Save

Item	Description	Remarks
Basic Info		
Login Username	Usernames for the remote users to log in to the virtual gateway on the SSL VPN client. Separate usernames with commas.	[Example] user1,user2
Enabled State	Whether to enable user information for authentication. Users in disabled status cannot be authenticated.	[Example] Enable
Group	Group to which the user belongs.	[Example] /default
Description	User description.	N/A
Password		

Item	Description	Remarks
Password	Shared password for the remote users to log in to the virtual gateway on the SSL VPN client.	N/A
Confirm Password	The value must be the same as that of **Password**.	N/A
Advanced Settings		
Bind IP/MAC	Whether to specify the IP or MAC address for user login: ● **Not Bind**: Unrestricted. ● **One-Way Binding**: A user can log in to the virtual gateway using only the specified IP or MAC address. ● **Two-Way Binding:** A user can log in to the virtual gateway using only the specified IP and MAC addresses.	N/A
Expiry Date	Expiry date of user identity information. When the expiry date is reached, the user is forced to go offline and cannot be authenticated again.	[Example] Permanent

(7) After verifying the configuration, click **Save**.

Follow-up Procedure

- To delete users in a batch, select the users and click **Delete**. After being deleted, the users cannot be authenticated.
- To disable users in a batch, select the users and click **Disable**. After being disabled, the users cannot be authenticated.
- To enable users in a batch, select the users and click **Enable**.

7.18.3 Authentication Domain Management

Application Scenario

When a firewall functions as an SSL VPN gateway, the firewall implements the same policies, including login authentication and resource authorization, for users in the same authentication domain, facilitating unified management.

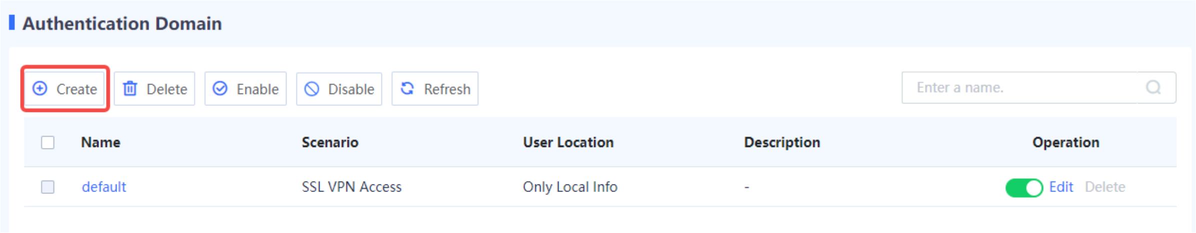
Prerequisites

You have configured user information on the firewall or authentication server. For details, see 7.18.2 User Management. For details on how to configure user information on the authentication server, see the corresponding server manual.

Procedure

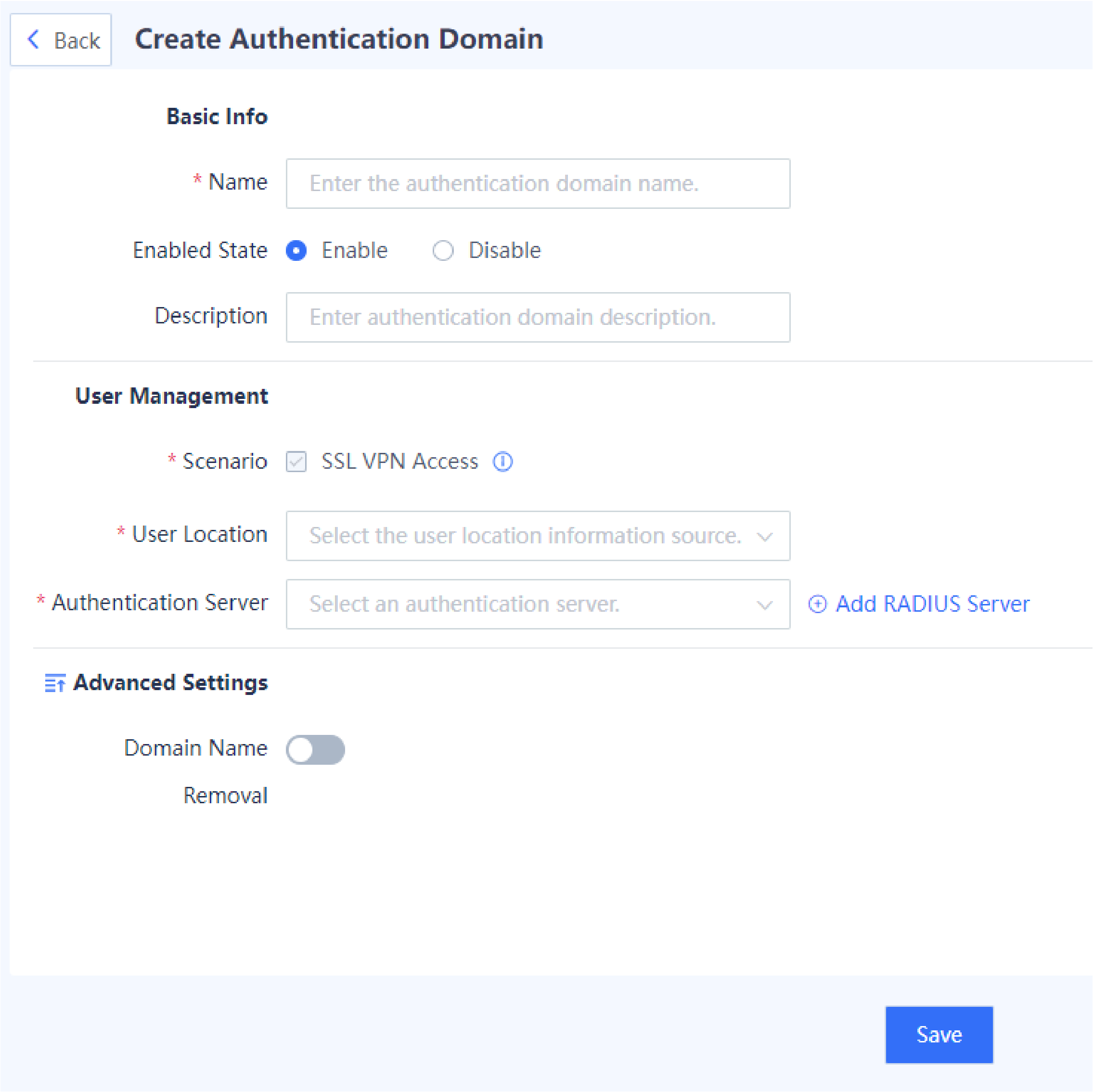
(1) Choose **Object** > **User Authentication** > **Authentication Domain**.

(2) Click **Create**.



□	Name	Scenario	User Location	Description	Operation
□	default	SSL VPN Access	Only Local Info	-	Edit Delete

(3) Configure authentication domain information.



* Name: Enter the authentication domain name.

Enabled State: ● Enable ○ Disable

Description: Enter authentication domain description.

* Scenario: ☑ SSL VPN Access

* User Location: Select the user location information source.

* Authentication Server: Select an authentication server.

Domain Name Removal: Off

Item	Description	Remarks
Basic Info		
Name	Authentication domain name.	[Example] auth_domain_1
Enabled State	Whether to enable the authentication domain.	[Example] Enable
Description	Authentication domain description.	N/A
User Management		
User Location	Set the user authentication mode. The options are as follows: ● **Prefer Info on Server**: User identity information, including the username and password, is stored on the authentication server or local firewall. The information on the authentication server is preferentially used for authentication. ● **Prefer Local Info**: User identity information, including the username and password, is stored on the authentication server or local firewall. The information on the local firewall is preferentially used for authentication. ● **Only Info on Server**: User identity information, including the username and password, is stored on the authentication server for authentication. ● **Only Local Info**: User identity information, including the username and password, is stored on the local firewall for authentication.	N/A
Authentication Server	Authentication server.	N/A
Advanced Settings		

Item	Description	Remarks
Domain Name Removal	Whether to remove the authentication domain name from the input username when a user logs in to the virtual gateway on the SSL VPN client. By default, the authentication domain name is not removed.	N/A

(4) After verifying the configuration, click **Save**.

Follow-up Procedure

- To delete authentication domains in a batch, select the domains and click **Delete**. After an authentication domain is deleted, all users and user groups in the domain are also deleted.
- To disable authentication domains in a batch, select the domains and click **Disable**.
- To enable authentication domains in a batch, select the domains and click **Enable**.

7.18.4 Authentication Settings

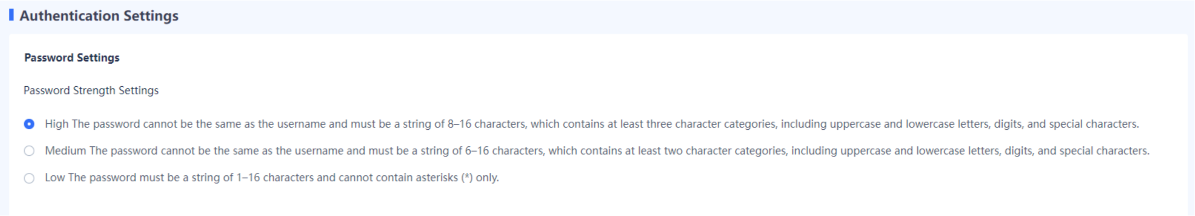
Application Scenario

Set password complexity requirements for user login to reduce the risk caused by weak passwords.

Procedure

(1) Choose **Object** > **User Authentication** > **Authentication Settings**.

(2) Select a password strength level as required.



Authentication Settings

Password Settings

Password Strength Settings

● High The password cannot be the same as the username and must be a string of 8–16 characters, which contains at least three character categories, including uppercase and lowercase letters, digits, and special characters.

○ Medium The password cannot be the same as the username and must be a string of 6–16 characters, which contains at least two character categories, including uppercase and lowercase letters, digits, and special characters.

○ Low The password must be a string of 1–16 characters and cannot contain asterisks (*) only.

Note

After the password strength level is changed, the passwords of newly added users must meet the complexity requirements of the new strength level. For details about user creation, see 7.18.2 7.18.2 2. Configuring Users.

7.18.5 Authentication Server

Application Scenario

When a firewall functions as an SSL VPN gateway and server authentication is required, you need to configure user identity information on the RADIUS server and add the RADIUS server on the firewall first.

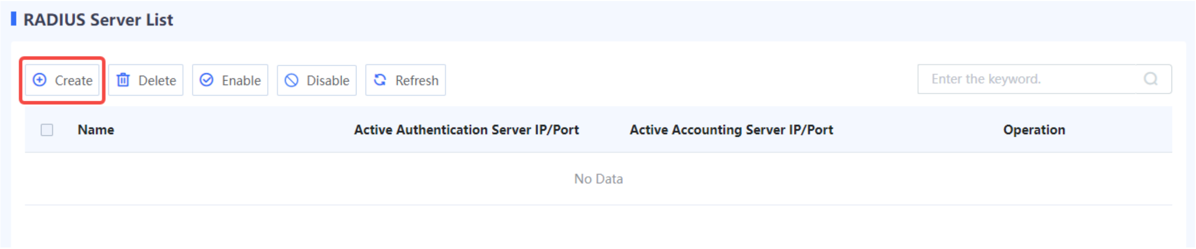
Precautions

- Ensure that the firewall can communicate with the authentication server. Otherwise, authentication may fail.
- Currently, accounting is not supported.

Procedure

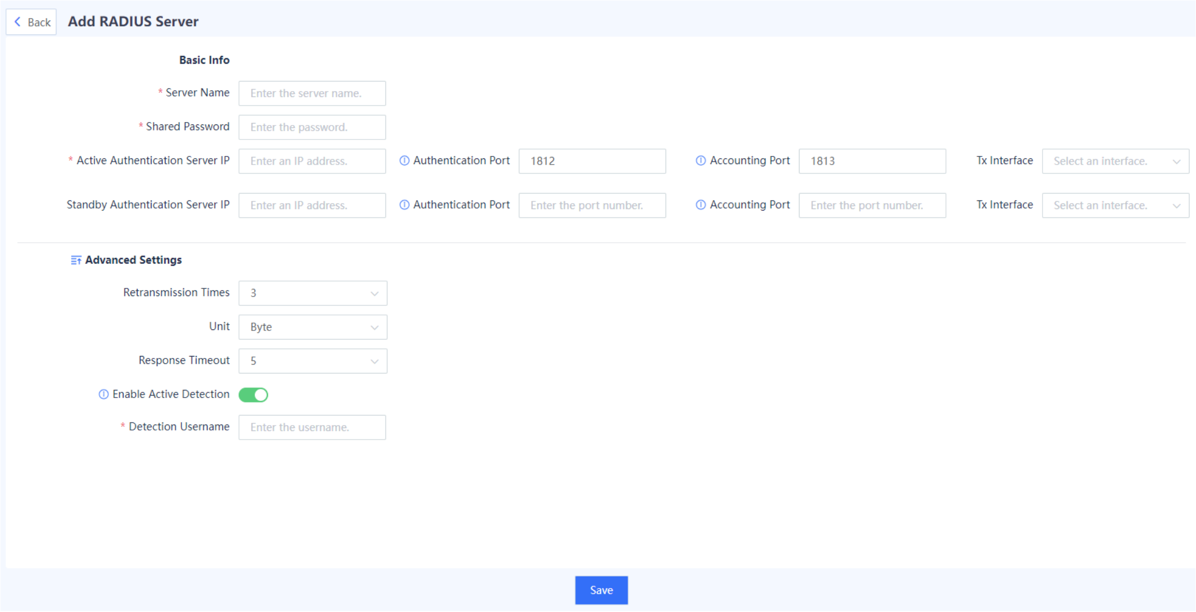
(1) Choose **Object** > **User Authentication** > **Authentication Server**.

(2) Click **Create**.



□	Name	Active Authentication Server IP/Port	Active Accounting Server IP/Port	Operation
		No Data		

(3) Configure the server.



Basic Info

* Server Name: Enter the server name.

* Shared Password: Enter the password.

* Active Authentication Server IP: Enter an IP address. | Authentication Port: 1812 | Accounting Port: 1813 | Tx Interface: Select an interface.

Standby Authentication Server IP: Enter an IP address. | Authentication Port: Enter the port number. | Accounting Port: Enter the port number. | Tx Interface: Select an interface.

Advanced Settings

Retransmission Times: 3

Unit: Byte

Response Timeout: 5

Enable Active Detection: on

* Detection Username: Enter the username.

Item	Description	Remarks
Basic Info		
Server Name	RADIUS server name.	[Example] server_1
Shared Password	Password for communication between the firewall and authentication server. The password must be the same as that set on the authentication server. Otherwise, authentication cannot be performed.	N/A
Active Authentication Server	Authentication server that performs authentication. ● **IP**: IP address of the authentication server. ● **Authentication Port**: Port on the authentication server that provides the authentication service. ● **Accounting Port**: Port on the authentication server that provides the accounting service. ● **Tx Interface**: Interface on the firewall for sending authentication packets.	N/A
Standby Authentication Server	When the active authentication server fails or has no user information, the standby authentication server performs authentication. ● **IP**: IP address of the authentication server. ● **Authentication Port**: Port on the authentication server that provides the authentication service. ● **Accounting Port**: Port on the authentication server that provides the accounting service. ● **Tx Interface**: Interface on the firewall for sending authentication packets.	N/A
Advanced Settings		

Retransmission Times	Maximum times of resending authentication request packets when the firewall does not receive a reply packet from the authentication server. If the retransmission times configured for both the active and standby servers are reached, the server is deemed as unreachable and the authentication fails.	[Example] 3
Unit	Unit of data flows that the firewall sends to the authentication server. The value must be the same as the traffic statistics unit on the server.	[Example] byte
Response Timeout	Timeout period in seconds for the firewall to receive a reply packet from the authentication server. When the timeout period expires, the firewall sends a request packet again.	[Example] 5
Enable Active Detection	After this function is enabled, the device sends a RADIUS packet every 10 minutes to detect whether the server can be connected.	-
Detection Username	Username carried in the RADIUS packet. You are advised to set it to the active detection username provided by the server. Otherwise, the server will generate a large number of authentication failure logs.	-

(4) After verifying the configuration, click **Save**.

Follow-up Procedure

- To delete authentication servers in a batch, select the servers and click **Delete**.
- To disable authentication servers in a batch, select the servers and click **Disable**.

To enable authentication servers in a batch, select the servers and click **Enable**.

8 Routine Maintenance

8.1 Checking Indicators on the Hardware Device Panel

Figure 8-1 and Table 8-1 describe the indicators on the device panel of the RG-WALL 1600-Z3200-S.

Figure 8-1 Front Panel

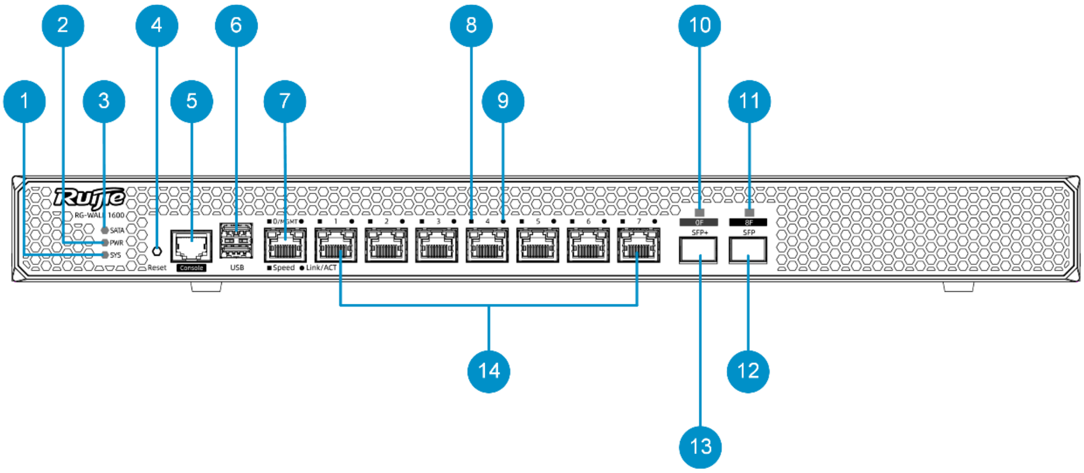


Table 8-1 Components on the Front Panel

No.	Component	Description
1	SYS indicator	● Blinking green: The device is powered on and being initialized. ● Steady green: Initialization is complete. ● Steady red: An alarm is generated.
2	PWR indicator	● Steady green: The power supply is normal. ● Off: The power supply is cut off or fails.
3	SATA hard disk indicator	● Steady green: A hard disk is connected. ● Blinking green: Data is being read or written.
4	Reset button	● Restarting the device: Press the button for less than 3

No.	Component	Description
		seconds. ● Restoring factory settings: Press the button for more than 3 seconds. When you perform either of the preceding operations, device status information is collected. After the device restarts, you can access the web UI of the firewall, choose **System** > **One-Click Collection**, and download the information.
5	Console port	It is used to connect to the console for device maintenance and diagnosis. Note: The console port is used only in special scenarios. For details, contact technical support personnel.
6	USB port	Two USB 2.0 ports can be used to connect USB drives.
7	Electrical port 0 (port 0/MGMT)	It is used to access the device management page upon first login.
8	Speed indicators (square) of electrical ports 0 to 7	● Steady orange: Gbit/s port speed ● Off: 100/10 Mbit/s port speed
9	Link/ACT status indicators (round) of electrical ports 0 to 7	● Steady green: The port is connected. ● Blinking green: The port is receiving or sending data. ● Off: The port is incorrectly connected.
10	Optical port 0F indicator	● Steady green: The port is connected. ● Blinking green: The port is receiving or sending data. ● Off: The optical port is incorrectly connected.
11	Optical port 8F indicator	● Steady green: The port is connected.

No.	Component	Description
		● Blinking green: The port is receiving or sending data. ● Off: The optical port is incorrectly connected.
12	Optical port 8F	Gigabit optical port. For details about optical modules that support this port, see Table 1-3.
13	Optical port 0F	10 Gigabit optical port. For details about optical modules that support this port, see Table 1-3.
14	Electrical ports 1 to 7	They are used to connect network cables.

8.2 Checking Basic Configurations

Application Scenario

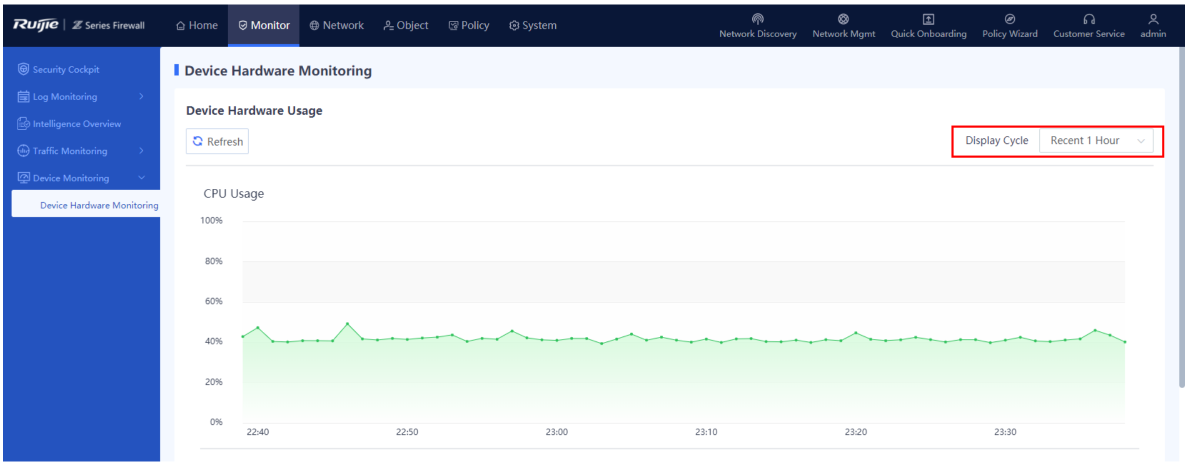
You can perform this operation to monitor the CPU, memory, and hard disk usage of the firewall. The information allows you to process exceptions in a timely manner.

You can set the display cycle to real-time, recent 24 hours, or recent 7 days. The system displays historical data about the CPU, memory, and hard disk usage in real time or of recent 24 hours or recent 7 days.

Procedure

(1) Choose **Monitor** > **Device Monitoring** > **Device Hardware Monitoring**.

(2) Set **Display Cycle**.

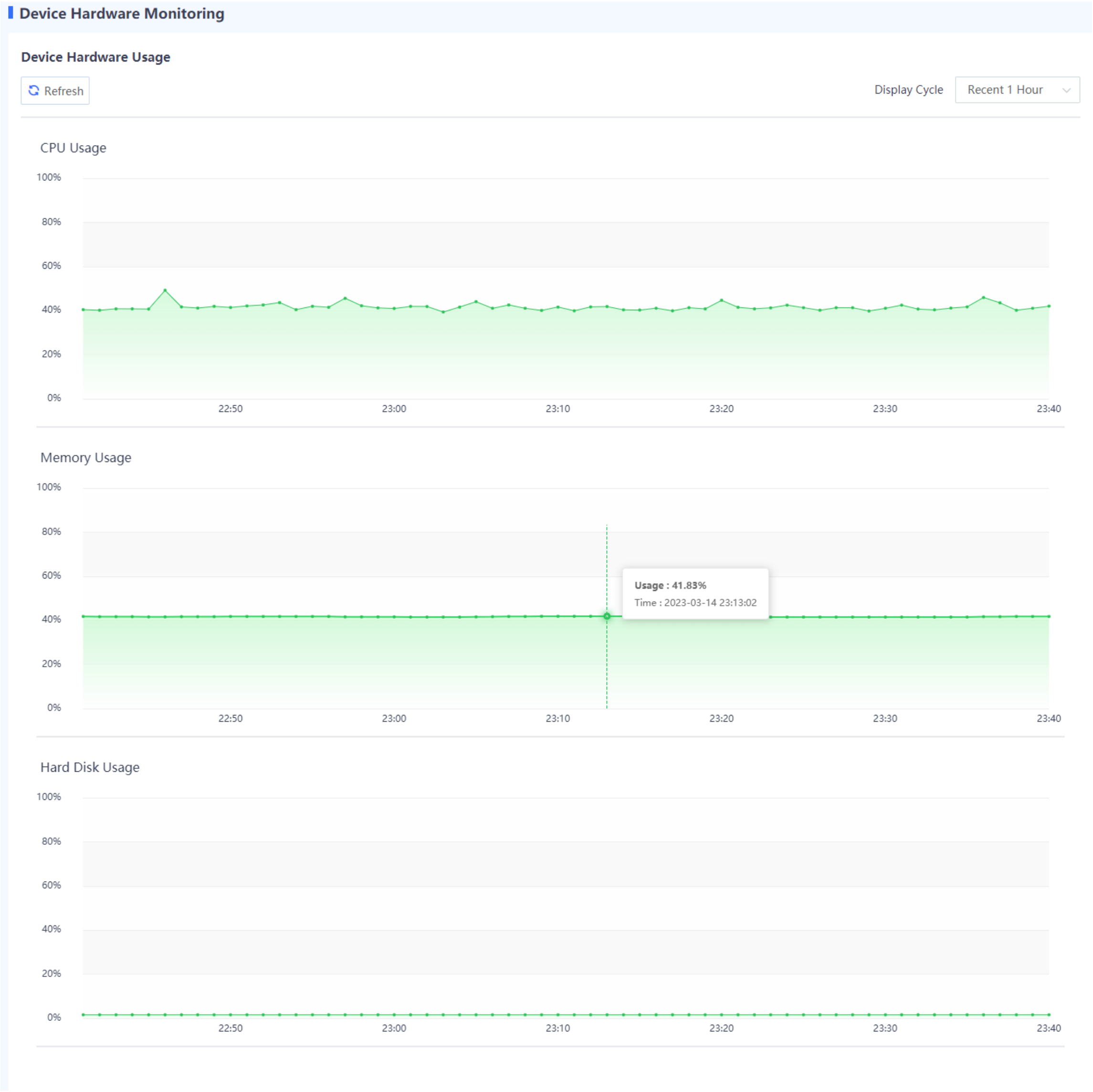


Device Hardware Monitoring

Device Hardware Usage

Display Cycle: Recent 1 Hour

(3) The page displays the CPU usage, memory usage, and hard disk usage in different areas.



Follow-up Procedure

Item	Description
CPU	In normal cases, the CPU usage should be lower than 80%. If the CPU usage is too high for a long time, check the device and analyze the causes. The possible causes for high CPU usage are as follows: ● App protection or DDoS protection is enabled. ● Too many connections are created, many of which are initiated by

	attackers.
Memory	In normal cases, the memory usage should be lower than 80%. If the memory usage is too high for a long time, check the device and analyze the causes.
Hard disk	In normal cases, the hard disk usage should be lower than 90%. If the remaining hard disk space is too small for a long time, check the device and clear the hard disk space.

8.3 Log Monitoring

Log information refers to the packet processing information recorded by the firewall. The network administrator can effectively monitor the network running information and diagnose network faults based on the log information. The network administrator can also track, record, and analyze network access of users in real time and audit network access behavior of users. The firewall can export system logs, security logs, and operation logs and back up log files to a third-party server through Syslog.

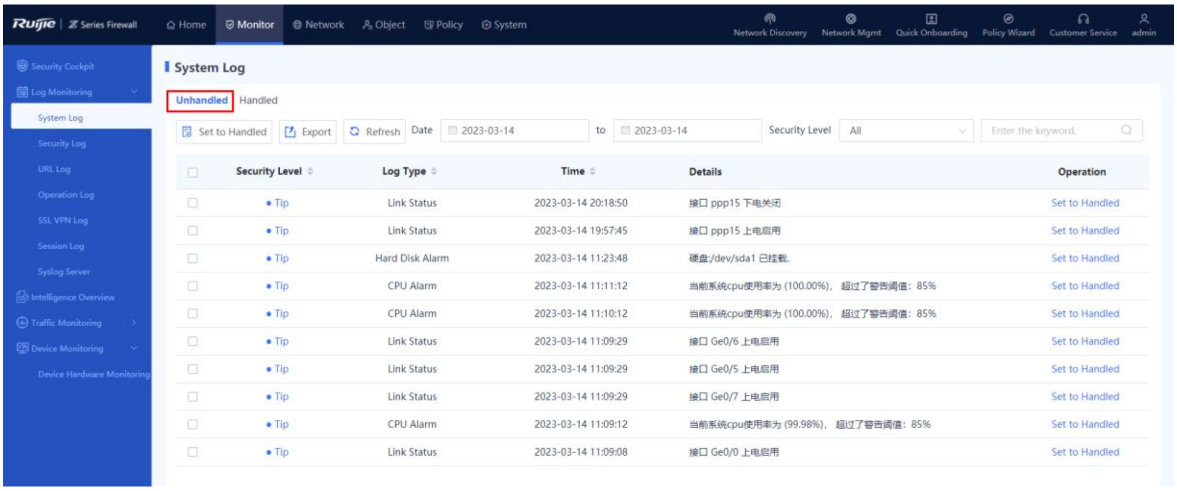
8.3.1 Querying System Logs

Application Scenario

By querying system logs, the administrator can view the runtime logs generated during the system running process and log records related to the hardware environment to check whether the firewall keeps running properly. If a fault occurs, the administrator can locate and analyze the fault based on the system logs.

Procedure

(1) Choose **Monitor** > **Log Monitoring** > **System Log** > **Unhandled**.



Date 2023-03-14 to 2023-03-14 Security Level All

☐	Security Level	Log Type	Time	Details	Operation
☐	• Tip	Link Status	2023-03-14 20:18:50	接口 ppp15 下电关闭	Set to Handled
☐	• Tip	Link Status	2023-03-14 19:57:45	接口 ppp15 上电启用	Set to Handled
☐	• Tip	Hard Disk Alarm	2023-03-14 11:23:48	硬盘:/dev/sda1 已挂载.	Set to Handled
☐	• Tip	CPU Alarm	2023-03-14 11:11:12	当前系统cpu使用率为 (100.00%)，超过了警告阈值：85%	Set to Handled
☐	• Tip	CPU Alarm	2023-03-14 11:10:12	当前系统cpu使用率为 (100.00%)，超过了警告阈值：85%	Set to Handled
☐	• Tip	Link Status	2023-03-14 11:09:29	接口 Ge0/6 上电启用	Set to Handled
☐	• Tip	Link Status	2023-03-14 11:09:29	接口 Ge0/5 上电启用	Set to Handled
☐	• Tip	Link Status	2023-03-14 11:09:29	接口 Ge0/7 上电启用	Set to Handled
☐	• Tip	CPU Alarm	2023-03-14 11:09:12	当前系统cpu使用率为 (99.98%)，超过了警告阈值：85%	Set to Handled
☐	• Tip	Link Status	2023-03-14 11:09:08	接口 Ge0/0 上电启用	Set to Handled

(2) The system log-related information is displayed on the web page.

Field	Description
Security Level	Security level of a system log.
Log Type	Type of a system log.
Time	Time when a system log is generated.
Details	Detailed information of a system log.
Operation	Click **Set to Handled** to mark a log as **Handled** and switch to the **Handled** tab to view handled logs.

Note

The system supports fuzzy match by the security level, log type, or other keywords. Only system logs matching the search criteria are displayed on the page.

Follow-up Procedure

- Select multiple logs and click **Set to Handled** to modify the status of the selected logs to **Handled** in a batch.
- Click **Export** to export system logs to the local device in the Excel format, facilitating subsequent query.
- Click **Refresh** to obtain the latest system logs.

8.3.2 Querying Security Logs

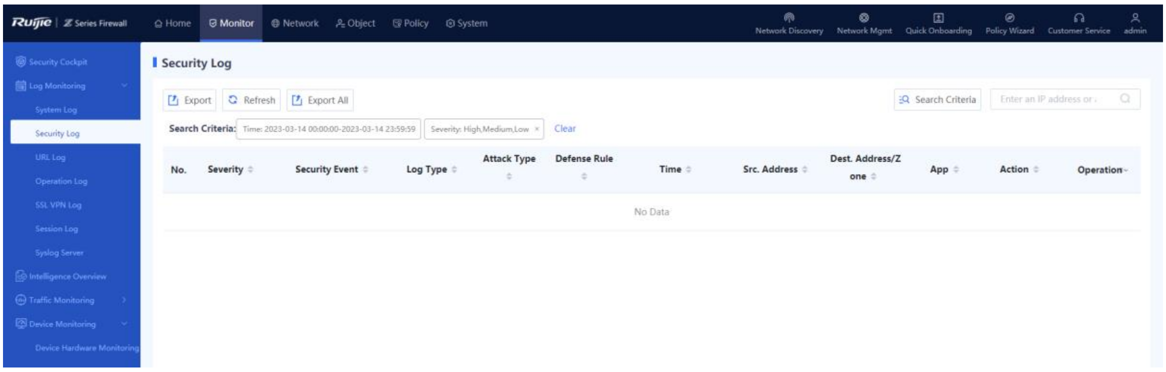
Application Scenario

By querying security logs, the administrator can obtain traffic attack information on the network to check the network bandwidth usage and whether security policies and bandwidth policies are effective.

Procedure

(1) Choose **Monitor** > **Log Monitoring** > **Security Log**.

(2) The security log-related information is displayed on the web page.



Search Criteria: Time: 2023-03-14 00:00:00-2023-03-14 23:59:59 Severity: High,Medium,Low

No.	Severity	Security Event	Log Type	Attack Type	Defense Rule	Time	Src. Address	Dest. Address/Zone	App	Action	Operation

No Data

Field	Description
Severity	Severity level of a problem marked in the security log.
Security Event	Description of a security event recorded in the log.
Log Type	Type of a security event recorded in the log. [Example] IPS attack
Attack Type	Type of the attack recorded in the log. [Example] Heap Overflow
Time	Time when a security log is generated.
Src. Security Zone	Source security zone in a security policy.
Src. Address	Source address in a security policy.
Src. Port	Source port in a security policy.
Dest. Port	Destination port in a security policy.

Field	Description
Dest. Security Zone	Destination security zone in a security policy.
Dest. Address/Zone	Destination address in a security policy.
Action	Operation result of a security policy on the traffic.
Operation	Click **View Details** to obtain details about a security log.

Note

You can click **Search Criteria** to set the keywords for log query. Only security logs matching the search criteria are displayed on the page.

Follow-up Procedure

- Click **Export** to export security logs to the local device in the Excel format, facilitating subsequent query.
- Click **Refresh** to obtain the latest security logs.

8.3.3 Querying Session Logs

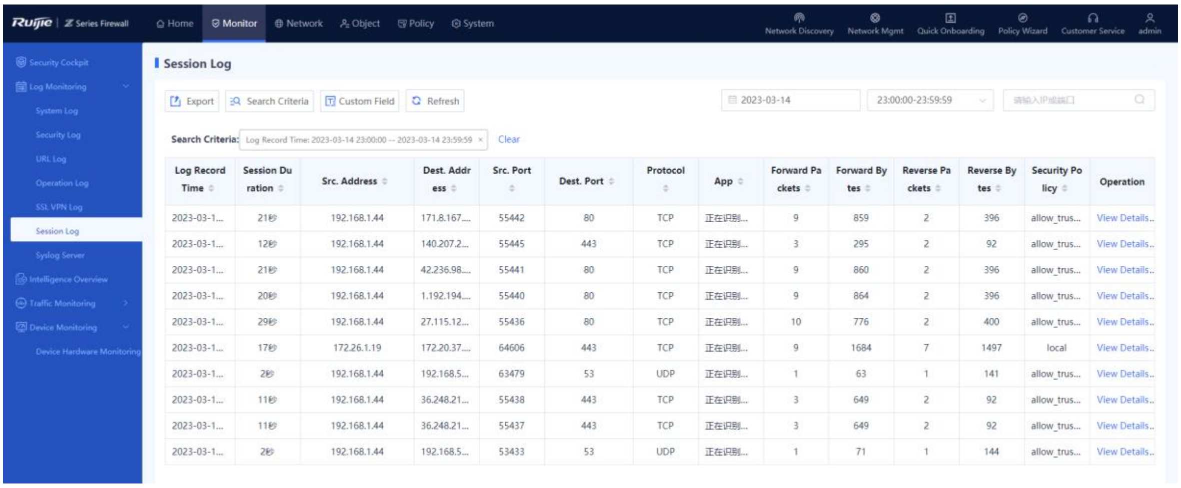
Application Scenario

By querying session logs, the administrator can view detailed information of each data flow, including 5-tuple information of the data flow (source IP address, source port, destination IP address, destination port, and protocol) as well as the security policy hit by the data flow and the application carried in the data flow.

Procedure

(1) Choose **Monitor** > **Log Monitoring** > **Session Log**.

(2) The session log-related information is displayed on the web page.



Session Log

2023-03-14 | 23:00:00-23:59:59 | 请输入IP或端口

Search Criteria: Log Record Time: 2023-03-14 23:00:00 -- 2023-03-14 23:59:59

Log Record Time	Session Duration	Src. Address	Dest. Address	Src. Port	Dest. Port	Protocol	App	Forward Packets	Forward Bytes	Reverse Packets	Reverse Bytes	Security Policy	Operation
2023-03-1...	21秒	192.168.1.44	171.8.167....	55442	80	TCP	正在识别...	9	859	2	396	allow_trus...	View Details...
2023-03-1...	12秒	192.168.1.44	140.207.2...	55445	443	TCP	正在识别...	3	295	2	92	allow_trus...	View Details...
2023-03-1...	21秒	192.168.1.44	42.236.98....	55441	80	TCP	正在识别...	9	860	2	396	allow_trus...	View Details...
2023-03-1...	20秒	192.168.1.44	1.192.194....	55440	80	TCP	正在识别...	9	864	2	396	allow_trus...	View Details...
2023-03-1...	29秒	192.168.1.44	27.115.12...	55436	80	TCP	正在识别...	10	776	2	400	allow_trus...	View Details...
2023-03-1...	17秒	172.26.1.19	172.20.37....	64606	443	TCP	正在识别...	9	1684	7	1497	local	View Details...
2023-03-1...	2秒	192.168.1.44	192.168.5...	63479	53	UDP	正在识别...	1	63	1	141	allow_trus...	View Details...
2023-03-1...	11秒	192.168.1.44	36.248.21...	55438	443	TCP	正在识别...	3	649	2	92	allow_trus...	View Details...
2023-03-1...	11秒	192.168.1.44	36.248.21...	55437	443	TCP	正在识别...	3	649	2	92	allow_trus...	View Details...
2023-03-1...	2秒	192.168.1.44	192.168.5...	53433	53	UDP	正在识别...	1	71	1	144	allow_trus...	View Details...

Note

You can click **Search Criteria** to set the keywords for log query. Only session logs matching the search criteria are displayed on the page.

Follow-up Procedure

- Click **Export** to export session logs to the local device in the Excel format, facilitating subsequent query.
- Click **Custom Field** to set the fields to be displayed on the page.
- Click **Refresh** to obtain the latest session logs.

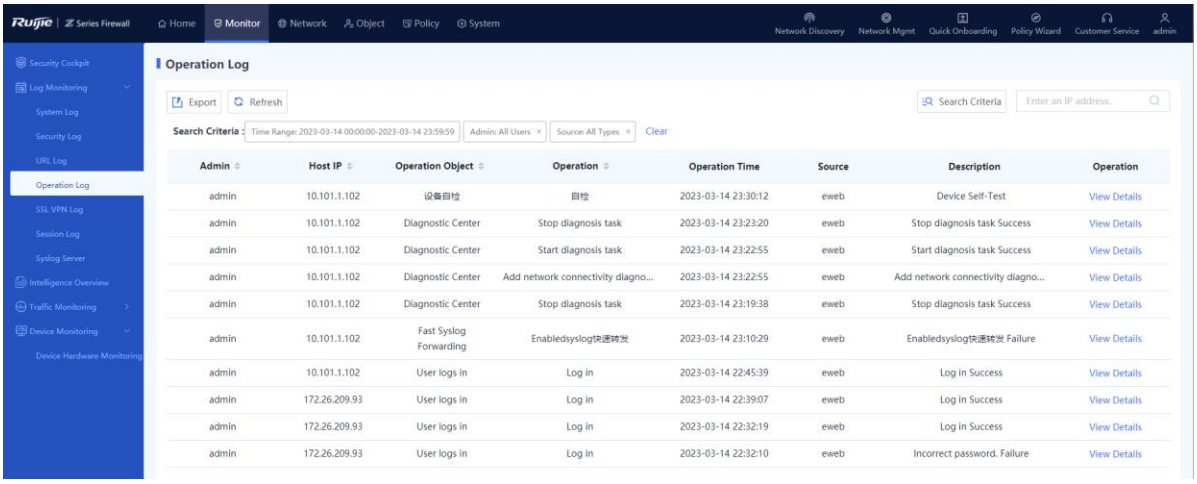
8.3.4 Querying Operation Logs

Application Scenario

By querying operation logs, the administrator can view the online records of users, including the IP address used for login, operation object, action, and operation time. This information allows the administrator to know user activities on the network, detect abnormal user login or network access behavior, and respond in time.

Procedure

(1) Choose **Monitor** > **Log Monitoring** > **Operation Log**.



Operation Log

Search Criteria : Time Range: 2023-03-14 00:00:00-2023-03-14 23:59:59 | Admin: All Users | Source: All Types

Admin	Host IP	Operation Object	Operation	Operation Time	Source	Description	Operation
admin	10.101.1.102	设备自检	自检	2023-03-14 23:30:12	eweb	Device Self-Test	View Details
admin	10.101.1.102	Diagnostic Center	Stop diagnosis task	2023-03-14 23:23:20	eweb	Stop diagnosis task Success	View Details
admin	10.101.1.102	Diagnostic Center	Start diagnosis task	2023-03-14 23:22:55	eweb	Start diagnosis task Success	View Details
admin	10.101.1.102	Diagnostic Center	Add network connectivity diagno...	2023-03-14 23:22:55	eweb	Add network connectivity diagno...	View Details
admin	10.101.1.102	Diagnostic Center	Stop diagnosis task	2023-03-14 23:19:38	eweb	Stop diagnosis task Success	View Details
admin	10.101.1.102	Fast Syslog Forwarding	Enabledsyslog快速转发	2023-03-14 23:10:29	eweb	Enabledsyslog快速转发 Failure	View Details
admin	10.101.1.102	User logs in	Log in	2023-03-14 22:45:39	eweb	Log in Success	View Details
admin	172.26.209.93	User logs in	Log in	2023-03-14 22:39:07	eweb	Log in Success	View Details
admin	172.26.209.93	User logs in	Log in	2023-03-14 22:32:19	eweb	Log in Success	View Details
admin	172.26.209.93	User logs in	Log in	2023-03-14 22:32:10	eweb	Incorrect password. Failure	View Details

(2) The operation log-related information is displayed on the web page.

Field	Description
Admin	Name of the administrator who performs the operation.
Host IP	Host IP address used by the administrator to log in to the firewall.
Operation Object	Type of the object managed by the administrator.
Operation	Specific operation performed by the administrator.
Operation Time	Time when the administrator performs the operation.
Description	Description of the operation log.
Operation	Click **View Details** to obtain details about an operation log.

Note

You can click **Search Criteria** to set the keywords for log query. Only operation logs matching the search criteria are displayed on the page.

Follow-up Procedure

- Click **Export** to export operation logs to the local device in the Excel format, facilitating subsequent query.

- Click **Refresh** to obtain the latest operation logs.

8.3.5 Configuring the Syslog Server

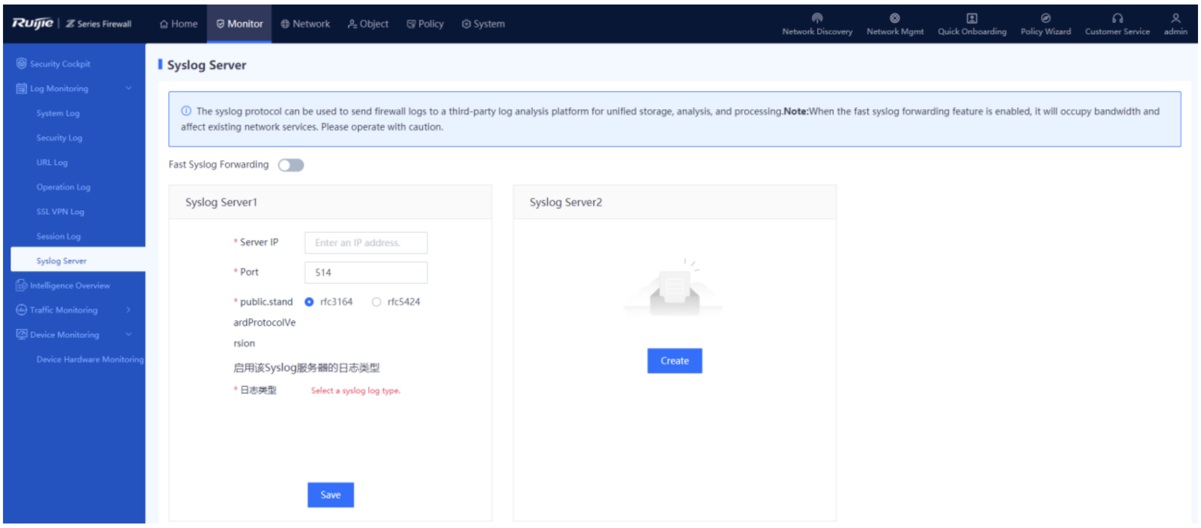
Application Scenario

If the firewall is not installed with a hard disk upon factory delivery, logs can only be stored in the memory (for no longer than 1 day) and all the logs in the memory will be lost after device restart. To ensure that more log information can be obtained, the system logs and security logs of the firewall can be transmitted to a third-party log platform through Syslog for storage and analysis.

Procedure

(1) Choose **Monitor** > **Log Monitoring** > **Syslog Server**.

(2) Set parameters for the Syslog server.



Syslog Server

ⓘ The syslog protocol can be used to send firewall logs to a third-party log analysis platform for unified storage, analysis, and processing.**Note:**When the fast syslog forwarding feature is enabled, it will occupy bandwidth and affect existing network services. Please operate with caution.

Fast Syslog Forwarding

Syslog Server1

* Server IP: Enter an IP address.

* Port: 514

* public.standardProtocolVersion: ● rfc3164 ○ rfc5424

启用该Syslog服务器的日志类型

* 日志类型: Select a syslog log type.

Syslog Server2

Item	Description	Remarks
Server IP	IP address of the Syslog server.	Set this parameter to the IP address of the Syslog server.
Port	Port number for receiving the log notifications.	The default value is 514. The value must be the same as that configured on the Syslog server.
Log Type	Type of the log in the Syslog	Select the log type for which a Syslog

	notification, including system log and security log.	notification needs to be sent.

(3) Click **Save**.

8.4 Traffic Monitoring

8.4.1 Querying Interface Traffic Monitoring

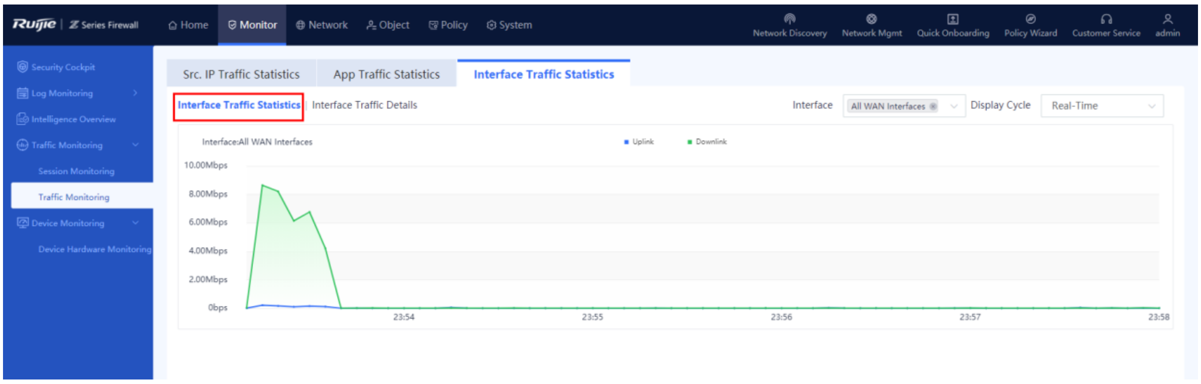
Application Scenario

Interface traffic monitoring is used to display the traffic trend of a device interface and the detailed traffic information of the interface in a certain period of time.

Procedure

(1) Choose **Monitor** > **Traffic Monitoring** > **Interface Traffic Statistics**.

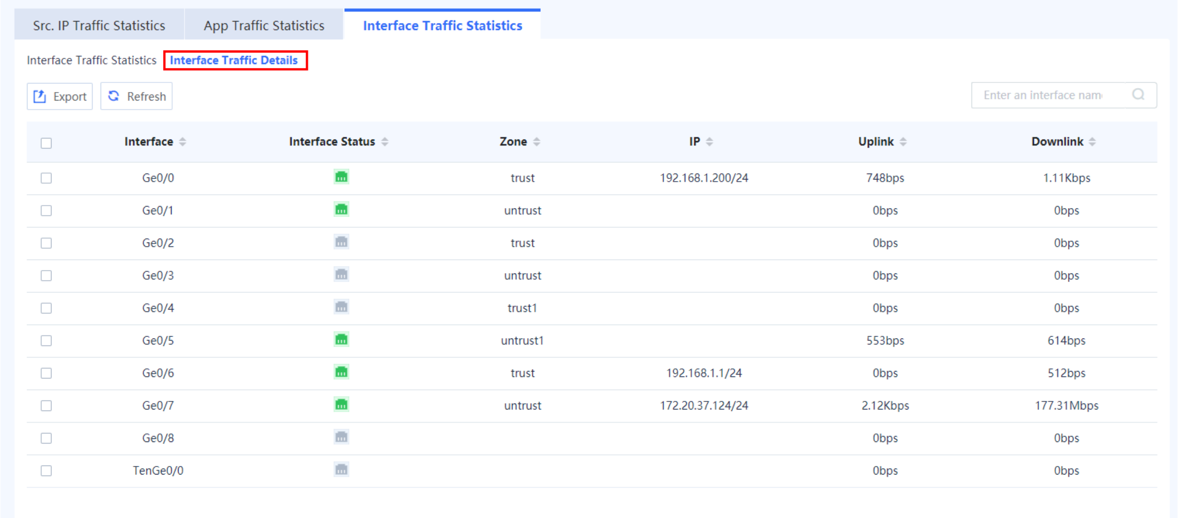
(2) Click **Interface Traffic Statistics**, select the interface to query, and set the query cycle. The system displays the interface traffic trend chart, including the uplink traffic and downlink traffic.



Interface: All WAN Interfaces

Display Cycle: Real-Time

(3) Click **Interface Traffic Details** to view the detailed traffic information of the interface.


Src. IP Traffic Statistics
App Traffic Statistics
Interface Traffic Statistics
Interface Traffic Statistics
Interface Traffic Details
Export
Refresh
Enter an interface nam

☐	Interface	Interface Status	Zone	IP	Uplink	Downlink
☐	Ge0/0	🟩	trust	192.168.1.200/24	748bps	1.11Kbps
☐	Ge0/1	🟩	untrust		0bps	0bps
☐	Ge0/2	⬜	trust		0bps	0bps
☐	Ge0/3	⬜	untrust		0bps	0bps
☐	Ge0/4	⬜	trust1		0bps	0bps
☐	Ge0/5	🟩	untrust1		553bps	614bps
☐	Ge0/6	🟩	trust	192.168.1.1/24	0bps	512bps
☐	Ge0/7	🟩	untrust	172.20.37.124/24	2.12Kbps	177.31Mbps
☐	Ge0/8	⬜			0bps	0bps
☐	TenGe0/0	⬜			0bps	0bps

Follow-up Procedure

- Click **Export** to export interface traffic information to the local device in the Excel format.
- Click **Refresh** to obtain the latest interface traffic information.

8.4.2 Querying Source IP Traffic Statistics

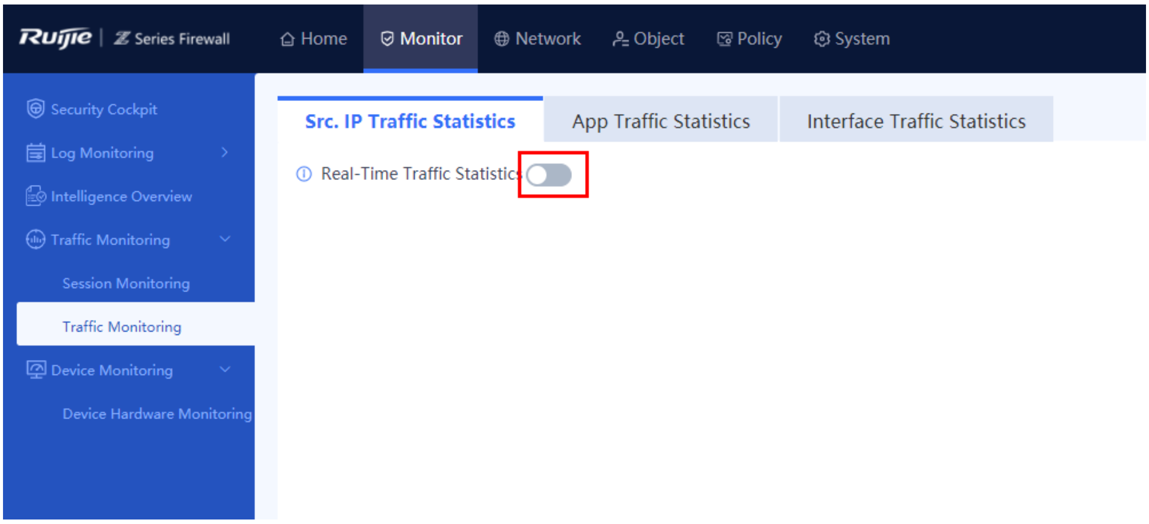
Application Scenario

Source IP traffic statistics collection is used to display the uplink traffic, downlink traffic, and number of sessions based on source IP traffic statistics. This function is disabled by default. After you enable this function, real-time app traffic statistics collection is also enabled, which consumes a high proportion of the device performance. You are advised to enable this function in an off-peak period.

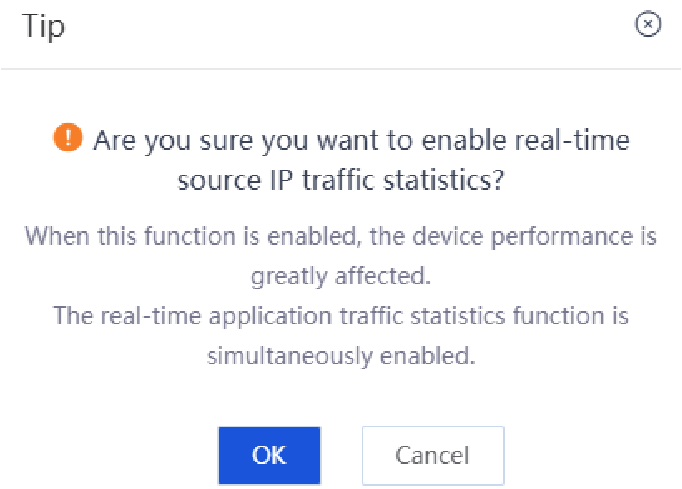
Procedure

(1) Choose **Monitor** > **Traffic Monitoring** > **Src. IP Traffic Statistics**.

(2) Enable **Real-Time Traffic Statistics**.



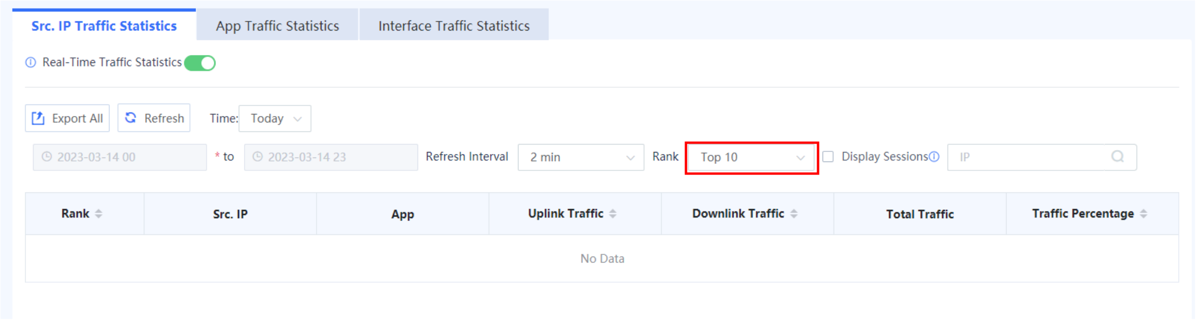
(3) In the dialog box that is displayed, click **OK**.


Tip

Are you sure you want to enable real-time source IP traffic statistics?

When this function is enabled, the device performance is greatly affected.
The real-time application traffic statistics function is simultaneously enabled.

(4) Top 10 source IP addresses with high traffic as well as the source IP address and other information are displayed on the page. You can set **Rank** to **Top 20** to display top 20 source IP addresses with high traffic.



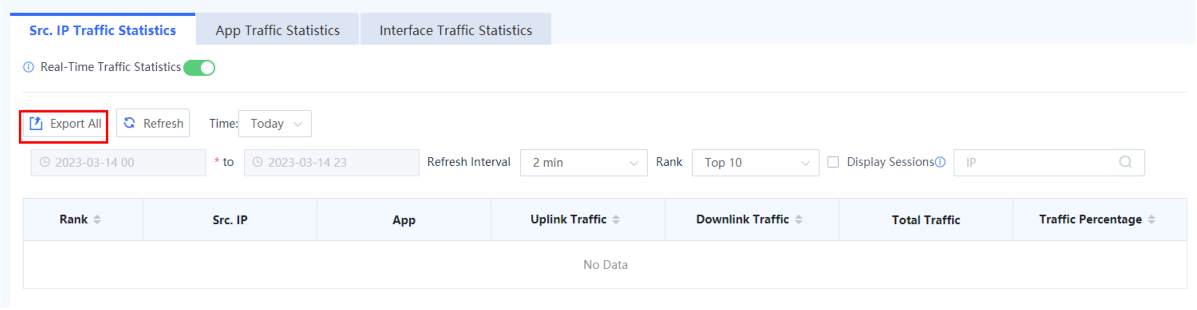
Real-Time Traffic Statistics

Time: Today

2023-03-14 00 * to 2023-03-14 23 Refresh Interval 2 min Rank Top 10

Rank	Src. IP	App	Uplink Traffic	Downlink Traffic	Total Traffic	Traffic Percentage
No Data						

(5) (Optional) Click **Export All** to export the real-time traffic statistics to the local device.



Real-Time Traffic Statistics

Time: Today

2023-03-14 00 * to 2023-03-14 23 Refresh Interval 2 min Rank Top 10 □ Display Sessions

Rank	Src. IP	App	Uplink Traffic	Downlink Traffic	Total Traffic	Traffic Percentage
No Data						

8.4.3 Querying App Traffic Statistics

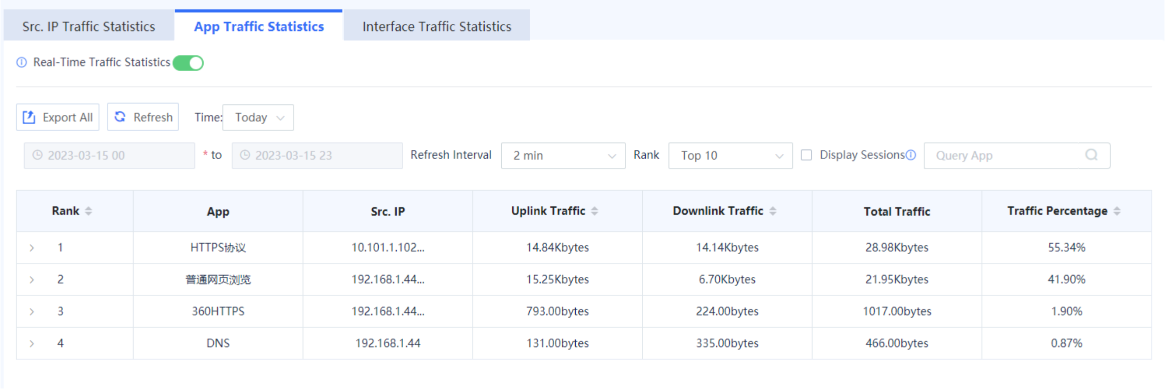
Application Scenario

App traffic statistics collection is used to display the uplink traffic, downlink traffic, and number of sessions by app. This function cannot be enabled or disabled separately. Its enabling or disabling status is the same as that of the source IP traffic statistics collection function.

Procedure

(1) Choose **Monitor** > **Traffic Monitoring** > **App Traffic Statistics**.

(2) Top 10 apps with high traffic as well as the traffic information are displayed on the page. You can set **Rank** to **Top 20** to display top 20 apps with high traffic.



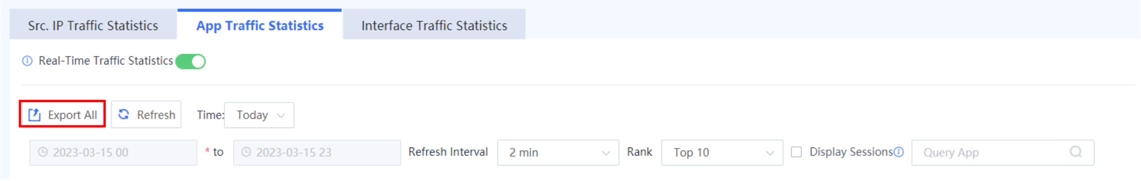
Real-Time Traffic Statistics

Time: Today

2023-03-15 00 * to 2023-03-15 23 Refresh Interval 2 min Rank Top 10 □ Display Sessions

Rank	App	Src. IP	Uplink Traffic	Downlink Traffic	Total Traffic	Traffic Percentage
1	HTTPS协议	10.101.1.102...	14.84Kbytes	14.14Kbytes	28.98Kbytes	55.34%
2	普通网页浏览	192.168.1.44...	15.25Kbytes	6.70Kbytes	21.95Kbytes	41.90%
3	360HTTPS	192.168.1.44...	793.00bytes	224.00bytes	1017.00bytes	1.90%
4	DNS	192.168.1.44	131.00bytes	335.00bytes	466.00bytes	0.87%

(3) (Optional) Click **Export All** to export the real-time traffic statistics to the local device.



Real-Time Traffic Statistics

Time: Today

2023-03-15 00 * to 2023-03-15 23 Refresh Interval 2 min Rank Top 10 □ Display Sessions

8.5 Session Monitoring

8.5.1 Overview

The firewall displays the status of a connection established between two parties in the communication by session. One session indicates a connection between the communicating parties. A session records 5-tuple information (source IP address, source port, destination IP address, destination port, and protocol) of a connection. Packets with the same 5-tuple information belong to the same connection, that is, the same session.

8.5.2 Real-Time Session Information

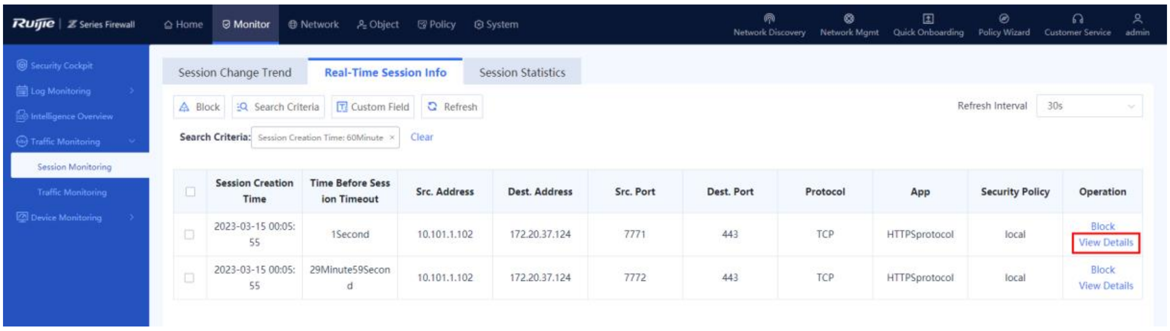
Application Scenario

The real-time session information function is used to collect and display the current number of sessions. You can block a session based on service needs. After a session is blocked, the firewall discards subsequent packets transmitted over this session and the session is no longer displayed on the page.

Procedure

(1) Choose **Monitor** > **Traffic Monitoring** > **Session Monitoring** > **Real-Time Session Info**.

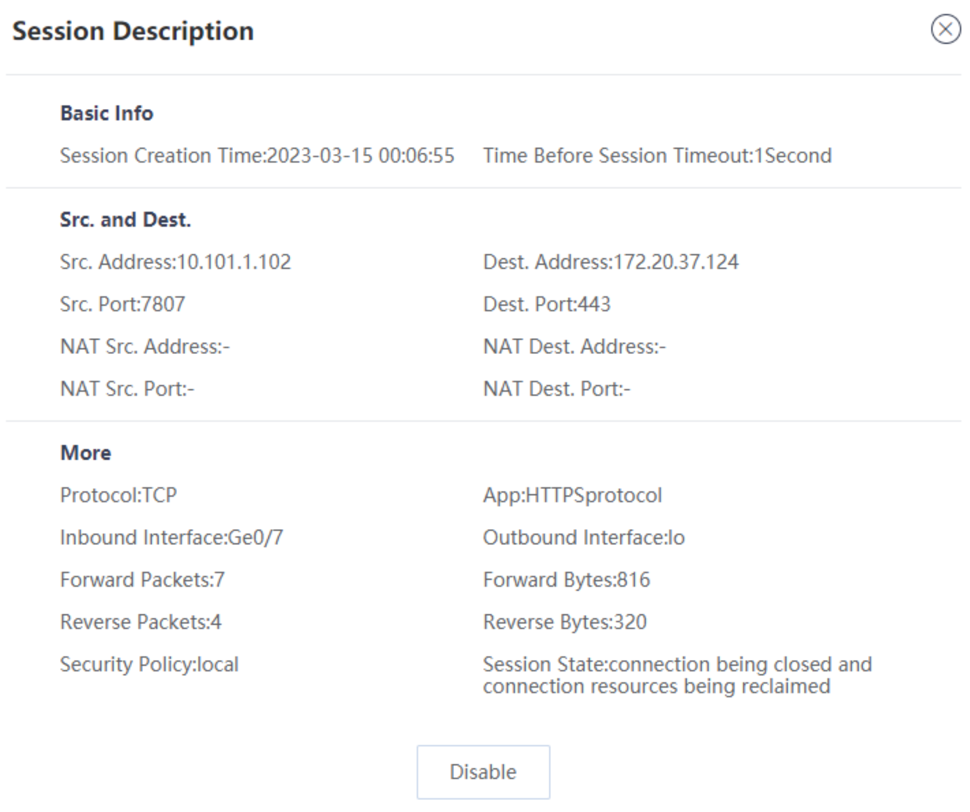
(2) Select the desired session and click **View Details** to view the session creation time, hit security policy, number of forward packets, and number of reverse packets.



Refresh Interval: 30s

Search Criteria: Session Creation Time: 60Minute

□	Session Creation Time	Time Before Session Timeout	Src. Address	Dest. Address	Src. Port	Dest. Port	Protocol	App	Security Policy	Operation
□	2023-03-15 00:05:55	1Second	10.101.1.102	172.20.37.124	7771	443	TCP	HTTPSprotocol	local	Block View Details
□	2023-03-15 00:05:55	29Minute59Second	10.101.1.102	172.20.37.124	7772	443	TCP	HTTPSprotocol	local	Block View Details



Session Description

Basic Info

Session Creation Time:2023-03-15 00:06:55

Time Before Session Timeout:1Second

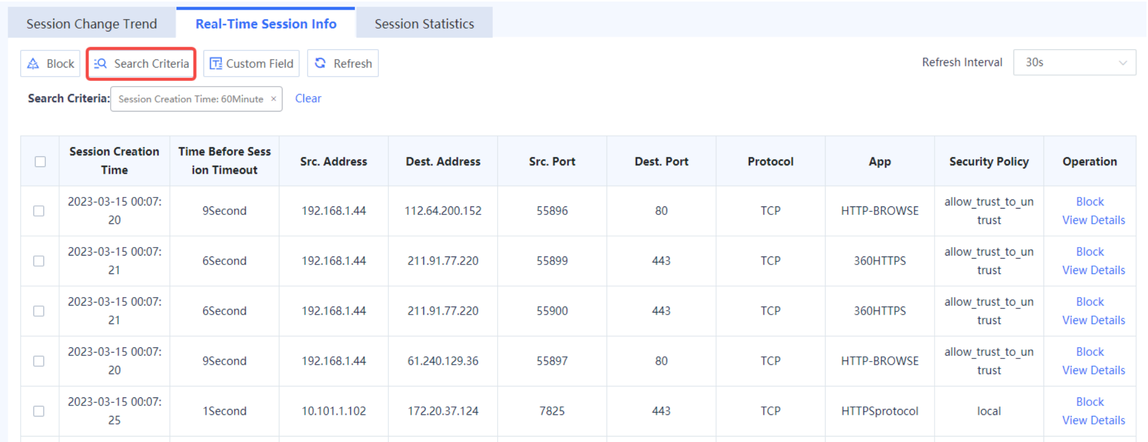
Src. and Dest.

Src. Address:10.101.1.102	Dest. Address:172.20.37.124
Src. Port:7807	Dest. Port:443
NAT Src. Address:-	NAT Dest. Address:-
NAT Src. Port:-	NAT Dest. Port:-

More

Protocol:TCP	App:HTTPSprotocol
Inbound Interface:Ge0/7	Outbound Interface:lo
Forward Packets:7	Forward Bytes:816
Reverse Packets:4	Reverse Bytes:320
Security Policy:local	Session State:connection being closed and connection resources being reclaimed

(3) (Optional) Click **Search Criteria** to set the criteria for filtering sessions.

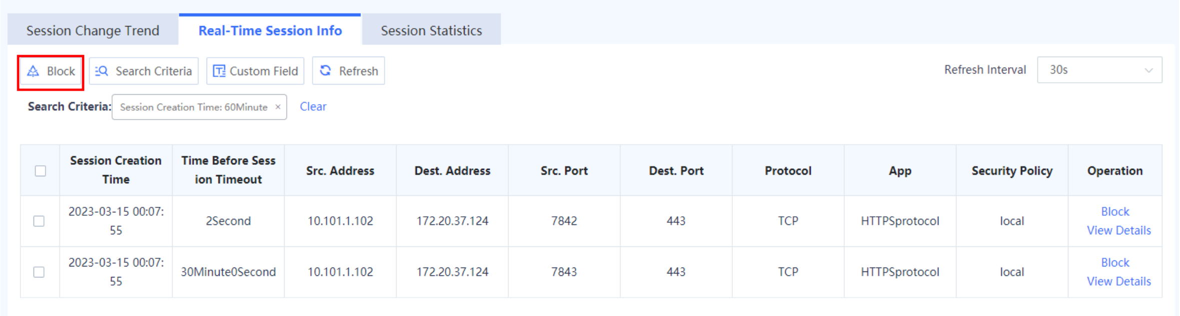


Refresh Interval 30s

Search Criteria: Session Creation Time: 60Minute × Clear

☐	Session Creation Time	Time Before Session Timeout	Src. Address	Dest. Address	Src. Port	Dest. Port	Protocol	App	Security Policy	Operation
☐	2023-03-15 00:07:20	9Second	192.168.1.44	112.64.200.152	55896	80	TCP	HTTP-BROWSE	allow_trust_to_untrust	Block View Details
☐	2023-03-15 00:07:21	6Second	192.168.1.44	211.91.77.220	55899	443	TCP	360HTTPS	allow_trust_to_untrust	Block View Details
☐	2023-03-15 00:07:21	6Second	192.168.1.44	211.91.77.220	55900	443	TCP	360HTTPS	allow_trust_to_untrust	Block View Details
☐	2023-03-15 00:07:20	9Second	192.168.1.44	61.240.129.36	55897	80	TCP	HTTP-BROWSE	allow_trust_to_untrust	Block View Details
☐	2023-03-15 00:07:25	1Second	10.101.1.102	172.20.37.124	7825	443	TCP	HTTPSprotocol	local	Block View Details

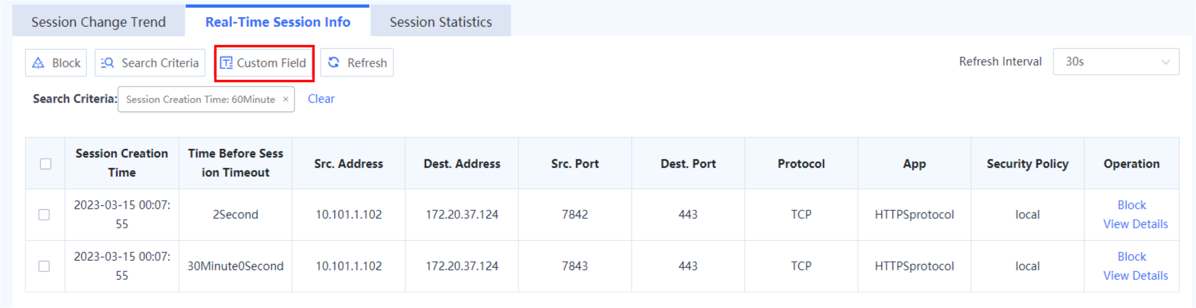
(4) (Optional) Select one or more sessions and click **Block** to block the selected sessions.



Search Criteria: Session Creation Time: 60Minute × Clear

☐	Session Creation Time	Time Before Session Timeout	Src. Address	Dest. Address	Src. Port	Dest. Port	Protocol	App	Security Policy	Operation
☐	2023-03-15 00:07:55	2Second	10.101.1.102	172.20.37.124	7842	443	TCP	HTTPSprotocol	local	Block View Details
☐	2023-03-15 00:07:55	30Minute0Second	10.101.1.102	172.20.37.124	7843	443	TCP	HTTPSprotocol	local	Block View Details

(5) (Optional) Click **Custom Field** to set the session fields to be displayed on the page.



Search Criteria: Session Creation Time: 60Minute × Clear

☐	Session Creation Time	Time Before Session Timeout	Src. Address	Dest. Address	Src. Port	Dest. Port	Protocol	App	Security Policy	Operation
☐	2023-03-15 00:07:55	2Second	10.101.1.102	172.20.37.124	7842	443	TCP	HTTPSprotocol	local	Block View Details
☐	2023-03-15 00:07:55	30Minute0Second	10.101.1.102	172.20.37.124	7843	443	TCP	HTTPSprotocol	local	Block View Details

8.5.3 Session Statistics Collection

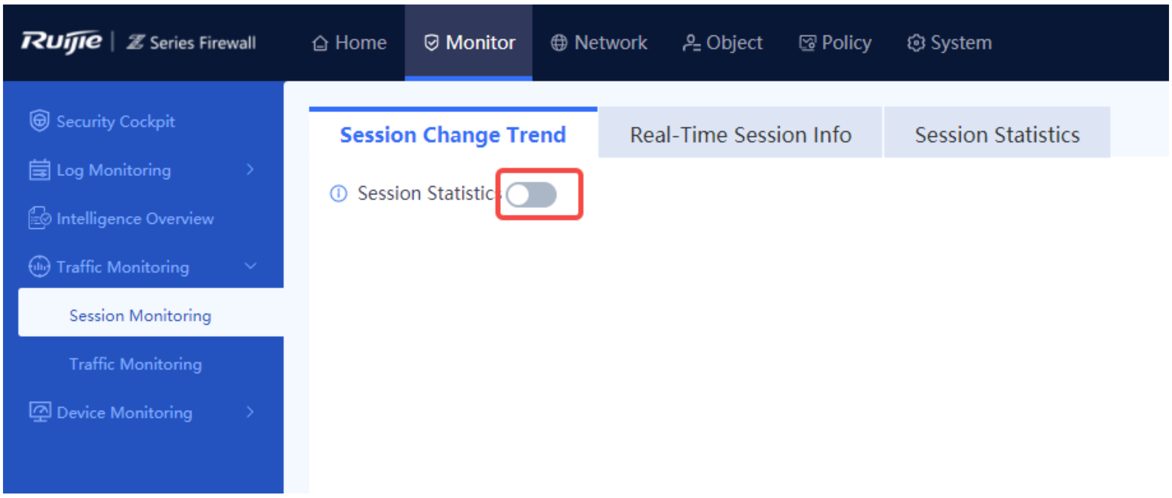
Application Scenario

The session statistics collection function is used to collect the total number of sessions, number of TCP sessions, and number of UDP sessions established for each source IP address and the number of sessions added per second. Enabling this function consumes a high proportion of the device performance. You are advised to enable this function in an off-peak period.

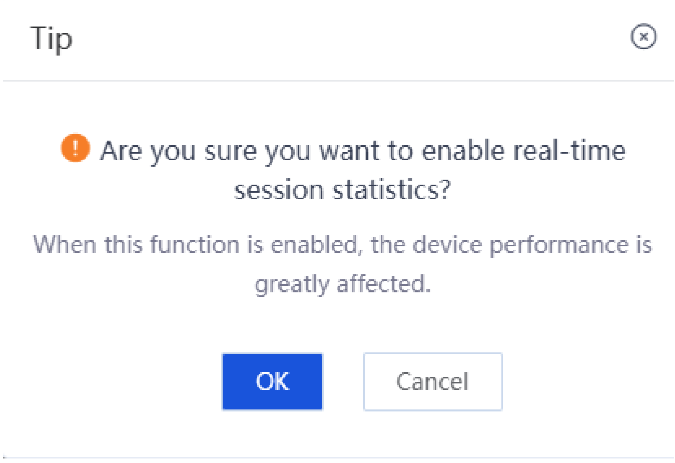
Procedure

(1) Choose **Monitor** > **Session Monitoring** > **Session Change Trend**.

(2) Enable **Session Statistics**.



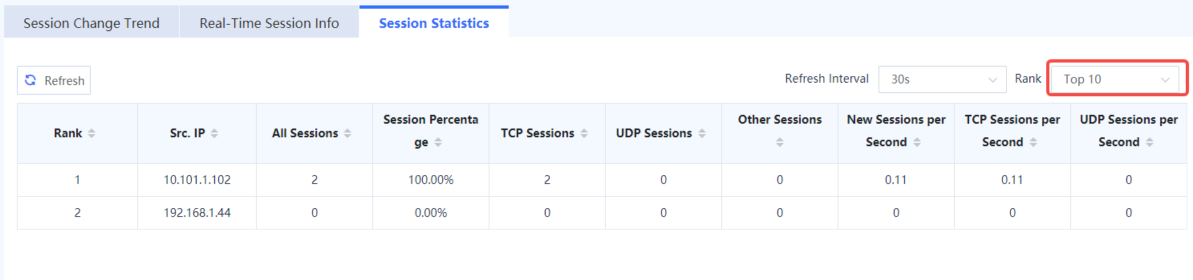
(3) In the dialog box that is displayed, click **OK**.


Tip

Are you sure you want to enable real-time session statistics?

When this function is enabled, the device performance is greatly affected.

(4) Click the **Session Statistics** tab to view top 10 source IP addresses with high session quantity as well as the session information. You can set **Rank** to **Top 20** to display top 20 source IP addresses with high session quantity.



Refresh Interval 30s Rank Top 10

Rank	Src. IP	All Sessions	Session Percentage	TCP Sessions	UDP Sessions	Other Sessions	New Sessions per Second	TCP Sessions per Second	UDP Sessions per Second
1	10.101.1.102	2	100.00%	2	0	0	0.11	0.11	0
2	192.168.1.44	0	0.00%	0	0	0	0	0	0

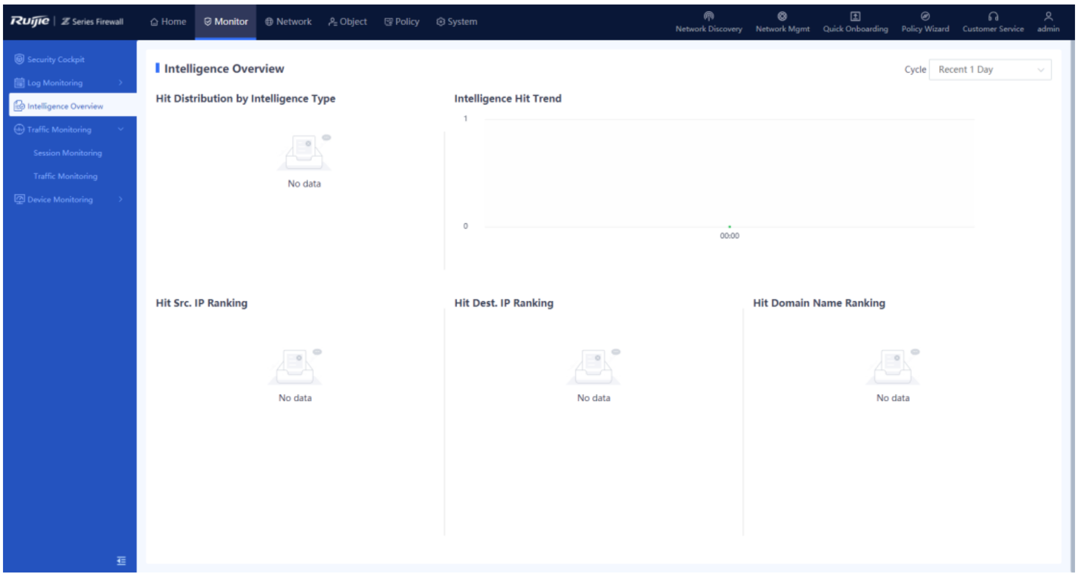
8.6 Intelligence Overview

Application Scenario

The intelligence overview function is used to display the hit distribution by intelligence type and the intelligence hit trend. This information can help administrators effectively master threats in the current network environment and then develop more refined protection policies to protect LAN hosts.

Procedure

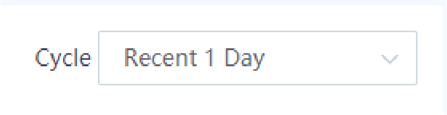
(1) Choose **Monitor** > **Intelligence Overview**.



Intelligence Overview

Cycle: Recent 1 Day

(2) Click the drop-down list box in the upper right corner of the page and set a cycle for collecting intelligence hit statistics. The system displays the intelligence hit data in the specified cycle.



Cycle: Recent 1 Day

(3) View the intelligence hit data on the page. The information consists of five parts as listed in the following table.

Item	Description
Hit Distribution	Displays hit distribution by intelligence type in a pie chart. This information

by Intelligence Type	allows administrators to master major threats in the current network environment so that they can intensify protection accordingly. Move the pointer over this area to view the number of hits of each intelligence type and the proportion.
Intelligence Hit Trend	Displays the number of hits of threat intelligence in various periods within the statistical cycle in a line chart. This information helps administrators find periods with high occurrence of attack threats or check whether protection measures are effective. Move the pointer over the line chart to view the number of hits over each period.
Hit Src. IP Ranking	Displays the ranking of source IP addresses with threat intelligence by the number of hits. This information helps administrators analyze the threat source and then develop corresponding protection measures to block the traffic from these source IP addresses. Click an IP address to switch to the security log page. Security logs of this source IP address are automatically filtered out.
Hit Dest. IP Ranking	Displays the ranking of destination IP addresses with threat intelligence by the number of hits. This information helps administrators analyze addresses of compromised hosts on the botnet or IP addresses attacked by malicious programs and then develop corresponding protection measures to protect these hosts. Click an IP address to switch to the security log page. Security logs of this destination IP address are automatically filtered out.
Hit Domain Name Ranking	Displays the ranking of domain name addresses with threat intelligence by the number of hits. This information helps administrators analyze malicious domain names and then develop corresponding protection measures to block and protect the traffic from these domain names. Click a domain name to switch to the security log page. Security logs of this domain name are automatically filtered out.

9 Advanced Features

9.1 ALG

9.1.1 Overview

Application Level Gateway (ALG) analyzes application layer packet information using the multi-channel protocol and performs address translation on the IP address, port number, and special fields in the payload to ensure correct communication at the application layer. For special applications such as TFTP and FTP, data ports must be randomly enabled according to the session process. The Z-S series firewall can identify these protocols and dynamically enable or disable ports during the session control process to guarantee application availability to the maximum extent.

Related Concepts

- Session: A session records packet exchange information at the transport layer, including the source IP address, source port, destination IP address, destination port, protocol type, and VPN instance to which the source/destination IP address belongs. Exchange information of the same packet belongs to the same flow. One session corresponds to two flows in the forward and reverse directions.
- Dynamic channel: When an application layer protocol packet contains address information, the address information is used to set up a dynamic channel. After that, packets from this address are automatically transmitted over this dynamic channel.

Technical Principles

The ALG feature can be used with the NAT feature to implement address translation on the packet payload and be used with the Application Specific Packet Filter (ASPF) feature to implement dynamic channel detection and application layer status detection.

For a multi-channel application protocol, address information in the data payload of IP packets must be translated to ensure successful setup of subsequent dynamic channel on a NAT-enabled network. The role of ALG is to implement address translation on the payload.

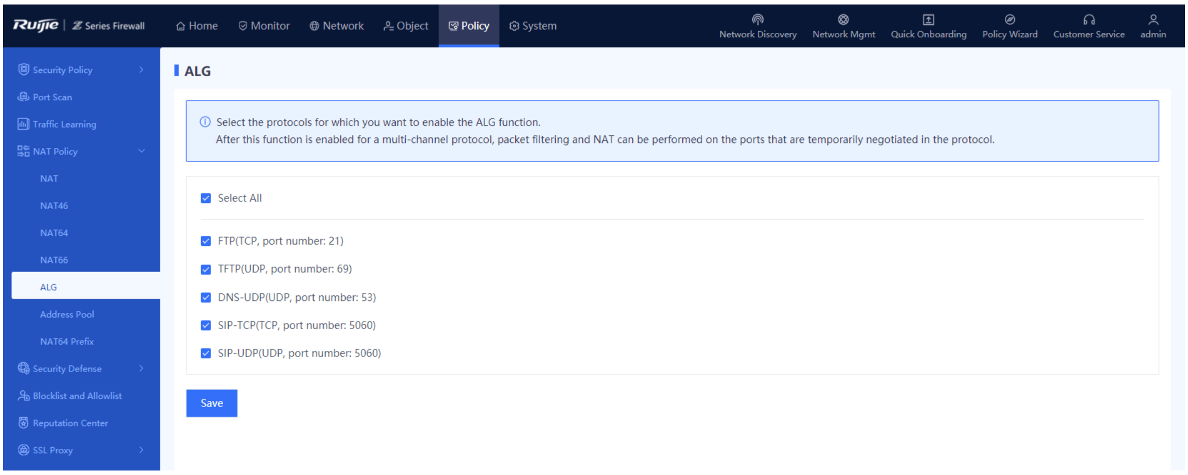
9.1.2 Configuring ALG

Application Scenario

ALG guarantees normal packet filtering and NAT based on the temporarily negotiated port number when a multi-channel protocol is used for data transmission.

Procedure

(1) Choose **Policy** > **NAT Policy** > **ALG**.



ALG

Select the protocols for which you want to enable the ALG function.
After this function is enabled for a multi-channel protocol, packet filtering and NAT can be performed on the ports that are temporarily negotiated in the protocol.

☑ Select All

☑ FTP(TCP, port number: 21)

☑ TFTP(UDP, port number: 69)

☑ DNS-UDP(UDP, port number: 53)

☑ SIP-TCP(TCP, port number: 5060)

☑ SIP-UDP(UDP, port number: 5060)

(2) Select the protocol names for which ALG needs to be enabled and click **Save**.

After the ALG function is enabled, information in the packets of these protocols can be translated by NAT.

10 FAQs

10.1 Product Knowledge

10.1.1 What Is the Hardware Architecture of the RG-WALL 1600-Z-S Series Firewall?

The RG-WALL 1600-Z-S series firewall uses a hardware architecture with multi-core CPU and multiple ASIC chips. With the onboard design for the CPU memory, the firewall supports ECC, hardware flow attack defense, dual-boot instruction to reduce the probability of device start failures caused by boot problems. The design of multiple ASIC chips enables the firewall to support eight electrical ports, two GE optical ports, and four 10GE optical ports.

The performance of the RG-WALL 1600-Z-S series firewall can be expanded through license authorization, capable for all the 3G–10G forwarding scenarios. Apart from software performance expansion, the hardware can also be well expanded. The firewall supports two expansion slots and can be expanded to support 40GE port, 4GE electrical port + 4GE optical port, redundant power modules, and 1 TB hard disk.

The overall hardware design adopts the area-based power solution to avoid whole machine restart caused by short circuit of the USB drive or optical module.

10.1.2 What Are the Restrictions of Port MGMT?

It is not recommended to use port MGMT as a service port, and port MGMT cannot be configured to work in transparent or off-path mode.

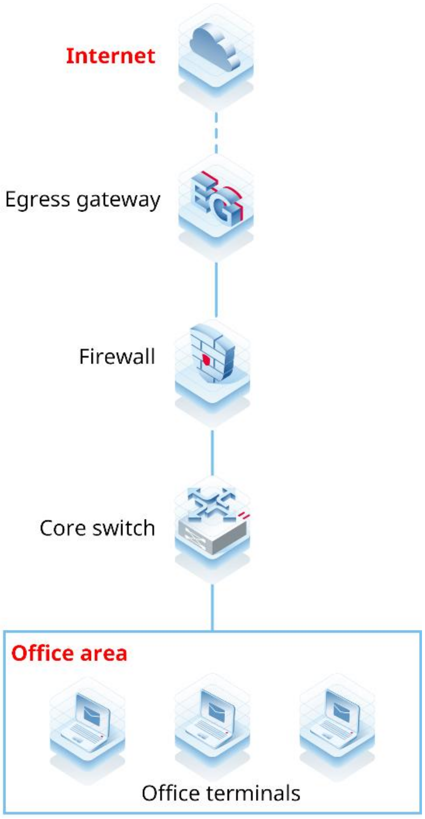
10.2 Firewall Deployment

10.2.1 What Firewall Deployment Modes Are Supported?

As a security device used to protect the network infrastructure, the Z-S series firewall can be widely used on various types of networks. The Z-S series firewall supports multiple deployment modes and network features to adapt to diversified network environments. The major deployment modes of the Z-S series firewalls include:

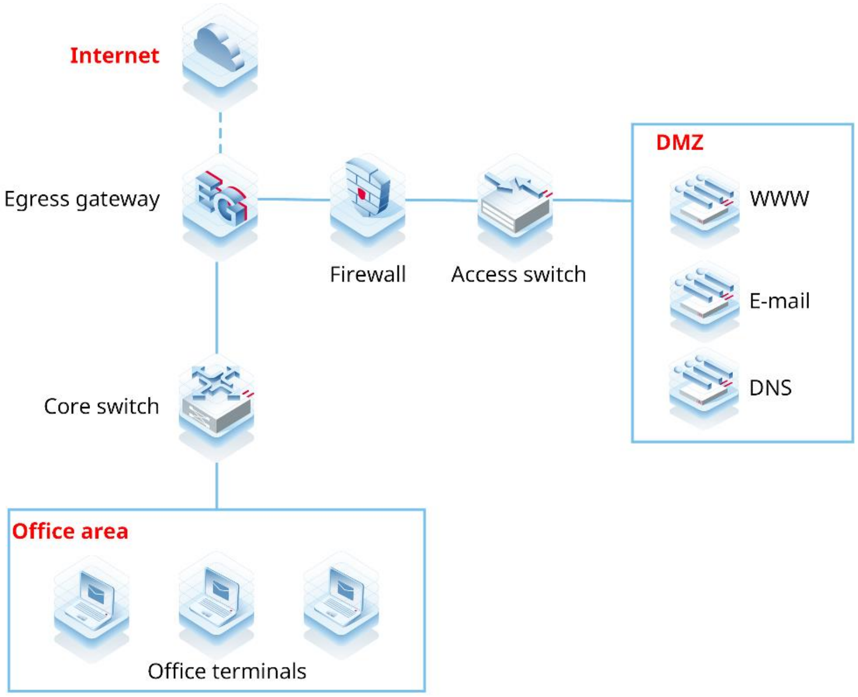
- Transparent mode - office network egress link - single-in single-out

  Scenario overview: The firewall is transparently deployed between the egress gateway and core switch through one GE electrical port on each side. Access control policies, IPS policies, DDoS policies, and application control policies are enabled on the firewall to control and protect assets on the public network.



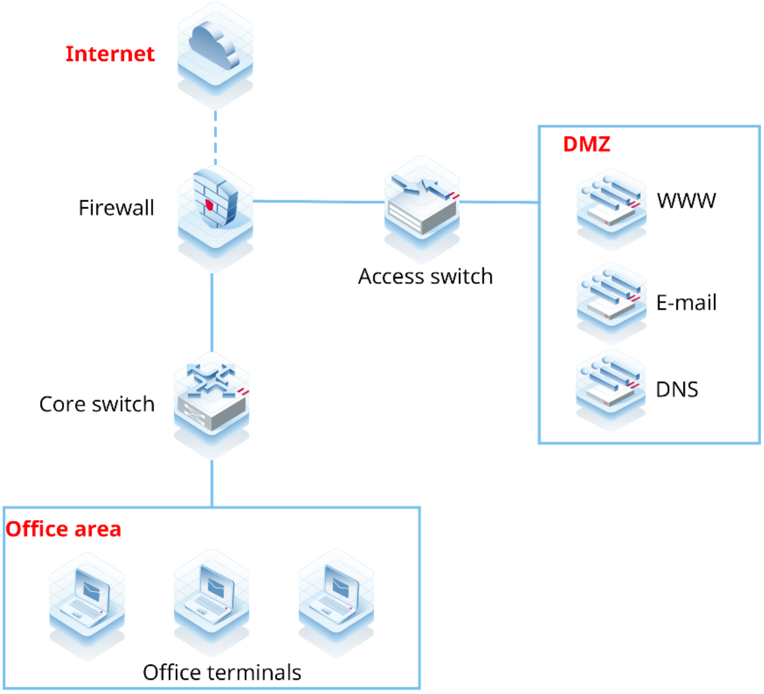
- Transparent mode – area boundary - single-in single-out

Scenario overview: The firewall is transparently deployed at an area boundary (such as the DMZ) between the egress gateway and access switch through one GE electrical port on each side. The firewall generates refined access control policies for users through port scan and traffic learning and is enabled with IPS, DDoS, and application control to control and protect assets (such as servers providing services to external users) in an area.



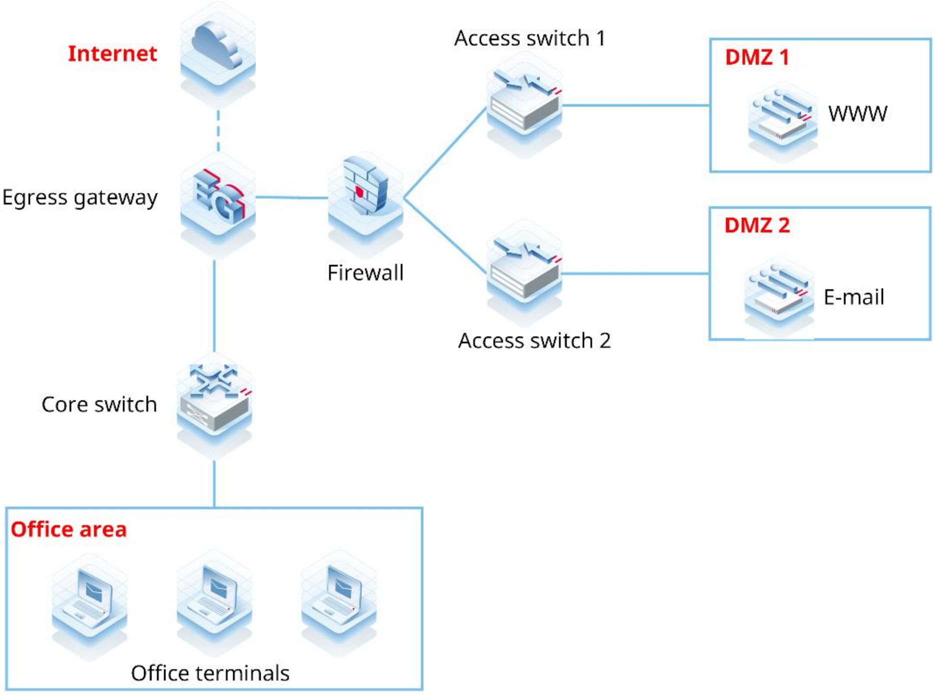
- Gateway mode - single ISP access

  Scenario overview: The firewall is deployed at the Internet egress in gateway mode and is connected to a single ISP. The WAN GE port is configured with DHCP or a fixed IP address. The firewall connects to the LAN office area and the DMZ server area through GE electrical ports. NAT and DHCP are enabled on the firewall to allow office terminals to access the Internet. Access control policies, IPS policies, DDoS policies, and application control policies are enabled on the firewall through port scan and traffic learning to control and protect assets and servers on the office network.



- Transparent mode - multi-in single-out

  Scenario overview: The firewall is transparently deployed on the network. It connects to the LAN areas through multiple ports and connects to the Internet through the same WAN port to provide services to external users.



10.2.2 Can GE Optical Port and 10GE Optical Port Form a Bridge?

The GE optical port and 10GE optical port can form a bridge.

10.3 Typical Feature Configuration

10.3.1 How Is Source NAT Implemented?

Source NAT means source network address translation for packets, which is implemented through NAT policies. You need to specify the source security zone, source address, destination security zone, destination address, and data packet after translation in a NAT policy.

10.3.2 Does the Firewall Support Link Detection?

The firewalls running NTOS1.0R3 and later versions support link detection.

10.3.3 Does the Z-S Series Firewall Block TCP Sessions in the Secondary Traversal Scenario?

No. However, if the same packet flow traverses the firewall for a second time, secondary authentication of SYN-Cookie will be triggered if SYN flood attack defense (DDoS attack defense) is enabled, causing TCP connection setup failure.

10.3.4 Does the Firewall Support Port Aggregation?

The firewalls running NTOS1.0R4 and later versions support port aggregation.

10.4 Login Management

10.4.1 What Can I Do If I Fail to Log In to the Web Page?

Possible Causes

- The firewall is not fully started.
- A network connection error occurs between the PC and firewall.
- The address https://*Device IP address* is incorrect. (The default address https://192.168.1.200 can be used.)
- The browser is incompatible.

Solution

(1) Wait for about 2 minutes until the firewall is started. Observe indicators (including PWR, SYS, and interface status indicators) on the firewall until all of them are on and try again.

(2) Check the Link/ACT indicator on the interface. If the indicator is blinking green or steady on, the connection is normal. Check whether the IP addresses of the PC and firewall are on the same network segment. (The default address 192.168.1.9 can be used.)

(3) Confirm that the address (https://*Device IP address*) entered in the address bar is correct. (The default address https://192.168.1.200 can be used.)

(4) Change the browser.

10.4.2 What Can I Do If I Fail to Log In to the System Through SSH?

Possible Causes

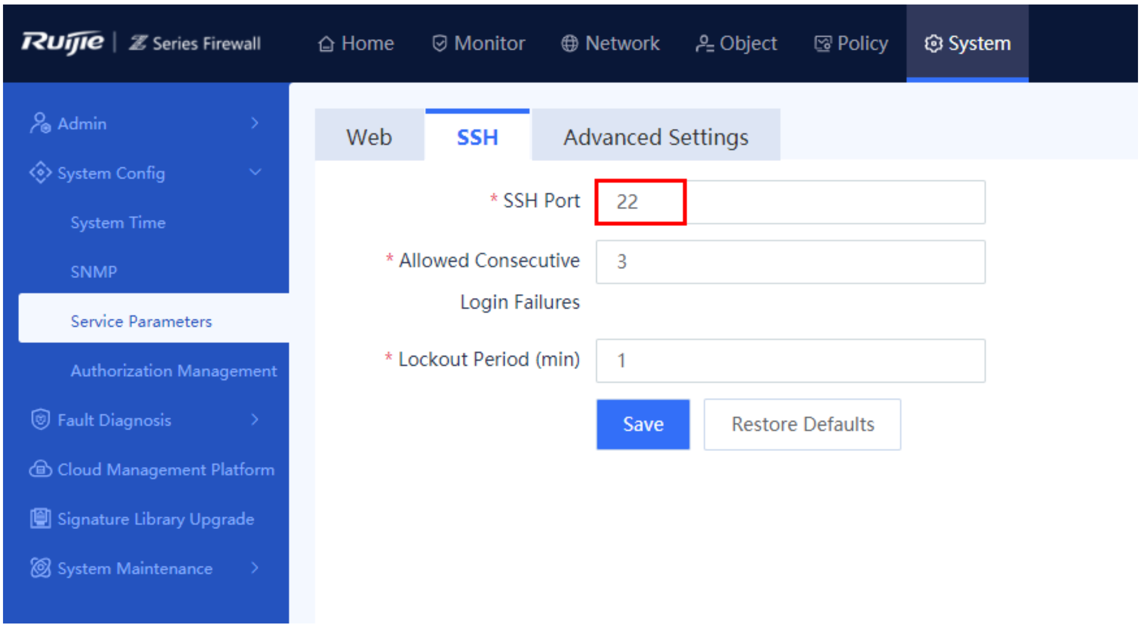
The SSH port number is incorrect.

Solution

(1) Check the network connection.

(2) If the network connection is normal, choose **System** > **System Config** > **Service Parameters** > **SSH** and modify the SSH port number.

Figure 10-1Modifying the SSH Port Number



* SSH Port: 22

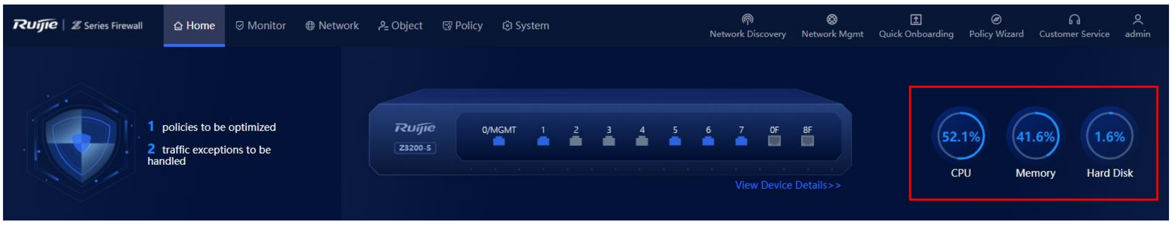
* Allowed Consecutive Login Failures: 3

* Lockout Period (min): 1

10.5 O&M and Monitoring

10.5.1 How Do I View the CPU, Memory, and Hard Disk Information of the Firewall?

Log in to the web management page, and view the CPU, memory, and hard disk usage on the home page.



1 policies to be optimized

2 traffic exceptions to be handled

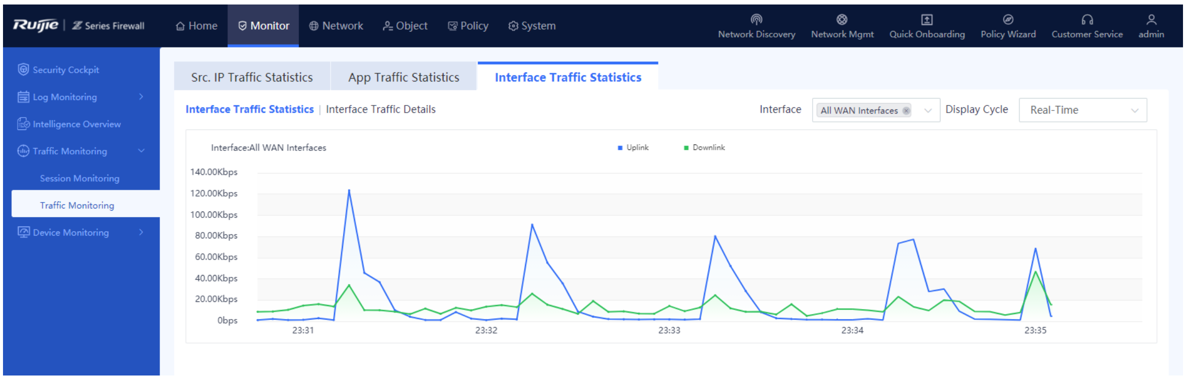
52.1% CPU

41.6% Memory

1.6% Hard Disk

10.5.2 How Do I View the Interface Traffic of the Firewall?

Log in to the web management page, choose **Monitor** > **Traffic Monitoring** > **Traffic Monitoring** > **Interface Traffic Statistics**, and view the interface traffic.



Interface: All WAN Interfaces

Display Cycle: Real-Time

Interface:All WAN Interfaces

Select an interface and set the display cycle to view the real-time traffic or traffic trend of the interface.

11 Troubleshooting

11.1 Security Policy

11.1.1 Principle

(1) The NGFW uses security policies to control data flows in a unified manner and facilitate user configuration and management. Security policies can be configured on the firewall to effectively control and manage data flows passing through it.

(2) After a firewall receives a data packet, the firewall matches the packet information including the direction, source address, destination address, protocol, and port number with security policies configured by the user to determine whether to set up a data flow. After a data flow is set up, the firewall associates the data flow with a policy to permit or discard subsequent packets transmitted over this data flow. You can determine whether to perform Layer 7 service processing on the permitted data flows.

(3) Layer 7 service processing means that the firewall can block data flows or generate alarms based on the IPS and virus protection rules. The firewall permits data flows that do not match any IPS or virus protection rule.

(4) If no security policy is configured, the system has a default policy in which all items are set to **any** and the action is **Deny**. In this case, the firewall blocks all the data flows passing through it.

(5) Security policies are matched from up down to process data flows passing through the firewall. They do not apply to data flows destined to the firewall or data flows sent by the firewall.

11.1.2 Configuration Points of Security Policies

Basic elements of a security policy include matching condition and action. Matching conditions include the data flow direction, source address, destination address, service, and policy effective time range.

The data flow direction is determined by the source security zone and destination security zone, while the source address, destination address, service, and time range can directly reference defined objects.

(1) Source security zone: Incoming direction of a data flow, which must be a defined security zone. The value **any** indicates all security zones.

(2) Source address: Source address of a data flow, which can be referenced from a defined address object or address group object. The value **any** indicates any source address.

(3) Destination security zone: Outgoing direction of a data flow, which must be a defined security zone. The value **any** indicates all interfaces.

(4) Destination address: Destination address of a data flow, which can be referenced from a defined address object or address group object or be referenced from a virtually mapped IP address.

(5) Policy effective time range: Time when a policy takes effect, which can be referenced from a configured time object. The value **any** indicates all the time.

(6) Service: Service attributes of a data flow, including the protocol, source port, and destination port, which can be referenced from a system pre-defined service or a defined service object or service group object. The value **any** indicates all services.

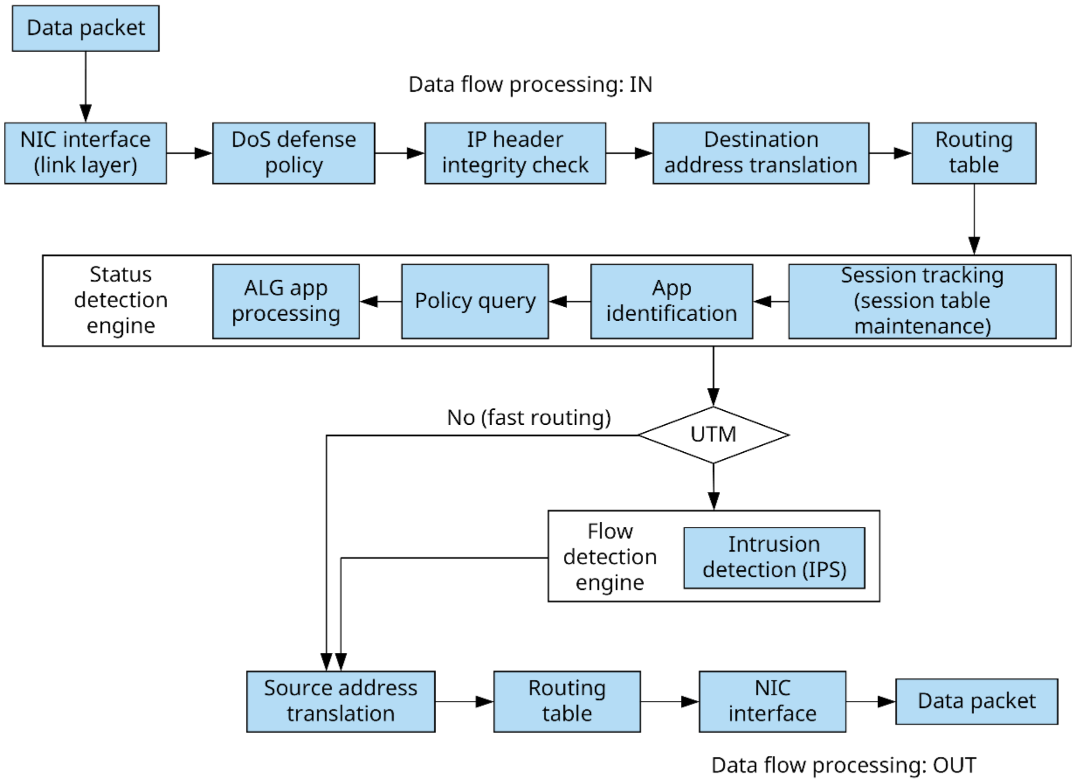
(7) Application: Application type of a data flow. The value **any** indicates any application.

(8) Action: Action performed on data flows meeting the matching conditions. The action can be **Permit** or **Deny**.

(9) Content security: Content template that can be selected for permitted data flows. The firewall matches the data flows based on rules in the selected template. Currently, only URL filtering, intrusion prevention, and virus protection templates are supported.

11.2 Data Packet Processing

The following figure shows data packet processing of the firewall.



(1) Interface (NIC interface)

The NIC interface drive is responsible for receiving data packets and forwarding the packets to the next node.

(2) DoS sensor (DoS defense, disabled by default)

The DoS sensor is responsible for filtering out DoS attacks such as SYN flood, UDP flood, and ICMP flood and limiting the number of concurrent connections of the specified source or destination IP address.

(3) IP header integrity check

The firewall checks the integrity of the data packet header.

(4) DNAT (destination NAT)

The firewall checks the destination IP address in the data packet. If the destination IP address is in the VIP (destination NAT) table, the firewall translates the destination IP address into a mapped IP address (real IP address) and port number.

(5) Routing

The firewall determines the outbound interface of the data packet based on the destination IP address.

(6) Stateful inspection engine

The stateful inspection engine consists of the following components:

- Policy lookup

  In the session setup stage, the firewall determines whether to allow data to pass, sets up a session statue, and determines whether to send the data to the flow-based inspection engine based on whether the policy is associated with a content template.

- Session track

  The firewall maintains the session table and tracks the session status, NAT, and other relevant functions. After a session is set up, the firewall no longer matches policies for subsequent data packets but directly forwards the packets based on the session status.

- Session helpers (that is, ALG)

The firewall can dynamically enable policies, be enabled with NAT, automatically modify the payload, and take other measures to ensure normal communication of special applications such as FTP and TFTP.

(7) Flow-based inspection engine

If IPS is enabled in a firewall policy, the flow-based inspection engine takes over to process subsequent data packets of a session.

(8) Source NAT

If NAT is enabled in a policy, the firewall translates the source IP address and source port of a data packet into the destination interface address or an IP address in an IP address pool (usually a public network IP address).

(9) Routing

The firewall determines the outbound interface of a data packet and forwards the data packet using the routing engine.

(10) Egress

The NIC of the flow outbound interface sends the data packet out of the firewall.

11.3 Diagnostic Center

Application Scenario

The diagnostic center integrates various functions including traffic receiving detection, basic configuration (security policy and NAT policy) detection, packet tracing, and traffic forwarding detection and provides a standard troubleshooting roadmap to help you locate network faults with one click. It also offers explicit and practicable recommendations to achieve efficient and easy network troubleshooting.

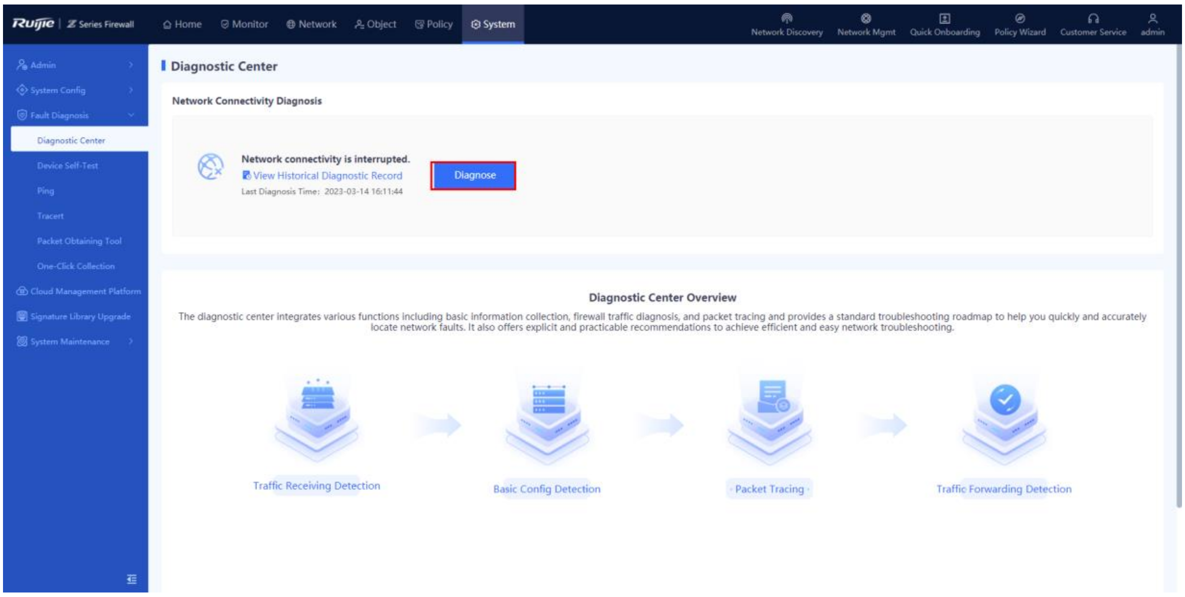
Note

The diagnostic center function is supported from NTOS1.0R3. If your version is lower than NTOS1.0R3, upgrade it to NTOS1.0R3 or higher.

Procedure

(1) Choose **System** > **Fault Diagnosis** > **Diagnostic Center**.

(2) Click **Diagnose**.



Diagnostic Center

Network Connectivity Diagnosis

Network connectivity is interrupted.

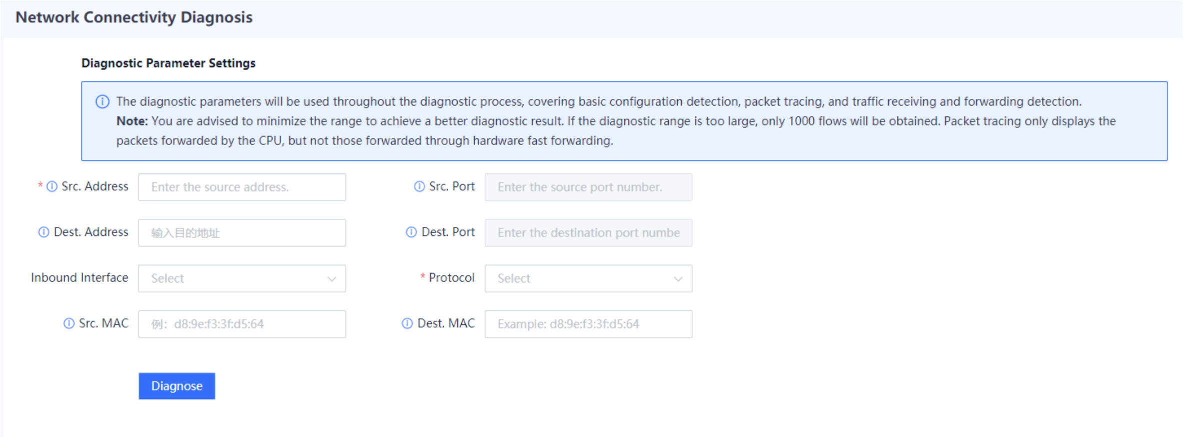
View Historical Diagnostic Record

Last Diagnosis Time: 2023-03-14 16:11:44

Diagnostic Center Overview

The diagnostic center integrates various functions including basic information collection, firewall traffic diagnosis, and packet tracing and provides a standard troubleshooting roadmap to help you quickly and accurately locate network faults. It also offers explicit and practicable recommendations to achieve efficient and easy network troubleshooting.

(3) Enter the source/destination IP address, source/destination port, source/destination MAC address, inbound interface, and protocol, and click **Diagnose**. The firewall checks the network connectivity between the specified source and destination IP addresses.



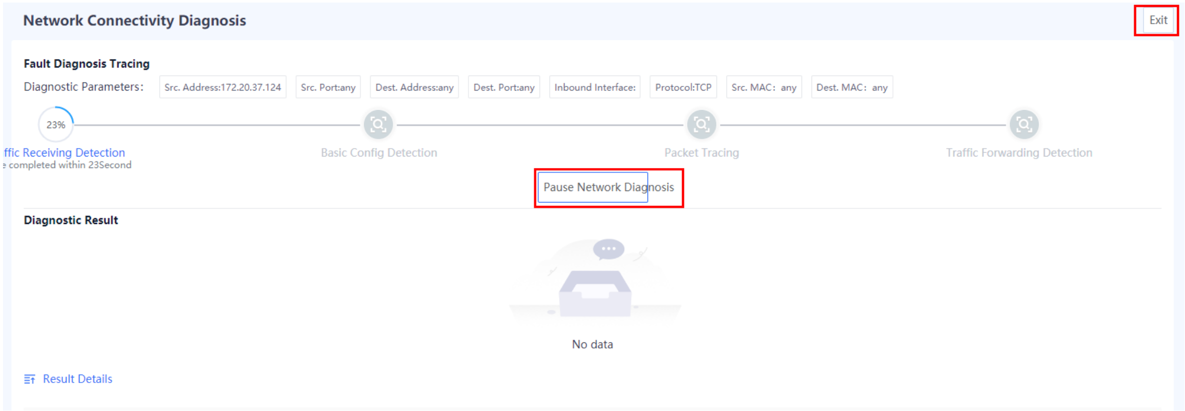
Network Connectivity Diagnosis

Diagnostic Parameter Settings

ⓘ The diagnostic parameters will be used throughout the diagnostic process, covering basic configuration detection, packet tracing, and traffic receiving and forwarding detection.
Note: You are advised to minimize the range to achieve a better diagnostic result. If the diagnostic range is too large, only 1000 flows will be obtained. Packet tracing only displays the packets forwarded by the CPU, but not those forwarded through hardware fast forwarding.

* ⓘ Src. Address	Enter the source address.	ⓘ Src. Port	Enter the source port number.
ⓘ Dest. Address	输入目的地址	ⓘ Dest. Port	Enter the destination port numbe
Inbound Interface	Select	* Protocol	Select
ⓘ Src. MAC	例：d8:9e:f3:3f:d5:64	ⓘ Dest. MAC	Example: d8:9e:f3:3f:d5:64

(4) (Optional) Stop diagnosis or exit the diagnostic task at any time if required.



Network Connectivity Diagnosis

Exit

Fault Diagnosis Tracing

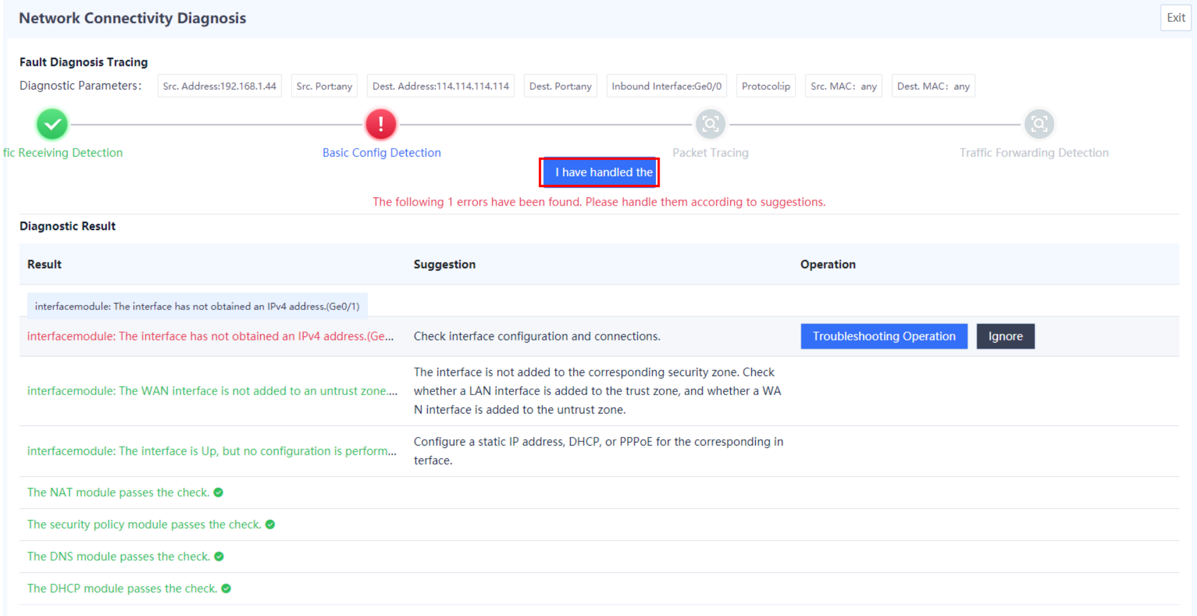
Diagnostic Parameters: Src. Address:172.20.37.124 | Src. Port:any | Dest. Address:any | Dest. Port:any | Inbound Interface: | Protocol:TCP | Src. MAC: any | Dest. MAC: any

Diagnostic Result

No data

Result Details

(5) After the diagnosis is complete, the diagnostic result and diagnostic details are displayed in the lower part of the page. After you troubleshoot the fault based on the diagnostic details, click **I have handled the problem**.



Network Connectivity Diagnosis

Exit

Fault Diagnosis Tracing

Diagnostic Parameters: Src. Address:192.168.1.44 | Src. Port:any | Dest. Address:114.114.114.114 | Dest. Port:any | Inbound Interface:Ge0/0 | Protocol:ip | Src. MAC: any | Dest. MAC: any

The following 1 errors have been found. Please handle them according to suggestions.

Diagnostic Result

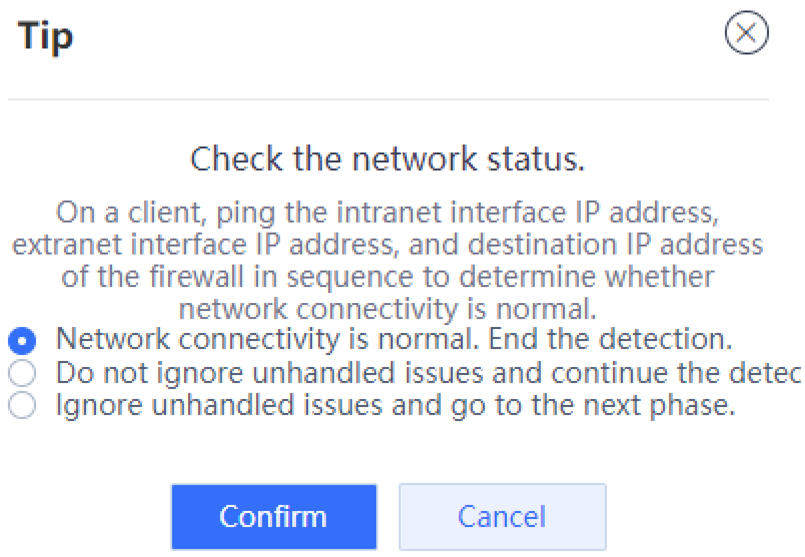
interfacemodule: The interface has not obtained an IPv4 address.(Ge0/1)

Result	Suggestion	Operation
interfacemodule: The interface has not obtained an IPv4 address.(Ge...	Check interface configuration and connections.	Troubleshooting Operation Ignore
interfacemodule: The WAN interface is not added to an untrust zone....	The interface is not added to the corresponding security zone. Check whether a LAN interface is added to the trust zone, and whether a WA N interface is added to the untrust zone.	
interfacemodule: The interface is Up, but no configuration is perform...	Configure a static IP address, DHCP, or PPPoE for the corresponding in terface.	
The NAT module passes the check. ✓		
The security policy module passes the check. ✓		
The DNS module passes the check. ✓		
The DHCP module passes the check. ✓		

(6) In the **Tip** dialog box, select **Network connectivity is normal.** and click **Confirm**. The firewall continues to check the next item.

Note

If the fault is not rectified, select **Do not ignore unhandled issues and continue the detection.** The firewall performs the detection again.



Tip

Check the network status.

On a client, ping the intranet interface IP address, extranet interface IP address, and destination IP address of the firewall in sequence to determine whether network connectivity is normal.

● Network connectivity is normal. End the detection.

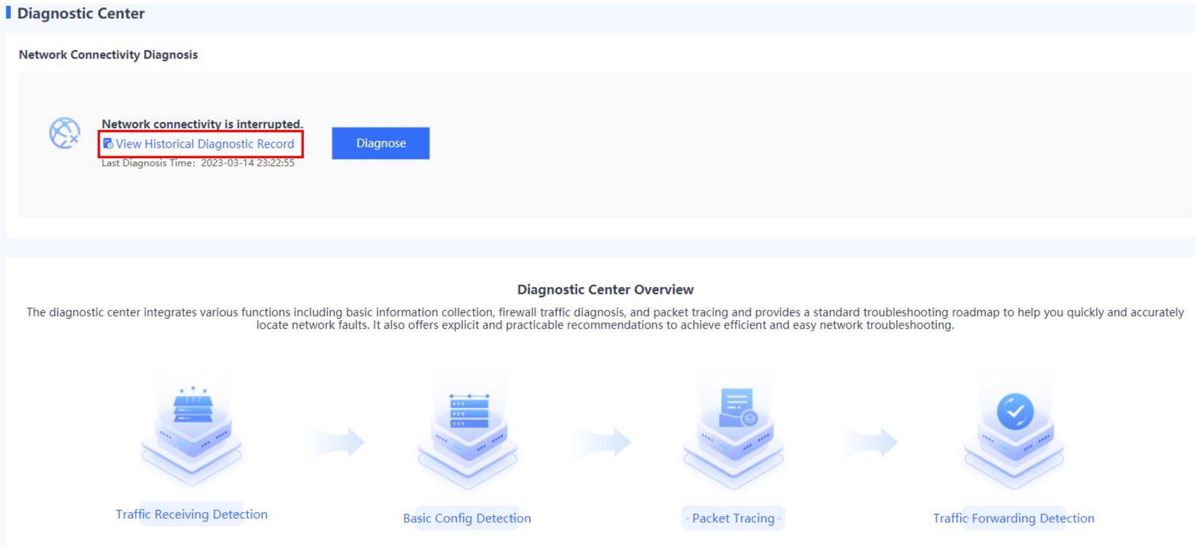
○ Do not ignore unhandled issues and continue the detec

○ Ignore unhandled issues and go to the next phase.

(7) Repeat steps (5) and (6) until all the items are checked.

Follow-up Procedure

Click **View Historical Diagnostic Record** to view and download historical diagnostic records.



Diagnostic Center

Network Connectivity Diagnosis

Network connectivity is interrupted.

View Historical Diagnostic Record

Last Diagnosis Time: 2023-03-14 23:22:55

Diagnostic Center Overview

The diagnostic center integrates various functions including basic information collection, firewall traffic diagnosis, and packet tracing and provides a standard troubleshooting roadmap to help you quickly and accurately locate network faults. It also offers explicit and practicable recommendations to achieve efficient and easy network troubleshooting.

11.4 Packet Obtaining

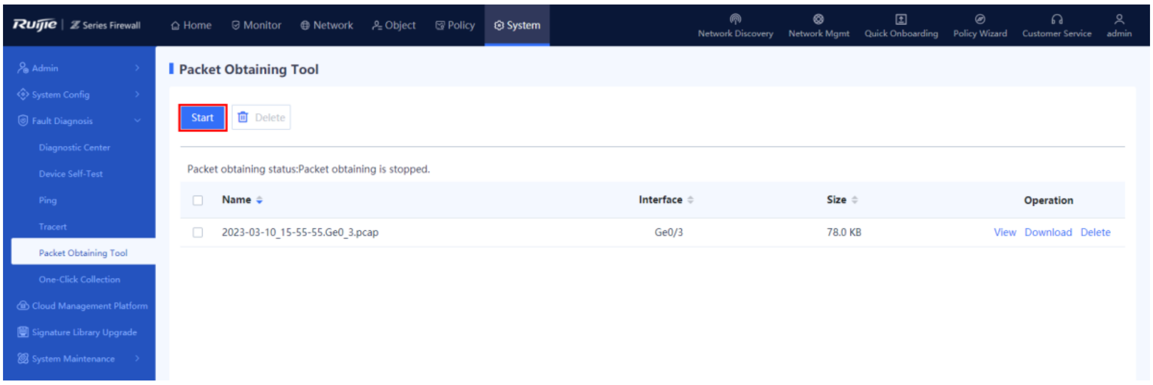
Application Scenario

The web management page provides the packet obtaining function. If a software fault occurs, administrators can use the packet obtaining tool to assist troubleshooting of R&D personnel. The packet obtaining tool is used to obtain data packets on the network and save them to a file. Development personnel can analyze the obtained data packets to quickly locate software faults.

Procedure

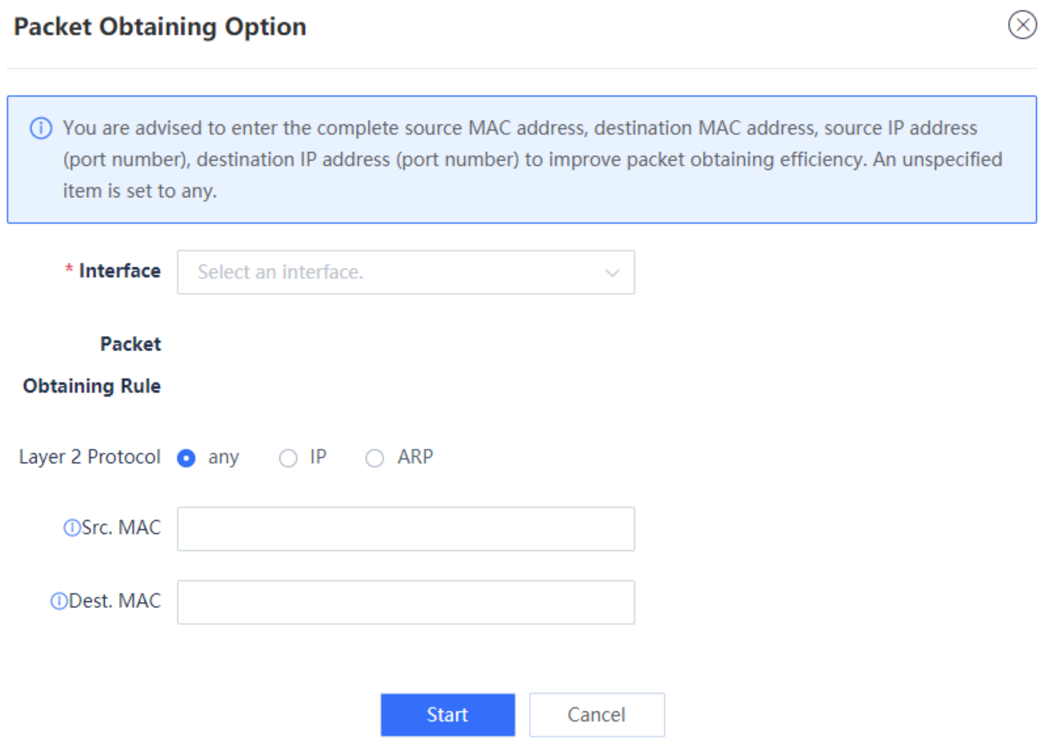
(1) Choose **System** > **Fault Diagnosis** > **Packet Obtaining Tool**.

(2) Click **Start**.



Packet obtaining status:Packet obtaining is stopped.

□	Name	Interface	Size	Operation
□	2023-03-10_15-55-55.Ge0_3.pcap	Ge0/3	78.0 KB	View Download Delete



You are advised to enter the complete source MAC address, destination MAC address, source IP address (port number), destination IP address (port number) to improve packet obtaining efficiency. An unspecified item is set to any.

* Interface: Select an interface.

Packet Obtaining Rule

Layer 2 Protocol ● any ○ IP ○ ARP

Src. MAC:

Dest. MAC:

(3) Set the packet obtaining option.

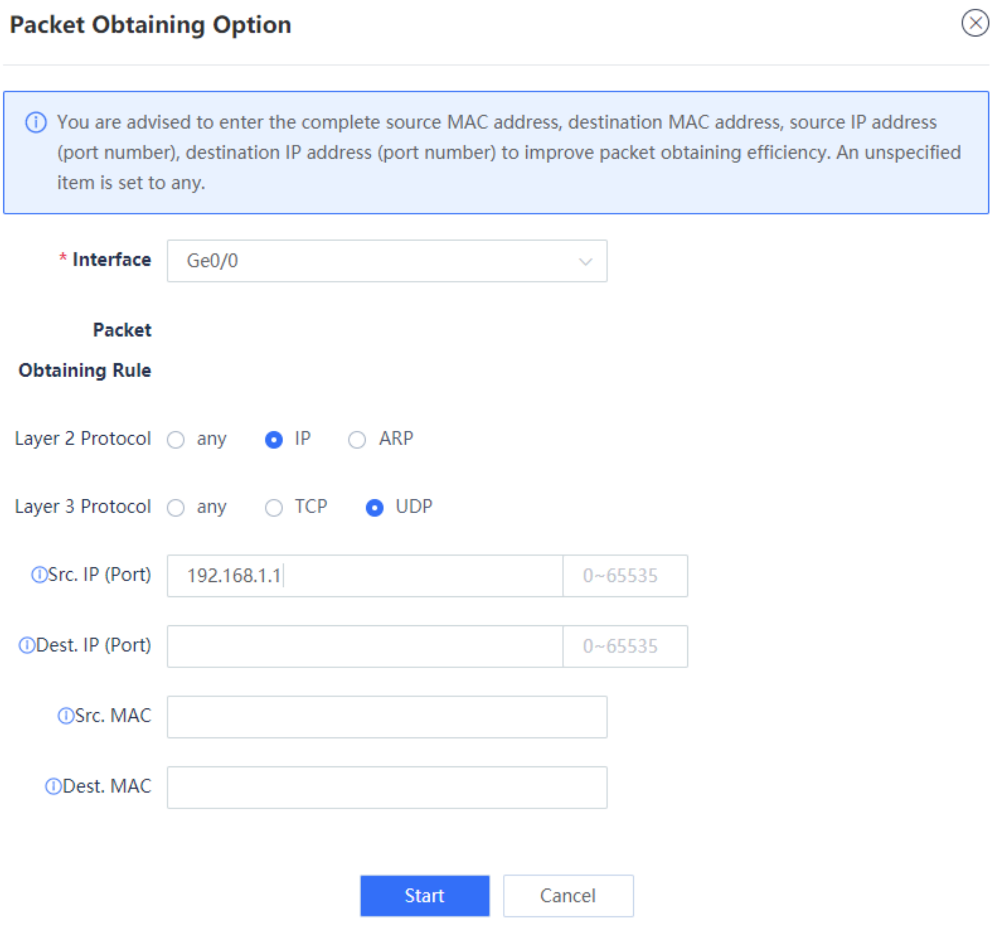
- Interface: Select a physical interface or subinterface from which packets are obtained.
- Layer 2 Protocol
  - When you set this parameter to **any**, you can enter the source or destination MAC address.

If you enter only one MAC address (source or destination MAC address), the tool obtains data packets of this MAC address. If you enter both the source MAC address and destination MAC address, the tool obtains all the packets exchanged between the two MAC addresses.

  - If you set this parameter to **ARP**, the tool obtains ARP packets only. You can enter the source or destination MAC address. If you enter only one MAC address (source or destination MAC address), the tool obtains data packets of this MAC address. If you enter both the source MAC address and destination MAC address, the tool obtains all ARP packets exchanged between the two MAC addresses.
  - If you set this parameter to **IP**, you can further select **any**, **TCP**, or **UDP**.

- If you specify only the source options (source MAC address, source IP address, and source port) or the destination options (destination MAC address, destination IP address, and destination port), the tool obtains packets with the specified source or destination options. If you specify both the source options and the destination options, the tool obtains all the packets meeting these options.

Configuration Example 1



Packet Obtaining Option

You are advised to enter the complete source MAC address, destination MAC address, source IP address (port number), destination IP address (port number) to improve packet obtaining efficiency. An unspecified item is set to any.

* Interface: Ge0/0

Packet Obtaining Rule

Layer 2 Protocol ○ any ● IP ○ ARP

Layer 3 Protocol ○ any ○ TCP ● UDP

Src. IP (Port): 192.168.1.1 | 0~65535

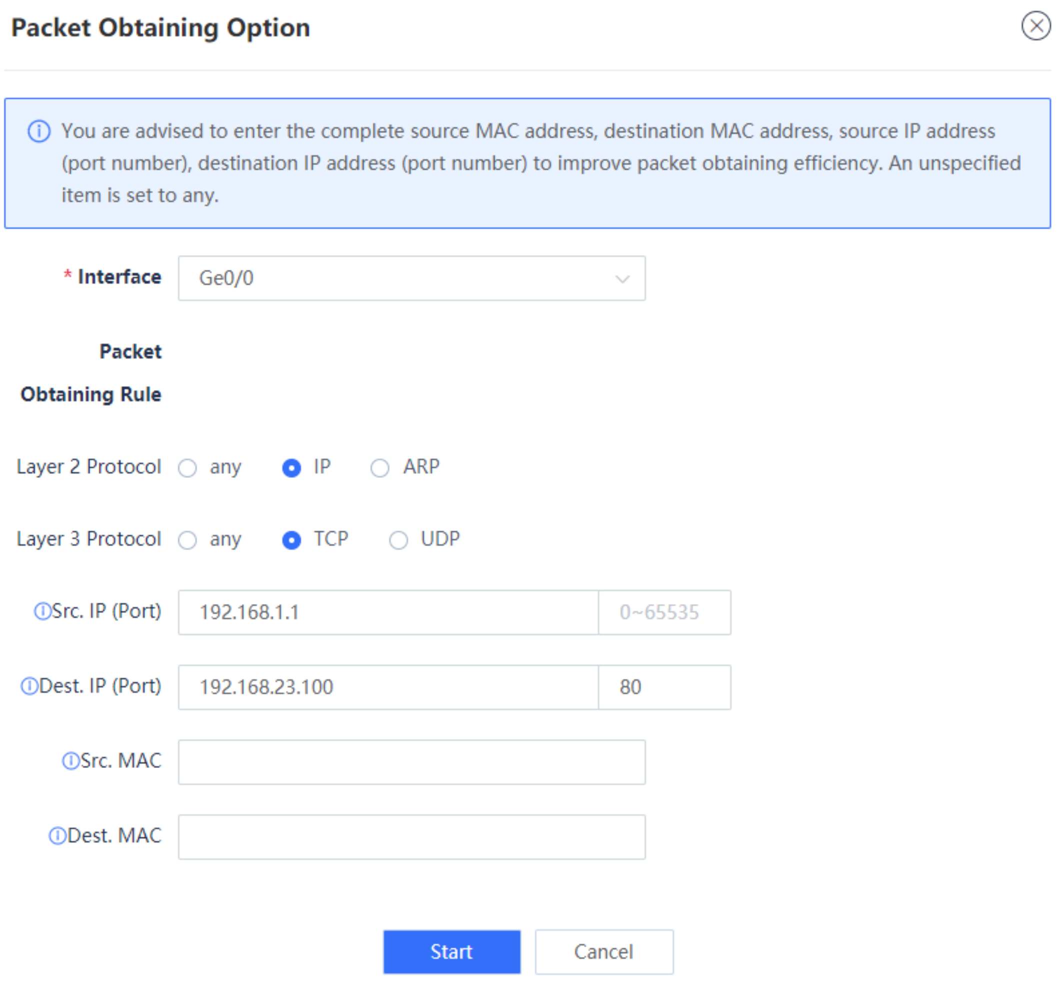
Dest. IP (Port): | 0~65535

Src. MAC:

Dest. MAC:

The tool obtains all the UDP packets passing through Ge0/0 with the source IP address 192.168.1.1 or destination IP address 192.168.1.1.

Configuration Example 2



Packet Obtaining Option

ⓘ You are advised to enter the complete source MAC address, destination MAC address, source IP address (port number), destination IP address (port number) to improve packet obtaining efficiency. An unspecified item is set to any.

* Interface: Ge0/0

Packet Obtaining Rule

Layer 2 Protocol ○ any ● IP ○ ARP

Layer 3 Protocol ○ any ● TCP ○ UDP

ⓘSrc. IP (Port): 192.168.1.1 | 0~65535

ⓘDest. IP (Port): 192.168.23.100 | 80

ⓘSrc. MAC:

ⓘDest. MAC:

The tool obtains all the packets passing through Ge0/0 with the source IP address 192.168.1.1 and destination IP address 192.168.23.100:80 or with the source IP address 192.168.23.100:80 and destination IP address 192.168.1.1.

Follow-up Procedure

After packet obtaining is complete, click **View** to view and analyze the packet obtaining file in online mode and download the packet obtaining result to the PC. The file can be analyzed using a packet obtaining tool such as Wireshark.

11.5 Device Self-Test

Application Scenario

The device self-test function can detect the device version, CPU usage, memory usage, and whether risky configuration exists.

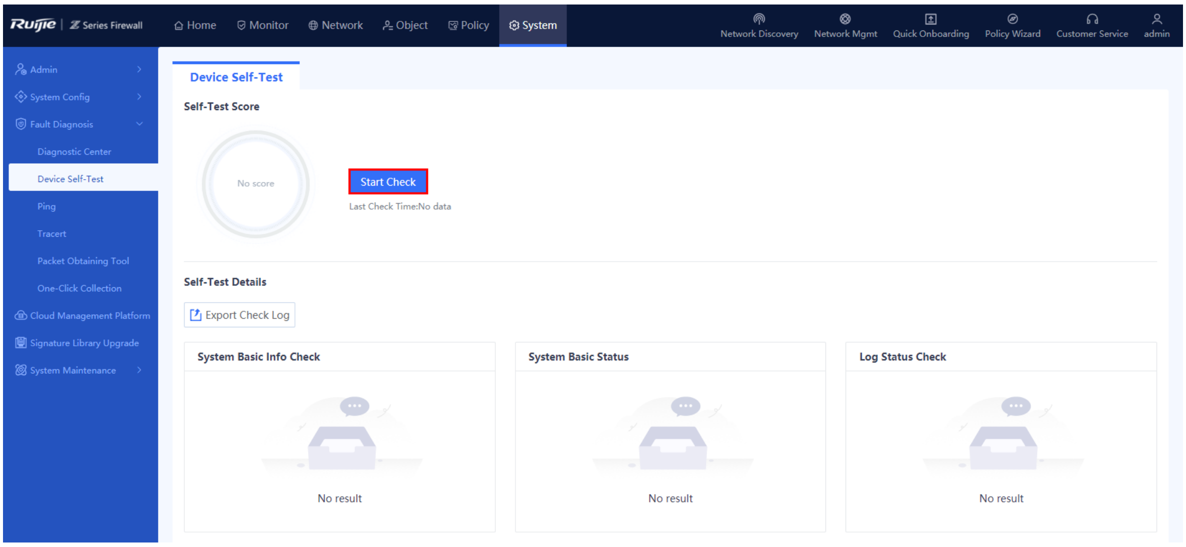
Note

The device self-test function is supported from NTOS1.0R3. If your version is lower than NTOS1.0R3, upgrade it to NTOS1.0R3 or higher.

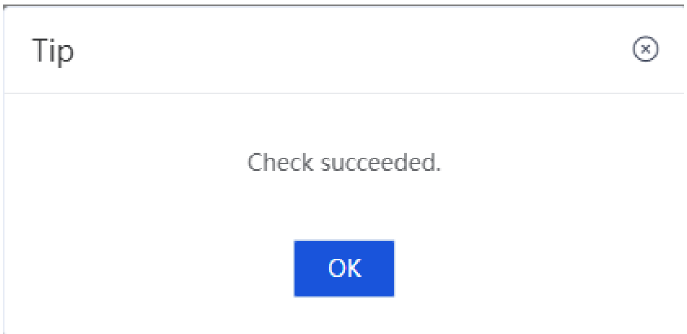
Procedure

(1) Choose **System** > **Fault Diagnosis** > **Device Self-Test** > **Device Self-Test**. The **Device Self-Test** page is displayed.

(2) Click **Start Check** to start device self-test.

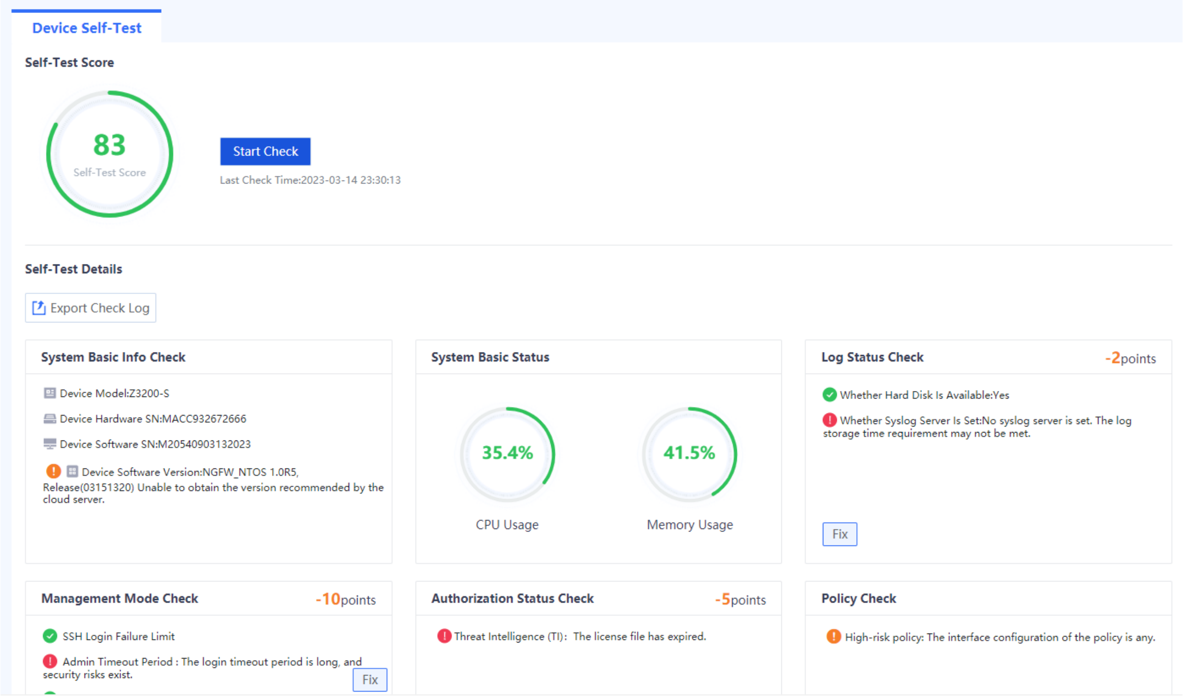


(3) After device self-test is complete, in the dialog box that is displayed, click **OK**.


Tip

Check succeeded.

(4) For an abnormal item, click **Fix** to switch to the corresponding configuration page.



Last Check Time:2023-03-14 23:30:13

Self-Test Details

System Basic Info Check

Device Model:Z3200-S

Device Hardware SN:MACC932672666

Device Software SN:M20540903132023

Device Software Version:NGFW_NTOS 1.0R5, Release(03151320) Unable to obtain the version recommended by the cloud server.

System Basic Status

Log Status Check -2points

Whether Hard Disk Is Available:Yes

Whether Syslog Server Is Set:No syslog server is set. The log storage time requirement may not be met.

Management Mode Check -10points

SSH Login Failure Limit

Admin Timeout Period : The login timeout period is long, and security risks exist.

Authorization Status Check -5points

Threat Intelligence (TI): The license file has expired.

Policy Check

High-risk policy: The interface configuration of the policy is any.

11.6 One-Click Fault Information Collection

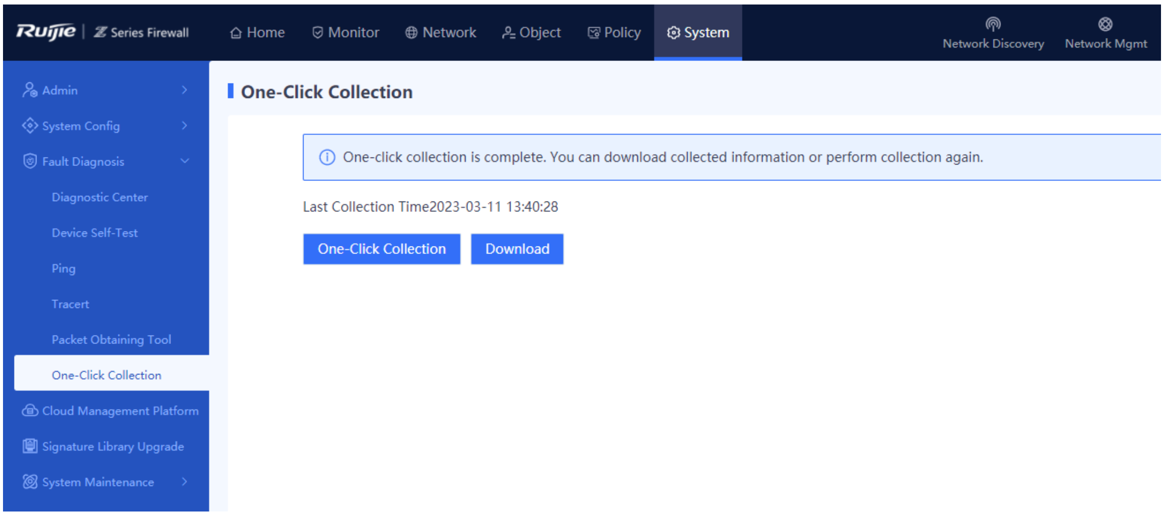
Application Scenario

When a device fault occurs, you can collect the fault information of devices with one click to facilitate analysis by troubleshooting personnel.

Procedure

(1) Access the **One-Click Collection** page.

Choose **System** > **Fault Diagnosis** > **One-Click Collection**.



One-click collection is complete. You can download collected information or perform collection again.

Last Collection Time2023-03-11 13:40:28

(2) Click **One-Click Collection** and wait for 3 to 5 minutes until information collection is complete.

(3) Click **Download** to download the collected fault information to the PC for fault analysis.

11.7 Data Flow Diagnosis

11.7.1 Packet Statistics Collection

1. cmd debug-support fp exec stats

This command is used to collect the number of sent and received packets of an interface and packet processing information in the forwarding path. The fields with annotation need your attention.

```
firewall> cmd debug-support fp exec stats
==== interface stats:
lo-vr0 port:65534
_eth0-vr0 port:65534
_eth1-vr0 port:65534
_eth2-vr0 port:65534
Ge0_0-vr0 port:65534
   ifs_ipackets:124720        --->Number of packets received by the interface
   ifs_ibytes:14454713        --->Number of bytes in the packet received by the interface
   ifs_opackets:23430         --->Number of packets sent by the interface
   ifs_obytes:29152694        --->Number of bytes in the packet sent by the interface
TenGe0_0-vr0 port:65534
   ifs_opackets:739
   ifs_obytes:33994
....
br0-vr0 port:65534
   ifs_ipackets:306
   ifs_ibytes:18360
==== global stats:
   fp_dropped:11053053
   fp_dropped_excp:14155
   fp_dropped_ether:326
   fp_dropped_bridge:2
   fp_dropped_npf:11038563    --->Total number of lost service packets in the flow platform.
The data will be used with statistical analysis of the flow platform later.
```

```
  fp_dropped_system:6
==== exception stats:
  LocalFPTunExceptions:253437
  ExceptionByModule:
    fp_exception_ether:199272
    fp_exception_bridge:734
    fp_exception_ip:37548
    fp_exception_ipv6:15883
  LocalExceptionClass:
    FPTUN_EXC_SP_FUNC:206764
    FPTUN_EXC_ETHER_DST:28299
    FPTUN_EXC_IP_DST:15196
    FPTUN_EXC_ICMP_NEEDED:687
    FPTUN_EXC_NDISC_NEEDED:2491
  LocalExceptionType:
    FPTUN_IPV4_OUTPUT_EXCEPT:2491
    FPTUN_ETH_INPUT_EXCEPT:250946
    FPTUN_ETH_SP_OUTPUT_REQ:2444
  ExcpDroppedFpToLinuxUserExcSendtoFailure:102
==== IPv4 stats:
  IpForwDatagrams:1648056613
  IpInReceives:1648056613
==== arp stats:
  arp_unhandled:168695
==== IPv6 stats:
==== TCP stats:
total packets received:6758
# of packets not managed by MCORE_SOCKET:6758
==== UDP stats:
==== vlan stats:
==== dsa stats:
  DsaDroppedInOperative:1
==== bridge stats:
  L2ForwFrames:251334551
  BridgeDroppedNoOutputPort:2
==== ebtables stats:
==== pppoe stats:
```

2. cmd debug-support npf exec stats

This command is used to display statistics of various services in the flow platform.

```
firewall> cmd debug-support npf exec stats
Policy action:                    --->Statistical summary of a security policy
          1008 Policy permit          ---> Number of flows permitted by the security policy
          0 Policy deny               ---> Number of flows blocked by the security policy
Packets dropped:                  --->Total number of lost service packets in the flow platform
          0 RPF check drop
          0 Connection create failed drop
          0 Connection install failed drop
          0 Connection threshold drop
          0 Connection invalid state drop
          0 Invalid connection drop
          0 Do SNAT drop
          0 Do DNAT drop
          0 NAT transition drop
          0 Do ALG drop
          624879 Route error drop
          0 thd-event mlist full drop
          0 thd-event error drop
          0 Prepend failed drop
          0 Header too short drop
          0 Fragment failure drop
          0 Invalid IP drop
Wrong packets dropped:
          0 Interface error
          0 Ip header error
          0 Frament packet
          0 IP header hl error
          0 TCP header error
          0 UDP header error
          0 ICMP header error
          0 ICMP packet error
          0 ICMP6 header error
          0 ICMP6 packet error
          0 checksum error
          0 Ipv6 header error
```

```
            0 Ipv6 extension header error
Connection entries:
            625887 Connection allocations
            0 Connection reverse
            625886 Connection release
            625884 Connection destructions
            0 Connection refresh conflict
            0 Connection allocation failures
            0 Connection ID limit
            0 Connection ID invalid
            0 Connection ID no entry
NAT entries:
            0 NAT entry allocations
            0 NAT entry destructions
            0 NAT entry allocation failures
            0 NAT port allocation failures
Invalid packet state cases:
            0 cases in total
            0 TCP case invalid first packet
            0 TCP case RST
            0 TCP case invalid transition
            0 TCP case REOPEN
            0 TCP case Out of window range
            0 TCP case Invalid seq
            0 TCP case Invalid ack
TCP Reass:
            0 TCP Reass present
            0 TCP Reass present cover
            0 TCP Reass present overlap
            0 TCP Reass present cut
            0 TCP Reass cache
            0 TCP Reass cache head
            0 TCP Reass cache tail
            0 TCP Reass cache head overlap
            0 TCP Reass cache tail overlap
            0 TCP Reass cache new drop
            0 TCP Reass cache old drop
            0 TCP Reass cache overflow
            0 TCP Reass cache timeout
            0 TCP Reass cache release
            0 TCP Reass error
Packets reentrant:
            0 reentrant
            0 reentrant drop
Packet race cases:
            0 NAT association race
            0 duplicate state race
```

11.7.2 Flow Status

The **show nfp flows stats** command is used to display flow table statistics.

The **show nfp flows** command is used to display all the flow entries in the system.

The **show nfp flows filter** { **app** *appid* **|** **addr** *address* **|** **dport** *port* **|** **dstif** *interface* **|** **policy** *policy-id* **|** **proto** *protocol-id* **|** **saddr** *address* **|** **session-id** *id* **|** **sport** *port* **|** **srcif** *interface* } command is used to display flow tables by filtering condition.

This command is used when flow tables are created based on the specified control flow (for example, data flows in the ALG scenario).

```
firewall> show nfp flows
38:
        proto:17    tsdiff:7    timeout:120    State:established
        FORW 20.0.0.2:39304 -> 114.114.114.114:53
        BACK 114.114.114.114:53 -> 20.0.0.2:39304
        Srcif:lo       Dstif:Ge0/0    alg:none    flags:0x2000000
        vrf:0    Appid:0-0-0-0     Policy:local    action:permit
        Send packets:2    bytes:136
        Recv packets:2    bytes:622
firewall> show nfp flows filter dport 9209
1191:
        proto:6    tsdiff:1    timeout:1800    State:established
        FORW 172.16.33.5:9404 -> 172.18.142.16:9209
        BACK 172.18.142.16:9209 -> 20.0.0.2:52438
        snat id: 0
        Srcif:Ge0/1    Dstif:Ge0/0    alg:none    flags:0x804a000
        vrf:0    Appid:0-0-0-0     Policy:8192    action:permit
        Send packets:16572    bytes:2435798
        Recv packets:8331    bytes:2114493
```

```
firewall> show nfp flows stats
The capacity of the flow: 1000000
Allocated flows num: 63
Active flows num: 63
```

Note: The following part describes fields in the flow table.

```
1191:
        proto:6    tsdiff:1    timeout:1800    State:established
        FORW 172.16.33.5:9404 -> 172.18.142.16:9209
        BACK 172.18.142.16:9209 -> 20.0.0.2:52438
        snat id: 0
        Srcif:Ge0/1    Dstif:Ge0/0    alg:none    flags:0x804a000
        vrf:0    Appid:0-0-0-0     Policy:8192    action:permit    --->Security policy matching result.
The value of local indicates access to the local host or access actively initiated by the local host,
which is not restricted. The value of default indicates that the default block policy is matched.
The value of bypass indicates that a whitelist is matched. If a number is displayed, the number
indicates the ID of a specific policy.
        Action:security-defend(1) Reason:flood detect(11)    -->Module and cause. The
information is displayed only when packet loss in the flow is not caused by a security policy.
        Send packets:16572    bytes:2435798
        Recv packets:8331    bytes:2114493
         1191: Flow id/session id
         Proto: Protocol number (1:icmp    6:tcp    17:udp)
         tsdiff: Session idle time (remaining time before session aging)
         timeout: Session aging time
         State: Session status
         FORW: Quadruple information of the forward session flow
         BACK: Quadruple information of the reverse session flow
         snat id: ID of the NAT policy hit by the flow
         Srcif: Source interface of the forward flow
         Dstif: Destination interface of the forward flow
         Alg: ALG type of the flow
         Flags: Flow table status
         vrf: vrf id
         Appid: Application identification ID
         Policy: ID of the security policy hit by the flow
         Action: Policy action (permit/deny)
         Action: Module with packet loss
   security-defend:DDOS
```

```
Reason for packet loss (Reason):
    XXX
         Send packets: Number of sent packets
         Recv packets: Number of packets received
```

11.7.3 Packet Tracing

Use command (1) to configure filtering conditions and command (2) to configure the module (type-on field in command 2) to be enabled. In most cases, you are advised to use the recommended command.

Commands:

(1) **cmd trace-filter enabled true** [**proto** *protocol-id*] [**saddr** *address*] [**sport** *port*] [**daddr** *address*] [**dport** *port*] [**ifid1** *interface-id*] [**ifid2** *interface-id*]

```
firewall>cmd trace level DEBUG max-number 0 timeout 0 type-off "all" type-on "NFP BASIC"
firewall>cmd trace-filter enabled true proto 1 saddr 10.1.1.10
firewall> show log max-lines 2000
[2022/02/17 11:24:39]Feb 17 11:23:51 firewall fp-rte[1339]: fp_ether_input(ifp=Ge0_6 port=65534)
[2022/02/17 11:24:39]Feb 17 11:23:51 firewall fp-rte[1339]: fp_ether_input_one(ifp=Ge0_6 port=65534)
[2022/02/17 11:24:39]Feb 17 11:23:51 firewall fp-rte[1339]: fp_ip_input_bulk_check: mbuf=0x18ad669c0
[2022/02/17 11:24:39]Feb 17 11:23:51 firewall fp-rte[1339]: npf_packet_handler: mbuf=0x18ad669c0, npf_mode=0
[2022/02/17 11:24:39]Feb 17 11:23:51 firewall fp-rte[1339]: npf: mbuf 0x18ad669c0 find connection 662, dir=back
[2022/02/17 11:24:39]Feb 17 11:23:51 firewall fp-rte[1339]:          vrfid 0 flags 0x804a000 alg none policy 8192 action permit
[2022/02/17 11:24:39]Feb 17 11:23:51 firewall fp-rte[1339]:          forw proto 1 5.0.64.53:1-> 172.18.25.214:1
[2022/02/17 11:24:39]Feb 17 11:23:51 firewall fp-rte[1339]:          back proto 1 172.18.25.214:458-> 192.168.101.2:458
[2022/02/17 11:24:39]Feb 17 11:23:51 firewall fp-rte[1339]: fast path: security_defend returns 0
[2022/02/17 11:24:39]Feb 17 11:23:51 firewall fp-rte[1339]: fast path: conn_reroute returns 0
[2022/02/17 11:24:39]Feb 17 11:23:51 firewall fp-rte[1339]: fast path: conn_update returns 0
[2022/02/17 11:24:39]Feb 17 11:23:51 firewall fp-rte[1339]: fast path: policy_rematch returns 0
[2022/02/17 11:24:39]Feb 17 11:23:51 firewall fp-rte[1339]: fast path: service_chain returns 0
[2022/02/17 11:24:39]Feb 17 11:23:51 firewall fp-rte[1339]: fast path: alg returns 0
```

```
[2022/02/17 11:24:39]Feb 17 11:23:51 firewall fp-rte[1339]: fast path: do_nat returns 0
[2022/02/17 11:24:39]Feb 17 11:23:51 firewall fp-rte[1339]: fast path: security_defend returns 0
[2022/02/17 11:24:39]rns 0
[2022/02/17 11:24:39]Feb 17 11:23:51 firewall fp-rte[1339]: fp_fast_ip_input_pre_routing:
mbuf=0x18ad669c0
[2022/02/17 11:24:39]Feb 17 11:23:51 firewall fp-rte[1339]: fp_fast_ip_output_post_routing:
mbuf=0x18ad669c0
[2022/02/17 11:24:39]Feb 17 11:23:51 firewall fp-rte[1339]: fp_ether_output:
mbuf=0x18ad669c0, ifp=Ge0_1 port=65534
[2022/02/17 11:24:39]Feb 17 11:23:51 firewall fp-rte[1339]: fp_if_output: mbuf=0x18ad669c0,
ifp=eth0, port=0
[2022/02/17 11:24:39]Feb 17 11:23:51 firewall uwsgi[2445]: <190>1
2022-02-17T03:23:51.525503Z firewall web 2445 - [operationLog@4881 ip="192.168.1.100"
operator="<E7><AB><AF><E5><8F<8F><A3><E6><98><A0><E5><B0><84>"
operate="<E5><90><AF><E7><94><A8>/<E7><A6><81><E7><94><A8><E7><AB><AF
><E5><8F><A3><E6><98><A0><E5><B0><84>"
description="<E7><<AB><AF><E5><8F><A3><E6><98><A0><E5><B0><84>
<E5><90><AF><E7><94><A8>/<E7><A6><8<81><E7><94><A8><E7><AB><AF><E5><
8F><A3><E6><98><A0><E5><B0><84><E6><88><90><E5><8A><9F>"
timestamp="1645068231" admin="admin"]
[2022/02/17 11:24:39]Feb 17 11:23:52 firewall fp-rte[1339]:
[2022/02/17 11:24:39]Feb 17 11:23:52 firewall fp-rte[1339]: fp_ether_input(ifp=eth0 port=0)
[2022/02/17 11:24:39]Feb 17 11:23:52 firewall fp-rte[1339]: sbuf data at [0x18e60ab82], len=78
[2022/02/17 11:24:39]Feb 17 11:23:52 firewall fp-rte[1339]: 00000000 30 0D 9E 41 D8 D1 22 22
22 22 22 24 C0 10 00 00
[2022/02/17 11:24:39]Feb 17 11:23:52 firewall fp-rte[1339]: 00000010 08 00 45 00 00 3C 3E 34
00 00 40 01 31 70 05 00
[2022/02/17 11:24:39]Feb 17 11:23:52 firewall fp-rte[1339]: 00000020 40 35 AC 12 19 D6 08 00
19 14 00 01 34 47 61 62
[2022/02/17 11:24:39]Feb 17 11:23:52 firewall fp-rte[1339]: 00000030 63 64 65 66 67 68 69 6A
6B 6C 6D 6E 6F 70 71 72
[2022/02/17 11:24:39]Feb 17 11:23:52 firewall fp-rte[1339]: 00000040 73 74 75 76 77 61 62 63
64 65 66 67 68 69
[2022/02/17 11:24:39]Feb 17 11:23:52 firewall fp-rte[1339]: fp_ether_input(ifp=Ge0_1
port=65534)
[2022/02/17 11:24:39]Feb 17 11:23:52 firewall fp-rte[1339]: fp_ether_input_one(ifp=Ge0_1
port=65534)
```

```
[2022/02/17 11:24:39]Feb 17 11:23:52 firewall fp-rte[1339]: fp_ip_input_bulk_check:
mbuf=0x18e60a900
[2022/02/17 11:24:39]Feb 17 11:23:52 firewall fp-rte[1339]: npf_packet_handler:
mbuf=0x18e60a900, npf_mode=0
[2022/02/17 11:24:39]Feb 17 11:23:52 firewall fp-rte[1339]: npf_packet_handler, 1029: conn 662
is expired, drop the mbuf 0x18e60a900!packet m=0x18e60a900 dropped at
npf_packet_handler():1030
[2022/02/17 11:24:39]Feb 17 11:23:53 firewall fp-rte[1339]: flow-log 1230 send: src 83902517
sport 16374 dst 1964509311 dport 80 natsrc 3232261378 natsport 9278 natdst 1964509311
natdport 80 proto 6 direct 1 sendbytes 415 recvbytes 410 sendpkts 8 recvpkts 2 srcif Ge0_1 dstif
Ge0_6 appid 0-0-0-0 policy allow_all action 0 module    reason    time 1645068232
[2022/02/17 11:24:39]Feb 17 11:23:53 firewall fp-rte[1339]: flow-log 662 send: src 83902517
sport 1 dst 2886867414 dport 1 natsrc 3232261378 natsport 458 natdst 2886867414 natdport
458 proto 1 direct 1 sendbytes 54068232
[2022/02/17 11:24:39]Feb 17 11:23:53 firewall fp-rte[1339]: flow-log 710 send: src 83902517
sport 12345 dst 660748687 dport 8000 natsrc 3232261378 natsport 8959 natdst 660748687
natdport 8000 proto 17 direct 1 sendbytes 205 recvbytes 0 sendpkts 1 recvpkts 0 srcif Ge0_1
dstif Ge0_6 appid 0-0-0-0 policy allow_all action 0 module    reason    time 1645068232
[2022/02/17 11:24:39]Feb 17 11:23:53 firewall fp-rte[1339]: flow-log 138 send: src 83902517
sport 61509 dst 2567170222 dport 8000 natsrc 3232241498 natsport 8326 natdst 2567170222
natdport 8000 proto 17 direct 1 sendbytes 1170 recvbytes 70 sendpkts 6 recvpkts 1 srcif Ge0_1
dstif Ge0_7 appid 0-0-0-0 policy allow_all action 0 module    reason    time 1645068233
[2022/02/17 11:24:39]Feb 17 11:23:53 firewall fp-rte[1339]: Connection 662 is destroyed
```

(2) **cmd trace** [**level** EMERG | ALERT | CRIT | ERR | WARNING | NOTICE | INFO | DEBUG] [**max-number** *line*] [**timeout** *seconds*] [**type-off** "all"] [**type-on** "NFP BASIC "]

This command is used to set the output level of debugging logs, the maximum number of rows in a log, maximum record timeout period (in seconds), and module enabling/disabling log.

- **max-number**: Specifies the maximum number of rows in a printed log.
- **timeout:** Specifies the time when the log is printed.

Note

The levels in the command format are ranked in descending order by the severity. The default level is ERR. After a level is set, all the logs higher than or equal to this level will be printed.

The following command is used to display the forwarding packet loss information.

```
cmd trace level DEBUG max-number 0 timeout 180 type-off "all" type-on " NFP BASIC "
```

max-number 0 timeout 180 indicates that log recording is automatically disabled in 3 minutes. If both **max-number** and **timeout** are set to 0, log recording must be disabled manually after information collection.

Use the following command to disable log recording (restoring to the default value).

```
cmd trace level ERR max-number 5000 timeout 60 type-off "all"
```

12 Running Status Check After Product Implementation

12.1 Checking the Software Version

Standards

- The software version must be the latest. Confirm on the Secure Cloud Platform or choose **System** > **System Maintenance** > **System Upgrade** > **Online Upgrade** to check whether a recommended version is available. If no, the system displays that the current version is already the latest version.
- Users have purchased the online upgrade service for the app identification signature library and IPS signature library and the current version is the latest.

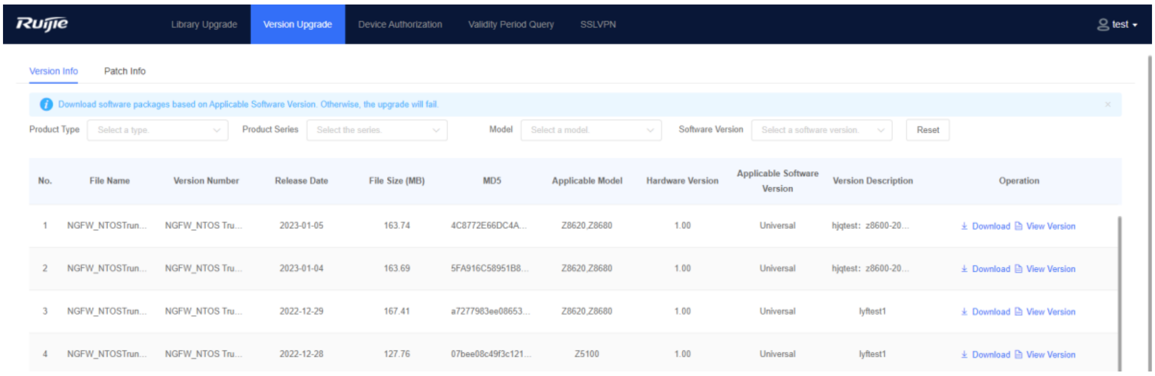
Precautions

- The device needs to be restarted after online device upgrade, which may cause customer service interruption.
- Users can upgrade to the latest signature libraries only after they purchase the upgrade service for the Ruijie IPS signature library and virus library.
- DNS and the time zone must be correctly configured to allow the app identification signature library and IPS signature library to access the Internet.

Method

(1) Check whether the software version is recommended using one of the following methods:

- Method 1: Log in to the Secure Cloud Platform (https://secloud-en.ruijienetworks.com/), click **Version Upgrade**, and select an applicable version to download it.

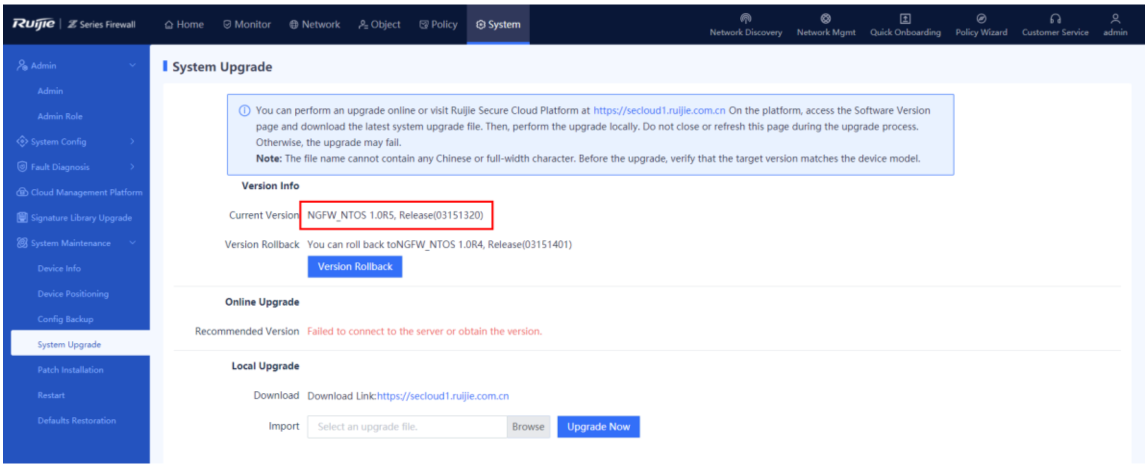


Download software packages based on Applicable Software Version. Otherwise, the upgrade will fail.

Product Type: Select a type. Product Series: Select the series. Model: Select a model. Software Version: Select a software version. Reset

No.	File Name	Version Number	Release Date	File Size (MB)	MD5	Applicable Model	Hardware Version	Applicable Software Version	Version Description	Operation
1	NGFW_NTOSTrun...	NGFW_NTOS Tru...	2023-01-05	163.74	4C8772E66DC4A...	Z8620,Z8680	1.00	Universal	hjqtest: z8600-20...	Download View Version
2	NGFW_NTOSTrun...	NGFW_NTOS Tru...	2023-01-04	163.69	5FA916C58951B8...	Z8620,Z8680	1.00	Universal	hjqtest: z8600-20...	Download View Version
3	NGFW_NTOSTrun...	NGFW_NTOS Tru...	2022-12-29	167.41	a7277983ee08653...	Z8620,Z8680	1.00	Universal	lyftest1	Download View Version
4	NGFW_NTOSTrun...	NGFW_NTOS Tru...	2022-12-28	127.76	07bee08c49f3c121...	Z5100	1.00	Universal	lyftest1	Download View Version

- Method 2: Log in to the web page of the firewall and choose **Home** > **View Device Detail** > **Version Info** or **System** > **System Maintenance** > **System Upgrade**.



System Upgrade

You can perform an upgrade online or visit Ruijie Secure Cloud Platform at https://secloud1.ruijie.com.cn On the platform, access the Software Version page and download the latest system upgrade file. Then, perform the upgrade locally. Do not close or refresh this page during the upgrade process. Otherwise, the upgrade may fail.
Note: The file name cannot contain any Chinese or full-width character. Before the upgrade, verify that the target version matches the device model.

Version Info

Current Version NGFW_NTOS 1.0R5, Release(03151320)

Version Rollback You can roll back toNGFW_NTOS 1.0R4, Release(03151401)

Version Rollback

Online Upgrade

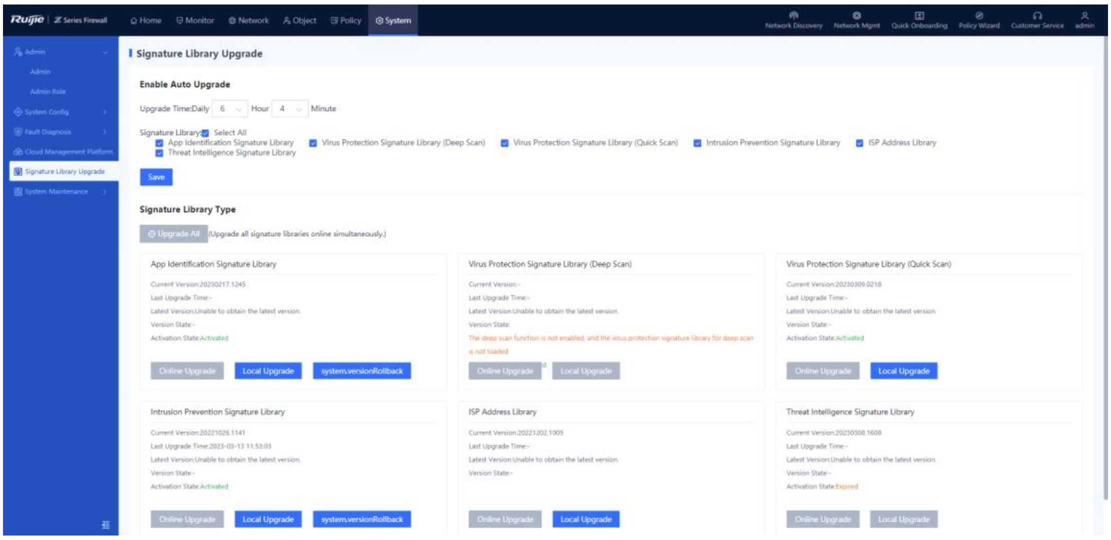
Recommended Version Failed to connect to the server or obtain the version.

Local Upgrade

Download Download Link:https://secloud1.ruijie.com.cn

Import Select an upgrade file. Browse Upgrade Now

(2) Check whether signature libraries (app identification signature library, IPS signature library, virus protection signature library, ISP address library, threat intelligence signature library) are of the latest version.



Signature Library Upgrade

Enable Auto Upgrade

Upgrade Time:Daily 6 Hour 4 Minute

Signature Library:☑ Select All
☑ App Identification Signature Library ☑ Virus Protection Signature Library (Deep Scan) ☑ Virus Protection Signature Library (Quick Scan) ☑ Intrusion Prevention Signature Library ☑ ISP Address Library
☑ Threat Intelligence Signature Library

Save

Signature Library Type

Upgrade All (Upgrade all signature libraries online simultaneously.)

App Identification Signature Library
Current Version:20230217.1245
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated
Online Upgrade Local Upgrade system.versionRollback

Virus Protection Signature Library (Deep Scan)
Current Version:-
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:
The deep scan function is not enabled, and the virus protection signature library for deep scan is not loaded
Online Upgrade Local Upgrade

Virus Protection Signature Library (Quick Scan)
Current Version:20230309.0218
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated
Online Upgrade Local Upgrade

Intrusion Prevention Signature Library
Current Version:20221026.1141
Last Upgrade Time:2023-03-13 11:53:03
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Activated
Online Upgrade Local Upgrade system.versionRollback

ISP Address Library
Current Version:20221202.1005
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Online Upgrade Local Upgrade

Threat Intelligence Signature Library
Current Version:20230308.1608
Last Upgrade Time:-
Latest Version:Unable to obtain the latest version.
Version State:-
Activation State:Expired
Online Upgrade Local Upgrade

12.2 Checking the Management Mode

Standards

- Preferentially use secure management modes HTTPS and SSH and test whether the firewall can be remotely managed over the customer LAN or Internet.
- Confirm that the administrator login timeout period is not over 30 minutes. (**A too long timeout period causes security risks.**)
- It is recommended that the allowed consecutive login failures be not higher than 6 and the lockout duration be not less than 300s. (A large login failure count will lead to brute-force attack risks. The re-login interval cannot be set to a too small value.)
- Confirm that the firewall restricts management hosts.

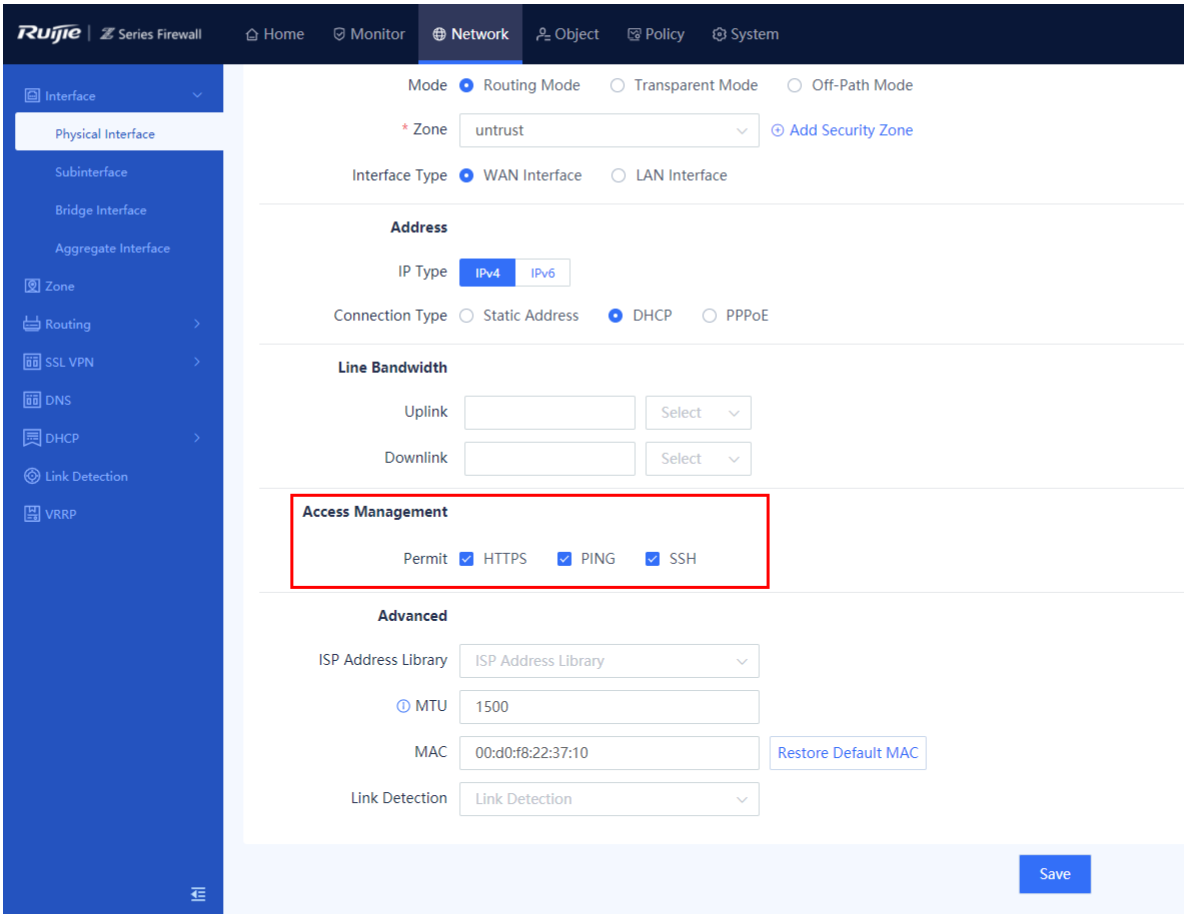
Precautions

- By default, ping or SSH is disabled on the interface.
- The default timeout period is 30 minutes and maximum configurable timeout period is 1440 minutes.
- The default allowed consecutive login failures is 6 and the re-login interval is 3 minutes.
- A specific host address rather than a network segment must be added for a management host. Fully consider the probability of LAN and WAN management to properly add management hosts.

Method

(1) Check whether remote management is enabled on the interface.

Log in to the web management page and choose **Network** > **Interface** > **Physical Interface**.



Mode ● Routing Mode ○ Transparent Mode ○ Off-Path Mode

* Zone untrust

Interface Type ● WAN Interface ○ LAN Interface

Address

IP Type IPv4 IPv6

Connection Type ○ Static Address ● DHCP ○ PPPoE

Line Bandwidth

Uplink Select

Downlink Select

Access Management

Permit ☑ HTTPS ☑ PING ☑ SSH

Advanced

ISP Address Library ISP Address Library

MTU 1500

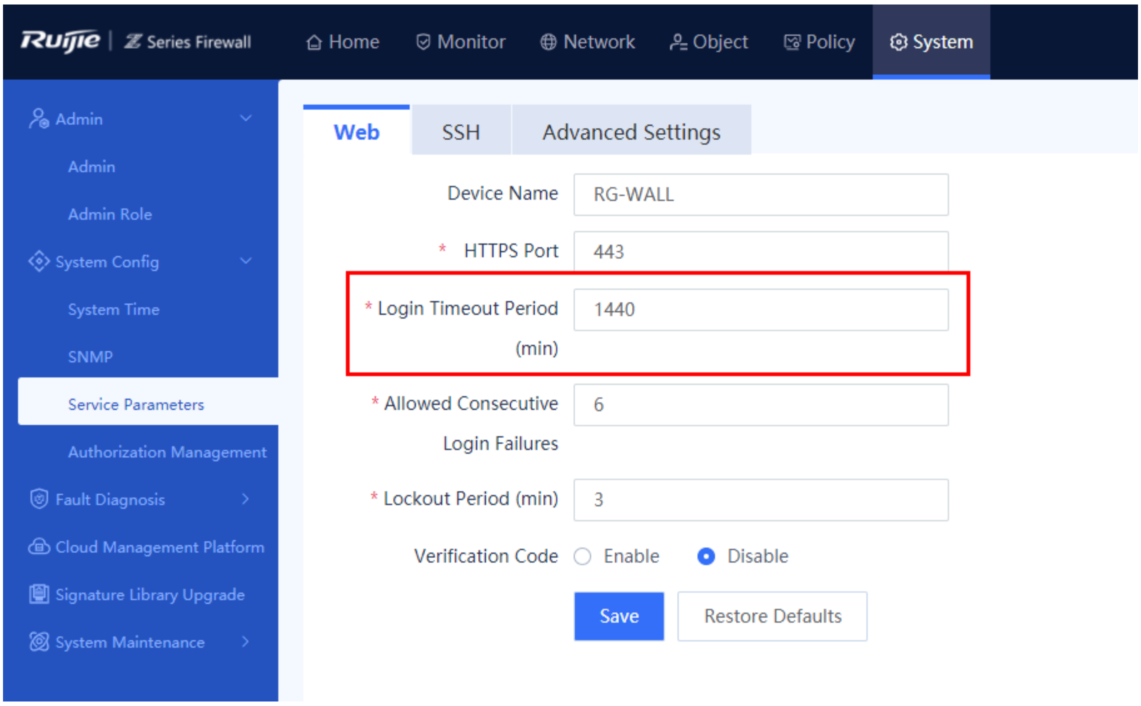
MAC 00:d0:f8:22:37:10

Link Detection Link Detection

(2) Check whether web service parameters are set.

- Administrator login timeout period

  Log in to the web management page and choose **System** > **System Config** > **Service Parameters**.



Device Name: RG-WALL

* HTTPS Port: 443

* Login Timeout Period (min): 1440

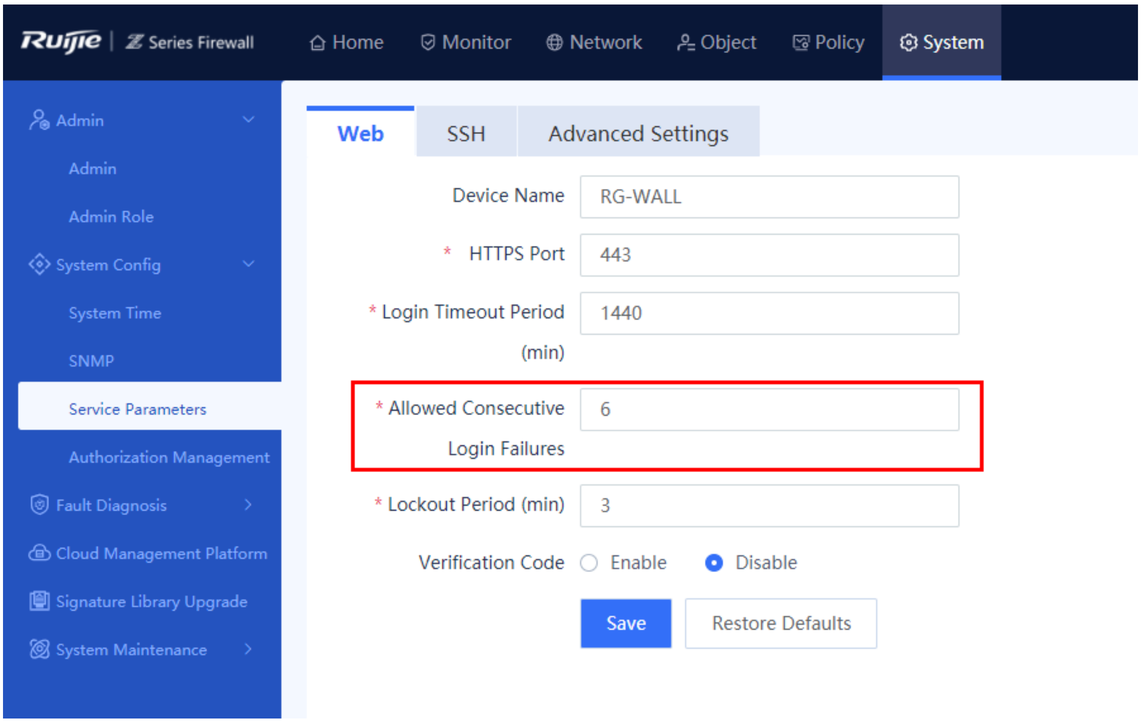
* Allowed Consecutive Login Failures: 6

* Lockout Period (min): 3

Verification Code: ○ Enable ● Disable

- Limit on administrator login failures

Log in to the web management page and choose **System** > **System Config** > **Service Parameters**.



Device Name: RG-WALL

* HTTPS Port: 443

* Login Timeout Period (min): 1440

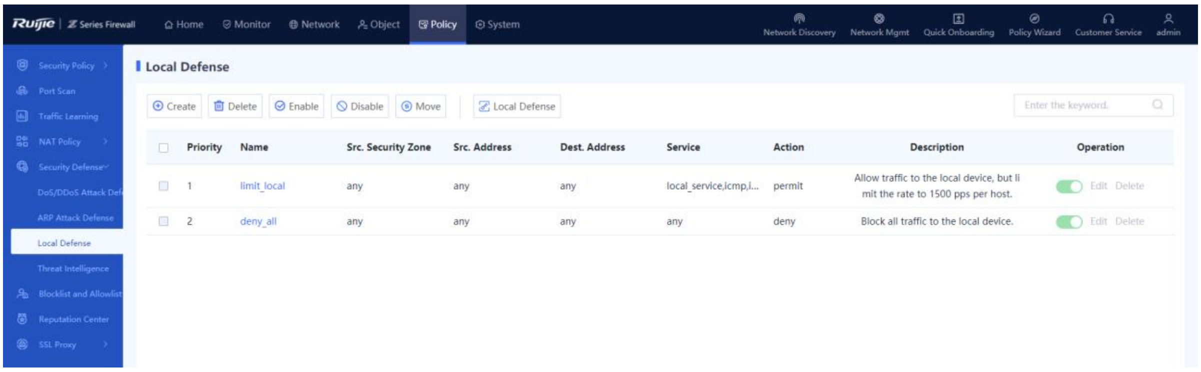
* Allowed Consecutive Login Failures: 6

* Lockout Period (min): 3

Verification Code: ○ Enable ● Disable

(3) Management host settings

Log in to the web management page and choose **Policy** > **Security Defense** > **Local Defense**.



Local Defense

□	Priority	Name	Src. Security Zone	Src. Address	Dest. Address	Service	Action	Description	Operation
□	1	limit_local	any	any	any	local_service,icmp,i...	permit	Allow traffic to the local device, but li mit the rate to 1500 pps per host.	Edit Delete
□	2	deny_all	any	any	any	any	deny	Block all traffic to the local device.	Edit Delete

12.3 Checking Firewall Policies

Standards

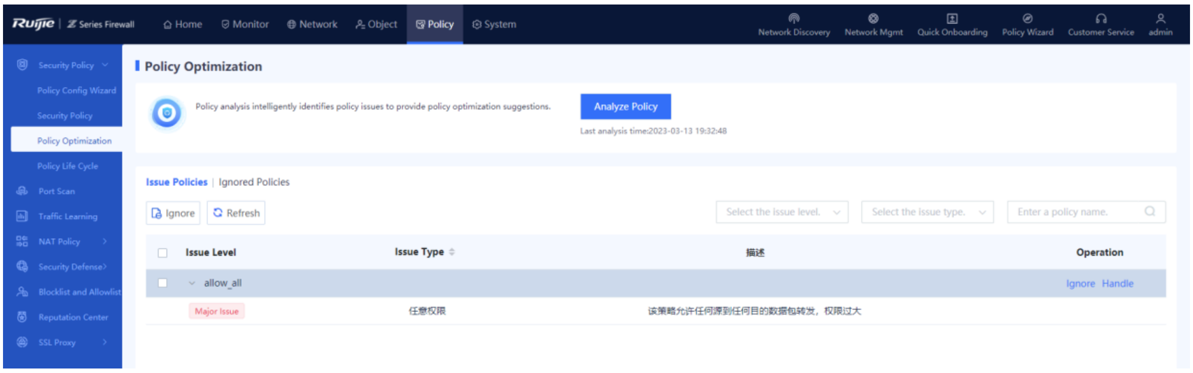
- An any-to-any policy makes the firewall meaningless and cannot achieve the purpose of access control. Administrators must know the data flow direction of customer services and implement access control based on the IP address and port number.
- All policies must be enabled. If a policy is not matched or does not hit any data flow within 90 days, the policy is considered to be improper.
- If the matching scope of one policy covers that of another policy but the two policies define different actions, a policy conflict occurs.

Method

Log in to the web management page and choose **Policy** > **Security Policy** > **Policy Optimization**.

Check whether policies with major problems exist in the **Issue Policies** area.

- Policy with all permissions (All objects in the policy are set to **any**.)
- Policy not matched within 90 days (The policy does not match any data flow within 90 days, according to the last time the policy is matched.)
- Completely conflicting policy (The matching scope of policy A covers that of policy B but the two policies define different actions.)



Policy Optimization

Policy analysis intelligently identifies policy issues to provide policy optimization suggestions.

Last analysis time:2023-03-13 19:32:48

□	Issue Level	Issue Type	描述	Operation
□	allow_all			Ignore Handle
	Major Issue	任意权限	该策略允许任何源到任何目的数据包转发，权限过大	

12.4 Checking the Operation Status

Standards

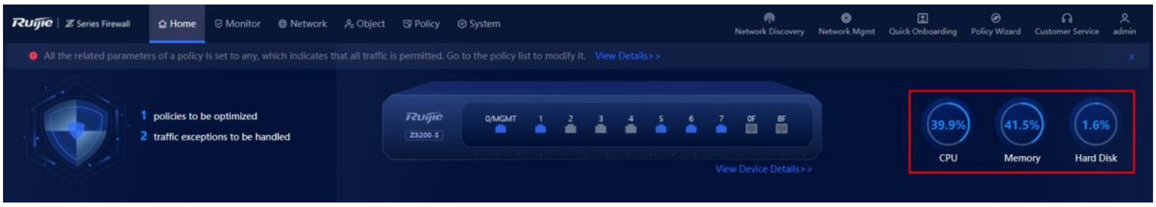
- Ensure that the CPU usage is lower than 75% during the service peak period. If the CPU usage of the firewall is too high, it may be encountered with attacks or abnormal traffic. In this case, the firewall stops forwarding data or discards packets and the firewall cannot be managed.
- Ensure that the memory usage is lower than 75% during the service peak period. If the memory usage of the firewall is too high, it may be encountered with attacks or abnormal traffic, or the number of abnormal concurrency is too high, which causes firewall exceptions.

Precautions

- The possible causes for high CPU usage are as follows:
  - The output of the **top** command indicates that some processes consume high CPU.
  - The UTM security function is enabled.
  - Abnormal traffic from attackers such as DDoS and broadcast storm exists.
- The possible causes for high memory usage are as follows:
  - The output of the **top** command indicates that some processes consume high memory.
  - The UTM security function is enabled.
  - The idle memory (cached or swap) is used to improve the system performance, which has no impact on services. You can run the **show memory** command to view the memory allocation information.

Method

Log in to the web management page and click **Home** to view the CPU usage and memory usage.



All the related parameters of a policy is set to any, which indicates that all traffic is permitted. Go to the policy list to modify it.

1 policies to be optimized

2 traffic exceptions to be handled

12.5 Checking the System Status

Standards

- Check whether the NTP server is configured and whether the time zone is correct.
- Confirm that the customer has purchased a license for the upgrade service and the license is still valid.

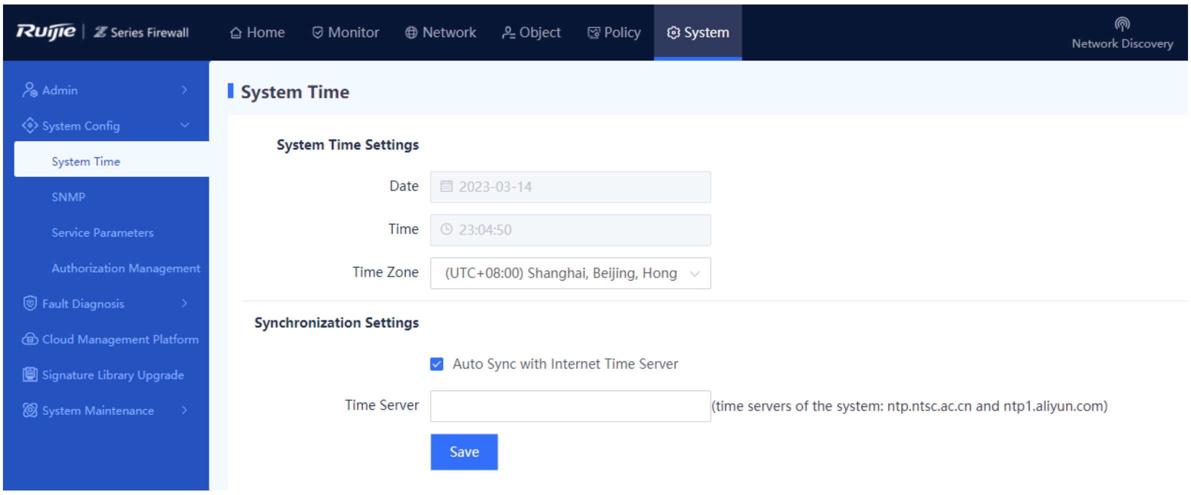
Precautions

Confirm that the customer has purchased the relevant license.

Method

(1) Check whether the system time is accurate.

Log in to the web management page and choose **System** > **System Config** > **System Time**.



System Time

System Time Settings

Date: 2023-03-14

Time: 23:04:50

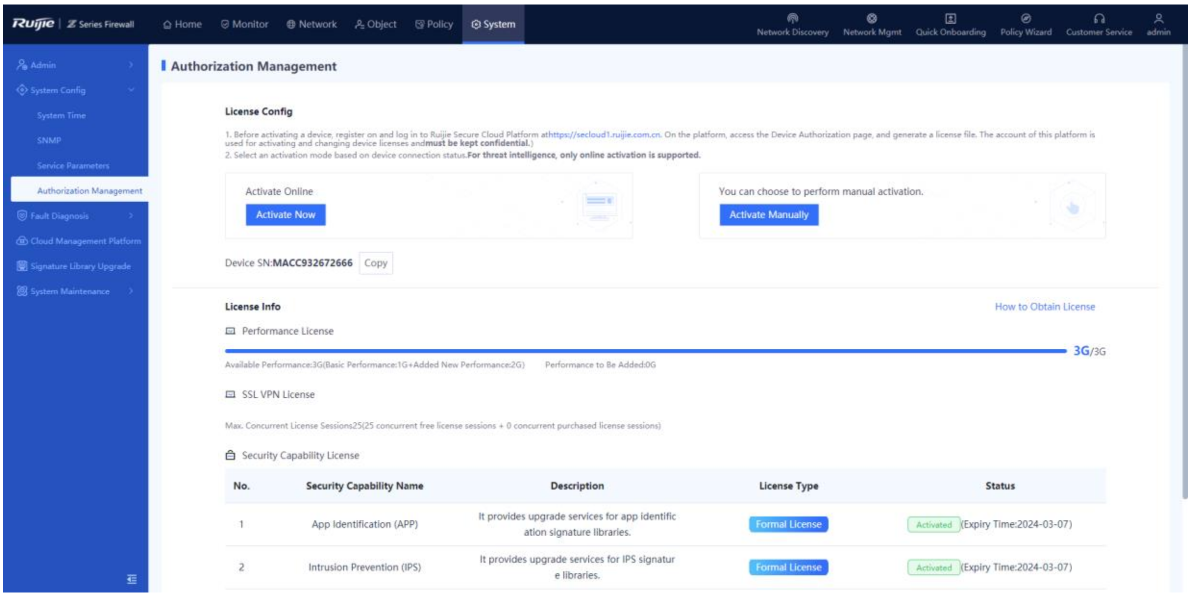
Time Zone: (UTC+08:00) Shanghai, Beijing, Hong

Synchronization Settings

☑ Auto Sync with Internet Time Server

Time Server: (time servers of the system: ntp.ntsc.ac.cn and ntp1.aliyun.com)

(2) Check the license status to confirm that the purchased license for the upgrade service is still valid.



Authorization Management

License Config

1. Before activating a device, register on and log in to Ruijie Secure Cloud Platform athttps://secloud1.ruijie.com.cn. On the platform, access the Device Authorization page, and generate a license file. The account of this platform is used for activating and changing device licenses and**must be kept confidential.**)

2. Select an activation mode based on device connection status.**For threat intelligence, only online activation is supported.**

Activate Online
Activate Now

You can choose to perform manual activation.
Activate Manually

Device SN:**MACC932672666** Copy

License Info
How to Obtain License

Performance License
3G/3G
Available Performance:3G(Basic Performance:1G+Added New Performance:2G) Performance to Be Added:0G

SSL VPN License
Max. Concurrent License Sessions25(25 concurrent free license sessions + 0 concurrent purchased license sessions)

Security Capability License

No.	Security Capability Name	Description	License Type	Status
1	App Identification (APP)	It provides upgrade services for app identification signature libraries.	Formal License	Activated (Expiry Time:2024-03-07)
2	Intrusion Prevention (IPS)	It provides upgrade services for IPS signature libraries.	Formal License	Activated (Expiry Time:2024-03-07)

12.6 Checking the Log Status

Standards

- If no hard disk is available, logs cannot be stored for 180 days.
- If no hard disk is available and no Syslog server is configured, the required storage time cannot be satisfied.

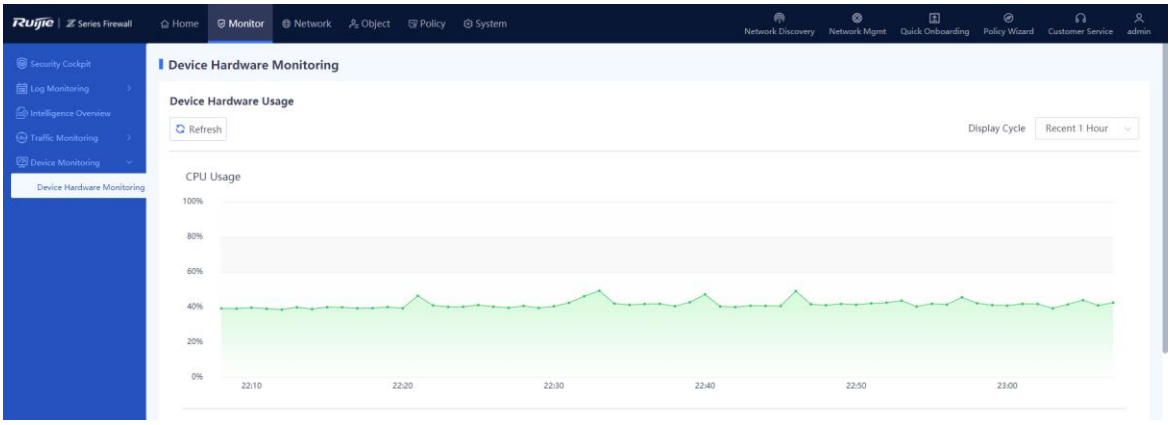
Precautions

- Confirm that the customer has purchased a hard disk.
- If no hard disk is available, the Syslog server is configured.

Method

(1) Check whether a hard disk is available.

- Log in to the web management page and choose **Monitor** > **Device Monitoring** > **Device Hardware Monitoring**.

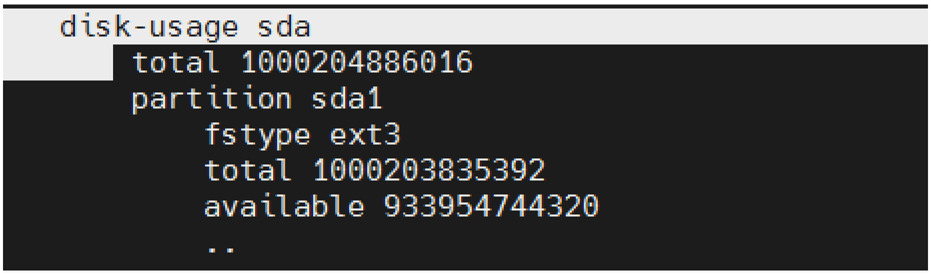


Device Hardware Monitoring

Device Hardware Usage

Display Cycle Recent 1 Hour

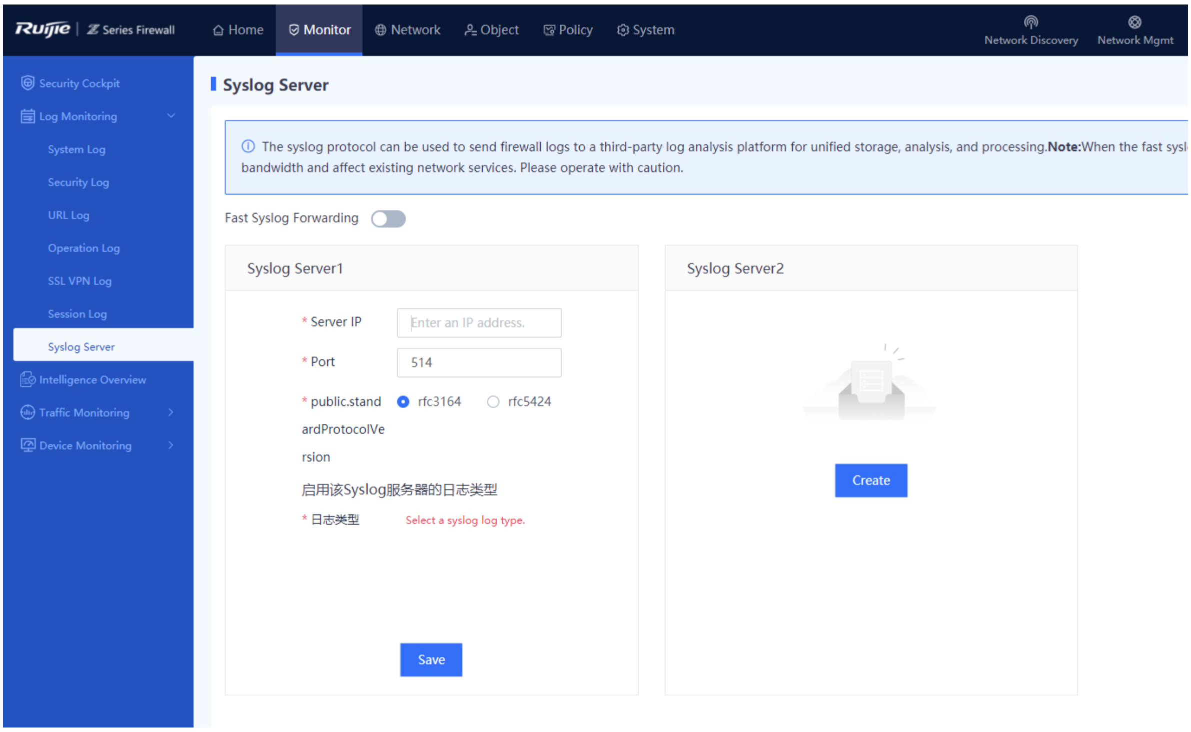
- Run the **firewall> show state system linux** command in the CLI.



```
    disk-usage sda
        total 1000204886016
        partition sda1
            fstype ext3
            total 1000203835392
            available 933954744320
            ..
```

(2) Check whether the Syslog server is configured and whether Syslog recording is enabled.

Log in to the web management page and choose **Monitor** > **Log Monitoring** > **Syslog Server**.



Syslog Server

ⓘ The syslog protocol can be used to send firewall logs to a third-party log analysis platform for unified storage, analysis, and processing.**Note:**When the fast sysl bandwidth and affect existing network services. Please operate with caution.

Fast Syslog Forwarding ○

Syslog Server1

* Server IP: Enter an IP address.
* Port: 514
* public.standardProtocolVersion: ● rfc3164 ○ rfc5424

启用该Syslog服务器的日志类型

* 日志类型: Select a syslog log type.

Syslog Server2

12.7 Checking the Network Connectivity

Standards

Use the traceroute method to check the network connectivity and data forwarding path. The purpose is to test the consistency of each path in the forward and reverse directions in the routing design. Specify a test plan according to the network planning in advance.

(1) Select typical test items according to the actual service routes of the customer.

(2) Suggestion: Test packets of the lengths 500, 2000, and 65000 to ensure that packets of different sizes can be normally forwarded.

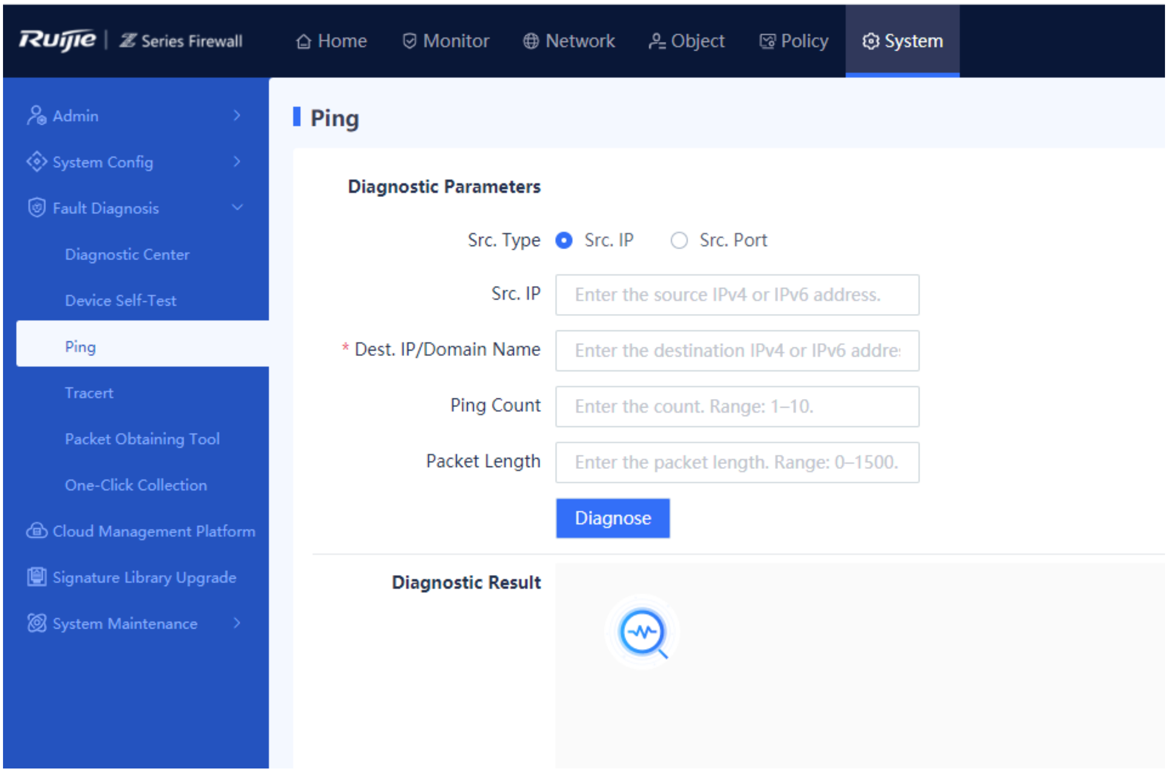
Note

ICMP filtering is enabled on some network devices by default. When you perform the preceding operations on these devices, packet loss may occur periodically. You are advised not to set the destination address to the device IP address during the execution.

Method

Check the service paths and then check the interface negotiation status after a certain time of delay.

Perform the traceroute or ping test on the web management page to check the connectivity of an Internet access device in the LAN.



Src. Type ● Src. IP ○ Src. Port

Src. IP: Enter the source IPv4 or IPv6 address.

* Dest. IP/Domain Name: Enter the destination IPv4 or IPv6 addre

Ping Count: Enter the count. Range: 1–10.

Packet Length: Enter the packet length. Range: 0–1500.

12.8 Checking the Service Use Status

Method

Select a typical service system to perform subjective inspection on the service application use.

Standards

Verify the network deployment correctness through real service testing.

Check the application service use of the customer and check whether the software service system is normal.

- Internet services: Web browsing, file downloading, QQ, email, online video watching, and other service system access
- Internal customer services: Video conference and OA office. Test specific application services involved in the customer site.